ROYAUME DU MAROC
Université Mohammed V - RABAT -
جامعة محمد الخامس – الرباط –
Faculté des sciences
كلية العلوم
CENTRE D'ÉTUDES DOCTORALES - SCIENCES ET TECHNOLOGIES

N° d'ordre : 3854

THÈSE

En vue de l'obtention du : ***DOCTORAT***

Structure de Recherche : Equipe de Science de la Matière et du Rayonnement.
Discipline : Physique.
Spécialité : Physique Théorique.

Présentée et soutenue le 13/10/2023 par :

Hasnaa HAJJI

Distribution semi-quantique de clés : sécurité et résistance aux stratégies d'interception

JURY

Yassine HASSOUNI	PES, Université Mohammed V de Rabat, Faculté des Sciences.	Président
Hamid EZ-ZAHRAOUY	PES, Université Mohammed V de Rabat, Faculté des Sciences.	Rapporteur/Examinateur
Mohammed EL FALAKI	PH, Université Chouaïb Doukkali, Faculté des Sciences d'El Jadida.	Rapporteur/Examinateur
Rachid AHL LAAMARA	PH, Université Mohammed V de Rabat, Faculté des Sciences.	Rapporteur/Examinateur
Saad RFIFI	PH, Université Abdelmalek Essâadi, Faculté Polydisciplinaire de Larache.	Examinateur
Eleni DIAMANTI	Professeur, Université de Paris, Sorbonne.	Examinateur
Morad EL BAZ	PES, Université Mohammed V de Rabat, Faculté des Sciences.	Directeur de thèse

Année Universitaire : 2023/2024

À ma mère,

Remerciements

Ce travail de thèse a été accompli au sein de l'Équipe de Science de la Matière et du Rayonnement sous la direction de Monsieur **Morad EL BAZ**, Professeur de l'Enseignement Supérieur à la Faculté des Sciences de l'Université Mohammed V de Rabat.

Mes remerciements s'adressent en premier lieu à mon Directeur de thèse, le Professeur **Morad EL BAZ**, qui a su tout au long de ce travail m'apporter un soutien continu, une disponibilité, une écoute, une confiance ainsi que des conseils précieux et avisés à la hauteur de son expertise. Je tiens à lui adresser ma sincère gratitude pour les nombreuses heures que nous avons passées à collaborer étroitement tout au long de cette recherche.

Ils s'adressent aussi à Monsieur **Yassine HASSOUNI**, Professeur de l'Enseignement Supérieur à la Faculté des Sciences de Rabat, pour l'honneur qu'il me fait en ayant accepté de présider le jury.

Ils s'adressent également à Monsieur **Hamid EZ-ZAHRAOUY**, Professeur de l'Enseignement Supérieur à la Faculté des Sciences de Rabat, pour avoir accépté de donner de son temps pour rapporter ce travail de thèse et membre du jury.

Mes remerciements s'adressent aussi au Monsieur **Mohammed EL FALAKI**, Professeur Habilité à la Faculté des Sciences d'El Jadida, pour l'honneur qu'il me fait en prenant la charge de rapporteur de ce travail de thèse et membre du jury.

Je tiens également à témoigner toute ma reconnaissance à Monsieur **Rachid AHL LAAMARA**, Professeur Habilité à la Faculté des Sciences de Rabat, pour l'honneur qu'il me fait en acceptant d'être rapporteur de ce travail de thèse et membre du jury.

J'adresse également tous mes remerciements à Monsieur **Saad RFIFI**, Professeur Habilité à la faculté Polydisciplinaire de Larache, pour l'honneur qu'il me fait en participant à ce jury en tant que examinateur.

Mes vifs remerciements s'adressent à Madame **Eleni DIAMANTI**, Professeur à Sorbonne Université de Paris de m'avoir fait l'honneur de participer à mon jury de thèse en tant que examinateur.

Je tiens à exprimer ma profonde gratitude envers le Centre National de la Recherche Scientifique et Technique (CNRST) pour avoir financé cette recherche.

Je ne saurais terminer ces remerciements sans mentionner ma famille et mes parents. Cette thèse n'aurait pas abouti sans les encouragements et la tendresse qu'ils m'ont offerts. Je les remercie pour leur patience et leur compréhension. Aucun mot ne peut exprimer la profonde reconnaissance que je ressens à leur égard, alors je leur dis simplement merci du fond du cœur.

Résumé

La préservation de la confidentialité lors de la transmission des informations sensibles a constamment suscité une préoccupation significative au sein de la société. Avec l'avènement de l'ère numérique, de nouvelles stratégies ont été développées pour assurer la sécurité des échanges et pour préserver l'intégrité des données. Au milieu de ces approches innovantes, la distribution semi-quantique de clés a émergé en tant que méthode pleine de potentiel, provoquant ainsi un intérêt considérable dans le domaine de la sécurité de l'information. Le travail présenté dans cette thèse se focalise sur l'analyse et l'amélioration des protocoles de distribution semi-quantique de clés. Ce prototype implique la nécessite que l'un des utilisateurs dispose de ressources quantiques alors que l'autre utilisateur muni des capacités semi-quantiques.

Dans un premier temps, nous introduisons une vision globale sur la cryptographie classique allant des principes fondamentaux jusqu'aux algorithmes les plus utilisés. Puis nous retracons l'évolution de la distribution quantique des clés au fil du temps, nous présentons également une étude détaillée des protocoles couramment utilisés pour les qubits unique et pour les qubits intriqués. Ensuite, nous procédons à une analyse de la sécurité du protocole de distribution de clés semi-quantique en déterminant une borne inférieure sur le taux de clés. Cette borne inférieure dépendante du bruit présent dans le canal quantique, un paramètre qui peut être précisément estimé par les parties légitimes. Cette analyse est menée en utilisant des états quantiques tridimensionnels et quadridimensionnels, et ce, dans le contexte d'une évaluation de leur résistance aux attaques collectives.

Par la suite, nous orientons notre attention vers l'étude d'une stratégie optimale d'interception. Cette approche repose sur la quantification de l'information mutuelle partagée entre Alice et Eve, en prenant en considération une perturbation prédéfinie. Nous visons ensuite à calculer la probabilité de réussite d'une écoute clandestine, en fonction du taux d'erreur résultant de cette interception. Finalement, notre recherche se concentre sur l'évaluation de la robustesse du protocole de distribution semi-quantique de clés contre une stratégie d'interception individuelle appliquée aux ensembles d'états bidimensionnels soumis à une altération par un bruit blanc.

Mots Clés : Information quantique, Sécurité des protocoles semi-quantiques, cryptographie classique, distribution de clé quantique.

Abstract

Preserving confidentiality during the transmission of sensitive information has always been a significant concern within society. With the advent of the digital age, new strategies have been developed to ensure secure exchanges and maintain data integrity. Amidst these innovative approaches, semi-quantum key distribution has emerged as a promising method, garnering considerable interest in the field of information security. The work presented in this thesis focuses on analyzing and enhancing semi-quantum key distribution protocols. This prototype involves the requirement that one user possesses quantum resources while the other user has semi-quantum capabilities.

Initially, we provide an overview of classical cryptography, ranging from fundamental principles to widely used algorithms. Then, we trace the evolution of quantum key distribution over time, presenting a detailed study of protocols commonly used for single qubits and entangled qubits. Subsequently, we undertake a security analysis of the semi-quantum key distribution protocol by establishing a lower bound on the key rate. This lower bound depends on the noise present in the quantum channel, a parameter that can be precisely estimated by legitimate parties. This analysis is conducted using three-dimensional and four-dimensional quantum states, within the context of evaluating their resilience against collective attacks.

Later, we turn our focus towards analyzing an optimal interception strategy. This approach is based on quantifying the mutual information shared between Alice and Eve, while considering a predefined perturbation. Then we aim to calculate the probability of successful eavesdropping, based on the error rate resulting from this interception. Finally, our research centers on evaluating the robustness of the semi-quantum key distribution protocol against an individual interception strategy applied to sets of two-dimensional states subjected to the addition of quantum noise.

Key Words : Quantum information, semi-quantum protocol security, classical cryptography, quantum key distribution.

Liste des publications

Durant la période de réalisation de ce manuscrit, les résultats obtenus ont engendré les publications suivantes :

1. **Qutrit-based semi-quantum key distribution protocol**
   Hasnaa Hajji, Morad El Baz
   Publication : Quantum Information Processing (2021).
   Preprint : arXiv :2101.02583.

2. **Mutually unbiased bases in 3 and 4 dimensions semi-quantum key distribution protocol**
   Hasnaa Hajji, Morad El Baz
   Publication : PhysicsLettersA426 (2022).
   Preprint : arXiv :2208.03548.

3. **Optimal eavesdropping in semi-quantum key distribution with Three-Dimensional Quantum States.** En cours de soumission
   Hasnaa Hajji, Morad El Baz

4. **Optimal eavesdropping on noisy states in semi-quantum key distribution.** En cours de soumission
   Hasnaa Hajji, Morad El Baz

Liste des abbreviations

- **J.-C** : Jésus-Christ.
- **NBS** : National Bureau of Standards.
- **NIST** : National Institute of Standards and Technology.
- **DES** : Data Encrytion Standard.
- **NSA** : National Security Agency.
- **AES** : Advanced Encryption Standard.
- **CAIN** : Confidentialité, Authentification, Intégrité, Non-répudiation.
- **ECB** : Electronic CodeBook.
- **CFB** : Cipher FeedBack.
- **CBC** : Cipher Block Chaining.
- **OFB** : Output FeedBack.
- **RSA** : Ronald L. Rivest, Adi Shamir et Leonard M. Adleman.
- **PGP** : Pretty Good Privacy.
- **UEP** : Unequal Error Protection.
- **OSA** : Optical Society of America.
- **QKD** : Quantum Key Distribution.
- **OTP** : One-Time Pad.
- **USD** : Unambiguous State Discrimination.
- **QKD** : Quantum Key Distribution.
- **EPR** : The Einstein–Podolsky–Rosen paradox.
- **CHSH** : John Clauser, Michael Horne, Abner Shimony, and Richard Holt.
- **BB84** : The Bennett-Brassard 1984 protocol.
- **B92** : Charles Bennett 1992 protocol.
- **E91** : Artur Ekert 1991 protocol
- **BBM92** : Charles H. Bennett , Gilles Brassard and N. David Mermin 1992 protocol.
- **IBM** : The International Business Machines Corporation.
- **SQKD** : Semi Quantum Key Distribution.
- **BKM07** : Michel Boyer, Dan Kenigsberg and Tal Mor 2007 protocol.
- **BGKM09** : Michel Boyer, Ran Gelles, Dan Kenigsberg and Tal Mor 2009 protocol.
- **QBER** : The Quantum Bit Error Rate.
- **MUBs** : Mutually Unbiased Bases.

Table des figures

Table des matières

Introduction

Depuis l'antiquité, l'homme a ressenti la nécessité de préserver la confidentialité des informations personnels ou d'échange des confidences. En réponse à cette nécessité, des méthodes primitives ont été élaborées, donnant lieu à l'émergence de la cryptographie en tant que science dédiée à la sécurité des données.

Dès l'époque du chiffrement de César jusqu'à l'utilisation actuelle du chiffrement asymétrique, en passant par la machine Enigma [1] qui a joué un rôle crucial lors de la Seconde Guerre mondiale, la cryptographie a toujours reposé sur la préservation des informations confidentielles partagées entre les utilisateurs, afin de faciliter des communications confidentielles. Cet aspect fondamental de la cryptographie a permis d'établir des protocoles sécurisés, garantissant ainsi la confidentialité des échanges et la protection des données sensibles.

Cette science ancienne repose sur le processus de chiffrement des données sensibles en les combinant avec une clé de chiffrement avant leur transmission, dans le but de garantir leur protection. Ce procédé de sécurisation empêche toute tentative d'accès non autorisé à ces données chiffrées, à moins que l'individu malveillant ne dispose de la clé de chiffrement appropriée. Le destinataire autorisé à ces données, étant en possession de la clé correspondante, est en mesure d'effectuer le processus de déchiffrement, ramenant ainsi les données à un état intelligible.

Actuellement, le domaine du chiffrement offre une variété considérable d'algorithmes. La sécurité de ces méthodes dépend largement de la longueur de la clé utilisée. Une clé plus longue confère une protection renforcée, rendant la tâche de déchiffrement des données par des tiers malveillants beaucoup plus compliquée. L'un des algorithmes les plus répandus est le Data Encryption Standard (DES) [2]. Cependant, en raison de sa vulnérabilité face aux avancées technologiques, notamment l'utilisation d'ordinateurs puissants, il n'est plus considéré comme suffisamment sûr. Afin de préserver l'intégrité des données sensibles, le Data Encryption Standard est progressivement remplacé par l'Advanced Encryption Standard (AES) [3]. Ce dernier utilise des clés de 256 bits, garantissant un niveau de protection considérablement plus élevé, même face aux capacités de calcul actuelles des superordinateurs.

Un deuxième facteur déterminant la sécurité de ces méthodes de chiffrement est le volume des données chiffrées sous une clé spécifique. En effectuant des changements fréquents de la clé, un individu malveillant tentant de déchiffrer ces données se retrouve avec un accès limité à l'information, réduisant ainsi considérablement les ressources disponibles pour sa tentative de déchiffrement. Lorsque la clé utilisée a la même longueur que le message et qu'elle n'est employée qu'une seule fois, la sécurité atteint un niveau absolu. Cette méthode, connue sous le nom « One-Time-Pad » en anglais [4], se distingue comme étant la seule à offrir une telle garantie de sécurité. En revanche, dans les autres cas, un individu malveillant dispose toujours de la possibilité d'explorer séquentiellement toutes les clés disponibles. Cependant, l'efficacité de cette recherche dépend largement de la longueur de la clé, car une clé suffisamment longue rend cette tentative compliquée et pratiquement irréalisable.

De ce fait, la sécurité du processus du chiffrement repose entièrement sur la confidentialité de la clé utilisée. Pour garantir cette confidentialité, il est essentiel d'utiliser un processus de génération de clé sécurisé et de s'assurer son échange entre les parties autorisées, de manière à éviter toute interception par un individu malveillant. Ce défi, identifié sous le nom de "problème de distribution de la clé", est un aspect fondamental en cryptographie, nécessitant une attention particulière et des solutions adaptées pour garantir la protection des communications confidentielles.

Pendant de nombreuses années, l'idée prédominante était que la seule méthode exploitable pour résoudre le problème de distribution de clés consistait à réaliser un échange de supports physiques. Cependant, à l'époque de la révolution numérique, cette solution s'avère clairement peu pratique. De plus, il reste difficile de garantir l'absence d'interception par des individus malveillants.

À la fin des années soixante et au milieu des années soixante-dix, des chercheurs ont élaboré une nouvelle approche. Cette approche conventionnelle repose sur l'utilisation des algorithmes de cryptographie à clé publique, impliquant l'usage de deux clés distinctes. Une clé désignée comme publique est utilisée pour le chiffrement des données, tandis qu'une seconde clé, connue comme privée, employée uniquement dans le processus de déchiffrement. Étant donné que les algorithmes de cryptographie à clé publique sont fondés sur des problèmes mathématiques complexes, par exemple la factorisation de nombres entiers, leur vitesse d'exécution est relativement lente par rapport aux algorithmes de cryptographie à clé privée. Ainsi, leur principal domaine d'application réside dans l'échange sécurisé de clés, qui seront ultérieurement utilisées pour le chiffrement avec des algorithmes tels que DES ou AES. Cependant, les algorithmes de chiffrement à clé publique présente deux vulnérabilités majeurs.

Vulnérabilité au progrès technologique : inverser une fonction à sens unique est possible, à condition de disposer d'un temps suffisant. Les ressources requises pour briser ces algorithmes, que ce soit en termes de puissance de calcul ou de temps, varient en fonction de la longueur de la clé utilisée. Ces algorithmes de chiffrement à clé publique sont également vulnérables face à un ordinateur quantique. En effet, il y a environ une quinzaine d'année,

un algorithme efficace pour factoriser des nombres entiers sur un ordinateur quantique a été inventé. Une fois qu'un tel ordinateur sera effectivement développé, cet algorithme pourra être utilisé pour compromettre les algorithmes de cryptographie à clé publique.

Cette vulnérabilité potentielle met en évidence la nécessité d'explorer des solutions de sécurité innovantes, ce qui nous amène à la cryptographie post-quantique. Cette nouvelle ère de la cryptographie s'impose comme la réponse proactive à la menace que représentent les ordinateurs quantiques, en élaborant des protocoles et des techniques de chiffrement conçus pour résister à ces défis. Au cœur de cette évolution, la cryptographie post-quantique offre une perspective prometteuse pour garantir la confidentialité et l'intégrité des données dans un monde où la technologie continuent de s'élargir.

Vulnérabilité au progrès théorique : la deuxième vulnérabilité des algorithmes de cryptographie à clé publique provient du manque de preuve formelle établissant l'impossibilité d'inverser les fonctions à sens unique. Malgré les efforts de nombreux spécialistes de la théorie des nombres, il reste incertain si un algorithme permettant de factoriser rapidement un grand nombre au moyen d'un ordinateur usuel existe.

En effet, ces deux vulnérabilités représentent une menace sérieuse, ce qui met en évidence l'importance du développement de nouvelles techniques de distribution de clés cryptographiques. Désormais, la cryptographie revêt une importance cruciale dans de nombreux domaines de notre quotidien. Elle est présente dans les cartes bancaires, les envois d'e-mails, les transactions sur internet, le paiement en ligne, le passeport biométrique,...etc. Elle est également utilisée dans le domaine du contrôle d'accès, permettant des fonctionnalités telles que le déverrouillage à distance des véhicules.

Toutefois, face aux avancées de l'informatique, la sécurité des méthodes de cryptographie, qui reposent essentiellement sur des problèmes mathématiques réputés difficiles, demeure un défi constant. Effectivement, la sécurité offerte par ces méthodes de cryptographie peut être mise en doute lorsqu'il s'agit de garantir la confidentialité des données sur le long terme. Cette vulnérabilité permettrait à un adversaire de conserver des données chiffrées en attendant l'arrivée de la technologie nécessaire pour leur déchiffrement. C'est dans ce contexte que l'exploitation des principes de la mécanique quantique pour traiter de l'information, et en particulier la cryptographie quantique, se présente comme une solution prometteuse pour résoudre le problème de la distribution des clés de chiffrement et garantir ainsi une sécurité inconditionnelle de la communication et des échanges de données.

Le concept fondamental de la cryptographie quantique repose principalement sur l'utilisation des lois fondamentales de la mécanique quantique pour distribuer des clés cryptographiques. Ainsi, le terme de «distribution quantique de clé» constitue une appellation plus exacte pour cette technique. Les clés secrètes ainsi générées sont ensuite utilisées pour le chiffrement des communications à l'aide de protocoles de cryptographie classique. L'association de la cryptographie classique et la cryptographie quantique offre ainsi de nouvelles opportunités pour la protection des informations confidentielles.

Le principe qui sous-tend la distribution quantique de clé est basé sur le principe d'incertitude d'Heisenberg, l'un des principes fondamentaux de la physique quantique. Ce principe souligne que toute mesure effectuée sur un système quantique perturbe intrinsèquement l'état de ce système, ce qui signifie qu'il est impossible de réaliser une mesure sans influencer l'objet mesuré. Dans le contexte de la distribution quantique de clé, cela permet de détecter la présence d'un espion potentiel dans un réseau sécurisé. Lorsqu'un système quantique est utilisé comme support d'un bit d'information, toute tentative d'interception par un tiers entraîne une perturbation. Cette perturbation engendre des erreurs dans les échanges de bits entre les parties légitimes. Il convient de noter que la vérification intervient après l'échange d'information, ce qui implique que la détection de la présence d'un espion ne peut se faire qu'a posteriori. En conséquence, cette approche est adoptée pour l'échange de clés plutôt que pour celui des données. Une fois la confidentialité de la clé vérifiée, elle peut être employée en toute sécurité pour le chiffrement des données.

De nos jours, il est tout à fait possible d'utiliser la cryptographie quantique en conditions réelles, ce qui signifie que cette technologie peut être mise en œuvre en dehors des laboratoires de recherche pour sécuriser les communications dans des environnements pratiques et réels. Les premières démonstrations de distribution quantique de clés ont eu lieu dans les années 90, depuis lors, la technologie a connu des améliorations progressives visant à accroître son débit, mesuré par le nombre de bits de clés échangés par seconde, et à étendre sa transmission. Ces avancées ont joué un rôle essentiel dans le développement et la maturité de la cryptographie quantique en tant que technologie viable pour la sécurité de l'information.

En 2003, *id Quantique*, une entreprise basée à Genève, a réalisé la première implémentation de la cryptographie quantique dans des équipements commerciaux dédiés à la sécurité de l'information. Ces avancées majeures dans le domaine de la cryptographie quantique ouvrent la voie à des applications pratiques pour sécuriser les communications dans des environnements réels, renforçant ainsi la sécurité des données dans notre ère numérique de plus en plus interconnectée et vulnérable aux menaces cybernétiques.

Bien que la cryptographie quantique offre une sécurité inconditionnelle, elle requiert une infrastructure spécifique et des équipements avancés, telles que les ordinateurs quantiques et les réseaux quantiques...etc. Toutefois, de nombreux autres défis doivent être relevés pour une adoption plus large de cette technologie, tels que les coûts de mise en œuvre, l'interopérabilité avec les infrastructures existantes et la scalabilité à grande échelle.

Par ce biais, Boyer et al. ont introduit une approche novatrice [5], connu sous le nom de "distribution semi-quantique de clés", qui combine des composants classiques avec des infrastructures moins coûteuses que celles nécessaires à la mise en œuvre de la cryptographie quantique. L'objectif principal de cette approche est de faciliter la distribution de clés cryptographiques tout en maintenant un niveau de sécurité satisfaisant.

La distribution semi-quantique de clés (SQKD) est conçue pour assurer une distribution de clés sécurisée entre les parties en communication. L'une des particularités de cette dernière est que la nature des utilisateurs peut être hétérogène, certains pouvant être classiques et d'autres quantiques. Les capacités quantiques sont indispensables pour l'expéditeur, tandis que le destinataire peut se contenter de capacités classiques. Plus précisément, l'expéditeur réalise différentes opérations, telles que la préparation d'états quantiques, la réalisation de mesures quantiques et le stockage d'états quantiques. De son côté, le récepteur effectue également plusieurs opérations, notamment la préparation de nouveaux qubits, la mesure des qubits, l'arrangement ordonné des qubits et la transmission des qubits sans perturber les canaux quantiques. Cette approche offre une alternative intéressante en termes de ressources quantiques nécessaires pour garantir la sécurité de la distribution des clés.

Depuis l'introduction de la distribution semi-quantique de clés, de nombreux scientifiques et chercheurs ont étudié de nombreuses variantes de systèmes de distribution semi-quantiques de clés (SQKD) au cours des années. Ces protocoles ont suscité un intérêt particulier en raison de leur tentative de réduire les exigences en ressources quantiques nécessaires. Boyer et al. [5] ont apporté une contribution significative avec un protocole réalisable reposant sur des systèmes à quatre niveaux. Xian-Zhou et al. [6] ont conçu et validé la robustesse d'un protocole destiné à distribuer des bits de clé entre une partie quantique et plusieurs parties classiques. Parallèlement, Jian et al. [7] ont proposé un protocole amélioré et sécurisé en utilisant des états intriqués, contribuant ainsi à l'avancement des protocoles de distribution de clés semi-quantiques. Zou et al. [8] ont développé un protocole SQKD robuste nécessitant moins de quatre états quantiques. Les chercheurs ont remarqué que le protocole utilisant un seul état quantique contient deux fois plus d'informations par rapport au le protocole de Boyer et al. [5].

Dans ses travaux, Krawec [9] a introduit des protocoles de distribution de clés semi-quantiques, basés sur un unique état quantique qui permettent d'utiliser des réflexions pour transporter des informations. Il a procédé à une analyse approfondie d'une attaque limitée par Eve et a démontré la robustesse du protocole. En outre, Krawec [10] a mis au point le protocole de distribution de clés semi-quantiques médiatisé, également connu sous le nom de protocole de distribution de clés quantiques multi-utilisateurs, permettant à deux utilisateurs classiques ou semi-quantiques limités d'établir une clé secrète en utilisant un serveur/centre quantique non fiable. Les résultats de l'étude ont démontré que le protocole semi-quantique offre une sécurité équivalente à celle du protocole quantique complet.

Dans leur publication, Lu et al. [11] ont développé un protocole basé sur l'expéditeur classique, autorisant à ce dernier d'envoyer des bits de clé encodés dans la base Z. Maitra et al. [12] ont procédé à l'analyse d'un schéma d'attaque bidirectionnelle visant à évaluer la sécurité d'un protocole SQKD. Dans une étude différente, Zhang et al. [13] ont apporté une preuve rigoureuse de la sécurité inconditionnelle du protocole de distribution de clés semi-quantique à état unique proposé par Zou et al. [14]

Dans ses recherches, Krawec [15, 16] a réalisé une analyse approfondie permettant de prouver la sécurité inconditionnelle du protocole semi-quantique développé par Boyer et al. [5]. Dans une autre étude, Iqbal et Krawec [17] ont mis en place un protocole de distribution de clés semi-quantiques utilisant des états quantiques de haute dimension et ont procédé à une analyse rigoureuse de sécurité pour évaluer sa robustesse face aux attaques potentielles. Ces travaux ont contribué à renforcer les bases de la distribution de clés semi-quantiques. En plus du protocole mentionné ci-dessus,le protocole de distribution de clés semi-quantiques a suscité l'intérêt de la communauté scientifique, attirant l'attention de divers chercheurs qui ont réalisé des travaux approfondis, [18–47], représentant une liste non exhaustive.

Ces recherches visent à déployer des solutions qui permettent une distribution de clés plus accessible tout en garantissant un niveau de sécurité satisfaisant, ouvrant ainsi la voie à de nouvelles perspectives dans le domaine de la sécurité de l'information, offrant des solutions potentielles pour les systèmes de communication où les ressources quantiques sont limitées ou difficiles à mettre en place. Cela pourrait être particulièrement bénéfique dans des environnements où des contraintes financières ou technologiques empêchent l'utilisation complète de la cryptographie quantique. Des recherches supplémentaires sont nécessaires pour explorer davantage les applications, les limites et les possibilités d'amélioration de cette approche prometteuse dans le contexte de la distribution de clés sécurisée.

En se fondant sur cette perspective, notre recherche se focalise sur l'analyse et l'amélioration des protocoles de distribution semi-quantique de clés. Notre travail consiste à évaluer la sécurité de ces protocoles face à diverses attaques. De plus, nous nous intéressons à l'optimisation des performances des protocoles de distribution semi-quantique de clés en prenant en compte des facteurs tels que la dimension, le taux de génération de clé sécurisée et leur résistance aux attaques. A travers ces résultats, nous visons à contribuer à l'avancement de la sécurité des systèmes de communication basés sur la distribution semi-quantique de clés.

Le manuscrit est organisé en trois chapitres de la manière suivante :

Chapitre 1 : La cryptographie classique.

Dans ce chapitre nous introduisons une perspective globale sur la cryptologie, allant des principes fondamentaux jusqu'aux algorithmes les plus utilisés. Nous présentons les repères historiques de la cryptographie en mettant en évidence les progrès réalisées au cours des siècles. Par ailleurs, nous abordons les différents types d'algorithmes de cryptographie, notamment les algorithmes à clé privée, qui utilisent une seule clé pour le chiffrement et le déchiffrement des messages, ainsi que les algorithmes à clé publique, qui reposent sur l'utilisation de paires de clés distinctes pour les opérations de chiffrement et de déchiffrement. En outre, nous poursuivons avec l'étude détailler du standard de chiffrement de données DES, du standard de chiffrement AES, du cryptosystème RSA, et le cryptosystème El Gamal. Enfin, nous concluons le chapitre avec les modèles d'attaques employés pour briser les systèmes cryptographiques.

Chapitre 2 : Distribution quantique de clé.

Nous commençons dans ce chapitre par retracer l'évolution de la distribution quantique de clés au fil du temps. Ensuite, nous introduisons les notions fondamentales de la mécanique quantique, telles que les états quantiques, la polarisation des photons et l'intrication, qui constituent les piliers sur lesquels repose à la distribution quantique de clés. L'objectif de cette approche est d'établir une clé secrète partagée entre deux parties de manière sécurisée. Nous présentons également le protocole générique de distribution quantique de clés et les ressources nécessaires à sa mise en œuvre. Par ailleurs, nous procédons à une étude détaillée des protocoles couramment utilisés, à savoir le protocole BB84, B92, Ekert 91 et le protocole BBM92, en analysant leur principe de fonctionnement et en évaluant leur niveau de sécurité. Pour clôturer ce chapitre, nous implémentons un algorithme d'extraction de clé secrète en utilisant l'environnement Python. Cet algorithme est basé sur les protocoles étudiés, en prenant en compte à la fois les scénarios avec et sans présence d'un espion.

Chapitre 3 : Distribution semi-quantique de clé.

Dans ce chapitre, nous traitons la sécurité des différents protocoles de distribution semi-quantique de clés. Nous commençons par présenter les préliminaires de la mécanique quantique ainsi que les différents concepts de la théorie de l'information, notamment l'information mutuelle, qui permet de quantifier l'information et de déterminer la quantité maximale pouvant être transmise par un canal bruité. Ensuite, nous décrivons les deux protocoles les plus connus de distribution semi-quantique de clés, à savoir BKM07 et BGKM09, qui ont été introduits respectivement par Boyer et al. en 2007 et 2009. Préalablement, nous introduisons le modèle générique du protocole de distribution quantique de clés. Nous nous concentrons sur l'étude de la robustesse des protocoles de distribution semi-quantiques de clés, en considérant des attaques d'écoute collective basés sur des systèmes de trois et quatre dimensions avec différentes bases mutuellement non biaisées. Par la suite, nous analysons une stratégie d'interception optimale pour le protocole de distribution semi-quantique de clés appliqué à des états quantiques tridimensionnels. Enfin, nous concluons avec une évaluation de la résistance du protocole de distribution semi-quantique de clés face à une stratégie d'interception individuelle pour un ensemble d'états bidimensionnels soumis à un mélange avec un bruit blanc.

Nous clôturons ce manuscrit par une synthèse du travail élaboré et quelques idées en perspective.

Une plus grande connaissance pourrait éclairer notre chemin.

Georges Lucas, La Guerre des Etoiles

1 La cryptographie classique

I La cryptologie

La cryptologie représente un ensemble de théories liées à la transmission de l'information. Étymologiquement, le terme « **cryptologie** » vient des mots grecs anciens : $\kappa\rho\upsilon\pi\tau\sigma\sigma$ `[kruptos]`, caché et $\lambda\sigma\gamma\sigma\sigma$ `[Logos]`, science, ce qui signifie la science du secert. Cette science a bénéficié d'un progrés scientifique important suite au développement de la société de l'information jusqu'à devenir un outil incontournable pour sécuriser les systèmes de l'information.

Traditionnellement la cryptologie est composée de deux branches indissociable. D'une part, **la cryptographie**, l'art de rendre l'information intelligible pour ceux qui ne sont pas habilités à en prendre connaissance. D'autre part, **la cryptanalyse**, l'art complémentaire consistant à analyser la résistance des méthodes cryptographique face à différentes attaques.

Ces deux branches de la cryptologie ont connu depuis l'existance de l'homme une concurrence, qui a permis une progression continue entre les deux disciplines. Évidemment il n' y a pas de cryptographie sans cryptanalyse et inversement.

II Terminologie

Mise en situation :

Les cryptologues ont la tradition de désignés les différents personnages intervenant dans les transmissions par les même prénoms. « **Alice** » expéditrice, très bavarde, souhaite envoyer des messages au destinataire « **Bob** », entiché d'Alice, à travers un canal

de communication sans qu'un tiers « **Eve** », l'adversaire d'Alice, espionnant leurs communications ne puisse connaitre le contenu des messages échangés.

Messages et chiffrement :

Alice transmet le message à Bob en utilisant un processus de **chiffrement** afin de transformer le message, le **texte clair** notée **M**, d'une manière à le rendre inintelligible. Le résultat de ce processus de chiffrement est appelé **texte chiffré**, ou encore **cryptogramme**, notée **C**. Le processus de chiffrement prend la forme d'une fonction mathématique notée $\mathcal{E}$:

$$\begin{array}{rccc} \mathcal{E}: & \mathcal{M} & \longrightarrow & \mathcal{C} \\ & M & \longmapsto & \mathcal{E}(M), \end{array}$$

où $\mathcal{M}$ est l'ensemble des textes clairs, et $\mathcal{C}$ est dénommé l'ensemble des textes chiffrés.

Bob de son côté réalise un processus de reconstruction : une opération inverse nommée **déchiffrement**, pour retrouver le texte clair originale à partir du texte chiffré C. Le processus de déchiffrement se fait à l'aide d'une autre fonction notée $\mathcal{D}$,

$$\begin{array}{rccc} \mathcal{D}: & \mathcal{C} & \longrightarrow & \mathcal{M} \\ & C & \longmapsto & \mathcal{D}(C) = \mathcal{D}(\mathcal{E}(M)). \end{array}$$

Il s'ensuit alors que pour tout élément M de $\mathcal{M}$ les opératitons, $\mathcal{E}()$ et $\mathcal{D}()$, ont pour but de vérifier l'identité suivante :

$$\mathcal{D}(\mathcal{E}(M)) = M.$$

Ces différents processus sont illustrés par la figure 1.1.

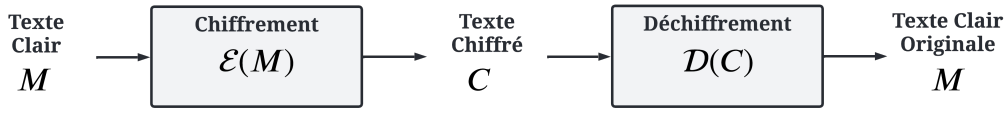


FIGURE 1.1 : Chiffrement et Déchiffrement.

III Repères historiques

L'histoire de la cryptologie s'amorce depuis des siècles ; ces premières traces semble être apparue environ 3 000 ans avant J.-C avec l'invention de l'écriture. C'est ce qui a fait de la cryptologie une science intimement liée à l'histoire de l'homme et qui a mis des siècles pour prendre forme.

L'histoire de la cryptologie retrace une époque dans laquelle une bataille acharnée s'est livré entre les cryptographes et les cryptanalystes. En effet, les évolutions des méthodes d'attaques permettent aux cryptographes de concevoir des moyens pour dissimuler le sens d'un message plus résistants et, à l'inverse, la résistance de ces moyens motive l'imagination des cryptanalystes à retrouver le sens caché d'une succession erratique de lettres, voir Fig. 1.2.

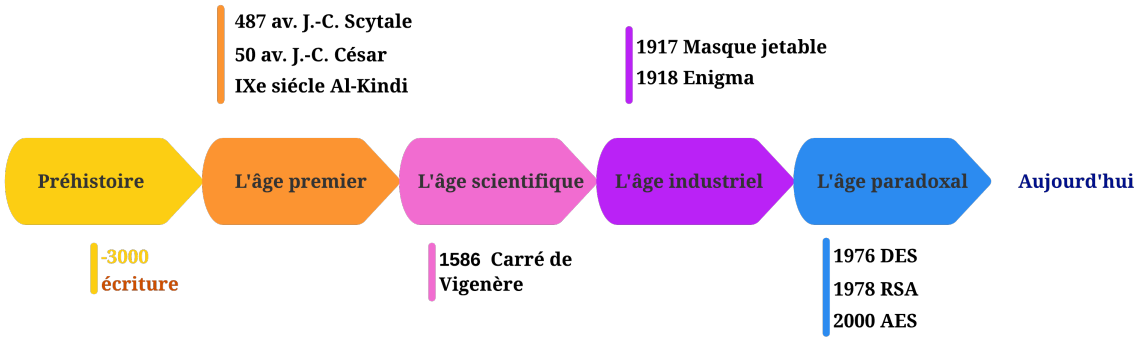


FIGURE 1.2 : Chronologie de l'histoire de la cryptographie.

L'âge premier :

Les plus anciens formes des techniques permettant de rendre une information illisible fut utilisé au temps de l'Eqypte ancienne. A cette époque, un scribe égyptien utilise des hiéroglyphes non conformes racontant la vie de son seigneur. L'intention n'était pas de rendre un texte secret mais plutôt de lui attribuer une dignité et une autorité.

Quelques siècles plus tard, les grecs ont développé une méthode originale pour l'échange de messages secrets. Celle-ci est basée sur un bâtonnet appelé la « **scytale** », un axe de bois autour duquel on enroulait une bande de cuir, une bandelette, sur laquelle on écrivait le message. Une fois la bandelette déroulée, le message devenait incompréhensible. Sans la connaissance du diamètre de la scytale, il était impossible de déchiffrer le message.

FIGURE 1.3 : Une scytale.

Les méthodes de cryptage de ce type, qui consistent à changer l'ordre des lettres, entrent dans la catégorie du **chiffrement par transposition**.

Au 1er siècle avant J.-C, l'empereur romain, Jules César a employé une technique modeste pour les communications gouvernementales secrètes. Il s'agit d'une **substitution monoalphabétique** définie par un décalage des 26 lettres de l'alphabet d'un certain nombre de pas, généralement 3 pas vers la droite. Autrement dit, avec un décalage de 3 pas, *A*

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
↓ ↓
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

serait remplacé par *D*, *B* par *E*, *C* par *F* ... etc. Ainsi le message « *Bonsoir BOB, Tout va bien !* » devient « *Erqvrlu ERE, Wrxw yd elhq* » comme illustré sur la figure 1.4.

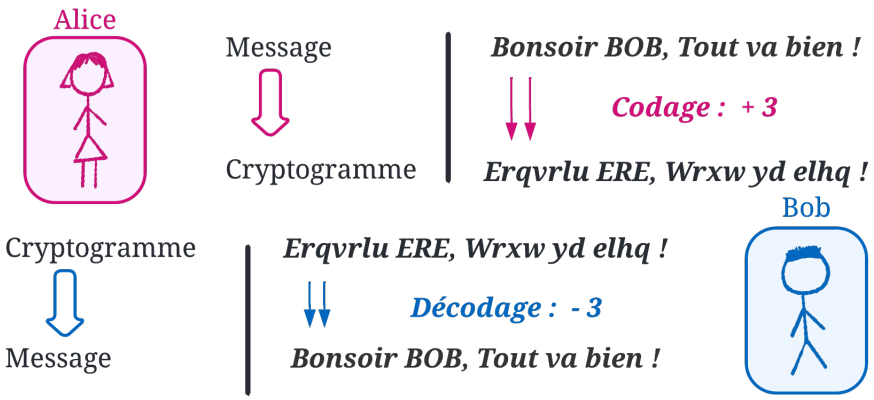


FIGURE 1.4 : Chiffrement de César.

Bien que le résultat semble tout à fait incompréhensible, la sécurité offerte par ce système de cryptage se révéla très limitée puisqu'il n'offre que 25 manières possibles pour crypter un message. Toutefois, il est toujours un bon exemple pédagogique utilisé que par les écoliers pour introduire les principes cryptographiques.

La substitution monoalphabétique a résisté plusieurs siècles à la perspicacité des cryptanalystes jusqu'à ce que le savant arabe Abu Yusuf al-Kindi mette au point, au IXème siècle, une technique appelée **analyse des fréquences**.

Al-Kindi a remarqué que selon la langue, chaque lettre est employée à une fréquence particulière (voir Fig. 1.5), par exemple dans un texte écrit en français, il y a presque toujours beaucoup plus de E que de W ! Il y a donc de fortes chances pour que, dans un texte chiffré, la lettre qui apparaît le plus fréquemment représente un E. Les lettres les moins fréquentes représentent probablement W ou K ou X, etc.

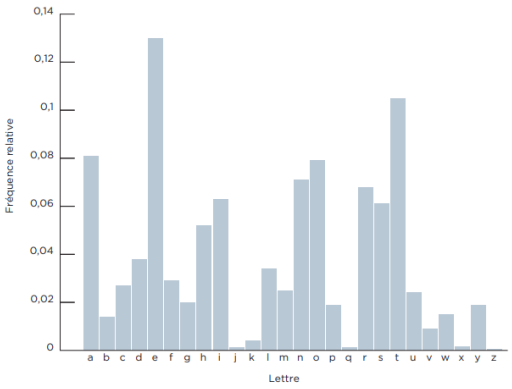


FIGURE 1.5 : Diagramme de fréquence des lettres françaises.

L'âge scientifique :

L'âge scientifique représente une période charnière pour le développement des méthodes cryptographiques. Ce fut en effet l'époque où les chiffrements à substitution monoalphabétique devinrent vulnérables, engendrant par là même l'apparition de nouvelles méthodes.

Vers 1465, Leon Battista Alberti inventa le premièr chiffrement par **substitution polyalphabétique** qui, comme son nom l'indique, faisait intervenir de multiples substitution des alphabets.

Il ouvrit ainsi la voie à une succession d'innovations dans ce domaine, dont la plus marquante fut celle du Français Blaise de Vigenère, aussi connue sous le nom de « **Chiffrement de Vigenère** » [48].

Ce chiffrement, résistant aux attaques pendant plusieurs siècles, repose sur une matrice de 26×26 cases, appelée « **carré de Vigenère** », voir Fig. 1.6, dont chaque ligne contient l'alphabet décalé d'une lettre par rapport à la ligne précédente [49]. Les lignes servent à choisir les lettres du texte clair, et les colonnes correspondantes aux lettres de la clé. Les intersections entre ces lignes et colonnes fourniront les lettres à utiliser dans le texte chiffré, voir Fig. 1.7.

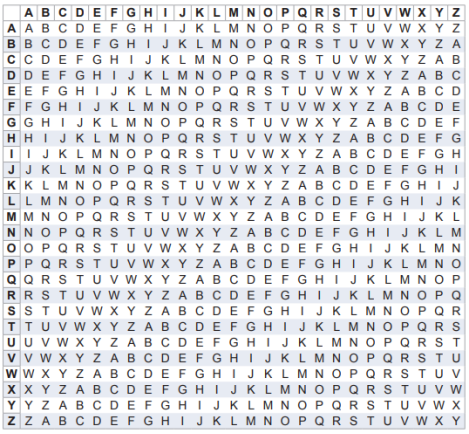


FIGURE 1.6 : Carré de Vigenère.

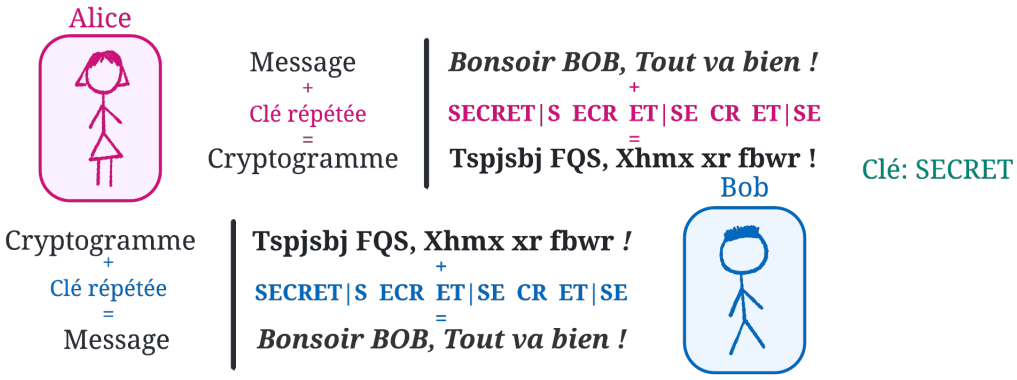


FIGURE 1.7 : Chiffrement de Vigenère.

L'avantage de cette méthode réside dans le fait, qu'en fonction de la clé, une lettre du texte chiffré correspond à plusieurs lettres du texte clair, ainsi l'analyse des fréquences se révèle inefficace et les failles du chiffrement par substitution monoalphabétique sont palliées.

Ce chiffrement polyalphabétique de Vigenère a résisté environ 3 siècles, jusqu'à ce que le mathématicien Charles Babbage élabore la théorie de son décodage en 1854. Ce n'est qu'en 1863 que cette découverte a été publiée par le major allemand Friedrich Kasiski, à qui parfois cette découverte est attribuée, dans son livre [50].

L'âge industriel :

L'accroissement du développement des réseaux de télécommunications, à la fin du XIXième siècle, ainsi que le début de la grande guerre mondiale furent un véritable catalyseur pour la cryptographie, et donc une victoire remarquable de la cryptanalyse. C'était

l'époque où la transmission d'un message se libère du transport, et l'interception des informations devint vital. Ce qui a poussé les cryptographes au développement de nouveaux systèmes cryptographiques, ouvrant la voie à la mécanisation de la cryptologie.

Lors de la Première Guerre Mondiale, en 1917, Gilbert Vernam conçut une méthode de chiffrement sécuritaire, nommée **« masque jetabte »**, one-time pad en anglais. Il s'agit d'une forme de chiffrement pratique de Vigenère qui consiste à combiner par l'opération booléenne XOR, « ou exclusif », entre le texte clair et la clé. Quoique le chiffrement de Vernam soit reconnu comme inconditionnellement sûr, i.e théoriquement impossible à « casser », il est irréaliste du point de vue pratique puisqu'il repose sur la génération et le transport de clé composée d'une suite aléatoire de caratères, au moins aussi longue que le texte clair, et ce pour une seule utilisation.

Après la première guerre mondiale, les cryptographes se tournèrent vers des machines à rotors dont la plus célèbre entre elles fut sans doute **« Enigma »**, une machine portable et puissante mise au point par l'ingénieur allemand Arthur Scherbius en 1918, utilisée pendant la Seconde Guerre mondiale.

Le machine électromécanique, Enigma, réalise une méthode de chiffrement par substitution polyalphabétique. Pour ses versions courantes, elle se compose d'un clavier alphabétique, d'un dispositif de chiffrement et d'un tableau lumineux, reliés par des cables électriques, voir Fig.1.8.

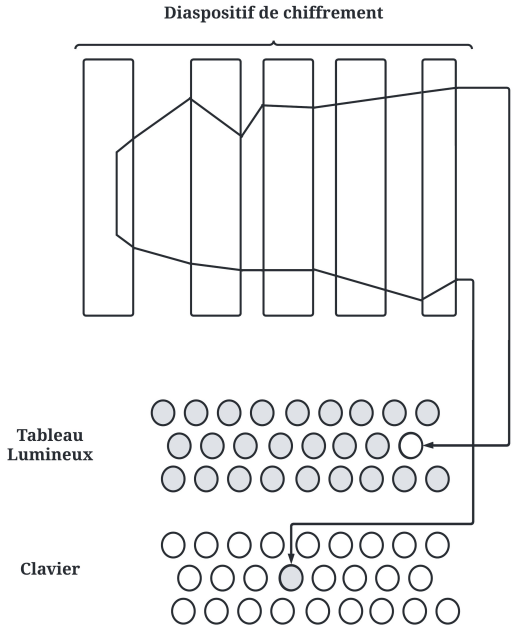


FIGURE 1.8 : Machine Enigma

Ainsi, pour chaque lettre saisie sur le clavier, un courant électrique issu du clavier traverse le dispositif de chiffrement et allume une ampoule du tableau lumineux qui correspond à une lettre chiffrée .

Le dispositif de chiffrement se compose de trois éléments distincts, qui tour à tour vont substituer la lettre provenant du clavier par une autre. Un tableau de connexion, sert à mélanger les lettres de l'alphabet en permutant deux à deux certaines d'entre

elles, un assemblage de trois rotors rotatifs bordés des 26 lettres de l'alphabet, réalisent une permutation entre les lettres de chaque bord chaque fois qu'une lettre est tapée. Un réflecteur permet de renvoyer le courant électrique de manière à ce qu'il repasse par les trois rotors puis de nouveau dans le tableau de connexion, avant qu'elle n'arrive au tableau lumineux pour afficher la lettre correspondante.

Le principe du fonctionnement de la machine Enigma s'avère d'une simplicité et d'une efficacité redoutable, présenté en figure 1.9. À titre d'exemple, si la lettre C est saisie sur le clavier un courant électrique traverse : le tableau de connexion transforme C en T, le rotor III il devient J ainsi avec le rotor II Il devient B puis avec le rotor I K. Le réflecteur transforme K en N. Le rotor I opère maintenant à l'envers, N devient K, K devient D avec le rotor II et D devient W avec le rotor III finalement la lettre H s'allume sur le tableau lumineux. Pour chaque lettre saisie sur le clavier, le chiffrement change puisque le rotor III tourne à nouveau d'un cran.

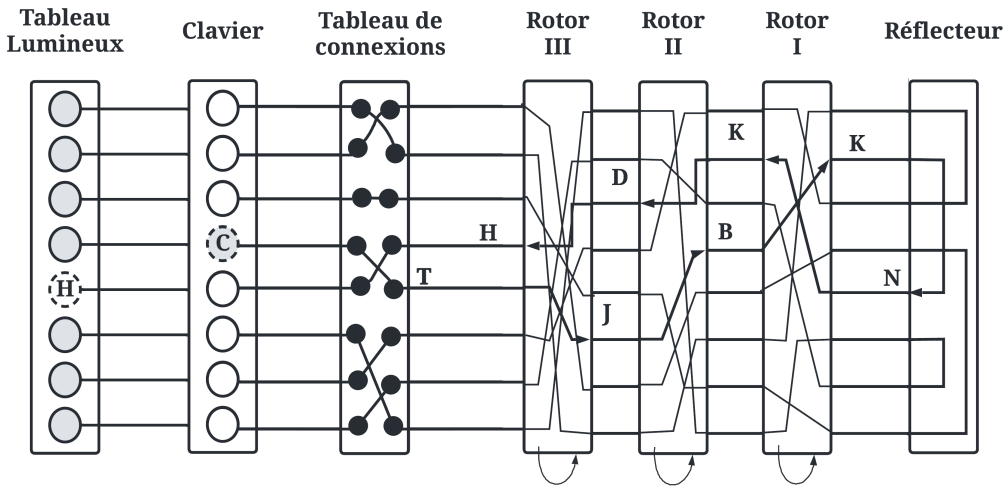


FIGURE 1.9 : Fonctionnement de la machine Enigma

Chaque rotor possède 26 positions. A chaque fois qu'une lettre est tapée, le premier rotor tourne d'un cran. Après 26 lettres, il revient à sa position initiale, et le second rotor tourne alors d'un cran. Quand le second rotor a retrouvé sa position initiale, c'est le troisième rotor qui tourne d'un cran. Bien que le fonctionnement de la machine soit complexe, le déchiffrement d'un texte clair suffirait de retrouver la configuration initiale de la machine Enigma.

La cryptanalyse de la machine a été réalisée à partir des travaux conjugués des chercheurs polonais en 1939 et d'Alan Turing (1939-1943). Ce dernier parvient à créer ce qu'il appelle à l'époque une « **bombe** », une machine électromécanique permettant d'analyser, beaucoup plus rapidement qu'à la main, différentes configurations possibles de la machine Enigma.

Avec la rupture technologique de la machine allemande Enigma, la course entre les cryptographes et les cryptanalystes s'est relancée. Cependant, la mécanisation du traitement de l'information ouvre la voie vers une nouvelle ére, celle de l'avènement de l'ordinateur.

L'âge paradoxal :

Devant le développement de l'informatique et l'apparition des réseaux, au début des années 70, le besoin pour sécuriser le stockage et le transfert de données dans le domaine civil a augmenté.

En 1973 le NBS, *National Bureau of Standards* américain, connu maintenant sous l'acronyme NIST pour *National Institute of Standards and Technology* lance un appel d'offre pour un cryptosystème, offrant un niveau de sécurité élevé, destiné aux communications industrielles.

Cet appel d'offre a donné naissance au cryptosystème **« DES »**, *Data Encrytion Standard* adopté par le NBS comme le standard du chiffrement symétrique en 1976. Issu d'un algorithme Lucifer créé par IBM, il fut modifié par la NSA, *National Security Agency* en vue de sa standardisation. Le DES est un chiffrement en bloc qui opère sur des blocs de 64 bits et utilise une clé secrète de 56 bits.

Les progrès de la cryptanalyse et l'accroissement de la puissance des ordinateurs ont permis de casser complétement le DES. En 1997, le NIST lance un nouvel appel à contribution mondiale pour définir un nouveau standard de chiffrement symétrique, l'**« AES »** *Advanced Encryption Standard* [51], le remplaceur de DES.

Suite à l'appel du NIST, seulement quinze cryptosystèmes remplissaient tous les critères nécessaires et ont été acceptés en tant que candidats AES parmi vingt-et-un reçues. En 1999, cinq candidats furent acceptés comme finalistes : MARS, RC6, Rijndael, Serpent et Twofish. Le 2 octobre 2000, Rijndael fut choisi en tant que standard avancé. Il opère sur des blocs de texte clair de 128 bits, avec trois tailles de clé differentes : 128, 192, ou 256 bits. Sa structure fait intervenir les opérations d'addition et de multiplication dans le corps fini à 256 éléments.

A l'époque du DES, plus précisément en 1976, Whitfield Diffie et Martin Hellman publient dans leur article intitulé *New directions in cryptography* [52], une nouvelle approche en cryptographie appelé le **chiffrement à clé publique**. Cette approche utilise des paires de clés, l'une rendue publique pour le chiffrement du texte clair et l'autre reste privée pour le déchiffrement.

Un an plus tard, le premier système de chiffrement à clé publique est réalisé en pratique par Rivest, Adi Shamir et Leonard Adleman connu sous l'acronyme **« RSA »** [53].

De nos jours, RSA est le chiffrement à clé publique le plus connu et le plus utilisé à travers le monde. Depuis lors, nombreuse découvertes de cryptosystèmes ont été proposés et implémentés selon cette approche.

IV La cryptographie

Le mot cryptographie est un terme générique désignant l'étude des différentes techniques reliées aux aspects de sécurité de l'information. En d'autres termes, elle consiste en l'étude des techniques utilisées entre deux entités soit pour stocker de l'information de manière sécuritaire, soit pour protéger de l'information lors de son transfert dans un canal de communication non sécurisé en présence d'une institution adverse.

Pour résister à cette tierce institution, ces techniques que l'on appelle des **cryptosys-**

tèmes, ou encore des **systèmes cryptographiques**, s'appuient sur des problèmes calculatoires réputés difficiles.

Par ailleurs, la plupart des cryptosystèmes peuvent montrer une performance satisfaisante sur des plateformes possédant une puissance de calcul suffisante pour gérer ce genre de calculs.

A Objectif de la cryptographie

Les systèmes cryptographiques apportent un certain nombre de propriétés visant à assurer des exigences résumées dans le sigle **CAIN** :

- **Confidentialité :** consiste à protéger l'information, qui transite dans un canal de communication, contre une divulgation en dehors des personnes autorisées à l'obtenir. Cela revient à garantir l'identité du destinataire.
- **Authentification :** consiste à vérifier l'identité des participants à une communication, cela revient à vérifier que l'information provient de l'expéditeur
- **Intégrité :** consiste à vérifier que l'information transmise n'a subi aucune altération lors de sa transmission sur le canal de communication. En d'autres termes, garantir que l'information reçu est bien celle qui a été envoyée, et que celle-ci n'a pas été modifée.
- **Non-répudiation :** consiste à assurer que les parties impliqués dans la communication ne peuvent nier y avoir participer. En d'autres termes, il vérifie que l'émetteur et le récepteur sont bien les parties qui ont respectivement envoyé ou reçu le message.

Historiquement, la confidentialité est le point principal parmi ces objectifs de la cryptographie.

B Principe de Kerckhoff

A l'époque où les algorithmes de chiffrement étaient mécaniques, Auguste Kerckhoffs publie dans son traité [54] intitulé *la cryptographie militaire*, six principes qui guident les travaux des cryptologues afin d'assurer la confidentialité d'un système.

i Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;

ii Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;

iii La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;

iv Il faut qu'il soit applicable à la correspondance télégraphique ;

v Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;

vi Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

De nos jours, le principe de Kerckhoffs que l'on peut déduire de ces principes est : *La sécurité d'un cryptosystème doit reposer exclusivement sur le secret de la clé.*

Il existe trois principaux arguments, à l'avantage du principe de Kerckhoffs. Le premièr est qu'il est beaucoup plus facile pour les parties de maintenir le secret d'une clé courte que de maintenir le secret d'un algorithme qui est des milliers de fois plus volumineux. Le deuxième argument est que si la clé est exposée, il sera beaucoup plus facile pour les parties de changer la clé que de remplacer l'algorithme utilisé. Enfin, dans le cas où de nombreuses entités ont besoin de crypter leur communication, il sera beaucoup plus facile d'utiliser le même algorithme des clés différentes que d'utiliser un algorithme différent.

V Algorithme de cryptographie

Un algorithme de cryptographie est une méthode permettant d'assurer la confidentialité en rendant un message inintelligible aux tierces entités non autorisées à l'utiliser ou le lire.

Basée sur le principe de kerckhoff, la confidentialité des messages repose sur une information secrète dite **clé**, utilisée avec un algorithme de cryptographie pour produire le texte chiffré. Selon la clé utilisée deux catégories d'algorithmes de cryptographie sont distinguées : (1) **algorithme de cryptographie à clé privée** et (2) **algorithme de cryptographie à clé publique**. Ces deux catégories sont respectivement abordées dans les sections qui suivent.

A Algorithme de cryptographie à clé privée

Depuis l'ère antique jusqu'en 1976, l'algorithme de cryptographie à clé privée était la seule méthode connue pour échanger de l'information. L'algorithme de cryptographie à clé privée, aussi connue sous le nom de **cryptographie symétrique**, a réussi le passage entre la cryptographie basée sur les opérations de transpositions et de substitutions, et la cryptographie moderne reposant sur les sciences mathématiques et informatiques.

Principe du chiffrement à clé privée :

Le principe d'un algorithme de cryptographie à clé privée consiste à utiliser la même clé secrète au chiffrement et au déchiffrement des messages, d'où le nom d'algorithmes symétriques, Fig.1.10. Cette technique nécessite que les deux parties, Alice et Bob, possèdent une clé secrète **identique** afin de s'échanger un message de manière sécuritaire. Sans cette clé, le cryptogramme est totalement illisible pour toutes personnes à qui n'est pas destiné.

L'analogie au coffre-fort est souvent utilisé pour caractériser cet algorithme cryptographique : Alice, l'émettrice, cache le message dans le coffre en utilisant la clé, seul Bob, le récepteur, peut l'ouvrir car il est le seul à posséder la même clé du coffre-fort.

En pratique, le chiffrement de l'algorithme de cryptographie à clé privée est défini de la manière suivante

$$\mathcal{E} : \mathcal{E}_k(M) = C.$$

Le déchiffrement est défini par l'opération suivante

$$\mathcal{D} : \mathcal{D}_k(C) = M.$$

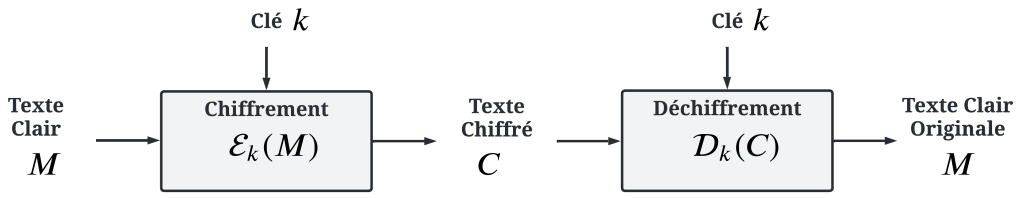


FIGURE 1.10 : Algorithme de cryptographie à clé secrète.

Deux méthodes existent pour établir un chiffrement symétrique : le **chiffrement par flot**, objet du présent paragraphe et le **chiffrement par bloc**, décrit dans le paragraphe suivant.

Algorithme de chiffrement par flot :

L'algorithme de chiffrement par flot tirant son nom de l'anglais **stream cipher**, consiste généralement à combiner chaque caractère, ou bit, du texte clair avec un bit d'une suite pseudo-aléatoire, par une opération symétrique conservant une distribution équiprobable. Le masque jetable, one-time-pad, propose à ce titre une base solide pour cette conception.

Le one time pad, appelé aussi **le masque de Vernam**, se résume à une addition binaire, bit à bit, du texte clair avec une clé secrète de même longueur. Le déchiffrement du cryptogramme est effectué par une opération **XOR** entre le texte chiffré et la suite secrète, voir Fig. 1.11.

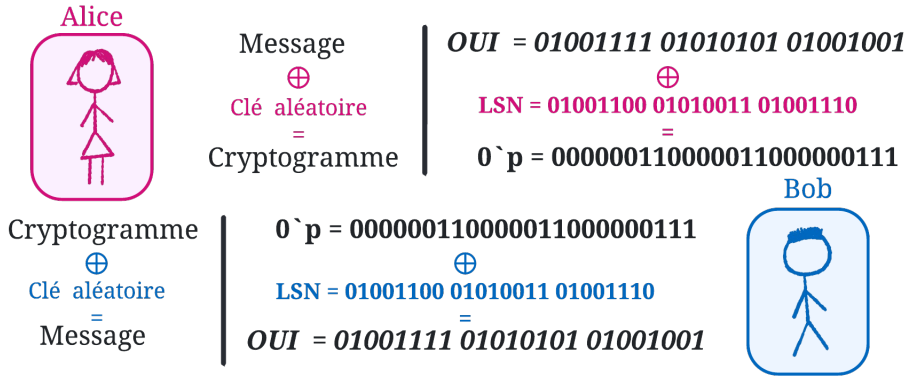


FIGURE 1.11 : Masque jetable

L'algorithme de chiffrement par flot est très rapides et très peu coûteux, par contre sa sécurité repose sur la sécurité et la qualité du générateur pseudo-aléatoire, un algorithme qui permet de dériver la suite secrète. Ces caractéristiques lui permettent d'être

parfaitement implémenté dans les protocoles des communications téléphoniques, Internet, Bluetooth ou encore dans le protocole WEP utilisé pour sécuriser les connexions WiFi.

Algorithme de chiffrement par bloc :

Les algorithmes de chiffrement par bloc, **block ciphers**, comme leur nom l'indique opèrent bloc de bits par bloc de bits. Un block ciphers agit de manière combinatoire sur le texte clair, découpant ce dernier en blocs de taille fixe. Les tailles usuelles sont de l'ordre de 64, 128 ou 256 bits, correspondant à la taille d'une clé pour fournir un bloc de cryptogramme. Le chiffrement par blocs nécessite l'utilisation d'un mode opératoire de chiffrement pour combinés les differents blocs.

L'algorithme de chiffrement par bloc est plus lent, un peu plus coûteux, et nécessite plus de moyens informatiques que l'algorithme de chiffrement par flot. Mais il est bien adapté à la cryptographie civile comme celle des banques. Cette catégorie d'algorithme de chiffrement symétrique est largement utiliséé en pratique avec le DES et le standard actuel AES.

Les modes opératoires : En pratique, les textes clairs sont de longeur arbitraire. Pour adapter la taille du message à celle de la clé, quatre modes de chiffrement par blocs sont possible : **ECB** (Fig. 1.12), **CBC** (Fig. 1.13), **CFB** (Fig. 1.14) et **OFB** (Fig. 1.15) qui sont standardisés par le NIST.

Le mode ECB : mode dictionnaire. ECB, signifie *Electronic Code Book*, est le mode opératoire le plus simple. Il consiste à chiffrer individuellement chaque bloc m_i avec la clé k par la fonction de chiffrement $\mathcal{E}_k$ donnant le cryptogramme c_i, comme indiqué dans la figure 1.12.

Formellement, le chiffrement en mode ECB est donné par

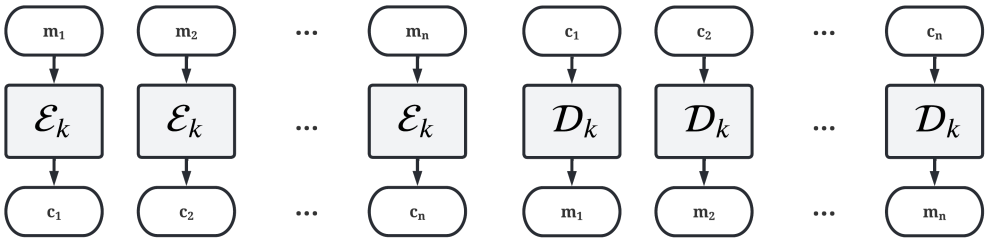
$$c_i = \mathcal{E}_k(m_i). \tag{1.1}$$

Le déchiffrement fonctionne de manière symétrique. Chaque bloc c_i du cryptogramme est déchiffré avec la clé k par la fonction de déchiffrement $\mathcal{D}_k$ permettant de recouvrer le bloc de texte clair m_i correspondant :

$$m_i = \mathcal{D}_k(c_i) \tag{1.2}$$

Le mode CBC : mode chaînage de blocs chiffrés. Le mode CBC, signifie *Cipher Block Chaining*, nécessite un bloc initial aléatoire appelé *Vecteur d'initialisation*, VI= c_0, qui permet d'initialiser le processus. Chaque bloc du message m_i est d'abord additionné modulo 2 au bloc de cryptogramme précédent avant d'être lui même chiffré par la fonction de chiffrement par blocs, comme illustré sur la figure 1.13.

$$\begin{aligned} c_1 &= \mathcal{E}_k(m_1 \oplus c_0) \\ c_i &= \mathcal{E}_k(m_i \oplus c_{i-1}), \text{ pour } i = 2, ..., n. \end{aligned} \tag{1.3}$$

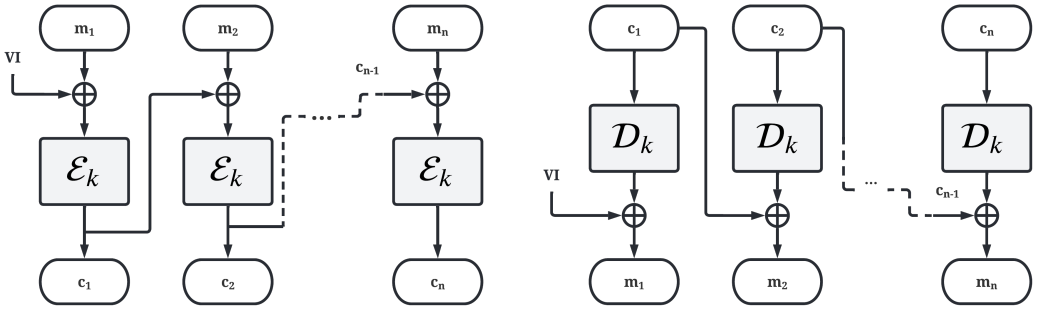


(a) Chiffrement (b) Déchiffrement

FIGURE 1.12 : Fonctionnement du mode ECB.

Le fonctionnement du déchiffrement illustré par la figure1.13, consiste à déchiffré le premier bloc du cryptogramme c_1 par la fonction de déchiffrement $\mathcal{D}_k$ puis le combiné par OU exclusif avec le cryptogramme précédent. Cela revient a effectué l'opération suivante

$$\begin{aligned} m_1 &= c_0 \oplus \mathcal{D}_k(c_1) \\ m_i &= c_{i-1} \oplus \mathcal{D}_k(c_i), \text{ pour } i = 2, ..., n. \end{aligned} \tag{1.4}$$



(a) Chiffrement (b) Déchiffrement

FIGURE 1.13 : Fonctionnement du mode CBC

Le mode CFB : mode rebouclage de texte chiffré. Le mode CFB, le mode de chiffrement à rétroaction, permet de chiffrer le message par unité de k bits plus petite que la taille b bits de bloc. Dans ce cas, le texte clair est découpé en segments de k bits.

Le mode CFB, *Cipher FeedBack*, utilise un registre de décalage de b bits initialisé en entrée avec un vecteur d'initialisation VI. Le principe du mode CFB consiste à chiffrer le registre de décalage par la focntion de chiffrement puis combiner les k bits les plus à gauche, les plus significatifs, du résultat par un OU exclusif avec le premier segment du message pour obtenir ainsi la première unité du cryptogramme. La nouvelle valeur du registre de décalage est obtenue en faisant un décalage vers la gauche de k bits, et en y

plaçant les k bits du cryptogramme à droite du registre. Ce processus se poursuit jusqu'à ce que le reste du texte clair soient chiffrées, suivant le schéma donné à la figure 1.14.

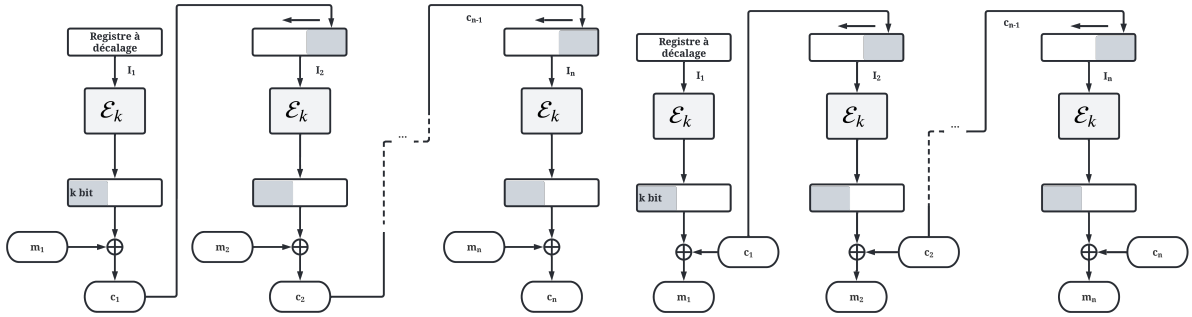
Le chiffrement en mode CFB s'effectue par les opérations suivantes :

$$\begin{aligned} I_1 &= VI \\ I_i &= I_{i-1}||c_{i-1}, \text{ pour } i = 2, ..., n \\ c_i &= m_i \oplus MSB_k(\mathcal{E}_k(I_i)), \text{ pour } i = 1, ..., n \end{aligned} \tag{1.5}$$

avec $MSB_k(X)$ définie comme les k bits les plus significatifs de x.

En mode CFB, le déchiffrement utilise le même schéma que le chiffrement, sauf que l'unité du cryptogramme est « Xoré » avec le résultat de la fonction de chiffrement pour produire l'unité du texte clair. Formellement, le déchiffrement en mode CFB correspond à

$$\begin{aligned} I_1 &= VI \\ I_i &= I_{i-1}||c_{i-1}, \text{ pour } i = 2, ..., n \\ m_i &= c_i \oplus MSB(\mathcal{E}_k(I_i)), \text{ pour } i = 1, ..., n. \end{aligned} \tag{1.6}$$



(a) Chiffrement (b) Déchiffrement

FIGURE 1.14 : Fonctionnement du mode CFB

Le mode OFB : mode rebouclage sur la sortie. Le mode OFB, qui signifie *output feedback*, est similaire au mode CFB sauf que les k premiers bits du résultat du chiffrement du registre de décalage du bloc précédent seront réutilisé pour le chiffrement du bloc courant.

Le mode OFB, le mode de rétroaction de sortie, consiste à chiffrer le registre de décalage par la focntion de chiffrement puis combiner les k bits les plus significatifs du résultat par un OU exclusif avec le premier segment du texte clair pour obtenir les k premiers bits du cryptogramme. La nouvelle valeur du registre de décalage est obtenue en faisant un décalage vers la gauche de k positions, et en y plaçant le résultat du chiffrement du registre de décalage dans les k bits les plus à droite du registre de décalage. Ce processus se poursuit jusqu'à ce que le reste du texte clair soient chiffré, suivant le schéma donné à la figure 1.15.

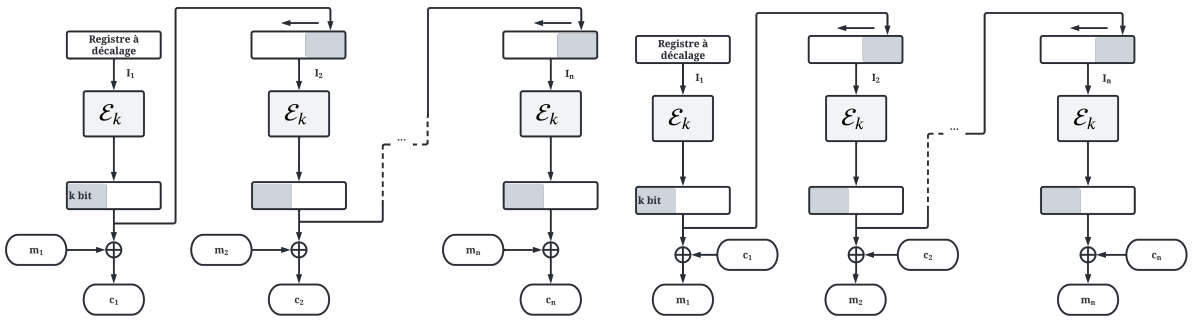
Le chiffrement en mode OFB peut être exprimé comme suite

$$\begin{aligned} I_1 &= VI \\ I_i &= I_{i-1}||MSB_k(\mathcal{E}_k(I_i)),\ \text{pour } i = 2, ..., n \\ c_i &= m_i \oplus MSB_k(\mathcal{E}_k(I_i)),\ \text{pour } i = 1, ..., n. \end{aligned} \tag{1.7}$$

Pour le déchiffrement, le même schéma est utilisé ; la fonction de chiffrement est appliqué au même registre de décalage ensuite les k premiers bits de ce résultat sont ajoutés au bloc précédent du cryptogramme.

Le déchiffrement en mode CFB s'effectue par les opérations suivantes

$$\begin{aligned} I_1 &= VI \\ I_i &= I_{i-1}||MSB_k(\mathcal{E}_k(I_i)),\ \text{pour } i = 2, ..., n \\ m_i &= c_i \oplus MSB_k(\mathcal{E}_k(I_i)),\ \text{pour } i = 1, ..., n. \end{aligned} \tag{1.8}$$



(a) Chiffrement (b) Déchiffrement

FIGURE 1.15 : Fonctionnement du mode OFB

Le principal avantage des algorithmes de cryptographie à clé privée est qu'ils sont efficaces en terme de temps de calcul. Néanmoins, Ces algorithmes posent un certain problème. Le premier, l'échange préalable de manière sécurisée de la clé symétrique entre les deux utilisateurs légitimes. En effet, cela nécessite des moyens conventionnels, comme une rencontre entre les deux interlocuteurs, ou encore, par l'utilisation d'un messager honnête. Le deuxième, est que la clé privée ne permet de sécuriser qu'une seule communication, entre les deux interlocuteurs, autrement dit la clé privée doit être renouvelée au même rythme que le message est envoyé. Ces deux problèmes furent pendant de nombreuses années un réel obstacle à résoudre pour les cryptographes. La solution leur vint à la fin des années 1970 avec l'invention de l'algorithme de cryptographie à clé publique.

B Algorithme de cryptographie à clé publique

Whitfield Diffie et Martin Hellman bouleversent l'année 1976 [52] par leur article *New directions in Cryptography*. Cet article a formalisé le concept de la cryptographie à clé

publique et, en même temps, propose le premier schéma permettant à deux protagonistes de créer un secret commun en utilisant seulement un canal de communication ouvert. En d'autres termes, il n'est pas nécessaire d'échanger préalablement la clé pour communiquer de manière sécurisée.

Leur idée simple et élégante s'appelle actuellement **le protocole d'échange de clef de Diffie-Hellman**, voir Fig 1.17.

Principe du chiffrement à clé publique :

La cryptographie à clé publique, aussi connue sous le nom **cryptographie asymétrique**, recommande la création de deux clés différentes associées ; l'une d'entre elle dite clé publique, peut être distribuée librement, et l'autre dite clé privée ne quitte jamais son propriétaire. Ainsi lorsque Alice désire envoyer un message à Bob, elle lui suffit de chiffrer le message au moyen de la clé publique de Bob, tandis que ce dernier se sert de la clé privée associée pour déchiffrer le message, voir Fig 1.16.

L'analogie de la boîte aux lettre est souvent utilisé pour caractériser l'algorithme de cryptographie à clé publique : Alice, connaissant l'adresse de Bob, envoie un courrier dans la boîte aux lettre mais uniquement Bob, le propriétaire, possédant la clé privée peut lire le courrier déposé dans sa boîte aux lettres.

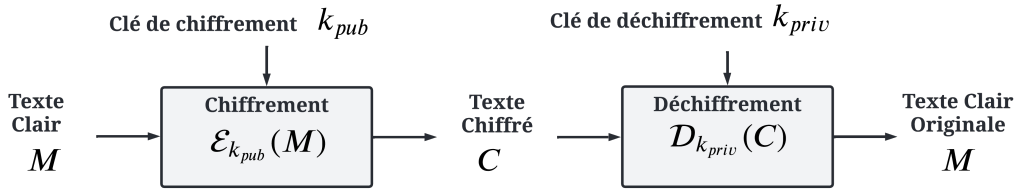


FIGURE 1.16 : Algorithme de cryptographie à clé publique

En pratique, le principe d'opération de chiffrement d'un algorithme de cryptographie à clé public est défini de la manière suivante

$$\mathcal{E} : \mathcal{E}_{k_{pub}}(M) = C.$$

L'opération de déchiffrement d'un algorithme de cryptographie à clé public est la suivante

$$\mathcal{D} : \mathcal{D}_{k_{priv}}(C) = M.$$

Les cryptosystèmes asymétriques reposent sur des fonctions mathématiques qui se calculent rapidement dans un sens mais dont l'inverse est extrêmement difficile à calculer, appelées **fonctions à sens unique**.

Deux exemples importants de problèmes mathématiques sur lesquels se reposent la création de protocoles cryptographiques asymétriques : le **problème de factorisation d'un nombre entier en produit de nombres premiers** et le **problème du logarithme discret**. Ces deux problèmes sont respectivement utilisés dans le système cryptographique RSA, cf. section VIII, et dans le système cryptographique d'Elgamal, cf. section IX.

Problème de la factorisation dentier :

Le problème de la factorisation consiste à retrouver la décomposition en facteurs premiers d'un entier donné, obtenu de manière secrète par la multiplication de deux nombres premiers, généralement de taille comparable.

Jusqu'à présent, il n'existe aucun algorithme de résolution de ce problème ayant un temps de calcul raisonnable en pratique pour traiter des entiers quelconques de grandes tailles.

Théorème V.1. *Tout entier > 1 peut être écrit de manière unique comme un produit de nombres premiers, chacun dentre eux élevé à une certaine puissance ≥ 1.*

Proposition 1. *Soit a un entier strictement positif, il existe un unique entier $r > 0$, une unique famille de nombre premiers $p_1, p_2, \ldots, p_r$ et une unique famille d'entiers $n_1, n_2, \ldots, n_r$ strictement positifs tels que*

$$a = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$$

Cette écriture est appelée la décomposition de a en facteurs irréductibles.

Le problème de la factorisation est l'un des plus vieux de la théorie des nombres. Toutefois, les algorithmes de factorisation se divisent en deux catégories : ceux dont l'objectif est de trouver le plus petit facteur premier, et ceux dont l'objectif est de trouver la factorisation complète. La compléxité du premier algorithme dépend essentiellement de la taille du plus petit facteur, quant au second algorithme la complexité dépend de la taille de l'entier à factoriser.

Problème de logarithme discret :

Soit g un générateur de $\mathbb{Z}_p^*$, l'ensemble des entiers positifs plus petits que p et premiers avec p. Considérons l'application :

$$x \mapsto g^x,$$

qui n'est autre que l'exponentiation discrète à la puissance x en base g, l'élément x étant un entier.

L'inverse de cette opération revient à résoudre le problème du logarithme discret, c'est-à dire retrouver l'exposant x étant donné $a = g^x$. Cet entier x bien déterminé porte le nom de logarithme discret en base g de l'élément a et est souvent noté $log_g(a)$.

La difficulté du problème de calcul de logarithme discret est à la base de la sécurité du protocole d'échange de clés Diffie–Hellman [52], qui a été décrit en 1976 et du cryptosystème de El Gamal [55], décrit en 1985.

À l'heure actuelle, il n'existe aucun algorithme à complexité polynomiale qui est capable de résoudre le problème du logarithme discret dans un temps de calcul raisonnable.

Protocole d'échange de clés Diffie–Hellman : Alice et Bob désirant partager une clé secréte commune, notée k. Pour cela ils commencent par se mettre d'accord sur deux nombres publiques ; un très grand nombre premier n et un générateur $g \in \mathbb{Z}_p^*$.

1. Alice choisit un nombre $x \in \mathbb{Z}_p^*$ secret ; puis envoie $A = g^x \mod n$ à Bob.
2. De même, Bob choisit un nombre $y \in \mathbb{Z}_p^*$ secret ; et envoie $B = g^y \mod n$ à Alice.
3. Alice calcule $k = B^x \mod n$ pendant que Bob calcule $k' = A^y \mod n$

Ainsi, Alice et Bob (se sont mis d'accord sur une clé privée) ont réussi à créer une clé privée, sans se l'être directement communiqué. En effet,

$$k \equiv B^x \mod n \equiv (g^y)^x \equiv g^{yx} \equiv (g^x)^y \equiv A^y \mod n \equiv k'$$

Cependant, Il est clair que la sécurité du Protocole d'échange de clés Diffie–Hellman, réside dans la difficulté de résoudre un problème du logarithme discret.

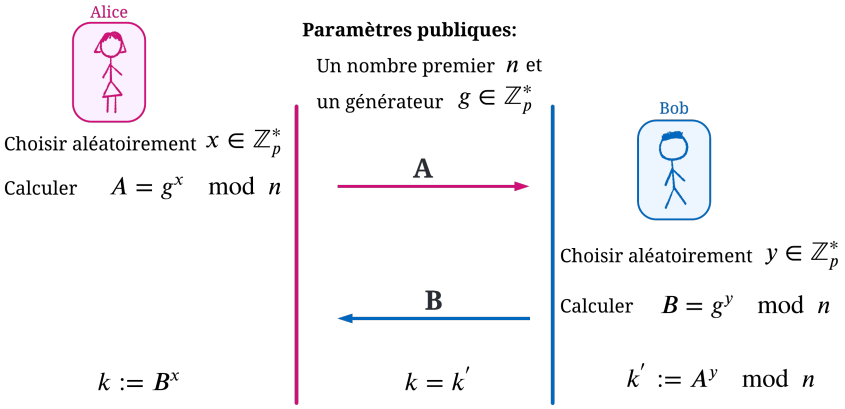


FIGURE 1.17 : Protocole déchange de clés DiffieHellman

La factorisation d'entier en produit de nombres premiers et logarithme discret sont à nos jours considérés insolubles pour de trés grandes valeurs, ils sont désormais la base de la sécurité d'un grand nombre de protocoles cryptographiques.

L'avantage majeur de l'algorithme à clé publique est qu'il ne requiert pas la nécessité d'échanger préalablement un secret pour communiquer de manière sécurisée. Par le fait que les communications découlent uniquement par l'utilisation de la clé publique, aucune clé privée n'est transmise ou partagée.

Cependant, la sécurité de l'algorithme est limitée par la difficulté calculatoire de retrouver la clé privée à partir du message et de la clé publique.

L'algorithme de cryptographie à clé publique est trés pratique pour s'échanger sécuritairement une clé symétrique,qui est ensuite utilisée pour chiffrer et déchiffrer de manière performante les messages échangés.

VI Le standard de Chiffrement de Données : DES

Data Encryption Standard, connu par son abréviation **DES**, un algorithme de cryptographie symétrique, sélectionné comme un standard en 1976.

Le DES tire son origine de l'algorithme Lucifer, un travail mené par le groupe cryptographique d'IBM, dont est le but de protéger les communication et les données personnelles mémorisées sur les ordinateurs.

L'algorithme DES est un chiffrement par bloc, basé sur le principe des **schémas de Feistel**. Il opére sur un bloc de texte clair de 64 bits en utilisant une clé de 56 bits, pour obtenir un bloc de texte chiffré de 64 bits à l'aide d'opérations compliquées.

A Le Schéma de Feistel

Le Schéma de Feistel appelé aussi **réseau de Feistel**, est une construction itérative datant du début des années 70. Le schéma découpe l'entrée de longeur n en deux moitiés, une entrée gauche x_g et une entrée droite x_d, de taille identique. L'image d'une moitié est calculé par une fonction f dite **fonction de Feistel** puis le résultat est ajouté par un OU exclusif à l'autre moitié.

Cette construction est itérée plusieurs fois en inversant les deux moitiés à chaque tour jusqu'à obtenir le cryptogramme, comme le montre la figure 1.18.

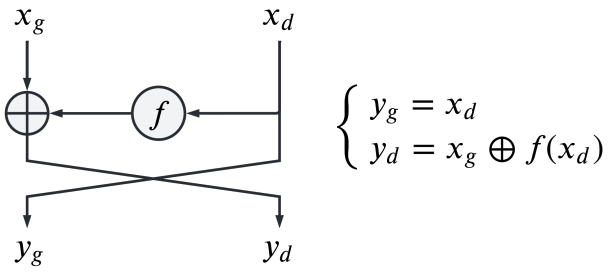


FIGURE 1.18 : Schéma de Feistel.

B Structure général de DES

La figure 1.19 représente une déscription générale de l'algorithme DES. Globalement, l'algorithme de chiffrement consiste à respecter les trois étapes suivants :

1. Permutation initiale.
2. Une structure Feistel à 16 tours.
3. Permutation finale.

Le bloc de texte clair subit une *permutation initiale*, puis *16 itérations* d'une procédure identique, où la moitié droite est recopiée telle quelle à gauche, et la moitié gauche est transmise à droite en subissant au passage une modification dépendante des sous-clés $k_1, ..., k_{16}$. A la fin, du 16^e tours les moitiés droite et gauche sont réassemblées et une *permutation finale* termine l'algorithme obtenant alors le bloc chiffré.

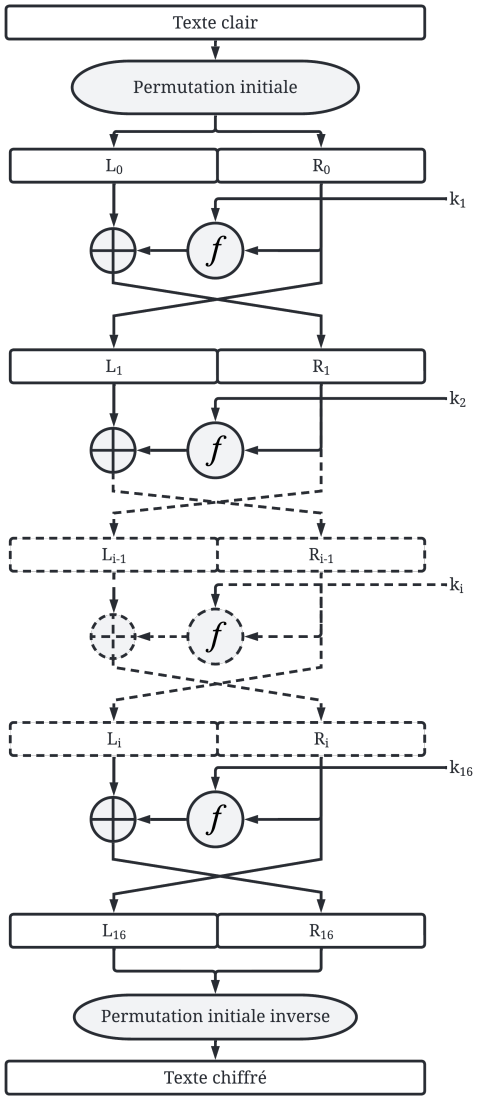


FIGURE 1.19 : Schéma général du DES.

C Opérations de chiffrement et de déchiffrement de l'algorithme DES

L'algorithme de chiffrement utilise des sous-clés k_i, obtenus à partir de la clé initiale k de taille 56 bits, pour opérer sur un texte clair donné. Ce dernier est fractionné dans un premier temps en blocs de 64 bits. Chaque bit d'un bloc subit une permutation représentée par le tableau de permutation initiale, notée IP, selon la figure 1.20. Ce tableau de permutation indique, en parcourant de gauche à droite et de haut en bas, que le $58^{ème}$ bit du bloc de texte se retrouve en première position, le $50^{ème}$ en seconde position et ainsi de suite. Une fois la permutaion initiale effectuée, la nouvelle disposition du bloc de 64 bits est séparé en deux moitiés de 32 bits, désignées par L_0 et R_0. Ces deux moitiés subiront une opération de chiffrement, appelée fonction de Feistel, avec clé et ce, 16 fois de suite. Cette opération de chiffrement est défini par :

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

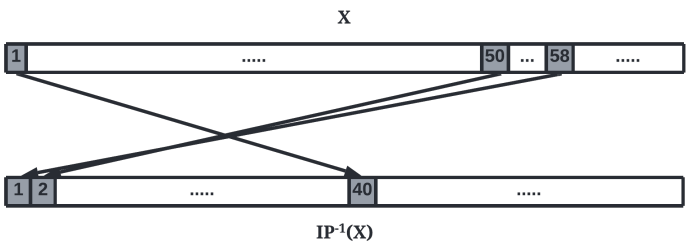


FIGURE 1.20 : Permutation initiale

$$\begin{aligned} L_i &= R_{i-1}, \\ R_i &= L_{i-1} \oplus f(R_{i-1}, k_i), \end{aligned} \tag{1.9}$$

pour $1 \leq i \leq 16$, f est une fonction décrite plus loin, et k_i sont les sous-clés de 48 bits obtenus par *diversification de clé*.

La fonction de chiffrement f est le coeur des 16 tours de l'algorithme, celle-ci prend en entrée un premier registe R_i de 32 bits et un second registe de 48 bits, le registe sous-clé k_i, et donne 32 bits en sortie. La fonction f de DES est constituée des phases, explicitées dans le schéma de la Figure 1.22 :

1. **Fonction d'expansion E :** Les 32 bits du bloc d'entrée R_0 sont étendus à 48 bits grâce à une table appelé *table d'expansion*, notée **E**, dans laquelle les 48 bits sont composés de tous les 32 bits du R_0 dans un certain ordre, 16 d'entre eux apparaissant deux fois.

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

2. **«ou exclusif»** entre le résultat de E(R_{i-1}) et k_i, une clé de tour de 48 bits. Le résultat de cette opération est découpé en 8 sous-blocs de 6 bits chacun.
3. **Fonction de substitution :** Les 8 sous-blocs sont soumis à une fonction de substitution réalisée à l'aide de huit tables de substitutions S-box, voir Fig. B.2, représentée dans l'appendice B. Chaque sous-blocs est manipulé séparément par une S-box différente pour fournir un bloc de 4 bits en sortie. Les 8 sorties de 4 bits des boîtes S sont regroupées pour former un bloc de 32 bits.
4. **Permutation :** Les bits du bloc de 32 bits obtenus sont réordonnés suivant une permutation fixée P à l'aide du tableau de transposition.

P							
16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Le résultat de la permutation P est combiné par OU exclusif avec la moitié gauche L_{i-1} du bloc initial de 64 bits pour donner R_i. La moitié droite R_{i-1} du bloc initial donne L_i. Le processus reprend de la même manière pour les 15 autres itérations.

Finalement, Aprés 16 tours, une permutation inverse IP^{-1} est appliquée, afin d'annuler la permutation initiale, décrite par le tableau 1.21 pour obtenir le bloc chiffré de 64 bits.

IP^{-1}							
40	**8**	**48**	**16**	**56**	**24**	**64**	**32**
39	**7**	**47**	**15**	**55**	**23**	**63**	**31**
38	**6**	**46**	**14**	**54**	**22**	**62**	**30**
37	**5**	**45**	**13**	**53**	**21**	**61**	**29**
36	**4**	**44**	**12**	**52**	**20**	**60**	**28**
35	**3**	**43**	**11**	**51**	**19**	**59**	**27**
34	**2**	**42**	**10**	**50**	**18**	**58**	**26**
33	**1**	**41**	**9**	**49**	**17**	**57**	**25**

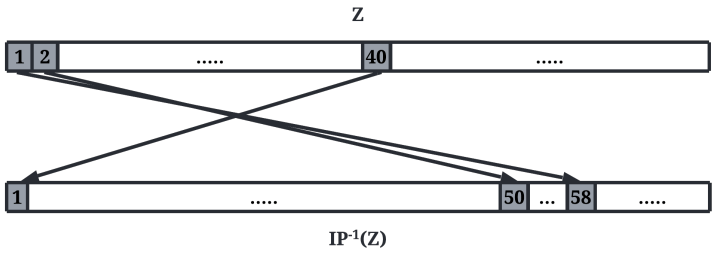


FIGURE 1.21 : Permutation finale

Le déchiffrement de l'algorithme DES s'effectue exactement de la même manière que le chiffrement, sauf que l'ordre d'application des sous-clés est inversée. Autrement dit, la sous-clés k_{16} est utilisée à la première itération, k_{15} à la seconde jusqu'à k_1 qui est utilisé à la 16^e et dernière itération.

D La diversification de la clé

Initialement, la clé de l'algorithme DES est composée de 64 bits, dont 56 bits définissent la clé k, et 8 sont des bits de parité. A chaque itération, l'algorithme utilise une clé différente k_i, avec $1 \leq i \leq 16$ de 48 bits obtenue à partir de la clé initiale k, suivant le fonctionnement du processus de diversification de la clé illustré dans la Figure 1.23.

1. Les 64 bits de la clé k sont réduits à 56 bits en surpprimant les 8 bits de parités. Ceci est réalisé par le tableau de permutation initiale PC-1, pour *permuted choice 1*.

PC-1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

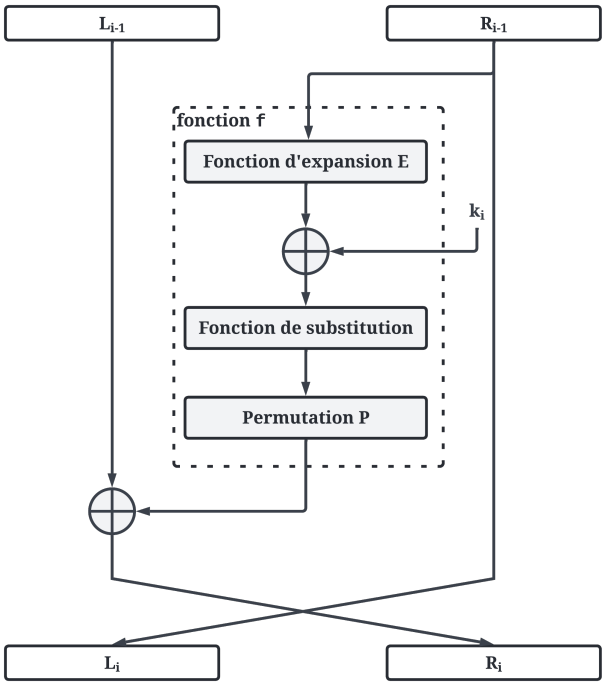


FIGURE 1.22 : Schéma de la fonction f.

2. Les 56 bits restants sont divisée en deux moitiés de 28 bits chacun LC et RC. Les moitiés LC et RC subissent un décalage vers la gauche d'une ou deux positions en fonction du tour. Le nombre de bits de décalage est donné par le tableau :

Tour	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Nombre de décalage	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

3. La valeur de la clé de tour k_i de 48 bits est obtenue par le regroupement des deux moitiés suivie d'une permutation PC-2 :

PC-2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Avec les progrès réalisés dans le domaine de la cryptanalyse et la progression de la puissance de calcul actuelles. L'algorithme DES avec sa longueur de clé fixe de 56 bits est aujourd'hui vulnérable à des attaques par force brute, ou des attaques exhaustives.

Une attaque consiste à tester toutes les clés possible, en effet une clé a une longueur de n bits, possède 2^n possibilités de clés différentes, alors $2^{(n-1)}$ essais en moyenne suffisent pour trouver la valeur de la bonne clé.

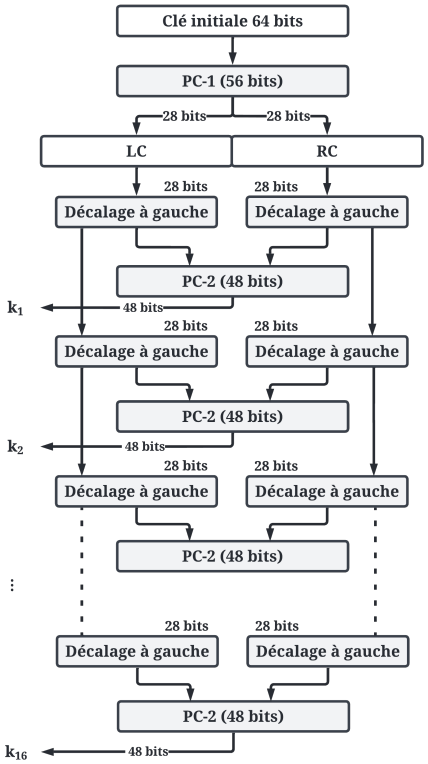


FIGURE 1.23 : La diversification de la clé k.

Pour pallier à cette faiblesse, une variance du DES en Triple-DES fut adopté en 1998. Cette variante n'est rien d'autre que l'algorithme de chiffrement DES appliqué deux fois avec un algorithme de déchiffrement DES selon le schéma suivant

$$Triple - DES_{k_1,k_2,k_3} = DES_{k_3}(DES_{k_2}^{-1}(DES_{k_1})).$$

L'algorithme Triple-DES est parfaitement sûr, d'ailleurs il est toujours utilisée pour sécuriser certaines cartes bancaires. Tout de même la recommandation actuelle est de l'éliminer progressivement en raison de sa petite longueur de bloc et du fait qu'il est trois fois plus lent que le DES. Quand le DES ne fut plus capable de répondre aux besoins de sécurité, le NIST a lançé, en janvier 1997, un appel d'offre international pour définir un successeur du DES, susceptible de subvenir aux besoins cryptographiques pendant de noumbreuses années.

Le standard de chiffrement de données a été remplacé en 2001 par l'algorithme AES, Advanced Encryption Standard, décrit dans la section suivante, avec une évaluation publique qui a duré plus de 4 ans.

VII Le nouveau standard de Chiffrement : AES

Advanced Encryption Standard (AES), également connue sous le nom de *Rijndael*, est un chiffrement moderne standard approuvé par le NIST (*National Institute of Standards*

and Technology). L'algorithme AES a été inventée par deux belges nommés Joan Daemen et Vincent Rijmen [51].

Depuis son adaptation en tant que standard, AES est l'un des algorithmes de chiffrement par blocs les plus populaires au monde qui utilise la **même clé** pour le chiffrement et le déchiffrement.

L'algorithme AES est conçu pour avoir les caractéristiques suivantes

- Résistance contre toutes les attaques connues.
- Vitesse et compacité sur une large gamme de platesformes.
- Simplicité de conception.

Le chiffrement par bloc AES autorise trois versions selon la longueur de la clé : *AES-128*, *AES-192* et *AES-256*, utilisant respectivement des clés de *128*, *192* ou *256* bits, pour des blocs de données en entrée et en sortie de *128* bits.

La taille de la clé de l'algorithme AES dépend du nombre de tours utilisés, le système AES effectue plusieurs tours d'une même composition de transformations qui seront détaillés dans la suite.

A Arithmétique dans $GF(2^8)$ du système AES

La conception de l'algorithme AES tourne autour des *corps de Galois*. Un corps de Galois, est un corps contenant un nombre fini d'éléments. Toutes les opérations d'AES s'effectuent au niveau de l'octet ou sur un mot de quatre octets.

Mathématiquement, un octet est considéré comme un élément de $GF(2^8)$, c'est-à-dire, un polynôme de degré inférieur ou égal à 7 à coefficients dans $\{0, 1\}$:

$$b_7X^7 + b_6X^6 + b_5X^5 + b_4X^4 + b_3X^3 + b_2X^2 + b_1X + b_0. \tag{1.10}$$

L'addition : L'addition de deux éléments dans $GF(2^8)$ est réalisée en ajoutant terme à terme les coefficients des deux polynômes. Cet ajout revient à appliquer un XOR sur les coefficients.

La multiplication : La multiplication dans $GF(2^8)$ est effectuée classiquement modulo un polynôme irréductible $m(X)$ de degré 8 sur $GF(2^8)$. Un tel polynôme s'écrit donc $m(X) = X^8 + X^4 + X^3 + X + 1$ ou $11B$ en notation hexadécimal.

La réduction modulaire permet de garantir que le résultat de la multiplication sera un polynôme de degré inférieur ou égal à 7.

La multiplication par X dans $GF(2^8)$: La multiplication du polynôme binaire défini dans l'équation 1.10 avec X donne

$$X \cdot b(X) = b_7X^8 + b_6X^7 + b_5X^6 + b_4X^5 + b_3X^4 + b_2X^3 + b_1X2 + b_0X. \tag{1.11}$$

Le résultat $X \cdot b(X)$ est obtenu par la réduction du résultat ci-dessus modulo $m(X)$.

Soit $b_7 = 0$, le résultat est déjà sous forme réduite modulo $m(X)$, soit $b_7 = 1$, la réduction est accomplie par la soustraction du polynôme $m(x)$.

Il s'ensuit que la multiplication par X, c'est-à-dire 00000010 ou 02, au niveau de l'octet est réaliser sous la forme d'un décalage vers la gauche suivi d'un XOR binaire avec $1B$.

B Représentation des données :

L'AES utilise les termes de représentation de données suivants :

Bit : Un bit est un chiffre binaire avec une valeur 0 ou 1.

Octet : Un groupe de 8 bits forme un octet. Un octet peut être arrangé comme une matrice de lignes de huit bits (1×8) ou une matrice de colonnes de huit bits (8×1).

$$1octet \rightarrow [b_0 b_1 b_2 b_3 b_4 b_5 b_6 b_7] \rightarrow \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix}$$

Mot : Un mot est un groupe de 4 octets qui peut être traité comme une matrice de lignes de 4 octets ou une matrice de colonnes de 4 octets.

$$1mot \rightarrow [B_0 B_1 B_2 B_3] \rightarrow \begin{bmatrix} B_0 \\ B_1 \\ B_2 \\ B_3 \end{bmatrix} où \begin{matrix} B_0 = octet_0 \\ B_1 = octet_1 \\ B_2 = octet_2 \\ B_3 = octet_3 \end{matrix}$$

Bloc : Un bloc est constitué de 16 octets.

État : Définit la condition actuelle (état) du bloc à différentes étapes de chaque tour. L'état à différentes étapes est normalement appelé "s" :

$$\begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix}$$

Les états, comme les blocs, sont constitués de 16 octets. Un état est un bloc de 128 bits ($16 \times 8 = 128$) composé d'une matrice 4×4 d'octets disposés comme suit :

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

Les 4 premiers octets du bloc d'entrée de 128 bits occupent la première colonne de la matrice 4×4 d'octets. Les 4 octets suivants occupent la deuxième colonne, et ainsi de suite ; c'est-à-dire qu'au début du chiffrement, les octets d'un bloc de données sont insérés dans un état, colonne par colonne. A la fin du chiffrement, les octets de l'état sont extraits de la même manière.

Cette matrice 4×4 est également appelée tableau d'états. Chaque cycle de traitement fonctionne dans le tableau d'état d'entrée et produit un tableau d'état de sortie.

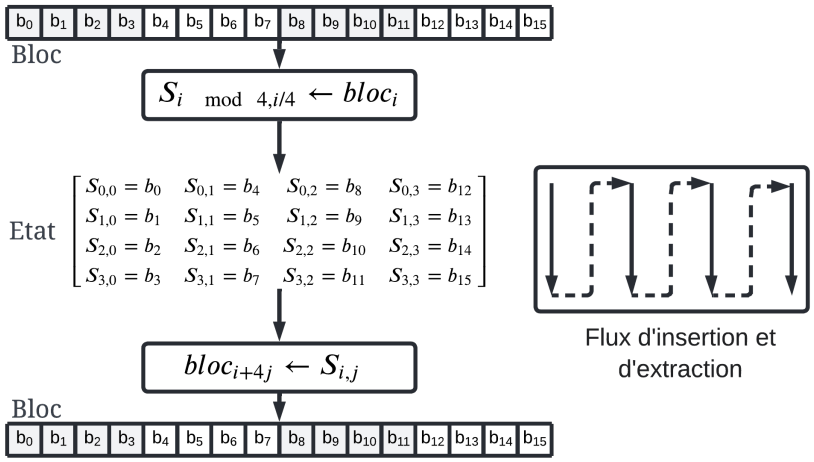


FIGURE 1.24 : Transformations du bloc à l'état et de l'état au bloc.

C Structure Générale de AES

L'AES est un algorithme *itératif*, cela signifie que les mêmes opérations sont effectuées plusieurs fois sur un nombre fixe d'octets. Ces opérations définissent un **« tour »**.

L'algorithme AES utilise plusieurs tours dans lesquels chaque tour est composé de plusieurs étapes.

- Une étape de substitution basée sur un octet
- Une étape de permutation ligne par ligne
- Une étape de mélange par colonne
- L'ajout de la clé de tour

L'ordre d'exécution de ces quatre étapes est différent pour les opérations de chiffrement et de déchiffrement. Le nombre de tours de l'algorithme dépendant de la longueur de la clé : 10 tours pour une clé de 16 octets, 12 tours pour une clé de 24 octets et 14 tours pour une clé de 32 octets, voir tableau 1.1.

Version de AES	Taille de la clé (N_k, octets)	Taille du bloc (N_b, octets)	Nombre de Tours (N_r)
AES-128	16 (*128* bits)	16 (*128* bits)	10
AES-162	24 (*192* bits)	16 (*128* bits)	12
AES-256	32 (*256* bits)	16 (*128* bits)	14

TABLE 1.1 : Taille de la clé AES et nombre de tours.

La structure globale du fonctionnement de l'algorithme AES pour une clé de chiffrement de M bits est représentée dans la figure 1.25. L'algorithme AES comprend une transformation initiale, $N-1$ tours intermédiaires et un tour final.

La transformation initiale avant le premier tour peut être considéré comme le tour 0, les $N-1$ tours intermédiaires exécutent quatre fonctions de transformation distinctes qui sont décrites plus loin, section suivante, et le tour final diffère des $N-1$ tours intermédiaires, par le fait qu'il ne contient que trois transformations.

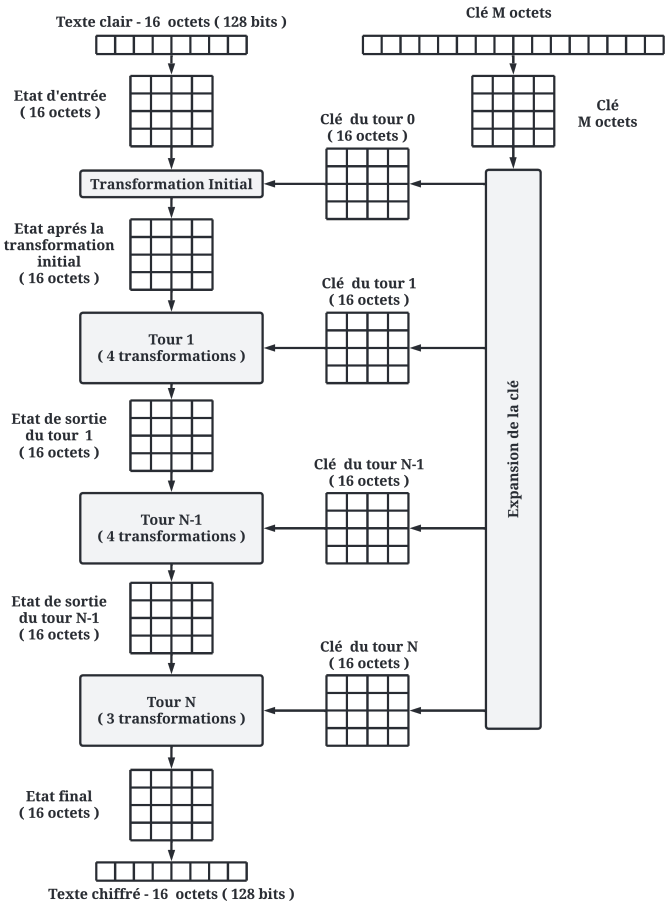


FIGURE 1.25 : Structure générale de l'algorithme AES.

Les blocs de données fournis en entrée sont transformés dans le tableau d'états qui est modifié à chaque transformation.

D Opérations de chiffrement et de déchiffrement de l'algorithme AES :

La figure 1.26 montre le chiffrement ainsi que le déchiffrement de la version *AES-128* plus détaillé, indiquant la séquence de transformations à chaque tour.

L'algorithme de l'AES dispose de deux entrées, texte clair à chiffrer de taille fixé à *128* bits et une clé de longeur *128* bits. Cette dernière subit une transformation d'expansion de clé pour générer une clé pour chacun tour à partir de la clé étendue w .

Pour les opérations de chiffrement telles que les opérations de déchiffrement, l'algorithme de l'AES commence par une étape AddRoundKey suivie de 9 tours de quatre étapes et d'un dixième tour de trois étapes. A l'exception que chaque étape d'un tour de l'algorithme de déchiffrement est l'inverse de sa contrepartie dans l'algorithme de chiffrement.

Les quatre étapes d'opération de chiffrement sont les suivantes :

- Substitute bytes

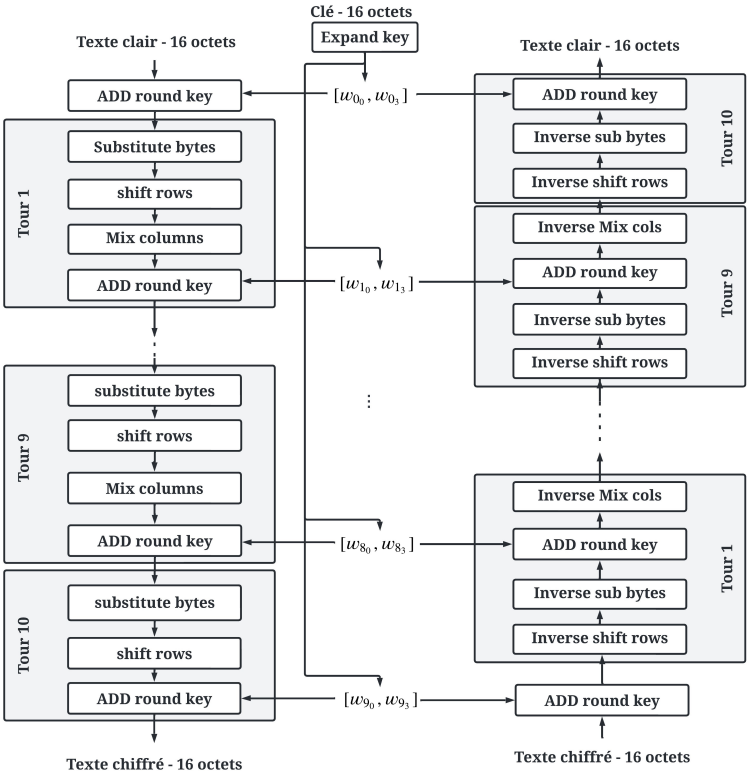


FIGURE 1.26 : Cryptage et décryptage AES.

- Shift rows
- Mix column
- Add round key

Le dixième tour, fournit un texte chiffré de 16 octets (128 bits), et correspond à un tour dans lequel l'étape Mix Columns est omise.

Pour le déchiffrement, il suffit d'utiliser les opérations inverses des quatre fonctions de chiffrement sont généralement nommées :

- Inverse Substitute bytes
- Inverse Shift rows
- Inverse Mix column
- Inverse Add round key

Encore une fois, le dixième tour supprime l'étape Inverse Mix Columns.

AES transformation functions

Pour chaque étape, nous décrivons l'algorithme direct (chiffrement), l'algorithme inverse (déchiffrement)

Transformation Add Round Key La transformation Add Round Key effectue une opération Xor de chaque *128* bits de l'état avec la clé de tour, comme le montre la figure 1.27. La transformation Add Round Key inverse est identique à la transformation Add Round Key puisque l'opération XOR est son propre inverse.

Transformation Substitute bytes La transformation de substitution d'octets , appelée

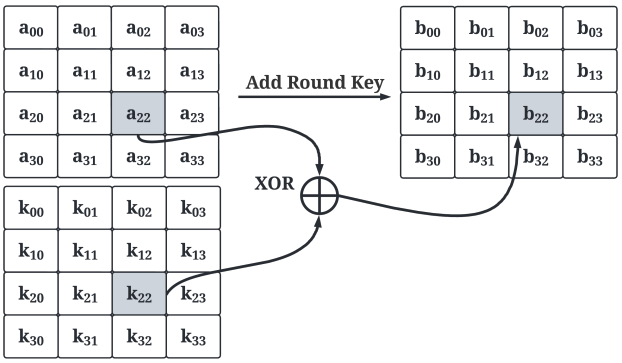


FIGURE 1.27 : Add round key.

SubBytes, est un remplacement de chaque octet de la matrice d'état par un autre octet selon une boîte S (S-box) unique et fixe. La boîte S est constituée de toutes les permuta-

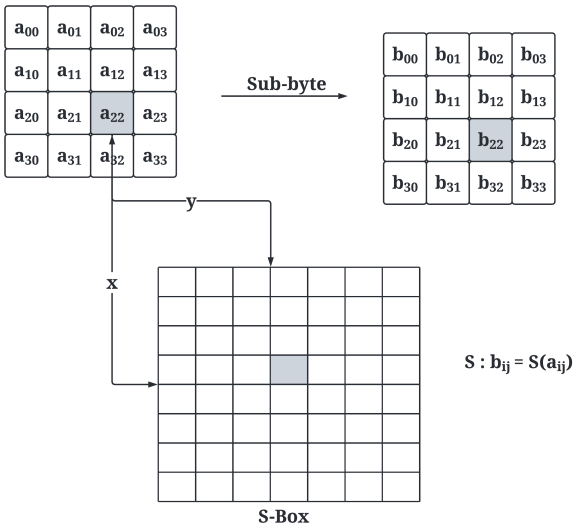


FIGURE 1.28 : Substitution byte.

tions possibles d'une séquence de 8 bits ($28 = 16 \times 16 = 256$). Cependant, la S-box n'est pas simplement une permutation aléatoire de ces valeurs, et il existe une méthode bien définie pour créer les tables S-box.

La transformation de substitution d'octet inverse, également appelée InvSubByte, utilise une S-box inverse.

Shift rows Transformation Cette transformation, illustrée à la figure 1.29, consiste à opérer une permutation circulaire sur chaque ligne de l'état. Cette permutation fonctionne comme suit :

- La première ligne reste inchangée.
- La deuxième ligne est décalée d'un octet vers la gauche de manière circulaire.
- La troisième ligne est décalée de 2 octets vers la gauche de manière circulaire
- La quatrième ligne est décalée de 3 octets vers la gauche de manière circulaire.

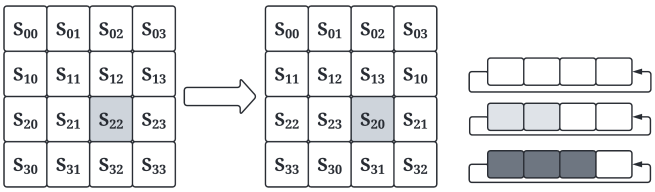


FIGURE 1.29 : Shift row transformation.

La transformation Shift row inverse, InvShiftRows, effectue les décalages ci-dessus circulaires dans le sens opposé pour chacune des trois dernières lignes.

Transformation Mix column Key La transformation MixColumns est une substitution qui utilise l'arithmétique de GF(28). Chaque colonne de l'état est vue comme un polynôme a(X) de degré 3.

Le MixColumns consiste à effectuer pour chaque colonne de l'état une multiplication par le polynôme $C(x) = 03x^3 + 01x^2 + 01x + 02$ modulo $x^4 + 1$, cela signifie, réaliser l'opération : $(03x^3 + 01x^2 + 01x + 02) \times a(X) \mod (x^4 + 1)$.

D'un point de vue matriciel, cette opération, illustrée dans la figure 1.30, s'écrit

$$b(X) = c(X) \times a(X) \mod (X^4 + 1) \Longleftrightarrow \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

Ainsi, les quatre octets d'une colonne du tableau d'états sont remplacés par les octets suivants

$$s'_{0,j} = (2 \cdot s_{0,j}) \oplus (3 \cdot s_{1,j}) \oplus s_{2,j} \oplus s_{3,j} \tag{1.12}$$
$$s'_{1,j} = s_{0,j} \oplus (2 \cdot s_{1,j}) \oplus (3 \cdot s_{2,j}) \oplus s_{3,j}$$
$$s'_{2,j} = s_{0,j} \oplus s_{1,j} \oplus (2 \cdot s_{2,j}) \oplus (3 \cdot s_{3,j}) \tag{1.13}$$
$$s'_{3,j} = (3 \cdot s_{0,j}) \oplus s_{1,j} \oplus s_{2,j} \oplus (2 \cdot s_{3,j})$$

L'inverse de la transformation MixColumn, Inverse MixColumn, effectue une multiplication par le polynôme inverse $C^{-1}(x) = 11x^3 + 13x^2 + 09x + 14$ modulo $x^4 + 1$.

Expansion de la clé

A partir d'une clé de chiffrement k de *128*, *192* ou *256* bits, l'algorithme de AES exécute un algorithme de diversification de la clé pour générer les clés de tours d'un total de $N_b(N_r + 1)$ mots = 44 mots de 32 bits soit 11 clés de *128* bits.

Cet algorithme fait intervenir deux fonctions SubWord et RotWord ainsi qu'une constante de tour Rcon.

- **Subword :** Une fonction prenant un mot de quatre octets en entrée, applique la S-Box sur chacun des octets.
- **RotWord :** La fonction RotWord prend un mot de quatre octets en entrée $w = [a0, a1, a2, a3]$, effectue une permutation circulaire sur les octets de façon à obtenir le mot $w' = [a1, a2, a3, a0]$.

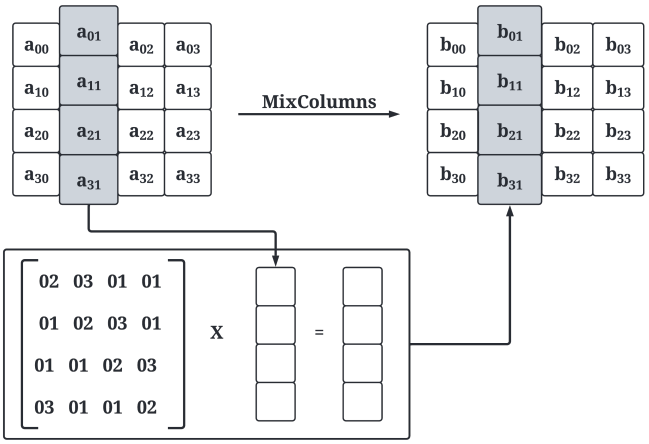


FIGURE 1.30 : Transformation Mix column Key

- La constante de tour **Rcon** est un tableau de mots de quatre octets défini par $Rcon[i] = [x^{i-1}, 00, 00, 00]$ où x^{i-1} représente un élément de GF(2^8).

Les clés de chaque tours i sont definit par : $k_i = w_{i_0} w_{i_1} w_{i_2} w_{i_3}$. Le premier mot w_{i_0} de la clé de tour i est calculé selon l'équation suivante :

$$w_{i_0} = w_{(i-1)_0} \oplus (SubWord \cdot RotWord(w_{(i-1)_3}) \oplus Rcon_i. \tag{1.14}$$

Les mots suivants w_{i_1}, w_{i_2} et w_{i_3} sont calculés selon l'équation suivante

$$w_{i_n} = w_{i_{(n-1)}} \oplus w_{(i-1)_n} \tag{1.15}$$

avec $1 \leq n \leq 3$.

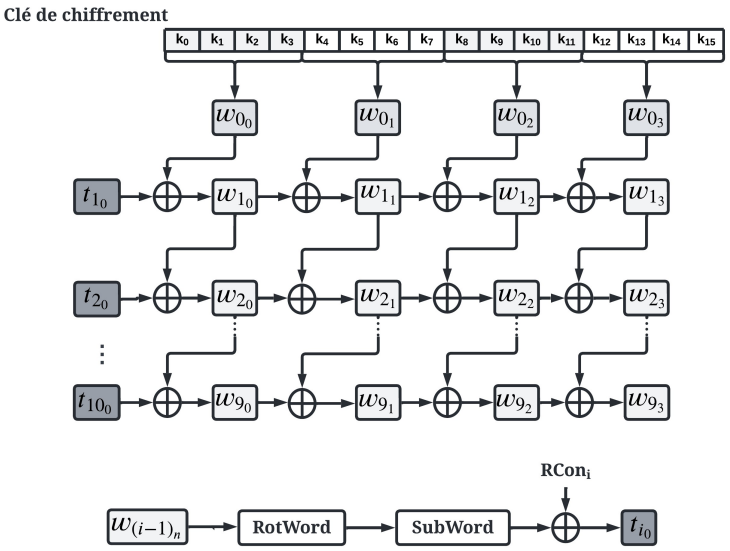


FIGURE 1.31 : Opération KeyExpansion dans AES.

L'algorithme de l'AES a fait l'objet d'un examen minutieux au cours du processus de sélection et a continué à être étudié depuis. À ce jour, il n'y a pas d'attaques cryptanaly-

tiques pratiques qui soient significativement meilleures qu'une recherche exhaustive de la clé.

Jusqu'à présent, l'algorithme de l'AES constitue un excellent choix pour tout schéma cryptographique nécessitant une permutation pseudo-aléatoire, de plus il est standardisé, efficace et hautement sécurisé.

VIII Le cryptosystème RSA

Le système **RSA**, publié en 1978, est l'une des premières réponses réussies au défi de proposer un algorithme cryptographique répondant aux exigences des systèmes à clé publique [53]. Il tire son nom des initiales de ses inventeurs : Ronald L. **R**ivest, Adi **S**hamir et Leonard M. **A**dleman.

Depuis lors, le système cryptographique à clé publique, RSA règne en maître en tant que l'un des algorithmes de chiffrement et d'authentification les plus connus et les plus utilisés à travers le monde. Ansi on le retrouve dans le protocole https qui sécurise les sites internet ou dans le logiciel de chiffrement de messages PGP. Le système RSA est un des algorithmes les plus étudiés que ce soit d'un point de vue théorique [56–59] ou pratique [60–62].

A Théories des nombres :

La théorie des nombres joue un rôle imporant dans la cryptographie. Parmi les applications en cryptographie, les plus intéressantes résident en cryptographie a clé publique. A titre d'exemple l'algorithme à clé publique RSA.

L'ensemble des entiers relatifs est noté $\mathbb{Z}$. Celui des entiers positifs est noté $\mathbb{N}$. L'expression "un entier" désigne toujours un entier relatif.

Arithmétique modulaire/ Division euclidienne

Definition VIII.1. *Soient a et b deux entiers. On dit que a divise b ou encore que a est un diviseur de b et on note $a|b$, s'il existe un entier c tel que $b = ac$. Dans ce cas, on dit également que b est un multiple de a.*

Notion de nombre premier

Definition VIII.2. *Soit p un entier positif, $p \geq 2$. On dit que p est premier si ses seuls diviseurs positifs sont 1 et lui-même.*

Proposition 2. *Soit p un nombre premier et a,b deux entiers tels que $p|ab$. Alors $p|a$ ou $p|b$.*

Algorithme d'Euclide étendu

C'est un algorithme qui permet de déterminer le plus grand commun diviseur de deux nombres. Il découle du théorème suivant :

Théorème VIII.1 (Euclide)**.** *Soient $a, b \in \mathbb{Z}$ tels que $b \neq 0$ et r le reste de la division euclidienne de a par b. Alors*

$$pgcd(a, b) = pgcd(b, r).$$

où pgcd(x,y) désigne le plus grand diviseur commun de x et y.

L'algorithme d'Euclide consiste alors à réitérer les manipulations suivantes :

- Effectuer la division euclidienne de a par b. Soit $r = a\%b$ le reste.
- Remplacer a par b et b par r
- Le *pgcd* est le dernier reste non nul.

Il existe une version étendue de l'algorithme d'Euclide, appelée **Algorithme d'Euclide étendu**, qui permet de calcluer les coéfficients de Bézout u et v tels que $au+bv = pgcd(a, b)$. L'idée est la suivante : Supposons que a et b soient des entiers positifs et que $b \neq 0$ et soit $a = bq + r$ avec $0 \leq r < b$ la division euclidienne de a par b.

Soient u' et v' les coefficients de Bezout de b et r, alors :

$$\begin{aligned} d &= pgcd(a, b) = pgcd(b, r) \\ &= bu' + rv' = bu' + (a - bq)v' \\ &= av' + (u' - qv')b \end{aligned}$$

Ainsi, les coefficients de Bézout de (a, b) peuvent être calculés à partir des coefficients de Bézout de (b, r).

Petit théorème de Fermat

Théorème VIII.2 (Petit théorème de Fermat)**.** *Soit p un nombre premier et x un entier non nul dans $\mathbb{Z}$. Alors :*

$$x^p \equiv x \mod p.$$

En particulier, pour tout entier x non divisible par p alors :

$$x^{p-1} \equiv 1 \mod p.$$

Théorème VIII.3 (Petit théorème de Fermat amélioré)**.** *Soient p et q deux nombres premiers distincts et soit $n = pq$. Pour tout $a \in \mathbb{Z}$ tel que $pgcd(a, n) = 1$ alors :*

$$a^{(p-1)(q-1)} \equiv 1 \mod n.$$

Inverse modulo n

Definition VIII.3. *On dit qu'un entier a est inversible modulo n s'il existe un entier x tel que*

$$ax \equiv 1 \mod n.$$

Proposition 3. *Soient a et n deux entiers avec $n \geq 2$. Alors, a est inversible modulo n si et seulement si $pgcd(a, n) = 1$.*

B Génération des clés :

Alice souhaite pouvoir recevoir des messages confidentiels.

Alice génére une paire de clés (publique, privée) par la méthode suivante :

1. Choisir aléatoirement deux grands nombres premiers p et q distincts, dont elle calcule le produit n, appelé *module du cryptosystème* : $n = p \times q$
2. Déterminer la fonction d'Euler $\phi(n) = (p-1)(q-1)$ associée à n.
3. Choisir un entier e l'*exposant de la clé publique*, telle que e et $\phi(n)$ soient relativement premiers.
4. Utiliser l'algorithme d'Euclide étendu pour calculer l'inverse d de e modulo $\phi(n)$, d est appelé l'*exposant de la clé secrète*.

Finalement, Alice rend public dans un annuaire les nombres n et e qui forment sa clé publique de chiffrement et garde secrets p, q et d qui forment sa clé secrète de déchiffrement.

En pratique les nombre premiers p et q sont de taille comparable de telle sorte que leur produit $n = p \times q$ soit un nombre d'au moins 300 chiffres en base 10 (128 bytes = 1024 bits en base 2).

C Description du cryptosystème RSA :

Quand Bob souhaite transmettre un message confidentiel à Alice, il commence par récupérer dans l'annuaire la clé publique de chiffrement (n, e) de Alice, et numérise le message en utilisant le code ASCII. Il découpe le message M en m blocs de taille comprise entre 0 et $n-1$. Il chiffre chacun des blocs de son message M par la formule

$$c_i = m_i^e \mod n.$$

A la réception du message chiffré C, Alice utilise la clé privée du déchiffrement (d, n) pour déchiffre chacun des blocs c_i du message chiffré par la formule

$$m_i = c_i^d \mod n.$$

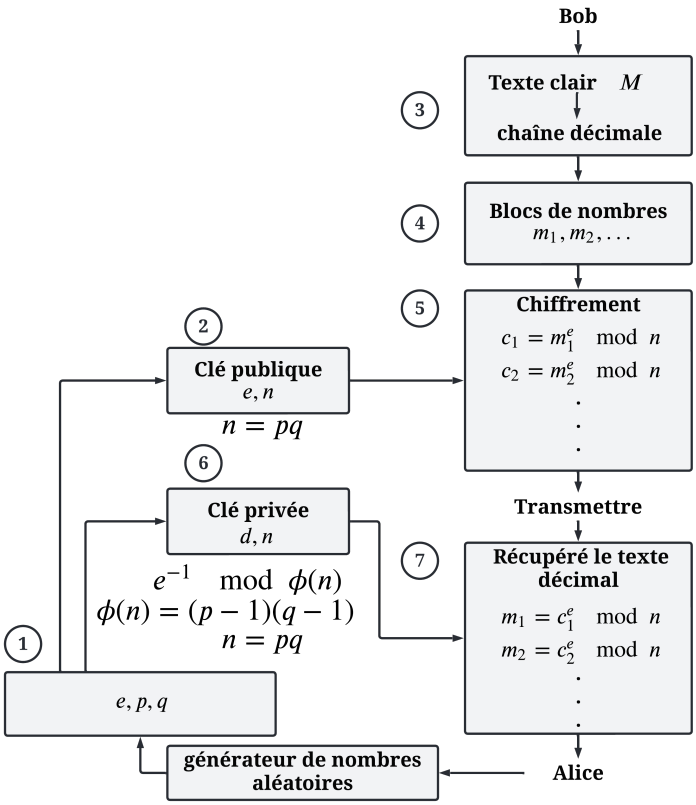


FIGURE 1.32 : Approche générale de RSA

Ensuite, Alice convertit le message numérique obtenu du code ASCII en lettres correspondantes pour retrouver le message d'origine M.

La figure 1.32 illustre les séquences des événements de l'algorithme RSA. Les nombres encerclés indiquent l'ordre dans lequel les opérations sont effectuées.

L'algorithme de cryptographie à clé publique RSA, a survécu à toutes les attaques pendant plus d'un quart de siécle. La sécurité de cet algorithme repose sur un problème reconnu comme difficile, *le problème de la factorisation d'entier*.

Il est aisé de calculer le produit de deux grands nombres premiers ; néanmoins, étant donné le résultat, retrouver les deux termes qui le composent est beaucoup plus difficile, y compris pour un ordinateur si l'on choisit des nombres assez grands.

IX Le cryptosystème El Gamal

L'algorithme **El Gamal**, décrit par Taher Elgamal en 1985 [55], appartient à la famille des cryptosystèmes à clé publique. Il fournit une alternative à l'algorithme RSA pour le chiffrement à clé publique.

Contrairement au RSA, le niveau de sécurité ne dépend pas de la difficulté à factoriser de grands entiers mais sur le problème du logarithme discret, qui semble comparable à celle du problème de factorisation, dont l'opération de base est la multiplication modulaire. Comme pour le RSA, cet algorithme peut aussi bien être utilisé pour le chiffrement de

messages ou la signature de documents électroniques.

A Théorie des groupes :

En général, l'algorithme El Gamal réalise l'échange dans le groupe multiplicatif d'un coprs fini G. De plus, les groupes cycliques sont utilisés en cryptographie notamment en ce qui concerne le problème du logarithme discret.

Definition IX.1 (Groupe)**.** *Le groupe, désigne tout couple $(G, \cdot)$ constitué par un ensemble non vide G, et d'une loi de composition interne $\cdot$ verifiant :*

1. *La loi $\cdot$ est associative i.e. : $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ pour tous $x, y, z \in G$*
2. *Il existe $e \in G$ élément neutre tel que : $e \cdot x = x \cdot e$ pour tout $x \cdot G$*
3. *$\forall x$ élément appartenant à G, il existe $x^{-1} \in G$ tel que : $x \cdot x^{-1} = x^{-1} \cdot x = e$*

Definition IX.2 (Groupe abélien)**.** *Le groupe $(G, \cdot)$ est dit **commutatif** (ou **abélien**) si*

$$x \cdot y = y \cdot x \, \forall (x, y) \in G^2.$$

L'**ordre du groupe**, noté $|G|$, est le cardinal de l'ensemble G. Si l'ensemble G contient un nombre fini n d'éléments, alors on dit que le groupe $(G, \cdot)$ est d'ordre n ; sinon, il est dit d'ordre infini.

Definition IX.3 (Groupe cyclique)**.** *Un groupe G est appelé **groupe cyclique** ou **monogène** s'il existe un élément g dans G, tel que $\langle g \rangle = \{g^k | k \in \mathbb{Z}\}$ est égal à G.*

Autrement dit, pour tout $\alpha \in G$ il existe k compris entre 0 et $n-1$ tel que $g^k = \alpha$. Cet élément g est appelé générateur ou primitif de G.

B Génération de clés

Alice souhaite se faire envoyer des messages confidentiellement en utilisant cet algorithme.

Alice génère une paire de clés (privée, publique) comme suit :

1. Choisir aléatoirement un grand nombre premier p tel que le problème du logarithme direct soit difficile.
2. Choisir un générateur du groupe multipicatif.
3. Sélectionner un nombre secret "a" compris entre 1 et $p-1$, qu'elle considère comme sa clé privée.
4. Calculer la quantité : $A = g^a \mod p$.
5. Rendre public le tripet (p, g, A) en gardant la valeur de a secréte.

C Déscription du chiffrement El Gamal

Si Bob souhaite envoyer un message M à Alice, il commence par récupèrer la clé publique (p, g, A) de Alice. Il découpe le message M en blocs m de longueur inférieure à p. Ensuite, il convertit chaque bloc en un entier m_i modulo p. Bob choisit aléatoirement un entier k compris entre 1 et $p-1$ pour chacun des blocs m_i et calcule, pour tout i,

$$c_1 \equiv g^k \mod p,$$
$$c_{2,i} \equiv m_i.A^k \mod p.$$

Le message chiffré C est le couple (c_1, c_2) que Bob envoi à Alice où $c_2 = (c_{2,1}, c_{2,2}, ...)$.

A la réception, Alice déchiffre le message en calculant à l'aide de sa clé secrète a :

$$c_{2,i}(c_1^a)^{-1} \equiv m_i \mod p.$$

Afin de retouver le message, Alice convertit chaque m_i en un bloc de lettres.

La figure 1.33 illustre les séquences des événements de l'algorithme El Gamal. Les nombres encerclés indiquent l'ordre dans lequel les opérations sont effectuées.

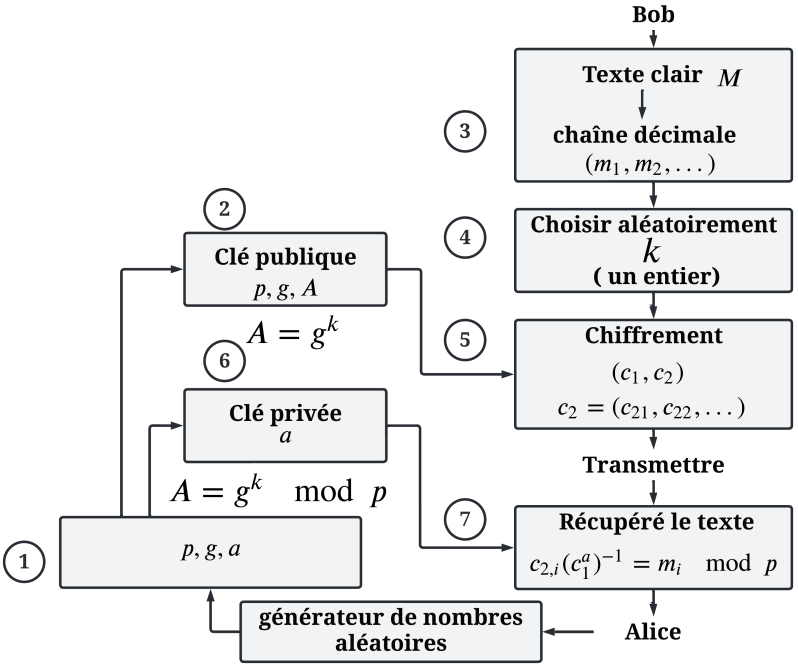


FIGURE 1.33 : Approche générale d'El Gamal.

L'algorithme de chiffrement El Gamal a la particularité d'être non déterministe. En effet, l'opération de chiffrement dépend, en plus du choix de m, d'une valeur aléatoire k choisie. Ainsi, Cet algorithme présente l'inconvénient que le texte chiffré est deux fois plus long que le texte clair.

A priori, la fiabilité de ce genre de cryptosystèmes dépend fortement des progrès fait en matière de résolution du logarithme discret. Cependant, rien ne prouve qu'il ne soit pas cassable par un autre moyen.

X La cryptanalyse

Intuitivement, la cryptanalyse est une attaque contre un cryptosystème en vue de déterminer les informations permettant de révéler leur contenus. En général, la cryptanalyse est une méthode d'analyser l'ensemble des failles d'un système cryptographique afin de les casser sans la nécessité d'avoir connaissance des outils requis tels les algorithmes de chiffrements et les clés utilisées.

La premiere méthode de cryptanalyse remonte à la civilisation arabo-musulmane, par l'utilisation de l'analyse de la fréquence des lettres pour attaquer un chiffrement de substitution. Cette méthode est décrite dans « *Manuscrit sur le déchiffrement des messages cryptographiques* » écrit par le savant Al-Kindi au IXème siécle.

Depuis lors, les techniques d'attaques contre les algorithmes de chiffrement se sont améliorées profitant de l'évolution des connaissances mathématiques et de l'explosion de la puissance de calcul des ordinateurs.

Modèles d'attaque

Il y a souvent quatre modèles d'attaques cryptanalystiques évoquées dans la littérature, chacune d'entre elles repose sur l'hypothèse que le cryptanalyste dispose de la connaissance complète de l'algorithme de chiffrement

Les attaques à texte chiffré seul :

L'attaquant a accés au texte chiffré de plusieurs messages, ayant tous été chiffrés avec le même algorithme. La tâche de l'attaquant est de retrouver le texte clair ou de trouver la ou les clés utilisées pour chiffrer les messages.

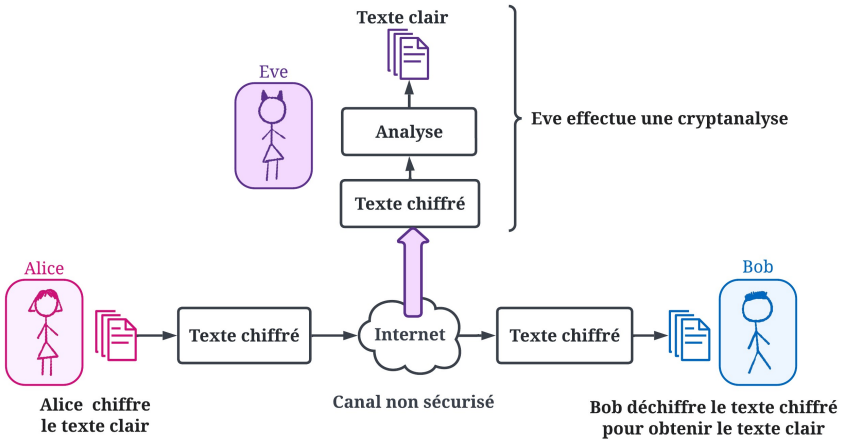


FIGURE 1.34 : L'attaque à texte chiffré seul.

Les attaques à texte clair connu :

L'attaquant possède un certain nombre de textes chiffrés de plusieurs messages ainsi que les textes en clair correspondants. C'est le cas par exemple lorsque les anciens textes

chiffrés sont dévoilés. La tâche du cryptanalyste est de retrouver la ou les clés utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clé.

Dans la figure 1.35, Alice souhaite envoyer un texte chiffré à Bob ; par la suite, Alice rend public le contenu de ce texte. L'attaquant, Eve, conserve ce texte clair comme échantillon pour casser le prochain message d'Alice à Bob, en supposant qu'Alice n'a pas changé sa clé.

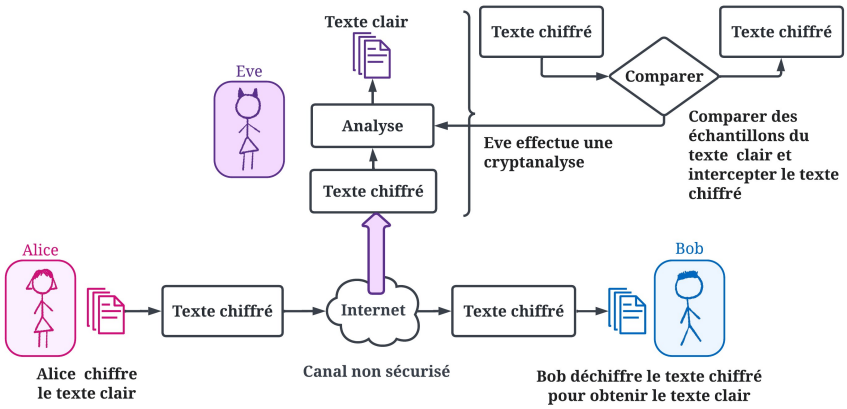


FIGURE 1.35 : L'attaque à texte clair connu.

Les attaques à texte clair choisi :

L'attaquant a accès aux textes chiffrés et aux textes en clair, de plus, il peut choisir arbitrairement les textes en clair à chiffrer. Cela est possible lorsque Eve a accès à l'ordinateur d'Alice. Il peut choisir du texte clair et intercepter le texte chiffré créé, comme illustré à la figure 1.36.

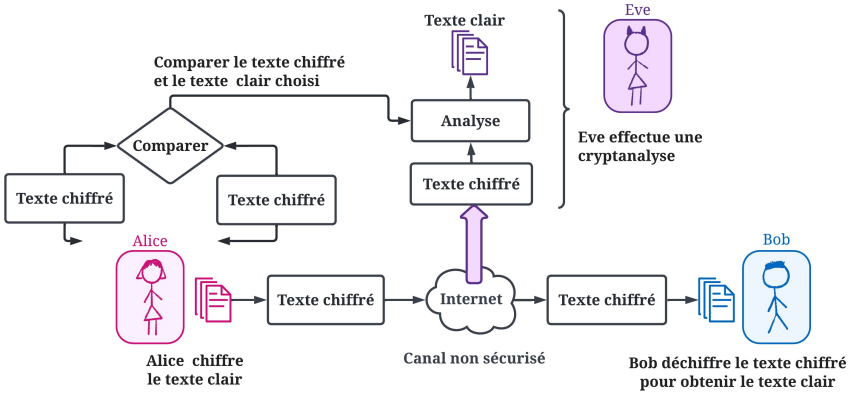


FIGURE 1.36 : L'attaque à texte clair choisi.

La tâche de l'attaquant consiste à retrouver la ou les clés utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clé.

Les attaques à texte chiffré choisi :

L'attaquant peut choisir différents textes chiffrés à déchiffrer ; les textes clairs lui sont alors fournis. L'attaquant, Eve, a la capacité de faire déchiffrer à Bob un texte chiffré sélectionné et de lui envoyer le résultat. En analysant le texte chiffré choisi et le texte clair reçu correspondant, Eve les relie pour deviner la clé envoyée qui a été utilisée par Bob. La tâche du cryptanalyste consiste à retrouver la clé utilisée pour chiffrer.

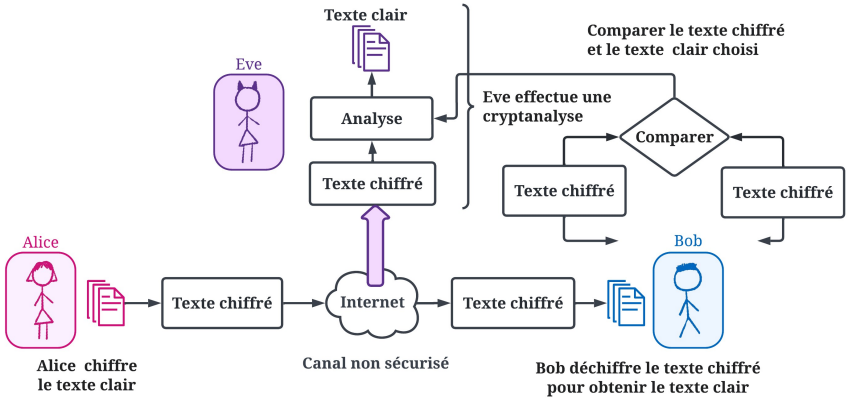


FIGURE 1.37 : L'attaque à texte chiffré choisi.

Le processus d'attaque d'un système cryptographique visant à découvrir le texte clair ou la clé est généralement perçu comme un outil destructeur, mais il sert en réalité de moyen pour renforcer la sécurité des méthodes de chiffrement, ce qui aide les cryptographes à développer des algorithmes encore plus résistants et sécurisés.

Grâce à la physique quantique, l'impensable, l'inénarrable, est.

Pascal Lefeuvre

2 Distribution quantique de clé

I De la cryptographie classique à la cryptographie quantique

La nécessité d'une communication sécurisée, même en présence d'un espion susceptible d'intercepter les informations échangées, est un problème ancien que les chercheurs tentent de résoudre depuis des siècles.

De l'antiquité jusqu'au XIX siècle la cryptographie a essentiellement été utilisée à des fins politiques et militaires. Durant la première et la deuxième guerre mondiale, la cryptographie a pris son essor avec le développement des réseaux de communication. C'est durant cette période que le secret commence à être dépendant d'une courte quantité d'informations appelée clé, permettant ainsi de révéler publiquement l'algorithme de chiffrement tout en ne gardant que la clé secrète.

Actuellement, il existe deux grandes familles la cryptographie à clé privée ou **symétrique** et la cryptographie à clé publique ou **asymétrique**.

- La cryptographie à clé privée ou symétrique est essentiellement représenté par le masque jetable, appelé **"One-Time-Pad"** en anglais, proposé par G. Vernam, qui offre une sécurité théorique absolue [63]. Malgré sa sécurité *inconditionnelle*, cette méthode est peu utilisée en pratique car elle nécessite la génération d'une *clé parfaitement aléatoire*. De plus, cette clé doit être aussi *longue* que le message, et doit être partagée entre deux partenaires distants par des moyens conventionnels, comme une rencontre préalable entre les deux interlocuteurs, ou encore, par l'utilisation d'un messager honnête.

- La cryptographie à clé publique ou asymétrique : C'est une méthode omniprésente dans les systèmes de chiffrement actuels. L'exemple le plus connu porte le nom de RSA pour R. Rivest, A. Shamir et L. Adleman [53]. La sécurité du protocole repose à la fois sur *les capacités de calcul* offertes à l'espion, et sur *la difficulté de factoriser le produit* de deux grands nombres premiers. Jusqu'à présent, aucun algorithme efficace n'a été trouvé pour factoriser de grands nombres entiers en un temps polynomial à l'aide d'un ordinateur classique.

L'avènement de l'information quantique donne lieu à des *préoccupations* importantes pour la cryptographie classique. En effet, il a été constaté que les problèmes difficiles, basés sur la **complexité du calcul**, pour un ordinateur classique peuvent être résolus efficacement par un ordinateur quantique.

Cependant, l'information quantique fournit également un moyen de résoudre le problème de la génération de clés de manière aléatoire, communément appelée **cryptographie quantique** également connue sous le nom de **distribution quantique de clés** ou **quantum key distribution (QKD)** en anglais, qui promet en principe la sécurité inconditionnelle des communications reposant uniquement sur les *lois* de la physique.

En contrepartie, la cryptographie quantique ne permet pas directement la communication de messages *intelligibles*, mais autorise principalement *la distribution de clé* cryptographique, ce qui conduit souvent à désigner la distribution quantique de clé par le terme plus général de cryptographie quantique. En effet, elle apparaît donc comme un complément de la cryptographie classique, puisqu'elle répond à son besoin de distribution de clé privée.

II Repère historique

L'histoire de la cryptographie quantique remonte au début des années 1970 lorsque Stephen Wiesner a écrit *Conjugate Coding*. Malheureusement, cet article était tellement en avance sur son temps qu'il est passé presque inaperçu jusqu'au 1983 [64].

Wiesner a expliqué le principe de l'utilisation de la mécanique quantique pour fabriquer des billlets de banque imposssibles à contrefaire selon les lois de la nature, et a également suggéré un canal de multiplexage quantique permettant de multiplexer deux messages de façon à ce qu'il soit possible de récupérer parfaitement l'un des deux au prix de la destruction irréversible de l'autre message.

Suite à ces idées, Charles H.Bennett, Gilles Brassard, Seth Breidbart et Stephen Wiesner, ont montré comment combiner les *techniques* de la cryptographie à clé publique avec le *codage quantique* dans l'intention d'aboutir à la fabrication des jetons de métro *infalsifiables* correspondant à un stockage quantique de l'information [65].

Un an après la publication des travaux fondateurs de Wiesner, Bennett et Brassard ont réalisé que les photons sont mieux utilisés pour transmettre des informations quantique plutôt que pour les stocker. Peu de temps après, Bennett et Brassard ont proposé en 1984 la première idée de distribution de clé quantique, d'où le nom du **protocole BB84**, exploitant à nouveau les propriétés contre-intuitives de la mécanique quantique.

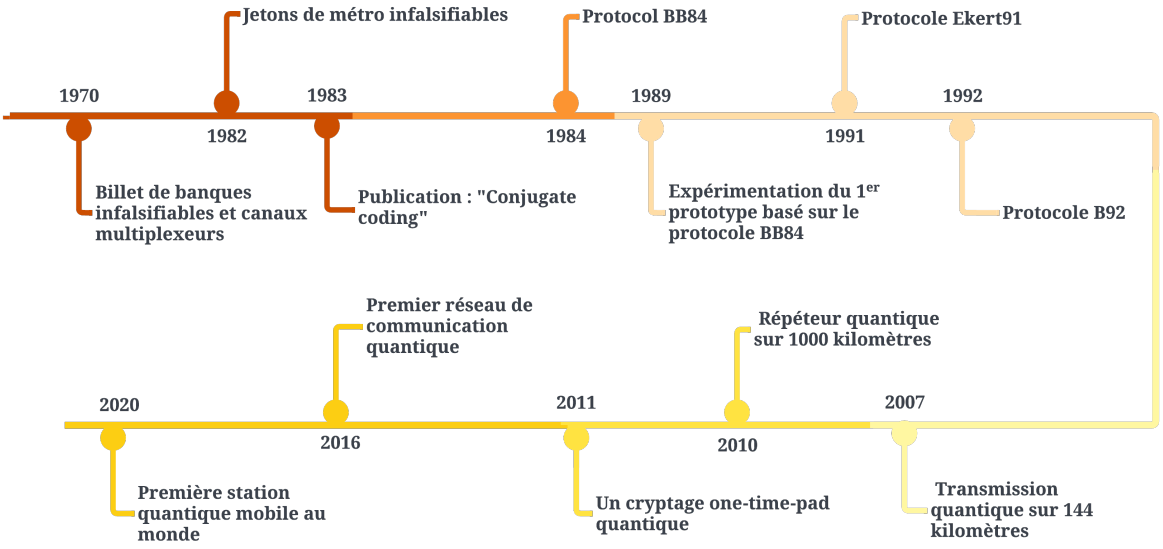


FIGURE 2.1 : La chronologie de l'histoire.

Bien que leur article ait également rencontré des difficultés à être publié, il est devenu l'article fondateur qui a donné naissance du domaine, désormais très prolifique, de la cryptographie quantique [66].

Les deux chercheurs ont décidé qu'ils devaient démontrer physiquement leur schéma pour suscité beaucoup d'enthousiasme dans la communauté scientifique. En 1989, Ils recrutèrent de l'aide et effectuent une première transmission quantique de clés secrètes de plusieurs milliers de bits entre deux points distants de 32 centimètres en air libre.

Suite au protocole BB84, d'autres protocoles de distribution quantique de clé ont été proposés. En 1991, Artur Ekert a développé une approche différente de la distribution quantique des clés basée sur des corrélations quantiques particulières connues sous le nom **d'intrication quantique** [67].

En 1992, Bennett a proposé une mise en oeuvre du protocole BB84 connu sous le nom de **protocole B92**. Ceci a donné lieu depuis à de nombreux réalisations dans les *aspects théoriques* et *pratiques* de la distribution quantique des clés.

Aujourd'hui, le domaine suscite un énorme intérêt dans le monde entier, et les expériences qui transmettent de véritables bits quantiques établissent constamment de nouveaux records en termes de distance.

Comme mentionné ci-dessus, Bennett et Brassard ont commencé en 1989 par mesurer les distances en centimètres, et progressaient de là à des distances d'environ 100 kilomètres. Entre-temps, le record de transmission de photons en plein air a atteint 144 kilomètres, d'une clé envoyée d'une île Canaries à une autre.

En 2010, lors de la réunion annuelle de l'OSA, *Optical Society of America*, des chercheurs du Georgia Institute of Technology avait construit un répéteur quantique qui permet d'envoyer des bits quantiques sur des distances de 1 000 kilomètres ou plus.

En 2011, un article intitulé *Field test of quantum key distribution in the Tokyo QKD Network* avec 46 auteurs [68] décrivait un réseau de distribution quantique de clé qui

réalisait un cryptage quantique **OTP**, *One-Time Pad*, pour des distances allant jusqu'à 135 km à un débit suffisamment rapide pour permettre la sécurisation de la visioconférence.

En 2016, la Chine a mis en place un canal quantique de 2 000 Km de long, reliant Pékin et Shanghai. Ce canal s'appuie sur 32 noeuds de confiance en cours de route pour rafraîchir le signal [69].

Les Chinois ont également lancé un satellite, en 2016, dans le but d'établir un lien pour la distribution de clés quantiques en orbite. En 2020, il échangeait avec succès la clé avec une station terrestre mobile, pèse plus de 80 kg.La fabrication de cette station terrestre quantique mobile a été motivée par la demande de la *Banque industrielle et commerciale de Chine* (ICBC) qui cherche à utiliser ce type d'équipement pour sécuriser ses infrastructures à l'aide de clés quantiques mais avec des stations au sol plus lourdes, mais plus rapides.

III Notions de la mécanique quantique

La mécanique quantique représente une des théories scientifiques les plus révolutionnaires du XX^e siècle développée à l'origine par des scientifiques tel que Max Planck, Albert Einstein, Niels Bohr ou encore Erwin Schrödinger.

La mécanique quantique est une branche de la physique qui se concentre sur les *plus petites* échelles soit les domaines atomique et subatomique.

L'idée d'utiliser les atomes, photon et autres particules en tant que *ressources* pour le traitement de l'information a conduit à offrir des *performaces* considérablement améliorées par rapport à la physique classique qui sert à décrire des phénomènes macroscopiques.

A Etat quantique

L'état quantique est un objet fondamental de la mécanique quantique réside dans un espace de Hilbert, $\mathcal{H}$, de dimension finie d. Un espace de Hilbert est un espace vectoriel muni d'un produit scalaire, et est complet par rapport à la norme définie par le produit scalaire.

Un qubit est un état quantique bidimensionnel, décrit par un espace de Hilbert à deux états de base dont les éléments sont des vecteurs, notés suivant la notation de Dirac, $|0\rangle, |1\rangle \in \mathcal{H}$:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad\qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{2.1}$$

Les vecteurs forment une base particulière $\{|0\rangle, |1\rangle\}$ appelée **base rectiligne** de l'espace de Hilbert associé à un qubit. En effet, un qubit peut être non seulement dans l'état $|0\rangle$ ou $|1\rangle$, mais il peut être trouvé dans des états de *superposition* arbitraires selon la mécanique quantique.

En termes mathématiques, tout état du qubit peut être écrit comme :

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2.2}$$

où α et β sont des nombres complexes, représentant les amplitudes de probabilités d'obtenir $|0\rangle$ ou $|1\rangle$ respectivement lors de la mesure de $|\psi\rangle$, respectant la condition de normalisation :

$$|\alpha|^2 + |\beta|^2 = 1. \tag{2.3}$$

Un qubit est par nature une unité à deux états, défini par le spin d'un électron qui peut pointer vers le haut ou le bas, un état de la polarisation d'un photon (*horizontale, verticale ou circulaire*) ou encore un atome qui peut se retrouver dans l'état *fondamental* ou *excité*, etc.

Sphère de Bloch

L'espace de Hilbert bidimensionnel utilisé pour décrire l'espace vectoriel associé aux états de qubit peut être projeté sur la surface d'une sphère. Cette sphère, connue sous le nom de **sphère de Bloch**, permet de visualiser l'état d'un seul qubit dans un espace tridimensionnel comme le montre la figure 2.2. Un qubit peut exister sur n'importe quel point de la surface de la sphère de Bloch.

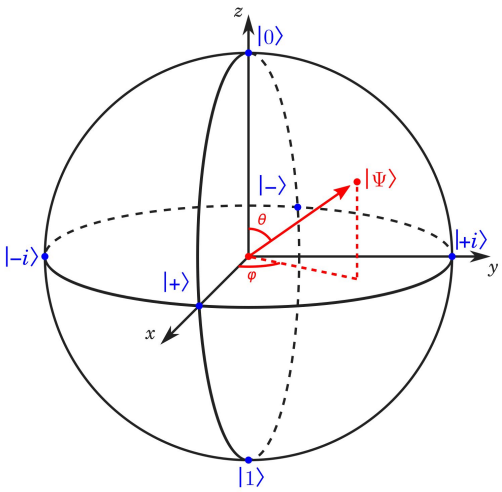


FIGURE 2.2 : Représentation d'un état quantique sur la sphère de Bloch.

Un état de qubit tel que celui écrit dans l'équation 2.2 peut être réécrit comme suit :

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle, \tag{2.4}$$

avec $\theta \in [0, \pi]$ et $\phi \in [0, 2\pi]$. Les réels θ et ϕ définissent un point unique sur la sphère, comme le montre la figure 2.2, de coordonnées (x, y, z) :

$$\begin{aligned} x &= \sin\theta\cos\phi \\ y &= \sin\theta\sin\phi \\ z &= \cos\theta \end{aligned} \tag{2.5}$$

Jusqu'à présent, l'état d'un qubit est représenté comme une combinaison linéaire des vecteurs de la base rectiligne $\{|0\rangle, |1\rangle\}$. Néanmoins, l'état d'un qubit dans un espace de

Hilbert à deux dimensions peut être représenté généralement comme une combinaison linéaire de deux vecteurs d'état orthonormés quelconques. Il existe deux autres bases dites conjuguées sont $\{|+\rangle, |-\rangle\}$ et $\{|+i\rangle, |-i\rangle\}$ donné par :

$$|+\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{2.6}$$

$$|+i\rangle := \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \qquad |-i\rangle := \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \tag{2.7}$$

Ces trois ensembles d'états, $\{|0/1\rangle\}$, $\{|+/-\rangle\}$ et $\{|+i/-i\rangle\}$ correspond aux états propres des opérateurs de Pauli σ_z, σ_x et σ_y respectivement, forment un ensemble de vecteurs mutuellement orthogonaux sur la sphère de Bloch, figure 2.2.

Un état quantique est défini comme un vecteur pointant à la surface de la sphère de Bloch caractérisé par les angles θ et ϕ à condition que la relation de normalisation est respectée.

Mesure quantique

La mesure quantique est une opération physique *irréversible*, appliquée à un état quantique, détruit l'information quantique sur une propriété mesurable, appelé **observable**, d'un système quantique et la remplace par une information classique.

En mécanique quantique, la mesure d'un état quantique a pour conséquence de projeter l'état dans une base de mesure. Le résultat de cette mesure, sur un qubit dans une superposition de deux états, est probabiliste et aléatoire.

Les probabilités de détection sont données par les modules carrés des amplitudes de probabilités. Formellement, pour un état général $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ la probabilité d'obtenir $|0\rangle$ (respectivement $|1\rangle$) lorsqu'on mesure $|\psi\rangle$ dans la base recteligne est de $|\alpha|^2$ (respectivement $|\beta|^2$).

De manière plus générale, le principe de mesure en mécanique quantique est aussi associé à un opérateur hermitique agissant sur des vecteurs de l'espace de Hilbert $\mathcal{H}$, permettant de déterminer les résultats possibles avec les probabilités associées à chaque résultat d'une mesure pour un état quantique.

B Polarisation des photons

La lumière est l'ensemble des ondes électromagnétiques transversales composées des vecteurs de champ électrique et magnétique perpendiculaires les uns aux autres et également perpendiculaires à la direction de propagation. Classiquement, la polarisation de la lumière est le comportement du vecteur champ électrique dans le plan transverse à la direction de propagation. En général, il existe plusieurs sortes de polarisation : linéaire, circulaire et elliptique.

En mécanique quantique, la lumière est constituée d'unités élémentaires appelées photons, ces dernière transportent une quantité fixe d'énergie et constituent le support de l'information.

L'état de polarisation d'un photon est l'une des observables les plus utilisées pour encoder de l'information et notamment générer des qubits. A titre d'illustration des concepts

précédents, l'état de polarisation **horizontale** $|H\rangle$ est associé à l'état $|0\rangle$ tandis que l'état de polarisation **verticale** $|V\rangle$ est associé à l'état $|1\rangle$. L'ensemble $\{|H\rangle, |V\rangle\}$ est une base pour l'espace de Hilbert décrivant la polarisation d'un photon. De plus, leur combinaison linéaire permet d'obtenir d'autres états de polarisation tel que l'état de polarisation **diagonale** à 45°, polarisation **anti-diagonale** 135° et l'état de polarisation **circulaire**.

Base rectiligne	+	:	Horizontale	$\|H\rangle$	$\equiv$	$\|0\rangle$
			Verticale	$\|V\rangle$	$\equiv$	$\|1\rangle$
Base diagonale	$\times$	:	Diagonale	$\|A\rangle$	$\equiv$	$\|+\rangle$
			Anti-diagonale	$\|D\rangle$	$\equiv$	$\|-\rangle$
Base circulaire	◯	:	Circulaire droit	$\|R\rangle$	$\equiv$	$\|+i\rangle$
			Circulaire gauche	$\|L\rangle$	$\equiv$	$\|-i\rangle$

C L'intrication

La physique quantique permet de préparer une paire ou un groupe de systèmes dans un état tel qu'ils auront une connexion spécifique, ce qui rend impossible la description des systèmes séparément les uns des autres. Une telle relation persiste même si les systèmes sont séparés par des distances infiniment grandes.

Etats à deux qubits

Considérons un système quantique constitué de deux qubits labellisés A et B. Le qubit A peut être exprimé comme une superposition des deux états $|0\rangle_A$ et $|1\rangle_A \in \mathcal{H}_A$. De même, le qubit associé à la particule B peut être exprimé en superposition dans la base $\{|0\rangle_B, |1\rangle_B\}$ de l'espace de Hilbert $\mathcal{H}_B$.

L'état $|\psi\rangle_{AB}$ du système global est considéré comme un vecteur dans un espace de Hilbert $\mathcal{H}_{AB}$ de dimension 2^2, défini mathématiquement comme étant le produit tensoriel des espaces de Hilbert associés à chaque qubit.

Grâce au principe de superposition, l'état de ce système s'éxprime alors comme une combinaison linéaire des états possibles du système :

$$|\psi\rangle_{AB} = \alpha|0\rangle_A|0\rangle_B + \beta|0\rangle_A|1\rangle_B + \gamma|1\rangle_A|0\rangle_B + \delta|1\rangle_A|1\rangle_B, \tag{2.8}$$

où $\alpha, \beta, \gamma, \delta \in \mathbb{C}$, respectant la règle de normalisation

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1. \tag{2.9}$$

Lorsque l'état du qubit A est connu, $|\psi\rangle_A = \alpha_A|0\rangle_A + \beta_A|1\rangle_A$, et que l'état du qubit B est aussi connu, $|\psi\rangle_B = \alpha_B|0\rangle_B + \beta_B|1\rangle_B$, alors l'état du système global $|\psi\rangle_{AB}$ peut être exprimer à partir du produit tensoriel suivant :

$$\begin{aligned} |\psi\rangle_{AB} &= |\psi\rangle_A \otimes |\psi\rangle_B \\ &= \alpha_{AB}|0\rangle_A|0\rangle_B + \beta_{AB}|0\rangle_A|1\rangle_B + \gamma_{AB}|1\rangle_A|0\rangle_B + \delta_{AB}|1\rangle_A|1\rangle_B, \end{aligned} \tag{2.10}$$

avec

$$\begin{cases} \alpha_{AB} & = \alpha_A \alpha_B \\ \beta_{AB} & = \beta_A \alpha_B \\ \gamma_{AB} & = \alpha_A \beta_B \\ \delta_{AB} & = \beta_A \beta_B \end{cases}$$

En revanche, il n'est pas toujours possible de décrire l'état de deux qubits comme un état factorisable, en établissant un produit tensoriel de l'état du qubit A par l'état du qubit B *i.e* $|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B$. De tels état non séparable est appelé états intriqué.

Les états intriqués

L'intrication quantique est un phénomène particulier à l'échelle subatomique n'ayant pas de l'équivalent dans le monde macroscopique.

Ce phénomène implique deux particules ou plus. Théoriquement, il n'y a pas de limite au nombre de particules pouvant être intriquées, pratiquement il s'agit d'une procédure complexe, généralement réalisée avec une paire de particules.

Après le processus d'intrication dans lequel une paire de particules interagit physiquement et se lient d'une certaine manière, l'état quantique d'une particule est fortement corrélé à l'autre de telle sorte que toute action effectuée sur l'une affecte l'autre. Cette liaison est toujours valable même si les deux particules sont placées à de grandes distances.

Mathématiquement, deux états intriqués peuvent être exprimés comme suit :

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b + |1\rangle_a|0\rangle_b)$$

Cet état est l'un des quatre états de Bell intriqués au maximum. La mesure sur cette état peut conduire au résultat $|00\rangle$ ou $|11\rangle$ avec une probabilité de 50%. En outre, il n'y a aucune chance que des qubits puissent être trouvés dans les états $|01\rangle$ ou $|10\rangle$.

Ainsi, si une mesure est effectuée sur le qubit A, et que le résultat de cette mesure est l'état $|0\rangle$, alors en déduit immédiatement que le qubit B est à l'état $|0\rangle$ avec une probabilité de 100% et vice-versa pour l'état $|1\rangle$.

Il existe les 3 autres états de Bell qui sont les suivants :

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b + |1\rangle_a|1\rangle_b)$$
$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a|0\rangle_b - |1\rangle_a|1\rangle_b)$$
$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_a|1\rangle_b - |1\rangle_a|0\rangle_b)$$

Historiquement, Les états de Bell furent les premier états maximalement intriqués entre deux qubits introduit dans la littérature.

D Principe d'incertitude de Heisenberg

La mécanique quantique ne nous permet pas de visualiser correctement le mouvement de la particule quantique en raison des propriétés ondulatoires des particules. Ceci implique en fait l'incertitude de la mesure quantique.

Heisenberg a reconnu ces propriétés et a prédit que, puisque les particules de la mécanique quantique ont une propriété d'onde, elles ne peuvent pas avoir ni une position et une vitesse bien définies ni une position et une impulsion. En d'autres termes, les nouvelles lois quantiques impliquent une limitation fondamentale de la précision des mesures expérimentales.

Cependant la mesure de la position et de l'impulsion d'une particule de mécanique quantique doit obéir à une limitation donnée par l'inégalité d'incertitude de Heisenberg

$$\Delta x \Delta p \geq \hbar/2 \tag{2.11}$$

où $\hbar = h/2\pi$ est la constante de Planck réduite, x désigne la position de la particule et p désigne sa quantité de mouvement. Les variances Δx et Δp représentent les incertitudes.

L'inégalité de Heisenberg suggère qu'il est impossible de mesurer les quantités x et p aussi précisément souhaitable. En d'autres termes, il est impossible de réduire à la fois Δx et Δp, car le produit des incertitudes doit toujours être égal ou supérieur à une constante. En termes plus explicites, si la position est mesurée avec précision, la quantité de mouvement sera totalement aléatoire ou incertain, et vice versa.

Le principe d'incertitude de Heisenberg peut être prouvé avec précision à l'aide d'outils mathématiques. En général, le principe d'incertitude de Heisenberg s'écrit sous la forme :

$$\Delta \hat{A} \Delta \hat{B} \geq |\langle [\hat{A}, \hat{B}] \rangle|/2, \tag{2.12}$$

où $\hat{A}$ et $\hat{B}$ sont des opérateurs de mécanique quantique, $[A, B] = AB - BA$ représente la relation de commutation et $\langle \ldots \rangle$ désigne la moyenne. L'équation 2.11 peut être retrouver si les opérateurs $\hat{A}$ et $\hat{B}$ satisfont $[A, B] = i\hbar$.

L'inégalité 2.12 suggère que deux opérateurs quantiques non-commutants ne peuvent pas être mesurés simultanément avec précision arbitraire.

Le principe d'incertitude contre une écoute clandestine

Le principe d'incertitude de Heisenberg suggère que pour deux observables non commutants, la mesure précise d'une observable randomise nécessairement la valeur de l'autre. Cette incertitude peut être utilisée pour mettre en œuvre une communication sécurisée.

Pour la transmission des qubits sur de grandes distances, le support privilégié est le photon, qui autorise l'encodage de l'information sur des observables telles que la polarisation. Un photon peut être polarisé dans les orientations suivantes : **horizontale**, **verticale**, **diagonale** à 45° diagonale, **anti-diagonale** à 135°, **circulaire gauche**, et **circulaire droite**. Ces orientations appartiennent à trois bases :

Base rectiligne	$+$	$\rightarrow$	{ Horizontale, Verticale }
Base diagonale	$\times$	$\rightarrow$	{ Diagonale, Anti-diagonale }
Base circulaire	$\bigcirc$	$\rightarrow$	{ Circulaire droit, Circulaire gauche }

La figure 2.3 illustre des photons polarisés traversent un prisme de Wollaston dont l'angle est fixé à 0° correspondant à état de polarisation horizontale de la base recteligne, de sorte que le détecteur peut mesurer la polarisation des photons à 0° ou 90° avec certitude.

Dans le cas particulier, où la polarisation des photons correspondant à la base x, le résultat de la mesure montre que la moitié des photons apparaissent à gauche avec l'angle de 0° et la moitié d'entre eux apparaissent à droite avec l'angle 90°. Une situation analogue se présente dans le cas des photons avec des polarisations circulaires sont utilisés.

L'implication de l'analyse ci-dessus est que l'utilisation de deux bases arbitraires pour mettre en oeuvre une communication conduit vers une communication sécurisée. Cela est dû au fait que toute écoute utilisant une mauvaise base sera traduit par une polarisation aléatoire des photons, ce qui cause sa détéction par le récepteur.

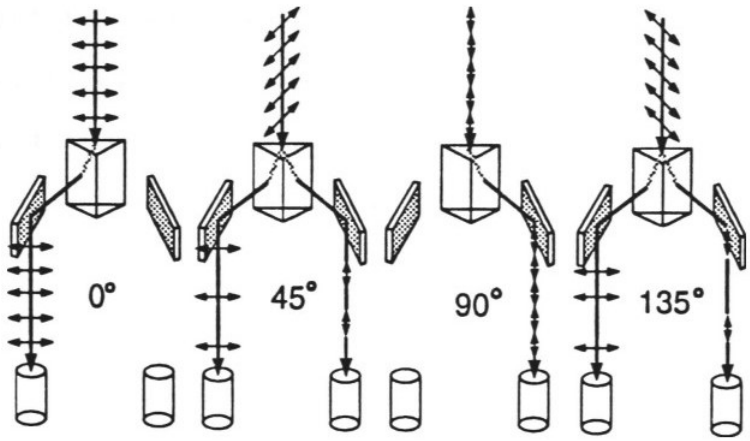


FIGURE 2.3 : Des photons polarisés passent à travers un prisme de Wollaston.

IV La distribution quantique de clés :

Distribution de clé quantique, ou quantum key distribution en anglais, comme son nom l'indique c'est une technique de distribution à distance de clés secrètes. Plus précisément, elle consiste à utiliser les propriétés de la physique quantique pour échanger une chaine de bits secrète entre deux interlocuteur distants, traditionnellement appelés Alice et Bob, à travers un environnement contrôlé par un espion, Ève, qui tente d'intercepter la communication.

A Objectif du protocole

La distribution quantique de clés est un protocole permettant d'établir un secret commun entre deux interlocuteur distants. La distribution de clés est une primitive essentielle

utilisée par un algorithme de cryptographie conventionnel telles que le masque jetable en vue d'avoir un système parfaitement sûr.

L'objectif du protocole est d'assurer des communications inviolables. Autrement dit s'assurer que l'espion Eve ne puisse pas obtenir d'information sur la clé partagée par Alice et Bob.

B Ressources nécessaires aux protocoles

Le schéma général d'un protocole de distribution quantique de clé est représenté dans la figure 2.4. Alice et Bob disposent d'un canal de transmission quantique pour le partage de l'information, il s'agit d'une fibre optique où l'espion peut y accéder et manipuler. Ainsi que d'un canal publique ou bien classique authentifié, déstiné à la communication où l'espion a accès à son contenu mais ne peut pas modifier les messages qui y passent, ce canal peut être une ligne téléphonique ou généralement un réseau internet.

La distinction faite entre les deux canaux tient uniquement au type de l'information transmise, les états quantiques dans le premier canal et les bits de l'information classiques dans le second.

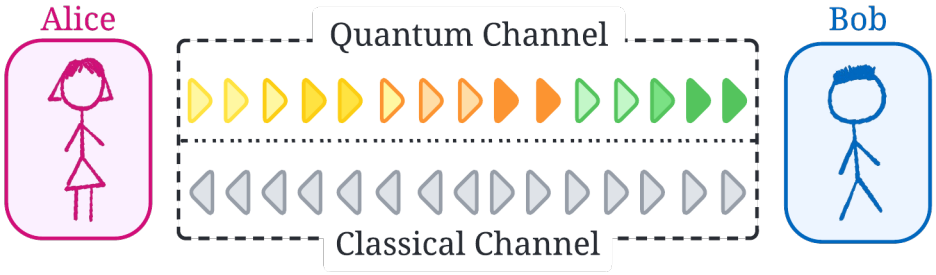


FIGURE 2.4 : Le protocole de distribution quantique de clé.

C Le protocole générique de distribution quantique de clés

Un protocole général de distribution quantique de clé se compose de différentes étapes, illustrées dans la figure 2.5.

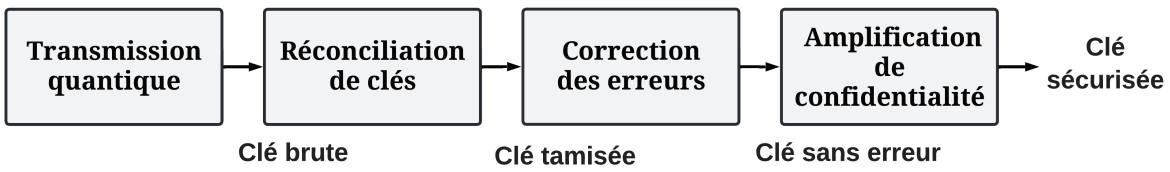


FIGURE 2.5 : Les étapes du protocole général de distribution quantique de clé.

Transmission quantique

Dans cette première étape, qui est le noyau du protocole de distribution quantique de clé, Alice et Bob partagent une chaîne aléatoire de bits transmise sur un canal quantique. La plupart des protocoles de distribution quantique de clés basés soit sur des qubits uniques, soit sur des paires de qubits intriqués.

Les protocoles à qubit unique utilisent les propriétés d'incertitude de mesure, discutées à la Sec.D, pour assurer la sécurité de la transmission. Des exemples importants de protocoles à qubit unique sont les protocoles BB84, B92 et le protocole à six états [66, 70–72]. Les Sec.V,VI sont désignée à la discussion du protocole BB84 et B92 respectivement. Dans ce type de protocole, Alice prépare des qubits uniques à partir de ses choix de bits classiques. Cela revient à choisir de façon aléatoire une base, généralement parmi deux bases non orthogonales, de même que la valeur en bits de ses qubits uniques et les envoie à Bob sur un canal quantique. Bob mesure également chaque qubit sur une base choisie au hasard. Ceci conclut l'étape de transmission quantique.

Les protocoles de qubit intriqués utilisent les corrélations non locales discutées dans les Sec. VIII et IX pour assurer la sécurité de communication. Ils reposent sur le fait que s'il existe une variable locale qui prédit l'état d'une paire de qubits intriqués, alors les corrélations non locales ne sont pas observées. Des exemples importants de protocoles qubit intriqués sont les protocoles Ekert91 et BBM92 [67, 73] détaillé dans la Sec. VIII et IX respectivement.

Dans ce type de protocole, au lieu de préparer des photons uniques, Alice et Bob reçoivent chacun un qubit d'une paire de photons intriqués et mesurent son état dans une base choisie aléatoirement. Le résultat de la transmission quantique est une séquence de bits appelé clé brute.

Réconciliation des clés

Dans l'étape de réconciliation des clés, Alice et Bob échangent à travers un canal de communication classique des informations liées à leur mesure en particulier les bases utilisées pour préparer ou mesurer leurs qubits. À ce stade, Alice et Bob rejettent les bits dans le cas où ils utilisaient des bases différentes.

Les imperfections des systèmes expérimentaux et les contraintes environnementales s'exerçant sur le canal de transmission sont les sources d'erreurs qui ne peuvent pas être distinguées des erreurs dues à l'écoute clandestine. Ainsi la déclaration selon laquelle toute écoute clandestine entraînera inévitablement des erreurs et révélera l'écoute clandestine, n'est pas une preuve de sécurité suffisante.

Les systèmes expérimentaux de distribution quantique de clés gèrent les erreurs du système et l'écoute clandestine en complétant la transmission quantique et la réconciliation par deux étapes supplémentaires importantes : la correction des erreurs et l'amplification de la confidentialité. Ces étapes sont effectuées à l'aide d'un canal de communication publique et il ne nécessite aucun échange supplémentaires de qubits.

Correction des erreurs

L'étape de correction des erreurs a pour double objectif de corriger tous les bits erronée reçus et de donner une estimation du taux d'erreur. Cela ne peut se faire qu'en échangeant des informations supplémentaires sur le canal de communication publique et décider soit de poursuivre le reste du protocole ou d'abandonner le protocole si le taux d'erreur est substantiel.

A titre d'exemple, Alice et Bob peuvent regrouper leurs bits en segments et vérifier la parité de chaque segment, optimisant ainsi la taille du segment au fur et à mesure que le processus de correction des erreurs se poursuit.

Amplification de confidentialité

Afin de tenir compte des informations que Eve pourrait obtenir lors de la transmission quantique ou/et lors de la correction d'erreur, une étape finale d'amplification de la confidentialité est réalisée.

Dans l'étape de l'amplification de la confidentialité, Alice et Bob appliquent une transformation sur leur chaîne de clés, bits partiellement secrètes, produisant une nouvelle chaîne de bits plus courte, indépendante des informations dont l'espion détient sur la clé.

D La sécurité des protocoles de Distribution Quantique de Clés

La distribution quantique de clés est souvent décrite comme *"inconditionnellement sécurisée"* pour souligner sa différence avec les protocoles cryptographiques classiques sécurisés par le calcul.

Cependant, le terme *"inconditionnel"* implique que la sécurité n'est conditionnée par aucune hypothèse ou repose uniquement sur l'hypothèse fondamentale qui exige que l'espion, Eve, possède une puissance de calcul infinie, et qu'il n'est limitée que par les lois de la mécanique quantique. Bien qu'il existe de nombreux arguments mathématiques formels [74–76] qui doivent être remplies pour que la distribution quantique de clé soit sécurisée. L'expression *"inconditionnellement sécurisée"* est justifiée non seulement par le fait que les conditions sont réduites, mais elles sont en quelque sorte des conditions nécessaires minimales vu que la sécurité ne peut pas venir de rien.

Intuitivement, la sécurité dans le contexte de distribution quantique de clés consiste à s'assurer que l'espion, Eve, ne dispose que d'une quantité négligeable de l'informations sur la clé partagées entre Alice et Bob après le protocole.

Toute preuve de sécurité pour les protocoles de distribution quantique de clés est déterminée par le taux de clé secrète étant donné qu'il est difficile de définir avec précision la quantité d'informations qu'Eve peut obtenir du canal de communication.

Soit n la taille de la clé tamisée après l'étape de réconciliation de clés, et $l(n) \leq n$ la taille de la clé securisée après l'étape de l'amplification de la confidentialité, alors le taux de clé secrète, noté r, dans le scénario asymptotique, où $n \to \infty$, est défini comme suit :

$$r := \lim_{n\to\infty} \frac{l(n)}{n} \tag{2.13}$$

Une technique plus récente de preuve de sécurité est due à Devetak et Winter [77]. Cette technique de preuve s'applique au cas où Eve est restreinte aux attaques collectives. La technique Devetak-Winter donne une expression explicite pour une borne inférieure sur le taux de clé r :

$$r \geq \inf[S(A|E) - H(A|B)], \tag{2.14}$$

où $S(A|E)$ est l'entropie conditionnelle de von Neumann, défini comme $S(A|E) = S(A,E) - S(E)$ tandis que $H(A|B)$ est l'entropie conditionnelle classique de Shannon. Cette expression indique que le taux de clé est juste la différence entre la quantité de l'incertitude qu'Eve a sur la clé d'Alice qui doit être élevée, et la quantité de l'incertitude que Bob a sur la clé d'Alice qui doit être faible, pour que Alice et Bob peuvent distiller une clé secrète sécurisée.

Différentes classes d'attaques

Afin de pouvoir estimer les taux de clés qu'il est possible de transmettre, il est nécessaire de modéliser les différents modèles de sécurité associés à différents types d'attaques qu'Ève peut implémenter.

Attaques individuelles :

Les attaques individuelles représentent la catégorie des attaques pour lesquelles l'espion, Ève, a accès à une mémoire quantique.

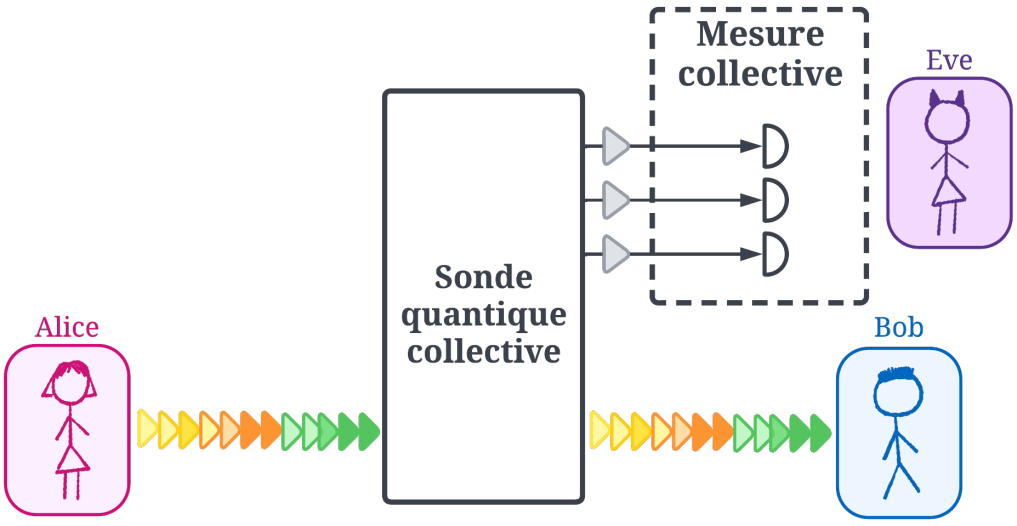


FIGURE 2.6 : Représentation de l'attaque individuelle.

Ce type d'attaque est modélisé de la façon suivante : Ève est autorisée à interagir de manière individuelle chaque état quantique, qubit, envoyé par Alice avec une sonde quantique et le stoker dans une mémoire quantique. Puis elle effectue une mesure sur

chacun de ces sondes individuellement après la révélation des bases que Bob a choisi de mesurer.

Attaques collectives :

L'attaque collective est considérer une généralisation d'attaque individuelle puisque Ève emploie la même stratégie d'attaque sur chacun des qubits envoyés par Alice, à la différence que cette fois-ci Ève est autorisée à attendre la fin des étapes classiques d'extraction de clé pour effectuer la mesure la plus adaptée.

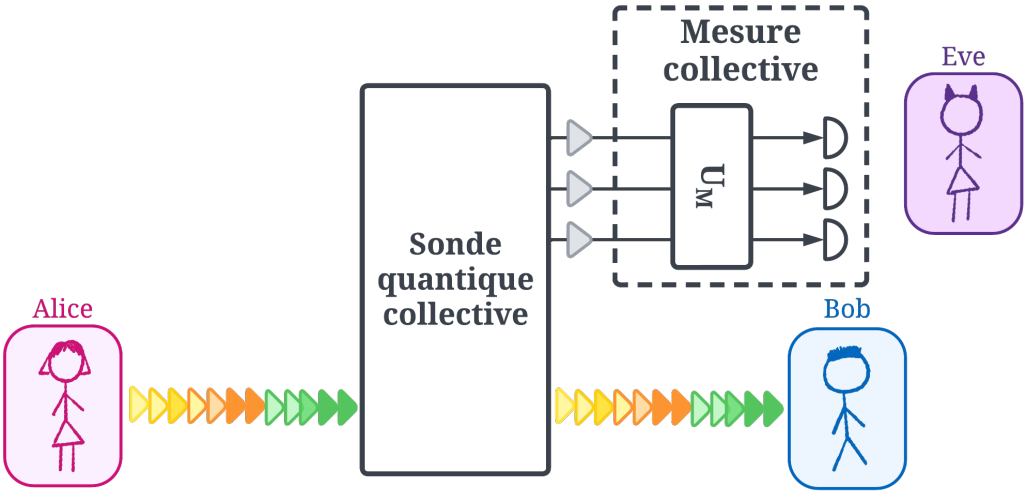


FIGURE 2.7 : Représentation de l'attaque collective.

Cette mesure collective est réalisée en appliquant une transformation unitaire qui a pour entrées l'ensemble des sondes suivie d'une mesure individuelle des sorties.

Attaques cohérentes :

Les attaques cohérentes sont les attaques les plus générales et les plus puissantes autorisées par la mécanique quantique modéliser de façon similaire aux attaques collectives. Dans cette attaque Ève peut prélever de l'information faisant tout d'abord intriquer toutes ses sondes avant de les faire interagir collectivement avec tous les états cohérents qui transitent dans le canal quantique .

Attaques incohérente :

La différence entre l'attaque cohérente et l'attaque incohérente réside dans le fait que dans cette dernière Ève est obligé de s'occupe de chaque état cohérent qui transite dans le canal quantique et de stocker chacun dans une mémoire quantique.

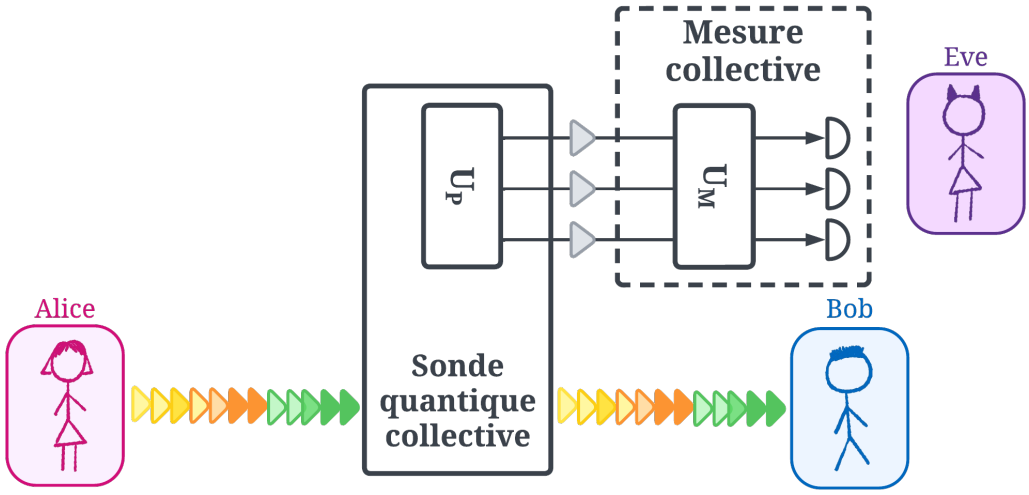


FIGURE 2.8 : Représentation de l'attaque cohérente.

V Protocole à quatres états : BB84

Le protocole BB84 [66] a marqué le début de la cryptographie quantique, il s'agit d'une méthode standard pour nommer ce protocole, élaboré en 1984 par Charles Bennett et Gilles Brassard. Il introduit une ambiguïté, dans le codage, qui va rendre l'espionnage du signal quantique impossible.

A Principe de fonctionnement

L'idée fondatrice est de permettre à deux interlocuteurs, Alice et Bob, de construire une clé secrète commune qui repose sur le codage en polarisation d'une séquence de qubits uniques, effectué sur quatre états de polarisation constituent deux bases conjuguées appelées base rectiligne $\{|0\rangle, |1\rangle\}$ et base diagonale $\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$.

Généralement ces deux bases s'écrivent comme $H^b|x\rangle$ où H est la transformation de Hadamard [1], $x \in \{0,1\}$ et $b \in \{0,1\}$.

Le partage d'une clé secrète suivant le protocole BB84 contient :

Transmission quantique

- Alice commence par préparer l'état $H^{b_1}|x_1\rangle \otimes ... \otimes H^{b_n}|x_n\rangle$, alors elle choisit une séquence de n bits aléatoires représentés par la variable aléatoire $X = (X_1, ..., X_n)$,

1. La transformation de Hadamard est définie par :

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

codés aléatoirement dans l'une des deux bases de polarisation et l'envoi à Bob par l'intermédiaire du canal quantique.

- Bob de son côté désire identifier l'état mais comme il ne connaît pas la base de préparation, il effectue la mesure dans une base choisie aléatoirement, il obtient ainsi une séquence de bits représentés par la variable aléatoire $Y = (Y_1, ..., Y_n)$ appelée *clé brute*, qui diffère de celle envoyée par Alice pour plusieurs raison :
  - Sa base de mesure n'est pas toujours celle choisie par Alice.
  - Erreur de transmission.

Réconciliation des clés

- Alice et Bob dévoilent publiquement, une partie de leurs séquences, via un canal classique leurs choix de base et non pas les résultats de leurs mesures.

- Ils choisissent alors de conserver que les bits pour lesquels leur choix de base coïncide.

- En moyenne ces chaines sont deux fois plus courtes que les chaines de départ.

Correction d'erreur

Alice et Bob estiment le taux d'erreur dans leur clé en dévoilent publiquement une petite partie de leurs séquences de mesure. Si ce taux d'erreur est trop élevés, cela signifie qu'ils ont été espionnés, ils rejettent les données échangées et recommencent à nouveau. Sinon ils disposent d'une chaine de bits identiques sur lesquelles Ève peut encore posséder une certaine quantité d'information. Pour remédier à ce problème, Alice et Bob tentent de corriger les incohérences présentes dans leur clé en procédant par un simple calcul de parités et des échanges interactifs :

- Alice et Bob divisent les bits restants de leur clé en blocs de longueur L. Cette longueur est choisie afin qu'il soit improbable qu'il y ait plus d'une erreur par blocs ($RL << 1$, avec R le taux d'erreur estimé précédemment).

- Alice et Bob calculent les parités de chacun de leurs blocs, les comparent publiquement et suppriment à chaque fois le dernier bit des blocs.
  - Si la parité obtenue chez Alice et Bob est différente, alors ils localisent et suppriment le bit erroné du bloc en procédant par bissection.

- À la fin, avec une probabilité élevée, Alice et Bob partagent la même chaîne de bits.

Amplification de confidentialité

Alice et Bob appliquant un protocole d'amplification de confidentialité qui permet de réduire le niveau d'information acquis par Ève à un niveau arbitrairement

faible ainsi que la réduction de la taille de la clé.

- Alice et Bob estiment à partir du taux d'erreur R précédemment obtenu le nombre maximal de bits k connus par Eve. Soit s un paramètre de sécurité.

- Alice et Bob choisissent au hasard $(n - k - s)$ sous-ensembles de leur clé, où n représente le nombre de bits de la clé.

- Les parités de ces sous-ensembles deviennent la clé secrète finale. Cette clé est plus sécurisée que la précédente, car Eve doit savoir quelque chose sur chaque bit d'un sous-ensemble afin d'obtenir des informations sur sa parité.

Remarques 1.

- *Les deux interlocuteurs ne peuvent pas décider les résultats de la clé secrète puisqu'ils choisissent au hasard entre les bases.*
- *Les bits choisis pour la comparaison ont été sacrifiés puisqu'ils ont été communiqués et donc ont pu être interceptés.*
- *A la fin de toutes ces opérations Alice et Bob partagent une clé totalement secrète donc le processus réel de cryptage sécurisé d'un message peut commencer.*

B La sécurité du protocole

La sécurité du protocole BB84 a été prouvée en tenant compte de nombreux types d'attaques différents. Cependant, l'attaque la plus simple qu'Eve puisse effectuer est connue sous le nom d'attaque interception-réémission. Cette attaque consiste à :

1. Intercepter chaque qubit du canal quantique
2. Mesurer son état au hasard sur l'une des deux bases
3. Préparer un qubit dans l'état correspondant au résultat de mesure
4. Envoyer ce qubit à Bob

Lors des interceptions, Eve a une probabilité de 50% pour mesurer correctement le qubit envoyé par Alice. Dans ce cas, son intervention n'est pas remarquée par les utilisateurs légitimes. Cependant, dans les cas restants la base choisie pour la mesure ne correspond pas à celle utilisée pour préparer le qubit, vu qu'Eve n'a aucune information sur le choix d'Alice. Statistiquement dans au moins 50% des cas, l'interception d'Eve se traduirait par des erreurs dans la mesures de Bob.

Ainsi, l'attaque d'interception-réémission fournit à Eve la moitié d'information, transmise par Alice, des bits de la clé secrète au prix d'une augmentation d'un taux d'erreur d'environ 25% entre Alice et Bob. Cette augmentation des erreurs peut être utilisée pour détecter la présence d'un espion.

Pour évaluer le taux d'erreur, Alice et Bob peuvent simplement sacrifier une petite fraction de leur clé sur le canal publique pour être en mesure de s'assurer de la confidentialité de la clé. Dans le cas où la valeur du taux d'erreur dépasse le seuil requis, Alice et Bob rejetteront la clé en raison de la forte probabilité de présence d'un espion sur le canal quantique et ils recommencent le protocole du début.

Après tout, la sécurité du protocole BB84 a été discutée en profondeur et en tenant compte de nombreux types d'attaques différents. Un résultat principal de ces preuves montre que si le taux d'erreur est inférieur à une valeur maximale de 11%, la clé obtenue peut être considérée comme absolument inconditionnellement sécurisée contre toute attaque éventuelle [78].

VI Protocole à deux états : B92

Charles Bennett a remarqué qu'en réalité, la sécurité du protocole BB84 repose sur l'utilisation d'états non orthogonaux.

En 1992, il a proposé un protocole simple similaire au protocole de polarisations BB84 connu sous le nom de B92 ou protocole de deux états [70], sauf que ce dernier utilise deux états non orthogonaux plutôt que quatre états.

A Etapes principales du protocole

Le partage d'une clé sécurisée suivant le protocole $B92$ s'effectue en deux étapes principales qui peuvent être distinguées comme suit :

Transmission quantique

- Alice prépare une chaîne binaire aléatoire $A_i \in \{0, 1\}$. Elle envoie à Bob via un canal quantique l'état :

$$|0\rangle \qquad si \quad A_i = 0 \tag{2.15}$$

$$H|0\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad si \quad A_i = 1 \tag{2.16}$$

- Bob génère à son tour, une suite binaire aléatoire $B_i \in \{0, 1\}$ par une mesure de chaque état quantique reçu sur une des deux bases $\{|0\rangle, |1\rangle\}$ ou $\{|+\rangle, |-\rangle\}$, appelées respectivement base rectiligne + et base diagonale $\times$, choisies aléatoirement.

Réconciliation des clés

Sur un canal classique, Bob identifie les mesures incertaines à Alice, pour qu'elle les omette.

Il existe plusieurs scénarios possibles pouvant survenir :

Si Bob utilise la base + et observe
- $|1\rangle \Rightarrow$ Bob sait qu'Alice doit avoir envoyé $|+\rangle \Rightarrow$ Bit 1
- $|0\rangle \Rightarrow$ Bob est en doute $\Rightarrow$ Bob néglige ce bit

$$\text{Si Bob utilise la base } \times \text{ et observe} \begin{cases} |-\rangle \Rightarrow \text{Bob sait qu'Alice doit avoir envoyé } |0\rangle \Rightarrow \text{Bit 0} \\ |+\rangle \Rightarrow \text{Bob est en doute} \Rightarrow \text{Bob néglige ce bit} \end{cases}$$

À ce stade, Alice et Bob partagent une clé secrète. Mais pour ne pas avoir doute d'un espion, Ils peuvent, comme le cas du protocole BB84, sacrifier d'une partie de leurs chaines de bits et les comparer publiquement. S'ils s'entendent pour un nombre significatif, ils savent qu'il a eu espionnage et que la chaine de bits doit être rejetée, sinon deux phases additionnelles de correction d'erreurs et d'amplification de la confidentialité sont possibles pour établir une clé sécurisée partagée entre eux.

B Sécurité du protocole

L'efficacité du protocole B92 est de 25%. Ceci signifie que 75% des qubits seront abandonnées, et que seulement 25% sont employés générer la clé secrète. En effet, Bob a une probabilité de 50% pour mesurer dans la base correspond au qubit envoyé par Alice et une probabilité 50% d'obtenir un résultat concluant.

De ce fait, pour générer une clé securisée de taille n, Alice doit envoyer en moyenne 4 fois plus la taille n.

Le protocole B92 est un protocole typique pour lequel un cas particulier d'une attaque d'interception-réémission connu par l'attaque de discrimination d'état sans ambiguïté se pose. Ce type d'attaque s'applique chaque fois que les états quantique envoyés par Alice sont indépendants.

Dans ce cas, Ève peut effectuer une mesure de discrimination d'état sans ambiguïté sur les états quantique de sorte que, dans les cas où elle connait avec certitude l'état, elle l'envoie à Bob tandis que dans les autres cas, elle n'envoie aucun qubit. Avec cette stratégie, elle est capable d'imiter un canal à perte.

Sous un seuil de $\eta \simeq 0.293$ qui dépend de la non orthogonalité de l'état, aucune transmission de clé sécurisée n'est possible. Ce seuil est défini comme la transmissivité où la probabilité de succès d'une mesure USD est égale à la probabilité de détection de Bob sur le canal à perte [79].

VII Extraction de la clé secrète : protocole à qubit unique

En se basant sur l'environnement de développement, du langage de programmation Python, Jupyter sous la plateforme Windows nous avons réalisé un programme d'extraction de la clé secrète suivant le principe des protocoles présentés précédemment.

Nous avons ainsi développé à l'aide de la bibliothéque Tkinter, un ensemble d'interfaces graphiques permettant de faciliter l'utilisation et le lancement de l'implémentation des protocoles d'extraction de la clé secrète ainsi que la visualisation des résultats.

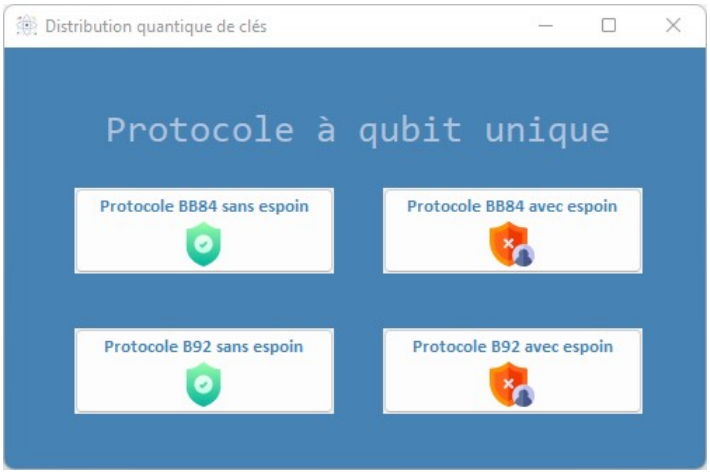
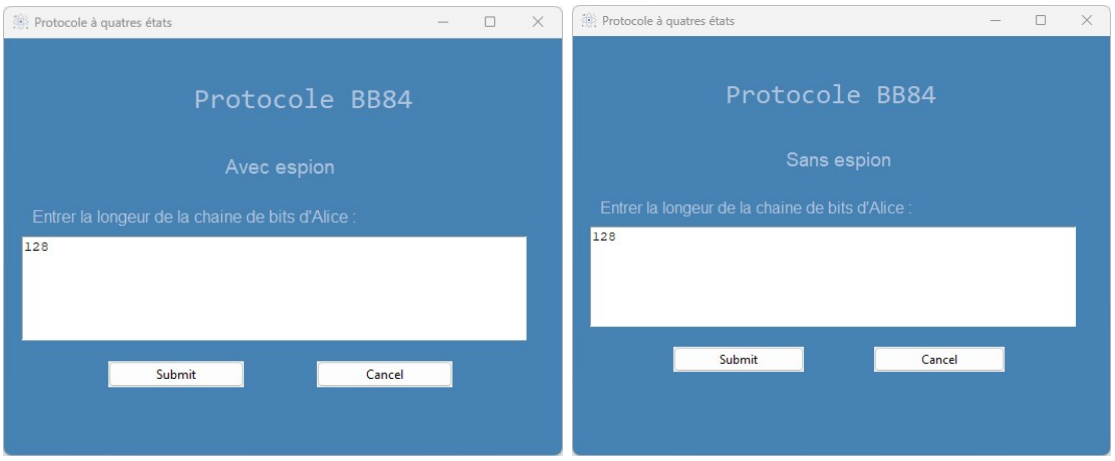


FIGURE 2.9 : L'interface d'accueil.

Au lancement du programme, une interface principale s'affiche présentant un menu de démarrage représenté à la figure 2.9. Ce menu offre à l'utilisateur les different choix des protocoles qui peuvent être exécutés.

A Extraction de la clé secrète : Protocole BB84

Le menu de démarrage propose à l'utilisateur une exécution du protocole BB84 avec la présence ou non d'une écoute clandestine. Une fois le choix est effectué, l'utilisateur est invité a saisir la longeur de la chaîne de bits d'Alice dans la fenêtre illustré par la figure 2.10.



(a) Présence d'espion (b) Absence d'espion

FIGURE 2.10 : Interface de saisie du protocole BB84.

Ce protocole utilise quatre états de polarisation à partir de deux bases conjugées :

— **La base rectiligne** : constituée des états de polarisation verticale 'V' et horizontale 'H'. Cette base est notée par le symbole $'+'$.

— **La base diagonale** : constituée des états de polarisation diagonale 'D' et anti-diagonale 'A'. Cette base est notée par le symbole $'\times'$.

Les états de polarisation utilisées dans le protocole sont encodées selon la convention en bit classique. Le bit 0 est associé aux états de polarisation horizontale et anti-diagonale, et les deux états de polarisation, verticale et diagonale, sont représentées par le bit 1.

Le programme d'extraction effectue les différentes étapes requises par le protocole BB84 à savoir transmission quantique, réconciliation des clés, l'estimation du taux d'erreur pour vérifier la présence d'un espion, correction d'erreur et amplification de confidentialité.

Pour rendre les choses plus précises, en cas de présence d'un espion, nous avons supposer qu'Eve intercept chaque photon destiné à Bob et mesure sa polarisation selon l'une des deux bases, recteligne + ou diagonale $\times$, avant de le transmettre à Bob.

Les résultats des figures ci-dessous représentent l'exécution du programme pour une longeur de 128 bits envoyé par Alice générer aléatoirement pour chaque exécution en cas de présence d'un espion, la figure 2.11 et en cas d'absence d'un espion, la figure 2.12.

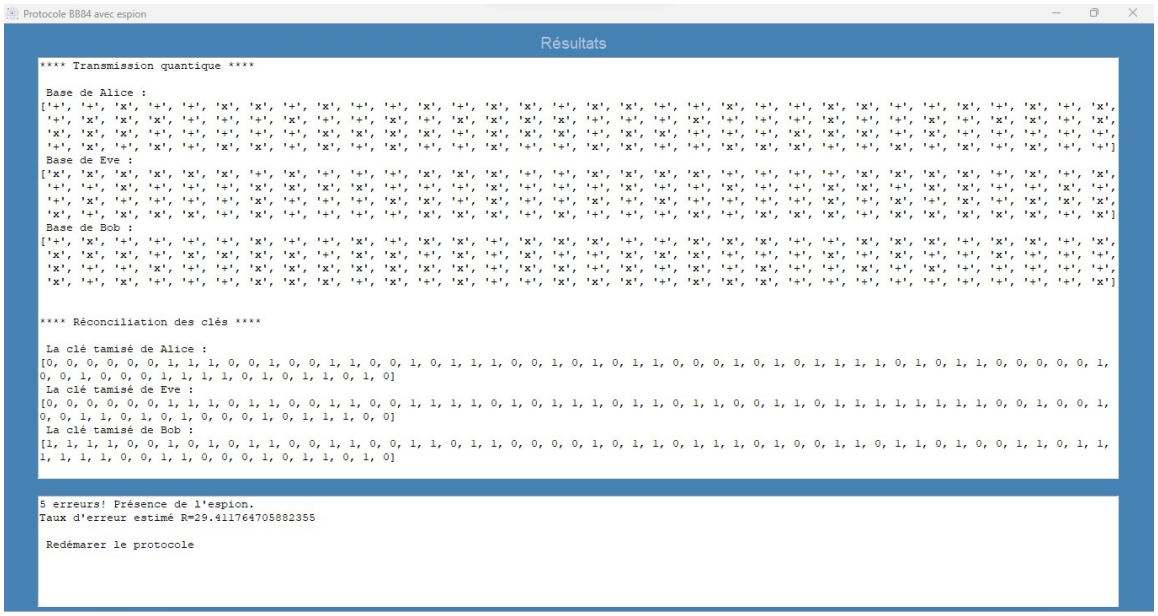


FIGURE 2.11 : L'exécution du protocole BB84 en cas de présence d'Ève.

L'espion peut avoir une chance d'être indétectable si l'estimation du taux d'erreur est tolérable. Néanmoins, un protocole classique de correction d'erreur est utilisé pour identifier et éliminer les différences dans les chaîne de clés. En outre un dernier processus appele amplification de confidentialité pour minimiser la quantité d'informations divulguées à l'espion. La figure suivante 2.13 montre le résultat de l'exécution du programme pour une longeur de 128 bits.

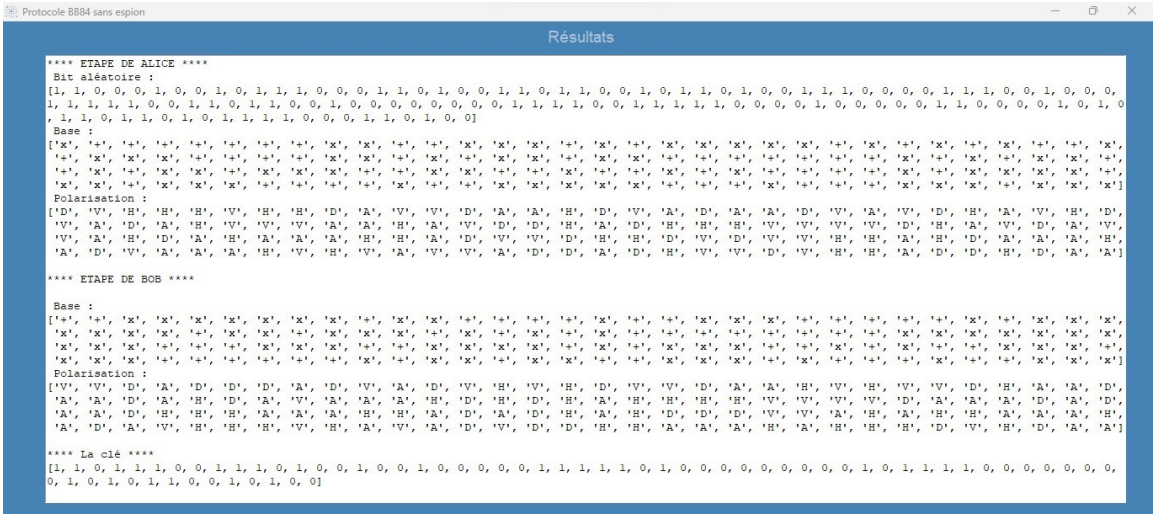


FIGURE 2.12 : L'exécution du protocole BB84 en cas d'absence d'Ève.

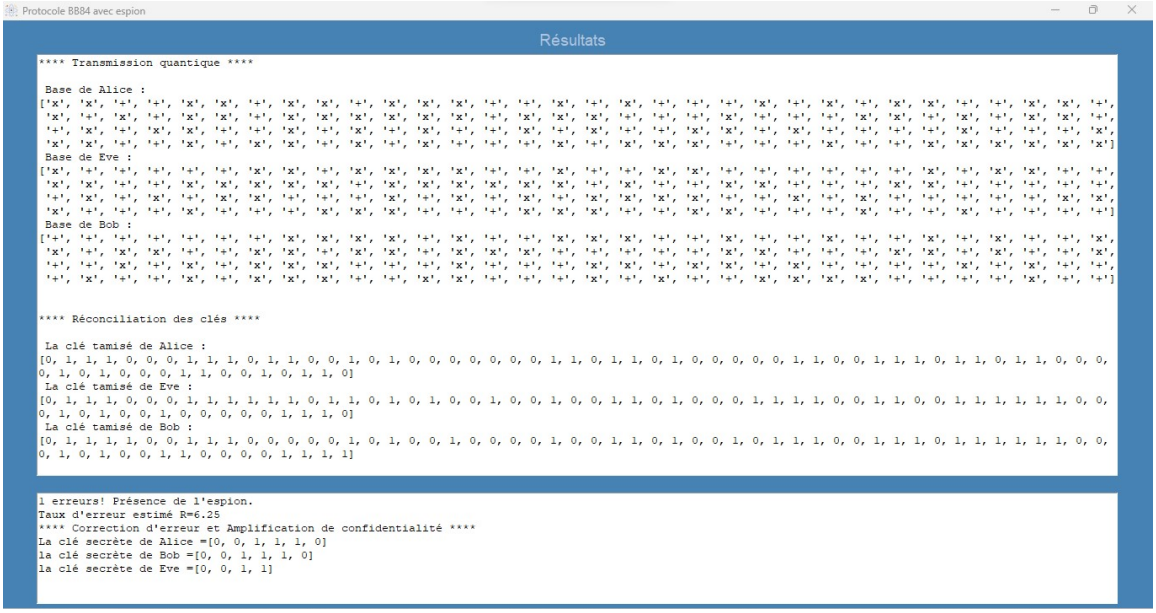
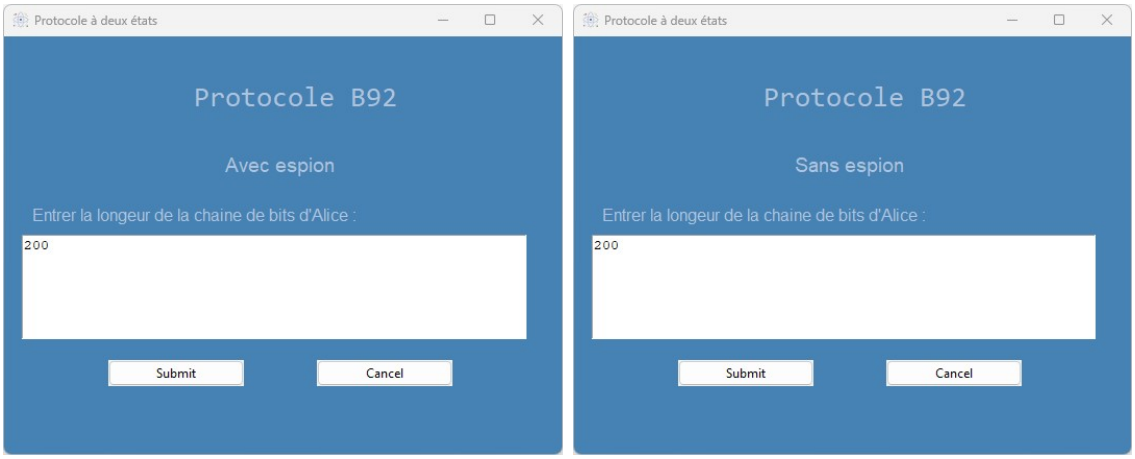


FIGURE 2.13 : L'exécution du protocole BB84 avec la présence d'Ève.

B Extraction de la clé secrète : Protocole B92

Le menu de démarrage propose également à l'utilisateur une execution du protocole B92 avec la présence ou non d'une écoute clandestine. Une fois le choix est effectué, l'utilisateur est invité de nouveau a saisir la longeur de la chaîne de bits d'Alice dans la fenêtre illustré par la figure 2.14.



(a) Présence d'espion (b) Absence d'espion

FIGURE 2.14 : Interface de saisie du protocole B92.

Le protocole B92 nécessite deux états non orthogonaux dont les états 'H', 'D' et 'A', 'V' représentant respectivement les bits classique 0 et 1. Le programme d'extraction est identique à celui du protocole BB84, il effectue plusieurs étapes afin établir une clé sécurisée.

Le résultats de la figure ci-dessous représentent l'exécution du programme pour une longeur de 200 bits envoyé par Alice générer aléatoirement pour chaque exécution en cas d'absence d'espion, la figure 2.15 et en cas de présence d'espion, la figure 2.16.

La présence d'Eve est intégrée dans le programme d'extraction en implémentant la stratégie d'interception-réémission. De ce fait, nous avons supposer qu'Eve intercepte tous les photons qu'Alice envoie à Bob et qu'elle est capable d'effectuer les mesures dans la même base rectiligne ou diagonale que celles utilisées par Bob et par conséquent avoir accès aux résultats des mesures de ce dernier.

Comme dans le cas du protocole BB84, il est possible d'estimer l'information d'un espion à partir du taux d'erreur. Sous certaines conditions, il est possible d'obtenir une clé sécurisée, si le taux d'erreur est inférieur à une valeur limite, aprés les processus d'une communication classique : correction d'erreurs et l'amplification de confidentialité. Les figures 2.17 et 2.18 montrent le résultat de l'exécution d'une clé totalement sécurisée selon le programme pour une longeur de 200 bits.

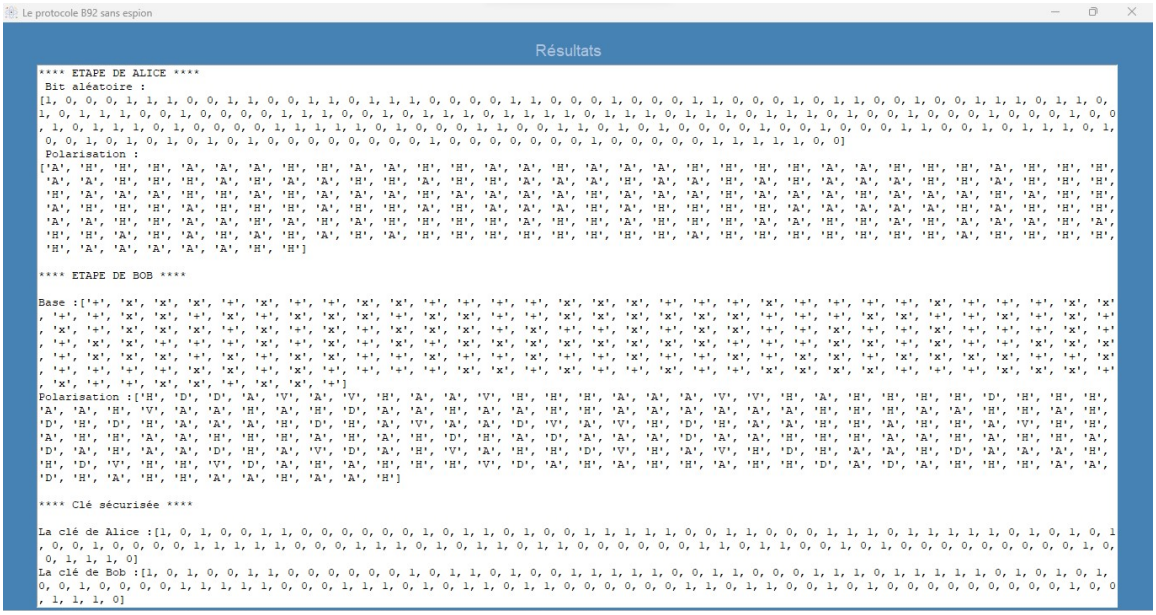


FIGURE 2.15 : L'exécution du protocole B92 en cas d'absence d'Ève.

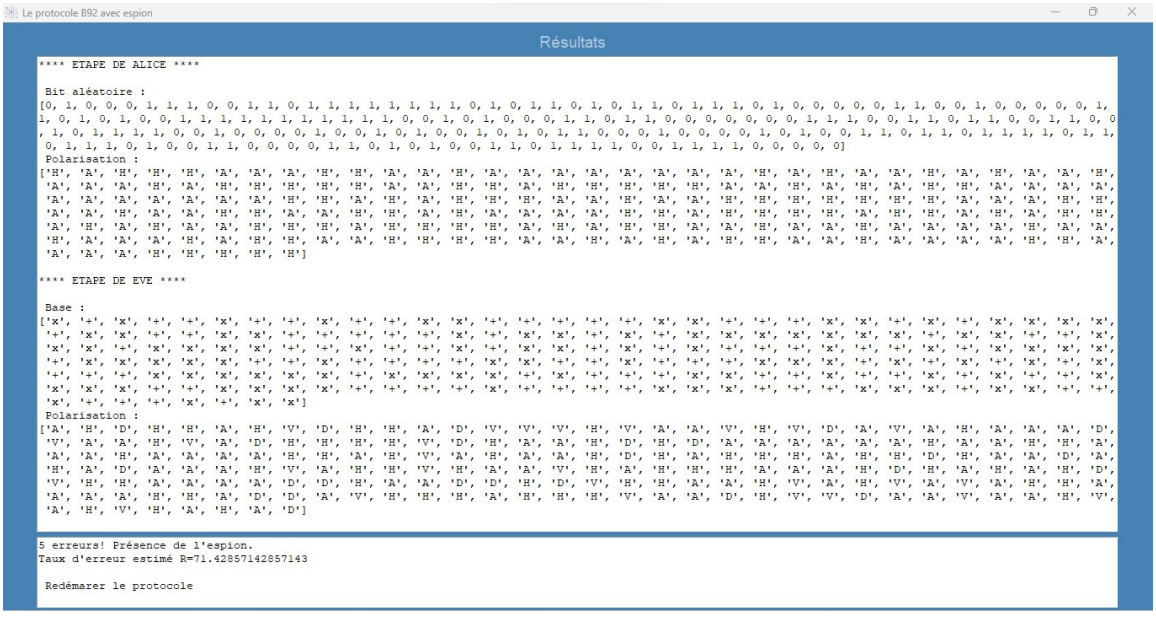


FIGURE 2.16 : L'exécution du Protocole B92 en cas de présence d'Ève.

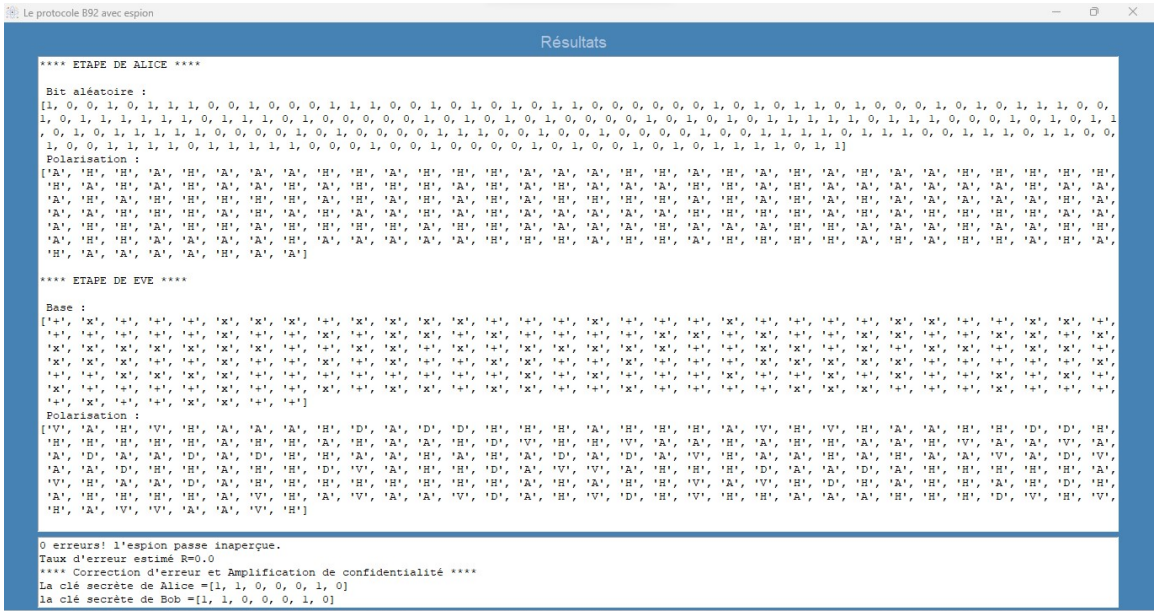


FIGURE 2.17 : L'exécution du protocole B92 avec la présence d'Ève.

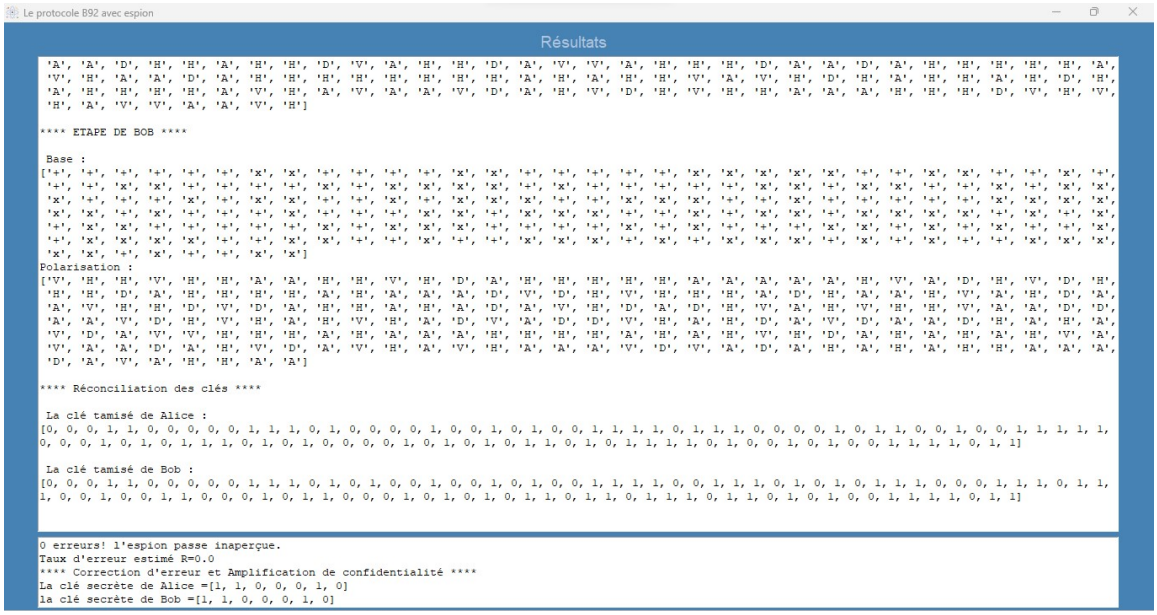


FIGURE 2.18 : L'exécution du protocole B92 avec la présence d'Ève.

VIII Protocole Ekert 91

En 1991, Artur Ekert a proposé une approche différente pour la distribution quantique de clé basée sur des états intriquées comme une ressource pour générer à distance des mesures corrélées chez Alice et chez Bob.

Ekert a envisagé l'utilité de l'expérience EPR et l'inégalité de Bell de façon à assure la sécurité des communications [67].

Dans le schéma proposé par Ekert, le partage d'une clé secrète entre Alice et Bob résulte des corrélations quantiques portées par une source de paires de qubits intriqués dont l'un est mesuré par Alice et l'autres par Bob. Le principe est schématisé sur la figure 2.19.

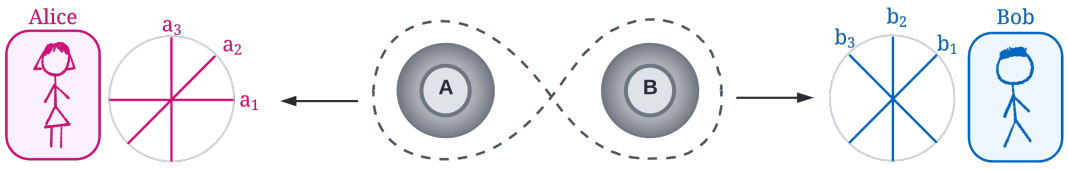


FIGURE 2.19 : Le principe du protocole E91.

A Principe de fonctionnement

Le protocole Ekert 91, abrégé en E91, souvent aussi connu par le protocole Einstein-Podolsky-Rosen en raison de sa connexion directe au paradoxe EPR, fonctionne comme suit :

Transmission quantique

- Une source émet des paires de qubits dans un état intriqué à Alice et Bob

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{2.17}$$

- Alice choisit au hasard l'une des trois bases définies par trois orientations $\{a_1 = 0, a_2 = \frac{1}{4}\pi, a_3 = \frac{1}{2}\pi\}$ pour mesurer la polarisation du qubit reçu.
- De même Bob choisit de manière aléatoire l'une des trois bases entre $\{b_1 = \frac{1}{4}\pi, b_2 = \frac{1}{2}\pi, b_3 = \frac{3}{4}\pi\}$ pour mesurer le qubit reçu.

Réconciliation des clés

- Alice et Bob révèlent ensuite publiquement sur un canal classique authentifié la séquence des bases utilisées pour chacune de leurs mesure. Ils séparent les mesures en deux groupes distincts :

— Premier groupe : Constitué de résultats obtenus lorsque des mesures différentes ont été effectuées. Ce premier groupe est utilisé pour vérifier la violation des inégalités de Bell.
— Deuxième groupe : Constitué de résultats obtenus lorsque des mesures identiques ont été effectuées. Ce deuxième groupe est utilisé pour établir une clé sécurisée.

Enfin, Alice et Bob annoncent publiquement leurs résultats du premier groupe pour s'assurer de la présence ou non d'une écoute clandestine. En cas de violation, Alice et Bob peuvent utiliser les mesures du deuxième groupe pour obtenir une chaîne secrète de bits, appelée clé.

B Sécurité du protocole

Après qu'un nombre suffisant de paires de photons ont été distribués, Alice et Bob révèlent sur un canal public authentifié les bases de mesure qu'ils utilisent pour chaque mesure.

Ils utilisent leurs résultats du premier groupe, mesures avec orientation différente, pour établir la valeur de S. La valeur de corrélation S doit satisfaire à l'exigence :

$$S = -2\sqrt{2} \tag{2.18}$$

Cette exigence est connu sous le nom de CHSH de l'inégalité de Bell, du nom de John Clauser, Michael Horne, Abner Shimony et Richard Holt, qui ont mis la déclaration originale de Bell dans cette forme plus intuitive, et représente la valeur de corrélation maximale entre deux qubits [80]. Par conséquent, une corrélation approximativement égale à cette valeur est considérée comme la preuve que personne n'a interféré avec la communication.

Cela garantit que les résultats du deuxième groupe, mesures avec la même orientation, sont anticorrélés et peuvent être utilisés pour établir une clé sécurisée [81].

Toutefois, Lorsque une écoute clandestine se produit, l'inégalité CHSH n'est pas violée et la valeur de corrélation sera dans l'interval :

$$-\sqrt{2} \leq S \leq \sqrt{2} \tag{2.19}$$

Ainsi, Alice et Bob se rendre compte que quelqu'un a interféré avec la communication, car le résultat 2.19 sera toujours inférieur au $|S| = 2\sqrt{2}$ demandé.

Le protocole Ekert 91 permet d'assurer une meilleure sécurité sans augmenter significativement la complexité du protocole [82]. Son avantage réside dans le fait qu'aucune information sur la clé n'est révélée pour savoir si une écoute indiscrète était présente au prix d'une réduction du taux de génération de clés. Toutefois, il y a au total 9 combinaisons possibles pour le choix des bases dont seulement 2 d'entre elles contribuent au tamisage. Ainsi la longueur de la clé tamisée, avant toute correction ou amplification de confidentialité est d'environ $\frac{2}{9}N$.

IX le protocole BBM92

Le protocole BBM92 décrit par Bennett, Brassard et Mermin en 1992 propose une variante simplifiée du protocole Ekert où un test d'inégalité CHSH n'est pas nécessaire pour la sécurité du protocole [73]. Le protocole BBM92 utilisant des paires de photons intriqués en polarisation est une variante très élégante du protocole BB84.

A Principe de fonctionnement

Le principe de fonctionnement de ce protocole effectue selon les étapes suivantes :

Transmission quantique

- Alice et Bob reçoivent leur qubit intriqué $|\psi^-\rangle$ d'une source placée sur la ligne de communication entre eux.
- De manière aléatoire, Alice et Bob choisissent chacun une des deux bases, à savoir la base rectiligne + et la base diagonale $\times$, afin d'effectuer une mesure sur le qubit qu'ils reçoivent.

Réconciliation des clés

- Alice et Bob comparent publiquement sur un canal classique authentique leurs choix de bases utilisées pour effectuer leurs mesures. Ils conservent les qubit pour lesquels leur choix de base coïncide et rejettent le qubit de base opposée.
- Étant donné que l'état $|\psi^-\rangle$ produit des résultats anticorrélés, Bob inverse sa chaîne de bits de façon à ce qu'il obtient une clé identique, aléatoire et partagée avec Alice.

Correction des erreurs

- Alice et Bob partagent quelques bits pour une estimation du taux d'erreur. Pour un taux d'erreur supérieur à un certain seuil, ils supposent que les erreurs proviennent d'une écoute clandestine et démarrent un nouvel échange. Sinon, ils procèdent à la correction des erreurs.

Amplification de confidentialité

- Alice et Bob exécutent un protocole d'amplification de confidentialité classique sur leur clé corrigée des erreurs pour réduire le maximum d'informations potentielles qu'Eve aurait pu obtenir sur la clé à une valeur arbitrairement petite.

Alice et Bob possèdent maintenant une clé secrète sécurisée et aléatoire qu'ils peuvent utiliser avec le Vernam One-Time Pad pour communiquer en toute sécurité entre eux.

B La sécurité du protocole

Dans leur article, Bennett et al. ont prouvé qu'un tiers malveillant, Eve, ne peut pas modifier la source EPR afin d'obtenir des informations. Le mieux qu'Eve puisse faire est une simple approche d'une écoute clandestine où elle intercepte et mesure les qubits, destinés à Bob, dans l'une des deux bases de polarisation, ensuite elle renvoie un autre qubit polarisé selon le résultat de sa mesure à Bob.

Ainsi, tout ce qu'Alice et Bob doivent faire pour vérifier la sécurité de leur communication, est de comparer un sous-ensemble aléatoire des bits de leur clé tamisée sur le canal classique pour estimer le taux d'erreur tolérable d'environ 14.6% [83] pour la distribution de clés sécurisée contre une attaque individuelles.

Toutefois, Eve a une chance de 50% de mesurer dans l'une des deux bases, Si elle mesure sur la même base que Bob, elle n'introduit aucune erreur. Alors Alice et Bob obtiennent les résultats de mesure anti-corrélés qu'ils attendent. Par contre Eve a une probabilité $\frac{1}{2}$ de mesurer dans la base complémentaire et d'introduit une erreur avec une probabilité de $\frac{1}{2}$ dans la clé de Bob, en raison de sa mesure complémentaire ultérieure et du principe d'incertitude de Heisenberg. En conséquence, le taux d'erreur total induit par Eve est de 25% cela signifie qu'une écoute clandestine est détectée.

X Extraction de la clé secrète : protocole à qubit intriqué

Afin d'implémenter les différents protocoles à qubit intriqué de distribution de clés quantique, nous avons utilisé la programmation de circuits quantique basé sur Qiskit suivant le principe des protocoles présentés précédement.

Qiskit ou Quantum Information Software Kit est un framework open source pour traiter de l'informatique quantique avec des ordinateurs quantiques au niveau des impulsions, des circuits et des algorithmes [84].

Le framework est supporté par IBM et développé à l'aide du langage de programmation Python, qui permet de programmer de vrais ordinateurs quantiques exploitant le programme IBM Quantum Experience. L'objectif principal de Qiskit est de créer un logiciel qui facilite l'utilisation des processeurs quantiques par des utilisateurs. De plus, Qiskit propose un outil pour concevoir des expériences et les exécuter à la fois sur des simulateurs et sur de vrais processeurs quantiques.

Pour construire un circuit, un registre quantique et un registre classique doivent être définis. Le premier registre est nécessaire pour effectuer des calculs, tandis que le second registre pour stocker des informations sur les résultats de mesure.

La première étape des protocoles à qubit intriqué correspond à la génération de l'un des états de Bell. Dans notre scénatio, le choix était de laisser un tiers, Charlie le propriétaire du dispositif de préparation d'état singulet, produire des états intriqués.

En utilisant des portes quantiques, Charlie crée un état correspondant à un état singulet [16], défini par :

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.20}$$

Pour la simulation de ce circuit, nous avons besoin d'un registre quantique a une

dimension de 2 pour créer une paire de qubits intriqués et d'un registre classique a la dimension 2 pour stocker les résultats de mesure des participants, un bit classique pour Alice et Bob.

Une fois générée, chaque paire est instantanément divisée et envoyée à Alice et Bob. Convenons que le premier qubit de la paire sera envoyé à Alice et le second à Bob.

En conséquence, le circuit quantique suivant est généré, voir la figure 2.20 :

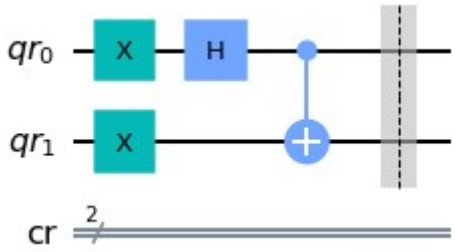


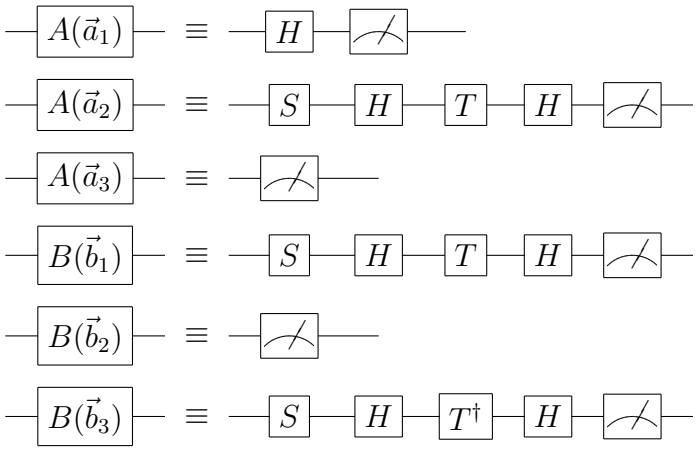
FIGURE 2.20 : Le circuit de la source.

A Extraction de la clé secrète : Protocole E91

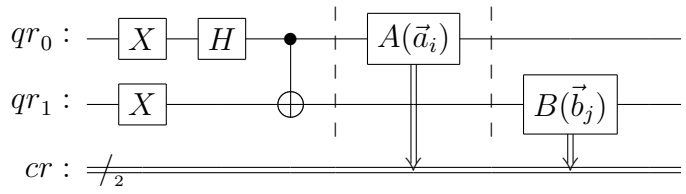
Un programme simulant l'exécution du protocole E91 sur un simulateur d'information quantique intégré de Qiskit en reproduisant les mêmes étapes prévues par le protocole en cas de présence d'un espion et en cas d'absence d'un espion.

Au début de la simulation, Alice et Bob reçoivent chacun un qubit état singulet créés par Charlie, la figure 2.20. Les qubits qr_0 et qr_1 appartiennent respectivement à Alice et Bob.

Les participants choisissent indépendamment l'une des directions sur lesquelles ils mesurent les projections de spin de leurs qubits. Pour effectuer ces mesures, nous définissons $A(\vec{a_i})$ et $B(\vec{b_j})$ comme les observables de projection de spin utilisées par Alice et Bob définies comme suit :



Ainsi, le circuit quantique qui modélise la création de l'état singulet, la mesure de la projection de spin sur les directions $\vec{a}_i, \vec{b}_j$ dans le cas d'absence d'un espion est le suivant :



A ce stade, Alice et Bob comparent les projections de spin choisie lors de la mesure afin d'éliminer les qubits mesurés dans des direction différentes alors que les résultats obtenus lors de la mesure dans les mêmes directions sont conservés en tant qu'éléments de clés.

La figure 2.21 symbolise l'exemple du circuit quantique modélisant la mesure d'Alice de l'observable $A(\vec{a}_1)$ sur son qubit et la mesure de Bob de l'observable $B(\vec{b}_2)$ sur le sien.

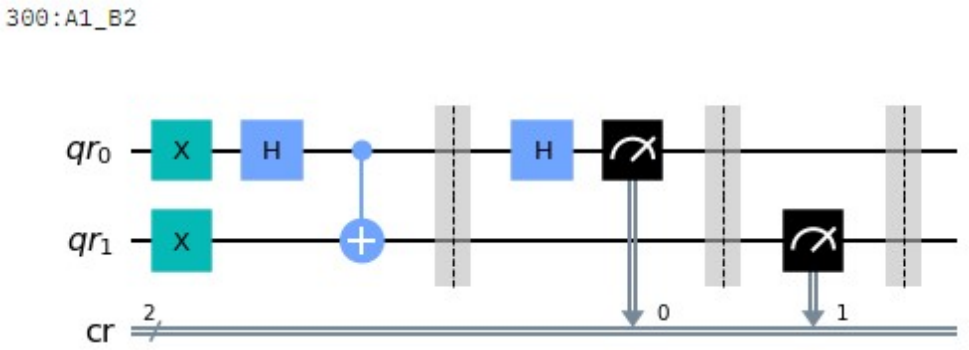


FIGURE 2.21 : Le circuit quantique du protocole E91 en absence d'un espion

Etant donné que seules deux des neuf combinaisons possibles de mesures s'avèrent utiles, projection sur de spin sur les directions $\vec{a}_2, \vec{b}_1$ et sur les directions $\vec{a}_3, \vec{b}_2$, il faut s'attendre à ce que le rapport entre la longeur de la clé tamisée et le nombre de paires intriqués utilisées soit proche de 2/9.

Comme mentionné précédemment dans le protocole E91, la valeur de corrélation CHSH est un indicateur de l'intrication des états intriqués. Ainsi, en utilisant les mesures de la projection de spin prises dans différentes directions, Alice et Bob peuvent déduire le taux d'interférence dans la communication.

L'exécution du programme de distribution d'une clé secrète du protocole E91 à partir de $N = 500$ paires états intriqués ont été réalisées sur le simulateur.

Les résultats de l'exécution sont présentés dans la figure 2.22. En raison de l'utilisation d'un simulateur qui ne tient pas compte du bruit, de la non-idéalité de l'équipement et également en raison de l'absence d'espion dans le canal, la valeur de corrélation calculée de CHSH est proche de $-2\sqrt{2} \simeq -2,828$. Il convient également de noter que le rapport entre la longueur moyenne de la clé et le nombre d'états intriqués utilisés est proche de 2/9, ce qui était tout à fait prévisible

Jusqu'à présent, nous avons modélisé le protocole E91 sans l'intervention d'un espion sur le canal de communication. Supposons maintenant qu'un attaquant, Eve, tente d'extraire certaines informations en interceptant les états intriqués, en les mesurant et en les transmettant aux participants de la communication.

```
Valeur de correlation CHSH: -2.899

Longeur de la clé secrete: 110
Nombre de bits incompatibles: 0

Clé de Alice: [0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0,
0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0,
0, 0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1,
1, 0, 0, 1, 0, 1, 0]

Clé de Bob: [0, 1, 1, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0,
0, 0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0,
0, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 1, 1, 1,
0, 0, 1, 0, 1, 0]
```

FIGURE 2.22 : L'exécution du protocole E91 en cas d'absence d'espion.

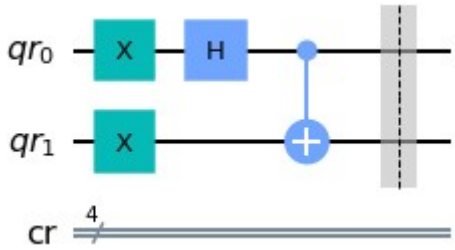
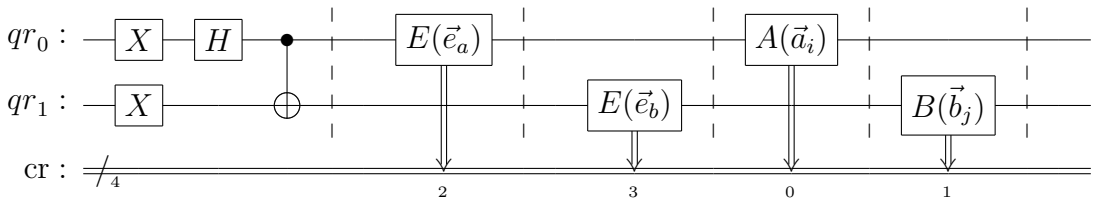


FIGURE 2.23 : Le circuit source avec intervention d'un espion.

En vue de simuler le modéle d'intervention, le registre classique s'étend à quatre bits. Un bit classique pour Alice, un bit classique Bob et deux autres bits classiques sont utilisés par Eve pour enregistrer les résultats de la mesure sur qubits d'Alice et de Bob.

Le circuit quantique qui décrit la distribution quantique de clé selon le protocole E91 avec la présence d'un espion est de la forme :



où $E(\vec{e}_a)$, $E(\vec{e}_b)$ sont les observables des projections de spin des qubits d'Alice et de Bob sur les directions $\vec{a}_k$, $\vec{b}_l$ choisies par Eve. Comme précédemment, le nom de chaque circuit contient des informations sur les mesures appliquées par Alice, Bob et Eve. L'exemple de la figure 2.24 indique que, lors de la mesure de la première paire de qubits, Alice a projeté un spin dans la direction $\vec{a}_2$, Bob dans la direction $\vec{b}_2$, et Eve a projeté le qubit d'Alice sur $\vec{e}_2$ et le qubit de Bob sur $\vec{b}_1$.

Une nouvelle valeur QBER, Qauntum Bit Error Rate a également été introduite, qui caractérise le taux d'erreur des clés d'Alice et de Bob. Elle correspond au rapport entre le nombre de bits incompatible de la clé et sa longueur. Pour définir la valeur de QBER, Alice et Bob doivent sacrifier une partie de leurs clés et y trouver des erreurs.

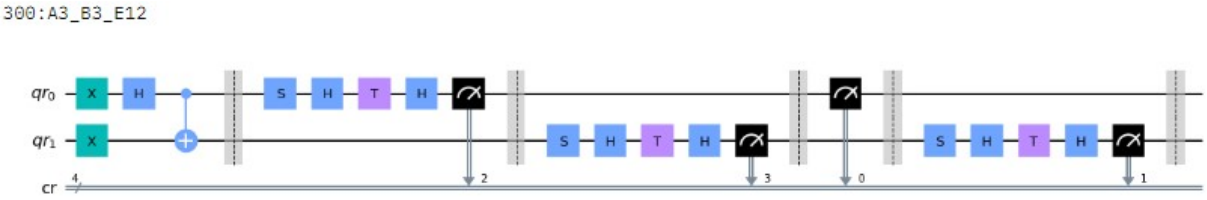


FIGURE 2.24 : Le circuit quantique du protocole E91 en présence d'espion.

Les résultats de l'exécution du programme qui simule la distribution de clé à qubit intriqué selon le protocole E91 avec l'intervention d'un espion utilisant la stratégie d'attaque interception-réémission est représenté dans la figure 2.25.

```
Valeur de correlation CHSH:  -1.288

QBER =  18.181818181818183 %

Longeur de la clé secrete:163
Nombre de bits incompatibles: 49

La quantité d'information de Eve sur la clé de Alice: 94.48 %
La quantité d'information de Eve sur la clé de Bob: 91.41 %
```

FIGURE 2.25 : L'exécution du protocole E91 en cas de présence dun espion.

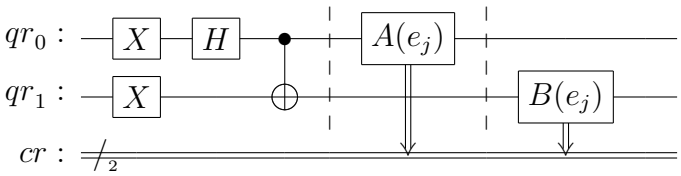
Le résultat de la simulation montre qu'Eve dispose de l'information, presque complète, sur les clés d'Alice et de Bob. Mais en même temps, elle introduit une erreur remarquable dans le coefficient de corrélation CHSH et QBER. Ceci entaîne la détection de l'écoute clandestine et impose Alice et Bob de mettre fin à la communication.

B Extraction de la clé secrète : Protocole BBM92

Considérons l'implémentation du protocole BBM92 sur un simulateur qui simule le fonctionnement d'un ordinateur quantique avec l'intervention ou non d'une écoute clandestine.

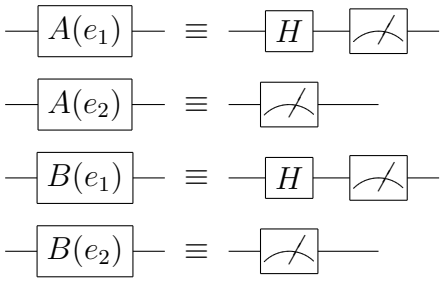
La première étape du protocole correspond à la distribution des qubits intriqués définie dans la section X et déterminés par le circuit quantique de la figure 2.20.

La deuxième étape du protocole consiste à la sélection des bases de mesure. À cette étape, Alice et Bob mesureront indépendamment les qubits reçus. La modélisation du protocole sans l'intervention d'une écoute clandestine, est la mise en oeuvre N des circuits suivants :



où $A(e_i)$ et $B(e_i)$, $i = 1, 2$ sont des mesures utilisées par Alice et Bob respectivement de leurs qubits dans les bases $\{e_i\}$ choisies au hasard et indépendamment du choix de l'autre.

Les algorithmes de mesure des qubits dans différentes bases sont définies par :



À la troisième étape du protocole, Alice et Bob doivent mesurer simultanément les états des qubits reçus de la paire intriquée. Pour simuler ce processus, il est nécessaire de créer N circuits quantiques en combinant le circuit source, figure 2.20, avec les circuits de mesure présentés ci-dessus.

La figure 2.26 représente un exemple du circuit d'un cycle de N étapes où à chaque ième étape une paire intriquée est formée, à partir de laquelle un qubit est envoyé à Alice et Bob. Ensuite, ils mesurent les qubits reçus conformément à l'ensemble préformé.

La tâche principale de cette étape est de mesurer les qubits reçus et de former des chaînes de bits d'Alice et de Bob dont les éléments sont les valeurs de la clé non tamisée.

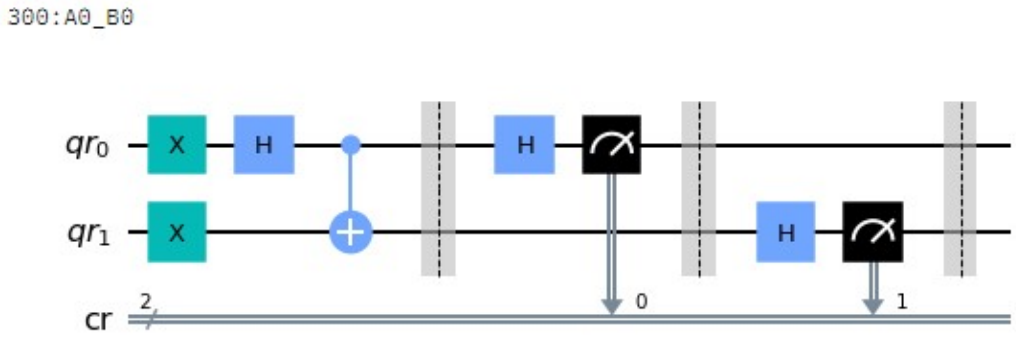


FIGURE 2.26 : Le circuit 300 du protocole BBM92 en absence d'un espion.

Comme tous les protocoles de cryptographie quantique, le protocole BBM92 permet de vérifier la sécurité d'une communication en se basant sur les résultats obtenus lors des mesures et de la génération des clés.

Après avoir effectué toutes les procédures du protocole vu préalablement, il ne reste plus qu'à compter le nombre de bits incompatibles et à afficher l'erreur QBER, suite à une révélation par Alice et Bob d'un certain nombre de bits pour estimer l'erreur dans la clé entière de manière assez précise.

```
QBER =  0.0 %

Longeur de la clé secrete: 125
Nombre de bits incompatibles: 0

Clé de Alice: [0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0,
0, 1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0,
0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1,
0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1]

Clé de Bob: [0, 0, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 0, 0, 0,
1, 1, 1, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0,
1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0,
1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 0, 1, 1, 1]
```

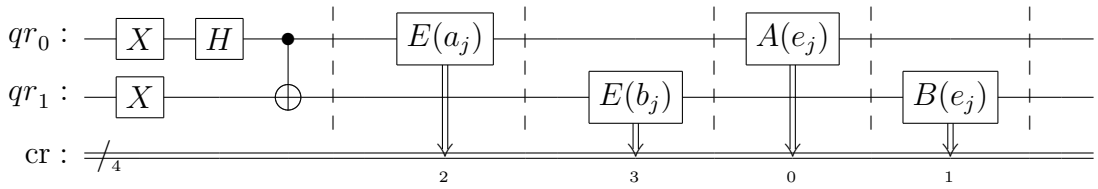
FIGURE 2.27 : L'exécution du protocole BBM92 en absence dun espion.

Les résultats du protocole BBM92 en cas d'absence d'une écoute clandestine pour le nombre de paires intriqués $N = 500$ sont représentés sur la figure 2.27. Comme prévu, la longueur finale de la clé secréte est d'environ un quart du nombre initial de paires de qubits intriqués. De plus, en l'absence d'une écoute clandestine et de bruit dans le canal quantique, aucun bit incompatible n'a été détecté et, par conséquent, la valeur de l'erreur QBER est nulle dans tous les cas.

A ce stade, la modélisation du protocole BBM92 est terminée. Nous allons ensuite considérer le fonctionnement du protocole en cas de présence de l'attaquant, Eve.

Pour mieux comprendre le principe de fonctionnement du protocole, une attaque interception-réémission est envisagée par Eve.

Dans cette attaque, l'attaquant Eve intercepte sur le canal quantique les qubits envoyés à Alice et Bob, elle les mesure dans des bases choisies au hasard, avant de les transmettre à leurs destinataire. Le schéma général du comportement de l'attaquant est illustré comme suit :



où $E(a_j)$ et $E(b_j)$ et l'une des actions d'Eve sur le qubit de Alice et Bob respectivement. Les actions d'Eve concernant le qubit intercepté sont aléatoires et indépendantes.

Afin de construire le modèle d'intervention, un changement du circuit précédent est nécessaire avec l'ajout de deux registre classique spécialement utilisés par Eve pour stocker ses résultats de mesure des qubits d'Alice et de Bob, voir la figure 2.23.

Un exemple de circuit formés est modélisé dans la figure 2.28. Étant donné que la stratégie d'Eve consiste à recevoir puis à renvoyer un qubit, ses circuits de mesure sont joints en premier, puis ceux d'Alice et Bob.

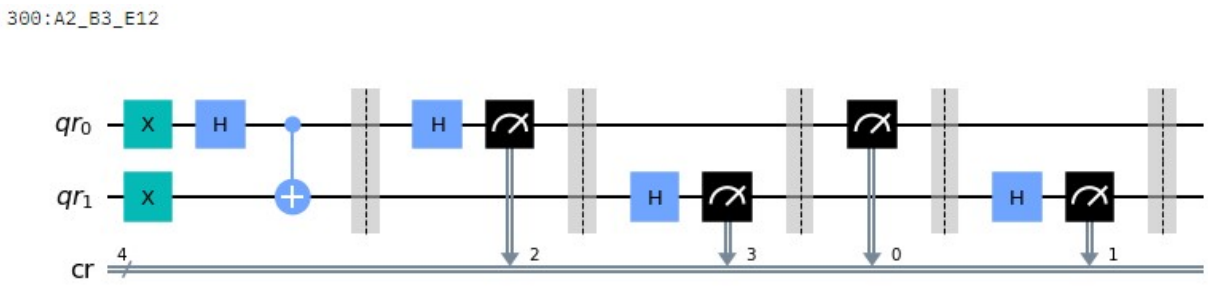


FIGURE 2.28 : Le circuit du protocole BBM92 avec présence d'espion.

Comme précédemment, Alice et Bob communiquent dans un canal classique un certains nombre de bits pour analyser la sécurité de la clé. Vu qu'Eve a la capacité d'écouter dans le canal classique, elle connaît donc exactement le nombre de ces bits qui doivent être vérifiés. Au final, toutes les parties à la communication régénérent une clé securisée si la veleur de l'erreur, QBER, est supérieure à 14.6%.

L'objectif de la simulation est d'étudier le fonctionnement du protocole BBM92 en cas de présence de l'espion. Pour cela, le calcule des valeurs suivantes est indispensable : QBER, la quantité moyenne d'informations dont Eve dispose, la longueur de la clé, et la quantité de l'information de Eve sur la clé par rapport aux clés d'Alice et de Bob séparément pour chacune, Voir la figure 2.29.

```
QBER =  28.31858407079646 %

Longeur de la clé secrete: 109
Nombre de bits incompatibles: 32

La quantité d'information de Eve sur la clé de Alice: 73.39 %
La quantité d'information de Eve sur la clé de Bob: 75.23 %
La quantité moyenne d'information de Eve : 74.31 %
```

FIGURE 2.29 : L'exécution du protocole BBM92 en présence d'un espion.

Comme on peut s'y attendre, avec un taux de présence suffisamment élevé, une quantité importante de perturbations parmi les participants légitimes, entraînant une augmentation du QBER.

Ceci termine l'implémentation du protocole BBM92 à l'aide du simulateur qui simule la distribution quantique d'une clé entre deux utilisateurs, et envisage également la stratégie d'intervention d'un attaquant, appelée stratégie de interception-réémission.

Chercher n'est pas une chose et trouver une autre,
mais le gain de la recherche,
c'est la recherche même.

Saint Grégoire de Nysse

3 Distribution semi-quantique de clé

I De la distribution quantique de clés à la distribution semi-quantique de clés

La distribution quantique de clés a fait son apparition dans les années 1980 en tant que méthode novatrice pour générer des séquences de bits aléatoires et secrètes, connues sous le nom de clés, utilisées dans les systèmes de cryptographie afin d'assurer la sécurité des communications. L'avantage de la distribution quantique de clés réside dans le fait que sa sécurité repose sur **les lois fondamentales de la physique**, offrant ainsi une solution plus robuste et fiable contrairement aux méthodes classiques de distribution de clés qui s'appuient sur des problèmes mathématiques complexes ou sur la sécurité physique du processus de distribution.

Un protocole typique de distribution quantique de clés implique deux parties, conventionnellement appelées Alice et Bob, qui cherchent à générer une clé secrète en échangeant des systèmes quantiques sur un canal de communication non sécurisé. La sécurité de ce dernier est évaluée en prenant en compte l'attaque la plus puissante sur le canal, où un intercepteur, généralement appelé Eve, perturbe les systèmes quantiques en utilisant les stratégies les plus générales permises par la mécanique quantique.

Cependant, dans un protocole de distribution de clés quantiques, chaque partie est tenue de posséder *des ressources quantiques*, ce qui nécessite souvent l'utilisation de dizaines de millions de dispositifs de génération quantique et d'équipements de fonctionnement. Cette exigence suscite des inquiétudes chez de nombreux utilisateurs, qui hésitent à adopter cette technologie étant donné que le matériel informatique quantique est extrêmement coûteux.

Dans le but d'accroître l'accessibilité de ces protocoles à un plus grand nombre d'utilisateurs, Boyer et al. [5,85] ont proposé en 2007 et en 2009 respectivement deux nouveaux protocoles de **distribution de clés semi-quantiques (SQKD)**, marquant ainsi l'émergence de la distribution semi-quantique de clé. Ces deux protocoles, mentionnés ci-dessus, nécessitent que l'un des utilisateurs dispose de ressources quantiques, en l'occurrence l'expéditeur Alice, alors que l'autre utilisateur muni des capacités quantiques restreintes désigner comme étant utilisateur "classique".

II Préliminaire

A Matrice densité

Un opérateur densité, également connu sous le nom de matrice densité, est un formalisme qui permet de décrire l'état quantique d'un système physique en prenant en compte l'ensemble des états quantique possibles à un instant donné.

Formellement, un opérateur densité ρ, est un opérateur hermitien, positif semi-défini, de trace 1 sur l'espace de Hilbert. Un opérateur densité associée à un ensemble d'états pur de distribution de probabilités $\{p_i, |\psi_i\rangle\}$ s'écrit de la façon suivante :

$$\rho = \sum_{i=1} p_i |\psi_i\rangle\langle\psi_i| \tag{3.1}$$

où p_i est la probabilité associée à un état pur particulier $|\psi_i\rangle$, qui satisfait à la relation $\sum_{i=1}^{n} p_i = 1$, où n est le nombre total d'états purs possibles.

Matrice densité résuite

Considérons un système composite AB, constitué de deux sous systèmes A et B, représenté par un opérateur densité ρ_{AB}. L'état du sous système A est obtenu grâce à une opération dite trace partielle de ρ_{AB} sur le sous système B qui est définie par

$$\rho_A = Tr_B(\rho_{AB}), \tag{3.2}$$

où ρ_A est l'opérateur densité réduit, appelé aussi trace partielle de ρ_{AB} sur B. Il contient toute information qui peut être extraite par mesure sur le sous-système A.

B Éléments de la théorie de l'information classique

La théorie de l'information classique, élaborée par le mathématicien Claude Shannon en 1948 dans son article A Mathematical Theory of Communications, est une théorie mathématique probabiliste appliquée aux techniques de la télécommunication. Cette théorie repose principalement sur la mesure de la quantité d'information contenue dans un message. Elle permet de quantifier la quantité d'information qui peut être transmise à travers un canal de communication, en prenant en compte les perturbations et les bruits éventuels qui peuvent altérer la transmission du message.

Entropie de Shannon

La notion d'entropie, est une grandeur thermodynamique liée au désordre d'un ensemble d'entités moléculaires, a été développée par Rudolf Clausius en 1865 et améliorée par Ludwig Boltzmann en 1872 dans le cadre de la physique statistique. Par la suite, Claude Shannon a étendu la notion d'entropie en l'appliquant au domaine de la théorie de l'information. Il a considéré l'entropie comme une grandeur mesurant la quantité d'incertitude associée à une source d'information donnée. Et il a établi une corrélation entre cette grandeur et la quantité minimale de bits nécessaires pour transmettre l'information de manière optimale.

Etant donnée une variable aléatoire discrète X donnant comme résultats $x_1, x_2, ..., x_i$ avec des distribution de probabilités $p_1, p_2, .., p_i$. Par définition l'entropie de Shannon $H(X)$ de X est

$$H(X) = -\sum_{x \in X} p(x) \log p(x) \tag{3.3}$$

L'unité de mesure de l'information dans l'entropie de Shannon est déterminée de manière proportionnelle par la base du logarithme utilisé. Par convention, la base 2 du logarithme est souvent utilisée pour exprimer l'entropie en bits.

Dans le cas où x_j est un résultat certain $p(X = x_j) = 1$, alors tous les autres résultats ont forcément $p(X = x_i) = 0$. Pour $i \neq j$. Ainsi, l'entropie $H(X) = 0$. En revanche, si tous les résultats sont équiprobables, chaque résultat a la même probabilité d'être transmis, l'entropie de la variable X est maximale et vaut $\log_2(n)$, où n est le nombre total de résultats possibles.

Plus particulièrement, l'entropie d'une variable aléatoire à deux résultats possibles, est définie comme suit

$$H(X) = -p(x) \log_2 p(x) - (1 - p(x)) \log_2(1 - p(x)), \tag{3.4}$$

Cette formule désigne l'entropie binaire où $p(x)$ et $1 - p(x)$ sont les probabilités des deux résultats possibles.

L'entropie conjointe, l'entropie conditionnelle et l'information mutuelle

Considérons un couple de variables aléatoires X et Y. Les résultats possibles pour X sont $x_1, x_2, ..., x_i$ et celle pour Y sont $y_1, y_2, ..., y_j$, alors l'information apportée par la connaissance simultanée du couple (X, Y) est définie par *l'entropie conjointe*, donnée par

$$H(X, Y) = -\sum_{x \in X, y \in Y} p(x, y) \log_2 p(x, y) \tag{3.5}$$

Dans le cas où X et Y sont indépendantes, l'entropie du couple (X, Y) est la somme des entropies individuelles

$$H(X, Y) = H(X) + H(Y) \tag{3.6}$$

L'entropie conditionnelle se définit comme étant la mesure de l'information acquise suite à l'observation d'un résultat spécifique issu d'une variable aléatoire, en présence d'une information préalable.

$$H(Y|X) \;=\; H(X,Y) \;-\; H(X). \tag{3.7}$$

À partir de cette définition, l'entropie conditionnelle peut être exprimée en termes de logarithmes, est donnée par :

$$\begin{aligned} H(Y|X) \;&=\; \sum_{x_i \in X} p(X = x_i) H(Y|X = x_i) \\ &=\; -\sum_{x_i \in X, y_j \in Y} p(X = x_i, Y = y_j) \log_2 p(Y = y_j | X = x_i). \end{aligned} \tag{3.8}$$

L'information mutuelle entre deux variables aléatoires X et Y notée $I(X : Y)$, où I_{XY}, mesure la quantité d'information partagée entre ces deux variables aléatoires. Elle correspond également une mesure de la corrélation entre les variables X et Y :

$$I(X : Y) \;=\; \sum_{x \in X} \sum_{y \in Y} p(x, y) \log \frac{p(x, y)}{p(x) p(y)}. \tag{3.9}$$

D'après les propriétés fondamentales de l'information mutuelle, il apparaît clairement que cette dérnière est nulle lorsque les deux variables aléatoires sont indépendantes. Cette information mutuelle est également toujours positive ou nulle. En outre, il est possible de vérifier les relations suivantes en se basant sur les définitions énoncées précédemment

$$\begin{aligned} I(X : Y) &= H(X) \;-\; H(X|Y) \\ &=\; H(Y) \;-\; H(Y|X) \\ &=\; H(X) \;+\; H(Y) \;-\; H(X,Y). \end{aligned} \tag{3.10}$$

C Éléments de la théorie de l'information quantique

John von Neumann a élaboré une théorie de l'information qui s'appuie sur des définitions fondamentales différentes de celles proposées par Shannon, mais dont certaines propriétés sont communes. La théorie de l'information de von Neumann se concentre sur l'étude de la quantification et de la transmission de l'information dans le cadre de la mécanique quantique, en se basant sur la notion de densité de probabilité plutôt que sur celle de variable aléatoire.

Entropie de Von Neumann

L'entropie de Von Neumann quantifie l'information contenue dans un système décrit par un état quantique ρ dans un espace de Hilbert $\mathcal{H}$

$$S(\rho) \;=\; -Tr(\rho \log \rho) \tag{3.11}$$

L'entropie de Von Neumann est une généralisation de l'entropie de Shannon pour tout état quantique ρ dans un espace de Hilbert $\mathcal{H}$. En effet, il est possible de décomposer

l'état quantique ρ sous forme diagonale $\widehat{\rho} = \sum_{i=1}^{d} \lambda_i |\psi_i\rangle\langle\psi_i|$, avec λ_i les valeurs propres de ρ remplacent la distribution de probabilités dans l'entropie de Shannon

$$S(\rho) = -\sum_i \lambda_i \log_2 \lambda_i. \tag{3.12}$$

Quelques propriétés de base

Quelques propriétés de base découlent immédiatement de la définition et des propriétés de l'entropie de Shannon. Pour une liste détaillée des propriétés de l'entropie de Von Neumann, le lecteur est invité à se référer aux ouvrages spécialisés tels que [82].

1. $S(\rho) \geq 0$, l'entropie vaut zéro si et seulement si l'état ρ est un état pur.
2. AB un système composé, dans un état pur, alors $S(\rho_A) = S(\rho_B)$
3. L'entropie d'un produit tensoriel de deux opérateurs de densité ρ et σ :

$$S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$$

4. L'entropie de Von Neumann est invariante par transformation unitaire U :

$$S(U\rho U^{-1}) = S(\rho)$$

5. Sous-additivité :

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B).$$

Entropie conjointe, entropie conditionnelle et l'information mutuelle

L'entropie conjointe de Von Neumann, $S(AB)$ est une mesure mathématique de l'incertitude quantique associée au système bipartite $\mathcal{H}_A \otimes \mathcal{H}_B$, représentée par la matrice de densité ρ_{AB}. Cette mesure est définie comme

$$S(AB) = S(\rho_{AB}) = -tr\left(\rho_{AB} \log_3 \rho_{AB}\right) = -\sum_i \lambda_i \log_3 \lambda_i \tag{3.13}$$

$$S(A,B) = -Tr(\rho_{AB} \log_2 \rho_{AB}), \tag{3.14}$$

Lemma 1. *Étant donné un espace de Hilbert à dimension finie $\mathcal{H} = \mathcal{H}_C \otimes \mathcal{H}_E$, où $|1\rangle_C, \ldots, |n\rangle_C$ est une base orthonormée de $\mathcal{H}_C$. Considérons l'opérateur de densité suivant agissant sur $\mathcal{H}$:*

$$\rho = \sum_{j=1}^{n} p_j |j\rangle\langle j|_C \otimes \sigma_E^{(j)}, \tag{3.15}$$

où $\sum p_i = 1, p_i \geq 0$, et chaque $\sigma_E^{(i)}$ est un opérateur hermitien semi-défini positif de trace unitaire agissant sur $\mathcal{H}_E$. Alors, l'entropie de von Neumann de ρ est donnée par :

$$S(\rho) = H(p_1, p_2, \ldots, p_n) + \sum_{j=1}^{n} p_j S(\sigma_E^{(i)}). \tag{3.16}$$

Pour une démonstration de ce lemme, vous pouvez vous référer au livre intitulé *"Quantum Computation and Quantum Information"* [82].

L'entropie conditionnelle est une mesure de l'information quantique apportée sur le système A par la connaissance conjointe du système composite AB, une fois que l'entropie de B est soustraite. Cela permet de quantifier l'information qui peut être obtenue sur le système A à partir de la connaissance de l'état du système B. Mathématiquement, Elle est représentée par la formule

$$S(A|B) \;=\; S(A,B) \;-\; S(B). \tag{3.17}$$

L'information mutuelle de Von Neumann, notée $S(A:B)$, est une mesure de la dépendance entre deux états quantiques. Elle est définie de manière similaire à l'information mutuelle classique [86], exprimée en termes d'entropie par

$$S(A:B) \;=\; S(A) \;+\; S(B) \;-\; S(A,B) \tag{3.18}$$

Tout comme dans le cas de l'information mutuelle classique, la quantité d'information mutuelle de Von Neumann est une grandeur symétrique :

$$S(A:B) = S(B:A)$$

D Les bases mutuellement non biaisées pour les états quantiques

Les bases mutuellement non biaisées, introduites par Schwinger en 1960 [87] comme des bases de mesure optimales incompatibles, ont attiré une attention considérable en tant que ressource cruciale dans le traitement de l'information quantique.

Les bases mutuellement non biaisées, généralement abrégées MUBs, sont utilisées dans la détermination de l'état quantique [88], la tomographie de l'état quantique [89] ainsi que les codes de correction d'erreur quantique [90]. De plus, les MUBs ont été appliquées avec succès dans les protocoles de distribution de clés quantiques grâce au fait que les mesures dans une base empêchent la connaissance de l'état dans toutes les autres [91, 92].

Un ensemble de deux bases de l'espace de Hilbert est dit mutuellement non biaisées si une mesure effectuée dans l'une des bases entraîne un résultat parfaitement aléatoire pour toute autre mesure effectuée dans l'autre base de l'ensemble.

De manière plus rigoureuse, deux bases orthonormales $|v_i\rangle$ et $|w_j\rangle$ d'un espace de Hilbert $\mathcal{H} = \mathbb{C}^d$ de dimension d, étant mutuellement non biaisées si et seulement si :

$$|\langle v_i|w_j\rangle| = \frac{1}{\sqrt{d}}, \tag{3.19}$$

pour tous les $i, j = 1, 2 \ldots, d$. Ces bases sont également appelés maximalement incompatibles, ou complémentaires. Il est bien connu que, dans un espace de Hilbert de dimension d, le nombre maximal de bases mutuellement non biaisées ne peut être que $d + 1$ dans un système de dimension première ou de dimension de puissance première. Ce résultat a été prouvé pour la première fois par Ivonovic en 1981, qui a introduit le concept de

MUBs, et a été démontré de manière plus explicite par Wootters et Fields en 1989, qui ont également fourni une méthode de construction explicite de MUBs pour les systèmes de dimension première et de puissance première [88, 93].

Pour un espace de dimension finie $d = 2$, l'ensemble des états propres des trois opérateurs de Pauli forme un ensemble complet de bases mutuellement non biaisées. Cette base peut être représentée par

$$\{|0\rangle, |1\rangle\} \qquad \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\} \qquad \{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

III Le modèle de distribution semi-quantique de clé

Dans le cadre de la distribution semi-quantique de clé, le modèle le plus répandu implique deux utilisateurs, à savoir Alice et Bob, avec Alice agissant en tant qu'utilisateur pleinement quantique et Bob en tant qu'utilisateur semi-quantique ou classique. Alice est dotée d'un canal quantique qui s'étend depuis son laboratoire, traverse un milieu extérieur, et revient finalement à son point de départ, alors que Bob n'a accès qu'à une partie de ce canal quantique.

Les protocoles semi-quantiques se basent ainsi sur un canal quantique bidirectionnel, dans lequel les états quantiques voyagent d'abord de l'utilisateur quantique Alice vers l'utilisateur classique Bob, avant de retourner à nouveau à l'utilisateur quantique. Ce modèle est illustré dans la figure 3.1.

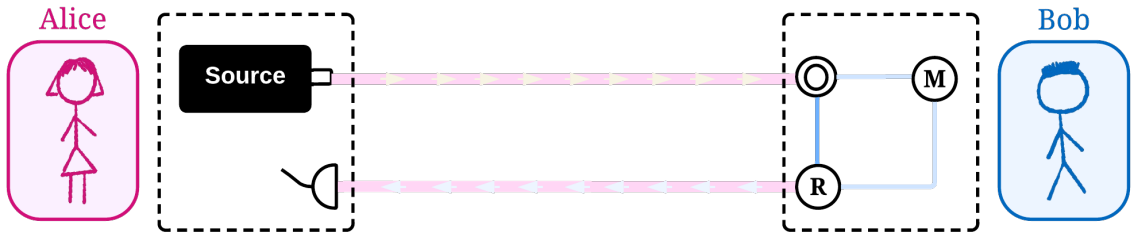


FIGURE 3.1 : Le modèle de distribution semi-quantique de clé.

Outre l'exigence d'un canal quantique bidirectionnel, les protocoles de distribution semi-quantique de clé imposent une restriction supplémentaire du côté de l'utilisateur classique. En effet, l'utilisateur classique ne peut effectuer des mesures que dans la base Z ou envoyer des états quantiques préparés dans cette base. Sinon, il doit simplement se déconnecter brièvement, permettant ainsi à l'utilisateur quantique Alice de communiquer avec elle-même.

Lors de la réception d'un état quantique, l'utilisateur classique, Bob, peut choisir parmi un ensemble limité d'opérations, à savoir :

1. Mesure : L'opération consiste à appliquer une mesure sur le qubit entrant dans la base Z, où la base Z correspond à la base standard des états quantiques, constituée des états de base $|0\rangle$ et $|1\rangle$.

2. Préparer : Il s'agit de la préparation d'un état quantique dans la base Z, qui est ensuite envoyé à Alice sur le canal quantique inverse.
3. Mesurer et renvoyer : Une opération combinée qui implique la soumission du qubit entrant à une mesure dans la base Z, suivie de l'envoi du résultat classique équivalent à Alice sous forme d'un qubit préparé dans la base Z.
4. Réfléchir : L'opération de réflexion consiste à renvoyer le qubit entrant à Alice sans perturber son état quantique. Cette opération est équivalente à une déconnexion du canal quantique et à un renvoi de tous les qubits à Alice. L'utilisateur classique ne reçoit aucune information sur l'état quantique du qubit lors de cette opération. Par conséquent, Alice devrait récupérer le qubit dans le même état quantique que celui qu'elle avait envoyé initialement à Bob.
5. Permutation : Cette opération consiste à réorganiser les qubits reçus ou un sous-ensemble de qubits reçus sans perturber leurs états sous-jacents. Elle permet à l'utilisateur classique de modifier l'ordre des qubits sans avoir accès à leur information quantique.

Les protocoles qui font appel à l'opération Réfléchir ainsi qu'à l'opération Mesurer et renvoyer sont communément désignés sous le terme de protocoles measure-resend. En revanche, ceux qui impliquent l'utilisation de l'opération Permutation sont généralement appelés protocoles basés sur la randomisation [85].

IV Protocoles de distribution semi-quantique de clé

Les protocoles les plus célèbres pour la distribution semi-quantique de clé sont les protocoles BKM07 [5] et BGKM09 [85]. Le premier est un protocole Mesurer-renvoyer (Measure-Resend SQKD) pour la distribution semi-quantique de clé, qui a été proposé par Michel Boyer, Dan Kenigsberg et Tal Mor en 2007. Quant au second, il s'agit d'un protocole, basé sur la randomisation (Randomization-Based SQKD) pour la distribution semi-quantique de clé, qui a été développé en 2009 par les mêmes auteurs en collaboration avec Ran Gelles.

A Principe de fonctionnement du protocole BKM07

Le protocole commence avec Alice qui à chaque itération du protocole, prépare un photon unique en choisissant aléatoirement une orientation de spin, correspondant à l'une des quatre polarisations possibles : 0°, 45°, 90° et 135°, représentant respectivement les spins horizontaux, diagonaux, verticaux et anti-diagonaux (voir la section B sur la polarisation pour plus de détails). Alice envoie ensuite le photon préparé à Bob, un utilisateur classique, tout en gardant en mémoire son choix initial.

Une fois que Bob reçoit le photon, il choisit aléatoirement l'une des deux opérations suivantes : Mesurer et renvoyer ou Réfléchir. Par la suite, Alice mesure le photon de retour dans la même base qu'elle a initialement utilisée pour le préparer.

Après la transmission quantique des états, Alice révèle à Bob la base qu'elle a utilisée pour préparer les photons envoyés à chaque itération, tandis que Bob dévoile l'opération

qu'il a utilisée pour chaque itération. Conformément au protocole, Alice garde secrètement les états quantiques initialement générés. De même, Bob garde également confidentiels les bits classiques obtenus à partir des itérations qu'il a choisis pour mesurer le qubit entrant.

Pour construire leur clé brute, ils utilisent les itérations où Alice choisit d'envoyer un photon de base Z et où Bob opte pour l'opération Mesurer et renvoyer, les deux parties doivent s'attendre à ce que les bits secrets résultants soient complètement corrélés. Les itération où Alice choisit d'envoyer les photons dans la base X et où Bob choisit l'opération Mesurer et Renvoyer, Bob doit s'attendre à une distribution uniforme des résultats classiques observés, c'est-à-dire $|0\rangle$ dans 50% des cas et $|1\rangle$ dans 50% des cas. Pour les itération restantes où Bob a choisi l'opération Réfléchir, Alice effectue une première estimation du taux d'erreur de bits quantiques QBER sur le canal de communication quantique, en fonction de ses choix possibles de bases pour préparer les photons, c'est-à-dire les bases Z et X.

Alice et Bob choisissent également un échantillon aléatoire de bits à partir de leurs clés tamisées, sur lequel ils effectuent une deuxième estimation des paramètres. Pour les deux groupes de bits utilisés dans les deux estimations de paramètres, si au moins un des QBER estimés est supérieur à une limite supérieure maximale prédéfinie, le protocole est abandonné. Sinon, les deux groupes de bits doivent être supprimés, ce qui entraîne une corrélation complète des bits sur leur clé tamisée raccourcie.

Le protocole comprend également les étapes standard de réconciliation des clés et d'amplification de la confidentialité pour corriger certaines erreurs restantes dans les clés tamisées et améliorer la sécurité de la clé réconciliée, respectivement. Finalement, à partir de ces deux dernières étapes, Alice et Bob doivent convenir de la clé symétrique finale résultante, qui sera utilisée pour sécuriser leurs communications.

B Principe de fonctionnement du protocole BGKM09

Dans le cadre du protocole BGKM09, une alternative à l'opération Measure-and-Resend est proposée par Bob, qui utilise plutôt l'opération Permute. Dans ce protocole, Alice suit le même processus de préparation des photons que dans le protocole BKM07. À chaque itération du protocole, Alice prépare un photon unique avec une orientation de spin aléatoire, représentant des spins horizontaux, diagonaux, verticaux ou anti-diagonaux, correspondant respectivement aux polarisations de 0°, 45°, 90° et 135°.

De son côté, Bob choisit de manière aléatoire entre les opérations Measure et Reflect pour les photons entrants. Lorsque Bob choisit l'opération Reflect, il effectue également l'opération Permute avant de renvoyer les photons à Alice.

Il est important de noter que dans cette opération, Bob n'effectue aucune mesure sur les photons ni ne les perturbe. Toutefois, il les réordonne avant de les renvoyer à Alice. En revanche, Bob renvoie les photons dans l'étape où il a choisi l'opération Mesurer. Alice stocke ensuite tous les photons retournés par Bob dans une mémoire quantique jusqu'à la fin de la transmission quantique des états.

A la fin de la transmission quantique des photons, Bob annonce publiquement les photons des itérations sur lesquels il a choisi l'opération Reflect, ainsi que l'ordre dans lequel il les a renvoyés à Alice en utilisant l'opération Permute. Alice rétablit alors l'ordre initial de ces photons, les mesurant selon la même base que celle utilisée lors de leur

préparation initiale.

Par la suite, Alice divulgue publiquement à Bob les itérations qu'elle a utilisées pour préparer les photons dans la base Z. Si Bob a choisi d'effectuer une mesure sur les photons dans ces itérations, alors les bits secrets partagés entre les deux parties sont corrélés, permettant ainsi la création de leur clé brute. Autrement dit, en ayant connaissance de la base de préparation de chaque photon, Bob peut réaliser une mesure dans la même base et obtenir des résultats corrélés avec ceux d'Alice, ce qui leur permet de construire leur clé de chiffrement.

Malgré tout, la clé filtrée pourrait contenir des erreurs, car Eve pourrait avoir intercepté certains de ces itérartions. Lors des itérations où Bob a choisi les opérations "Reflect" et "Permute", Alice réalise une première estimation des paramètres. En outre, Alice et Bob prélèvent également un échantillon aléatoire de bits à partir de leurs clés tamisées afin de réaliser une autre estimation des paramètres.

Sous l'hypothèse que le taux d'erreur estimés QBER est "suffisamment faible", Alice et Bob doivent effectuer l'étape de Réconciliation d'information pour corriger les erreurs restantes de leur clé tamisée raccourcie. De plus, ils peuvent également effectuer l'étape d'Amplification de confidentialité, à partir de laquelle ils conviennent d'une clé symétrique finale protégée contre tout accès non autorisé.

V SQKD basée sur les bases mutuellement non biaisées

Les travaux présentés dans cette section ont fait l'objet de deux articles publiés dans Quantum Information Processing et Physics Letters A.

Les protocoles de distribution de clés semi-quantiques peuvent être formulés et implémentés en utilisant des systèmes de différentes dimensions tels que les qubits et qutrits. L'augmentation de la dimension du système permet d'élargir le nombre de bases mutuellement non biaisées sur lesquelles le protocole peut s'appuyer, ce qui engendre de nombreuses versions et variantes du même protocole.

Dans cette section, nous nous concentrons sur la robustesse des protocoles de distribution de clés semi-quantiques basés sur qutrits et ququarts avec différentes bases mutuellement non biaisées, dans le cas d'attaques d'écoute collective. Nous établissons une borne inférieure sur le taux de clé qui dépend uniquement du bruit du canal quantique, un paramètre pouvant être estimé par les parties légitimes, et nous évaluons cette borne inférieure en considérant les formes les plus courantes de canaux, à savoir les canaux indépendants et les canaux dépendants. L'objectif de cette section est d'explorer l'utilisation des bases mutuellement non biaisées dans ces protocoles de distribution de clés semi-quantiques.

A Le principe de fonctionnement du protocole

Notre étude se concentre sur une extension du protocole de distribution de clés semi-quantique (SQKD) basé sur les qubits, tel qu'introduit dans la référence [5], appliqué cette fois-ci à des dimensions finies quelconques tout en faisant varier le nombre de bases mutuellement non biaisées employées. Cette extension entraîne l'émergence d'une variation

de nombre de base mutuellement non biaisées, MUBs, que Alice peut utiliser.

La phase de communication quantique du protocole se compose d'une série d'itérations jusqu'à ce qu'une clé brute suffisamment grande soit obtenue.

Transmission quantique

- Alice, en tant qu'utilisateur entièrement quantique, prépare aléatoirement un qudit dans un état choisi en fonction de la version du protocole adopté, *i.e.* nombre de bases mutuellement non biaisées utilisées. Ce qudit est ensuite envoyé à Bob pour traitement ultérieur.
- Bob, l'utilisateur classique, est restreint à choisir aléatoirement entre deux opérations : une opération de réflexion, R, dans laquelle il renvoie simplement le qudit à Alice sans le perturber, ou une opération de mesure et de renvoi, M, dans laquelle il effectue une mesure [1] du qudit dans la base du calcul $\mathcal{A} = \{|0\rangle, |1\rangle, |2\rangle ... |d-1\rangle\}$, et transmet le résultat de la mesure à Alice en l'encodant dans un état quantique équivalent au bit classique trouvé. Les objectifs de ces opérations seront décrits ci-dessous :
  - Les itérations lors desquels Bob choisit l'opération de mesure et de renvoi, qui se produit avec une fréquence plus élevée, sont désignés sous le nom de SIFT et sont utilisés pour établir les bits secrets qui composeront la clé secrète.
  - Les itérations au cours desquels Bob opte pour l'opération de réflexion, qui se produisent avec une fréquence plus faible, sont identifiés en tant que CTRL et sont destinés à détecter une éventuelle tentative d'interception de la part d'Eve.
- Pour le qudit renvoyés par Bob, Alice procède à une mesure de celui-ci dans la même base qu'elle avait utilisée lors de l'étape 1 pour le préparer.

Réconciliation des clés et estimation de paramètres

- En utilisant un canal classique authentifié, Alice et Bob échangent leurs choix respectifs : Alice communique sa base utilisée pour préparer le qudit tandis que Bob dévoile son choix d'opération mesurer (M) ou retourner (R) le qudit.
  - Les itérations lors desquels Alice choisit la base $\mathcal{A}$ pour encoder son qudit et Bob effectue l'opération de mesure et de renvoi(M), Alice et Bob conservent leurs résultats respectifs pour former leur propre version de la clé brute.
  - Lors de chaque itérations de CTRL, Alice estime le taux d'erreur du canal quantique. Si le taux d'erreur quantique (QBER) dépasse un seuil prédéfini, Alice notifie Bob pour qu'il abandonne le protocole. Dans le cas contraire, si QBER ne dépasse le seuil prédéfini, Alice et Bob rejettent toutes les itérations de CTRL précédentes et poursuivent le protocole.

1. La qualification de Bob en tant qu'utilisateur classique découle de son incapacité à mesurer et/ou préparer des états dans plus d'une base, contrairement à Alice, l'utilisatrice pleinement quantique, capable d'utiliser à la fois la base $\mathcal{A}$ et autres bases selon la version du protocole adoptée.

- De plus, Alice et Bob annoncent également les bits classiques de leurs clés tamisées, à partir d'un échantillon choisi au hasard parmi les itérations SIFT, pour effectuer une deuxième estimation de paramètres. Si le taux d'erreur quantique (QBER) dépasse un seuil prédéfini, ils abandonnent le protocole. Sinon, ils doivent supprimer ces bits classique et poursuivre l'exécution du protocole. Après cette étape, Alice et Bob disposent de leurs clés tamisées qui peuvent encore contenir des erreurs.

Correction d'erreur et Amplification de confidentialité

- Sous l'hypothèse que le bruit dans le canal est inférieur à un certain seuil, Alice et Bob appliquent un protocole de correction d'erreur ainsi qu'un protocole d'amplification de confidentialité afin d'éliminer toute fuite d'information restante lors des étapes de transmission d'états quantiques ou de réconciliation des clés, et de réduire les connaissances partielles qu'Eve pourrait avoir sur cette clé brute, ce qui conduit à une clé secrète.

B Attaque collective avec des états quantique à trois dimensions

Dans cette sous-section, nous prouvons la sécurité du protocole de distribution semi-quantique de clés basé sur la transmission de systèmes tridimensionnels, qutrits, avec deux, trois et quatre bases mutuellement non biaisées contre les attaques collectives. Cette classe d'attaques permet à l'adversaire, Eve, de conserver ses états auxiliaires dans une mémoire quantique jusqu'à ce qu'elle reçoive toutes les données classiques, y compris les données de correction d'erreur et d'amplification de confidentialité. Eve peut alors réaliser une mesure optimale sur ses états auxiliaires pour obtenir l'information maximale sur la clé finale.

En présence d'un adversaire restreint aux attaques collectives, la borne de Devetak-Winter [77] permet de calculer le taux de clé secrète possible en utilisant une réconciliation inverse :

$$r = inf[S(B|E) - H(B|A)], \tag{3.20}$$

Le taux de clé secrète correspond à la différence entre l'incertitude d'Eve sur la clé brute de Bob $S(B|E)$, qui doit être élevée pour garantir la sécurité du protocole, et l'incertitude d'Alice sur la clé de Bob $H(B|A)$, qui doit être faible. L'infimum, *inf*, est pris sur toutes les attaques collectives qui induisent les taux d'erreur observés. Pour notre travail, nous visons à établir une borne inférieure sur le taux de clé secrète du protocole, en considérant toutes les attaques collectives possibles qui peuvent engendrer les taux d'erreur observés.

Considérons l'espace de Hilbert, $\mathcal{H}_T$, qui représente le qutrit en transit, et l'espace de Hilbert, $\mathcal{H}_E$, qui représente l'ancilla privée de l'attaquant Eve pour une itération du protocole. Pour mener son attaque, Eve utilise une paire d'opérateurs d'attaque unitaires (U_F, U_R) agissant sur $\mathcal{H}_T \otimes \mathcal{H}_E$. L'opérateur unitaire U_F attaquant les états quantiques envoyé par Alice à Bob (*i.e.*, le canal direct), et l'opérateur unitaire U_R est utilisé lorsqu'ils retournent de Bob à Alice (*i.e.*, canal inverse).

De manière conventionnelle, la première base du protocole est généralement associée à la base de calcul, telle que $\{|0\rangle, |1\rangle, |2\rangle\}$ dans un espace de Hilbert tridimensionnel. En supposant que l'ancilla de l'attaquant Eve est préalablement réinitialisée à un état $|E\rangle \in \mathcal{H}_E$, sans perte de généralité, Eve peut procéder à une attaque en utilisant l'opérateur unitaire U_F, qui agit sur les états de la manière suivante

$$\begin{aligned} |0\rangle \otimes |E\rangle &\xrightarrow{U_F} |0\rangle|e_{00}\rangle + |1\rangle|e_{01}\rangle + |2\rangle|e_{02}\rangle, \\ |1\rangle \otimes |E\rangle &\xrightarrow{U_F} |0\rangle|e_{10}\rangle + |1\rangle|e_{11}\rangle + |2\rangle|e_{12}\rangle, \\ |2\rangle \otimes |E\rangle &\xrightarrow{U_F} |0\rangle|e_{20}\rangle + |1\rangle|e_{21}\rangle + |2\rangle|e_{22}\rangle, \end{aligned} \tag{3.21}$$

où $|e_{ji}\rangle$ sont des états arbitraires dans $\mathcal{H}_E$, qui ne sont pas nécessairement normalisés ni orthogonaux, avec $i, j = 0, 1, 2$. L'unitarité de l'opérateur U_F impose, sur les produits scalaires entre les états de sortie de l'attaquant Eve les conditions suivantes

$$\begin{aligned} \langle e_{00}|e_{10}\rangle + \langle e_{01}|e_{11}\rangle + \langle e_{02}|e_{12}\rangle &= 0 \\ \langle e_{10}|e_{20}\rangle + \langle e_{11}|e_{21}\rangle + \langle e_{12}|e_{22}\rangle &= 0 \\ \langle e_{00}|e_{20}\rangle + \langle e_{01}|e_{21}\rangle + \langle e_{02}|e_{22}\rangle &= 0. \end{aligned} \tag{3.22}$$

Évidemment, sur le canal de retour l'attaquant Eve intercepte le qutrit de transit, applique son deuxième opérateur d'attaque U_R sur les états de la forme $|i, e_j\rangle$. L'action de cet opérateur sans perte de généralité, est exprimée de la manière suivante

$$|i, e_{ji}\rangle \xrightarrow{U_R} |0, e^0_{i,ji}\rangle + |1, e^1_{i,ji}\rangle + |2, e^2_{i,ji}\rangle. \tag{3.23}$$

Les $|e^k_{i,ji}\rangle$ représentent les états auxiliaires d'Eve, qui ne sont pas nécessairement normalisés ni orthogonaux.

En utilisant la notation décrite précédemment, nous sommes maintenant en mesure de déduire le système quantique commun modélisant une itération unique du protocole, en prenant en compte les événements qui contribuent à la production d'une clé brute.

Conditionnons l'événement selon lequel cette itération est utilisée pour contribuer à la clé brute, Alice envoie $|0\rangle$, $|1\rangle$ ou $|2\rangle$ avec une probabilité de 1/3 chacun. Eve attaque ensuite le qutrit en utilisant U_F, puis le transmet à Bob qui le mesure dans la base $\mathcal{A}$, renvoyant son résultat de mesure sous forme d'un nouveau qutrit. Ce qutrit est à nouveau intercepté par Eve qui l'attaque avec U_R. Enfin, Alice effectue une mesure dans la base $\mathcal{A}$. En éliminant le système de Alice par le biais de la trace partielle, nous obtenons la matrice de densité ρ_{BE} qui représente l'état quantique réduit des systèmes de Bob et Eve :

$$
\begin{aligned}
\rho_{BE} =& \frac{1}{3}|0\rangle\langle 0|_B \otimes \Big(|e^0_{0,00}\rangle\langle e^0_{0,00}| + |e^1_{0,00}\rangle\langle e^1_{0,00}| + |e^2_{0,00}\rangle\langle e^2_{0,00}| + |e^0_{0,10}\rangle\langle e^0_{0,10}| \\
&+ |e^1_{0,10}\rangle\langle e^1_{0,10}| + |e^2_{0,10}\rangle\langle e^2_{0,10}| + |e^0_{0,20}\rangle\langle e^0_{0,20}| + |e^1_{0,20}\rangle\langle e^1_{0,20}| + |e^2_{0,20}\rangle\langle e^2_{0,20}| \Big) \\
&+ \frac{1}{3}|1\rangle\langle 1|_B \otimes \Big(|e^0_{1,01}\rangle\langle e^0_{1,01}| + |e^1_{1,01}\rangle\langle e^1_{1,01}| + |e^2_{1,01}\rangle\langle e^2_{1,01}| + |e^0_{1,11}\rangle\langle e^0_{1,11}| \\
&+ |e^1_{1,11}\rangle\langle e^1_{1,11}| + |e^2_{1,11}\rangle\langle e^2_{1,11}| + |e^0_{1,21}\rangle\langle e^0_{1,21}| + |e^1_{1,21}\rangle\langle e^1_{1,21}| + |e^2_{1,21}\rangle\langle e^2_{1,21}| \Big) \\
&+ \frac{1}{3}|2\rangle\langle 2|_B \otimes \Big(|e^0_{2,02}\rangle\langle e^0_{2,02}| + |e^1_{2,02}\rangle\langle e^1_{2,02}| + |e^2_{2,02}\rangle\langle e^2_{2,02}| + |e^0_{2,12}\rangle\langle e^0_{2,12}| \\
&+ |e^1_{2,12}\rangle\langle e^1_{2,12}| + |e^2_{2,12}\rangle\langle e^2_{2,12}| + |e^0_{2,22}\rangle\langle e^0_{2,22}| + |e^1_{2,22}\rangle\langle e^1_{2,22}| + |e^2_{2,22}\rangle\langle e^2_{2,22}| \Big).
\end{aligned}
\tag{3.24}
$$

L'utilisation de l'équation (3.20) permet d'établir une borne inférieure sur le taux de clé en limitant l'entropie de von Neumann $S(B|E)$.Toutefois, en raison de la dimension supérieure du système, cela pourrait s'avérer difficile. Pour y parvenir, nous utiliserons une technique proposée dans [94] et également utilisée dans [16]. Cette technique nécessite de conditionner une variable aléatoire supplémentaire C, afin de simplifier les calculs d'entropie. Avec sa propriété de sous-additivité rigoureuse, l'entropie de von Neumann de tout système tripartite satisfait

$$S(B|E) \geq S(B|EC), \tag{3.25}$$

où C est une variable aléatoire supplémentaire introduite pour former un système composite à quatre parties $ABEC$. Ainsi, l'inégalité (3.25) nous fournit donc une borne inférieure sur le taux de clé :

$$r \geq inf[S(B|E) - H(B|A)] \geq inf[S(B|EC) - H(B|A)], \tag{3.26}$$

Le système C est situé dans un espace à quatre dimensions, défini par les états $|c,0\rangle$, $|c,1\rangle$, $|w,1\rangle$ et $|w,2\rangle$. Les états $|c,i\rangle$ représentent les cas où les bits de clé brute d'Alice et Bob sont identiques et où le qutrit envoyé par Alice a été inversé i fois, tandis que, les états $|w,i\rangle$ représentent les cas où les bits de clé brute d'Alice et Bob ne correspondent pas, tout en étant inversés i fois.

Il est possible de réécrire l'état (3.24) sous la forme d'une matrice diagonale, dont les

éléments diagonaux sont des éléments de la forme $\frac{1}{3}\langle e^k_{i,ji}|e^k_{i,ji}\rangle$ pour tous les $|e^k_{i,ji}\rangle$.

$$\begin{aligned}
\rho_{BEC} =& \frac{1}{3}|0\rangle\langle 0|_B \otimes (|e^0_{0,00}\rangle\langle e^0_{0,00}| \otimes |c,0\rangle\langle c,0| + |e^1_{0,00}\rangle\langle e^1_{0,00}| \otimes |w,1\rangle\langle w,1| \\
&+ |e^2_{0,00}\rangle\langle e^2_{0,00}| \otimes |w,1\rangle\langle w,1| + |e^0_{0,10}\rangle\langle e^0_{0,10}| \otimes |c,1\rangle\langle c,1| \\
&+ |e^1_{0,10}\rangle\langle e^1_{0,10}| \otimes |w,2\rangle\langle w,2| + |e^2_{0,10}\rangle\langle e^2_{0,10}| \otimes |w,2\rangle\langle w,2| \\
&+ |e^0_{0,20}\rangle\langle e^0_{0,20}| \otimes |c,1\rangle\langle c,1| + |e^1_{0,20}\rangle\langle e^1_{0,20}| \otimes |w,2\rangle\langle w,2| \\
&+ |e^2_{0,20}\rangle\langle e^2_{0,20}| \otimes |w,2\rangle\langle w,2|) \\
&+ \frac{1}{3}|1\rangle\langle 1|_B \otimes (|e^0_{1,01}\rangle\langle e^0_{1,01}| \otimes |w,2\rangle\langle w,2| + |e^1_{1,01}\rangle\langle e^1_{1,01}| \otimes |c,1\rangle\langle c,1| \\
&+ |e^2_{1,01}\rangle\langle e^2_{1,01}| \otimes |w,2\rangle\langle w,2| + |e^0_{1,11}\rangle\langle e^0_{1,11}| \otimes |w,1\rangle\langle w,1| \\
&+ |e^1_{1,11}\rangle\langle e^1_{1,11}| \otimes |c,0\rangle\langle c,0| + |e^2_{1,11}\rangle\langle e^2_{1,11}| \otimes |w,1\rangle\langle w,1| \\
&+ |e^0_{1,21}\rangle\langle e^0_{1,21}| \otimes |w,2\rangle\langle w,2| + |e^1_{1,21}\rangle\langle e^1_{1,21}| \otimes |c,1\rangle\langle c,1| \\
&+ |e^2_{1,21}\rangle\langle e^2_{1,21}| \otimes |w,2\rangle\langle w,2|) \\
&+ \frac{1}{3}|2\rangle\langle 2|_B \otimes (|e^0_{2,02}\rangle\langle e^0_{2,02}| \otimes |w,2\rangle\langle w,2| + |e^1_{2,02}\rangle\langle e^1_{2,02}| \otimes |w,2\rangle\langle w,2| \\
&+ |e^2_{2,02}\rangle\langle e^2_{2,02}| \otimes |c,1\rangle\langle c,1| + |e^0_{2,12}\rangle\langle e^0_{2,12}| \otimes |w,2\rangle\langle w,2| \\
&+ |e^1_{2,12}\rangle\langle e^1_{2,12}| \otimes |w,2\rangle\langle w,2| + |e^2_{2,12}\rangle\langle e^2_{2,12}| \otimes |c,1\rangle\langle c,1| \\
&+ |e^0_{2,22}\rangle\langle e^0_{2,22}| \otimes |w,1\rangle\langle w,1| + |e^1_{2,22}\rangle\langle e^1_{2,22}| \otimes |w,1\rangle\langle w,1| \\
&+ |e^2_{2,22}\rangle\langle e^2_{2,22}| \otimes |c,0\rangle\langle c,0|).
\end{aligned} \tag{3.27}$$

En effet, Alice et Bob ont la capacité d'estimer la probabilité $p_{i,j,k}$, qui correspond à la probabilité que Alice envoie initialement l'état $|i\rangle$, que Bob le mesure en tant que $|j\rangle$, et qu'ensuite Alice mesure l'état $|k\rangle$ après avoir reçu l'état de Bob. Cette estimation est effectuée en utilisant une méthode itérative pour contribuer à la génération de la clé brute. Les probabilités ainsi obtenues sont utilisées pour estimer les valeurs de $\langle e^a_{b,c}|e^a_{b,c}\rangle$ de la manière suivante

$$\begin{array}{lll}
p_{0,0,0} = \langle e^0_{0,00}|e^0_{0,00}\rangle & p_{1,0,0} = \langle e^0_{0,10}|e^0_{0,10}\rangle & p_{2,0,0} = \langle e^0_{0,20}|e^0_{0,20}\rangle \\
p_{0,0,1} = \langle e^1_{0,00}|e^1_{0,00}\rangle & p_{1,0,1} = \langle e^1_{0,10}|e^1_{0,10}\rangle & p_{2,0,1} = \langle e^1_{0,20}|e^1_{0,20}\rangle \\
p_{0,0,2} = \langle e^2_{0,00}|e^2_{0,00}\rangle & p_{1,0,2} = \langle e^2_{0,10}|e^2_{0,10}\rangle & p_{2,0,2} = \langle e^2_{0,20}|e^2_{0,20}\rangle \\
p_{0,1,0} = \langle e^0_{1,01}|e^0_{1,01}\rangle & p_{1,1,0} = \langle e^0_{1,11}|e^0_{1,11}\rangle & p_{2,1,0} = \langle e^0_{1,21}|e^0_{1,21}\rangle \\
p_{0,1,1} = \langle e^1_{1,01}|e^1_{1,01}\rangle & p_{1,1,1} = \langle e^1_{1,11}|e^1_{1,11}\rangle & p_{2,1,1} = \langle e^1_{1,21}|e^1_{1,21}\rangle \\
p_{0,1,2} = \langle e^2_{1,01}|e^2_{1,01}\rangle & p_{1,1,2} = \langle e^2_{1,11}|e^2_{1,11}\rangle & p_{2,1,2} = \langle e^2_{1,21}|e^2_{1,21}\rangle \\
p_{0,2,0} = \langle e^0_{2,02}|e^0_{2,02}\rangle & p_{1,2,0} = \langle e^0_{2,12}|e^0_{2,12}\rangle & p_{2,2,0} = \langle e^0_{2,22}|e^0_{2,22}\rangle \\
p_{0,2,1} = \langle e^1_{2,02}|e^1_{2,02}\rangle & p_{1,2,1} = \langle e^1_{2,12}|e^1_{2,12}\rangle & p_{2,2,1} = \langle e^1_{2,22}|e^1_{2,22}\rangle \\
p_{0,2,2} = \langle e^2_{2,02}|e^2_{2,02}\rangle & p_{1,2,2} = \langle e^2_{2,12}|e^2_{2,12}\rangle & p_{2,2,2} = \langle e^2_{2,22}|e^2_{2,22}\rangle.
\end{array} \tag{3.28}$$

Étant donné ρ_{BEC}, il est possible de calculer aisément l'entropie conditionnelle de Bob, sachant EC, par le biais de la formule $S(B|EC) = S(BEC) - S(EC)$:

$$S(BEC) = S(\rho_{BEC}) = H(\frac{1}{3}p_{0,0,0}, \frac{1}{3}p_{0,0,1}, ..., \frac{1}{3}p_{2,2,2}), \tag{3.29}$$

De ce fait, le calcul de $S(EC)$ est trivial. En effet, en éliminant l'état de Bob par le biais de l'opération de trace partielle, il est possible d'obtenir l'état ρ_{EC} :

$$\begin{aligned}\rho_{EC} =&(\frac{1}{3}t_1\tilde{\sigma_1}) \otimes |c,0\rangle\langle c,0| + (\frac{1}{3}t_2\tilde{\sigma_2}) \otimes |c,1\rangle\langle c,1| \\ &+ (\frac{1}{3}t_3\tilde{\sigma_3}) \otimes |w,1\rangle\langle w,1| + (\frac{1}{3}t_4\tilde{\sigma_4}) \otimes |w,2\rangle\langle w,2|.\end{aligned} \tag{3.30}$$

Dans cette formulation, les quantités t_1, t_2, t_3 et t_4 sont respectivement les probabilités totales qu'il n'y ait pas d'erreurs dans les deux canaux, qu'il y ait une erreur dans le canal aller, qu'il y ait une erreur dans le canal retour et qu'il y ait une erreur dans les deux canaux. Les opérateurs $\tilde{\sigma_j} = \frac{\sigma_j}{t_j}$ représente la forme normalisée des opérateurs semi-définis positifs σ_j, obtenue par la division de ces opérateurs par $t_j = tr\sigma_j > 0$, définis par l'expression

$$\begin{aligned}
\sigma_1 &= |e^0_{0,00}\rangle\langle e^0_{0,00}| + |e^1_{1,11}\rangle\langle e^1_{1,11}| + |e^2_{2,22}\rangle\langle e^2_{2,22}|, \\
\sigma_2 &= |e^0_{0,10}\rangle\langle e^0_{0,10}| + |e^0_{0,20}\rangle\langle e^0_{0,20}| + |e^1_{1,01}\rangle\langle e^1_{1,01}| + |e^1_{1,21}\rangle\langle e^1_{1,21}| + |e^2_{2,02}\rangle\langle e^2_{2,02}| + |e^2_{2,12}\rangle\langle e^2_{2,12}|, \\
\sigma_3 &= |e^1_{0,00}\rangle\langle e^1_{0,00}| + |e^2_{0,00}\rangle\langle e^2_{0,00}| + |e^0_{1,11}\rangle\langle e^0_{1,11}| + |e^2_{1,11}\rangle\langle e^2_{1,11}| + |e^0_{2,22}\rangle\langle e^0_{2,22}| + |e^1_{2,22}\rangle\langle e^1_{2,22}|, \\
\sigma_4 &= |e^1_{0,10}\rangle\langle e^1_{0,10}| + |e^2_{0,10}\rangle\langle e^2_{0,10}| + |e^1_{0,20}\rangle\langle e^1_{0,20}| + |e^2_{0,20}\rangle\langle e^2_{0,20}| + |e^0_{1,01}\rangle\langle e^0_{1,01}| + |e^2_{1,01}\rangle\langle e^2_{1,01}| \\
&\quad + |e^0_{1,21}\rangle\langle e^0_{1,21}| + |e^2_{1,21}\rangle\langle e^2_{1,21}| + |e^0_{2,02}\rangle\langle e^0_{2,02}| + |e^1_{2,02}\rangle\langle e^1_{2,02}| + |e^0_{2,12}\rangle\langle e^0_{2,12}| + |e^1_{2,12}\rangle\langle e^1_{2,12}|.
\end{aligned}$$

A ce point, en utilisant le Lemme 1, nous pouvons déduire l'expression suivante pour $S(EC)$

$$S(EC) = S(\rho_{EC}) = H(\frac{1}{3}t_1, ..., \frac{1}{3}t_4) + \frac{1}{3}\sum_{j=1}^{4} t_j S(\tilde{\sigma_j}). \tag{3.31}$$

Pour obtenir une borne inférieure sur le taux de clé, il est nécessaire de déterminer une borne supérieure sur $S(EC)$. Cette borne peut être déterminé à l'aide de l'équation (3.31) :

$$\begin{aligned}S(EC) \leq& H\left(\frac{1}{3}t_1, \frac{1}{3}t_2, \frac{1}{3}t_3, \frac{1}{3}t_4\right) \\ &+ \frac{1}{3}(t_2 + t_3 + t_4) + \frac{1}{3}t_1 S(\tilde{\sigma_1}).\end{aligned} \tag{3.32}$$

Il est évident que si le niveau de bruit présent dans le canal quantique est faible, on peut s'attendre à ce que les probabilités $p_{i,j,k}$ soient également faibles, à l'exception

de $p_{0,0,0}$, $p_{1,1,1}$ et $p_{2,2,2}$ qui devraient être élevées. Nous pouvons ainsi obtenir une borne inférieure sur le taux de clé r en trouvant une borne supérieure sur la quantité $S(\tilde{\sigma_1})$.

Soit $\{|a\rangle, |b\rangle, |c\rangle\}$ une base orthonormée pour le système de qutrit considéré, sans perte de généralité, nous pouvons alors exprimer les états du système dans cette nouvelle base en écrivant

$$\begin{aligned} |e^0_{0,00}\rangle &= \chi|a\rangle + \sigma|b\rangle + \rho|c\rangle, \\ |e^1_{1,11}\rangle &= \sqrt{p_{1,1,1}}|c\rangle, \\ |e^2_{2,22}\rangle &= \sqrt{p_{2,2,2}}|c\rangle, \end{aligned} \tag{3.33}$$

où $\langle a|a\rangle = \langle b|b\rangle = \langle c|c\rangle = 1$, $\langle a|b\rangle = \langle b|c\rangle = \langle a|c\rangle = 0$, et $\chi, \sigma, \rho \in \mathbb{C}$. Cela implique en outre que

$$|\chi|^2 + |\sigma|^2 + |\rho|^2 = \langle e^0_{0,00}|e^0_{0,00}\rangle = p_{0,0,0}.$$

L'introduction d'une nouvelle base orthonormée $\{|a\rangle, |b\rangle, |c\rangle\}$ permet d'exprimer $\tilde{\sigma_1}$ sous la forme mathématique suivante

$$\tilde{\sigma_1} = \frac{1}{p_{0,0,0} + p_{1,1,1} + p_{2,2,2}} \begin{bmatrix} |\chi|^2 & \chi\sigma^* & \chi\rho^* \\ \sigma\chi^* & |\sigma|^2 & \sigma\rho^* \\ \rho\chi^* & \rho\sigma^* & p_{1,1,1} + p_{2,2,2} + |\rho|^2 \end{bmatrix}.$$

Après des manipulations algébriques, nous pouvons obtenir les valeurs propres de cette quantité, notées $\tilde{\lambda_0}$, $\tilde{\lambda_1}$ et $\tilde{\lambda_2}$:

$$\tilde{\lambda_0} = 0, \tag{3.34}$$

$$\tilde{\lambda_1} = \frac{1}{2} + \frac{\sqrt{4p + p^2_{0,0,0} - 2p_{0,0,0}p_{1,1,1} + p^2_{1,1,1} - 2p_{0,0,0}p_{2,2,2} - 2p_{1,1,1}p_{2,2,2} + p^2_{2,2,2}}}{2(p_{0,0,0} + p_{1,1,1} + p_{2,2,2})}, \tag{3.35}$$

$$\tilde{\lambda_2} = \frac{1}{2} - \frac{\sqrt{4p + p^2_{0,0,0} - 2p_{0,0,0}p_{1,1,1} + p^2_{1,1,1} - 2p_{0,0,0}p_{2,2,2} - 2p_{1,1,1}p_{2,2,2} + p^2_{2,2,2}}}{2(p_{0,0,0} + p_{1,1,1} + p_{2,2,2})}, \tag{3.36}$$

où $p = \left(|\langle e^0_{0,00}|e^1_{1,11}\rangle|^2 + |\langle e^0_{0,00}|e^2_{2,22}\rangle|^2 + |\langle e^1_{1,11}|e^2_{2,22}\rangle|^2\right)$.

La combinaison de toutes les équations précédentes conduit à la détermination de la borne supérieure suivante pour la quantité $S(EC)$:

$$S(EC) \leq H\left(\frac{1}{3}t_1, \frac{1}{3}t_2, \frac{1}{3}t_3, \frac{1}{3}t_4\right) + \frac{1}{3}(t_2 + t_3 + t_4) + \frac{1}{3}t_1\left(H(\tilde{\lambda_1}) + H(\tilde{\lambda_2})\right). \tag{3.37}$$

L'inégalité ci-dessus montre que les valeurs propres (3.35) et (3.36) dépendent non seulement des valeurs $p_{i,j,k}$, mais également de la quantité p qui ne peut être observée directement, $p = \left(|\langle e^0_{0,00}|e^1_{1,11}\rangle|^2 + |\langle e^0_{0,00}|e^2_{2,22}\rangle|^2 + |\langle e^1_{1,11}|e^2_{2,22}\rangle|^2\right)$.

Par l'intégration de l'ensemble des équations,(3.29),(3.37), la borne de taux de clé (3.26) est déterminée comme étant

$$\begin{aligned} r \geq & H(\frac{1}{3}p_{0,0,0}, \frac{1}{3}p_{0,0,1}, ..., \frac{1}{3}p_{2,2,2}) - H\left(\frac{1}{3}t_1, \frac{1}{3}t_2, \frac{1}{3}t_3, \frac{1}{3}t_4\right) \\ & - \frac{1}{3}(t_2 + t_3 + t_4) - \frac{1}{3}t_1 H(\tilde{\lambda_1}, \tilde{\lambda_2}) - H(B|A), \end{aligned} \tag{3.38}$$

La définition de l'entropie conditionnelle $H(B|A)$ comme étant $H(B, A) - H(A)$ peut s'effectuer de manière aisée. En effet, si l'on considère la probabilité $p(b, a)$ que le trit de Bob soit b alors que celui d'Alice est a, ces probabilités sont déterminée par

$$\begin{aligned} p(0,0) &= \frac{1}{3}(p_{000} + p_{100} + p_{200}) \quad p(0,1) = \frac{2}{3}(p_{001} + p_{101} + p_{201}) \quad p(0,2) = \frac{2}{3}(p_{002} + p_{102} + p_{202}) \\ p(1,0) &= \frac{2}{3}(p_{010} + p_{110} + p_{210}) \quad p(1,1) = \frac{1}{3}(p_{011} + p_{111} + p_{211}) \quad p(1,2) = \frac{2}{3}(p_{012} + p_{112} + p_{212}) \\ p(2,0) &= \frac{2}{3}(p_{020} + p_{120} + p_{220}) \quad p(2,1) = \frac{2}{3}(p_{021} + p_{121} + p_{221}) \quad p(2,2) = \frac{1}{3}(p_{022} + p_{122} + p_{222}) \end{aligned} \tag{3.39}$$

Par ailleurs, en considérant la probabilité $p_A(0)$ que le trit d'Alice soit zéro, ainsi que les probabilités $p_A(1)$ et $p_A(2)$ respectivement associées à la valeur un et deux, nous pouvons alors écrire :

$$\begin{aligned} p_A(0) &= \frac{1}{3}p_{000} + \frac{2}{3}p_{010} + \frac{2}{3}p_{020} + \frac{2}{3}p_{110} + \frac{1}{3}p_{100} + \frac{2}{3}p_{120} + \frac{1}{3}p_{200} + \frac{2}{3}p_{210} + \frac{2}{3}p_{220} \\ p_A(1) &= \frac{2}{3}p_{001} + \frac{1}{3}p_{011} + \frac{2}{3}p_{021} + \frac{2}{3}p_{101} + \frac{1}{3}p_{111} + \frac{2}{3}p_{121} + \frac{2}{3}p_{201} + \frac{1}{3}p_{211} + \frac{2}{3}p_{221} \\ p_A(2) &= \frac{2}{3}p_{002} + \frac{2}{3}p_{012} + \frac{1}{3}p_{022} + \frac{2}{3}p_{102} + \frac{2}{3}p_{112} + \frac{1}{3}p_{122} + \frac{2}{3}p_{202} + \frac{2}{3}p_{212} + \frac{1}{3}p_{222} \end{aligned} \tag{3.40}$$

En rassemblant toutes les équations, la borne supérieure du taux de clé est déterminée selon la définition suivante

$$\begin{aligned} r \geq & H(\frac{1}{3}p_{0,0,0}, \frac{1}{3}p_{0,0,1}, ..., \frac{1}{3}p_{2,2,2}) - H\left(\frac{1}{3}t_1, \frac{1}{3}t_2, \frac{1}{3}t_3, \frac{1}{3}t_4\right) - \frac{1}{3}(t_2 + t_3 + t_4) \\ & - \frac{1}{3}t_1\left(H(\tilde{\lambda_1}) + H(\tilde{\lambda_2})\right) + H(p_A(0), p_A(1), p_A(2)) \\ & - H(p(0,0), p(0,1), p(0,2), p(1,0), p(1,1), p(1,2), p(2,0), p(2,1), p(2,2)). \end{aligned} \tag{3.41}$$

Les $\tilde{\lambda}$ présents dans cette équation sont issus des équations (3.35) et (3.36), ce sont des fonctions dépendant uniquement des paramètres à estimer par Alice et Bob.

Cependant, en utilisant le taux d'erreur dans les différents nombres de bases mutuellement non biaisées, Alice et Bob peuvent déterminer des bornes sur ces quantités. Nous abordons cette dernière en détail dans les sous-sections ci-dessous dans le cas d'un protocole utilisant respectivement deux, trois et quatre bases MUB.

Deux bases mutuellement non biaisées

Nous proposons une variante du protocole de distribution de clés semi-quantique, qui utilise deux ensembles des six états, notés Φ_1 et Φ_2, appartenant respectivement aux bases $\mathcal{A}$,$\mathcal{T}$ et $\mathcal{A}$, $\mathcal{K}$

$$\Phi_1 = \{|0\rangle, |1\rangle, |2\rangle, |0'\rangle, |1'\rangle, |2'\rangle\}, \tag{3.42}$$
$$\Phi_2 = \{|0\rangle, |1\rangle, |2\rangle, |0''\rangle, |1''\rangle, |2''\rangle\}. \tag{3.43}$$

Les vecteurs unitaires $\{|0\rangle, |1\rangle, |2\rangle\}$ forment la base $\mathcal{A}$ dans un espace de Hilbert tridimensionnel. La base $\mathcal{T}$, constituée des vecteurs $\{|0'\rangle, |1'\rangle, |2'\rangle\}$ définie par

$$\begin{aligned} |0'\rangle &= \frac{1}{\sqrt{3}}(e^{\frac{2i\pi}{3}}|0\rangle + |1\rangle + |2\rangle), \\ |1'\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + e^{\frac{2i\pi}{3}}|1\rangle + |2\rangle), \\ |2'\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + e^{\frac{2i\pi}{3}}|2\rangle). \end{aligned} \tag{3.44}$$

De plus, la base $\mathcal{K}$ est définie par les vecteurs $\{|0''\rangle, |1''\rangle, |2''\rangle\}$

$$\begin{aligned} |0''\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), \\ |1''\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + e^{\frac{2i\pi}{3}}|1\rangle + e^{\frac{-2i\pi}{3}}|2\rangle), \\ |2''\rangle &= \frac{1}{\sqrt{3}}(|0\rangle + e^{\frac{-2i\pi}{3}}|1\rangle + e^{\frac{2i\pi}{3}}|2\rangle). \end{aligned} \tag{3.45}$$

Nous avons spécifiquement choisi ces deux ensembles uniques pour comparer l'évaluation de leurs taux de clés.

Estimation du bruit de base $\mathcal{T}$:

Afin d'estimer le niveau de bruit présent dans le canal de communication dans la base $\mathcal{T}$ de manière précise, il est nécessaire de procéder à la détermination d'une borne supérieure pour la quantité $p = \left(|\langle e^0_{0,00}|e^1_{1,11}\rangle|^2 + |\langle e^0_{0,00}|e^2_{2,22}\rangle|^2 + |\langle e^1_{1,11}|e^2_{2,22}\rangle|^2\right)$. Ainsi, en considérant uniquement les itérations où Alice encode son qutrit dans la base $\mathcal{T}$ définie par les vecteurs $|0'\rangle, |1'\rangle, |2'\rangle$ dans l'equation 3.44, tandis que Bob choisisse de réfléchir, et qu'Alice mesure ensuite dans cette même base, une borne supérieure pour p peut être établie avec précision.

Tout d'abord, il convient de remarquer qu'une borne inférieure du produit scalaire est définie comme suit

$$\begin{aligned} |\langle e^0_{0,00}|e^1_{1,11}\rangle|^2 &\geq Re^2(\langle e^0_{0,00}|e^1_{1,11}\rangle), \\ |\langle e^0_{0,00}|e^2_{2,22}\rangle|^2 &\geq Re^2(\langle e^0_{0,00}|e^2_{2,22}\rangle), \\ |\langle e^1_{1,11}|e^2_{2,22}\rangle|^2 &\geq Re^2(\langle e^1_{1,11}|e^2_{2,22}\rangle). \end{aligned}$$

Étant donné que Bob choisit l'opération R, le canal quantique bidirectionnel devient essentiellement un canal unidirectionnel, où Eve attaque à travers l'opérateur unitaire $V = U_R U_F$. Comme précédemment, on suppose, sans perte de généralité, que l'ancilla d'Eve est initialisée à l'état $|0\rangle_E$, ce qui signifie que son action sur les états de base peut être décrite de la manière suivante

$$\begin{aligned} V|0,0\rangle &= U_R(|0,e_{00}\rangle + |1,e_{01}\rangle + |2,e_{02}\rangle) \\ &= |0\rangle \otimes \underbrace{(|e^0_{0,00}\rangle + |e^0_{1,01}\rangle + |e^0_{2,02}\rangle)}_{|f_0\rangle} + |1\rangle \otimes \underbrace{(|e^1_{0,00}\rangle + |e^1_{1,01}\rangle + |e^1_{2,02}\rangle)}_{|f_1\rangle} \\ &\quad + |2\rangle \otimes \underbrace{(|e^2_{0,00}\rangle + |e^2_{1,01}\rangle + |e^2_{2,02}\rangle)}_{|f_2\rangle} \\ &= |0,f_0\rangle + |1,f_1\rangle + |2,f_2\rangle; \end{aligned} \tag{3.46}$$

$$\begin{aligned} V|1,0\rangle &= U_R(|0,e_{10}\rangle + |1,e_{11}\rangle + |2,e_{12}\rangle) \\ &= |0\rangle \otimes (|e^0_{0,10}\rangle + |e^0_{1,4}\rangle + |e^0_{2,12}\rangle) + |1\rangle \otimes (|e^1_{0,10}\rangle + |e^1_{1,4}\rangle + |e^1_{2,12}\rangle) \\ &\quad + |2\rangle \otimes (|e^2_{0,10}\rangle + |e^2_{1,11}\rangle + |e^2_{2,12}\rangle) \\ &= |0,f_3\rangle + |1,f_4\rangle + |2,f_5\rangle; \end{aligned} \tag{3.47}$$

$$\begin{aligned} V|2,0\rangle &= U_R(|0,e_{20}\rangle + |1,e_{21}\rangle + |2,e_{22}\rangle) \\ &= |0\rangle \otimes (|e^0_{0,20}\rangle + |e^0_{1,21}\rangle + |e^0_{2,22}\rangle) + |1\rangle \otimes (|e^1_{0,20}\rangle + |e^1_{1,21}\rangle + |e^1_{2,22}\rangle) \\ &\quad + |2\rangle \otimes (|e^2_{0,20}\rangle + |e^2_{1,21}\rangle + |e^2_{2,22}\rangle) \\ &= |0,f_6\rangle + |1,f_7\rangle + |2,f_8\rangle. \end{aligned} \tag{3.48}$$

Tout d'abord, il est important de souligner que grâce à l'unitarité de U_F et U_R, nous pouvons obtenir

$$\begin{aligned} \langle f_0|f_0\rangle + \langle f_1|f_1\rangle + \langle f_2|f_2\rangle &= \langle f_3|f_3\rangle + \langle f_4|f_4\rangle + \langle f_5|f_5\rangle \\ &= \langle f_6|f_6\rangle + \langle f_7|f_7\rangle + \langle f_8|f_8\rangle = 1, \\ \langle f_0|f_3\rangle + \langle f_1|f_4\rangle + \langle f_2|f_8\rangle &= \langle f_3|f_6\rangle + \langle f_4|f_7\rangle + \langle f_5|f_8\rangle \\ &= \langle f_0|f_6\rangle + \langle f_1|f_7\rangle + \langle f_2|f_8\rangle = 0. \end{aligned} \tag{3.49}$$

En revanche, en exploitant sa linéarité, nous pouvons décrire l'effet de V sur la base $\mathcal{T}$ de la manière suivante :

$$\begin{aligned} V|0',0\rangle &= |0',g_0\rangle + |1',g_1\rangle + |2',g_2\rangle, \\ V|1',0\rangle &= |0',g_3\rangle + |1',g_4\rangle + |2',g_5\rangle, \\ V|2',0\rangle &= |0',g_6\rangle + |1',g_7\rangle + |2',g_8\rangle. \end{aligned} \tag{3.50}$$

Les états $|g_i\rangle$ pour $i = 0, 1, \ldots, 8$ sont des combinaisons linéaires des états $|f_j\rangle$ pour $j = 0, 1, \ldots, 8$ avec des coefficients complexes, qui sont donnés dans les expressions correspondantes pour les états $|g_i\rangle$:

$$
\begin{aligned}
|g_0\rangle &= \frac{1}{3}(|f_0\rangle + e^{\frac{2i\pi}{3}}|f_1\rangle + e^{\frac{2i\pi}{3}}|f_2\rangle + e^{\frac{-2i\pi}{3}}|f_3\rangle + |f_4\rangle + |f_5\rangle + e^{\frac{-2i\pi}{3}}|f_6\rangle + |f_7\rangle + |f_8\rangle)\\
|g_1\rangle &= \frac{1}{3}(e^{\frac{2i\pi}{3}}|f_0\rangle + |f_1\rangle + e^{\frac{2i\pi}{3}}|f_2\rangle + |f_3\rangle + e^{\frac{-2i\pi}{3}}|f_4\rangle + |f_5\rangle + |f_6\rangle + e^{\frac{-2i\pi}{3}}|f_7\rangle + |f_8\rangle)\\
|g_2\rangle &= \frac{1}{3}(e^{\frac{2i\pi}{3}}|f_0\rangle + e^{\frac{2i\pi}{3}}|f_1\rangle + |f_2\rangle + |f_3\rangle + |f_4\rangle + e^{\frac{-2i\pi}{3}}|f_5\rangle + |f_6\rangle + |f_7\rangle + e^{\frac{-2i\pi}{3}}|f_8\rangle)\\
|g_3\rangle &= \frac{1}{3}(e^{\frac{-2i\pi}{3}}|f_0\rangle + |f_1\rangle + |f_2\rangle + |f_3\rangle + e^{\frac{2i\pi}{3}}|f_4\rangle + e^{\frac{2i\pi}{3}}|f_5\rangle + e^{\frac{-2i\pi}{3}}|f_6\rangle + |f_7\rangle + |f_8\rangle)\\
|g_4\rangle &= \frac{1}{3}(|f_0\rangle + e^{\frac{-2i\pi}{3}}|f_1\rangle + |f_2\rangle + e^{\frac{2i\pi}{3}}|f_3\rangle + |f_4\rangle + e^{\frac{2i\pi}{3}}|f_5\rangle + |f_6\rangle + e^{\frac{-2i\pi}{3}}|f_7\rangle + |f_8\rangle)\\
|g_5\rangle &= \frac{1}{3}(|f_0\rangle + |f_1\rangle + e^{\frac{-2i\pi}{3}}|f_2\rangle + e^{\frac{2i\pi}{3}}|f_3\rangle + e^{\frac{2i\pi}{3}}|f_4\rangle + |f_5\rangle + |f_6\rangle + |f_7\rangle + e^{\frac{-2i\pi}{3}}|f_8\rangle)\\
|g_6\rangle &= \frac{1}{3}(e^{\frac{-2i\pi}{3}}|f_0\rangle + |f_1\rangle + |f_2\rangle + e^{\frac{-2i\pi}{3}}|f_3\rangle + |f_4\rangle + |f_5\rangle + |f_6\rangle + e^{\frac{2i\pi}{3}}|f_7\rangle + e^{\frac{2i\pi}{3}}|f_8\rangle)\\
|g_7\rangle &= \frac{1}{3}(|f_0\rangle + e^{\frac{-2i\pi}{3}}|f_1\rangle + |f_2\rangle + |f_3\rangle + e^{\frac{-2i\pi}{3}}|f_4\rangle + |f_5\rangle + e^{\frac{2i\pi}{3}}|f_6\rangle + |f_7\rangle + e^{\frac{2i\pi}{3}}|f_8\rangle)\\
|g_8\rangle &= \frac{1}{3}(|f_0\rangle + |f_1\rangle + e^{\frac{-2i\pi}{3}}|f_2\rangle + |f_3\rangle + |f_4\rangle + e^{\frac{-2i\pi}{3}}|f_5\rangle + e^{\frac{2i\pi}{3}}|f_6\rangle + e^{\frac{2i\pi}{3}}|f_7\rangle + |f_8\rangle)
\end{aligned}
\tag{3.51}
$$

Dans le formalisme mathématique utilisé, la mesure de l'état $|1'\rangle$ par Alice lorsqu'elle a initialement envoyé $|0'\rangle$ est représentée par $\langle g_1|g_1\rangle$, tandis que la mesure de $|2'\rangle$ par Alice lorsqu'elle a initialement envoyé $|0'\rangle$ est représentée par $\langle g_2|g_2\rangle$. $\langle g_3|g_3\rangle$, $\langle g_5|g_5\rangle$, $\langle g_6|g_6\rangle$ et $\langle g_7|g_7\rangle$ peuvent être définies de manière similaire en utilisant les résultats de mesure pour différentes combinaisons d'états initiaux et finaux.

Soient les probabilités de transition $p_{0'1'}$, $p_{0'2'}$, $p_{1'0'}$, $p_{1'2'}$, $p_{2'0'}$ et $p_{2'1'}$, qui représentent respectivement les probabilités de mesure des différentes combinaisons d'états $\langle g_1|g_1\rangle$, $\langle g_2|g_2\rangle$, $\langle g_3|g_3\rangle$, $\langle g_5|g_5\rangle$, $\langle g_6|g_6\rangle$ et $\langle g_7|g_7\rangle$, nous avons alors

$$
\begin{aligned}
p_{0'1'} =& \langle g_1|g_1\rangle\\
=& \frac{1}{3} + \frac{1}{9}Re(\langle f_3|f_1\rangle + \langle f_5|f_1\rangle + \langle f_6|f_1\rangle + \langle f_8|f_1\rangle + \langle f_1|f_3\rangle + \langle f_5|f_3\rangle\\
&\quad + \langle f_8|f_3\rangle + \langle f_1|f_5\rangle + \langle f_3|f_5\rangle + \langle f_6|f_5\rangle + \langle f_1|f_6\rangle + \langle f_5|f_6\rangle\\
&\quad + \langle f_8|f_6\rangle + \langle f_1|f_8\rangle + \langle f_3|f_8\rangle + \langle f_6|f_8\rangle + \langle f_2|f_0\rangle + \langle f_0|f_2\rangle)\\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}}Re(\langle f_0|f_1\rangle + \langle f_2|f_1\rangle + \langle f_2|f_3\rangle + \langle f_0|f_5\rangle + \langle f_2|f_6\rangle + \langle f_0|f_8\rangle\\
&\quad + \langle f_4|f_0\rangle + \langle f_7|f_0\rangle + \langle f_4 f_2\rangle + \langle f_7|f_2\rangle + \langle f_3|f_4\rangle + \langle f_5|f_4\rangle\\
&\quad + \langle f_6|f_4\rangle + \langle f_8|f_4\rangle + \langle f_3|f_7\rangle + \langle f_5|f_7\rangle + \langle f_6|f_7\rangle + \langle f_8|f_7\rangle)\\
&+ \frac{1}{9}e^{\frac{2i\pi}{3}}Re(\langle f_4|f_3\rangle + \langle f_7|f_3\rangle + \langle f_4|f_5\rangle + \langle f_7|f_5\rangle + \langle f_4|f_6\rangle + \langle f_7|f_6\rangle\\
&\quad + \langle f_4|f_8\rangle + \langle f_7|f_8\rangle + \langle f_1|f_0\rangle + \langle f_5|f_0\rangle + \langle f_8|f_0\rangle + \langle f_1|f_2\rangle\\
&\quad + \langle f_3|f_2\rangle + \langle f_6|f_2\rangle + \langle f_0|f_4\rangle + \langle f_2|f_4\rangle + \langle f_0|f_7\rangle + \langle f_2|f_7\rangle)
\end{aligned}
\tag{3.52}
$$

$$
\begin{aligned}
p_{0'2'} =& \langle g_2|g_2\rangle \\
=& \frac{1}{3} + \frac{1}{9}Re(\langle f_1|f_0\rangle + \langle f_0|f_1\rangle + \langle f_3|f_2\rangle + \langle f_4|f_2\rangle + \langle f_6|f_2\rangle + \langle f_7|f_2\rangle \\
&\quad + \langle f_2|f_3\rangle + \langle f_4|f_3\rangle + \langle f_7|f_3\rangle + \langle f_2|f_4\rangle + \langle f_3|f_4\rangle + \langle f_6|f_4\rangle \\
&\quad + \langle f_2|f_6\rangle + \langle f_4|f_6\rangle + \langle f_7|f_6\rangle + \langle f_2|f_7\rangle + \langle f_3|f_7\rangle + \langle f_6|f_7\rangle) \\
&+ \frac{1}{9}e^{\frac{2i\pi}{3}}Re(\langle f_2|f_0\rangle + \langle f_4|f_0\rangle + \langle f_7|f_0\rangle + \langle f_2|f_1\rangle + \langle f_3|f_1\rangle + \langle f_6|f_1\rangle \\
&\quad + \langle f_5|f_3\rangle + \langle f_8|f_3\rangle + \langle f_5|f_4\rangle + \langle f_8|f_4\rangle + \langle f_0|f_5\rangle + \langle f_1|f_5\rangle \\
&\quad + \langle f_5|f_6\rangle + \langle f_8|f_6\rangle + \langle f_5|f_7\rangle + \langle f_8|f_7\rangle + \langle f_0|f_8\rangle + \langle f_1|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}}Re(\langle f_5|f_0\rangle + \langle f_8|f_0\rangle + \langle f_5|f_1\rangle + \langle f_8|f_1\rangle + \langle f_0|f_2\rangle + \langle f_1|f_2\rangle \\
&\quad + \langle f_1|f_3\rangle + \langle f_0|f_4\rangle + \langle f_3|f_5\rangle + \langle f_4|f_5\rangle + \langle f_6|f_5\rangle + \langle f_7|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_0|f_7\rangle + \langle f_3|f_8\rangle + \langle f_4|f_8\rangle + \langle f_6|f_8\rangle + \langle f_7|f_8\rangle)
\end{aligned}
\tag{3.53}
$$

$$
\begin{aligned}
p_{1'0'} =& \langle g_3|g_3\rangle \\
=& \frac{1}{3} + \frac{1}{9}Re(\langle f_2|f_1\rangle + \langle f_3|f_1\rangle + \langle f_8|f_1\rangle + \langle f_1|f_2\rangle + \langle f_3|f_2\rangle + \langle f_7|f_2\rangle \\
&\quad + \langle f_1|f_3\rangle + \langle f_2|f_3\rangle + \langle f_7|f_3\rangle + \langle f_8|f_3\rangle + \langle f_5|f_4\rangle + \langle f_4|f_5\rangle \\
&\quad + \langle f_2|f_7\rangle + \langle f_3|f_7\rangle + \langle f_8|f_7\rangle + \langle f_1|f_8\rangle + \langle f_3|f_8\rangle + \langle f_7|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}}Re(\langle f_1|f_0\rangle + \langle f_2|f_0\rangle + \langle f_7|f_0\rangle + \langle f_8|f_0\rangle + \langle f_5|f_1\rangle + \langle f_4|f_2\rangle \\
&\quad + \langle f_4|f_3\rangle + \langle f_5|f_3\rangle + \langle f_0|f_4\rangle + \langle f_6|f_4\rangle + \langle f_0|f_5\rangle + \langle f_6|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_2|f_6\rangle + \langle f_7|f_6\rangle + \langle f_8|f_6\rangle + \langle f_5|f_7\rangle + \langle f_4|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{2i\pi}{3}}Re(\langle f_4|f_0\rangle + \langle f_5|f_0\rangle + \langle f_0|f_1\rangle + \langle f_6|f_1\rangle + \langle f_0|f_2\rangle + \langle f_6|f_2\rangle \\
&\quad + \langle f_2|f_4\rangle + \langle f_3|f_4\rangle + \langle f_8|f_4\rangle + \langle f_1|f_5\rangle + \langle f_3|f_5\rangle + \langle f_7|f_5\rangle \\
&\quad + \langle f_4|f_6\rangle + \langle f_5|f_6\rangle + \langle f_0|f_7\rangle + \langle f_6|f_7\rangle + \langle f_0|f_8\rangle + \langle f_6|f_8\rangle)
\end{aligned}
\tag{3.54}
$$

$$
\begin{aligned}
p_{1'2'} =& \langle g_5|g_5\rangle \\
=& \frac{1}{3} + \frac{1}{9}Re(\langle f_1|f_0\rangle + \langle f_5|f_0\rangle + \langle f_7|f_0\rangle + \langle f_0|f_1\rangle + \langle f_5|f_1\rangle + \langle f_6|f_1\rangle \\
&\quad + \langle f_4|f_3\rangle + \langle f_3|f_4\rangle + \langle f_0|f_5\rangle + \langle f_1|f_5\rangle + \langle f_6|f_5\rangle + \langle f_7|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_5|f_6\rangle + \langle f_7|f_6\rangle + \langle f_0|f_7\rangle + \langle f_5|f_7\rangle + \langle f_6|f_7\rangle) \\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}}Re(\langle f_4|f_0\rangle + \langle f_3|f_1\rangle + \langle f_0|f_2\rangle + \langle f_1|f_2\rangle + \langle f_6|f_2\rangle + \langle f_7|f_2\rangle \\
&\quad + \langle f_2|f_3\rangle + \langle f_8|f_3\rangle + \langle f_2|f_4\rangle + \langle f_8|f_4\rangle + \langle f_3|f_5\rangle + \langle f_4|f_5\rangle \\
&\quad + \langle f_4|f_6\rangle + \langle f_3|f_7\rangle + \langle f_0|f_8\rangle + \langle f_1|f_8\rangle + \langle f_6|f_8\rangle + \langle f_7|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{2i\pi}{3}}Re(\langle f_2|f_0\rangle + \langle f_8|f_0\rangle + \langle f_2|f_1\rangle + \langle f_8|f_1\rangle + \langle f_3|f_2\rangle + \langle f_4|f_2\rangle \\
&\quad + \langle f_1|f_3\rangle + \langle f_5|f_3\rangle + \langle f_7|f_3\rangle + \langle f_0|f_4\rangle + \langle f_5|f_4\rangle + \langle f_6|f_4\rangle \\
&\quad + \langle f_2|f_6\rangle + \langle f_8|f_6\rangle + \langle f_2|f_7\rangle + \langle f_8|f_7\rangle + \langle f_3|f_8\rangle + \langle f_4|f_8\rangle)
\end{aligned}
\tag{3.55}
$$

$$
\begin{aligned}
p_{2'0'} =& \langle g_6|g_6\rangle \\
=& \frac{1}{3} + \frac{1}{9} Re(\langle f_2|f_1\rangle + \langle f_5|f_1\rangle + \langle f_6|f_1\rangle + \langle f_1|f_2\rangle + \langle f_4|f_2\rangle + \langle f_6|f_2\rangle \\
&\quad + \langle f_2|f_4\rangle + \langle f_5|f_4\rangle + \langle f_6|f_4\rangle + \langle f_1|f_5\rangle + \langle f_4|f_5\rangle + \langle f_6|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_2|f_6\rangle + \langle f_4|f_6\rangle + \langle f_5|f_6\rangle + \langle f_8|f_7\rangle + \langle f_7|f_8\rangle) \\
&+ \frac{1}{9} e^{\frac{-2i\pi}{3}} Re(\langle f_1|f_0\rangle + \langle f_2|f_0\rangle + \langle f_4|f_0\rangle + \langle f_5|f_0\rangle + \langle f_8|f_1\rangle + \langle f_7|f_2\rangle \\
&\quad + \langle f_1|f_3\rangle + \langle f_2|f_3\rangle + \langle f_4|f_3\rangle + \langle f_5|f_3\rangle + \langle f_8|f_4\rangle + \langle f_7|f_5\rangle \\
&\quad + \langle f_7|f_6\rangle + \langle f_8|f_6\rangle + \langle f_0|f_7\rangle + \langle f_3|f_7\rangle + \langle f_0|f_8\rangle + \langle f_3|f_8\rangle) \\
&+ \frac{1}{9} e^{\frac{-2i\pi}{3}} Re(\langle f_7|f_0\rangle + \langle f_8|f_0\rangle + \langle f_0|f_1\rangle + \langle f_3|f_1\rangle + \langle f_0|f_2\rangle + \langle f_3|f_2\rangle \\
&\quad + \langle f_7|f_3\rangle + \langle f_8|f_3\rangle + \langle f_0|f_4\rangle + \langle f_3|f_4\rangle + \langle f_0|f_5\rangle + \langle f_3|f_5\rangle \\
&\quad + \langle f_0|f_6\rangle + \langle f_1|f_7\rangle + \langle f_2|f_7\rangle + \langle f_5|f_7\rangle + \langle f_6|f_7\rangle + \langle f_1|f_8\rangle \\
&\quad + \langle f_2|f_8\rangle + \langle f_4|f_8\rangle + \langle f_6|f_8\rangle)
\end{aligned}
\tag{3.56}
$$

$$
\begin{aligned}
p_{2'1'} =& \langle g_7|g_7\rangle \\
=& \frac{1}{3} + \frac{1}{9} Re(\langle f_2|f_0\rangle + \langle f_5|f_0\rangle + \langle f_7|f_0\rangle + \langle f_0|f_2\rangle + \langle f_3|f_2\rangle + \langle f_7|f_2\rangle \\
&\quad + \langle f_0|f_3\rangle + \langle f_2|f_3\rangle + \langle f_5|f_3\rangle + \langle f_7|f_3\rangle + \langle f_1|f_4\rangle + \langle f_0|f_5\rangle \\
&\quad + \langle f_2|f_5\rangle + \langle f_3|f_5\rangle + \langle f_7|f_5\rangle + \langle f_8|f_6\rangle + \langle f_0|f_7\rangle + \langle f_2|f_7\rangle \\
&\quad + \langle f_3|f_7\rangle + \langle f_5|f_7\rangle + \langle f_6|f_8\rangle) \\
&+ \frac{1}{9} e^{\frac{-2i\pi}{3}} Re(\langle f_8|f_0\rangle + \langle f_0|f_1\rangle + \langle f_2|f_1\rangle + \langle f_3|f_1\rangle + \langle f_5|f_1\rangle + \langle f_6|f_2\rangle \\
&\quad + \langle f_8|f_3\rangle + \langle f_0|f_4\rangle + \langle f_2|f_4\rangle + \langle f_3|f_4\rangle + \langle f_5|f_4\rangle + \langle f_6|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_4|f_6\rangle + \langle f_6|f_7\rangle + \langle f_8|f_7\rangle + \langle f_1|f_8\rangle + \langle f_4|f_8\rangle) \\
&+ \frac{1}{9} e^{\frac{-2i\pi}{3}} Re(\langle f_1|f_0\rangle + \langle f_4|f_0\rangle + \langle f_6|f_1\rangle + \langle f_8|f_1\rangle + \langle f_1|f_2\rangle + \langle f_4|f_2\rangle \\
&\quad + \langle f_1|f_3\rangle + \langle f_4|f_3\rangle + \langle f_6|f_4\rangle + \langle f_8|f_4\rangle + \langle f_1|f_5\rangle + \langle f_4|f_5\rangle \\
&\quad + \langle f_2|f_6\rangle + \langle f_5|f_6\rangle + \langle f_7|f_6\rangle + \langle f_0|f_8\rangle + \langle f_3|f_8\rangle + \langle f_7|f_8\rangle)
\end{aligned}
\tag{3.57}
$$

Ces quantités, qui seront évaluées par Alice lors de l'étape d'estimation des paramètres, représentent l'erreur engendrée par l'attaque d'Eve dans la base $\mathcal{T}$.

En additionnant ces expressions et en les développant, nous obtenons une équation pour la partie réelle de h_e. En résolvant cette équation, nous obtenons une expression pour cette quantité :

$$
\begin{aligned}
X_{\phi_1} \geq 3 &- \frac{3}{2}(p_{0'1'} + p_{0'2'} + p_{1'0'} + p_{1'2'} + p_{2'0'} + p_{2'1'}) \\
&+ \frac{1}{2}(\langle f_5|f_1\rangle + \langle f_7|f_2\rangle + \langle f_2|f_3\rangle + \langle f_6|f_5\rangle + \langle f_1|f_6\rangle + \langle f_3|f_7\rangle).
\end{aligned}
\tag{3.58}
$$

En utilisant l'inégalité de Cauchy-Schwarz et des manipulations algébriques, on peut montrer que la quantité $X_{\phi_1} = Re(\langle e^0_{0,00}|e^1_{1,11}\rangle) + Re(\langle e^0_{0,00}|e^2_{2,22}\rangle) + Re(\langle e^1_{1,11}|e^2_{2,22}\rangle)$ peut être bornée comme suit :

$$
\begin{aligned}
X_{\phi_1} \geq 3 &- \frac{3}{2}(p_{0'1'} + p_{0'2'} + p_{1'0'} + p_{1'2'} + p_{2'0'} + p_{2'1'}) \\
&+ \frac{1}{2}(\sqrt{p_{001}p_{102}} + \sqrt{p_{011}p_{102}} + \sqrt{p_{021}p_{102}} + \sqrt{p_{001}p_{112}} + \sqrt{p_{011}p_{112}} \\
&+ \sqrt{p_{021}p_{112}} + \sqrt{p_{001}p_{122}} + \sqrt{p_{011}p_{122}} + \sqrt{p_{021}p_{122}} + \sqrt{p_{001}p_{200}} \\
&+ \sqrt{p_{011}p_{200}} + \sqrt{p_{021}p_{200}} + \sqrt{p_{001}p_{210}} + \sqrt{p_{011}p_{210}} + \sqrt{p_{021}p_{210}} \\
&+ \sqrt{p_{001}p_{220}} + \sqrt{p_{011}p_{220}} + \sqrt{p_{021}p_{220}} + \sqrt{p_{002}p_{100}} + \sqrt{p_{012}p_{100}} \\
&+ \sqrt{p_{022}p_{100}} + \sqrt{p_{002}p_{110}} + \sqrt{p_{012}p_{110}} + \sqrt{p_{022}p_{110}} + \sqrt{p_{002}p_{120}} \\
&+ \sqrt{p_{012}p_{120}} + \sqrt{p_{022}p_{120}} + \sqrt{p_{002}p_{201}} + \sqrt{p_{012}p_{201}} + \sqrt{p_{022}p_{201}} \\
&+ \sqrt{p_{002}p_{211}} + \sqrt{p_{012}p_{211}} + \sqrt{p_{022}p_{211}} + \sqrt{p_{002}p_{221}} + \sqrt{p_{012}p_{221}} \\
&+ \sqrt{p_{022}p_{221}} + \sqrt{p_{100}p_{201}} + \sqrt{p_{110}p_{201}} + \sqrt{p_{120}p_{201}} + \sqrt{p_{100}p_{211}} \\
&+ \sqrt{p_{110}p_{211}} + \sqrt{p_{120}p_{211}} + \sqrt{p_{100}p_{221}} + \sqrt{p_{110}p_{221}} + \sqrt{p_{120}p_{221}} \\
&+ \sqrt{p_{102}p_{200}} + \sqrt{p_{112}p_{200}} + \sqrt{p_{122}p_{200}} + \sqrt{p_{102}p_{210}} + \sqrt{p_{112}p_{210}} \\
&+ \sqrt{p_{122}p_{210}} + \sqrt{p_{102}p_{220}} + \sqrt{p_{112}p_{220}} + \sqrt{p_{122}p_{220}}) \\
&- (\sqrt{p_{000}p_{101}} + \sqrt{p_{010}p_{101}} + \sqrt{p_{020}p_{101}} + \sqrt{p_{010}p_{111}} + \sqrt{p_{020}p_{111}} \\
&+ \sqrt{p_{000}p_{121}} + \sqrt{p_{010}p_{121}} + \sqrt{p_{020}p_{121}} + \sqrt{p_{000}p_{202}} + \sqrt{p_{010}p_{202}} \\
&+ \sqrt{p_{020}p_{202}} + \sqrt{p_{000}p_{212}} + \sqrt{p_{010}p_{212}} + \sqrt{p_{020}p_{212}} + \sqrt{p_{010}p_{222}} \\
&+ \sqrt{p_{020}p_{222}} + \sqrt{p_{101}p_{202}} + \sqrt{p_{111}p_{202}} + \sqrt{p_{121}p_{202}} + \sqrt{p_{101}p_{212}} \\
&+ \sqrt{p_{111}p_{212}} + \sqrt{p_{121}p_{212}} + \sqrt{p_{101}p_{222}} + \sqrt{p_{121}p_{222}}).
\end{aligned}
\tag{3.59}
$$

En remarquant que $X_{\phi_1} = Re(\langle e^0_{0,00}|e^1_{1,11}\rangle) + Re(\langle e^0_{0,00}|e^2_{2,22}\rangle) + Re(\langle e^1_{1,11}|e^2_{2,22}\rangle)$, le terme de droite de l'équation 3.59, dénommé S, est supposé être non négatif, ce qui devrait être le cas si le niveau de bruit est suffisamment faible. Plus précisément, soit :

$$
\mathcal{S} = \begin{cases} X^2_{\phi_1} & \text{if } X_{\phi_1} \geq 0 \\ 0 & Sinon \end{cases}, \tag{3.60}
$$

où

$$
X_{\phi_1} = Re(\langle e^0_{0,00}|e^1_{1,11}\rangle) + Re(\langle e^0_{0,00}|e^2_{2,22}\rangle) + Re(\langle e^1_{1,11}|e^2_{2,22}\rangle), \tag{3.61}
$$

En conséquence, de la discussion précédente, il est clair que $X_{\phi_1} = |\langle e^0_{0,00}|e^1_{1,11}\rangle + \langle e^0_{0,00}|e^2_{2,22}\rangle + \langle e^1_{1,11}|e^2_{2,22}\rangle|^2 \geq \mathcal{S}$, en notant que X_{ϕ_1} est toujours non négatif, ce qui suggère de limiter la valeur de $\mathcal{S}$ à zéro si elle est négative. En utilisant cette propriété, ainsi que les équation (3.35) et (3.36) et la discussion qui la précède immédiatement, nous pouvons borner supérieurement l'entropie de von Neumann $S(EC)$ et, par conséquent, trouver une borne inférieure sur l'entropie conditionnelle $S(B|EC)$, comme indiqué dans (3.25).

Estimation du bruit de base $\mathcal{K}$:

Lorsque Alice dispose de l'ensemble Φ_2 comme choix d'états, il est possible d'estimer le bruit présent dans la base $\mathcal{K}$ en suivant une procédure analogue à celle exposée dans la section précédente. Ainsi, la quantité $p = |\langle e^0_{0,00}|e^1_{1,11}\rangle|^2 + |\langle e^0_{0,00}|e^2_{2,22}\rangle|^2 + |\langle e^1_{1,11}|e^2_{2,22}\rangle|^2$

peut être bornée en considérant les itérations où Alice prépare et mesure initialement dans la base $\mathcal{K}$, tandis que Bob choisit de réfléchir le qutrit. Dans de telles circonstances, l'opération de Bob se réduit à l'opérateur identité, tandis que l'opération d'Eve est représentée par l'opérateur unitaire V qui est le produit de deux autres opérations unitaires, U_R et U_F tels que décrits dans les équations (3.79) et (3.80).

Les effets de l'action d'Eve sur les états de base $\mathcal{K}$ peuvent être exprimés mathématiquement à l'aide d'équations analogues à celles présentées dans les équations (3.46-3.48), en prenant en compte que l'ancilla associée à Eve est initialisée à l'état $|0\rangle_E$ au commencement du processus :

$$\begin{aligned} V|0'',0\rangle &= |0'',h_0\rangle + |1'',h_1\rangle + |2'',h_2\rangle, \\ V|1'',0\rangle &= |0'',h_3\rangle + |1'',h_4\rangle + |2'',h_5\rangle, \\ V|2'',0\rangle &= |0'',h_6\rangle + |1'',h_7\rangle + |2'',h_8\rangle, \end{aligned} \tag{3.62}$$

où

$$\begin{aligned} |h_1\rangle &= \frac{1}{3}(|f_0\rangle + e^{\frac{-2i\pi}{3}}|f_1\rangle + e^{\frac{2i\pi}{3}}|f_2\rangle + |f_3\rangle + e^{\frac{-2i\pi}{3}}|f_4\rangle + e^{\frac{2i\pi}{3}}|f_5\rangle + |f_6\rangle + e^{\frac{-2i\pi}{3}}|f_7\rangle + e^{\frac{2i\pi}{3}}|f_8\rangle) \\ |h_2\rangle &= \frac{1}{3}(|f_0\rangle + e^{\frac{2i\pi}{3}}|f_1\rangle + e^{\frac{-2i\pi}{3}}|f_2\rangle + |f_3\rangle + e^{\frac{2i\pi}{3}}|f_4\rangle + e^{\frac{-2i\pi}{3}}|f_5\rangle + |f_6\rangle + e^{\frac{2i\pi}{3}}|f_7\rangle + e^{\frac{-2i\pi}{3}}|f_8\rangle) \\ |h_3\rangle &= \frac{1}{3}(|f_0\rangle + |f_1\rangle + |f_2\rangle + e^{\frac{2i\pi}{3}}|f_3\rangle + e^{\frac{2i\pi}{3}}|f_4\rangle + e^{\frac{2i\pi}{3}}|f_5\rangle + e^{\frac{-2i\pi}{3}}|f_6\rangle + e^{\frac{-2i\pi}{3}}|f_7\rangle + e^{\frac{-2i\pi}{3}}|f_8\rangle) \\ |h_5\rangle &= \frac{1}{3}(|f_0\rangle + e^{\frac{2i\pi}{3}}|f_1\rangle + e^{\frac{-2i\pi}{3}}|f_2\rangle + e^{\frac{2i\pi}{3}}|f_3\rangle + e^{\frac{-2i\pi}{3}}|f_4\rangle + |f_5\rangle + e^{\frac{-2i\pi}{3}}|f_6\rangle + |f_7\rangle + e^{\frac{2i\pi}{3}}|f_8\rangle) \\ |h_6\rangle &= \frac{1}{3}(|f_0\rangle + |f_1\rangle + |f_2\rangle + e^{\frac{-2i\pi}{3}}|f_3\rangle + e^{\frac{-2i\pi}{3}}|f_4\rangle + e^{\frac{-2i\pi}{3}}|f_5\rangle + e^{\frac{2i\pi}{3}}|f_6\rangle + e^{\frac{2i\pi}{3}}|f_7\rangle + e^{\frac{2i\pi}{3}}|f_8\rangle) \\ |h_7\rangle &= \frac{1}{3}(|f_0\rangle + e^{\frac{-2i\pi}{3}}|f_1\rangle + e^{\frac{2i\pi}{3}}|f_2\rangle + e^{\frac{-2i\pi}{3}}|f_3\rangle + e^{\frac{2i\pi}{3}}|f_4\rangle + |f_5\rangle + e^{\frac{2i\pi}{3}}|f_6\rangle + |f_7\rangle + e^{\frac{-2i\pi}{3}}|f_8\rangle) \end{aligned} \tag{3.63}$$

Dans la suite de nos calculs, les états $|h_0\rangle$, $|h_4\rangle$ et $|h_8\rangle$ ne sont pas pertinents, raison pour laquelle ils ont été omis.

Dans la même lignée que dans la sous-section précédente, nous introduisons les probabilités $p_{i''j''}$ pour $\{i'',j''\} = \{0'',1'',2''\}$, la probabilité qu'Alice mesure le qutrit renvoyé dans l'état $|j''\rangle$ lorsqu'elle l'a initialement préparé dans l'état $|i''\rangle$.

Les équations (A.1-A.6) présentées dans l'appendice A fournissent les expressions analytiques de ces probabilités.

Après avoir effectué les mêmes manipulations algébriques que précédemment, il en découle de l'inégalité de Cauchy que la quantité $X_{\phi_2} = Re(\langle e^0_{0,00}|e^1_{1,11}\rangle) + Re(\langle e^0_{0,00}|e^2_{2,22}\rangle) + Re(\langle e^1_{1,11}|e^2_{2,22}\rangle)$ est bornée de la manière suivante

$$
\begin{aligned}
X_{\phi_2} \geq 3 - \frac{3}{2}(&p_{0''1''} + p_{0''2''} + p_{1''0''} + p_{1''2''} + p_{2''0''} + p_{2''1''} \\
&- (\sqrt{p_{001}p_{102}} + \sqrt{p_{011}p_{102}} + \sqrt{p_{021}p_{102}} + \sqrt{p_{001}p_{112}} + \sqrt{p_{011}p_{112}} \\
&+ \sqrt{p_{021}p_{112}} + \sqrt{p_{001}p_{122}} + \sqrt{p_{011}p_{122}} + \sqrt{p_{021}p_{122}} + \sqrt{p_{001}p_{200}} \\
&+ \sqrt{p_{011}p_{200}} + \sqrt{p_{021}p_{200}} + \sqrt{p_{001}p_{210}} + \sqrt{p_{011}p_{210}} + \sqrt{p_{021}p_{210}} \\
&+ \sqrt{p_{001}p_{220}} + \sqrt{p_{011}p_{220}} + \sqrt{p_{021}p_{220}} + \sqrt{p_{002}p_{100}} + \sqrt{p_{012}p_{100}} \\
&+ \sqrt{p_{022}p_{100}} + \sqrt{p_{002}p_{110}} + \sqrt{p_{012}p_{110}} + \sqrt{p_{022}p_{110}} + \sqrt{p_{002}p_{120}} \\
&+ \sqrt{p_{012}p_{120}} + \sqrt{p_{022}p_{120}} + \sqrt{p_{002}p_{201}} + \sqrt{p_{012}p_{201}} + \sqrt{p_{022}p_{201}} \\
&+ \sqrt{p_{002}p_{211}} + \sqrt{p_{012}p_{211}} + \sqrt{p_{022}p_{211}} + \sqrt{p_{002}p_{221}} + \sqrt{p_{012}p_{221}} \\
&+ \sqrt{p_{022}p_{221}} + \sqrt{p_{100}p_{201}} + \sqrt{p_{110}p_{201}} + \sqrt{p_{120}p_{201}} + \sqrt{p_{100}p_{211}} \\
&+ \sqrt{p_{110}p_{211}} + \sqrt{p_{120}p_{211}} + \sqrt{p_{100}p_{221}} + \sqrt{p_{110}p_{221}} + \sqrt{p_{120}p_{221}} \\
&+ \sqrt{p_{102}p_{200}} + \sqrt{p_{112}p_{200}} + \sqrt{p_{122}p_{200}} + \sqrt{p_{102}p_{210}} + \sqrt{p_{112}p_{210}} \\
&+ \sqrt{p_{122}p_{210}} + \sqrt{p_{102}p_{220}} + \sqrt{p_{112}p_{220}} + \sqrt{p_{122}p_{220}}) \\
&- (\sqrt{p_{000}p_{101}} + \sqrt{p_{010}p_{101}} + \sqrt{p_{020}p_{101}} + \sqrt{p_{010}p_{111}} + \sqrt{p_{020}p_{111}} \\
&+ \sqrt{p_{000}p_{121}} + \sqrt{p_{010}p_{121}} + \sqrt{p_{020}p_{121}} + \sqrt{p_{000}p_{202}} + \sqrt{p_{010}p_{202}} \\
&+ \sqrt{p_{020}p_{202}} + \sqrt{p_{000}p_{212}}\sqrt{p_{010}p_{212}} + \sqrt{p_{020}p_{212}} + \sqrt{p_{010}p_{222}} \\
&+ \sqrt{p_{020}p_{222}} + \sqrt{p_{101}p_{202}} + \sqrt{p_{111}p_{202}} + \sqrt{p_{121}p_{202}} + \sqrt{p_{101}p_{212}} \\
&+ \sqrt{p_{111}p_{212}} + \sqrt{p_{121}p_{212}} + \sqrt{p_{101}p_{222}} + \sqrt{p_{121}p_{222}})
\end{aligned}
\tag{3.64}
$$

Étant donné l'argument précédemment utilisé, il est envisageable d'introduire une notation adéquate à ce protocole :

$$
\mathcal{S} = \begin{cases} X_{\phi_2}^2 & \text{if } X_{\phi_2} \geq 0 \\ 0 & Sinon \end{cases}, \tag{3.65}
$$

avec

$$
X_{\phi_2} = Re(\langle e^0_{0,00} | e^1_{1,11} \rangle) + Re(\langle e^0_{0,00} | e^2_{2,22} \rangle) + Re(\langle e^1_{1,11} | e^2_{2,22} \rangle). \tag{3.66}
$$

L'équation (3.64) permet d'établir une borne inférieure en exploitant cette propriété, ce qui permet ensuite d'obtenir une limite inférieure sur l'entropie conditionnelle $S(B|EC)$ dans l'équation (3.25).

Trois bases mutuellement non biaisées

En prenant en considération le bruit présent dans deux bases quantiques mutuellement non biaisées, il est possible d'établir une borne supérieure pour la quantité p, définie comme $|\langle e^0_{0,00} | e^1_{1,11} \rangle|^2$, $|\langle e^0_{0,00} | e^2_{2,22} \rangle|^2$ et $|\langle e^1_{1,11} | e^2_{2,22} \rangle|^2$, où ces bases sont données par :

$$
\begin{aligned}
|X\rangle_0 &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), \\
|X\rangle_1 &= \frac{1}{\sqrt{3}}(|0\rangle + \eta|1\rangle + \eta^*|2\rangle), \\
|X\rangle_2 &= \frac{1}{\sqrt{3}}(|0\rangle + \eta^*|1\rangle + \eta|2\rangle).
\end{aligned}
\tag{3.67}
$$

$$
\begin{aligned}
|Y\rangle_0 &= \frac{1}{\sqrt{3}}(\eta|0\rangle + |1\rangle + |2\rangle),\\
|Y\rangle_1 &= \frac{1}{\sqrt{3}}(|0\rangle + \eta|1\rangle + |2\rangle),\\
|Y\rangle_2 &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + \eta|2\rangle).
\end{aligned} \tag{3.68}
$$

Avec $\eta = e^{\frac{2i\pi}{3}}$, on peut vérifier aisément que le produit scalaire entre deux états de base appartenant à des bases mutuellement non biaisées différentes est égal à $\frac{1}{\sqrt{3}}$.

Nous nous concentrons sur l'itération où Alice choisit d'encoder son qutrit dans l'un des six états définis définis ci-dessus, tandis que Bob opte pour une opération de réflexion, et qu'ensuite, Alice effectue une mesure dans la même base qu'elle a initialement utilisée pour préparer l'état.

En conséquence, le canal quantique bidirectionnel devient un canal unidirectionnel avec Eve tentant d'intercepter les informations en utilisant l'opérateur unitaire $V = U_R U_F$. Sans perte de généralité, nous pouvons supposer que l'ancilla d'Eve est initialisée à l'état $|0\rangle_E$. Ainsi, l'action de celle-ci sur les états de base peut être décrite comme suit

$$
|i\rangle \otimes |0\rangle_E \xrightarrow{V} |i\rangle|f_{ii}\rangle + |i+1\rangle|f_{ii+1}\rangle + |i+2\rangle|f_{ii+2}\rangle. \tag{3.69}
$$

La propriété d'unitarité de V conduit à des contraintes :

$$
\langle f_{ii}|f_{ji}\rangle + \langle f_{ij}|f_{jj}\rangle + \langle f_{ik}|f_{jk}\rangle = 0. \tag{3.70}
$$

où $i = 0, j = 1, k = 2$, et où les permutations cycliques de ces valeurs sont également prises en compte.

Par ailleurs, il a été démontré [95] que la symétrie réduit considérablement la complexité de l'analyse. La condition de symétrie est définie en imposant certaines restrictions sur les produits scalaires qui caractérisent l'opération unitaire V de la stratégie d'écoute clandestine d'Eve. Principalement, les produits scalaires de la stratégie d'écoute clandestine d'Eve doivent être invariants sous l'échange des indices (0, 1 et 2). Cette invariance permet de diviser les produits scalaires en six groupes distincts :

$$
\begin{aligned}
a =& \langle f_{ii}|f_{ij}\rangle, && \text{pour } i \neq j,\\
b =& \langle f_{ii}|f_{jk}\rangle, && \text{où } i, j, \text{et } k \text{ sont tous différents},\\
c =& \langle f_{ij}|f_{ik}\rangle, && \text{où } i, j, \text{et } k \text{ sont tous différents},\\
z =& \langle f_{ij}|f_{ji}\rangle, && \text{pour } i \neq j,\\
m =& \langle f_{ij}|f_{ki}\rangle, && \text{où } i, j, \text{et } k \text{ sont tous différents},\\
t =& \langle f_{ii}|f_{jj}\rangle, && \text{pour } i \neq j\,;\ t \text{ est réel.}
\end{aligned} \tag{3.71}
$$

En tenant compte de la propriété d'unitarité (3.70) ainsi que des conditions de symétrie (3.71), nous déduisons l'expression suivante

$$\begin{aligned} t = 1 - \frac{1}{4}(&P_{X_0X_1} + P_{X_0X_2} + P_{X_1X_0} + P_{X_1X_2} \\ &+ P_{X_2X_1} + P_{X_2X_0} + P_{Y_0Y_1} + P_{Y_0Y_2} + P_{Y_1Y_0} \\ &+ P_{Y_1Y_2} + P_{Y_2Y_1} + P_{Y_2Y_0}) - \frac{1}{2}Re(m). \end{aligned} \tag{3.72}$$

La probabilité P_{ij} pour $\{i,j\} = \{X_0, X_1, X_2\}$ ou $\{i,j\} = \{Y_0, Y_1, Y_2\}$, correspond à la probabilité que Alice mesure un qutrit retourné dans l'état $|j\rangle$ après avoir initialement préparé l'état $|i\rangle$.

À partir de l'inégalité de Cauchy-Schwarz, il s'ensuit que la quantité $X_{3MUBs} = Re(p)$ peut être bornée de la manière suivante.

$$\begin{aligned} X_{3MUBs} \geq 3 - \frac{3}{4}(&P_{X_0X_1} + P_{X_0X_2} + P_{X_1X_0} + P_{X_1X_2} + P_{X_2X_1} + P_{X_2X_0} + P_{Y_0Y_1} \\ &+ P_{Y_0Y_2} + P_{Y_1Y_0} + P_{Y_1Y_2} + P_{Y_2Y_1} + P_{Y_2Y_0}) \\ - \frac{3}{2}(&\sqrt{p_{001}p_{102}} + \sqrt{p_{011}p_{102}} + \sqrt{p_{021}p_{102}} + \sqrt{p_{001}p_{112}} + \sqrt{p_{011}p_{112}} \\ &+ \sqrt{p_{021}p_{112}} + \sqrt{p_{001}p_{122}} + \sqrt{p_{011}p_{122}} + \sqrt{p_{021}p_{122}}) \\ - 3(&\sqrt{p_{000}p_{101}} + \sqrt{p_{010}p_{101}} + \sqrt{p_{020}p_{101}} + \sqrt{p_{010}p_{111}} + \sqrt{p_{020}p_{111}} \\ &+ \sqrt{p_{000}p_{121}} + \sqrt{p_{010}p_{121}} + \sqrt{p_{020}p_{121}}). \end{aligned} \tag{3.73}$$

Dans la Figure 3.3, nous avons représenté le résultat obtenu ainsi que les autres cas utilisant deux MUBs [96]. Les quatre MUBs que nous étudierons ci-dessous sont également présentés.

Quatre bases mutuellement non biaisées

Dans cette partie, nous exprimons une borne inférieure de la quantité p en utilisant trois bases mutuellement orthogonales au lieu de deux bases mutuellement orthogonales, $p = \left(|\langle e^0_{0,00}|e^1_{1,11}\rangle|^2 + |\langle e^0_{0,00}|e^2_{2,22}\rangle|^2 + |\langle e^1_{1,11}|e^2_{2,22}\rangle|^2\right)$.

En outre des deux bases précédemment définies (3.103, 3.68), nous définissons une troisième base qui est obtenue en remplaçant le paramètre dans la base Y par sa valeur complexe conjuguée.

$$\begin{aligned} |Z\rangle_0 &= \frac{1}{\sqrt{3}}(\eta^*|0\rangle + |1\rangle + |2\rangle), \\ |Z\rangle_1 &= \frac{1}{\sqrt{3}}(|0\rangle + \eta^*|1\rangle + |2\rangle), \\ |Z\rangle_2 &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + \eta^*|2\rangle). \end{aligned} \tag{3.74}$$

En procédant de la même manière que précédemment, nous obtenons l'expression suivante pour t ainsi que pour les autres probabilités

$$\begin{aligned} t = 1 - \frac{1}{6}(&P_{X_0X_1} + P_{X_0X_2} + P_{X_1X_0} + P_{X_1X_2} + P_{X_2X_1} + P_{X_2X_0} \\ &+ P_{Y_0Y_1} + P_{Y_0Y_2} + P_{Y_1Y_0} + P_{Y_1Y_2} + P_{Y_2Y_1} + P_{Y_2Y_0} \\ &+ P_{Z_0Z_1} + P_{Z_0Z_2} + P_{Z_1Z_0} + P_{Z_1Z_2} + P_{Z_2Z_1} + P_{Z_2Z_0}), \end{aligned} \tag{3.75}$$

où, comme auparavant, les probabilités P_{ij} pour $\{i,j\} = \{X_0, X_1, X_2\}$, $\{i,j\} = \{Y_0, Y_1, Y_2\}$ ou $\{i,j\} = \{Z_0, Z_1, Z_2\}$, représentent les cas où Alice mesure le qutrit renvoyé dans l'état $|j\rangle$ lorsqu'elle l'a initialement préparé dans l'état $|i\rangle$. Nous pouvons également remarquer que les autres produits scalaires restants sont nuls, *i.e.* $a = b = c = z = m = 0$. Dans ce cas, une borne peut être dérivée pour les probabilités considérées :

$$\begin{aligned} X_{4MUBs} \geq 3 - \frac{1}{2}(&P_{X_0X_1} + P_{X_0X_2} + P_{X_1X_0} + P_{X_1X_2} + P_{X_2X_1} + P_{X_2X_0} \\ &+ P_{Y_0Y_1} + P_{Y_0Y_2} + P_{Y_1Y_0} + P_{Y_1Y_2} + P_{Y_2Y_1} + P_{Y_2Y_0} \\ &+ P_{Z_0Z_1} + P_{Z_0Z_2} + P_{Z_1Z_0} + P_{Z_1Z_2} + P_{Z_2Z_1} + P_{Z_2Z_0}) \\ &- 3(\sqrt{p_{000}p_{101}} + \sqrt{p_{010}p_{101}} + \sqrt{p_{020}p_{101}} + \sqrt{p_{010}p_{111}} \\ &+ \sqrt{p_{020}p_{111}} + \sqrt{p_{000}p_{121}} + \sqrt{p_{010}p_{121}} + \sqrt{p_{020}p_{121}}). \end{aligned} \tag{3.76}$$

Nous introduisons la notation suivante :

$$\mathcal{S} = \begin{cases} X_i^2 & \text{if } X_i \geq 0 \\ 0 & Sinon \end{cases}, \tag{3.77}$$

où $i = \{3MUBs, 4MUBs\}$, combinant ainsi les deux cas étudiés :

$$X_i = Re(\langle e^0_{0,00}|e^1_{1,11}\rangle) + Re(\langle e^0_{0,00}|e^2_{2,22}\rangle) + Re(\langle e^1_{1,11}|e^2_{2,22}\rangle). \tag{3.78}$$

En utilisant la borne inférieure dérivée dans (3.73, 3.76) pour trois et quatre bases mutuellement non-biaisées respectivement, ainsi que le fait que $p = |\langle e^0_{0,00}|e^1_{1,11}\rangle + \langle e^0_{0,00}|e^2_{2,22}\rangle + \langle e^1_{1,11}|e^2_{2,22}\rangle|^2 \geq \mathcal{S}$, cela permet de borner inférieurement p et donc de majorer l'entropie de von Neumann $S(EC)$ et finalement trouver une borne inférieure pour l'entropie conditionnelle $S(B|EC)$ conformément à l'équation (3.25).

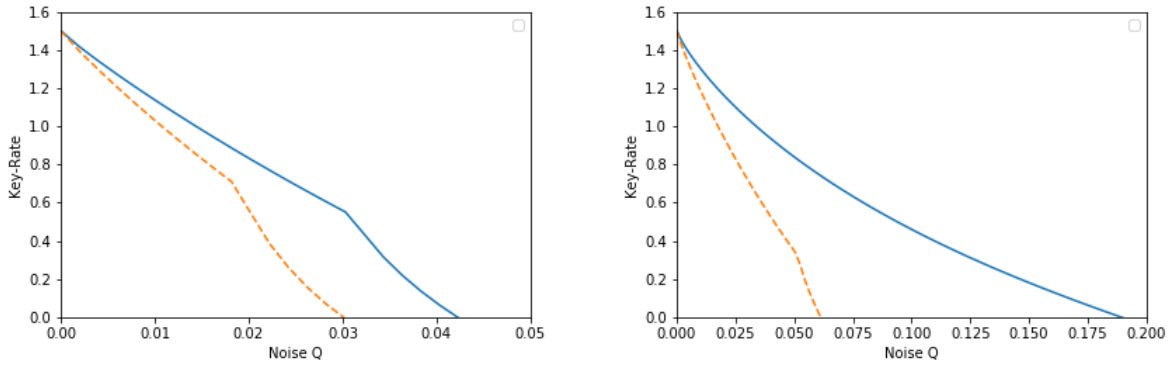
La figure 3.3 illustre une représentation graphique des solutions numériques pour la borne inférieure du taux de clé r en fonction du bruit Q dans deux scénarios, à savoir le canal dépendant, figure 3.3a, où le bruit sur les deux canaux (direct-inverse) dépendent l'un de l'autre, et le canal indépendant, figure 3.3b, où ces bruits sont indépendants l'un de l'autre. Nous avons observé que pour les états $\{|k\rangle\}\, i$ avec $k = X, Y, Z$ et $i = 0, 1, 2$, le bruit de base accumulé par le qutrit lors de son passage à travers des deux canaux lorsque Bob choisit de réfléchir est donné par $Q_{ind} = 2Q(2 - 3Q)$. En revanche, lorsque le bruit est dépendant, le bruit correspondant est de $Q_{dep} = Q$.

La variation de la borne inférieure du taux de clé r en fonction du paramètre Q pour le protocole SQKD tridimensionnel, lorsque Alice choisit ses états qutrits à partir de

l'ensemble Φ_2, est représentée sur la figure 3.2 (a). Les résultats de notre étude révèlent que le taux de clé est positif pour toutes les valeurs de Q ne dépassant pas 3 dans le cas d'un canal de communication indépendant. En revanche, dans le cas d'un canal dépendant, ce taux de clé reste positif pour toutes les valeurs de Q ne dépassant pas 4.2.

La figure 3.2(b) met en évidence une similitude de comportement lorsque les états choisis par Alice appartiennent à l'ensemble Φ_1. Nous constatons que la tolérance maximale au bruit pour un canal dépendant est de 19.1, tandis que pour un canal indépendant, elle chute à 6.1.

Il est intéressant de constater que le protocole SQKD Φ_1 permet d'obtenir un taux de clé supérieur à celui du protocole SQKD Φ_2. En outre, notre protocole est capable de tolérer une quantité de bruit supérieure à celle tolérée par le protocole 2D SQKD, qui est de 5.34 [16]. Cette tolérance est également supérieure à celle du protocole QKD, qui peut tolérer jusqu'à 15 de bruit d'après [97]. Ces résultats démontrent que l'avantage des dimensions élevées, typiquement associé aux protocoles de distribution quantique de clé, est également applicable aux modèles semi-quantiques.

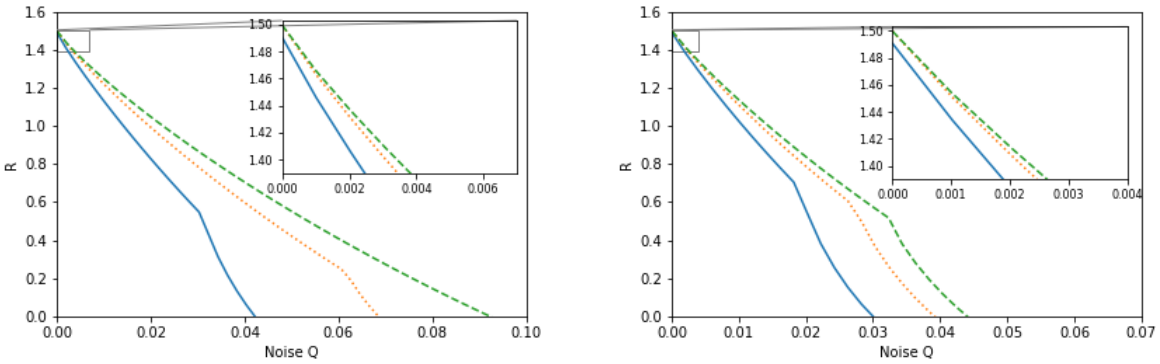


(a) (b)

FIGURE 3.2 : Évolution du taux de clé en fonction du bruit Q. La ligne en pointillé représente le canal indépendant $Q_{ind} = 2Q(2-3Q)$, tandis que pour la ligne pleine correspond au canal dépendant $Q_{dep} = Q$. (a) Cas du le protocole Φ_1-SQKD. (b) Cas du protocole Φ_2-SQKD.

Pour trois MUBs, nous avons constaté que le taux de clé est positif tant que $Q_{indep} \leq 3.95$ pour le cas de canal indépendant et $Q_{dep} \leq 6.89$ pour le cas de canal dépendant. En d'autres termes, pour toute valeur de bruit inférieure à ces valeurs seuils, Alice et Bob peuvent extraire une clé secrète sécurisée.

Les résultats montrent clairement que la valeur seuil du bruit tolérable augmente avec le nombre de bases mutuellement non baisées, mais le taux de clé lui-même augmente faiblement pour de faibles valeurs de bruit. Ces résultats sont synthétisés dans le Tableau 3.1.



(a) (b)

FIGURE 3.3 : Le taux de clé en fonction du bruit Q pour les états quantiques tridimensionnels avec deux (représentée par la ligne bleue), trois (représentée par la ligne orange) et quatre (représentée par la ligne verte) bases mutuellement non biaisées. Deux scénarios sont considérés : (a) le cas du canal dépendant et (b) le cas du canal indépendant.

TABLE 3.1 : La tolérance maximale au bruit pour un protocole SQKD tridimensionnel dans différents nombres de bases mutuellement non biaisées.

Nombre de MUBs utilisées	Dépendant	Indépendant
2 MUBs [96]	4.247%	3.05%
3 MUBs	6.89%	3.95%
4 MUBs	9.32%	4.43%

C Attaque collective avec des états quantique à quatre dimensions

Nous allons à présent nous focaliser sur l'étude du protocole SQKD qui repose sur l'utilisation de systèmes ququart, c'est-à-dire des systèmes à quatre dimensions ($d = 4$), plutôt que sur des qutrits.

L'objectif de cette analyse est de déterminer les niveaux de sécurité relatifs à la stratégie d'écoute collective, en fonction du nombre de bases mutuellement non biaisées employées dans le protocole. Plus précisément, nous étudierons les cas où le protocole utilise deux, trois, quatre ou cinq bases mutuellement impartiales. Nous nous concentrerons sur les résultats dérivés de cette étude pour évaluer la pertinence de ce protocole pour des applications pratiques.

En utilisant la base rectiligne $|0\rangle, |1\rangle, |2\rangle, |3\rangle$, il est envisageable d'exprimer la stratégie d'écoute unitaire la plus générale pour un ensemble d'états quantiques à quatre dimensions dans le canal aller, de la manière suivante

$$
\begin{aligned}
&|0\rangle \otimes |E\rangle \xrightarrow{U_F} |0\rangle|e_{00}\rangle + |1\rangle|e_{01}\rangle + |2\rangle|e_{02}\rangle + |3\rangle|e_{03}\rangle,\\
&|1\rangle \otimes |E\rangle \xrightarrow{U_F} |0\rangle|e_{10}\rangle + |1\rangle|e_{11}\rangle + |2\rangle|e_{12}\rangle + |3\rangle|e_{13}\rangle,\\
&|2\rangle \otimes |E\rangle \xrightarrow{U_F} |0\rangle|e_{20}\rangle + |1\rangle|e_{21}\rangle + |2\rangle|e_{22}\rangle + |3\rangle|e_{23}\rangle,\\
&|3\rangle \otimes |E\rangle \xrightarrow{U_F} |0\rangle|e_{30}\rangle + |1\rangle|e_{31}\rangle + |2\rangle|e_{32}\rangle + |3\rangle|e_{33}\rangle.
\end{aligned}
\tag{3.79}
$$

Lorsqu'une attaque est effectuée sur le canal de retour, l'état global final peut être exprimé de la manière suivante

$$
|i, e_{ji}\rangle \xrightarrow{U_R} |0, e^0_{i,ji}\rangle + |1, e^1_{i,ji}\rangle + |2, e^2_{i,ji}\rangle + |3, e^3_{i,ji}\rangle. \tag{3.80}
$$

Nous adoptons une méthode similaire à celle décrite dans la section précédente pour étudier le processus par lequel une itération contribue à la clé brute dans le protocole en question. Nous nous intéressons en particulier aux situations où Alice envoie un état de base de calcul, c'est-à-dire $|0\rangle$, $|1\rangle$, $|2\rangle$ ou $|3\rangle$, choisis chacun avec une probabilité égale de $1/4$, et où Bob mesure ensuite cet état avant de le renvoyer.

Grâce à la sous-additivité forte de l'entropie de Von Neumann, nous pouvons établir la limite inférieure du taux de clé :

$$
\begin{aligned}
r \geq & H(\frac{1}{4}p_{0,0,0}, \frac{1}{4}p_{0,0,1}, ..., \frac{1}{4}p_{3,3,3}) - H\left(\frac{1}{4}t_1, \frac{1}{4}t_2, \frac{1}{4}t_3, \frac{1}{4}t_4\right) - \frac{1}{4}(t_2 + t_3 + t_4)\\
& - \frac{1}{4}t_1 H(\tilde{\lambda_1}, \tilde{\lambda_2}) + H(p_A(0), p_A(1), p_A(2), p_A(3)) - H(\{p(i,j)\}_{i,j=0,1,2,3}).
\end{aligned}
\tag{3.81}
$$

Les mêmes notations que celles présentées dans l'équation (3.38) ont été utilisées avec les valeurs propres $\tilde{\lambda_i}$ explicitement définies selon les termes suivants

$$
\begin{aligned}
\tilde{\lambda_1} &= \frac{1}{2} + \frac{\sqrt{4p - 4p_{1,1,1}p_{2,2,2} - 4p_{0,0,0}p_{3,3,3} + (p_{0,0,0} - p_{1,1,1} - p_{2,2,2} + p_{3,3,3})^2}}{2(p_{0,0,0} + p_{1,1,1} + p_{2,2,2} + p_{3,3,3})},\\
\tilde{\lambda_2} &= \frac{1}{2} - \frac{\sqrt{4p - 4p_{1,1,1}p_{2,2,2} - 4p_{0,0,0}p_{3,3,3} + (p_{0,0,0} - p_{1,1,1} - p_{2,2,2} + p_{3,3,3})^2}}{2(p_{0,0,0} + p_{1,1,1} + p_{2,2,2} + p_{3,3,3})},
\end{aligned}
\tag{3.82}
$$

où

$$
\begin{aligned}
p = & |\langle e^0_{0,00}|e^1_{1,11}\rangle|^2 + |\langle e^0_{0,00}|e^2_{2,22}\rangle|^2 + |\langle e^0_{0,00}|e^3_{3,33}\rangle|^2 + |\langle e^1_{1,11}|e^2_{2,22}\rangle|^2 + |\langle e^1_{1,11}|e^3_{3,33}\rangle|^2\\
& + |\langle e^2_{2,22}|e^3_{3,33}\rangle|^2.
\end{aligned}
$$

Afin de déduire une expression de la borne inférieure de r, il est nécessaire de déterminer une borne inférieure de la quantité p en utilisant le taux d'erreur dans les différentes bases mutuellement non biaisées utilisées dans le protocole.

Nous allons procéder ainsi en fonction du nombre de bases utilisées dans le protocole. En fait, pour un espace de Hilbert de dimension quatre, il est possible de définir jusqu'à

cinq bases mutuellement non biaisées [98]. En plus de la base de calcul $\{|i\rangle\}_{i=0,1,2,3}$, quatre autres bases peuvent être ajoutées. La première base est généralement choisie comme étant la transformée de Fourier discrète de la base de calcul.

$$\begin{aligned}
|A\rangle_0 &= \frac{1}{2}(|0\rangle + |1\rangle + |2\rangle + |3\rangle),\\
|A\rangle_1 &= \frac{1}{2}(|0\rangle + |1\rangle - |2\rangle - |3\rangle),\\
|A\rangle_2 &= \frac{1}{2}(|0\rangle - |1\rangle - |2\rangle + |3\rangle),\\
|A\rangle_3 &= \frac{1}{2}(|0\rangle - |1\rangle + |2\rangle - |3\rangle).
\end{aligned} \tag{3.83}$$

La deuxième base est définie par

$$\begin{aligned}
|B\rangle_0 &= \frac{1}{2}(|0\rangle - |1\rangle - i|2\rangle - i|3\rangle),\\
|B\rangle_1 &= \frac{1}{2}(|0\rangle - |1\rangle + i|2\rangle + i|3\rangle),\\
|B\rangle_2 &= \frac{1}{2}(|0\rangle + |1\rangle + i|2\rangle - i|3\rangle),\\
|B\rangle_3 &= \frac{1}{2}(|0\rangle + |1\rangle - i|2\rangle + i|3\rangle).
\end{aligned} \tag{3.84}$$

De même, la troisième base est définie de la manière suivante

$$\begin{aligned}
|C\rangle_0 &= \frac{1}{2}(|0\rangle - i|1\rangle - i|2\rangle - |3\rangle),\\
|C\rangle_1 &= \frac{1}{2}(|0\rangle - i|1\rangle + i|2\rangle + |3\rangle),\\
|C\rangle_2 &= \frac{1}{2}(|0\rangle + i|1\rangle + i|2\rangle - |3\rangle),\\
|C\rangle_3 &= \frac{1}{2}(|0\rangle + i|1\rangle - i|2\rangle + |3\rangle),
\end{aligned} \tag{3.85}$$

Quant à la quatrième base, elle est définie de la façon suivante

$$\begin{aligned}
|D\rangle_0 &= \frac{1}{2}(|0\rangle - i|1\rangle - |2\rangle - i|3\rangle),\\
|D\rangle_1 &= \frac{1}{2}(|0\rangle - i|1\rangle + |2\rangle + i|3\rangle),\\
|D\rangle_2 &= \frac{1}{2}(|0\rangle + i|1\rangle - |2\rangle + i|3\rangle),\\
|D\rangle_3 &= \frac{1}{2}(|0\rangle + i|1\rangle + |2\rangle - i|3\rangle).
\end{aligned} \tag{3.86}$$

Les états mentionnés ci-dessus correspondent au nombre maximal de bases mutuellement non biaisées pour les ququarts.

En considérant les itérations du protocole où Alice envoie et mesure des états dans des bases en fonction du nombre de bases mutuellement non biaisées (MUB), alors que Bob

choisit de réfléchir le ququart, l'opération de Bob est équivalente à l'opérateur d'identité tandis que l'action d'Eve correspond à l'application de l'opération unitaire $V = U_R U_F$.

$$|i\rangle \otimes |0\rangle_E \xrightarrow{V} |i\rangle|f_{ii}\rangle + |i+1\rangle|f_{ii+1}\rangle + |i+2\rangle|f_{ii+2}\rangle + |i+3\rangle|f_{ii+3}\rangle, \tag{3.87}$$

Pour toutes les valeurs de i appartenant à l'ensemble $\{0, 1, 2, 3\}$, on applique la notation en indice addition modulo 4. Les produits scalaires entre les états de sortie d'Eve doivent respecter des contraintes similaires à celles du cas tridimensionnel (3.70) conduisant à nouveau à la classification des états de sortie d'Eve en six ensembles de produits scalaires, chacun définissant un paramètre libre :

$$\begin{aligned}
a &= \langle f_{ii}|f_{ij}\rangle, && \text{pour } i \neq j, \\
b &= \langle f_{ii}|f_{jk}\rangle, && \text{où } i, j, \text{et } k \text{ sont tous différents}, \\
c &= \langle f_{ij}|f_{ik}\rangle, && \text{où } i, j, \text{et } k \text{ sont tous différents}, \\
z &= \langle f_{ij}|f_{jh}\rangle, && \text{où } i, j, \text{et } h \text{ sont tous différents}, \\
m &= \langle f_{ij}|f_{hk}\rangle, && \text{où } j \neq i, (h = j \text{ and } k = i) \\
& && \text{or } (h, k, i \text{ and } j \text{ sont tous différents}); \text{ m est réel}, \\
t &= \langle f_{ii}|f_{jj}\rangle, && \text{pour } i \neq j \text{ ; t est réel.}
\end{aligned} \tag{3.88}$$

En appliquant conjointement la condition de symétrie, la condition unitaire ainsi que les erreurs induites par l'attaque d'Eve lors de l'utilisation de différents nombres de MUB, on peut en déduire l'expression présentée dans le Tableau 3.2.

TABLE 3.2 : Résultats de l'estimation du bruit dans les protocoles SQKD basés sur les ququarts en utilisant différents nombres de MUBs. Nous utilisons les notations $A = \sum_{i,j;i\neq j} p_{ij}$ for $\{i, j\} = \{A_0, A_1, A_2, A_3\}$, $B = \sum_{i,j;i\neq j} p_{ij}$ for $\{i, j\} = \{B_0, B_1, B_2, B_3\}$, $C = \sum_{i,j;i\neq j} p_{ij}$ for $\{i, j\} = \{C_0, C_1, C_2, C_3\}$, $D = \sum_{i,j;i\neq j} p_{ij}$ for $\{i, j\} = \{D_0, D_1, D_2, D_3\}$, afin de désigner la probabilité de l'événement selon lequel Alice mesure le ququart renvoyé dans l'état $|j\rangle$ lorsqu'elle l'a préparé initialement dans l'état $|i\rangle$ dans la base correspondante.

Bases	Vectors	Expression
2	4	$t = 1 - \frac{1}{3}A - 3Re(m)$
3	8	$t = 1 - \frac{1}{6}(A + B) - Re(m)$
4	12	$t = 1 - \frac{1}{9}(A + B + C) - \frac{1}{3}Re(m)$
5	16	$t = 1 - \frac{1}{12}(A + B + C + D)$

En appliquant l'inégalité de Cauchy-Schwarz, on obtient une borne pour la quantité $W_{i-MUBs} = Re(p)$.

□ *Deux MUBs* :

$$\begin{aligned}
W_{2-MUBs} \geq 6 &- 2(P_{A_0A_1} + P_{A_0A_2} + P_{A_0A_3} + P_{A_1A_0} + P_{A_1A_2} + P_{A_1A_3} \\
&+ P_{A_2A_1} + P_{A_2A_0} + P_{A_2A_3} + P_{A_3A_1} + P_{A_3A_0} + P_{A_3A_2}) \\
&- 18(\sqrt{P_{100}P_{001}} + \sqrt{P_{110}P_{001}} + \sqrt{P_{120}P_{001}} + \sqrt{P_{130}P_{001}} \\
&+ \sqrt{P_{100}P_{011}} + \sqrt{P_{110}P_{011}} + \sqrt{P_{120}P_{011}} + \sqrt{P_{130}P_{011}} \\
&+ \sqrt{P_{100}P_{021}} + \sqrt{P_{110}P_{021}} + \sqrt{P_{120}P_{021}} + \sqrt{P_{130}P_{021}} \\
&+ \sqrt{P_{100}P_{031}} + \sqrt{P_{110}P_{031}} + \sqrt{P_{120}P_{031}} + \sqrt{P_{130}P_{031}}) \\
&- 6(\sqrt{P_{101}P_{000}} + \sqrt{P_{121}P_{000}} + \sqrt{P_{131}P_{000}} + \sqrt{P_{101}P_{010}} \\
&+ \sqrt{P_{111}P_{010}} + \sqrt{P_{121}P_{010}} + \sqrt{P_{131}P_{010}} + \sqrt{P_{101}P_{020}} \\
&+ \sqrt{P_{111}P_{020}} + \sqrt{P_{121}P_{020}} + \sqrt{P_{131}P_{020}} + \sqrt{P_{101}P_{030}} \\
&+ \sqrt{P_{111}P_{030}} + \sqrt{P_{121}P_{030}} + \sqrt{P_{131}P_{030}}).
\end{aligned} \tag{3.89}$$

□ *Trois MUBs* :

$$\begin{aligned}
W_{3-MUBs} \geq 6 &- (P_{A_0A_1} + P_{A_0A_2} + P_{A_0A_3} + P_{A_1A_0} + P_{A_1A_2} + P_{A_1A_3} \\
&+ P_{A_2A_1} + P_{A_2A_0} + P_{A_2A_3} + P_{A_3A_1} + P_{A_3A_0} + P_{A_3A_2} \\
&+ P_{B_0B_1} + P_{B_0B_2} + P_{B_0B_3} + P_{B_1B_0} + P_{B_1B_2} + P_{B_1B_3} \\
&+ P_{B_2B_1} + P_{B_2B_0} + P_{B_2B_3} + P_{B_3B_1} + P_{B_3B_0} + P_{B_3B_2}) \\
&- 6(\sqrt{P_{100}P_{001}} + \sqrt{P_{110}P_{001}} + \sqrt{P_{120}P_{001}} + \sqrt{P_{130}P_{001}} \\
&+ \sqrt{P_{100}P_{011}} + \sqrt{P_{110}P_{011}} + \sqrt{P_{120}P_{011}} + \sqrt{P_{130}P_{011}} \\
&+ \sqrt{P_{100}P_{021}} + \sqrt{P_{110}P_{021}} + \sqrt{P_{120}P_{021}} + \sqrt{P_{130}P_{021}} \\
&+ \sqrt{P_{100}P_{031}} + \sqrt{P_{110}P_{031}} + \sqrt{P_{120}P_{031}} + \sqrt{P_{130}P_{031}}) \\
&- 6(\sqrt{P_{101}P_{000}} + \sqrt{P_{121}P_{000}} + \sqrt{P_{131}P_{000}} + \sqrt{P_{101}P_{010}} \\
&+ \sqrt{P_{111}P_{010}} + \sqrt{P_{121}P_{010}} + \sqrt{P_{131}P_{010}} + \sqrt{P_{101}P_{020}} \\
&+ \sqrt{P_{111}P_{020}} + \sqrt{P_{121}P_{020}} + \sqrt{P_{131}P_{020}} + \sqrt{P_{101}P_{030}} \\
&+ \sqrt{P_{111}P_{030}} + \sqrt{P_{121}P_{030}} + \sqrt{P_{131}P_{030}}).
\end{aligned} \tag{3.90}$$

□ *Quatre MUBs* :

$$\begin{aligned}
W_{4-MUBs} \geq 6 &- \frac{2}{3}(P_{A_0A_1} + P_{A_0A_2} + P_{A_0A_3} + P_{A_1A_0} + P_{A_1A_2} + P_{A_1A_3} \\
&+ P_{A_2A_1} + P_{A_2A_0} + P_{A_2A_3} + P_{A_3A_1} + P_{A_3A_0} + P_{A_3A_2} \\
&+ P_{B_0B_1} + P_{B_0B_2} + P_{B_0B_3} + P_{B_1B_0} + P_{B_1B_2} + P_{B_1B_3} \\
&+ P_{B_2B_1} + P_{B_2B_0} + P_{B_2B_3} + P_{B_3B_1} + P_{B_3B_0} + P_{B_3B_2} \\
&+ P_{C_0C_1} + P_{C_0C_2} + P_{C_0C_3} + P_{C_1C_0} + P_{C_1C_2} + P_{C_1C_3} \\
&+ P_{C_2C_1} + P_{C_2C_0} + P_{C_2C_3} + P_{C_3C_1} + P_{C_3C_0} + P_{C_3C_2}) \\
&- 2(\sqrt{P_{100}P_{001}} + \sqrt{P_{110}P_{001}} + \sqrt{P_{120}P_{001}} + \sqrt{P_{130}P_{001}} \\
&+ \sqrt{P_{100}P_{011}} + \sqrt{P_{110}P_{011}} + \sqrt{P_{120}P_{011}} + \sqrt{P_{130}P_{011}} \\
&+ \sqrt{P_{100}P_{021}} + \sqrt{P_{110}P_{021}} + \sqrt{P_{120}P_{021}} + \sqrt{P_{130}P_{021}} \\
&+ \sqrt{P_{100}P_{031}} + \sqrt{P_{110}P_{031}} + \sqrt{P_{120}P_{031}} + \sqrt{P_{130}P_{031}}) \\
&- 6(\sqrt{P_{101}P_{000}} + \sqrt{P_{121}P_{000}} + \sqrt{P_{131}P_{000}} + \sqrt{P_{101}P_{010}} \\
&+ \sqrt{P_{111}P_{010}} + \sqrt{P_{121}P_{010}} + \sqrt{P_{131}P_{010}} + \sqrt{P_{101}P_{020}} \\
&+ \sqrt{P_{111}P_{020}} + \sqrt{P_{121}P_{020}} + \sqrt{P_{131}P_{020}} + \sqrt{P_{101}P_{030}} \\
&+ \sqrt{P_{111}P_{030}} + \sqrt{P_{121}P_{030}} + \sqrt{P_{131}P_{030}}).
\end{aligned} \tag{3.91}$$

□ *Cinq MUBs* :

$$\begin{aligned} W_{5-MUBs} \geq 6 - \frac{1}{2}(&P_{A_0A_1} + P_{A_0A_2} + P_{A_0A_3} + P_{A_1A_0} + P_{A_1A_2} + P_{A_1A_3} \\ &+ P_{A_2A_1} + P_{A_2A_0} + P_{A_2A_3} + P_{A_3A_1} + P_{A_3A_0} + P_{A_3A_2} \\ &+ P_{B_0B_1} + P_{B_0B_2} + P_{B_0B_3} + P_{B_1B_0} + P_{B_1B_2} + P_{B_1B_3} \\ &+ P_{B_2B_1} + P_{B_2B_0} + P_{B_2B_3} + P_{B_3B_1} + P_{B_3B_0} + P_{B_3B_2} \\ &+ P_{C_0C_1} + P_{C_0C_2} + P_{C_0C_3} + P_{C_1C_0} + P_{C_1C_2} + P_{C_1C_3} \\ &+ P_{C_2C_1} + P_{C_2C_0} + P_{C_2C_3} + P_{C_3C_1} + P_{C_3C_0} + P_{C_3C_2} \\ &+ P_{D_0D_1} + P_{D_0D_2} + P_{D_0D_3} + P_{D_1D_0} + P_{D_1D_2} + P_{D_1D_3} \\ &+ P_{D_2D_1} + P_{D_2D_0} + P_{D_2D_3} + P_{D_3D_1} + P_{D_3D_0} + P_{D_3D_2}) \\ - 6(&\sqrt{P_{101}P_{000}} + \sqrt{P_{121}P_{000}} + \sqrt{P_{131}P_{000}} + \sqrt{P_{101}P_{010}} \\ &+ \sqrt{P_{111}P_{010}} + \sqrt{P_{121}P_{010}} + \sqrt{P_{131}P_{010}} + \sqrt{P_{101}P_{020}} \\ &+ \sqrt{P_{111}P_{020}} + \sqrt{P_{121}P_{020}} + \sqrt{P_{131}P_{020}} + \sqrt{P_{101}P_{030}} \\ &+ \sqrt{P_{111}P_{030}} + \sqrt{P_{121}P_{030}} + \sqrt{P_{131}P_{030}}). \end{aligned} \tag{3.92}$$

Encore une fois, en utilisant la notation suivante

$$\mathcal{S} = \begin{cases} W_i^2 & \text{if } W_i \geq 0 \\ 0 & Sinon \end{cases}, \tag{3.93}$$

où $i = \{2MUBs, 3MUBs, 4MUBs, 5MUBs\}$ et

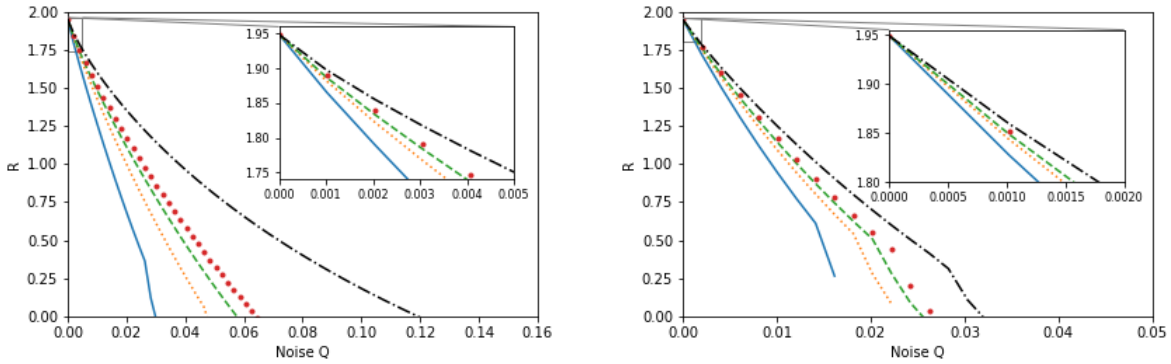
$$\begin{aligned} W_i = &Re(\langle e^0_{0,00}|e^1_{1,11}\rangle) + Re(\langle e^0_{0,00}|e^2_{2,22}\rangle) + Re(\langle e^0_{0,00}|e^3_{3,33}\rangle) \\ &+Re(\langle e^1_{1,11}|e^2_{2,22}\rangle) + Re(\langle e^1_{1,11}|e^3_{3,33}\rangle) + Re(\langle e^2_{2,22}|e^3_{3,33}\rangle), \end{aligned} \tag{3.94}$$

La borne sur la quantité en question permet d'obtenir facilement une borne inférieure sur le taux de clé qui est exprimé en fonction des paramètres déterminés par le canal quantique. Ainsi, on peut déduire que le taux de clé est positif si et seulement si Eve dispose d'une quantité d'information inférieure à celle de Bob. Cette conclusion résulte de l'utilisation de la formule mathématique précédente qui prend en compte les différentes contraintes sur le système quantique lors de la communication sécurisée.

La borne inférieure du taux clé en fonction du paramètre de bruit Q, pour différents nombres de bases mutuellement non biaisées, est représentée sur la figure 3.4 en considérant deux types de canaux : canaux dépendants (Figure 3.4a) et indépendants (Figure 3.4b).

D'après nos observations numériques, il apparaît que plus le nombre de bases mutuellement non-biaisées augmente, plus la capacité de tolérance au bruit maximal atteint 6.48% dans le cas dépendant et 2.65% dans le cas indépendant, tous deux obtenus en utilisant le nombre maximal de bases mutuellement non-biaisées, *i.e.* quatre bases.

On peut également observer en comparant ces résultats avec ceux de la section précédente, où des qutrits ont été utilisés, que la tolérance au bruit pour le schéma à quatre dimensions est inférieure par rapport au schéma à trois dimensions, mais cela est compensé par une augmentation du taux de génération de clés, qui passe de 1.5 à 2.



(a) (b)

FIGURE 3.4 : Le taux de clé en fonction du bruit Q pour des états quantiques à quatre dimensions avec deux (ligne bleue), trois (ligne orange), quatre (ligne verte) et cinq (ligne rouge) bases mutuellement non biaisées. (a) montre le canal dépendant (lorsque les $\{|k\rangle\}_i$ pour $\{k = A, B, C, D\}, \{i = 0, 1, 2, 3\}$ ont un bruit de base de Q) tandis que (b) représente le canal indépendant (dans ce cas, le bruit est Q_k=2Q(3-6Q) pour $k = A, B, C, D$).

Pour mettre en évidence l'importance du choix des bases à utiliser, nous présentons sur les mêmes graphiques (Fig. 3.4) le cas où seules les deux bases mutuellement non-biaisées sont utilisées, à savoir la base de calcul et la deuxième base (3.84). Ce dérnier est représentée par la ligne noire sur ces figures.

TABLE 3.3 : Tolérance maximale au bruit pour un protocole SQKD à quatre dimensions dans des scénarios de canaux dépendants et indépendants.

Nombre de MUBs utilisées	Dépendant	Indépendant
2MUBs	3%	1.62%
3MUBs	4.77%	2.24%
4MUBs	5.79%	2.58%
5MUBs	6.48%	2.65%

Les résultats obtenus montrent que le choix des bases utilisées peut avoir un impact significatif sur la tolérance au bruit des schémas de génération de clés quantiques basés sur les MUBs. En particulier, il est observé que la tolérance maximale au bruit peut varier considérablement selon les bases choisies. La tolérance maximale au bruit chute à 3.22% dans le cas du canal indépendant, tandis qu'elle atteint 12.05% dans le cas du canal dépendant. Ces résultats soulignent l'importance de prendre en compte à la fois la quantité et la qualité des bases utilisées dans la conception des protocoles de génération de clés quantiques basés sur les MUBs. Les résultats concernants la tolérance au bruit maximal pour différents nombres de bases mutuellement non biaisées sont rassemblés dans le tableau 3.3.

Les principales conclusions que l'on peut retenir de cette section sont les suivants :

1. L'augmentation du nombre de bases mutuellement non biaisées permet d'accroître la résistance du canal quantique au bruit.
2. L'encodage dans des bases mutuellement non biaisées (MUB) de plus grande dimension améliore la sécurité contre les écoutes clandestines et permet d'obtenir des taux de génération de clé sécurisée plus élevés, tout en réduisant le taux d'erreur.

Toutefois, une analyse qualitative suggère que, dans certains cas, le choix de travailler avec seulement deux bases peut être préférable à l'utilisation de $d+1$ bases, car cela peut réduire le taux d'erreur maximal.

VI L'interception optimale dans le protocole SQKD.

Les travaux présentés dans cette section ont fait l'objet d'un article soumis en publication.

La distribution semi-quantique de clé, telle que suggérée initialement par Michel Boyer, Dan Kenigsberg et Tal Mor (BKM07) [5], vise à établir une clé secrète avec deux entités de capacités différentes, reliées par le biais d'un canal quantique et d'un canal classique authentifié. Récemment, l'utilisation de systèmes tridimensionnels plutôt que des systèmes bidimensionnels pour établir une clé quantique sécurisée a été suggérée [96].

Pour pouvoir évaluer la sécurité du protocole de distribution de clés semi-quantique, appliqué à des états quantiques tridimensionnels présenté précédemment, nous nous intéressons sur l'analyse d'une stratégie d'interception optimale en termes de l'information mutuelle partagée entre Alice et Eve, en prenant en compte d'une perturbation donnée tout en respectant les exigences de l'unitarité. L'objectif principal de cette section est de dériver la probabilité de réussite de l'écoute clandestine en fonction du taux d'erreur causée par celle-ci.

A Analyse de sécurité

Dans cette sous-section, notre attention est principalement portée sur les attaques incohérentes. Plus précisément, nous considérons l'interaction où un adversaire, Eve, est autorisée à interagir avec un seul état quantique en transit à la fois. Elle conserve ses états auxiliaires dans une mémoire quantique jusqu'à ce qu'elle reçoive toutes les données classiques, y compris les données de correction d'erreur et d'amplification de confidentialité puis effectue une mesure sur chacun de ses états auxiliaires pour obtenir autant d'informations que possible sur la clé finale.

La quantité de l'information qu'un adversaire, Eve, peut extraire de ses états auxiliaires dépend de la puissance de l'attaque et de la manière dont elle mesure ensuite ces états auxiliaires. Lorsque l'attaque est plus puissante, Eve peut extraire davantage de l'informations à partir des états auxiliaires, mais cela entraîne une augmentation de la perturbation sur le système reçu par Alice. Ainsi, il existe un compromis entre la quantité de l'information obtenue par Eve et le niveau de perturbation introduit dans le système en transit entre Alice et Bob, ainsi qu'ultérieurement entre Bob et Alice.

Dans les paragraphes suivants, nous cherchons à optimiser le gain de l'information pour une valeur donnée de la perturbation.

Dans un schéma de communication à deux voies, une stratégie d'écoute donnée peut être caractérisée par une paire d'opérations unitaires (U_F, U_R) agissant sur $\mathcal{H}_T \otimes \mathcal{H}_E$, où $\mathcal{H}_T$ l'espace de Hilbert modélisant le qutrit en transit, et $\mathcal{H}_E$ représente l'ancilla privée de Eve pour une itération du protocole. L'opérateur unitaire U_F est utilisée pour attaquer les états quantiques lors de leur passage de l'émetteur Alice à Bob, (*i.e.*, le canal direct), l'opérateur unitaire U_R est utilisée pour attaquer les états quantiques lorsqu'ils retournent de Bob à Alice (*i.e.*, canal inverse).

Conventionnellement, la première base du protocole correspond génaralement à la base de calcul, c'est-à-dire que dans un espace de Hilbert tridimensionnel, nous la désignons par $\{|0\rangle, |1\rangle, |2\rangle\}$. Ainsi, la stratégie d'interception symétrique la plus générale pour les qutrits se présente sous la forme suivante

$$\begin{aligned}
U_F(|0\rangle \otimes |0\rangle) =& \sqrt{1-D}|0\rangle|E_{00}\rangle + \sqrt{\frac{D}{2}}|1\rangle|E_{01}\rangle + \sqrt{\frac{D}{2}}|2\rangle|E_{02}\rangle,\\
U_F(|1\rangle \otimes |0\rangle) =& \sqrt{\frac{D}{2}}|0\rangle|E_{10}\rangle + \sqrt{1-D}|1\rangle|E_{11}\rangle + \sqrt{\frac{D}{2}}|2\rangle|E_{12}\rangle,\\
U_F(|2\rangle \otimes |0\rangle) =& \sqrt{\frac{D}{2}}|0\rangle|E_{20}\rangle + \sqrt{\frac{D}{2}}|1\rangle|E_{21}\rangle + \sqrt{1-D}|2\rangle|E_{22}\rangle,
\end{aligned}$$

où $|0\rangle$ désigne l'état initial d'Eve, et $|E_{00}\rangle$, $|E_{01}\rangle$, $|E_{02}\rangle$, $|E_{10}\rangle$, $|E_{11}\rangle$, $|E_{12}\rangle$, $|E_{20}\rangle$, $|E_{21}\rangle$ et $|E_{22}\rangle$ se réfèrent à ses états après la transformation. Le paramètre $D \in [0, 1/2]$ correspond à la perturbation.

Pour assurer l'unitarité de l'opérateur U_F, il est nécessaire que les produits scalaires entre les états de sortie d'Ève respectent des relations spécifiques.

$$\sqrt{\frac{D(1-D)}{2}}(\langle E_{ij}|E_{jj}\rangle + \langle E_{i,i}|E_{ji}\rangle) + \frac{D}{2}\langle E_{ik}|E_{jk}\rangle = 0, \tag{3.95}$$

où $i = 0, j = 1, k = 2$ et où les permutations cycliques de ces valeurs sont également prises en compte. De toute évidence, l'attaquant Eve intercepte le qutrit de transit lors de son retour, applique son deuxième opérateur d'attaque U_R sur les états de la forme $|i, e_j\rangle$. L'action de cet opérateur sans perte de généralité, peut être exprimée comme suit :

$$U_R(|i\rangle|E_{ji}\rangle) \otimes |0\rangle = \sqrt{1-D}|i\rangle|E^i_{i,ji}\rangle + \sqrt{\frac{D}{2}}|i+1\rangle|E^{i+1}_{i,ji}\rangle + \sqrt{\frac{D}{2}}|i+2\rangle|E^{i+2}_{i,ji}\rangle. \tag{3.96}$$

En utilisant la notation décrite ci-dessus, nous sommes désormais en mesure de dériver le système quantique commun qui représente une seule itération du protocole, en tenant compte des événements qui contribuent à établir la clé secrète.

Suite à l'interaction avec Eve, nous pouvons déterminer l'état quantique global partagé entre Bob et Eve, symbolisé par ρ_i^{BE}

$$
\begin{aligned}
\rho_0^{BE} = {} & |0\rangle\langle 0| \left((1-D)^2 |E^0_{0,00}\rangle\langle E^0_{0,00}| + \frac{D^2}{4} |E^0_{1,01}\rangle\langle E^0_{1,01}| + \frac{D^2}{4} |E^0_{2,02}\rangle\langle E^0_{2,02}| \right) \\
& + |0\rangle\langle 1| \left((1-D)\sqrt{\frac{D(1-D)}{2}} |E^0_{0,00}\rangle\langle E^1_{0,00}| + \frac{D^2}{4} |E^0_{2,02}\rangle\langle E^1_{2,02}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^0_{1,01}\rangle\langle E^1_{1,01}| \right) \\
& + |0\rangle\langle 2| \left((1-D)\sqrt{\frac{D(1-D)}{2}} |E^0_{0,00}\rangle\langle E^2_{0,00}| + \frac{D^2}{4} |E^0_{1,01}\rangle\langle E^2_{1,01}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^0_{2,02}\rangle\langle E^2_{2,02}| \right) \\
& + |1\rangle\langle 0| \left((1-D)\sqrt{\frac{D(1-D)}{2}} |E^1_{0,00}\rangle\langle E^0_{0,00}| + \frac{D^2}{4} |E^1_{2,02}\rangle\langle E^0_{2,02}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^1_{1,01}\rangle\langle E^0_{1,01}| \right) \\
& + |1\rangle\langle 1| \left(\frac{D(1-D)}{2} |E^1_{0,00}\rangle\langle E^1_{0,00}| + \frac{D(1-D)}{2} |E^1_{1,01}\rangle\langle E^1_{1,01}| + \frac{D^2}{4} |E^1_{2,02}\rangle\langle E^1_{2,02}| \right) \\
& + |1\rangle\langle 2| \left(\frac{D(1-D)}{2} |E^1_{0,00}\rangle\langle E^2_{0,00}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^1_{2,02}\rangle\langle E^2_{2,02}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^1_{1,01}\rangle\langle E^2_{1,01}| \right) \\
& + |2\rangle\langle 0| \left((1-D)\sqrt{\frac{D(1-D)}{2}} |E^2_{0,00}\rangle\langle E^0_{0,00}| + \frac{D^2}{4} |E^2_{1,01}\rangle\langle E^0_{1,01}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^2_{2,02}\rangle\langle E^0_{2,02}| \right) \\
& + |2\rangle\langle 1| \left(\frac{D(1-D)}{2} |E^2_{0,00}\rangle\langle E^1_{0,00}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^2_{1,01}\rangle\langle E^1_{1,01}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^2_{2,02}\rangle\langle E^1_{2,02}| \right) \\
& + |2\rangle\langle 2| \left(\frac{D(1-D)}{2} |E^2_{0,00}\rangle\langle E^2_{0,00}| + \frac{D(1-D)}{2} |E^2_{2,02}\rangle\langle E^2_{2,02}| + \frac{D^2}{4} |E^2_{1,01}\rangle\langle E^2_{1,01}| \right)
\end{aligned}
$$

$$
\begin{aligned}
\rho_1^{BE} = {} & |0\rangle\langle 0| \left(\frac{D(1-D)}{2} |E^0_{0,10}\rangle\langle E^0_{0,10}| + \frac{D(1-D)}{2} |E^0_{1,11}\rangle\langle E^0_{1,11}| + \frac{D^2}{4} |E^0_{2,12}\rangle\langle E^0_{2,12}| \right) \\
& + |0\rangle\langle 1| \left(\frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^0_{0,10}\rangle\langle E^1_{0,10}| + (1-D)\sqrt{\frac{D(1-D)}{2}} |E^0_{1,01}\rangle\langle E^1_{1,11}| + \frac{D^2}{4} |E^0_{2,12}\rangle\langle E^1_{2,12}| \right) \\
& + |0\rangle\langle 2| \left(\frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^0_{0,10}\rangle\langle E^2_{0,10}| + \frac{D(1-D)}{2} |E^0_{1,11}\rangle\langle E^2_{1,11}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^0_{2,12}\rangle\langle E^2_{2,12}| \right) \\
& + |1\rangle\langle 0| \left(\frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^1_{0,10}\rangle\langle E^0_{0,10}| + (1-D)\sqrt{\frac{D(1-D)}{2}} |E^1_{1,11}\rangle\langle E^0_{1,11}| + \frac{D^2}{4} |E^1_{2,12}\rangle\langle E^0_{2,12}| \right) \\
& + |1\rangle\langle 1| \left((1-D)^2 |E^1_{1,11}\rangle\langle E^1_{1,11}| + \frac{D^2}{4} |E^1_{0,10}\rangle\langle E^1_{0,10}| + \frac{D^2}{4} |E^1_{2,12}\rangle\langle E^1_{2,12}| \right) \\
& + |1\rangle\langle 2| \left(\frac{D^2}{4} |E^1_{0,10}\rangle\langle E^2_{0,10}| + (1-D)\sqrt{\frac{D(1-D)}{2}} |E^1_{1,11}\rangle\langle E^2_{1,11}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^1_{2,12}\rangle\langle E^2_{2,12}| \right) \\
& + |2\rangle\langle 0| \left(\frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^2_{0,10}\rangle\langle E^0_{0,10}| + \frac{D(1-D)}{2} |E^2_{1,11}\rangle\langle E^0_{1,11}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^2_{2,12}\rangle\langle E^0_{2,12}| \right) \\
& + |2\rangle\langle 1| \left(\frac{D^2}{4} |E^2_{0,10}\rangle\langle E^1_{0,10}| + (1-D)\sqrt{\frac{D(1-D)}{2}} |E^2_{1,11}\rangle\langle E^1_{1,11}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^2_{2,12}\rangle\langle E^1_{2,12}| \right) \\
& + |2\rangle\langle 2| \left(\frac{D^2}{4} |E^2_{0,10}\rangle\langle E^2_{0,10}| + \frac{D(1-D)}{2} |E^2_{1,11}\rangle\langle E^2_{1,11}| + \frac{D(1-D)}{2} |E^2_{2,12}\rangle\langle E^2_{2,12}| \right)
\end{aligned}
$$

$$
\begin{aligned}
\rho_2^{BE} &= |0\rangle\langle 0| \left(\frac{D(1-D)}{2} |E^0_{0,20}\rangle\langle E^0_{0,20}| + \frac{D^2}{4} |E^0_{1,21}\rangle\langle E^0_{1,21}| + \frac{D(1-D)}{2} |E^0_{2,22}\rangle\langle E^0_{2,22}| \right) \\
&+ |1\rangle\langle 1| \left(\frac{D^2}{4} |E^1_{0,20}\rangle\langle E^1_{0,20}| + \frac{D(1-D)}{2} |E^1_{1,21}\rangle\langle E^1_{1,21}| + \frac{D(1-D)}{2} |E^1_{2,22}\rangle\langle E^1_{2,22}| \right) \\
&+ |1\rangle\langle 2| \left(\frac{D^2}{4} |E^1_{0,20}\rangle\langle E^2_{0,20}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^1_{1,21}\rangle\langle E^2_{1,21}| + (1-D)\sqrt{\frac{D(1-D)}{2}} |E^1_{2,22}\rangle\langle E^2_{2,22}| \right) \\
&+ |2\rangle\langle 1| \left(\frac{D^2}{4} |E^2_{0,20}\rangle\langle E^1_{0,20}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^2_{1,21}\rangle\langle E^1_{1,21}| + (1-D)\sqrt{\frac{D(1-D)}{2}} |E^2_{2,22}\rangle\langle E^1_{2,22}| \right) \\
&+ |2\rangle\langle 2| \left((1-D)^2 |E^2_{2,22}\rangle\langle E^2_{2,22}| + \frac{D^2}{4} |E^2_{0,20}\rangle\langle E^2_{0,20}| + \frac{D^2}{4} |E^2_{1,21}\rangle\langle E^2_{1,21}| \right) \\
&+ |0\rangle\langle 1| \left(\frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^0_{0,20}\rangle\langle E^1_{0,20}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^0_{1,21}\rangle\langle E^1_{1,21}| + \frac{D(1-D)}{2} |E^0_{2,22}\rangle\langle E^1_{2,22}| \right) \\
&+ |0\rangle\langle 2| \left(\frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^0_{0,20}\rangle\langle E^2_{0,20}| + \frac{D^2}{4} |E^0_{1,21}\rangle\langle E^2_{1,21}| + (1-D)\sqrt{\frac{D(1-D)}{2}} |E^0_{2,22}\rangle\langle E^2_{2,22}| \right) \\
&+ |1\rangle\langle 0| \left(\frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^1_{0,20}\rangle\langle E^0_{0,20}| + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^1_{1,21}\rangle\langle E^0_{1,21}| + \frac{D(1-D)}{2} |E^1_{2,22}\rangle\langle E^0_{2,22}| \right) \\
&+ |2\rangle\langle 0| \left(\frac{D}{2}\sqrt{\frac{D(1-D)}{2}} |E^2_{0,20}\rangle\langle E^0_{0,20}| + \frac{D^2}{4} |E^2_{1,21}\rangle\langle E^0_{1,21}| + (1-D)\sqrt{\frac{D(1-D)}{2}} |E^2_{2,22}\rangle\langle E^0_{2,22}| \right).
\end{aligned}
$$

Le taux d'erreur quantique dans la base Z, désigné par Q_Z, correspond à la proportion des états initiaux $|i\rangle$ émis par Alice, mais qui sont interprétés comme des états $|j\rangle$ par Alice pour $i, j = \{0, 1, 2\}$:

$$
\begin{aligned}
Q_Z &= \langle 1|\rho_0^A|1\rangle = \langle 1|\rho_2^A|1\rangle = \langle 0|\rho_1^A|0\rangle = \langle 2|\rho_0^A|2\rangle = \langle 0|\rho_2^A|0\rangle = \langle 2|\rho_1^A|2\rangle \\
&= D - \frac{3D^2}{4},
\end{aligned} \tag{3.97}
$$

Les opérateurs de densité réduite ρ_0^A, ρ_1^A et ρ_2^A sont obtenus en réalisant une opération de trace partielle sur ρ_i^{BE} afin d'éliminer l'état de Eve. Ces opérateurs de densité réduite représentent les états que Alice reçoit lorsqu'elle envoie initialement les qutrits $|0\rangle$, $|1\rangle$ et $|2\rangle$ respectivement.

Prenons en considération l'information mutuelle entre deux variables aléatoires X et Y, avec des valeurs possibles x et y respectivement. Cette mesure, notée I_{XY}, quantifie l'information partagée entre deux parties, est définie de la manière suivante :

$$
I(X:Y) \;=\; \sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(y|x) - \sum_{y\in Y} p(y)\log p(y), \tag{3.98}
$$

où $p(x, y) = p(x)p(y|x)$ est la probabilité conjointe de trouver x et y, et $p(y|x)$ est la probabilité conditionnelle de y sachant x. Toutes les opérations logarithmiques sont effectuées en utilisant une base 3.

Nous allons maintenant quantifier l'information que Alice peut extraire de son état initial, noté I^{AB}. Pour ce faire, nous considérerons l'information mutuelle entre l'état initial d'Alice, X, et la clé secrète partagée avec Bob, Y.

Les probabilités conditionnelles des mesures de l'état $|j\rangle$ par Alice, lorsqu'elle a préparé initialement le qutrit dans l'état $|i\rangle$, sont déterminées respectivement par les états quantiques ρ_0^A, ρ_1^A et ρ_2^A.

$$
\begin{aligned}
p(0|\rho_0^A) &= \langle 0|\rho_0^A|0\rangle = 1 - 2D + \frac{3D^2}{2} \\
p(1|\rho_0^A) &= \langle 1|\rho_0^A|1\rangle = D - \frac{3D^2}{4} \\
p(2|\rho_0^A) &= \langle 2|\rho_0^A|2\rangle = D - \frac{3D^2}{4} \\
p(0|\rho_1^A) &= \langle 0|\rho_1^A|0\rangle = D - \frac{3D^2}{4} \\
p(1|\rho_1^A) &= \langle 1|\rho_1^A|1\rangle = 1 - 2D + \frac{3D^2}{2} \\
p(2|\rho_1^A) &= \langle 2|\rho_1^A|2\rangle = D - \frac{3D^2}{4} \\
p(0|\rho_2^A) &= \langle 0|\rho_2^A|0\rangle = D - \frac{3D^2}{4} \\
p(1|\rho_2^A) &= \langle 1|\rho_2^A|1\rangle = D - \frac{3D^2}{4} \\
p(2|\rho_2^A) &= \langle 2|\rho_2^A|2\rangle = 1 - 2D + \frac{3D^2}{2}
\end{aligned}
$$

Par ailleurs, en considérant la probabilité $p_A(0)$ que le trit d'Alice soit zéro, ainsi que les probabilités $p_A(1)$ et $p_A(2)$ respectivement associées à la valeur un et deux, nous pouvons alors écrire :

$$
\begin{aligned}
p_A(0) &= \frac{1}{3}(1 - 2D + \frac{3D^2}{2} + D - \frac{3D^2}{4} + D - \frac{3D^2}{4}) = \frac{1}{3} \\
p_A(1) &= \frac{1}{3}(1 - 2D + \frac{3D^2}{2} + D - \frac{3D^2}{4} + D - \frac{3D^2}{4}) = \frac{1}{3} \\
p_A(2) &= \frac{1}{3}(1 - 2D + \frac{3D^2}{2} + D - \frac{3D^2}{4} + D - \frac{3D^2}{4}) = \frac{1}{3}
\end{aligned}
\tag{3.99}
$$

À partir de la définition 3.98, l'information mutuelle que Alice obtient est donnée par

$$
I^{AB} = \sum_{x,y} p(x)p(y|x)\log p(y|x) - \sum_y p(y)\log p(y) \tag{3.100}
$$

$$
= 1 + (1 - 2D + \frac{3D^2}{2})\log(1 - 2D + \frac{3D^2}{2}) + 2(D - \frac{3D^2}{4})\log(D - \frac{3D^2}{4}) \tag{3.101}
$$

En appliquant l'équation 3.97, Nous reformulons l'information mutuelle précédente 3.101 en utilisant le taux d'erreur quantique Q.

$$
I^{AB} = 1 + (1 - Q)\log(1 - Q) + Q\log\frac{Q}{2} \tag{3.102}
$$

B L'attaque optimale en termes de l'information mutuelle

Dans l'intention de dériver la stratégie d'interception optimale pour le protocole de distribution semi-quantique de clés en termes de l'information mutuelle partagée entre Alice et Eve, nous choisissons la deuxième bases comme étant la transformée de Fourier discrète de la base computationnelle définie de la manière suivante :

$$\begin{aligned}
|X\rangle_0 &= \frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), \\
|X\rangle_1 &= \frac{1}{\sqrt{3}}(|0\rangle + \eta|1\rangle + \eta^*|2\rangle), \\
|X\rangle_2 &= \frac{1}{\sqrt{3}}\left(|0\rangle + \eta^*|1\rangle + \eta|2\rangle\right).
\end{aligned} \tag{3.103}$$

Considérons uniquement les itérations où Alice encode son qutrit dans une base déterminée par les vecteurs $\{|X\rangle_0, |X\rangle_1, |X\rangle_2\}$, tandis que Bob choisit de réaliser une opération de réflexion. Par conséquent, le canal quantique bidirectionnel devient essentiellement un canal unidirectionnel, où Eve attaque à travers l'opérateur unitaire $V = U_R U_F$.

Comme précédemment, on suppose, sans perte de généralité, que l'ancilla d'Eve est initialisée à l'état $|0\rangle_E$, ce qui signifie que son action sur les états de base peut être décrite de la manière suivante

$$\begin{aligned}
V|0\rangle|0\rangle|0\rangle =& |0\rangle((1-D)|E^0_{0,00}\rangle + \frac{D}{2}|E^0_{1,01}\rangle + \frac{D}{2}|E^0_{2,02}\rangle) \\
&+ |1\rangle\left(\sqrt{\frac{D(1-D)}{2}}|E^1_{0,00}\rangle + \sqrt{\frac{D(1-D)}{2}}|E^1_{1,01}\rangle + \frac{D}{2}|E^1_{2,02}\rangle\right), \\
&+ |2\rangle\left(\sqrt{\frac{D(1-D)}{2}}|E^2_{0,00}\rangle + \frac{D}{2}|E^2_{1,01}\rangle + \sqrt{\frac{D(1-D)}{2}}|E^2_{2,02}\rangle\right), \\
V|1\rangle|0\rangle|0\rangle =& |0\rangle\left(\sqrt{\frac{D(1-D)}{2}}|E^0_{0,10}\rangle + \sqrt{\frac{D(1-D)}{2}}|E^0_{1,11}\rangle + \frac{D}{2}|E^0_{2,12}\rangle\right), \\
&+ |1\rangle(\frac{D}{2}|E^1_{0,10}\rangle + (1-D)|E^1_{1,11}\rangle + \frac{D}{2}|E^1_{2,12}\rangle) \\
&+ |2\rangle\left(\frac{D}{2}|E^2_{0,10}\rangle + \sqrt{\frac{D(1-D)}{2}}|E^2_{1,11}\rangle + \sqrt{\frac{D(1-D)}{2}}|E^2_{2,12}\rangle\right), \\
V|2\rangle|0\rangle|0\rangle =& |0\rangle\left(\sqrt{\frac{D(1-D)}{2}}|E^0_{0,20}\rangle + \sqrt{\frac{D(1-D)}{2}}|E^0_{2,22}\rangle + \frac{D}{2}|E^0_{1,21}\rangle\right), \\
&+ |1\rangle\left(\frac{D}{2}|E^1_{0,20}\rangle + \sqrt{\frac{D(1-D)}{2}}|E^1_{1,21}\rangle + \sqrt{\frac{D(1-D)}{2}}|E^1_{2,22}\rangle\right), \\
&+ |2\rangle(\frac{D}{2}|E^2_{1,21}\rangle + (1-D)|E^2_{2,22}\rangle + \frac{D}{2}|E^2_{0,20}\rangle),
\end{aligned} \tag{3.104}$$

Compte tenu de la propriété d'unitarité à la fois des opérateurs U_R et U_F, il en résulte que $V = U_R U_F$ conserve également cette propriété unitaire. Par conséquent, nous pouvons déduire :

$$
\begin{aligned}
&(1-D)\sqrt{\frac{D(1-D)}{2}}(\langle E^i_{i,ii}|E^i_{i,ji}\rangle + \langle E^i_{i,ii}|E^i_{j,jj}\rangle + \langle E^j_{i,ii}|E^j_{j,jj}\rangle + \langle E^j_{j,ij}|E^j_{j,jj}\rangle) \qquad (3.105)\\
&+ \frac{D(1-D)}{2}(\langle E^i_{i,ii}|E^i_{k,jk}\rangle + \langle E^j_{k,ik}|E^j_{j,jj}\rangle + \langle E^k_{i,ii}|E^k_{j,jj}\rangle + \langle E^k_{i,ii}|E^k_{k,jk}\rangle + \langle E^k_{k,ik}|E^k_{j,jj}\rangle\\
&+ \langle E^k_{k,ik}|E^k_{k,jk}\rangle) + \frac{D}{2}\frac{D}{2}(\langle E^i_{j,ij}|E^i_{k,jk}\rangle + \langle E^i_{k,ik}|E^i_{k,jk}\rangle + \langle E^j_{k,ik}|E^j_{i,ji}\rangle + \langle E^j_{k,ik}|E^j_{k,jk}\rangle + \langle E^k_{j,ij}|E^k_{i,ji}\rangle)\\
&+ \frac{D}{2}\sqrt{\frac{D(1-D)}{2}}(\langle E^i_{j,ij}|E^i_{i,ji}\rangle + \langle E^i_{j,ij}|E^i_{j,jj}\rangle + \langle E^i_{k,ik}|E^i_{i,ji}\rangle + \langle E^i_{k,ik}|E^i_{j,jj}\rangle + \langle E^j_{i,ii}|E^j_{i,ji}\rangle\\
&+ \langle E^j_{i,ii}|E^j_{k,jk}\rangle + \langle E^j_{j,ij}|E^j_{i,ji}\rangle + \langle E^j_{j,ij}|E^j_{k,jk}\rangle + \langle E^k_{i,ii}|E^k_{i,ji}\rangle + \langle E^k_{j,ij}|E^k_{j,jj}\rangle + \langle E^k_{j,ij}|E^k_{k,jk}\rangle\\
&+ \langle E^k_{k,ik}|E^k_{i,ji}\rangle) = 0
\end{aligned}
$$

$$
\begin{aligned}
&(1-D)(1-D)\langle E^i_{i,ii}|E^i_{i,ii}\rangle + \frac{D(1-D)}{2}(\langle E^i_{i,ii}|E^i_{j,ij}\rangle + \langle E^i_{i,ii}|E^i_{k,ik}\rangle + \langle E^i_{j,ij}|E^i_{i,ii}\rangle \qquad (3.106)\\
&+ \langle E^i_{k,ik}|E^i_{i,ii}\rangle + \langle E^j_{i,ii}|E^j_{i,ii}\rangle + \langle E^j_{i,ii}|E^j_{j,ij}\rangle + \langle E^j_{j,ij}|E^j_{i,ii}\rangle + \langle E^j_{j,ij}|E^j_{j,ij}\rangle + \langle E^k_{i,ii}|E^k_{i,ii}\rangle + \langle E^k_{i,ii}|E^k_{k,ik}\rangle\\
&+ \langle E^k_{k,ik}|E^k_{i,ii}\rangle + \langle E^k_{k,ik}|E^k_{k,ik}\rangle) + \frac{D}{2}\frac{D}{2}(\langle E^i_{j,ij}|E^i_{j,ij}\rangle + \langle E^i_{j,ij}|E^i_{k,ik}\rangle + \langle E^i_{k,ik}|E^i_{j,ij}\rangle + \langle E^i_{k,ik}|E^i_{k,ik}\rangle\\
&+ \langle E^j_{k,ik}|E^j_{k,ik}\rangle + \langle E^k_{j,ij}|E^k_{j,ij}\rangle) + \frac{D}{2}\sqrt{\frac{D(1-D)}{2}}(\langle E^j_{i,ii}|E^j_{k,ik}\rangle + \langle E^j_{j,ij}|E^j_{k,ik}\rangle + \langle E^j_{k,ik}|E^j_{i,ii}\rangle\\
&+ \langle E^j_{k,ik}|E^j_{j,ij}\rangle + \langle E^k_{i,ii}|E^k_{j,ij}\rangle + \langle E^k_{j,ij}|E^k_{i,ii}\rangle + \langle E^k_{j,ij}|E^k_{k,ik}\rangle + \langle E^k_{k,ik}|E^k_{j,ij}\rangle) = 1
\end{aligned}
$$

Nous restreignons notre analyse au cas des attaques symétriques, ce qui signifie qu'Eve est supposée introduire une perturbation équivalente à tous les états d'entrée possibles. Cette perturbation est exprimée par la forme suivante

$$D = 1 - F = 1 - Tr(|i\rangle\langle i|\rho_A)$$

Où $|i\rangle$ est l'un des états possibles envoyés par Alice et ρ_A désigne l'opérateur de densité réduit de l'état correspondant, transmis à Alice après avoir subi l'interaction avec Eve via l'opérateur unitaire V. Il convient de noter que cet opérateur conserve la même valeur pour les trois états d'entrée possibles.

Dans le cadre de la stratégie d'interception abordée dans cette section, nous définisons les termes *"Match"* et *"Mismatch"* pour désigner les résultats des mesures réalisées par Ève sur les qutrits transmis entre Alice et Bob. Plus précisément, le terme *"Match"* décrit la situation où Ève observe des résultats identiques dans les deux directions, tandis que le terme *"Mismatch"* se rapporte aux cas où Ève observe des résultats diffèrents dans ces deux directions.

En considérant le scénario du *"Match"*, nous examinons le taux d'erreur quantique, symbolisé par la variable Q_{Match}. Ce taux d'erreur est défini comme la proportion d'états initialement émis par Alice sous la forme $|i\rangle$, mais qui sont incorrectement interprétés comme des états $|j\rangle$, où $i, j = 0, 1, 2$ avec $i \neq j$

$$\begin{aligned} Q_{\text{Match}} &= \langle X_1|\rho^A_{X_0}|X_1\rangle = \langle X_1|\rho^A_{X_2}|X_1\rangle \\ &= \langle X_0|\rho^A_{X_1}|X_0\rangle = \langle X_2|\rho^A_{X_0}|X_2\rangle \\ &= \langle X_0|\rho^A_{X_2}|X_0\rangle = \langle X_2|\rho^A_{X_1}|X_2\rangle \end{aligned}$$

Nous supposons que le taux d'erreur est uniforme sur tous les états, *i.e* $Q_Z = Q_{Match}$. En exprimant la perturbation introduite par la transformation d'interception 3.104 comme une fonction des produits scalaires des états d'Eve, et en tenant compte de l'unitarité 3.95, nous obtenons une forme simple qui s'exprime comme suit :

$$s = \frac{2 - Q(3 + 2w)}{2}, \tag{3.107}$$

avec s représentant la situation où l'état parvient correctement à Alice, et w indiquant le cas où Alice détecte une erreur, nous pouvons classer les états de sortie dans w en trois ensembles distincts : le premier ensemble correspond aux situations où une erreur se produit lors de la transmission d'Alice à Bob, *i.e* canal direct, le deuxième ensemble correspond aux situations où une erreur se produit lors de la transmission de Bob à Alice, *i.e* canal inverse, et le troisième ensemble concerne les situations où des erreurs surviennent dans les deux canaux.

Pour évaluer l'efficacité de l'attaque d'écoute, nous allons à présent dériver la transformation d'interception optimale pour une valeur fixe Q du taux d'erreur. En d'autres termes, nous cherchons à maximiser l'information mutuelle I^{AE} entre Alice et Eve. Pour obtenir cette expression de l'information mutuelle entre Alice et Eve, nous introduisons une paramétrisation générale des états de sortie normalisés.

Dans le cadre de la paramétrisation relative aux cas où l'état est correctement reçu par Alice, les coefficients a et b peuvent être traités en tant que réels. La base $\{|\bar{0}\rangle, |\bar{1}\rangle, |\bar{2}\rangle\}$, étant orthonormale et orthogonale par rapport à tous les autres états auxiliaires, est utilisée. De cette manière, la probabilité pour Eve de deviner correctement l'état est a^2, tandis que la probabilité totale de commettre une erreur est de $1 - a^2 = 2b^2$.

Il convient de souligner que les trois autres ensembles d'états du w sont paramétrisés de manière similaire, où nous utilisons respectivement deux autres réels γ et λ, au lieu de a et b. De plus, la base $\{|\bar{0}\rangle, |\bar{1}\rangle, |\bar{2}\rangle\}$ est remplacée par trois autres bases orthogonales distinctes : $\{|\tilde{0}\rangle, |\tilde{1}\rangle, |\tilde{2}\rangle\}$, $\{|\hat{0}\rangle, |\hat{1}\rangle, |\hat{2}\rangle\}$ et $\{|\bar{\bar{0}}\rangle, |\bar{\bar{1}}\rangle, |\bar{\bar{2}}\rangle\}$. Néanmoins, une distinction s'opère entre ces trois ensembles d'états d'erreur : le premier ensemble englobe les situations où l'erreur réside dans le canal de retour, le deuxième concerne les cas où l'erreur se situe dans le canal d'aller, tandis que le troisième ensemble englobe les cas où une erreur affecte simultanément les deux canaux.

Cependant, la probabilité pour qu'Eve devine correctement le qutrit lorsque Alice le reçoit sans perturbation est a^2, tandis que lorsque l'état de Alice est perturbé, sa probabilité de deviner correctement le qutrit est γ^2. Ainsi, nous sommes en mesure de calculer la probabilité globale, symbolisée par P_E, pour laquelle Eve réussit à déterminer correctement le qutrit.

$$P_E = (1-Q)a^2 + Q\gamma^2. \tag{3.108}$$

En exploitant l'équation 3.107, les valeurs de a^2 et γ^2 peuvent être exprimées en fonction de Q et w.

$$a^2 \equiv f(Q,w) = \frac{1}{9}(3 + Q(3+2w) + 2\sqrt{2}\sqrt{-Q(3+2w)(-3+Q(3+2w))}), \tag{3.109}$$

$$\gamma^2 \equiv \phi(w) = \frac{1}{9}(5 - 2w - 4\sqrt{1+w-2w^2}), \tag{3.110}$$

En se basant sur ces probabilités, l'information mutuelle entre Alice et Ève, désignée par I^{AE} et dépendante du taux d'erreur Q ainsi que du paramètre w, peut être exprimée de la manière suivante :

$$\begin{aligned} I^{AE} = 1 &+ (1-Q)f(Q,w)\log_3(f(Q,w)) + (1-f(Q,w))\log_3(\frac{1-f(Q,w)}{2}) \\ &+ Q\phi(w)\log_3(\phi(w)) + (1-\phi(w))\log_3(\frac{1-\phi(w)}{2}). \end{aligned}$$

Après des manipulations algébriques, nous parvenons à démontrer que, pour une valeur fixe de Q, l'information mutuelle $I^{AE}(Q,w)$ atteint son maximum lorsque $\tilde{w} = \frac{2-3Q}{2(1+Q)}$. Cette valeur de $\tilde{w}$ correspond à $f(Q,\tilde{w}) = \phi(\tilde{w})$, et par conséquent, $I^{AE}(Q,\tilde{w})$ représente l'information mutuelle optimale entre Alice et Ève, adoptant la forme simple suivante :

$$I^{AE} = 1 + f(Q,\tilde{w})\log_3(f(Q,\tilde{w})) + (1-f(Q,\tilde{w}))\log_3(\frac{1-f(Q,\tilde{w})}{2}), \tag{3.111}$$

où $f(Q,\tilde{w})$ est donné par

$$f(Q,\tilde{w}) = \frac{3 + 8Q + 2\sqrt{10}\sqrt{Q(3-2Q)}}{9(1+Q)}.$$

Le résultat de l'information mutuelle optimale entre Alice et Eve, est graphiquement représenté dans la Figure 3.5. Comme il est clairement illustré, l'information mutuelle I^{AB} et I^{AE} se croisent au niveau de la valeur critique du taux d'erreur, correspondant à $Q = 17.5\%$. En dessous de cette valeur critique, le protocole offre une garantie de sécurité.

Lors de la dérivation de la stratégie optimale pour le scénario de *"Mismatch"*, où Ève, en tant qu'un espion, observe des résultats de mesure différents dans les deux directions, elle adopte une approche sélective. Plus précisément, elle rejette son estimation dans la canal inverse et se focalise uniquement sur son estimation dans la canal direct.

Conformément à la démarche précédente, nous aboutissons à ce que, pour une valeur fixe de Q, l'information mutuelle $I^{AE}(Q, w)$ est maximisée pour la valeur $\tilde{w} = 1 - \frac{3Q}{2}$. Par conséquent, $I^{AE}(Q, \tilde{w})$ représente l'information mutuelle optimale entre Alice et Ève, notée $I^{AE}(Q, \tilde{w})$, se simplifie comme suit :

$$I^{A\to E} = 1 + f(Q,\tilde{w})\log_3(f(Q,\tilde{w})) + (1 - f(Q,\tilde{w}))\log_3(\frac{1 - f(Q,\tilde{w})}{2}), \tag{3.112}$$

où $f(Q, \tilde{w})$ est donné par

$$f(Q,\tilde{w}) = \frac{1}{3}(1 + Q + 2\sqrt{2}\sqrt{Q(1-Q)}).$$

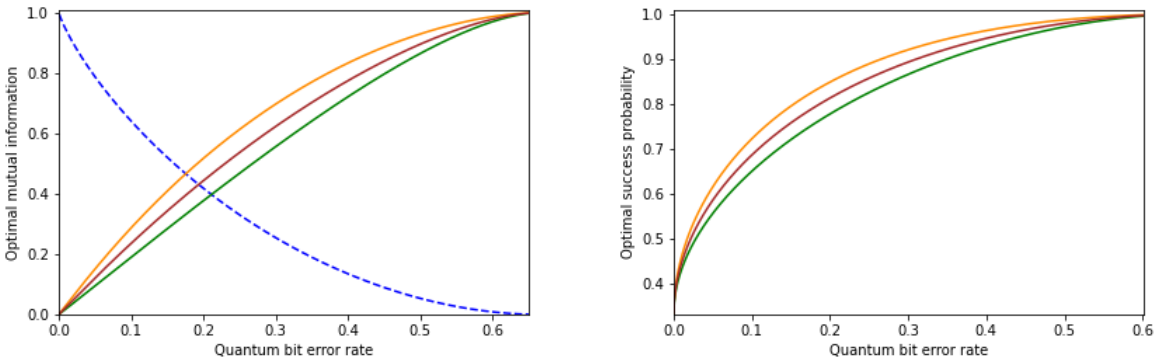


FIGURE 3.5 : La figure (a) représente l'information mutuelle I^{AE} et I^{AB} en fonction du taux d'erreur de bit quantique Q. La figure (b) illustre la probabilité de succès optimale en fonction du taux d'erreur de bit quantique. La ligne orange représente le cas du "Match", tandis que la ligne verte représente le cas du "Mismatch".

Nous observons que l'information partagée entre Alice et Eve, ainsi que l'information mutuelle I^{AB}, se croisent à un taux d'erreur Q plus élevé dans le contexte du scénario *"Mismatch"* par rapport au scénario *"Match"*. Plus précisément, nous identifions que Q atteint une valeur de 21.1% dans le cas du *"Mismatch"*, tandis que dans le cas du *"Match"*, cette valeur est de 17.5%. Cette observation signifie que la scénario de *"Mismatch"* est plus sécurisé en ce sens qu'il nécessite un niveau de perturbation plus élevé.

Par ailleurs, il convient de noter que la courbe illustrant la probabilité de réussite optimale d'Eve dans la Figure 3.5 en fonction du taux d'erreur Q met en évidence que cette stratégie d'interception permet à Eve d'acquérir une quantité d'information plus importante sur la clé partagée dans le cadre du scénario *"Match"*, par rapport à ce qui est réalisable dans le scénario *"Mismatch"* où l'interception par Eve se limite aux qutrits

transmis par Alice vers Bob.

Du fait que le protocole de distribution semi-quantique de clé repose sur un canal quantique bidirectionnel, Eve peut adopté une stratégie d'interception sophistiquée. Concrètement, lorsque les résultats observés par Eve dans les deux directions coïncident avec le même bit b, elle en conclut que ce bit b a été effectivement envoyé par Alice. Dans les cas où les résultats sont incohérents, Eve ne tient compte que des résultats du premier canal, (*i.e*, le canal direct). Cette stratégie de détection est illustrée par la ligne rouge dans les figures 3.5.

Notre analyse nous amène à conclure que la stratégie d'interception bidirectionnel appliquée au protocole de distribution de clé semi-quantique permet d'extraire une quantité supérieure de l'informations relatives à la clé partagée, comparativement à la stratégie d'interception de type unidirectionnelle.

VII L'attaque optimale appliquée sur des états bruités

Les travaux présentés dans cette section ont fait l'objet d'un article soumis en publication.

Notre recherche se concentre sur l'évaluation de la résistance du protocole de distribution semi-quantique de clés face à la stratégie d'interception la plus générale pour un ensemble d'états bidimensionnels lorsque les états sont soumis à un mélange avec un bruit blanc. Cette situation peut se produire soit par l'ajout délibéré de bruit par Alice aux états avant leur émission, soit par une situation réaliste où Ève ne peut pas remplacer le canal quantique bruité par un canal sans bruit.

Nous déterminons l'information mutuelle optimale entre Ève et Alice, dans le cas d'attaques individuelles, en fonction du taux d'erreur des qubits. Nos résultats mettent en évidence que l'ajout de bruit quantique réduit davantage l'information mutuelle d'Ève que celle de Bob.

A Le principe de fonctionnement du protocole

Dans cette section, nous proposons une version modifiée du protocole de distribution de clés semi-quantique (SQKD), appelé BKM07, introduit dans la section IV. Cette nouvelle version peut être utilisé selon l'un des deux configurations en fonction des capacités du utilisateur quantique : en CONFIG-2 seules deux bases sont utilisées, la base Z $\{|0\rangle, |1\rangle\}$ et la base X qui est définie comme suit

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad (3.113)$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

En CONFIG-3, l'utilisateur quantique utilise trois bases au lieu de deux. La troisième base, en plus des précédentes, est désignée par Y et est définie comme suit :

$$|R\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \tag{3.114}$$
$$|L\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

La phase de communication quantique du protocole se compose d'une série d'itérations jusqu'à ce qu'une clé brute suffisamment grande soit obtenue.

Transmission quantique

- En fonction de la configuration du protocole adopté, Alice, en tant qu'utilisateur quantique, choisie d'envoyer un état mixte plutôt qu'un état pur.

$$\rho_i = (1-p)|i\rangle\langle i| + \frac{p}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \tag{3.115}$$

  Lorsque la configuration est CONFIG-2, l'état $|i\rangle$ est défini dans l'ensemble $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. En revanche, dans le cas de la configuration CONFIG-3, l'état $|i\rangle$ appartient à l'ensemble $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |R\rangle, |L\rangle\}$. Le paramètre p est utilisé pour quantifier la quantité de bruit, avec sa valeur est comprise entre 0 et 1. Nous supposons que le bruit est uniforme dans toutes les bases, ce qui correspond à ce qu'on appelle le canal de déparisation.
- A la réception, l'utilisateur classique Bob, choisit aléatoirement entre deux opérations : une opération de réflexion, R, dans laquelle il renvoie simplement le qudit à Alice sans le perturber, ou une opération de mesure et de renvoi, M, dans laquelle il effectue une mesure dans la base Z.
- Alice effectue la mesure du qubit de retour dans la même base que celle utilisée initialement.

Réconciliation des clés et estimation de paramètres

- Alice et Bob échangent leurs information quantiques à l'aide d'un canal de communication authentifié. Alice divulgue la base utilisée pour préparer le qubit, tandis que Bob révèle son choix d'opération : mesurer (M) ou réflexion (R).
  - Les itérations lors desquels Alice choisit la base Z et Bob effectue l'opération de mesure et de renvoi(M), Alice et Bob conservent leurs résultats respectifs pour contribuer à leur clé brute.
  - Dans le cas où la condition précédente n'est pas satisfaite, Les itérations sont utilisées ultérieurement pour vérifier la présence éventuelle d'une tentative d'interception par Eve. Si le taux d'erreur quantique (QBER) dépasse un seuil prédéfini, Alice informe Bob pour qu'il abandonne le protocole. Cependant, si QBER demeure en dessous, Alice et Bob rejettent toutes les itérations de CTRL précédentes et poursuivent le protocole.

Suite à la phase de communication quantique, et sous l'hypothèse d'un niveau de bruit suffisamment faible, la correction d'erreurs suivie de l'amplification de confidentialité permettra de générer une clé secrète. Ces étapes sont des processus standard et pour obtenir plus d'informations, le lecteur est renvoyé à la sous-section A du chapitre 2.

B Analyse de sécurité

Notre étude se focalise sur le scénario où un l'intercepteur, Eve, perturbe tous les états quantiques possibles de manière équivalente, c'est-à-dire que Eve est autorisée à interagir de manière individuelle chaque état quantique, qubit, avec une sonde quantique et le stoker dans une mémoire quantique. Par la suite, elle effectue une mesure sur chacun de ces sondes individuellement après la révélation des données de correction d'erreur et d'amplification de confidentialité.

Une attaque individuelle contre un protocole semi-quantique peut être modélisée de manière générale, sans perte de généralité, par une paire d'opérateurs (U_F, U_R) agissant sur l'espace de Hilbert $\mathcal{H}_T \otimes \mathcal{H}_E$, où $\mathcal{H}_T$ représente l'espace de Hilbert bidimensionnel qui modélise le qubit en transit entre Alice et Bob, et ultérieurement entre Bob et Alice, tandis que $\mathcal{H}_E$ représente l'espace de Hilbert modélisant la mémoire quantique de Eve.

Conformément à la convention, la première base du protocole correspond à la base de calcul $\{|0\rangle, |1\rangle\}$, symbolisée par Z dans un espace de Hilbert bidimensionnel. Par conséquent, la stratégie d'interception symétrique la plus générale que Eve peut concevoir pour les qubits peut être formulée comme suit

$$\begin{aligned} U|0\rangle|0\rangle &= \sqrt{1-D}|0\rangle|E_{00}\rangle + \sqrt{D}|1\rangle|E_{01}\rangle \\ U|1\rangle|0\rangle &= \sqrt{D}|0\rangle|E_{10}\rangle + \sqrt{1-D}|1\rangle|E_{11}\rangle \end{aligned} \tag{3.116}$$

où D est la perturbation introduite par Ève et $F = 1 - D$ est la mesure de fidélité de l'état parvenant Bob après l'attaque d'écoute clandestine. Nous avons indiqué par $|0\rangle$ l'état initial du système d'Ève, tandis que ses états après l'interaction sont désignés par $|E_{00}\rangle, |E_{01}\rangle, |E_{10}\rangle$, et $|E_{11}\rangle$ et sont tous normalisés.

Afin de satisfaire l'unitarité de U_F, les produits scalaires entre les états de sortie d'Ève doivent obéir à des relations de la forme :

$$\langle E_{00}|E_{10}\rangle + \langle E_{01}|E_{11}\rangle = 0$$

$$(1-D)\langle E_{00}|E_{00}\rangle + D\langle E_{01}|E_{01}\rangle = 1$$

$$(1-D)\langle E_{11}|E_{11}\rangle + D\langle E_{10}|E_{10}\rangle = 1$$

Incontestablement, le qubit de Bob subit une transformation unitaire U_R sur le canal de retour, ce qui conduit à la formation de l'état quantique global final :

$$U|i\rangle|e_{ij}\rangle = \sqrt{1-D}|i\rangle|E^i_{i,ij}\rangle + \sqrt{D}|j\rangle|E^j_{i,ij}\rangle \tag{3.117}$$

En conditionnant sur le fait que cette itération est utilisée pour contribuer à la clé brute, Alice envoie $|0\rangle$ ou $|1\rangle$ avec une probabilité de 1/2 chacun. Eve intervient ensuite en altérant le qubit en utilisant U_F, puis le transmet à Bob qui effectue une mesure dans la base Z, renvoyant le résultat de mesure sous forme d'un nouveau qubit. Eve intervient une nouvelle fois en utilisant U_R pour altérer ce nouveau qubit. Ceci conduit à l'opérateur de densité suivant

$$\begin{aligned}
\rho_0^{BE} = &\left(1-\frac{p}{2}\right)\{|0\rangle\langle 0|((1-D)^2|E^0_{0,00}\rangle\langle E^0_{0,00}| + D^2|E^0_{1,01}\rangle\langle E^0_{1,01}|) \\
&+ |0\rangle\langle 1|\left((1-D)\sqrt{D(1-D)}|E^0_{0,00}\rangle\langle E^1_{0,00}| + D\sqrt{D(1-D)}|E^0_{1,01}\rangle\langle E^1_{1,01}|\right) \\
&+ |1\rangle\langle 0|\left((1-D)\sqrt{D(1-D)}|E^1_{0,00}\rangle\langle E^0_{0,00}| + D\sqrt{D(1-D)}|E^1_{1,01}\rangle\langle E^0_{1,01}|\right) \\
&+ |1\rangle\langle 1|(D(1-D)|E^1_{0,00}\rangle\langle E^1_{0,00}| + D(1-D)|E^1_{1,01}\rangle\langle E^1_{1,01}|)\} \\
&+ \frac{p}{2}\{|0\rangle\langle 0|((1-D)D|E^0_{1,11}\rangle\langle E^0_{1,11}| + D(1-D)|E^0_{0,10}\rangle\langle E^0_{0,10}|) \\
&+ |0\rangle\langle 1|\left((1-D)\sqrt{D(1-D)}|E^0_{1,11}\rangle\langle E^1_{1,11}| + D\sqrt{D(1-D)}|E^0_{0,10}\rangle\langle E^1_{0,10}|\right) \\
&+ |1\rangle\langle 0|\left((1-D)\sqrt{D(1-D)}|E^1_{1,11}\rangle\langle E^0_{1,11}| + D\sqrt{D(1-D)}|E^1_{0,10}\rangle\langle E^0_{0,10}|\right) \\
&+ |1\rangle\langle 1|((1-D)^2|E^1_{1,11}\rangle\langle E^1_{1,11}| + D^2|E^1_{0,10}\rangle\langle E^1_{0,10}|)\}
\end{aligned}$$

$$\begin{aligned}
\rho_1^{BE} = &\left(1-\frac{p}{2}\right)\{|0\rangle\langle 0|((1-D)D|E^0_{1,11}\rangle\langle E^0_{1,11}| + D(1-D)|E^0_{0,10}\rangle\langle E^0_{0,10}|) \\
&+ |0\rangle\langle 1|\left((1-D)\sqrt{D(1-D)}|E^0_{1,11}\rangle\langle E^1_{1,11}| + D\sqrt{D(1-D)}|E^0_{0,10}\rangle\langle E^1_{0,10}|\right) \\
&+ |1\rangle\langle 0|\left((1-D)\sqrt{D(1-D)}|E^1_{1,11}\rangle\langle E^0_{1,11}| + D\sqrt{D(1-D)}|E^1_{0,10}\rangle\langle E^0_{0,10}|\right) \\
&+ |1\rangle\langle 1|((1-D)^2|E^1_{1,11}\rangle\langle E^1_{1,11}| + D^2|E^1_{0,10}\rangle\langle E^1_{0,10}|)\} \\
&+ \frac{p}{2}\{|0\rangle\langle 0|((1-D)^2|E^0_{0,00}\rangle\langle E^0_{0,00}| + D^2|E^0_{1,01}\rangle\langle E^0_{1,01}|) \\
&+ |0\rangle\langle 1|\left((1-D)\sqrt{D(1-D)}|E^0_{0,00}\rangle\langle E^1_{0,00}| + D\sqrt{D(1-D)}|E^0_{1,01}\rangle\langle E^1_{1,01}|\right) \\
&+ |1\rangle\langle 0|\left((1-D)\sqrt{D(1-D)}|E^1_{0,00}\rangle\langle E^0_{0,00}| + D\sqrt{D(1-D)}|E^1_{1,01}\rangle\langle E^0_{1,01}|\right) \\
&+ |1\rangle\langle 1|(D(1-D)|E^1_{0,00}\rangle\langle E^1_{0,00}| + D(1-D)|E^1_{1,01}\rangle\langle E^1_{1,01}|)\}
\end{aligned}$$

Le taux d'erreur quantique dans la base Z est représenté par Q_Z et est exprimé comme la fraction des états $|0\rangle$, $|1\rangle$, initialement envoyés par Alice, mais qui sont interprétés comme des états $|1\rangle$, $|0\rangle$

$$\begin{aligned} Q_Z &= \frac{1}{2}\langle 1|\rho_0^A|1\rangle + \frac{1}{2}\langle 0|\rho_1^A|0\rangle, \\ &= 2D(1-D1)(1-p) + \frac{p}{2}, \end{aligned} \tag{3.118}$$

où ρ_0^A et ρ_1^A sont des opérateurs de densité réduit correspondant aux états que Alice reçoit lorsqu'elle envoie initialement $|0\rangle$ et $|1\rangle$ respectivement.

Considérons l'information mutuelle entre deux variables aléatoires X et Y, avec des valeurs possibles x et y respectivement. Cette mesure, notée I_{XY}, permet de quantifier la quantité d'information commune entre ces deux variables. Elle est définie mathématiquement de la manière suivante :

$$I(X:Y) \;=\; \sum_{x\in X}\sum_{y\in Y} p(x,y)\log p(y|x) - \sum_{y\in Y} p(y)\log p(y), \tag{3.119}$$

où $p(x,y) = p(x)p(y|x)$ est la probabilité conjointe de X et Y, et $p(y|x)$ est la probabilité conditionnelle de y sachant x. Toutes les opérations logarithmiques sont effectuées en utilisant une base 2. Nous déterminons mesure de la quantité de l'information que Alice extrait de son état initial.

Les probabilités conditionnelles dans les cas où Alice mesure le qubit renvoyé dans l'état $|j\rangle$ lorsqu'elle l'a initialement préparé dans l'état $|i\rangle$ sont

$$\begin{aligned} p(0|\rho_0^A) &= (1-\frac{p}{2})((1-D)^2+D^2) + \frac{p}{2}(2D(1-D)) \\ p(1|\rho_0^A) &= (1-\frac{p}{2})(2D(1-D)) + \frac{p}{2}((1-D)^2+D^2) \\ p(0|\rho_1^A) &= (1-\frac{p}{2})(2D(1-D)) + \frac{p}{2}((1-D)^2+D^2) \\ p(1|\rho_1^A) &= (1-\frac{p}{2})((1-D)^2+D^2) + \frac{p}{2}(2D(1-D)) \end{aligned} \tag{3.120}$$

Considérons $p_A(0)$, $p_A(1)$ la probabilité respectives que son bit soit zéro ou un.

$$\begin{aligned} p_A(0) &= \frac{1}{2}((1-\frac{p}{2})((1-D)^2+D^2) + \frac{p}{2}(2D(1-D)) + (1-\frac{p}{2})(2D(1-D)) \\ &\quad + \frac{p}{2}((1-D)^2+D^2)) = \frac{1}{2} \\ p_A(1) &= \frac{1}{2}((1-\frac{p}{2})(2D(1-D)) + \frac{p}{2}((1-D)^2+D^2) + (1-\frac{p}{2})((1-D)^2+D^2) \\ &\quad + \frac{p}{2}(2D(1-D))) = \frac{1}{2} \end{aligned}$$

D'après la définition 3.119, l'information mutuelle que Alice obtient est

$$\begin{aligned} I^{AB} = 1 &+ (1 + 2D(-1 + D + p - Dp - \frac{p}{2})) \log(1 + 2D(-1 + D + p - Dp - \frac{p}{2})) \\ &+ (2D(1 - D)(1 - p) + \frac{p}{2}) \log(2D(1 - D)(1 - p) + \frac{p}{2}). \end{aligned} \tag{3.121}$$

En utilisant l'équation 3.118, nous pouvons réexprimer l'information mutuelle précédente 3.121 en fonction du taux d'erreur quantique Q.

$$I^{AB} = 1 + (1 - Q) \log(1 - Q) + Q \log Q. \tag{3.122}$$

L'attaque optimale pour CONFIG-2

En utilisant notre protocole en CONFIG-2, nous considérons uniquement les itérations où Alice choisit d'encoder son qubit en utilisant la base X déterminée par les vecteurs $\{|+\rangle, |-\rangle\}$, donnée dans l'équation ci-dessous, et où Bob opte pour l'opération de réflexion.

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ |-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned} \tag{3.123}$$

En raison du choix de Bob d'opter pour l'opération de réflexion, le canal quantique bidirectionnel devient essentiellement un canal unidirectionnel, à travers lequel Eve mène des attaques en utilisant l'opérateur unitaire $V = U_R U_F$.

Comme précédemment, nous supposons, sans perte de généralité, que l'ancilla d'Eve est initialement dans l'état $|0\rangle_E$, ce qui signifie que son action sur les états de base peut être décrite de la manière suivante :

$$\begin{aligned} V|0\rangle|0\rangle|0\rangle =& |0\rangle((1 - D)|E^0_{0,00}\rangle + D|E^0_{1,01}\rangle) \\ &+ |1\rangle \left(\sqrt{D(1 - D)}|E^1_{0,00}\rangle + \sqrt{D(1 - D)}|E^1_{1,01}\rangle\right), \\ V|1\rangle|0\rangle|0\rangle =& |0\rangle \left(\sqrt{D(1 - D)}|E^0_{0,10}\rangle + \sqrt{D(1 - D)}|E^0_{1,11}\rangle\right) \\ &+ |1\rangle(D|E^1_{0,10}\rangle + (1 - D)|E^1_{1,11}\rangle). \end{aligned} \tag{3.124}$$

Du fait que U_R et U_F sont tous deux des opérateurs unitaires, il en découle que $V = U_R U_F$ est également un opérateur unitaire, ce qui engendre

$$(1-D)^2\langle E^0_{0,00}|E^0_{0,00}\rangle + D(1-D)[\langle E^0_{0,00}|E^0_{1,01}\rangle + \langle E^0_{1,01}|E^0_{0,00}\rangle + \langle E^1_{0,00}|E^1_{0,00}\rangle + \langle E^1_{0,00}|E^1_{1,01}\rangle + \langle E^1_{1,01}|E^1_{0,00}\rangle + \langle E^1_{1,01}|E^1_{1,01}\rangle] + D^2\langle E^0_{1,01}|E^0_{1,01}\rangle = 1$$

$$D(1-D)(\langle E^0_{0,10}|E^0_{0,10}\rangle + \langle E^0_{0,10}|E^0_{1,11}\rangle + \langle E^0_{1,11}|E^0_{0,10}\rangle + \langle E^0_{1,11}|E^0_{1,11}\rangle + \langle E^1_{0,10}|E^1_{1,11}\rangle + \langle E^1_{1,11}|E^1_{0,10}\rangle) + D^2\langle E^1_{0,10}|E^1_{0,10}\rangle + (1-D)^2\langle E^1_{1,11}|E^1_{1,11}\rangle = 1$$

$$(1-D)\sqrt{D(1-D)}(\langle E^0_{0,00}|E^0_{0,10}\rangle + \langle E^0_{0,00}|E^0_{1,11}\rangle + \langle E^1_{0,00}|E^1_{1,11}\rangle + \langle E^1_{1,01}|E^1_{1,11}\rangle) + D\sqrt{D(1-D)}(\langle E^0_{1,01}|E^0_{0,10}\rangle + \langle E^0_{1,01}|E^0_{1,11}\rangle + \langle E^1_{0,00}|E^1_{0,10}\rangle + \langle E^1_{1,01}|E^1_{0,10}\rangle) = 0$$

En utilisant l'attaque décrite ci-dessus, nous avons la possibilité de procéder au calcul de l'état du système résultant, que nous noterons ρ_i^{BE} avec $i = \{+, -\}$:

$$\begin{aligned}
\rho_+^{BE} =& \frac{1}{2}\{|0\rangle\langle 0|((1-D)^2|E^0_{0,00}\rangle\langle E^0_{0,00}| + D(1-D)(|E^0_{0,00}\rangle\langle E^0_{1,01}| + |E^0_{1,01}\rangle\langle E^0_{0,00}| + \\
& |E^0_{0,10}\rangle\langle E^0_{0,10}| + |E^0_{0,10}\rangle\langle E^0_{1,11}| + |E^0_{1,11}\rangle\langle E^0_{0,10}| + |E^0_{1,11}\rangle\langle E^0_{1,11}|) + D^2|E^0_{1,01}\rangle\langle E^0_{1,01}|) \\
& + |0\rangle\langle 1|(D\sqrt{D(1-D)}(|E^0_{1,01}\rangle\langle E^1_{0,00}| + |E^0_{1,01}\rangle\langle E^1_{1,01}| + |E^0_{0,10}\rangle\langle E^1_{0,10}| + |E^0_{1,11}\rangle\langle E^1_{0,10}|) \\
& + (1-D)\sqrt{D(1-D)}(|E^0_{0,00}\rangle\langle E^1_{0,00}| + |E^0_{0,00}\rangle\langle E^1_{1,01}| + |E^0_{0,10}\rangle\langle E^1_{1,11}| + |E^0_{1,11}\rangle\langle E^1_{1,11}|)) \\
& + |1\rangle\langle 0|(D\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^0_{1,01}| + |E^1_{1,01}\rangle\langle E^0_{1,01}| + |E^1_{0,10}\rangle\langle E^0_{0,10}| + |E^1_{0,10}\rangle\langle E^0_{1,11}| \\
& + (1-D)\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^0_{0,00}| + |E^1_{1,01}\rangle\langle E^0_{0,00}| + |E^1_{1,11}\rangle\langle E^0_{0,10}| + |E^1_{1,11}\rangle\langle E^0_{1,11}|)) \\
& + |1\rangle\langle 1|((1-D)^2|E^1_{1,11}\rangle\langle E^1_{1,11}| + D(1-D)(|E^1_{0,00}\rangle\langle E^1_{0,00}| + |E^1_{0,00}\rangle\langle E^1_{1,01}| + \\
& |E^1_{1,01}\rangle\langle E^1_{0,00}| + |E^1_{1,01}\rangle\langle E^1_{1,01}| + |E^1_{0,10}\rangle\langle E^1_{1,11}| + |E^1_{1,11}\rangle\langle E^1_{0,10}|) + D^2|E^1_{0,10}\rangle\langle E^1_{0,10}|)\} \\
& + \frac{1}{2}(1-p)\{|0\rangle\langle 0|((1-D)\sqrt{D(1-D)}(|E^0_{0,00}\rangle\langle E^0_{0,10}| + |E^0_{0,00}\rangle\langle E^0_{1,11}| + |E^0_{0,10}\rangle\langle E^0_{0,00}| \\
& + |E^0_{1,11}\rangle\langle E^0_{0,00}|) + D\sqrt{D(1-D)}(|E^0_{1,01}\rangle\langle E^0_{0,10}| + |E^0_{1,01}\rangle\langle E^0_{1,11}| + |E^0_{0,10}\rangle\langle E^0_{1,01}| \\
& + |E^0_{1,11}\rangle\langle E^0_{1,01}|)) \\
& + |0\rangle\langle 1|((1-D)^2|E^0_{0,00}\rangle\langle E^1_{1,11}| + D(1-D)(|E^0_{0,00}\rangle\langle E^1_{0,10}| + |E^0_{1,01}\rangle\langle E^1_{1,11}| \\
& + |E^0_{0,10}\rangle\langle E^1_{0,00}| + |E^0_{0,10}\rangle\langle E^1_{1,01}| + |E^0_{1,11}\rangle\langle E^1_{0,00}| + |E^0_{1,11}\rangle\langle E^1_{1,01}|) + D^2|E^0_{1,01}\rangle\langle E^1_{0,10}|) \\
& + |1\rangle\langle 0|((1-D)^2|E^1_{1,11}\rangle\langle E^0_{0,00}| + D(1-D)(|E^1_{0,00}\rangle\langle E^0_{0,10}| + |E^1_{0,00}\rangle\langle E^0_{1,11}| \\
& + |E^1_{1,01}\rangle\langle E^0_{0,10}| + |E^1_{1,01}\rangle\langle E^0_{1,11}| + |E^1_{0,10}\rangle\langle E^0_{0,00}| + |E^1_{1,11}\rangle\langle E^0_{1,01}|) + D^2|E^1_{0,10}\rangle\langle E^0_{1,01}|) \\
& + |1\rangle\langle 1|((1-D)\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^1_{1,11}| + |E^1_{1,01}\rangle\langle E^1_{1,11}| + |E^1_{1,11}\rangle\langle E^1_{0,00}| \\
& + |E^1_{1,11}\rangle\langle E^1_{1,01}|) \\
& + D\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^1_{0,10}| + |E^1_{1,01}\rangle\langle E^1_{0,10}| + |E^1_{0,10}\rangle\langle E^1_{0,00}| + |E^1_{0,10}\rangle\langle E^1_{1,01}|))\}
\end{aligned}$$

$$
\begin{aligned}
\rho_{-}^{BE} =& \frac{1}{2}\{|0\rangle\langle 0|((1-D)^2|E^0_{0,00}\rangle\langle E^0_{0,00}| + D(1-D)(|E^0_{0,00}\rangle\langle E^0_{1,01}| + |E^0_{1,01}\rangle\langle E^0_{0,00}| \\
&+ |E^0_{0,10}\rangle\langle E^0_{0,10}| + |E^0_{0,10}\rangle\langle E^0_{1,11}| + |E^0_{1,11}\rangle\langle E^0_{0,10}| + |E^0_{1,11}\rangle\langle E^0_{1,11}|) + D^2|E^0_{1,01}\rangle\langle E^0_{1,01}|) \\
&+ |0\rangle\langle 1|((1-D)\sqrt{D(1-D)}(|E^0_{0,00}\rangle\langle E^1_{0,00}| + |E^0_{0,00}\rangle\langle E^1_{1,01}| + |E^0_{0,10}\rangle\langle E^1_{1,11}| \\
&+ |E^0_{1,11}\rangle\langle E^1_{1,11}|) \\
&+ D\sqrt{D(1-D)}(|E^0_{1,01}\rangle\langle E^1_{0,00}| + |E^0_{1,01}\rangle\langle E^1_{1,01}| + |E^0_{0,10}\rangle\langle E^1_{0,10}| + |E^0_{1,11}\rangle\langle E^1_{0,10}|)) \\
&+ |1\rangle\langle 0|(D\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^0_{1,01}| + |E^1_{1,01}\rangle\langle E^0_{1,01}| + |E^1_{0,10}\rangle\langle E^0_{0,10}| + |E^1_{0,10}\rangle\langle E^0_{1,11}|) \\
&+ (1-D)\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^0_{0,00}| + |E^1_{1,01}\rangle\langle E^0_{0,00}| + |E^1_{1,11}\rangle\langle E^0_{0,10}| + |E^1_{1,11}\rangle\langle E^0_{1,11}|)) \\
&+ |1\rangle\langle 1|((1-D)^2|E^1_{1,11}\rangle\langle E^1_{1,11}| + D(1-D)(|E^1_{0,00}\rangle\langle E^1_{0,00}| + |E^1_{0,00}\rangle\langle E^1_{1,01}| \\
&+ |E^1_{1,01}\rangle\langle E^1_{0,00}| + |E^1_{1,01}\rangle\langle E^1_{1,01}| + |E^1_{0,10}\rangle\langle E^1_{1,11}| + |E^1_{1,11}\rangle\langle E^1_{0,10}|) + D^2|E^1_{0,10}\rangle\langle E^1_{0,10}|)\} \\
&- \frac{1}{2}(1-p)\{|0\rangle\langle 0|((1-D)\sqrt{D(1-D)}(|E^0_{0,00}\rangle\langle E^0_{0,10}| + |E^0_{0,00}\rangle\langle E^0_{1,11}| + |E^0_{0,10}\rangle\langle E^0_{0,00}| \\
&+ |E^0_{1,11}\rangle\langle E^0_{0,00}|) + D\sqrt{D(1-D)}(|E^0_{1,01}\rangle\langle E^0_{0,10}| + |E^0_{1,01}\rangle\langle E^0_{1,11}| + |E^0_{0,10}\rangle\langle E^0_{1,01}| \\
&+ |E^0_{1,11}\rangle\langle E^0_{1,01}|)) \\
&+ |0\rangle\langle 1|((1-D)^2|E^0_{0,00}\rangle\langle E^1_{1,11}| + D(1-D)(|E^0_{0,00}\rangle\langle E^1_{0,10}| + |E^0_{1,01}\rangle\langle E^1_{1,11}| \\
&+ |E^0_{0,10}\rangle\langle E^1_{0,00}| + |E^0_{0,10}\rangle\langle E^1_{1,01}| + |E^0_{1,11}\rangle\langle E^1_{0,00}| + |E^0_{1,11}\rangle\langle E^1_{1,01}|) + D^2|E^0_{1,01}\rangle\langle E^1_{0,10}|) \\
&+ |1\rangle\langle 0|((1-D)^2|E^1_{1,11}\rangle\langle E^0_{0,00}| + D(1-D)(|E^1_{0,00}\rangle\langle E^0_{0,10}| + |E^1_{0,00}\rangle\langle E^0_{1,11}| \\
&+ |E^1_{1,01}\rangle\langle E^0_{0,10}| + |E^1_{1,01}\rangle\langle E^0_{1,11}| + |E^1_{0,10}\rangle\langle E^0_{0,00}| + |E^1_{1,11}\rangle\langle E^0_{1,01}|) + D^2|E^1_{0,10}\rangle\langle E^0_{1,01}|) \\
&+ |1\rangle\langle 1|(D\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^1_{0,10}| + |E^1_{1,01}\rangle\langle E^1_{0,10}| + |E^1_{0,10}\rangle\langle E^1_{0,00}| + |E^1_{0,10}\rangle\langle E^1_{1,01}|) \\
&+ (1-D)\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^1_{1,11}| + |E^1_{1,01}\rangle\langle E^1_{1,11}| + |E^1_{1,11}\rangle\langle E^1_{0,00}| + |E^1_{1,11}\rangle\langle E^1_{1,01}|))\}
\end{aligned}
$$

Le taux d'erreur quantique dans la base X, noté Q_X, correspond à la proportion des états initiaux $|i\rangle$ émis par Alice, mais qui sont interprétés comme des états $|j\rangle$ par Alice pour $i, j = \{+, -\}$, et il est défini comme suit :

$$Q_X = \langle +|\rho_{-}^{A}|+\rangle = \langle +|\rho_{-}^{A}|+\rangle,$$

avec ρ_{+}^{A} et ρ_{-}^{A}, les opérateurs de densité réduite sont obtenus en effectuant une opération de trace partielle sur ρ_{i}^{BE} pour éliminer l'état d'Eve. Les expressions pour $\langle +|\rho_{-}^{A}|+\rangle$ et $\langle -|\rho_{-}^{A}|-\rangle$ sont déterminées par :

$$
\begin{aligned}
\langle -|\rho_{+}^{A}|-\rangle =& \frac{1}{2}\{1 - (1-D)\sqrt{D(1-D)}Re(\langle E^0_{0,00}|E^1_{0,00}\rangle + \langle E^0_{0,00}|E^1_{1,01}\rangle + \langle E^0_{0,10}|E^1_{1,11}\rangle + \langle E^0_{1,11}|E^1_{1,11}\rangle) \\
&- D\sqrt{D(1-D)}Re(\langle E^0_{1,01}|E^1_{0,00}\rangle + \langle E^0_{1,01}|E^1_{1,01}\rangle + \langle E^0_{0,10}|E^1_{0,10}\rangle + \langle E^0_{1,11}|E^1_{0,10}\rangle)\} \\
&- \frac{1}{2}(1-p)\{(1-D)^2Re(\langle E^0_{0,00}|E^1_{1,11}\rangle) + D^2Re(\langle E^0_{1,01}|E^1_{0,10}\rangle) + D(1-D)Re(\langle E^0_{0,10}|E^1_{0,00}\rangle \\
&+ \langle E^0_{1,11}|E^1_{0,00}\rangle + \langle E^0_{0,10}|E^1_{1,01}\rangle + \langle E^0_{1,11}|E^1_{1,01}\rangle + \langle E^0_{0,00}|E^1_{0,10}\rangle + \langle E^0_{1,01}|E^1_{1,11}\rangle)\}
\end{aligned}
\tag{3.125}
$$

$$\begin{aligned}\langle +|\rho_-^A|+\rangle = \frac{1}{2}\{1+(1-D)\sqrt{D(1-D)}Re(\langle E^0_{0,00}|E^1_{0,00}\rangle + \langle E^0_{0,00}|E^1_{1,01}\rangle + \langle E^0_{0,10}|E^1_{1,11}\rangle + \langle E^0_{1,11}|E^1_{1,11}\rangle)\\ + D\sqrt{D(1-D)}Re(\langle E^0_{1,01}|E^1_{0,00}\rangle + \langle E^0_{1,01}|E^1_{1,01}\rangle + \langle E^0_{0,10}|E^1_{0,10}\rangle + \langle E^0_{1,11}|E^1_{0,10}\rangle)\}\\ - \frac{1}{2}(1-p)\{(1-D)^2Re(\langle E^0_{0,00}|E^1_{1,11}\rangle) + D^2Re(\langle E^0_{1,01}|E^1_{0,10}\rangle) + D(1-D)Re(\langle E^0_{0,10}|E^1_{0,00}\rangle\\ + \langle E^0_{1,11}|E^1_{0,00}\rangle + \langle E^0_{0,10}|E^1_{1,01}\rangle + \langle E^0_{1,11}|E^1_{1,01}\rangle + \langle E^0_{0,00}|E^1_{0,10}\rangle + \langle E^0_{1,01}|E^1_{1,11}\rangle)\}\end{aligned} \tag{3.126}$$

L'inégalité établie par les équations 3.125 et 3.126 entraîne la restriction suivante sur les états d'Eve.

$$\begin{aligned}(1-D)\sqrt{D(1-D)}Re(\langle E^0_{0,00}|E^1_{0,00}\rangle + \langle E^0_{0,00}|E^1_{1,01}\rangle + \langle E^0_{0,10}|E^1_{1,11}\rangle + \langle E^0_{1,11}|E^1_{1,11}\rangle)\\ + D\sqrt{D(1-D)}Re(\langle E^0_{1,01}|E^1_{0,00}\rangle + \langle E^0_{1,01}|E^1_{1,01}\rangle + \langle E^0_{0,10}|E^1_{0,10}\rangle + \langle E^0_{1,11}|E^1_{0,10}\rangle) = 0\end{aligned}$$

Par conséquent, nous obtenons

$$\begin{aligned}QX = \frac{1}{2} - \frac{1}{2}(1-p)((1-D)^2Re(\langle E^0_{0,00}|E^1_{1,11}\rangle) + D^2Re(\langle E^0_{1,01}|E^1_{0,10}\rangle)\\ + D(1-D)Re(\langle E^0_{0,10}|E^1_{0,00}\rangle + \langle E^0_{1,11}|E^1_{0,00}\rangle\\ + \langle E^0_{0,10}|E^1_{1,01}\rangle + \langle E^0_{1,11}|E^1_{1,01}\rangle + \langle E^0_{0,00}|E^1_{0,10}\rangle + \langle E^0_{1,01}|E^1_{1,11}\rangle))\end{aligned} \tag{3.127}$$

Comme le bruit est supposé uniforme, nous supposons qu'Eve utilise une stratégie qui produit le même taux d'erreur de bit quantique dans les deux bases :

$$Q = Q_Z = Q_X$$

Nous sommes maintenant en mesure d'identifier quatre ensembles orthogonaux d'états de sortie, à savoir $\{|E^0_{0,00}\rangle, |E^1_{1,11}\rangle\}, \{|E^0_{1,01}\rangle, |E^1_{0,10}\rangle\}, \{|E^1_{1,01}\rangle, |E^0_{0,10}\rangle\}, \{|E^1_{0,00}\rangle, |E^0_{1,11}\rangle\}$. Le premier et Le deuxième ensemble correspond au cas où l'état est correctement reçu par Alice, ce qui se produit avec une probabilité $(1-D)^2$ et D^2. Le troisième et le quatrième ensembles correspondent aux cas où Alice obtient une erreur, cela se produit avec une probabilité totale $D(1-D)$.

Nous allons dériver la transformation d'interception optimale pour une valeur fixe D de la perturbation, en maximisant l'information mutuelle I^{AE} entre Alice et Eve. Pour ce faire, nous introduisons une paramétrisation générale des états de sortie normalisés. Il convient de souligner que les deux ensembles d'états $\{|E^0_{0,00}\rangle, |E^1_{1,11}\rangle\}, \{|E^0_{1,01}\rangle, |E^1_{0,10}\rangle\}$ sont paramétrés de manière similaire

$$|E^0_{0,00}\rangle = \alpha|\bar{0}\rangle + \beta|\bar{1}\rangle$$
$$|E^1_{1,11}\rangle = \beta|\bar{0}\rangle + \alpha|\bar{1}\rangle,$$

où α et β sont réels et $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ est une base orthonormale qui est orthogonale à tous les autres états auxiliaires.

Dans le même contexte, nous supposons que les deux autres ensembles d'états $\{|E^1_{1,01}\rangle$, $|E^0_{0,10}\rangle\}$, et $\{|E^1_{0,00}\rangle$, $|E^0_{1,11}\rangle\}$ sont soumis à une paramétrisation similaire. Dans ces ensembles, nous identifions respectivement deux autres nombres réels γ et λ, au lieu de α et β. En outre, la base $|\bar{i}\rangle$ est substituée par une autre base orthogonale notée $|\tilde{\bar{i}}\rangle$.

Toutefois, la probabilité que le qubit soit correctement deviné par Eve dépend de deux scénarios distincts : Dans le premier scénario, lorsque le qubit est transmis sans perturbation à Alice, la probabilité que Eve devine correctement sa valeur est représentée par α^2. Cependant, dans le second scénario, lorsque l'état du qubit est altéré en cours de transmission, la probabilité que Eve devine correctement le qutrit résultant est de γ^2.

En prenant en compte ces deux scénarios et leurs probabilités respectives, nous pouvons calculer la probabilité globale que Eve réussisse à deviner correctement le qubit, désignée par P_E

$$P_E = \frac{1}{2} + \frac{\sqrt{(p-1)(p-2Q)}}{1-2p+2Q}, \tag{3.128}$$

Ainsi, l'information mutuelle optimale entre Alice et Eve et peut être exprimée sous la forme simple suivante :

$$\begin{aligned} I^{A\to E} =& 1 + (1 - (\frac{1}{2} + \frac{\sqrt{(p-1)(p-2Q)}}{1-2p+2Q})) \log(1 - (\frac{1}{2} + \frac{\sqrt{(p-1)(p-2Q)}}{1-2p+2Q})) \\ &+ (\frac{1}{2} + \frac{\sqrt{(p-1)(p-2Q)}}{1-2p+2Q}) \log(\frac{1}{2} + \frac{\sqrt{(p-1)(p-2Q)}}{1-2p+2Q}) \end{aligned} \tag{3.129}$$

L'attaque optimale pour CONFIG-3

Nous dirigeons désormais notre attention vers le protocole en CONFIG-3. En plus des bases analysées dans la section précédente, nous avons la possibilité d'intégrer des situations dans lesquelles Alice envoie initialement et/ou effectue la mesure finale dans la base Y déterminée par les vecteurs $\{|R\rangle, |L\rangle\}$, donnée dans l'équation ci-dessous

$$\begin{aligned} |R\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \\ |L\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \end{aligned} \tag{3.130}$$

En suivant la même procédure que précédemment, nous obtenons les résultats suivants :

$$\begin{aligned}
\rho_R^{BE} =& \frac{1}{2}\{|0\rangle\langle 0|((1-D)^2|E^0_{0,00}\rangle\langle E^0_{0,00}| + D(1-D)(|E^0_{0,00}\rangle\langle E^0_{1,01}| + |E^0_{1,01}\rangle\langle E^0_{0,00}| \\
&+ |E^0_{0,10}\rangle\langle E^0_{0,10}| + |E^0_{0,10}\rangle\langle E^0_{1,11}| + |E^0_{1,11}\rangle\langle E^0_{0,10}| + |E^0_{1,11}\rangle\langle E^0_{1,11}|) + D^2|E^0_{1,01}\rangle\langle E^0_{1,01}|) \\
&+ |0\rangle\langle 1|(D\sqrt{D(1-D)}(|E^0_{1,01}\rangle\langle E^1_{0,00}| + |E^0_{1,01}\rangle\langle E^1_{1,01}| + |E^0_{0,10}\rangle\langle E^1_{0,10}| + |E^0_{1,11}\rangle\langle E^1_{0,10}|) \\
&+ (1-D)\sqrt{D(1-D)}(|E^0_{0,00}\rangle\langle E^1_{0,00}| + |E^0_{0,00}\rangle\langle E^1_{1,01}| + |E^0_{0,10}\rangle\langle E^1_{1,11}| + |E^0_{1,11}\rangle\langle E^1_{1,11}|)) \\
&+ |1\rangle\langle 0|(D\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^0_{1,01}| + |E^1_{1,01}\rangle\langle E^0_{1,01}| + |E^1_{0,10}\rangle\langle E^0_{0,10}| + |E^1_{0,10}\rangle\langle E^0_{1,11}|) \\
&+ (1-D)\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^0_{0,00}| + |E^1_{1,01}\rangle\langle E^0_{0,00}| + |E^1_{1,11}\rangle\langle E^0_{0,10}| + |E^1_{1,11}\rangle\langle E^0_{1,11}|)) \\
&+ |1\rangle\langle 1|((1-D)^2|E^1_{1,11}\rangle\langle E^1_{1,11}| + D(1-D)(|E^1_{0,00}\rangle\langle E^1_{0,00}| + |E^1_{0,00}\rangle\langle E^1_{1,01}| \\
&+ |E^1_{1,01}\rangle\langle E^1_{0,00}| + |E^1_{1,01}\rangle\langle E^1_{1,01}| + |E^1_{0,10}\rangle\langle E^1_{1,11}| + |E^1_{1,11}\rangle\langle E^1_{0,10}|) + D^2|E^1_{0,10}\rangle\langle E^1_{0,10}|)\} \\
&+ \frac{i}{2}(1-p)\{|0\rangle\langle 0|((1-D)\sqrt{D(1-D)}(|E^0_{0,10}\rangle\langle E^0_{0,00}| - |E^0_{0,00}\rangle\langle E^0_{0,10}| - |E^0_{0,00}\rangle\langle E^0_{1,11}| \\
&+ |E^0_{1,11}\rangle\langle E^0_{0,00}|) + D\sqrt{D(1-D)}(|E^0_{0,10}\rangle\langle E^0_{1,01}| - |E^0_{1,01}\rangle\langle E^0_{0,10}| - |E^0_{1,01}\rangle\langle E^0_{1,11}| \\
&+ |E^0_{1,11}\rangle\langle E^0_{1,01}|)) \\
&+ |0\rangle\langle 1|(D(1-D)(|E^0_{0,10}\rangle\langle E^1_{1,01}| - |E^0_{0,00}\rangle\langle E^1_{0,10}| - |E^0_{1,01}\rangle\langle E^1_{1,11}| + |E^0_{0,10}\rangle\langle E^1_{0,00}| \\
&+ |E^0_{1,11}\rangle\langle E^1_{0,00}| + |E^0_{1,11}\rangle\langle E^1_{1,01}|) - (1-D)^2|E^0_{0,00}\rangle\langle E^1_{1,11}| - D^2|E^0_{1,01}\rangle\langle E^1_{0,10}|) \\
&+ |1\rangle\langle 0|((1-D)^2|E^1_{1,11}\rangle\langle E^0_{0,00}| + D(1-D)(-|E^1_{0,00}\rangle\langle E^0_{0,10}| - |E^1_{0,00}\rangle\langle E^0_{1,11}| \\
&- |E^1_{1,01}\rangle\langle E^0_{0,10}| - |E^1_{1,01}\rangle\langle E^0_{1,11}| + |E^1_{0,10}\rangle\langle E^0_{0,00}| + |E^1_{1,11}\rangle\langle E^0_{1,01}|) + D^2|E^1_{0,10}\rangle\langle E^0_{1,01}|) \\
&+ |1\rangle\langle 1|(D\sqrt{D(1-D)}(|E^1_{0,10}\rangle\langle E^1_{0,00}| - |E^1_{0,00}\rangle\langle E^1_{0,10}| - |E^1_{1,01}\rangle\langle E^1_{0,10}| + |E^1_{0,10}\rangle\langle E^1_{1,01}|) \\
&+ (1-D)\sqrt{D(1-D)}(|E^1_{1,11}\rangle\langle E^1_{0,00}| - |E^1_{0,00}\rangle\langle E^1_{1,11}| - |E^1_{1,01}\rangle\langle E^1_{1,11}| + |E^1_{1,11}\rangle\langle E^1_{1,01}|))\}
\end{aligned}$$

$$
\begin{aligned}
\rho_L^{BE} =& \frac{1}{2}\{|0\rangle\langle 0|((1-D)^2|E^0_{0,00}\rangle\langle E^0_{0,00}| + D(1-D)(|E^0_{0,00}\rangle\langle E^0_{1,01}| + |E^0_{1,01}\rangle\langle E^0_{0,00}| \\
&+ |E^0_{0,10}\rangle\langle E^0_{0,10}| + |E^0_{0,10}\rangle\langle E^0_{1,11}| + |E^0_{1,11}\rangle\langle E^0_{0,10}| + |E^0_{1,11}\rangle\langle E^0_{1,11}|) + D^2|E^0_{1,01}\rangle\langle E^0_{1,01}|) \\
&+ |0\rangle\langle 1|(D\sqrt{D(1-D)}(|E^0_{1,01}\rangle\langle E^1_{0,00}| + |E^0_{1,01}\rangle\langle E^1_{1,01}| + |E^0_{0,10}\rangle\langle E^1_{0,10}| + |E^0_{1,11}\rangle\langle E^1_{0,10}|) \\
&+ (1-D)\sqrt{D(1-D)}(|E^0_{0,00}\rangle\langle E^1_{0,00}| + |E^0_{0,00}\rangle\langle E^1_{1,01}| + |E^0_{0,10}\rangle\langle E^1_{1,11}| + |E^0_{1,11}\rangle\langle E^1_{1,11}|)) \\
&+ |1\rangle\langle 0|(D\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^0_{1,01}| + |E^1_{1,01}\rangle\langle E^0_{1,01}| + |E^1_{0,10}\rangle\langle E^0_{0,10}| + |E^1_{0,10}\rangle\langle E^0_{1,11}|) \\
&+ (1-D)\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^0_{0,00}| + |E^1_{1,01}\rangle\langle E^0_{0,00}| + |E^1_{1,11}\rangle\langle E^0_{0,10}| + |E^1_{1,11}\rangle\langle E^0_{1,11}|)) \\
&+ |1\rangle\langle 1|((1-D)^2|E^1_{1,11}\rangle\langle E^1_{1,11}| + D(1-D)(|E^1_{0,00}\rangle\langle E^1_{0,00}| + |E^1_{0,00}\rangle\langle E^1_{1,01}| \\
&+ |E^1_{1,01}\rangle\langle E^1_{0,00}| + |E^1_{1,01}\rangle\langle E^1_{1,01}| + |E^1_{0,10}\rangle\langle E^1_{1,11}| + |E^1_{1,11}\rangle\langle E^1_{0,10}|) + D^2|E^1_{0,10}\rangle\langle E^1_{0,10}|)\} \\
&+ \frac{i}{2}(1-p)\{|0\rangle\langle 0|((1-D)\sqrt{D(1-D)}(|E^0_{0,00}\rangle\langle E^0_{0,10}| + |E^0_{0,00}\rangle\langle E^0_{1,11}| - |E^0_{0,10}\rangle\langle E^0_{0,00}| \\
&- |E^0_{1,11}\rangle\langle E^0_{0,00}|) + D\sqrt{D(1-D)}(|E^0_{1,01}\rangle\langle E^0_{0,10}| + |E^0_{1,01}\rangle\langle E^0_{1,11}| - |E^0_{0,10}\rangle\langle E^0_{1,01}| \\
&- |E^0_{1,11}\rangle\langle E^0_{1,01}|)) \\
&+ |0\rangle\langle 1|((1-D)^2|E^0_{0,00}\rangle\langle E^1_{1,11}| + D(1-D)(|E^0_{0,00}\rangle\langle E^1_{0,10}| + |E^0_{1,01}\rangle\langle E^1_{1,11}| \\
&- |E^0_{0,10}\rangle\langle E^1_{0,00}| - |E^0_{0,10}\rangle\langle E^1_{1,01}| - |E^0_{1,11}\rangle\langle E^1_{0,00}| - |E^0_{1,11}\rangle\langle E^1_{1,01}|) + D^2|E^0_{1,01}\rangle\langle E^1_{0,10}|) \\
&+ |1\rangle\langle 0|(-(1-D)^2|E^1_{1,11}\rangle\langle E^0_{0,00}| + D(1-D)(|E^1_{0,00}\rangle\langle E^0_{0,10}| + |E^1_{0,00}\rangle\langle E^0_{1,11}| \\
&+ |E^1_{1,01}\rangle\langle E^0_{0,10}| + |E^1_{1,01}\rangle\langle E^0_{1,11}| - |E^1_{0,10}\rangle\langle E^0_{0,00}| - |E^1_{1,11}\rangle\langle E^0_{1,01}|) - D^2|E^1_{0,10}\rangle\langle E^0_{1,01}|) \\
&+ |1\rangle\langle 1|(D\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^1_{0,10}| + |E^1_{1,01}\rangle\langle E^1_{0,10}| - |E^1_{0,10}\rangle\langle E^1_{0,00}| - |E^1_{0,10}\rangle\langle E^1_{1,01}|) \\
&+ (1-D)\sqrt{D(1-D)}(|E^1_{0,00}\rangle\langle E^1_{1,11}| + |E^1_{1,01}\rangle\langle E^1_{1,11}| - |E^1_{1,11}\rangle\langle E^1_{0,00}| - |E^1_{1,11}\rangle\langle E^1_{1,01}|))\}
\end{aligned}
$$

Nous restreignons notre analyse aux attaques symétriques, où nous supposons qu'Eve introduit une perturbation équivalente à tous les états d'entrée possibles. Cette perturbation peut être exprimée mathématiquement comme suit :

$$Q = Q_Z = Q_X = Q_Y = \langle L|\rho_R^A|L\rangle = \langle R|\rho_L^A|R\rangle \tag{3.131}$$

avec ρ_R^A et ρ_L^A, les opérateurs de densité réduite sont obtenus en effectuant une opération de trace partielle sur ρ_i^{BE} pour éliminer l'état d'Eve. Ces opérateurs de densité réduite représentent les états que Alice reçoit lorsqu'elle envoie initialement les qubits $|R\rangle$ et $|L\rangle$ respectivement. Nous obtenons les expressions suivantes pour $\langle L|\rho_R^A|L\rangle$ et $\langle R|\rho_L^A|R\rangle$:

$$\begin{aligned}\langle L|\rho_R^A|L\rangle =&\frac{1}{2}\{1-i(1-D)\sqrt{D(1-D)}Im(\langle E_{0,00}^0|E_{0,00}^1\rangle+\langle E_{0,00}^0|E_{1,01}^1\rangle\\&+\langle E_{0,10}^0|E_{1,11}^1\rangle+\langle E_{1,11}^0|E_{1,11}^1\rangle)-iD\sqrt{D(1-D)}Im(\langle E_{1,01}^0|E_{0,00}^1\rangle\\&+\langle E_{1,01}^0|E_{1,01}^1\rangle+\langle E_{0,10}^0|E_{0,10}^1\rangle+\langle E_{1,11}^0|E_{0,10}^1\rangle)\}\\&-\frac{1}{2}(1-p)\{(1-D)^2Re(\langle E_{0,00}^0|E_{1,11}^1\rangle)+D^2Re(\langle E_{1,01}^0|E_{0,10}^1\rangle)\\&+D(1-D)Re(-\langle E_{0,10}^0|E_{0,00}^1\rangle-\langle E_{1,11}^0|E_{0,00}^1\rangle\\&-\langle E_{0,10}^0|E_{1,01}^1\rangle-\langle E_{1,11}^0|E_{1,01}^1\rangle+\langle E_{0,00}^0|E_{0,10}^1\rangle+\langle E_{1,01}^0|E_{1,11}^1\rangle)\}\end{aligned}\tag{3.132}$$

$$\begin{aligned}\langle R|\rho_L^A|R\rangle =&\frac{1}{2}\{1+i(1-D)\sqrt{D(1-D)}Im(\langle E_{0,00}^0|E_{0,00}^1\rangle+\langle E_{0,00}^0|E_{1,01}^1\rangle\\&+\langle E_{0,10}^0|E_{1,11}^1\rangle+\langle E_{1,11}^0|E_{1,11}^1\rangle)+iD\sqrt{D(1-D)}Im(\langle E_{1,01}^0|E_{0,00}^1\rangle\\&+\langle E_{1,01}^0|E_{1,01}^1\rangle+\langle E_{0,10}^0|E_{0,10}^1\rangle+\langle E_{1,11}^0|E_{0,10}^1\rangle)\}\\&-\frac{1}{2}(1-p)\{(1-D)^2Re(\langle E_{0,00}^0|E_{1,11}^1\rangle)+D^2Re(\langle E_{1,01}^0|E_{0,10}^1\rangle)\\&+D(1-D)Re(\langle E_{0,00}^0|E_{0,10}^1\rangle+\langle E_{1,01}^0|E_{1,11}^1\rangle-\langle E_{0,10}^0|E_{0,00}^1\rangle\\&-\langle E_{1,11}^0|E_{0,00}^1\rangle-\langle E_{0,10}^0|E_{1,01}^1\rangle-\langle E_{1,11}^0|E_{1,01}^1\rangle)\}\end{aligned}\tag{3.133}$$

En substituant les expressions définies dans les équations 3.132 et 3.133 dans 3.131, nous obtenons à une restriction sur les états d'Eve, exprimée comme suit :

$$\begin{aligned}&(1-D)\sqrt{D(1-D)}Im(\langle E_{0,00}^0|E_{0,00}^1\rangle+\langle E_{0,00}^0|E_{1,01}^1\rangle+\langle E_{0,10}^0|E_{1,11}^1\rangle+\langle E_{1,11}^0|E_{1,11}^1\rangle)\\&+D\sqrt{D(1-D)}Im(\langle E_{1,01}^0|E_{0,00}^1\rangle+\langle E_{1,01}^0|E_{1,01}^1\rangle+\langle E_{0,10}^0|E_{0,10}^1\rangle+\langle E_{1,11}^0|E_{0,10}^1\rangle)=0\end{aligned}$$

En conséquence, l'expressions de Q_Y est

$$\begin{aligned}QY =&\frac{1}{2}-\frac{1}{2}(1-p)((1-D)^2Re(\langle E_{0,00}^0|E_{1,11}^1\rangle)+D^2Re(\langle E_{1,01}^0|E_{0,10}^1\rangle)\\&+D(1-D)Re(\langle E_{0,00}^0|E_{0,10}^1\rangle+\langle E_{1,01}^0|E_{1,11}^1\rangle)-D(1-D)Re(\langle E_{0,10}^0|E_{0,00}^1\rangle\\&-\langle E_{1,11}^0|E_{0,00}^1\rangle-\langle E_{0,10}^0|E_{1,01}^1\rangle-\langle E_{1,11}^0|E_{1,01}^1\rangle))\end{aligned}\tag{3.134}$$

Étant donné nous avons supposé que le taux d'erreur de bit quantique Q est équivalent dans toutes les états, c'est-à-dire $Q_X = Q_Y$ et en utilisant les équations 3.127 et 3.134, nous obtenons :

$$\begin{aligned}Q =&\frac{1}{2}-\frac{1}{2}(1-p)((1-D)^2Re(\langle E_{0,00}^0|E_{1,11}^1\rangle)+D^2Re(\langle E_{1,01}^0|E_{0,10}^1\rangle)\\&+D(1-D)Re(\langle E_{0,00}^0|E_{0,10}^1\rangle+\langle E_{1,01}^0|E_{1,11}^1\rangle)\end{aligned}\tag{3.135}$$

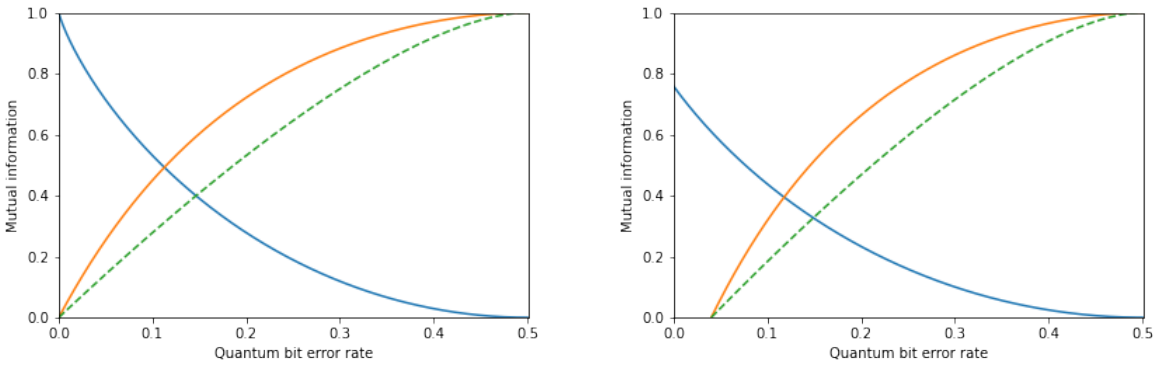
Suivant la paramétrisation précédemment décrite, pour les états de sortie d'Eve, nous trouvons que l'information mutuelle maximale entre Alice et Eve est donnée par la formule suivante :

$$\begin{aligned} I^{AE} =& 1 + (1 - (\frac{1}{2} + \frac{\sqrt{(p-2Q)(-2+p+2Q)}}{2(p-1)})) \log(1 - (\frac{1}{2} + \frac{\sqrt{(p-2Q)(-2+p+2Q)}}{2(p-1)})) \\ &+ (\frac{1}{2} + \frac{\sqrt{(p-2Q)(-2+p+2Q)}}{2(p-1)}) \log(\frac{1}{2} + \frac{\sqrt{(p-2Q)(-2+p+2Q)}}{2(p-1)}) \end{aligned} \tag{3.136}$$

C Evaluation

Nous évaluons les informations mutuelles I^{AB} et I^{AE} en fonction du taux d'erreur des qubits, noté Q, comme indiqué dans la Figure 3.6. La courbe en pointillés représente l'information mutuelle I^{AE} pour le protocole en CONFIG-3, tandis que les courbes pleines en orange et en bleu correspondent respectivement à l'information mutuelle I^{AE} pour le protocole en CONFIG-2 et à l'information mutuelle I^{AB}.

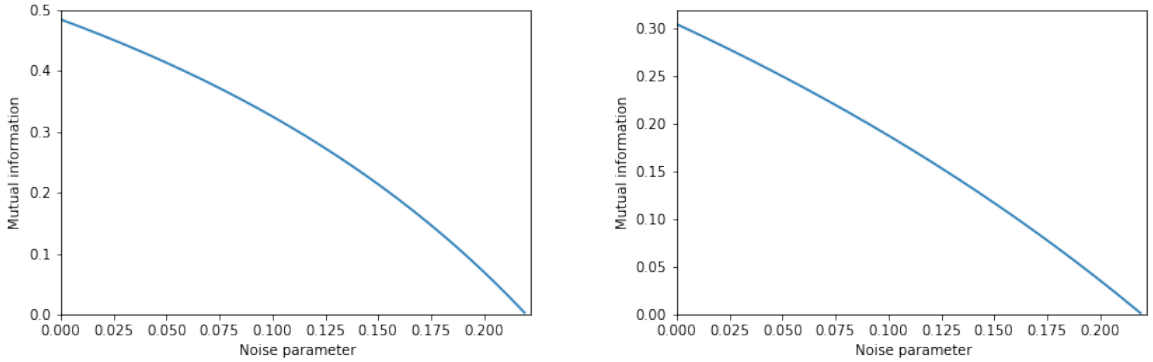
Nous remarquons pour $p = 0.08$, que l'information mutuelle I^{AE} dans les deux cas du protocole commencent à une valeur non nulle pour Q, contrairement au cas des états sont purs où $p = 0$. Par ailleurs, il est également observable que, pour $p = 0.08$, le point d'intersection entre les deux courbes d'information mutuelle se déplace vers des valeurs de Q plus élevées.



(a) (b)

FIGURE 3.6 : Information mutuelle $I^{A\to E}$ et $I^{A\to A}$ en fonction du taux d'erreur de bit quantique Q. (a) Dans le cas où le paramètre de bruit $p = 0$, (b) Dans le cas où le paramètre de bruit $p = 0.08$.

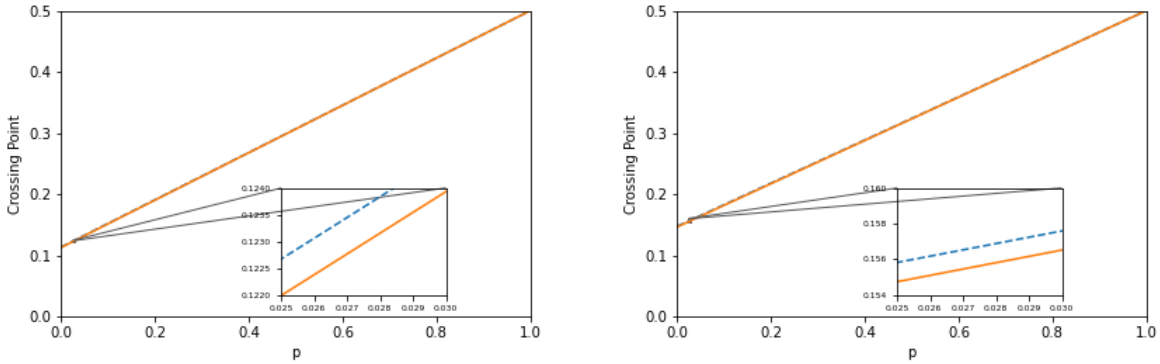
La Figure 3.7 présente l'évolution de l'information mutuelle I^{AE} entre Alice et Eve en fonction du paramètre de bruit p, pour un taux d'erreur des qubits $Q = 0.113$. Cette représentation graphique confirme que, à mesure que le paramètre de bruit p augmente, la quantité d'informations que peut obtenir Eve sur le qubit d'Alice diminue. De plus,



(a) (b)

FIGURE 3.7 : L'information mutuelle $I^{A\to E}$ en fonction du paramètre de bruit p.(a) Cas du le protocole en CONFIG-2. (b) Cas du protocole en CONFIG-3.

elle met en évidence que l'information mutuelle dans le cas du protocole en CONFIG-3 est inférieure à celle du protocole en CONFIG-2.

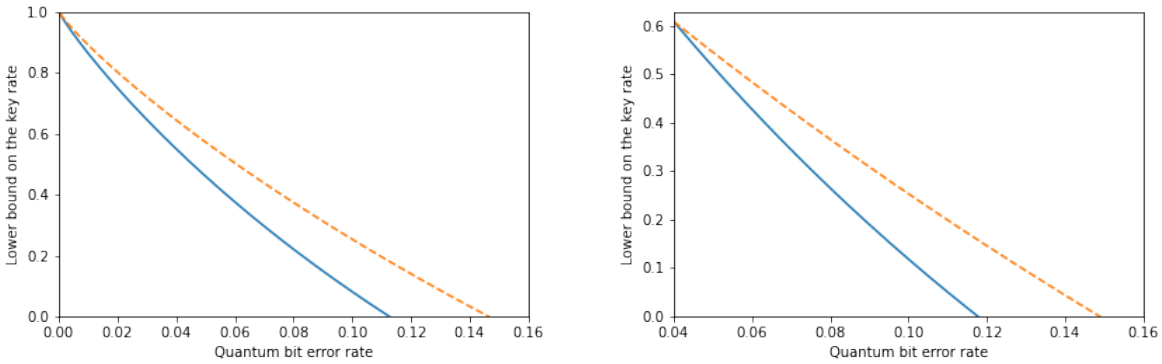


(a) (b)

FIGURE 3.8 : la valeur de Q pour le point d'intersection entre I^{AB} et I^{AE}, en fonction du paramètre de bruit p. (a) Cas du le protocole en CONFIG-2. (b) Cas du protocole en CONFIG-3.

Le résultat relatif à la valeur de Q correspondant au point d'intersection entre I^{AB} et I^{AE}, en fonction du paramètre de bruit p, est présenté dans la Figure 3.8. Il convient de rappeler la relation exprimant le lien entre le taux d'erreur Q, la perturbation D, et le paramètre de bruit p, est définie dans l'équation 3.118. Pour le cas où $p = 0$, les valeurs du point d'intersection sont de $Q(p = 0) = 0.113$ pour le protocole CONFIG-2 et de $Q(p = 0) = 0.147$ pour le protocole CONFIG-3, comme indiqué par la ligne en pointillés dans la Figure 3.8.

Cependant, la véritable valeur du point d'intersection est représentée par la ligne conti-



(a) (b)

FIGURE 3.9 : Évolution du taux de clé en fonction du taux d'erreur des qubits Q. La ligne en pointillé représente le cas du protocole en CONFIG-3, tandis que pour la ligne pleine correspond au cas du protocole en CONFIG-2. (a) Dans le cas où le paramètre de bruit $p = 0$, (b) Dans le cas où le paramètre de bruit $p = 0.08$.

nue qui se situe au-dessus de cette droite. La Figure 3.8 illustre de manière explicite que lorsque le paramètre p augmente, le point d'intersection entre les deux courbes d'information mutuelle se déplace également vers des valeurs de Q plus élevées. Par conséquent, l'ajout de bruit aux données quantiques élargit la plage de paramètres sécurisés de Q.

L'évolution du taux de clé en fonction du taux d'erreur Q est illustrée dans la figure 3.9 pour deux scénarios différents : l'un avec des états purs ($p = 0$) et l'autre avec des états mixtes ($p = 0.08$). Les résultats mettent en évidence une augmentation significative du taux d'erreur tolérable dans le cadre du protocole en CONFIG-3. De plus, ils démontrent que l'ajout de bruit améliore la borne inférieure du taux de clé.

Nous parvenons alors à la conclusion que l'ajout de bruit quantique peut renforcer considérablement la sécurité des protocoles de distribution semi-quantique de clés contre les attaques d'interception.

Conclusions et perspectives

L'évolution de la cryptographie depuis ses débuts a connu une transition progressive, passant d'une discipline centrée sur la préservation des informations personnels à une science visant la confidentialité de la transmission des données sensibles. Au cours du siècle écoulé, nous avons assisté à l'émergence de ce que nous appelons aujourd'hui la cryptographie moderne. Cela englobe l'avancement des algorithmes symétriques, dont la confiance que nous leur accordons est désormais presque inconditionnelle, ainsi que le développement d'algorithmes asymétriques qui ont ouvert la voie à de nouvelles fonctionnalités désormais intégrées quotidiennement sur Internet.

Néanmoins, la fiabilité assurée par ces approches techniques aux algorithmes de cryptographie peut être remise en question lorsqu'il s'agit de garantir la préservation à long terme de la confidentialité des données. Dans ce contexte, l'exploitation des principes de la mécanique quantique en vue du traitement de l'information, notamment l'application de la cryptographie quantique, se présente comme une perspective prometteuse pour aborder la problématique de la distribution de clés de chiffrement. Cette approche vise à assurer une sécurité inconditionnelle pour les communications et les échanges de données. Parmi ces approches, la distribution semi-quantique de clés s'est révélée être une méthode novatrice, et c'est précisément sur cette méthode que la thèse se focalise.

Dans le premier chapitre, nous avons abordé la cryptographie classique, couvrant à la fois son histoire et ses principes fondamentaux. Nous avons examiné les différents types d'algorithme utilisées, notamment les algorithme à clé privée et les algorithmes à clé publique. En outre, une attention particulière a été accordée à l'étude approfondie des algorithmes de chiffrement modernes tels que DES, AES, RSA et ElGamal. Ce chapitre a facilité notre acquisition des fondements et des évolutions significatives de la cryptographie moderne. Il nous a également permis de saisir la manière dont ces algorithmes ont été appliqués pour garantir la sécurité des échanges et des informations confidentielles. Cette compréhension a constitué une base solide pour la continuité de notre exploration de la cryptographie quantique et de ses implications dans la sécurisation des systèmes d'information.

Dans le second chapitre, nous avons abordé l'histoire de la cryptographie quantique. Nous avons introduit les concepts clés de la mécanique quantique tels que les états quantiques et l'intrication. Nous avons présenté la distribution de clés quantiques utilisant des

qubits uniques, en abordant en détail les protocoles BB84 et B92. Nous avons également présenté un algorithme d'extraction de clés basé sur Python. Par la suite, nous avons étudié le protocole de distribution de clés basé sur des qubits intriqués, en nous concentrant sur les protocoles E91 et BBM92. Ces protocoles exploitent l'intrication quantique pour établir des clés sécurisées à distance. De plus, nous avons présenté un autre algorithme d'extraction de clés utilisant Python, cette fois-ci avec l'utilisation de la bibliothèque Qiskit pour les opérations quantiques spécifiques. Ce chapitre a favorisé notre compréhension de l'évolution de la cryptographie classique vers la cryptographie quantique, exploitant les propriétés distinctives de la mécanique quantique pour consolider la sécurité des communications.

Dans le troisième chapitre, nous nous sommes concentrés sur la robustesse des protocoles de distribution semi-quantiques de clés basés sur les qutrits et les ququarts avec différentes bases mutuellement nonbiaisées, dans le cas de l'attaque collective. Nous avons dérivé une borne inférieure sur le taux de clé qui dépend uniquement du bruit du canal quantique, un paramètre pouvant être estimé par les parties légitimes. En outre, nous avons évalué cette borne inférieure en prenant en compte les formes les plus courantes de canaux, à savoir les canaux indépendants et les canaux dépendants. Nos résultats ont démontré que l'augmentation du nombre de bases mutuellement non biaisées conduit à une amélioration de la résistance du canal quantique face au bruit. De plus, l'utilisation de l'encodage dans des bases mutuellement non biaisées de dimensions supérieures renforce la sécurité contre les interceptions et permet d'atteindre des taux de génération de clé sécurisée plus élevés, tout en réduisant le taux d'erreur.

Au cours de cette thèse, nous avons également étudier une stratégie optimale d'interception, en prenant en considération l'information mutuelle partagée entre Alice et Eve. Cette étude a été menée dans des états quantiques tridimensionnels. Nous avons dérivé la probabilité de réussite de l'écoute clandestine en tenant compte du taux d'erreur engendré par cette interception, à la fois dans le scénario de "Match" et dans le scénario de "Mismatch". Ces termes se réfèrent aux résultats des mesures effectuées par Ève sur les qubits transmis entre Alice et Bob. Plus précisément, le scénario "Match" survient lorsque Ève observe des résultats identiques dans les deux directions, tandis que le scénario "Mismatch" se produit lorsque Ève détecte des résultats différents dans les deux directions. Nos conclusions ont révélé que la stratégie d'interception bidirectionnel appliquée au protocole de distribution de clé semi-quantique permet d'extraire une quantité supérieure des informations liées à la clé partagée, en comparaison avec la stratégie d'interception unidirectionnelle.

Finalement, nous avons étudié le protocole de distribution semi-quantique de clés, selon deux configurations en fonction des capacités de l'utilisateur quantique, avec un bruit supplémentaire sur tous les états quantique en présence d'un intercepteur. Nous avons dérivé l'information mutuelle optimale qu'Eve peut obtenir lorsqu'elle utilise des attaques individuelles sur des états quantiques bruités, et nous l'avons comparée à l'information mutuelle des états purs. Comme prévu, Alice, Bob et Eve perdent tous une partie de l'information en raison du bruit supplémentaire. Il a également été démontré que la valeur

seuil du taux d'erreur des bits quantique, en dessous de laquelle l'information mutuelle entre Alice et Bob est supérieure à celle entre Alice et Eve, se déplace vers des valeurs plus élevées, en fonction du paramètre de bruit. Cela conduit à une augmentation de la région admissible dans laquelle les parties de confiance peuvent générer une clé secrète. De plus, il a été observé que grâce au bruit additionnel, la borne inférieure sur le taux de la clé s'améliore. En réalité, le bruit supplémentaire améliore les performances du protocole à six états et le rend plus résistant à l'écoute clandestine.

Pour conclure, cette thèse propose une analyse approfondie de la distribution semi-quantique de clés. Elle examine en détail les fondements théoriques de cette méthode, explore ses divers protocoles, et procède à une évaluation rigoureuse de sa résistance face à différentes attaques potentielles. Les résultats obtenues contribuent de manière significative à notre appréhension des potentialités inhérentes à la cryptographie quantique, et par conséquent, elles ouvrent de nouvelles perspectives prometteuses pour l'établissement de communications sécurisées au sein de l'écosystème numérique contemporain.

Nous prévoyons la poursuite des recherches présentées dans cette thèse en élaborant un protocole de distribution semi-quantique de clé à variables continues. En poursuivant cette démarche, notre objectif est de concrétiser les principes théoriques en une application pratique, ouvrant ainsi la voie à des expérimentations concrètes dans le domaine de la distribution semi-quantique à variables continues. En contribuant à l'implémentation effective de ces concepts, nous espérons apporter une contribution significative à la fois à la recherche fondamentale en cryptographie et à l'éventuelle application pratique de la communication sécurisée dans le monde quantique. De plus, nous prévoyons de mettre en œuvre des mécanismes de contrôle et de correction d'erreurs pour garantir la fiabilité et la robustesse du protocole dans des environnements réels.

D'autre part, pour concrétiser cet objectif, nous envisageons d'adopter une approche pratique, notamment en s'appuyant sur des techniques bien établies, comme la simulation informatique, les réseaux quantiques et les ordinateurs quantiques. En particulier, nous prévoyons d'utiliser le langage de programmation Python pour élaborer des simulations informatiques avancées qui reproduiront les aspects essentiels du protocole de distribution semi-quantique de clé. De plus, nous comptons tirer parti des capacités des réseaux quantiques, qui permettent une distribution de l'information quantique à longue distance avec une sécurité accrue, pour tester nos protocoles et améliorations de manière pratique. Enfin, l'utilisation des ordinateurs quantiques, avec leur puissance de calcul exceptionnelle pour résoudre des problèmes quantiques complexes, sera un atout essentiel dans notre recherche pour analyser et optimiser les protocoles SQKD, ouvrant ainsi de nouvelles perspectives passionnantes pour la sécurité des communications quantiques.

A

Estimation du bruit de base $\mathcal{K}$

Soient les probabilités de transition $p_{0''1''}$, $p_{0''2''}$, $p_{1''0''}$, $p_{1''2''}$, $p_{2''0''}$ et $p_{2''1''}$, qui représentent respectivement les probabilités de mesure des différentes combinaisons d'états $\langle h_1|h_1\rangle$, $\langle h_2|h_2\rangle$, $\langle h_3|h_3\rangle$, $\langle h_5|h_5\rangle$, $\langle h_6|h_6\rangle$ et $\langle h_7|h_7\rangle$.En conséquence, nous pouvons déduire les expressions des quantités $p_{i''j''}$ à partir de l'équation (3.63) :

$$
\begin{aligned}
p_{0''1''} =& \langle h_1|h_1\rangle \\
=& \frac{1}{3} + \frac{1}{9}e^{\frac{2i\pi}{3}} Re(\langle f_1|f_0\rangle + \langle f_4|f_0\rangle + \langle f_7|f_0\rangle + \langle f_2|f_1\rangle + \langle f_5|f_1\rangle + \langle f_8|f_1\rangle \\
&\quad + \langle f_0|f_2\rangle + \langle f_3|f_2\rangle + \langle f_6 f_2\rangle + \langle f_1|f_3\rangle + \langle f_4|f_3\rangle + \langle f_7|f_3\rangle \\
&\quad + \langle f_2|f_4\rangle + \langle f_5|f_4\rangle + \langle f_8|f_4\rangle + \langle f_0|f_5\rangle + \langle f_3|f_5\rangle + \langle f_6|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_4|f_6\rangle + \langle f_7|f_6\rangle + \langle f_2|f_7\rangle + \langle f_5|f_7\rangle + \langle f_8|f_7\rangle \\
&\quad + \langle f_0|f_8\rangle + \langle f_3|f_8\rangle + \langle f_6|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}} Re(\langle f_2|f_0\rangle + \langle f_5|f_0\rangle + \langle f_8|f_0\rangle + \langle f_0|f_1\rangle + \langle f_3|f_1\rangle + \langle f_6|f_1\rangle \\
&\quad + \langle f_1|f_2\rangle + \langle f_4|f_2\rangle + \langle f_7|f_2\rangle + \langle f_2|f_3\rangle + \langle f_5|f_3\rangle + \langle f_8|f_3\rangle \\
&\quad + \langle f_0|f_4\rangle + \langle f_3|f_4\rangle + \langle f_6|f_4\rangle + \langle f_1|f_5\rangle + \langle f_4|f_5\rangle + \langle f_7|f_5\rangle \\
&\quad + \langle f_2|f_6\rangle + \langle f_5|f_6\rangle + \langle f_8|f_6\rangle + \langle f_0|f_7\rangle + \langle f_3|f_7\rangle + \langle f_6|f_7\rangle \\
&\quad + \langle f_1|f_8\rangle + \langle f_4|f_8\rangle + \langle f_7|f_8\rangle)
\end{aligned}
\tag{A.1}
$$

$$
\begin{aligned}
p_{0''2''} =& \langle h_2|h_2\rangle \\
=& \frac{1}{3} + \frac{1}{9}e^{\frac{-2i\pi}{3}} Re(\langle f_2|f_0\rangle + \langle f_5|f_0\rangle + \langle f_8|f_0\rangle + \langle f_0|f_1\rangle + \langle f_3|f_1\rangle + \langle f_6|f_1\rangle \\
&\quad + \langle f_1|f_2\rangle + \langle f_4|f_2\rangle + \langle f_7|f_2\rangle + \langle f_2|f_3\rangle + \langle f_5|f_3\rangle + \langle f_8|f_3\rangle \\
&\quad + \langle f_0|f_4\rangle + \langle f_3|f_4\rangle + \langle f_6|f_4\rangle + \langle f_1|f_5\rangle + \langle f_4|f_5\rangle + \langle f_7|f_5\rangle \\
&\quad + \langle f_2|f_6\rangle + \langle f_5|f_6\rangle + \langle f_8|f_6\rangle + \langle f_0|f_7\rangle + \langle f_3|f_7\rangle + \langle f_6|f_7\rangle \\
&\quad + \langle f_1|f_8\rangle + \langle f_4|f_8\rangle + \langle f_7|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}} Re(\langle f_1|f_0\rangle + \langle f_4|f_0\rangle + \langle f_7|f_0\rangle + \langle f_2|f_1\rangle + \langle f_5|f_1\rangle + \langle f_8|f_1\rangle \\
&\quad + \langle f_0|f_2\rangle + \langle f_3|f_2\rangle + \langle f_6 f_2\rangle + \langle f_1|f_3\rangle + \langle f_4|f_3\rangle + \langle f_7|f_3\rangle \\
&\quad + \langle f_2|f_4\rangle + \langle f_5|f_4\rangle + \langle f_8|f_4\rangle + \langle f_0|f_5\rangle + \langle f_3|f_5\rangle + \langle f_6|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_4|f_6\rangle + \langle f_7|f_6\rangle + \langle f_2|f_7\rangle + \langle f_5|f_7\rangle + \langle f_8|f_7\rangle \\
&\quad + \langle f_0|f_8\rangle + \langle f_3|f_8\rangle + \langle f_6|f_8\rangle)
\end{aligned} \tag{A.2}
$$

$$
\begin{aligned}
p_{1''0''} =& \langle h_3|h_3\rangle \\
=& \frac{1}{3} + \frac{1}{9}Re(\langle f_1|f_0\rangle + \langle f_2|f_0\rangle + \langle f_0|f_1\rangle + \langle f_2|f_1\rangle + \langle f_0|f_2\rangle + \langle f_1|f_2\rangle \\
&\quad + \langle f_4|f_3\rangle + \langle f_5|f_3\rangle + \langle f_3|f_4\rangle + \langle f_5|f_4\rangle + \langle f_3|f_5\rangle + \langle f_4|f_5\rangle \\
&\quad + \langle f_7|f_6\rangle + \langle f_8|f_6\rangle + \langle f_6|f_7\rangle + \langle f_8|f_7\rangle + \langle f_6|f_8\rangle + \langle f_7|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}} Re(\langle f_4|f_0\rangle + \langle f_5|f_0\rangle + \langle f_3|f_1\rangle + \langle f_5|f_1\rangle + \langle f_3|f_2\rangle + \langle f_4|f_2\rangle \\
&\quad + \langle f_7|f_3\rangle + \langle f_8|f_3\rangle + \langle f_6|f_4\rangle + \langle f_8|f_4\rangle + \langle f_6|f_5\rangle + \langle f_7|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_2|f_6\rangle + \langle f_0|f_7\rangle + \langle f_2|f_7\rangle + \langle f_0|f_8\rangle + \langle f_1|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{2i\pi}{3}} Re(\langle f_7|f_0\rangle + \langle f_8|f_0\rangle + \langle f_6|f_1\rangle + \langle f_8|f_1\rangle + \langle f_6|f_2\rangle + \langle f_7|f_2\rangle \\
&\quad + \langle f_1|f_3\rangle + \langle f_2|f_3\rangle + \langle f_0|f_4\rangle + \langle f_2|f_4\rangle + \langle f_0|f_5\rangle + \langle f_1|f_5\rangle \\
&\quad + \langle f_4|f_6\rangle + \langle f_5|f_6\rangle + \langle f_3|f_7\rangle + \langle f_5|f_7\rangle + \langle f_4|f_8\rangle + \langle f_3|f_8\rangle
\end{aligned} \tag{A.3}
$$

$$
\begin{aligned}
p_{1''2''} =& \langle h_5|h_5\rangle \\
=& \frac{1}{3} + \frac{1}{9}Re(\langle f_5|f_0\rangle + \langle f_7|f_0\rangle + \langle f_3|f_1\rangle + \langle f_8|f_1\rangle + \langle f_4|f_2\rangle + \langle f_6|f_2\rangle \\
&\quad + \langle f_1|f_3\rangle + \langle f_8|f_3\rangle + \langle f_2|f_4\rangle + \langle f_6|f_4\rangle + \langle f_0|f_5\rangle + \langle f_7|f_5\rangle \\
&\quad + \langle f_2|f_6\rangle + \langle f_4|f_6\rangle + \langle f_0|f_7\rangle + \langle f_5|f_7\rangle + \langle f_1|f_8\rangle + \langle f_3|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}} Re(\langle f_1|f_0\rangle + \langle f_8|f_0\rangle + \langle f_2|f_1\rangle + \langle f_6|f_1\rangle + \langle f_0|f_2\rangle + \langle f_7|f_2\rangle \\
&\quad + \langle f_2|f_3\rangle + \langle f_4|f_3\rangle + \langle f_0|f_4\rangle + \langle f_5|f_4\rangle + \langle f_1|f_5\rangle + \langle f_3|f_5\rangle \\
&\quad + \langle f_5|f_6\rangle + \langle f_7|f_6\rangle + \langle f_3|f_7\rangle + \langle f_8|f_7\rangle + \langle f_4|f_8\rangle + \langle f_6|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{2i\pi}{3}} Re(\langle f_2|f_0\rangle + \langle f_4|f_0\rangle + \langle f_0|f_1\rangle + \langle f_5|f_1\rangle + \langle f_1|f_2\rangle + \langle f_3|f_2\rangle \\
&\quad + \langle f_5|f_3\rangle + \langle f_7|f_3\rangle + \langle f_3|f_4\rangle + \langle f_8|f_4\rangle + \langle f_4|f_5\rangle + \langle f_6|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_8|f_6\rangle + \langle f_2|f_7\rangle + \langle f_6|f_7\rangle + \langle f_0|f_8\rangle + \langle f_7|f_8\rangle)
\end{aligned} \tag{A.4}
$$

$$
\begin{aligned}
p_{2''0''} =& \langle h_6|h_6\rangle \\
=& \frac{1}{3} + \frac{1}{9}Re(\langle f_2|f_1\rangle + \langle f_5|f_1\rangle + \langle f_6|f_1\rangle + \langle f_1|f_2\rangle + \langle f_4|f_2\rangle + \langle f_6|f_2\rangle \\
&\quad + \langle f_2|f_4\rangle + \langle f_5|f_4\rangle + \langle f_6|f_4\rangle + \langle f_1|f_5\rangle + \langle f_4|f_5\rangle + \langle f_6|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_2|f_6\rangle + \langle f_4|f_6\rangle + \langle f_5|f_6\rangle + \langle f_8|f_7\rangle + \langle f_7|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}}Re(\langle f_1|f_0\rangle + \langle f_2|f_0\rangle + \langle f_4|f_0\rangle + \langle f_5|f_0\rangle + \langle f_8|f_1\rangle + \langle f_7|f_2\rangle \\
&\quad + \langle f_1|f_3\rangle + \langle f_2|f_3\rangle + \langle f_4|f_3\rangle + \langle f_5|f_3\rangle + \langle f_8|f_4\rangle + \langle f_7|f_5\rangle \\
&\quad + \langle f_7|f_6\rangle + \langle f_8|f_6\rangle + \langle f_0|f_7\rangle + \langle f_3|f_7\rangle + \langle f_0|f_8\rangle + \langle f_3|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}}Re(\langle f_7|f_0\rangle + \langle f_8|f_0\rangle + \langle f_0|f_1\rangle + \langle f_3|f_1\rangle + \langle f_0|f_2\rangle + \langle f_3|f_2\rangle \\
&\quad + \langle f_7|f_3\rangle + \langle f_8|f_3\rangle + \langle f_0|f_4\rangle + \langle f_3|f_4\rangle + \langle f_0|f_5\rangle + \langle f_3|f_5\rangle \\
&\quad + \langle f_0|f_6\rangle + \langle f_1|f_7\rangle + \langle f_2|f_7\rangle + \langle f_5|f_7\rangle + \langle f_6|f_7\rangle + \langle f_1|f_8\rangle \\
&\quad + \langle f_2|f_8\rangle + \langle f_4|f_8\rangle + \langle f_6|f_8\rangle)
\end{aligned}
\tag{A.5}
$$

$$
\begin{aligned}
p_{2''1''} =& \langle h_7|h_7\rangle \\
=& \frac{1}{3} + \frac{1}{9}Re(\langle f_5|f_0\rangle + \langle f_7|f_0\rangle + \langle f_3|f_1\rangle + \langle f_8|f_1\rangle + \langle f_4|f_2\rangle + \langle f_6|f_2\rangle \\
&\quad + \langle f_1|f_3\rangle + \langle f_8|f_3\rangle + \langle f_2|f_4\rangle + \langle f_6|f_4\rangle + \langle f_0|f_5\rangle + \langle f_7|f_5\rangle \\
&\quad + \langle f_2|f_6\rangle + \langle f_4|f_6\rangle + \langle f_0|f_7\rangle + \langle f_5|f_7\rangle + \langle f_1|f_8\rangle + \langle f_3|f_8\rangle \\
&+ \frac{1}{9}e^{\frac{2i\pi}{3}}Re(\langle f_1|f_0\rangle + \langle f_8|f_0\rangle + \langle f_2|f_1\rangle + \langle f_6|f_1\rangle + \langle f_0|f_2\rangle + \langle f_7|f_2\rangle \\
&\quad + \langle f_2|f_3\rangle + \langle f_4|f_3\rangle + \langle f_0|f_4\rangle + \langle f_5|f_4\rangle + \langle f_1|f_5\rangle + \langle f_3|f_5\rangle \\
&\quad + \langle f_5|f_6\rangle + \langle f_7|f_6\rangle + \langle f_3|f_7\rangle + \langle f_8|f_7\rangle + \langle f_6|f_8\rangle + \langle f_4|f_8\rangle) \\
&+ \frac{1}{9}e^{\frac{-2i\pi}{3}}Re(\langle f_2|f_0\rangle + \langle f_4|f_0\rangle + \langle f_0|f_1\rangle + \langle f_5|f_1\rangle + \langle f_1|f_2\rangle + \langle f_3|f_2\rangle \\
&\quad + \langle f_5|f_3\rangle + \langle f_7|f_3\rangle + \langle f_3|f_4\rangle + \langle f_8|f_4\rangle + \langle f_4|f_5\rangle + \langle f_6|f_5\rangle \\
&\quad + \langle f_1|f_6\rangle + \langle f_8|f_6\rangle + \langle f_2|f_7\rangle + \langle f_6|f_7\rangle + \langle f_0|f_8\rangle + \langle f_7|f_8\rangle)
\end{aligned}
\tag{A.6}
$$

En utilisant l'inégalité de Cauchy-Schwarz, nous pouvons encadrer la quantité $X_{\phi_2} = Re(\langle e^0_{0,0}|e^1_{1,4}\rangle) + Re(\langle e^0_{0,0}|e^2_{2,8}\rangle) + Re(\langle e^1_{1,4}|e^2_{2,8}\rangle)$ comme suit :

$$
\begin{aligned}
X_{\phi_2} \geq & 3 - \frac{3}{2}(p_{0''1''} + p_{0''2''} + p_{1''0''} + p_{1''2''} + p_{2''0''} + p_{2''1''} \\
& - (\sqrt{p_{001}p_{102}} + \sqrt{p_{011}p_{102}} + \sqrt{p_{021}p_{102}} + \sqrt{p_{001}p_{112}} + \sqrt{p_{011}p_{112}} \\
& + \sqrt{p_{021}p_{112}} + \sqrt{p_{001}p_{122}} + \sqrt{p_{011}p_{122}} + \sqrt{p_{021}p_{122}} + \sqrt{p_{001}p_{200}} \\
& + \sqrt{p_{011}p_{200}} + \sqrt{p_{021}p_{200}} + \sqrt{p_{001}p_{210}} + \sqrt{p_{011}p_{210}} + \sqrt{p_{021}p_{210}} \\
& + \sqrt{p_{001}p_{220}} + \sqrt{p_{011}p_{220}} + \sqrt{p_{021}p_{220}} + \sqrt{p_{002}p_{100}} + \sqrt{p_{012}p_{100}} \\
& + \sqrt{p_{022}p_{100}} + \sqrt{p_{002}p_{110}} + \sqrt{p_{012}p_{110}} + \sqrt{p_{022}p_{110}} + \sqrt{p_{002}p_{120}} \\
& + \sqrt{p_{012}p_{120}} + \sqrt{p_{022}p_{120}} + \sqrt{p_{002}p_{201}} + \sqrt{p_{012}p_{201}} + \sqrt{p_{022}p_{201}} \\
& + \sqrt{p_{002}p_{211}} + \sqrt{p_{012}p_{211}} + \sqrt{p_{022}p_{211}} + \sqrt{p_{002}p_{221}} + \sqrt{p_{012}p_{221}} \\
& + \sqrt{p_{022}p_{221}} + \sqrt{p_{100}p_{201}} + \sqrt{p_{110}p_{201}} + \sqrt{p_{120}p_{201}} + \sqrt{p_{100}p_{211}} \\
& + \sqrt{p_{110}p_{211}} + \sqrt{p_{120}p_{211}} + \sqrt{p_{100}p_{221}} + \sqrt{p_{110}p_{221}} + \sqrt{p_{120}p_{221}} \\
& + \sqrt{p_{102}p_{200}} + \sqrt{p_{112}p_{200}} + \sqrt{p_{122}p_{200}} + \sqrt{p_{102}p_{210}} + \sqrt{p_{112}p_{210}} \\
& + \sqrt{p_{122}p_{210}} + \sqrt{p_{102}p_{220}} + \sqrt{p_{112}p_{220}} + \sqrt{p_{122}p_{220}}) \\
& - (\sqrt{p_{000}p_{101}} + \sqrt{p_{010}p_{101}} + \sqrt{p_{020}p_{101}} + \sqrt{p_{010}p_{111}} + \sqrt{p_{020}p_{111}} \\
& + \sqrt{p_{000}p_{121}} + \sqrt{p_{010}p_{121}} + \sqrt{p_{020}p_{121}} + \sqrt{p_{000}p_{202}} + \sqrt{p_{010}p_{202}} \\
& + \sqrt{p_{020}p_{202}} + \sqrt{p_{000}p_{212}} + \sqrt{p_{010}p_{212}} + \sqrt{p_{020}p_{212}} + \sqrt{p_{010}p_{222}} \\
& + \sqrt{p_{020}p_{222}} + \sqrt{p_{101}p_{202}} + \sqrt{p_{111}p_{202}} + \sqrt{p_{121}p_{202}} + \sqrt{p_{101}p_{212}} \\
& + \sqrt{p_{111}p_{212}} + \sqrt{p_{121}p_{212}} + \sqrt{p_{101}p_{222}} + \sqrt{p_{121}p_{222}}).
\end{aligned}
\tag{A.7}
$$

B
Appendice

L'appendice comprend les tables de substitution S-box utilisées dans les algorithmes de chiffrement AES et DES. Les S-box sont des éléments fondamentaux de ces algorithmes, jouant un rôle essentiel dans le processus de chiffrement et de déchiffrement des données.

La Figure B.1 présente la S-box de l'algorithme AES (**Advanced Encryption Standard**), ainsi que sa version inverse. L'algorithme AES est largement adopté pour sécuriser les données sensibles, et la sophistication de ces tables de substitution est cruciale pour protéger les données contre les tentatives de déchiffrement non autorisées. C'est pourquoi l'algorithme AES est devenu l'un des standards de chiffrement les plus fiables et les plus largement utilisés dans le domaine de la sécurité informatique.

D'autre part, la Figure B.2 met en évidence les huit tables de substitution, également connues sous le nom de S-Box, utilisées dans le chiffrement DES (**Data Encryption Standard**). Chacune de ces tables de substitution est indispensable pour transformer les blocs de données d'entrée en blocs chiffrés de sortie. Lorsqu'elles sont combinées avec d'autres étapes de l'algorithme DES, elles forment un système de chiffrement robuste et sécurisé, offrant une protection efficace contre les tentatives de déchiffrement non autorisées.

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
40	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

(a)

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	52	9	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
10	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
20	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
30	8	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
40	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
50	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
60	90	d8	ab	0	8c	bc	d3	0a	f7	e4	58	5	b8	b3	45	6
70	d0	2c	1e	8f	ca	3f	0f	2	c1	af	bd	3	1	13	8a	6b
80	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
90	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a0	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b0	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4

(b)

FIGURE B.1 : S-box de l'algorithme AES : (a) S-box et (b) S-box inverse.

S_1																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S_2																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S_3																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S_4																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S_5																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S_6																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S_7																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S_8																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

FIGURE B.2 : S-box de l'algorithme DES.

Bibliographie

[1] G. Bertrand, *Enigma : ou, La plus grande énigme de la guerre 1939-1945*. Plon, 1973.

[2] N. I. of Standards and Technology, "Data encryption standard (des)," Tech. Rep. FIPS PUB 46, National Institute of Standards and Technology, January 1977.

[3] N. I. of Standards and Technology, *Advanced Encryption Standard (AES) : 128-Bit Block Cipher*. U.S. Department of Commerce, 2001. Federal Information Processing Standards Publication 197.

[4] G. S. Vernam and J. O. Mauborgne, "One-time pad (otp) encryption," *Journal of the American Institute of Electrical Engineers*, vol. XLVI, no. 1, pp. 106–107, 1917.

[5] M. Boyer, D. Kenigsberg, and T. Mor, "Quantum key distribution with classical bob," *Phys. Rev. Lett.*, vol. 99, p. 140501, 2007.

[6] Z. Xian-Zhou, G. Wei-Gui, T. Yong-Gang, R. Zhen-Zhong, and G. Xiao-Tian, "Quantum key distribution series network protocol with m-classical bobs," *Chinese Physics B*, vol. 18, no. 6, p. 2143, 2009.

[7] J. Wang, S. Zhang, Q. Zhang, and C.-J. Tang, "Semiquantum key distribution using entangled states," *Chinese Physics Letters*, vol. 28, no. 10, p. 100301, 2011.

[8] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li, "Semiquantum-key distribution using less than four quantum states," *Phys. Rev. A*, vol. 79, p. 052312, 2009.

[9] W. O. Krawec, "Restricted attacks on semi-quantum key distribution protocols," *Quantum Information Processing*, vol. 13, pp. 2417–2436, 2014.

[10] W. O. Krawec, "Mediated semiquantum key distribution," *Phys. Rev. A*, vol. 91, p. 032323, 2015.

[11] H. Lu and Q.-Y. Cai, "Quantum key distribution with classical alice," *International Journal of Quantum Information*, vol. 06, pp. 1195–1202, 2008.

[12] A. Maitra and G. Paul, "Eavesdropping in semiquantum key distribution protocol," *Information Processing Letters*, vol. 113, no. 12, pp. 418–422, 2013.

[13] W. Zhang, D. Qiu, and P. Mateus, "Security of a single-state semi-quantum key distribution protocol," *Quantum Information Processing*, vol. 17, 2018.

[14] X. Zou, D. Qiu, L. Li, L. Wu, and L. Li, "Semiquantum-key distribution using less than four quantum states," *Phys. Rev. A*, vol. 79, p. 052312, 2009.

[15] W. O. Krawec, "Security of a semi-quantum protocol where reflections contribute to the secret key," *Quantum Information Processing*, vol. 15, pp. 2067—2090, 2016.

[16] W. O. Krawec, "Security proof of a semi-quantum key distribution protocol," in *2015 IEEE International Symposium on Information Theory (ISIT)*, pp. 686–690, 2015.

[17] H. Iqbal and W. Krawec, "High-dimensional semiquantum cryptography," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1–17, 2020.

[18] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Physical Review A*, vol. 61, pp. 0623081—06230812, 2000.

[19] Y.-g. Tan, H. Lu, and Q.-y. Cai, "Comment on "quantum key distribution with classical bob"," *Physical review letters*, vol. 102, no. 9, p. 098901, 2009.

[20] M. Boyer and T. Mor, "Comment on "semiquantum-key distribution using less than four quantum states"," *Physical Review A*, vol. 83, no. 4, p. 046301, 2011.

[21] X. Zou and D. Qiu, "Reply to "comment on 'semiquantum-key distribution using less than four quantum states' "," *Physical Review A*, vol. 83, pp. 046302–1—046302–2, 2011.

[22] P. Gurevich, *Experimental quantum key distribution with classical Alice*. The Technion - Israel Institute of Technology, Thesis Master of Science in Computer Science, 2013.

[23] Y.-y. Nie, Y.-h. Li, and Z.-s. Wang, "Semi-quantum information splitting using ghz-type states," *Quantum information processing*, vol. 12, no. 1, pp. 437–448, 2013.

[24] A. Maitra and G. Paul, "Eavesdropping in semiquantum key distribution protocol," *Information Processing Letters*, vol. 113, no. 12, pp. 418–422, 2013.

[25] M. Boyer and T. Mor, "On the robustness of quantum key distribution with classical alice (photons-based protocol)," in *Proceedings of the Ninth International Conference on Quantum, Nano/Bio, and Micro Technologies (ICQNM2015), Venice, Italy*, vol. 9, pp. 29–34, 2015.

[26] C. Xie, L. Li, and D. Qiu, "A novel semi-quantum secret sharing scheme of specific bits," *International Journal of Theoretical Physics*, vol. 54, no. 10, pp. 3819–3824, 2015.

[27] W. O. Krawec, *Semi-quantum key distribution : Protocols, security analysis, and new models*. PhD thesis, Stevens Institute of Technology, 2015.

[28] A. Yin and F. Fu, "Eavesdropping on semi-quantum secret sharing scheme of specific bits," *International Journal of Theoretical Physics*, vol. 55, no. 9, pp. 4027–4035, 2016.

[29] A. Meslouhi and Y. Hassouni, "Cryptanalysis on authenticated semi-quantum key distribution protocol using bell states," *Quantum Information Processing*, vol. 16, no. 18, pp. 1 – 17, 2017.

[30] W. Zhang, D. Qiu, and P. Mateus, "Single-state semi-quantum key distribution protocol and its security proof," *International Journal of Quantum Information*, vol. 18, no. 04, p. 2050013, 2020.

[31] C. Shukla, K. Thapliyal, and A. Pathak, "Semi-quantum communication : protocols for key agreement, controlled secure direct communication and dialogue," *Quantum Information Processing*, vol. 16, no. 12, pp. 2951 – 29519, 2017.

[32] X. Gao, S. Zhang, and Y. Chang, "Cryptanalysis and improvement of the semi-quantum secret sharing protocol," *International Journal of Theoretical Physics*, vol. 56, pp. 2512–2520, 2017.

[33] M.-H. Zhang, H.-F. Li, Z.-Q. Xia, X.-Y. Feng, and J.-Y. Peng, "Semiquantum secure direct communication using epr pairs," *Quantum Information Processing*, vol. 16, no. 5, pp. 117–1–117–14, 2017.

[34] A. Yin, Z. Wang, and F. Fu, "A novel semi-quantum secret sharing scheme based on bell states," *Modern Physics Letters B*, vol. 31, no. 13, pp. 1750150–1–1750150–6, 2017.

[35] K.-N. Zhu, N.-R. Zhou, Y.-Q. Wang, and X.-J. Wen, "Semi-quantum key distribution protocols with ghz states," *International Journal of Theoretical Physics*, vol. 57, no. 12, pp. 3621–3631, 2018.

[36] J. He, Q. Li, C. Wu, W. H. Chan, and S. Zhang, "Measurement-device-independent semiquantum key distribution," *International Journal of Quantum Information*, vol. 16, no. 2, pp. 1850012–1—1850012–10, 2018.

[37] W. O. Krawec, "Practical security of semi-quantum key distribution," in *Quantum Information Science, Sensing, and Computation X*, vol. 10660, pp. 33–45, SPIE, 2018.

[38] C. Xie, L. Li, H. Situ, and J. He, "Semi-quantum secure direct communication scheme based on bell states," *International Journal of Theoretical Physics*, vol. 57, no. 6, pp. 1881–1887, 2018.

[39] L. Liu, M. Xiao, and X. Song, "Authenticated semiquantum dialogue with secure delegated quantum computation over a collective noise channel," *Quantum Information Processing*, vol. 17, no. 12, pp. 342–1–342–17, 2018.

[40] W. Zhang, D. Qiu, and P. Mateus, "Security of a single-state semi-quantum key distribution protocol," *Quantum Information Processing*, vol. 17, pp. 135–1–135–21, 2018.

[41] L. Yan-Feng, "Semi-quantum private comparison using single photons," *International Journal of Theoretical Physics*, vol. 57, no. 10, pp. 3048–3055, 2018.

[42] T.-Y. Ye and C.-Q. Ye, "Measure-resend semi-quantum private comparison without entanglement," *International Journal of Theoretical Physics*, vol. 57, no. 12, pp. 3819–3834, 2018.

[43] X.-Q. Zhao, H.-Y. Chen, Y.-Q. Wang, and N.-R. Zhou, "Semi-quantum bi-signature scheme based on w states," *International Journal of Theoretical Physics*, vol. 58, no. 10, pp. 3239–3251, 2019.

[44] L. L. Yan, S. B. Zhang, Y. Chang, Z. W. Sheng, and F. Yang, "Mutual semi-quantum key agreement protocol using bell states," *Modern Physics Letters A*, vol. 34, no. 35, p. 1950294, 2019.

[45] L. Yan, S. Zhang, Y. Chang, Z. Sheng, and Y. Sun, "Semi-quantum key agreement and private comparison protocols using bell states," *International Journal of Theoretical Physics*, vol. 58, pp. 3852–3862, 2019.

[46] H. Lu, M. Barbeau, and A. Nayak, "Keyless semi-quantum point-to-point communication protocol with low resource requirements," *Scientific reports*, vol. 9, no. 1, pp. 64–1—64–15, 2019.

[47] C.-W. Tsai, C.-W. Yang, and N.-Y. Lee, "Lightweight mediated semi-quantum key distribution protocol," *Modern Physics Letters A*, vol. 34, no. 34, pp. 1950281–1–1950281–13, 2019.

[48] B. de Vigenere, *Traicté des chiffres, ou Secrètes manières d'escrire.* chez Abel L'Angelier, 1586.

[49] G. S. Christophe Jan, *La securite informatique*. Eyrolles, 1989.

[50] F. Kasiski, *Die geheimschriften und die dechiffrir-kunst : Mit besonderer berücksichtigung der deutschen und der französischen sprache.* E. S. Mittler und sohn, 1863.

[51] J. Daemen and V. Rijmen, *The Design of Rijndael : AES - The Advanced Encryption Standard*. Information Security and Cryptography, Springer Berlin Heidelberg, 2002.

[52] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[53] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, pp. 120–126, 1978.

[54] A. Kerckhoffs, "La cryptographie militaire," *Journal des Sciences Militaires*, pp. 161–191, 1883.

[55] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[56] E. Jochemsz and A. May, "A strategy for finding roots of multivariate polynomials with new applications in attacking rsa variants," in *Advances in Cryptology – ASIACRYPT 2006* (X. Lai and K. Chen, eds.), (Berlin, Heidelberg), pp. 267–282, Springer Berlin Heidelberg, 2006.

[57] D. Coppersmith, "Finding a small root of a bivariate integer equation ; factoring with high bits known," in *Advances in Cryptology — EUROCRYPT '96* (U. Maurer, ed.), (Berlin, Heidelberg), pp. 178–189, Springer Berlin Heidelberg, 1996.

[58] A. May, *New RSA Vulnerabilities Using Lattice Reduction Methods*. Universität Paderborn, 2003.

[59] N. Heninger and H. Shacham, "Reconstructing rsa private keys from random key bits," in *Advances in Cryptology - CRYPTO 2009* (S. Halevi, ed.), pp. 1–17, Springer Berlin Heidelberg, 2009.

[60] P.-A. Fouque, S. Kunz-Jacques, G. Martinet, F. Muller, and F. Valette, "Power attack on small rsa public exponent," in *Cryptographic Hardware and Embedded Systems - CHES 2006, 8th International Workshop*, vol. 4249 of *Lecture Notes in Computer Science*, pp. 339–353, Springer, 2006.

[61] A. K. Lenstra, "Memo on rsa signature generation in the presence of faults," 1996.

[62] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Advances in Cryptology — CRYPTO '96* (N. Koblitz, ed.), (Berlin, Heidelberg), pp. 104–113, Springer Berlin Heidelberg, 1996.

[63] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[64] S. Wiesner, "Conjugate coding," *SIGACT News*, vol. 15, pp. 78—88, 1983.

[65] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, "Quantum cryptography, or unforgeable subway tokens," in *Advances in Cryptology* (D. Chaum, R. L. Rivest, and A. T. Sherman, eds.), pp. 267–275, Springer US, 1983.

[66] C. H. Bennett and G. Brassard, "Quantum cryptography : Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, 1984.

[67] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, 1991.

[68] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the tokyo qkd network," *Opt. Express*, vol. 19, pp. 10387–10409, May 2011.

[69] R. Courtland, "China's 2,000-km quantum link is almost complete [news]," *IEEE Spectrum*, vol. 53, no. 11, pp. 11–12, 2016.

[70] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, 1992.

[71] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, pp. 3018–3021, 1998.

[72] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, pp. 1863–1869, 1995.

[73] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, 1992.

[74] D. Mayers, "Unconditionally secure quantum bit commitment is impossible," *Phys. Rev. Lett.*, vol. 78, pp. 3414–3417, 1997.

[75] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999.

[76] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Info. Comput.*, vol. 4, no. 5, pp. 325—360, 2004.

[77] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A : Mathematical, Physical and Engineering Sciences*, vol. 461, no. 2053, pp. 207–235, 2005.

[78] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, 2000.

[79] M. Dušek, M. Jahma, and N. Lütkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," *Phys. Rev. A*, vol. 62, p. 022306, 2000.

[80] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Phys. Rev. Lett.*, vol. 23, pp. 880–884, 1969.

[81] A. K. E. D. Bouwmeester and A. Zeilinger, *The Physics of Quantum Information : Quantum Cryptography, Quantum Teleportation, Quantum Computation*. Springer Berlin, 2000.

[82] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information : 10th Anniversary Edition*. Cambridge University Press, 2010.

[83] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[84] "Qiskit : An open-source framework for quantum computing," 2021.

[85] M. Boyer, R. Gelles, D. Kenigsberg, and T. Mor, "Semiquantum key distribution," *Phys. Rev. A*, vol. 79, p. 032341, 2009.

[86] V. Vedral, "The role of relative entropy in quantum information theory," *Reviews of Modern Physics*, vol. 74, no. 1, pp. 197–234, 2002.

[87] J. Schwinger, "Unitary operator bases," *Proceedings of the National Academy of Sciences*, vol. 46, pp. 570–579, 1960.

[88] I. D. Ivonovic, "Geometrical description of quantal state determination," *Journal of Physics A : Mathematical and General*, vol. 14, pp. 3241–3245, 1981.

[89] A. Fernández-Pérez, A. B. Klimov, and C. Saavedra, "Quantum process reconstruction based on mutually unbiased basis," *Phys. Rev. A*, vol. 83, p. 052332, 2011.

[90] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, "Quantum error correction and orthogonal geometry," *Phys. Rev. Lett.*, vol. 78, pp. 405–408, 1997.

[91] H. Bechmann-Pasquinucci and A. Peres, "Quantum cryptography with 3-state systems," *Phys. Rev. Lett.*, vol. 85, pp. 3313–3316, 2000.

[92] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Phys. Rev. A*, vol. 59, pp. 4238–4248, 1999.

[93] W. K. Wootters and B. D. Fields, "Optimal state-determination by mutually unbiased measurements," *Annals of Physics*, vol. 191, pp. 363 – 381, 1989.

[94] M. Christandl, R. Renner, and A. Ekert, "A generic security proof for quantum key distribution," *arXiv :quant-ph/0402131*, 2004.

[95] J. Cirac and N. Gisin, "Coherent eavesdropping strategies for the four state quantum cryptography protocol," *Phys. Lett. A*, vol. 229, 1997.

[96] H. Hajji and M. El Baz, "Qutrit-based semi-quantum key distribution protocol," *Quantum Information Processing*, vol. 20, no. 1, pp. 1–25, 2021.

[97] K. Brádler, M. Mirhosseini, R. Fickler, A. Broadbent, and R. Boyd, "Finite-key security analysis for multilevel quantum key distribution," *New Journal of Physics*, vol. 18, p. 073030, 2016.

[98] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, "On mutually unbiased bases," *International journal of quantum information*, vol. 8, no. 04, pp. 535–640, 2010.

[99] A. Acín, S. Massar, and S. Pironio, "Efficient quantum key distribution secure against no-signalling eavesdroppers," *New Journal of Physics*, vol. 8, pp. 126 – 126, 2006.

[100] F. Bouchard, K. Heshami, D. England, R. Fickler, R. W. Boyd, B.-G. Englert, L. L. Sánchez-Soto, and E. Karimi, "Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons," *Quantum*, vol. 2, p. 111, Dec. 2018.

[101] M. Boyer and T. Mor, "Comment on "semiquantum-key distribution using less than four quantum states"," *Phys. Rev. A*, vol. 83, p. 046301, Apr 2011.

[102] B. Kraus, N. Gisin, and R. Renner, "Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication.," *Physical review letters*, vol. 95 8, p. 080501, 2004.

[103] M. Christandl, R. König, and R. Renner, "Postselection technique for quantum channels with applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, p. 020504, 2009.

[104] Z.-X. Cui, W. Zhong, L. Zhou, and Y.-B. Sheng, "Measurement-device-independent quantum key distribution with hyper-encoding," *SCIENCE CHINA Physics, Mechanics & Astronomy*, vol. 62, no. 11, p. 110311, 2019.

[105] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, July 1948.

[106] F. Deng and G. Long, "Bidirectional quantum key distribution protocol with practical faint laser pulses," *Physical Review A*, vol. 70, p. 012311, 2004.

[107] J. Wang, S. Zhang, Q. Zhang, and C.-J. Tang, "Semiquantum key distribution using entangled states," *Chinese Physics Letters*, vol. 28, p. 100301, 2011.

[108] W. O. Krawec, "Quantum key distribution with mismatched measurements over arbitrary channels," *Quantum Info. Comput.*, vol. 17, pp. 209—241, 2017.

[109] Y.-P. Luo and T. Hwang, "Authenticated semi-quantum direct communication protocols using bell states," *Quantum Information Processing*, vol. 15, pp. 947–958, 2016.

[110] Q. Li, W. H. Chan, and D.-Y. Long, "Semiquantum secret sharing using entangled states," *Phys. Rev. A*, vol. 82, p. 022303, 2010.

[111] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner, "Security of two-way quantum key distribution," *Physical Review A*, vol. 88, pp. 062302–1–062302–9, 2013.

[112] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High-bit-rate continuous-variable quantum key distribution," *Physical Review A*, vol. 90, p. 042329, 2014.

[113] Q. Li, W. Chan, and S. Zhang, "Semiquantum key distribution with secure delegated quantum computation," *Scientific Reports*, vol. 6, 2015.

[114] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Physical Review A*, vol. 72, 2005.

[115] R. Renner, "Symmetry of large physical systems implies independence of subsystems," *Nature Physics*, vol. 3, pp. 645–649, 2007.

[116] C. Shukla, K. Thapliyal, and A. Pathak, "Semi-quantum communication : Protocols for key agreement, controlled secure direct communication and dialogue," *Quantum Information Processing*, vol. 16, 2017.

[117] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, 2009.

[118] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," *Physical Review X*, 2019.

[119] K. Thapliyal, R. D. Sharma, and A. Pathak, "Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment," *International Journal of Quantum Information*, vol. 16, p. 1850047, 2018.

[120] W. Zhang and D. Qiu, "A single-state semi-quantum key distribution protocol and its security proof," *arXiv :quant-ph/1612.03087*, 2016.

[121] W.-H. Chou, T. Hwang, and J. Gu, "Semi-quantum private comparison protocol under an almost-dishonest third party," *arXiv :quant-ph/1607.07961*, 2016.

[122] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, "Qudits and high-dimensional quantum computing," *arXiv preprint arXiv :2008.00959*, 2020.

[123] X. Zou, D. Qiu, S. Zhang, and P. Mateus, "Semiquantum key distribution without invoking the classical party's measurement capability," *Quantum Information Processing*, vol. 14, pp. 2981–2996, 2015.

[124] K.-F. Yu, C.-W. Yang, C.-H. Liao, and T. Hwang, "Authenticated semi-quantum key distribution protocol using bell states," *Quantum Information Processing*, vol. 13, p. 1457–1465, 2014.

[125] C.-W. Yang and T. Hwang, "Efficient key construction on semi-quantum secret sharing protocols," *International Journal of Quantum Information*, vol. 11, no. 05, p. 1350052, 2013.

[126] K.-F. Yu, J. Gu, T. Hwang, and P. Gope, "Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing," *Quantum Information Processing*, vol. 16, p. 194, 2017.

[127] L. Yan-Feng, "Semi-quantum private comparison using single photons," *International Journal of Theoretical Physics*, vol. 57, pp. 3048–3055, 2018.

[128] X. Zou and D. Qiu, "Three-step semiquantum secure direct communication protocol," *Science China Physics, Mechanics and Astronomy*, vol. 57, 2014.

[129] J. Boutros, *Réseaux de points pour les canaux à évanouissements.* PhD thesis, E.N.S.T., Paris, 1996.

[130] O. Amer and W. O. Krawec, "Semiquantum key distribution with high quantum noise tolerance," *Physical Review A*, 2018.

[131] C.-W. Tsai and C.-W. Yang, "Lightweight authenticated semi-quantum key distribution protocol without trojan horse attack," *Laser Physics Letters*, vol. 17, 2020.

[132] C.-L. Tsai and T. Hwang, "Semi-quantum key distribution robust against combined collective noise," *International Journal of Theoretical Physics*, vol. 57, pp. 3410–3418, 2018.

[133] D. Bacco, M. Canale, N. Laurenti, G. Vallone, and P. Villoresi, "Experimental quantum key distribution with finite-key security analysis for noisy channels," *Nature Communications*, vol. 4, 2013.

[134] P. hua Lin, C.-W. Tsai, and T. Hwang, "Mediated semi-quantum key distribution using single photons," *Annalen der Physik*, vol. 531, 2019.

[135] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber.," *Physical review letters*, vol. 125 1, p. 010502, 2020.

[136] M. Wang, L.-M. Gong, and L.-H. Shao, "Efficient semiquantum key distribution without entanglement," *Quantum Information Processing*, vol. 18, 2019.

[137] M. Boyer, R. Liss, and T. Mor, "Attacks against a simplified experimentally feasible semiquantum key distribution protocol," *Entropy*, vol. 20, 2018.

[138] R. Schwonnek, K. T. Goh, I. W. Primaatmaja, E. Y. Tan, R. Wolf, V. Scarani, and C. Lim, "Device-independent quantum key distribution with random key basis," *Nature Communications*, vol. 12, 2020.

[139] M. Zhang, H. Li, J. Peng, and X. Feng, "Fault-tolerant semiquantum key distribution over a collective-dephasing noise channel," *International Journal of Theoretical Physics*, vol. 56, pp. 2659–2670, 2017.

[140] X. Zou, D. Qiu, S. Zhang, and P. Mateus, "Semiquantum key distribution without invoking the classical party's measurement capability," *Quantum Information Processing*, vol. 14, pp. 2981–2996, 2015.

[141] T. Miyadera, "Relation between information and disturbance in quantum key distribution protocol with classical alice," *International Journal of Quantum Information*, vol. 09, pp. 1427–1435, 2011.

[142] N. Zhou, K.-N. Zhu, and Y. Wang, "Three-party semi-quantum key agreement protocol," *International Journal of Theoretical Physics*, vol. 59, pp. 663–676, 2020.

[143] L.-Y. Chen, L. Gong, and N. Zhou, "Two semi-quantum key distribution protocols with g-like states," *International Journal of Theoretical Physics*, vol. 59, pp. 1884–1896, 2020.

[144] Y.-C. Lu, C.-W. Tsai, and T. Hwang, "Collective attack and improvement on "mediated semi-quantum key distribution using single photons"," *Annalen der Physik*, vol. 532, 2020.

[145] I. W. Primaatmaja, C. C. Liang, G. Zhang, J. Y. Haw, C. Wang, and C. Lim, "Discrete-variable quantum key distribution with homodyne detection," *Quantum*, vol. 6, p. 613, 2021.

[146] W. Liu and H. Zhou, "A new semi-quantum key distribution protocol with high efficiency," *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, pp. 2424–2427, 2018.

[147] G. Gao, Y. Wang, and D. Wang, "Multiparty semiquantum secret sharing based on rearranging orders of qubits," *Modern Physics Letters B*, vol. 30, p. 1650130, 2016.

[148] C.-W. Yang and C.-W. Tsai, "Intercept-and-resend attack and improvement of semiquantum secure direct communication using epr pairs," *Quantum Information Processing*, vol. 18, 2019.

[149] Y. Chongqiang, L. Jian, C. Xiubo, T. Yuan, and H. Yanyan, "An efficient semiquantum key distribution protocol and its security proof," *IEEE Communications Letters*, vol. 26, pp. 1226–1230, 2022.

[150] J. Anderson, "The TURBO Coding Scheme," in *Proceedings of ISIT '94*, (Trondheim, Norway), 1994.

[151] D. Divsalar and F. Pollara, "Turbo Codes for Deep-Space Communications," TDA Progress Report 43-120, Jet Propulsion Laboratory (JPL), Feb. 1995.

[152] W. O. Krawec, R. Liss, and T. Mor, "Security proof against collective attacks for an experimentally feasible semi-quantum key distribution protocol," 2020.

[153] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. USA : Wiley-Interscience, 2006.

[154] D. J. C. MacKay, *Information Theory, Inference, and Learning Algorithms*. Copyright Cambridge University Press, 2003.

[155] A. Peres, *Quantum theory : concepts and methods*, vol. 57. Springer Science & Business Media, 2006.

ROYAUME DU MAROC
Université Mohammed V - RABAT -
جامعة محمد الخامس – الرباط –
Faculté des sciences
كلية العلوم
CENTRE D'ÉTUDES DOCTORALES - SCIENCES ET TECHNOLOGIES

Résumé

La préservation de la confidentialité lors de la transmission des informations sensibles a constamment suscité une préoccupation significative au sein de la société. Avec l'avènement de l'ère numérique, de nouvelles stratégies ont été développées pour assurer la sécurité des échanges et pour préserver l'intégrité des données. Au milieu de ces approches innovantes, la distribution semi-quantique de clés a émergé en tant que méthode pleine de potentiel, provoquant ainsi un intérêt considérable dans le domaine de la sécurité de l'information. Le travail présenté dans cette thèse se focalise sur l'analyse et l'amélioration des protocoles de distribution semi-quantique de clés. Dans un premier temps, nous introduisons une vision globale sur la cryptographie classique allant des principes fondamentaux jusqu'aux algorithmes les plus utilisés. Puis nous retraçons l'évolution de la distribution quantique des clés au fil du temps, nous présentons également une étude détaillée des protocoles couramment utilisés pour les qubits unique et pour les qubits intriqués. Ensuite, nous procédons à une analyse de la sécurité du protocole de distribution de clés semi-quantique en utilisant des états quantiques tridimensionnels et quadridimensionnels, et ce, dans le contexte d'une évaluation de leur résistance aux attaques collectives. Par la suite, nous orientons notre attention vers l'étude d'une stratégie optimale d'interception. Cette approche repose sur la quantification de l'information mutuelle partagée entre Alice et Eve, en prenant en considération une perturbation prédéfinie. Finalement, notre recherche se concentre sur l'évaluation de la robustesse du protocole de distribution semi-quantique de clés contre une stratégie d'interception individuelle appliquée aux ensembles d'états bidimensionnels soumis à une altération par un bruit blanc.

Mots-clés (4): Information quantique, Sécurité des protocoles semi-quantiques, cryptographie classique, distribution de clé quantique.

Abstract

Preserving confidentiality while transmitting sensitive information has always been a significant concern within society. With the advent of the digital age, new strategies have been developed to ensure secure exchanges and maintain data integrity. Amidst these innovative approaches, semi-quantum key distribution has emerged as a promising method, garnering considerable interest in the field of information security. The work presented in this thesis focuses on analyzing and enhancing semi-quantum key distribution protocols. Initially, we provide an overview of classical cryptography, ranging from fundamental principles to widely used algorithms. Then, we trace the evolution of quantum key distribution over time, presenting a detailed study of protocols commonly used for single qubits and entangled qubits. Subsequently, we analyze the security of the semi-quantum key distribution protocol using three-dimensional and four-dimensional quantum states. This analysis aims to determine the protocol's resilience against collective attacks. Later, we turn our focus toward analyzing an optimal interception strategy. This approach is based on quantifying the mutual information shared between Alice and Eve while considering a predefined perturbation. Finally, our research centers on evaluating the robustness of the semi-quantum key distribution protocol against an individual interception strategy applied to sets of two-dimensional states subjected to the addition of quantum noise.

Key Words (4): Quantum information, semi-quantum protocol security, classical cryptography, quantum key distribution.

✉ Faculté des Sciences, avenue Ibn Battouta, BP. 1014 RP, Rabat –Maroc
☎ 00212 (05) 37 77 18 76 🖷 00212(05) 37 77 42 61; http://www. fsr.um5.ac.ma