Le quantique, c'est fantastique !

Xavier Bonnetain
xavier.bonnetain@inria.fr

Inria

Résumé. L'informatique quantique est un sujet à la mode, dans lequel de nombreux états et grandes entreprises investissent des millions, si ce n'est des milliards de dollars. Cet article propose un panorama des conséquences de l'apparition de l'informatique quantique en cryptographie, tant du côté des primitives cryptographiques, symétriques et asymétriques, que des protocoles de communication.

1 L'informatique quantique ?

L'idée de faire des calculs en utilisant la mécanique quantique vient de la fin du XX^{e} siècle. La mécanique quantique décrit très bien notre réalité, mais l'étude théorique de systèmes quantiques complexes est très difficile. De plus, il n'est pas toujours envisageable de faire l'expérience, et ces systèmes sont bien souvent trop compliqués pour être simulés par ordinateur. Reste alors une autre possibilité : au lieu de faire directement l'expérience, utiliser une « maquette » dont le comportement sera similaire, mais qui sera plus facile à étudier. Cette idée de *simulateur quantique*, proposée par Feynman en 1982 [13], mènera à celle d'*ordinateur quantique*, où l'on ne cherche plus à simuler la nature, mais simplement à calculer plus efficacement.

Tout comme classiquement, où une tension peut représenter un 0 ou un 1, quantiquement, les valeurs sont encodées dans un *état quantique* (on peut penser à la position d'une particule, à l'énergie ou au spin d'un atome, et on parle d'*observable*), que l'on peut mesurer pour obtenir un nombre. Les opérations analogues aux portes logiques sont les *portes quantiques*, qui vont transformer un état quantique en un autre.

La différence fondamentale est qu'un observable n'a pas nécessairement une valeur fixée. Il peut être superposé entre plusieurs valeurs, et si on le mesure, on obtiendra une valeur parmi celles de la superposition. De plus, cette mesure projette l'état quantique, supprimant de la superposition toutes les valeurs incompatibles avec la mesure (notamment, si l'on mesure plusieurs fois de suite, on obtiendra toujours le même résultat). Enfin, contrairement à une valeur classique, il n'est pas possible de copier un état quantique, hormis en refaisant le processus qui l'a créé.

1.1 L'informatique quantique en une page

L'analogue quantique du bit est le qubit. Si les chaînes de bits vivent dans $\{0,1\}^n$, les qubits, eux, vivent dans $\mathbb{C}^{2^n}$. Ce sont donc des vecteurs complexes de taille 2^n. On note $|i\rangle$ la i-ème composante, et le qubit est noté $\sum_{i=0}^{2^n-1} \alpha_i |i\rangle$. Chaque composante représente une des valeurs possibles, et le coefficient α_i correspond à son *amplitude*. La probabilité de mesurer la valeur i est $|\alpha_i|^2$, et si l'on mesure i, l'état quantique est transformé en $|i\rangle$. La somme des probabilités devant faire 1, on a $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$. Il est à noter que si le vecteur est à valeurs complexes, seules les amplitudes sont continues. Les états que l'on peut mesurer (les $|i\rangle$) sont, eux, discrets.

On parle de *registre quantique* pour un groupe de qubits de taille donnée. On peut raisonner sur plusieurs registres, dans ce cas l'état quantique est noté $|x\rangle |y\rangle$.

Les opérations que l'on peut faire sur un état quantique sont nécessairement réversibles (mesure exceptée), et linéaires (c'est-à-dire que pour un opérateur O, on a $O(\alpha |a\rangle + \beta |b\rangle) = \alpha O |a\rangle + \beta O |b\rangle$).

Ainsi, la façon canonique de calculer des fonctions classiques est de renvoyer l'entrée avec la sortie : au lieu d'avoir un circuit qui transforme x en $f(x)$, on a un circuit qui transforme $\sum_{x,y} |x\rangle |y\rangle$ en $\sum_{x,y} |x\rangle |y \oplus f(x)\rangle$.

Le circuit peut être construit avec de simples briques de base, comme le CNOT, analogue du xor :

$$\mathrm{CNOT} |a\rangle |b\rangle = |a\rangle |a \oplus b\rangle$$

et la porte de Toffoli, analogue du « et logique » :

$$\mathrm{Tof} |a\rangle |b\rangle |c\rangle = |a\rangle |b\rangle |c \oplus (a \wedge b)\rangle .$$

Il existe aussi des opérations qui n'ont pas d'analogue classique. La *porte de Hadamard*, notée H, opère sur un qubit

$$H |b\rangle = \frac{1}{\sqrt{2}} \Big(|0\rangle + (-1)^b |1\rangle \Big) .$$

Cette opération est bien inversible, et même involutive : l'appliquer une deuxième fois redonne l'état initial.

La *transformée de Fourier quantique*, notée QFT, opère sur n qubits [1] :

$$QFT |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{\ell=0}^{2^n-1} \exp\left(2i\pi\ell x/2^n\right) |\ell\rangle$$

1. Son inverse est la même fonction, en remplaçant x par $-x$ dans l'amplitude.

On note $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ et $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Ces deux qubits sont une autre base de $\mathbb{C}^2$, et on passe de celle-ci à la base canonique $(|0\rangle, |1\rangle)$ avec la porte de Hadamard.

Le lecteur curieux pourra se tourner avantageusement vers [21].

2 Conséquences en cryptographie à clé publique

L'ordinateur quantique est capable d'effectuer efficacement certains calculs qu'un ordinateur classique ne peut faire que très difficilement. Or, la cryptographie a besoin de difficultés (par exemple, factoriser un nombre ou trouver une clé de chiffrement à partir de quelques couples clairs/chiffrés).

Or, un certain nombre de problèmes peuvent être résolus bien plus efficacement avec un ordinateur quantique. L'algorithme de Shor [1] permet de factoriser et de calculer des logarithmes discrets en temps polynomial. Ces problèmes sont très spécifiques, mais malheureusement, ils sont à l'origine de la sécurité du cryptosystème RSA et de l'échange de clé Diffie-Hellman (avec courbe elliptique ou non). Cela les rend donc inutilisables si l'on réussit à construire un ordinateur quantique suffisamment puissant.

On pourrait penser que puisqu'aujourd'hui, seuls des prototypes avec quelques dizaines de qubits existent, il n'est pas nécessaire de s'en préoccuper. Cela est faux, pour deux raisons :

— il faut que les systèmes de communications soient prêts le jour où un tel ordinateur sera construit, ce qui nécessite d'anticiper ;
— un tel ordinateur pourra potentiellement décrypter des messages d'aujourd'hui, dont les chiffrés auraient été stockés en attendant. Cela représente donc une menace pour les secrets à long terme, qui doivent être protégés maintenant contre un attaquant à venir.

Il est donc nécessaire de trouver (et de standardiser) des alternatives qui résistent à un ordinateur quantique. Plusieurs familles de cryptosystèmes potentiellement résistantes à un ordinateur quantique sont connues. On peut citer les systèmes basés sur le problème du décodage (les codes), dont le premier, proposé par McEliece, avait été publié un an après RSA [19], les systèmes basés sur la difficulté de résoudre un système linéaire bruité [22] (les lattices), qui permettent notamment de faire du chiffrement homomorphe, ou les cryptosystèmes multivariés, basés sur la difficulté de résoudre des équations polynomiales. Néanmoins, ces systèmes sont généralement plus lents, avec des clés plus grosses et sont parfois significativement plus difficiles à implémenter, ce qui les a laissés dans l'ombre de RSA et des courbes elliptiques.

Avoir des familles de cryptosystèmes est une chose, avoir des standards largement déployés en est une autre. C'est à cet effet que le NIST a lancé en 2017 un appel à soumission pour de nouveaux standards de signature et d'échange de clé résistant à un ordinateur quantique. Cet appel a eu beaucoup de succès, avec 82 soumissions, que l'on peut répartir en grandes familles (voir tableau 1).

	Lattices	**Codes**	**Multivarié**	**Fonction de hachage**	**Autre**
Échange de clés	24	19	6	/	10
Signature	4	5	7	4	3

Tableau 1. Nombre de soumissions à l'appel du NIST, par grandes familles

Une fois les candidats soumis, la communauté a pu les étudier en détail, et à l'heure actuelle, des attaques sur 22 soumissions ont été proposées. De façon intéressante, ces systèmes ont tous été attaqués de façon classique, sans avoir besoin d'un ordinateur quantique.

Les systèmes ont été comparés, certains qui étaient trop similaires ont été fusionnés, et le 30 janvier, après un délai dû au shutdown, le NIST a annoncé les 26 candidats qualifiés pour le tour suivant, répartis comme indiqué dans le tableau 2. Les résultats finaux sont attendus dans environ un an, et il faudra encore du temps pour que les sélectionnés soient implémentés en pratique.

	Lattices	**Codes**	**Multivarié**	**Fonctions de hachage**	**Autres**
Échange de clés	8	7	0	/	2
Signature	3	0	4	2	0

Tableau 2. Candidats restant au tour 2, par grandes familles

Le fait qu'un certain nombre de ces cryptosystèmes ne résiste pas à l'ordinateur classique montre bien que la seule garantie de sécurité est une étude dans la durée et par de nombreuses personnes des cryptosystèmes, et qu'il faut donc faire attention à ne pas passer trop vite à des systèmes peu étudiés.

3 La cryptographie quantique

Jusqu'ici, nous considérions de la cryptographie classique, attaquée quantiquement. Cependant, si l'avenir de l'ordinateur est l'ordinateur quantique, on peut aussi estimer qu'à très long terme, les *communications* pourront aussi être quantiques. Ainsi, au lieu de s'envoyer des messages classiques, des états quantiques pourront être transmis. Cela ouvre la porte à de nouveaux protocoles, et notamment à la distribution de clés quantique, imaginée dès 1984 par Bennett et Brassard [3], et parfois citée comme une alternative aux protocoles d'échange de clés. Leur protocole est simple :

- Alice envoie aléatoirement $|0\rangle, |1\rangle, |+\rangle, |-\rangle$ à Bob, n fois,
- Pour chaque qubit, Bob mesure aléatoirement dans la base $(|0\rangle, |1\rangle)$ ou $(|+\rangle, |-\rangle)$,
- Pour chaque qubit, Bob indique à Alice quelle base il a utilisé,
- Alice indique à Bob quels qubits ont été mesurés dans la bonne base,
- Alice et Bob s'échangent un sous-ensemble des valeurs des qubits correctement mesurés,
- En cas d'égalité, le secret partagé correspond aux valeurs correctement mesurées non échangées.

Ce protocole est correct, puisque si la base utilisée est la bonne, la mesure est déterministe, et Alice et Bob ont bien la même valeur. La sécurité repose sur la mécanique quantique : si un attaquant intercepte un des qubits, il ne peut pas en faire de copie, et s'il le mesure sans connaître la base, il a une chance sur deux de le modifier. Ainsi, cela va introduire des erreurs entre les deux parties, qui pourront détecter le problème.

Le lecteur attentif aura remarqué qu'il n'y a pas d'authentification dans ce protocole. La clé est donc échangée avec la personne de l'autre côté du canal, sans autre contrainte. Il faut rajouter un canal authentifié pour éviter ce problème. Or, on utilise de la cryptographie à clé publique pour faire cette authentification. Ce système d'échange de clés nous ramène donc au point de départ, avec deux différences, la première est que le système d'authentification doit seulement être sûr au moment de l'échange de clés pour que la clé reste secrète, la seconde est qu'il faut être capable d'envoyer et de recevoir des qubits.

4 Conséquences en cryptographie à clé secrète

La situation en cryptographie symétrique est légèrement différente. La recherche exhaustive d'une clé peut être effectuée avec l'algorithme

de Grover [14], qui peut tester N clés en un temps $\sqrt{N}$. Ce gain est notable, mais ne change pas fondamentalement la donne : si la taille de clé est doublée, on retrouve le niveau de sécurité initial. Si l'on estime qu'AES, avec ses 128 bits de clés, n'est pas assez résistant, on peut passer à AES-256. La seule différence est que l'algorithme est légèrement plus lent, et qu'il faut stocker 16 octets supplémentaires de clé.

La recherche de collision peut aussi être accélérée, mais moins. Une collision sur n bits peut être trouvée en $2^{n/3}$ requêtes [24], là où classiquement il en faut $2^{n/2}$.

L'algorithme de Grover change le coût de la recherche exhaustive, mais la sécurité est basée sur les attaques (ou leur absence malgré une étude approfondie), qui doivent avoir un coût inférieur à la recherche exhaustive. À l'heure actuelle, les attaques quantiques proposées en cryptographie symétrique s'inspirent d'attaques classiques, et sont accélérées en remplaçant certaines briques de recherche exhaustive par l'algorithme de Grover. Cela accélère l'attaque, dont le coût sera au mieux la racine carrée du coût classique. Or, le point de référence pour les attaques est la recherche exhaustive. Cela fait que de façon générale, les primitives symétriques sont plutôt *plus* sûres quantiquement que classiquement, dans le sens où la recherche exhaustive étant plus rapide, elle est plus difficile à battre. En ce qui concerne les chiffrements non cassés (pour lesquels on ne sait pas faire mieux que la recherche exhaustive), l'ordinateur quantique est significativement plus efficace, sans que cela soit catastrophique. Par exemple, le nombre d'opérations quantiques nécessaires pour casser AES-256 est comparable au nombre d'opérations classiques pour casser AES-128.

Par exemple, en l'état actuel de nos connaissances, il est possible de recouvrer la clé sur les versions réduites à respectivement 7,8 et 9 tours d'AES-128, AES-192 et AES-256 [2] avec des attaques de type Demirci-Selçuk meet-in-the-middle [10]. Quantiquement, à l'heure actuelle, on ne sait battre la recherche exhaustive (quantique) que pour des versions réduites à respectivement 6, 7 et 8 tours [8] en adaptant différentes attaques classiques. Les attaques quantiques ayant été beaucoup moins étudiées, cet écart d'un tour entre les meilleures attaques classiques et quantiques sera peut-être comblé, mais cela suggère que faire fonctionner une attaque quantique rajoute une couche de difficulté.

Il y a cependant une exception, dans le cas où il est possible d'exécuter, sur un ordinateur quantique, un système de chiffrement à clé inconnue. Cela est par exemple envisageable pour un chiffrement en boîte blanche : il est possible de réimplémenter un programme de chiffrement sur un

2. Les versions complètes contiennent respectivement 10, 12 et 14 tours.

ordinateur quantique. Dans ce cas, il est notamment possible d'utiliser l'algorithme de Simon [23].

4.1 Algorithme de Simon

Simon, dont l'algorithme [23] est un précurseur de l'algorithme de Shor, est un des premiers à avoir montré une supériorité très nette de l'ordinateur quantique pour certains problèmes.

On suppose avoir accès à un opérateur quantique $O_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$, qui calcule une fonction $f : \{0,1\}^n \to \{0,1\}^n$. De plus, on suppose qu'il existe s tel que, pour tout x, $f(x) = f(x \oplus s)$ (on dit que s est une période de f). Alors, l'algorithme peut retrouver s en environ n appels à O_f.

L'algorithme 1 décrit le fonctionnement de la routine quantique de l'algorithme de Simon. Jusqu'à l'étape 5, il n'y a rien de vraiment quantique : si on faisait une mesure à cette étape, on obtiendrait aléatoirement x_0 ou $x_0 \oplus s$, cela reviendrait exactement à tirer une entrée aléatoirement, et à en calculer son image.

La partie intéressante est l'étape 6. À cette étape, il y a une interférence entre les deux termes correspondant aux deux préimages. L'état quantique peut se réécrire ainsi :

$$\frac{1}{\sqrt{2^{n+1}}} \left(\sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y} (1 + (-1)^{s \cdot y}) |y\rangle \right).$$

En particulier, cela fait que l'amplitude de y vaut 0 si $s \cdot y = 1$, et $\frac{1}{\sqrt{2^{n-1}}}$ si $s \cdot y = 0$.

Cette routine produit donc des valeurs aléatoires vérifiant l'équation linéaire $y \cdot s = 0$. On peut ainsi retrouver s en appelant un peu plus de n fois la routine, puis en résolvant le système d'équations.

4.2 Cryptanalyse basée sur Simon

La cryptanalyse basée sur l'algorithme de Simon va chercher dans des constructions l'égalité $f(x) = f(x \oplus s)$, pour un s intéressant.

L'exemple le plus simple est l'attaque sur la construction Even-Mansour [17] (Figure 1). Ce chiffrement utilise une permutation aléatoire publique P et deux clés privées k_1, k_2. Le chiffrement en lui-même est défini comme $EM_{k_1,k_2}(x) = P(x \oplus k_1) \oplus k_2$.

Classiquement, il est prouvé que si P est une permutation de n bits choisie aléatoirement, on ne peut pas retrouver les clés en moins de $2^{n/2}$

opérations. Avec un ordinateur quantique, si on note $f(x) = EM_{k_1,k_2}(x) \oplus P(x)$, on a $f(x) = f(x \oplus k_1)$, et on peut retrouver k_1 avec l'algorithme de Simon.

Entrée : Un opérateur quantique calculant f, avec $f(x) = f(x + s)$
Sortie : y, vérifiant $y \cdot s = 0$

1: Initialiser deux registres de n bits

$$|0\rangle |0\rangle$$

2: Appliquer une porte de Hadamard à tous les qubits du premier registre

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle$$

3: Appliquer l'opérateur calculant f

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle$$

4: Mesurer un $f(x_0)$ dans le second registre

$$\frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus s\rangle) |f(x_0)\rangle$$

5: Oublier le second registre

$$\frac{1}{\sqrt{2}} (|x_0\rangle + |x_0 \oplus s\rangle)$$

6: Appliquer une porte de Hadamard à tous les qubits du premier registre

$$\frac{1}{\sqrt{2^{n+1}}} \left(\sum_{y=0}^{2^n-1} (-1)^{x_0 \cdot y} |y\rangle + (-1)^{(x_0 \oplus s) \cdot y} |y\rangle \right)$$

7: Mesurer un y dans le registre

Algorithme 1. Algorithme de Simon

Ce genre de structure apparaît aussi dans de nombreux MACs et chiffrements authentifiés [5, 16].

L'algorithme de Simon utilise a besoin d'une propriété forte ($f(x) = f(x \oplus s)$) pour être applicable. Sur la construction Even-Mansour (et plus généralement pour toutes les attaques de ce types), cela vient du fait que la clé k_1 est xorée. Si une addition modulaire était utilisée, on n'aurait plus $f(x) = f(x \oplus k_1)$, et l'algorithme de Simon ne serait plus applicable. Ainsi, une façon simple d'éviter cette attaque serait de remplacer les xor de la

clé par des additions. Malheureusement, j'ai pu montrer dans le cadre de ma thèse que la plupart des attaques basées sur l'algorithme de Simon peuvent se généraliser aux variantes utilisant des additions [6], avec des algorithmes quantiques moins efficaces que l'algorithme de Simon, mais encore très significativement plus efficaces que la recherche exhaustive.

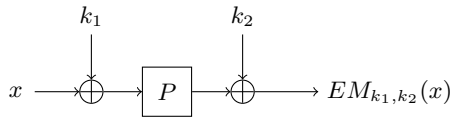

Fig. 1. Construction Even-Mansour

Enfin, si la plupart des familles d'attaques cryptographiques ne peuvent, à notre connaissance, qu'être accélérées avec au mieux l'algorithme de Grover, il est une exception notable : les *slide attacks*, une famille d'attaques sur des chiffrements itérés dont les tours sont similaires (soit sans cadencement de clé, soit avec un cadencement faible). Dans ce cas, il est parfois possible d'accélérer drastiquement l'attaque avec un ordinateur quantique [7].

Il convient donc d'y faire attention, que ce soit dans des cas où on pourrait exécuter un cryptosystème à clé inconnue sur un ordinateur quantique, ou simplement pour être certain qu'il n'y aura pas de problème, indépendamment du cas d'usage.

5 Conséquences sur les protocoles actuels

La quasi-totalité des protocoles de communication sécurisés actuels tels que TLS, SSH, IPsec, Signal ne proposent comme échange de clé ou signature que des cryptosystèmes qui ne résistent pas à un ordinateur quantique.

Une approche simple pour résoudre le problème de l'absence de protocole d'échange de clé est d'utiliser un secret partagé a priori. Cela réduit l'intérêt d'utiliser des systèmes à clé publique, mais a l'avantage d'être simple à mettre en place. Cette approche est notamment proposée par Wireguard [11] [3], un protocole de VPN dont les clés publiques des tiers de confiance sont déployées manuellement. Il propose en option d'utiliser en plus d'un échange de clés une clé symétrique de 256 bits partagée en amont. Cette clé doit être déployée manuellement, mais comme c'est

3. Wireguard a fait l'objet d'une présentation invitée lors de SSTIC 2018.

aussi le cas des clés publiques, cela ne change pas fondamentalement les contraintes de déploiement.

TLS permet aussi un tel mécanisme [12]. Cependant, cela nécessite que clients et serveurs se connaissent a priori, ce qui, dans l'écrasante majorité des cas d'utilisation actuelle de TLS, n'est pas le cas.

Il faut donc utiliser des systèmes plus résistants, ce qui nécessite la standardisation de nouvelles primitives dans TLS. Dans certains cas, il est possible de ne pas attendre, et c'est notamment ce qu'a fait Google, qui contrôle bon nombre de clients et de serveurs, en 2016 [9]. Certaines communications entre Chrome et les serveurs de Google ont utilisé un échange de clé non-standard : en parallèle d'un Diffie-Hellman standard, était utilisé le protocole NewHope [2], qui est un des candidats ayant passé le second tour de l'appel du NIST. Cette approche permet d'éviter qu'une faiblesse dans le nouvel algorithme ne réduise la sécurité classique du système, et a permis d'obtenir des informations sur le coût et les éventuels problèmes d'utilisation dans TLS de nouvelles primitives. En 2019, Google récidive [18], en se basant cette fois sur HRSS [15], qui, après fusion avec NTRUEncrypt, est aussi au second tour de l'appel du NIST.

TLS n'est pas le seul protocole pour lequel ces expérimentations existent. Openssh 8.0 [20], qui sera bientôt distribué, supporte aussi un échange de clé hybride, utilisant NTRUprime [4] et Diffie-Hellman.

Si ces expériences sont intéressantes et permettent d'étudier les problèmes pratiques de déploiements de nouvelles primitives, elles ne résolvent pas tout : en effet, comme pour la distribution de clé quantique, échanger des clés, c'est intéressant, mais savoir avec qui on les échange, c'est mieux. Il est donc nécessaire de supporter aussi des signatures résistantes pour authentifier l'autre partie et disposer d'un protocole résistant.

6 Conclusion

L'ordinateur quantique, en résolvant efficacement certains problèmes difficiles avec un ordinateur classique, impose de renouveler les standards de cryptographie à clé publique, processus qui est en cours, et de préparer les protocoles à l'utilisation de nouvelles primitives. En cryptographie symétrique, il peut être suffisant d'utiliser des clés plus longues, bien que dans certains cas, il soit possible de casser certaines constructions. Enfin, s'il est possible de faire de la distribution de clés avec des communications quantiques, cela ne suffit pas à remplacer les systèmes classiques d'échange de clé.

7 Remerciements

L'auteur remercie Benjamin Beurdouche et Nicolas David pour leurs relectures et commentaires sur une version préliminaire du manuscrit. L'auteur remercie André Schrottenloher pour ses relectures, ainsi que pour le prêt de son ordinateur dans la file d'attente de l'immigration de l'aéroport de San Francisco qui a permis de soumettre ce document.

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement no. 714294 - acronym QUASYModo).

Références

1. Leonard M. Adleman and Ming-Deh A. Huang, editors. *Algorithmic Number Theory, First International Symposium, ANTS-I, Ithaca, NY, USA, May 6-9, 1994, Proceedings*, volume 877 of *Lecture Notes in Computer Science*. Springer, 1994.
2. Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum Key Exchange - A New Hope. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 327–343, 2016.
3. C. H. Bennett and G. Brassard. Quantum cryptography : Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, page 175, India, 1984.
4. Daniel J. Bernstein, Chitchanok Chuengsatiansup, Tanja Lange, and Christine van Vredendaal. NTRU Prime : Reducing Attack Qurface at Low Cost. In *Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers*, pages 235–260, 2017.
5. Xavier Bonnetain. Quantum Key-Recovery on Full AEZ. In *Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16-18, 2017, Revised Selected Papers*, pages 394–406, 2017.
6. Xavier Bonnetain and María Naya-Plasencia. Hidden Shift Quantum Cryptanalysis and Implications. In *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, pages 560–592, 2018.
7. Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. On Quantum Slide Attacks. *IACR Cryptology ePrint Archive*, 2018 :1067, 2018.
8. Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. Quantum security analysis of AES. *IACR Cryptology ePrint Archive*, 2019 :272, 2019.
9. Matt Braithwaite. Experimenting with Post-Quantum Cryptography. https ://security.googleblog.com/2016/07/experimenting-with-post-quantum.html.
10. Patrick Derbez, Pierre-Alain Fouque, and Jérémy Jean. Improved Key Recovery Attacks on Reduced-Round AES in the Single-Key Setting. In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 371–387, 2013.

11. Jason A. Donenfeld. WireGuard : Next Generation Kernel Network Tunnel. In *24th Annual Network and Distributed System Security Symposium, NDSS 2017, San Diego, California, USA, February 26 - March 1, 2017*, 2017.
12. Pasi Eronen and Hannes Tschofenig. Pre-Shared Key Ciphersuites for Transport Layer Security (TLS). *RFC*, 4279 :1–15, 2005.
13. Richard P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21(6) :467–488, Jun 1982.
14. Lov K. Grover. A Fast Quantum Mechanical Algorithm for Database Search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219, 1996.
15. Andreas Hülsing, Joost Rijneveld, John M. Schanck, and Peter Schwabe. High-Speed Key Encapsulation from NTRU. In *Cryptographic Hardware and Embedded Systems - CHES 2017 - 19th International Conference, Taipei, Taiwan, September 25-28, 2017, Proceedings*, pages 232–252, 2017.
16. Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking Symmetric Cryptosystems Using Quantum Period Finding. In *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, pages 207–237, 2016.
17. Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type Even-Mansour cipher. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, pages 312–316, 2012.
18. Adam Langley. CECPQ2.
https ://www.imperialviolet.org/2018/12/12/cecpq2.html.
19. R. J. McEliece. A Public-Key Cryptosystem Based On Algebraic Coding Theory. *Deep Space Network Progress Report*, 44 :114–116, January 1978.
20. Damien Miller. Call for testing : OpenSSH 8.0.
https ://lists.mindrot.org/pipermail/openssh-unix-dev/2019-March/037672.html.
21. Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information : 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.
22. Oded Regev. On Lattices, Learning with Errors, Random Linear Codes, and Cryptography. In *Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing*, STOC '05, pages 84–93, New York, NY, USA, 2005. ACM.
23. Daniel R. Simon. On the Power of Quantum Computation. *SIAM J. Comput.*, 26(5) :1474–1483, 1997.
24. Alain Tapp. Quantum Algorithm for the Collision Problem. In *Encyclopedia of Algorithms*. 2008.