# Résumé de manuscrit : Cryptographie à clé secrète et attaquant quantique dans le monde des télécommunications

Paul Frixons
Orange Labs, Caen
Inria, Paris

Encadré par :

| | | |
|---|---|---|
| María Naya-Plasencia | Inria de Paris | Directrice |
| Sébastien Canard | Orange Labs | Co-directeur |
| Loïc Ferreira | Orange Labs | Co-encadrant |


La cryptographie est la science de la protection des données ainsi que la transmission d'information dans un canal non sécurisé. Elle accompagne les communications de l'antiquité à nos jours modernes. Cependant, elle n'est devenue une branche des mathématiques que dans le 20ème siècle associée à la théorie de la complexité, l'étude de la difficulté des problèmes.

## 1 Contexte

**Sécurité computationelle.** La cryptographie moderne est composée d'un certain ensemble d'outils, des objets mathématiques qui maintiennent la sécurité jusqu'à une borne de calcul. En effet, ces outils sont conçus pour rendre l'information illisible à toute entité non autorisée (ou adversaire) jusqu'à ce qu'elle dépense une certaine quantité (inaccessible) de ressources.

Il y a plusieurs façons d'assurer ce genre de sécurité. La première, usuellement appelée cryptographie à clé publique, est de se fier à la difficulté d'un problème général. Par exemple, RSA (l'un des cryptosystèmes les plus utilisés) repose sur la difficulté du problème de factorisation. Cette façon de construire est puissante, de nombreux outils pouvant être construits à partir d'un seul problème. De ce fait, le principal objectif de la vérification est le problème sous-jacent. Cependant, l'instanciation est toujours passée sous observation minutieuse (de nombreuses premières versions de RSA étaient vulnérables). La deuxième, usuellement appelée cryptographie à clé secrète, consiste à concevoir des éléments de base appelés « primitives » qui sont au centre de l'évaluation de la sécurité. Ensuite, ceux-ci peuvent être utilisés avec des modes opératoires qui permettent à ces primitives de chiffrer des messages pratiquement. Ces modes opératoires

sont également prouvés comme étant sûrs pour assurer la sécurité de l'ensemble du processus.

**Menace quantique.** Le concept d'ordinateurs quantiques a été proposé au début des années 1980 par des physiciens visionnaires. Simuler l'évolution de systèmes quantiques complexes, comme de longues molécules, est un problème difficile pour nos ordinateurs. Le concept des ordinateurs quantiques est de renverser ce problème, faisant des systèmes quantiques une nouvelle façon de calculer. Les physiciens qui ont travaillé dans cette direction ont rapidement compris que cela mènerait à un ordinateur quantique exécutant des algorithmes quantiques avec une notion de complexité propre.

La première démonstration des possibilités de l'informatique quantique a été faite en 1992 avec l'algorithme Deutsch-Jozsa, qui indique si une fonction de $\{0,1\}^n$ vers $\{0,1\}$ est constante ou équilibrée ($|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$) dans une seule requête, alors qu'un ordinateur classique en a besoin de $2^{n-1}+1$ pour obtenir la même certitude. Il a été suivi de près par l'algorithme de Simon et l'algorithme de Shor, tous deux en 1994. Le premier trouve des périodes cachées et le second factorise de grands nombres.

Or, la factorisation de grands nombres est justement le problème sur lequel RSA repose pour sa sécurité.

La réalisation de tels ordinateurs quantiques a commencé en 1998 avec un ordinateur à deux qubits fonctionnels implémentant l'algorithme Deutsch-Jozsa. Il a été suivi par la première factorisation utilisant l'algorithme de Shor en 2001 par IBM avec une machine à 7 qubits. Une autre étape importante a été la revendication par Google d'avoir atteint la suprématie quantique (avoir un ordinateur quantique résolvant un problème qui serait « irréalisable » pour tout ordinateur classique existant) en 2019. Aujourd'hui, nous en sommes au point qu'IBM promet un ordinateur à 1121 qubits en 2023 et un autre contenant un million de qubits d'ici 2030.

**Cryptanalyse quantique.** Nous avons confiance dans la sécurité des différentes constructions cryptographiques en contestant leurs limites de sécurité revendiquées. La cryptanalyse est l'ensemble des techniques utilisées et développées de cette manière.

La considération de l'ordinateur quantique comme un adversaire potentiel a conduit à de nombreuses nouvelles attaques et techniques connues comme cryptanalyse quantique. Alors que de nombreux systèmes et constructions ont été brisés, le véritable potentiel de l'informatique quantique est encore inconnu. En effet, les algorithmes quantiques découverts sont rares et même la combinaison d'algorithmes quantiques existants reste en majorité de l'ordre de l'inconnu.

**Preuves de sécurité.** La sécurité prouvable en tant que domaine a pour but de prouver la sécurité de diverses constructions sur l'hypothèse de la sécurité des blocs sous-jacents. Alors que nous sommes loin de déterminer la sécurité de chaque construction de cette façon, la sécurité prouvable a de nombreux outils à sa disposition contre les adversaires classiques.

Cependant, contre les adversaires quantiques beaucoup de ces outils ne sont pas efficaces car de nombreuses notions qui semblent triviales dans le monde classique sont caduques dans le monde quantique.

**Protocoles quantiques.** Comme la cryptographie consiste à transmettre l'information de manière sécurisée dans un canal non sécurisé, elle implique de bien maîtriser la façon dont l'information est globalement protéger dans ledit canal. Les protocoles cryptographiques peuvent être définis comme des procédures impliquant deux ou plusieurs entités légitimes dans le but de transmettre de façon sécurisée certaines informations et de vérifier certaines propriétés de sécurité.

De la même manière que les ordinateurs quantiques ont été conceptualisés en raison de la complexité des systèmes quantiques, la plupart des protocoles quantiques utilisent les propriétés de la mécanique quantique pour construire des matériaux inforgeables.

# 2 Objectifs et état de l'art

La zone d'impact d'un attaquant ayant accès à un ordinateur quantique est large dans le champ de la cryptographie et l'est d'autant plus encore dans un monde où l'ordinateur quantique a remplacé son équivalent classique. Aussi l'objectif de cette thèse est de couvrir le plus grand nombre de domaines possibles .

**Cryptanalyse quantique.** Bien que pour la cryptographie à clé publique, l'algorithme de Shor représente une menace quantique bien définie, la cryptographie à clé secrète n'a, pour un temps, vu que la présence de l'algorithme de Grover et l'idée était que la menace quantique pouvait être parée "juste" en doublant la taille des clés.

Cependant, en 2010, une première attaque quantique contredit cette pensée. En effet, Kuwakado et Morii montrent que l'algorithme de Simon, qui permet de chercher des périodes cachées en temps très réduit, peut être appliqué à la cryptanalyse des réseaux de Feistel, ici réduite à 3 tours, une construction célèbre pour son utilisation dans le DES (Data Encryption Standard), le standard du chiffrement à bloc jusqu'à son remplacement par l'AES (Advanced Encryption Standard) en 2001.

En 2012, ils réitèrent leur démonstration en attaquant la construction de chiffrement Even-Mansour, à la différence que cette fois-ci l'attaque récupère la clé.

En 2016, Kaplan, Leurent, Leverrier et Naya-Plasencia développent une série d'attaques quantiques qui consistent à retrouver des périodes cachées en utilisant l'algorithme de Simon. Ils brisent ainsi plusieurs schémas dont la construction LRW pour les chiffrements à bloc modifiables, les constructions CBC-MAC, PMAC, GMAC pour les codes d'authentification de messages et les constructions GCM et OCB pour les chiffrements authentifiés. Ceci a pour effet de mobiliser la communauté internationale sur ce sujet de la cryptanalyse quantique.

En 2017, Leander et May attaquent la construction d'extension de clé FX. Cette attaque est par ailleurs la première à combiner différents algorithmes quantiques, ici un algorithme de Simon est utilisé à l'intérieur d'une recherche par l'algorithme de Grover.

En 2019, Bonnetain, Hosoyamada, Naya-Plasencia, Sasaki et Schrottenloher développent une nouvelle attaque sur la construction Even-Mansour. Cette

dernière a la particularité de n'utiliser que des requêtes classiques, une première dans le domaine de la cryptanalyse quantique.

En 2021, Bonnetain, Leurent, Naya-Plasencia et Schrottenloher montrent un nouveau type d'attaques quantiques, nommées attaques par linéarisation. Ce qui fait leur nouveauté est l'utilisation de l'algorithme de Deutsch-Jozsa, ce qui étend les propriétés attaquables.

En partant de ces différents résultats, l'objectif de ce doctorat est d'améliorer notre connaissance dans ce domaine en montrant de nouvelles attaques et manières de mener ces attaques. Dans ce domaine, nous avons obtenu trois résultats [2, 1, 3].

**Preuves de sécurité.** Comme énoncé plus haut, les preuves de sécurité sont des théorèmes mathématiques qui réduisent la sécurité d'une construction à celle des primitives qu'elle emploie dans un certain modèle d'adversaire.

Pour construire ces preuves, des techniques maintenant bien maîtrisées sont généralement utilisées. La plus commune est celle du coefficient "H". Elle consiste à considérer le transcrit (l'ensemble des requêtes et réponses associées) de l'adversaire. Si nous arrivons à définir un ensemble de transcrits $A$ suffisamment grand et tel que la probabilité que l'adversaire obtienne un transcrit de $A$ est proche de ce que l'on pourrait attendre d'une construction parfaite, alors l'adversaire n'a pas d'avantage significatif pour distinguer la construction étudiée de la perfection.

Cependant, dès que l'adversaire a droit à des requêtes en superposition, ces considérations volent en éclat : le transcrit devient aussi une superposition qui peut contenir plus d'information que son équivalent classique, ce qui rend tout encadrement de celui-ci non trivial.

Une première méthode efficace qui permet de minorer le nombre nécessaire de requêtes quantiques pour résoudre un problème apparaît en 2001 par Beals, Buhrman, Cleve, Mosca et De Wolf. Cette méthode consiste à considérer la réponse du meilleur algorithme quantique comme un polynôme en les données, lier le degré du polynôme au nombre de requêtes de l'algorithme et d'exhiber une suite d'entrés possibles suffisamment longue pour minorer le degré du polynôme. Cette méthode a servi à donner une borne inférieure de la complexité de la recherche quantique de collision en 2004 par Aaronson et Shi, mais n'a pas servi directement à la construction de preuves de sécurité en cryptographie étant donné sa difficulté d'application.

La deuxième méthode connue est nommée oracle d'enregistrement, développé par Zhandry en 2018. Elle consiste à considérer la construction des transcrits et permet de "voir" la superposition des transcrits comme une base de données partielle dont on peut séparer la partie où la construction étudiée apparait comme parfaite du reste sous certaines conditions. Cette méthode a servi à montrer la sécurité de 4 tours de réseaux de Feistel en tant que fonction pseudo-aléatoire en 2019 par Hosoyamada et Iwata.

Le but de cette thèse dans ce domaine est de mener à bien de nouvelles preuves de sécurité dans le cadre quantique mais aussi classique.

**Protocoles dans un monde quantique.** Le domaine des protocoles quantiques existe depuis presque aussi longtemps que celui de l'ordinateur quantique avec le protocole BB84 proposé en 1984 par Bennett et Brassard. Depuis, un

certain nombre de protocoles basés sur les propriétés de la mécanique quantique ont vu le jour.

Cependant, un dénominateur commun de ces protocoles est le fait de se baser sur la sécurité inconditionnelle, ce qui restreint les possibilités de conception et surtout exclus les constructions actuelles.

Dans ce sens, en 2020, Music, Chevalier et Kashefi ont établi une attaque quantique contre le protocole de Yao, pionnier dans le calcul multipartite. La même année, Ebrahimi, Chevalier, Kaplan et Minelli ont attaqué un protocole de transfert évident, brique fondamentale du calcul multipartite. Ces deux travaux joints forment une première compréhension de l'impact de l'ordinateur quantique sur le monde des protocoles.

L'objectif de ce manuscrit de thèse dans ce domaine est de formaliser un modèle d'attaquant quantique cohérent avec un monde où les échanges sont en superposition et de prouver la possibilité d'un protocole calculatoirement sûr dans ce cadre qui ouvre tant de possibilités d'attaque.

# 3 Publications et pré-publications

Au cours de ce travail doctoral, quatre articles scientifiques ont été rédigés. Deux ont été acceptés en conférences internationales. Deux autres sont en cours de soumissions en conférences.


[1] Paul Frixons, María Naya-Plasencia, and André Schrottenloher. "Quantum Boomerang Attacks and Some Applications." *International Conference on Selected Areas in Cryptography.* Springer, Cham, 2022.

[2] Paul Frixons, and André Schrottenloher. "Quantum security of the legendre prf." *Mathematical Cryptology* 1.2 (2021) : 52-69.

[3] Ritam Bhaumik, André Chailloux, Paul Frixons, and María Naya-Plasencia. "Safely Doubling your Block Ciphers for a Post-Quantum World."

[4] Sébastien Canard, Loïc Ferreira, and Paul Frixons. "Quantum Security of the UMTS-AKA Protocol and its Primitives, Milenage and TUAK."


# 4 Contributions

Les contributions de cette thèse dans les domaines introduits ci-dessus sont très diverses.

**Algorithmique quantique.** Nous avons développé la première instance d'un algorithme Offline-Kuperberg ([2]), c'est-à-dire un algorithme quantique qui, à partir de requêtes classiques, trouve un décalage caché en utilisant l'algorithme Kuperberg. Nous l'avons appliqué au problème de symboles de Legendre décalés avec succès. Cette méthode est intéressante car elle rivalise asymptotiquement avec la recherche de collision basée sur une table, qui doit utiliser de la QRAM, une hypothèse supplémentaire. C'est aussi le seul algorithme connu de ce genre en plus de l'algorithme Offline-Simon.

**Cryptanalyse quantique.** Notre contribution dans ce domaine est double.

**Quantification des attaques classiques.** Nous avons proposé une attaque boomerang quantique efficace ([1]), ainsi qu'une variante pour les attaques mixing-boomerang. Nous avons proposé plusieurs améliorations pour différents cas, comme la réduction de la QRAM nécessaire ou faire des attaques $Q2$ qui fonctionnent en $Q1$ dans certaines circonstances. Dans certains cas, nos attaques atteignent une accélération quadratique par rapport aux attaques classiques. Cela montre que les attaques boomerang sont également des outils de cryptanalyse performants pour le monde post-quantique, qui seront nécessaires pour déterminer correctement les meilleures marges de sécurité.

**Nouvelle attaque quantique.** Nous avons présenté un nouveau type d'attaque basée sur l'algorithme de Simon sur la construction Encrypt-Mix-Encrypt (EME) [3]. Bien qu'une période n'apparaisse pas dans les différentes fonctions, ce qui était au centre des précédentes attaques basées sur l'algorithme de Simon, nous avons trouvé une périodicité dans l'ensemble des collisions, et effectué une attaque de récupération de clé.

**Nouvelle construction.** Nous avons proposé une nouvelle construction QuEME pour doubler les tailles de clés et d'état [3].

**Preuves de sécurité (quantique).** Notre contribution dans ce domaine est triple.

- Nous avons obtenu une preuve de sécurité IND-CCA pour notre nouvelle construction qui permet à un attaquant (classique) d'utiliser suffisamment de requêtes pour contenir une partie importante la table de valeur des sous-permutations, une borne non communément atteinte [3].
- Nous avons réussi à faire la première preuve de sécurité contre un attaquant quantique qui a accès aux chiffrement et déchiffrement, faisant de QuEME la première construction de chiffrement de bloc résistante aux attaques quantiques [3].
- Nous avons prouvé la sécurité de Milenage et TUAK comme primitives d'un UMTS-AKA quantique ([4]).

**Preuve de sécurité pour protocoles quantiques.** Nous avons proposé une version quantique du protocole UMTS-AKA et prouvé sa sécurité quantique. À notre connaissance, il s'agit de la première preuve rigoureuse de sécurité de ce type de protocoles dans un environnement quantique complet ([4]).

# 5 Organisation

Ce mémoire est construit de la manière suivante :

**Chapitre 1.** Nous présentons les outils de l'informatique quantique utilisés dans les chapitres suivants. Il commence par une histoire rapide du domaine et se poursuit avec les notions élémentaires de l'informatique quantique : qubits, superposition, intrication, opérateurs et complexité quantique.

**Chapitre 2.** Nous exposons les principaux blocs de construction algorithmique qui pavent notre travail : recherche de Grover et sa généralisation, l'algorithme d'amplification d'amplitude, recherche de collision BHT, Algorithme de Shor, algorithme de recherche de Simon et certaines de ses complexités et algorithme de Kuperberg.

**Chapitre 3.** Nous présentons les notions de cryptographie nécessaires aux chapitres suivants. Il commence par un aperçu du domaine, y compris la cryptographie asymétrique, la cryptographie symétrique et ses constructions. Il poursuit avec des bases de cryptanalyse et des notions spécifiques liées à la cryptanalyse quantique. Il se termine par un aperçu des protocoles de communication.

**Chapitre 4.** Nous exposons de nouvelles attaques quantiques contre la fonction pseudo aléatoire de Legendre, issues d'un travail conjoint avec André Schrottenloher, publié à MathCrypt en 2021 [2].

Nous présentons deux algorithmes quantiques pour résoudre le problème de décalage caché de Legendre (SLS) lorsque des requêtes classiques sont données, et sans RAM quantique. Le premier (collisions basées sur des tables) permet d'obtenir un avantage par rapport à l'algorithme de Grover lorsque plus de données sont fournies. Le second est l'algorithme Offline-Kuperberg, un développement inédit dans le domaine de l'algorithmique quantique qui permet d'utiliser l'algorithme de Kuperberg en tant que routine d'une recherche plus large.

**Chapitre 5.** Il est basé sur un travail conjoint avec Marìa Naya-Plasencia et André Schrottenloher publié à Selected Areas in Cryptography en 2021 [1].

Nous proposons une attaque de boomerang quantique efficace, ainsi qu'une variante pour mélanger les attaques de boomerang. Nous proposons plusieurs améliorations pour différents cas, car la réduction du besoin en RAM quantique ou la réalisation d'attaques $Q2$ fonctionnent en $Q1$ dans certaines circonstances. Dans certains cas, nos attaques atteignent une accélération quadratique par rapport aux attaques classiques. Cela montre que les attaques boomerang sont également des outils de cryptanalyse performants pour le monde post-quantique, qui seront nécessaires pour déterminer correctement les meilleures marges de sécurité.

**Chapitre 6.** Nous présentons un travail conjoint avec Marìa Naya-Plasencia, Ritam Bhaumik et André Chailloux qui est actuellement soumis en conférence internationale [3].

Il se concentre sur la construction EME. Nous présentons la première proposition d'un moyen générique pour étendre la clé et la taille de l'état, avec des arguments de sécurité quantique et des preuves classiques significatives. En outre, nous proposons un nouveau type d'attaques de superposition sur la construction EME, un distingueur original correspondant à la limite de notre construction, et une méthode envisageant des simulations pour soutenir les conjectures à partir de preuves.

**Chapitre 7.** Il est basé sur un travail conjoint avec Sébastien Canard et Loïc Ferreira qui est actuellement en cours de soumission en conférence internationale [4]. Nous définissons d'abord un modèle de sécurité qui ne repose pas sur une sécurité inconditionnelle et qui permet aux parties

honnêtes et aux attaquants d'utiliser des messages de superposition. En particulier, en supposant que nous sommes dans un monde quantique, nous fournissons une discussion sur ce qui peut être mis en superposition par le client, le serveur et l'opérateur lors d'une exécution honnête de la version quantique du protocole UMTS-AKA. Plus précisément, cette version suppose des calculs quantiques ainsi que des communications quantiques (c'est-à-dire que les messages échangés entre les parties sont dans une superposition d'états quantiques).

Nous prouvons alors formellement que cette version quantique de l'UMTS-AKA est aussi sécurisée dans ce modèle quantique que dans le contexte classique. Comme contribution supplémentaire, nous montrons également une nouvelle attaque contre la confidentialité de l'état d'un utilisateur mobile. Cette attaque entre dans le contexte quantique mais aussi dans le contexte classique.

Nous étudions enfin la sécurité des primitives sous-jacentes qui peuvent instancier UMTS-AKA, Milenage et TUAK. Nous montrons une attaque sur Milenage comme qPRF, mais le contexte de UMTS-AKA rend cette attaque irréaliste et nous prouvons encore la sécurité de Milenage basée sur la sécurité d'AES. Nous montrons également une réduction de la sécurité de TUAK à la sécurité de Keccak-f.

# 6 Conclusion

Dans ce mémoire de thèse doctorale, nous avons effectué un certain nombre de travaux autour de la cryptographie quantique. Nous avons fait avancer l'algorithmique quantique par la construction de l'algorithme Offline-Simon et la cryptanalyse quantique de part l'adaptation d'attaques classiques et en découvrant une nouvelle attaque. Nous avons contribué à la sécurité prouvable en apportant de nouvelles preuves dans le contexte classique et dans le contexte quantique pour une nouvelle construction. Nous avons établi les premières preuves de sécurité pour un protocole quantique basé sur la sécurité calculatoire.

Pour terminer, nous proposons ici quelques problèmes ouverts.

**Nouveaux algorithmes quantiques.** Bien que cette thèse ne montre aucune nouvelle brique algorithmique quantique, elle n'exclut certainement pas la possibilité d'un nouvel algorithme qui modifierait l'état de la cryptanalyse quantique dans quelques années.

Même sans découvrir un algorithme aussi dévastateur, l'amélioration des algorithmes quantiques connus n'est pas à perdre de vue. Un exemple peut être l'algorithme de Kuperberg, qui a vu de nombreuses itérations d'amélioration depuis sa découverte.

**Cryptanalyse quantique.** En parlant de cryptanalyse quantique, il y a encore beaucoup à découvrir sur l'algorithme de décalage caché et leurs applications. Par exemple, nous avons exposé dans cette thèse une nouvelle façon d'utiliser l'algorithme de Simon avec des sous-structures et d'élargir le type de propriétés qui peuvent être exploitées. Cette technique a été développée pour le cas de la construction EME avec l'ensemble de collision. Il pourrait être utile de

rechercher d'autres structures (conduisant à plus de propriétés à exploiter) et d'autres constructions (ce qui en fait une approche plus générale).

**Algorithmes quantiques hors ligne.** Bien que les attaques quantiques « hors ligne » actuelles nécessitent la connaissance des subtilités de l'attaque initiale pour se réaliser, ces attaques originales sont une application directe de l'algorithme de Simon ou de Kuperberg. Il serait intéressant d'examiner d'autres attaques quantiques fondées sur ces algorithmes.

Une autre approche est de chercher d'autres algorithmes quantiques pour faire des algorithmes hors ligne. Une possibilité pourrait être de considérer les attaques de linéarisation.

**Outils pour les épreuves de sécurité quantiques.** Alors que le domaine des preuves de sécurité contre les adversaires quantiques a évolué pour adapter de nombreux outils des preuves de sécurité contre les adversaires classiques, beaucoup manquent encore. L'étape la plus immédiate consiste à créer un oracle d'enregistrement pour les permutations aléatoires sur la base de ce qui existe pour les fonctions aléatoires.

**Protocoles quantiques.** Notre travail sur le protocole UMTS-AKA est un début pour les protocoles quantiques reposant sur la sécurité des primitives plus petites. Une possibilité de continuation est de chercher d'autres propriétés, comme la confidentialité revendiquée pour la version 5G du protocole UMTS-AKA. Une autre possibilité est de regarder d'autres protocoles.