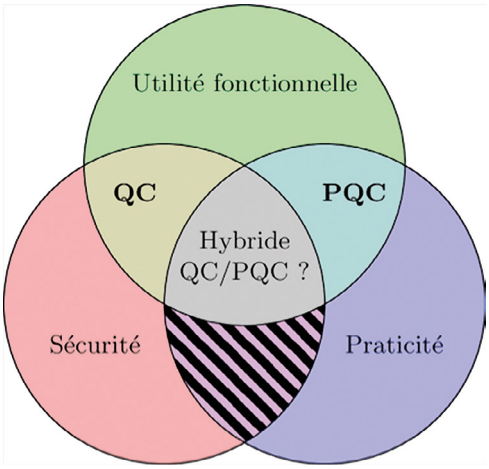
APPROCHES HYBRIDES EN CRYPTOGRAPHIE QUANTIQUE

Romain ALLÉAUME*, Tristan NEMOZ

Télécom Paris-LTCI, Institut Polytechnique de Paris, Inria, Palaiseau, France

* romain.alleaume@telecom-paris.fr



La cryptographie quantique s'est largement définie comme visant une sécurité inconditionnelle, en alternative à la cryptographie dite classique reposant sur la difficulté calculatoire conjecturée de certains problèmes mathématiques. Plutôt que d'opposer cryptographie quantique et classique, hybrider approches calculatoires post-quantiques (PQC) et cryptographie quantique (QC) ouvre des perspectives nouvelles, pour une cryptographie pratique, plus sûre et offrant plus de fonctionnalités.

https://doi.org/10.1051/photon/202513046

La cryptologie, et souvent par abus de langage que nous reprendrons, la cryptographie, est l'art d'assurer qu'une communication entre deux parties. Elle possède des propriétés désirables, comme la confidentialité, l'intégrité ou l'authenticité. Aujourd'hui, deux paradigmes différents semblent s'affronter : celui de la cryptographie post-quantique et celui de la cryptographie quantique.

En 1994, Peter Shor publie un algorithme qui révolutionne le monde de la cryptographie. Il annonce que si des ordinateurs quantiques venaient à exister, la cryptographie telle qu'elle était à l'époque, et est toujours en grande partie aujourd'hui, s'effondrerait. En effet, il a prouvé qu'un ordinateur quantique peut efficacement résoudre des problèmes mathématiques tels que la factorisation, sur lesquels sont fondés une grande partie de la cryptographie à clé publique, essentielle pour le fonctionnement et la sécurité d'Internet.

Face à la menace de l'ordinateur quantique, deux réponses sont alors possibles. La première est celle de l'approche de la cryptographie post-quantique qui consiste à trouver d'autres problèmes semblant difficiles pour les ordinateurs quantiques et de baser les protocoles cryptographiques sur ces problèmes. Une fois de tels problèmes trouvés, une telle solution a l'avantage d'être assez facilement déployable par une modification de la pile logicielle, mais sans nécessiter de changements dans l'infrastructure de nos réseaux. En revanche, on reste exposé à la possibilité qu'une solu tion au nouveau problème mathématique soit finalement trouvée, ce qui nous ferait revenir à la case départ. La seconde, c'est adopter une autre approche. C'est ce que propose la cryptographie quantique, où l'on fait en sorte que la sécurité du protocole repose non pas sur un problème mathématique, mais sur les lois de la physique quantique elles-mêmes. Le problème est alors inverse : bien qu'elle assure une sécurité parfaite en théorie, la cryptographie quantique reste délicate à mettre en œuvre. Elle fait de plus appel à du matériel spécifique comme les détecteurs d'états quantiques de la lumière et est limitée en débit et en distance.

Ainsi, chacune des deux approches effectue un compromis fondamentalement différent, ce qui a souvent mené à une opposition de ces deux paradigmes. Pourtant, il n'y a pas lieu de les opposer ! *A contrario*, on peut se demander s'il ne serait pas possible de tirer parti des forces ●●●

Dans cet article, nous avons souvent mentionné la notion de « niveau de sécurité » sans vraiment nous attarder dessus. Fondamentalement, le niveau de sécurité est relié aux hypothèses relatives à la complexité algorithmique des problèmes utilisés en cryptographie. Plus on fait d'hypothèses, plus on peut réaliser de fonctionnalités, mais réciproquement, plus on s'expose à ce que l'une des hypothèses soit fausse, et à des attaques.
La figure 2, inspirée des cinq mondes d'Impagliazzo [4], présente une hiérarchie en trois niveaux de sécurité. Le niveau avec le moins d'hypothèse, correspond à celui où tous les problèmes qui sont vérifiables sont également calculables. Inversement, le deuxième niveau à un monde ou les fonctions à sens uniques existent, rendant possible le chiffrement d'un grand message avec une petite clé. Enfin le dernier niveau correspond à un monde où la cryptographie à clé publique est possible, i.e. où il existe des fonctions à sens unique avec des trappes. Autrement dit, non seulement les fonctions à sens unique doivent y exister, mais certaines d'entre elles permettent de faire le chemin inverse si l'on possède la bonne information.

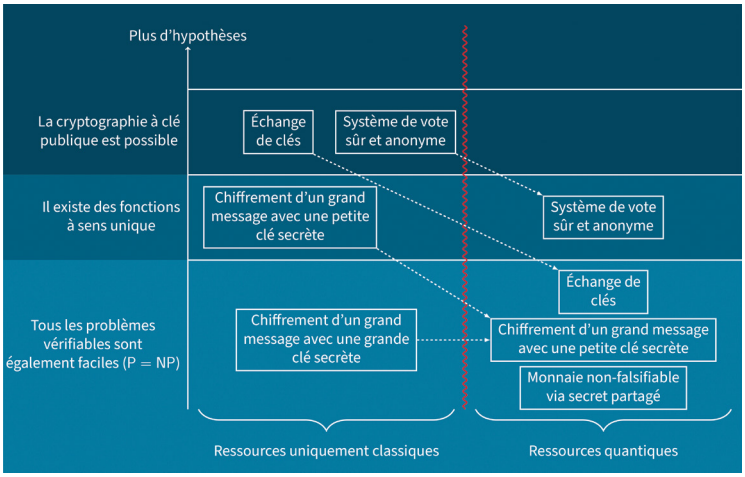


Figure. Représentation graphique des niveaux de sécurité et de fonctionnalité. À niveau de fonctionnalité équivalent, la cryptographie quantique assure généralement une sécurité plus élevée.

L'intérêt de la cryptographie quantique est visible sur la Figure 2 : pour un niveau de fonctionnalité donné, le niveau de sécurité est généralement plus haut que pour son équivalent classique, voire n'a pas d'équivalent classique. C'est notamment le cas d'un système où une banque dispose d'une clé privée servant à signer les billets électroniques : rien n'empêche un attaquant de copier un billet et de le soumettre à nouveau à la banque. Cela n'est cependant pas possible si l'on utilise intelligemment des ressources quantiques.
Si l'on pousse ce raisonnement à l'extrême, cela permet même d'imaginer un monde qui correspondrait à la première ligne de la figure ci-dessus, même s'il est peu probable, dans lequel la cryptographie traditionnelle est impossible, tandis que la cryptographie quantique permet tout de même d'assurer un nombre conséquent de fonctionnalités.

de chacune de ces deux approches afin de dépasser les problèmes inhérents à chacune, *via* des protocoles hybrides notamment. Cette hybridation peut se faire naturellement de deux manières. Dans la première, on peut combiner deux protocoles, un quantique et un classique en parallèle. Dans la seconde, on va combiner des éléments post-quantiques, offrant une sécurité calculatoire directement avec des éléments quantiques.

LES HYBRIDATIONS DES DEUX APPROCHES

L'hybridation parallèle

Le principe de l'hybridation parallèle consiste à utiliser à la fois une solution post-quantique et une solution quantique pour réaliser la même tâche. Par exemple dans le cas de l'échange de clés secrètes, il s'agirait d'utiliser un échange de clé post-quantique, tels que ceux proposés en 2023 après une large compétition internationale dédiée à la standardisation d'algorithmes de cryptographie post-quantique, et en parallèle d'effectuer un échange de clés qui repose sur une communication quantique réalisée sur des liaisons fibrées ou éventuellement des liens satellitaires [1]. On peut alors combiner les deux clés de telle sorte que casser la clé finale nécessiterait de casser à la fois les deux échanges, post-quantique et quantique, ce qui permet d'avoir une sécurité au moins aussi grande que la plus sûre des deux approches [2].

L'hybridation quantique et computationnelle

Étudions maintenant la deuxième approche : l'utilisation de composants typiquement post-quantiques au sein d'un protocole de cryptographie quantique. Une première méthode consiste par exemple à utiliser des fonctions à sens unique, typiques dans les protocoles post-quantiques, dans des protocoles de cryptographie quantique. Cette approche permet alors de réaliser de nouvelles fonctionnalités. Par exemple, avec cette hypothèse seule, il est possible de créer un système de vote sûr et garantissant l'anonymat de ses électeurs, ce qui n'est pas possible lorsque l'on considère uniquement des fonctions à sens uniques. Les ressources quantiques apportent donc un gain net par rapport à la cryptographie traditionnelle ! Cependant, bien qu'elle permette ces nouvelles fonctionnalités, cette approche ne résout *a priori* pas le problème principal de la cryptographie quantique, à savoir sa praticité.

Un objectif est alors de pouvoir utiliser une hypothèse computationnelle pour augmenter la praticité du protocole, tout en garantissant une sécurité de type *everlasting*, c'est à dire computationnelle durant l'exécution du protocole, mais inconditionnelle au-delà. Une façon d'obtenir une telle sécurité est de supposer qu'un attaquant est limité en temps ou en taille mémoire, dans sa capacité à stocker des états quantiques, ce qui est tout à fait réaliste au vu des technologies actuelles.

Imaginons alors la situation suivante : Alice génère un état quantique de grande dimension $|\psi\rangle$, et y encode un bit b. Elle envoie au préalable à Bob, avec un chiffrement computationnel, les informations sur la mesure permettant de retrouver b. Dès lors Alice peut envoyer $|\psi\rangle$ et Bob faire la mesure lui permettant d'obtenir b. Après un certain temps, un attaquant saura casser le chiffrement computationnel et aura également accès à la mesure. Néanmoins durant ce temps, un attaquant n'a d'autre choix que de stocker l'état quantique $|\psi\rangle$ en attendant d'avoir cassé le chiffrement. Mais si la capacité de l'attaquant à stocker de l'information quantique est limitée à des temps beaucoup plus courts que la sécurité computationnelle, ce qui est une hypothèse très bien vérifiée aujourd'hui, alors l'attaquant est dans une situation très défavorable le forçant à mesurer immédiatement l'état quantique de grande dimension sans connaître la mesure adéquate, sachant que le nombre de mesures peut croitre très rapidement avec la dimension. Ce modèle, appelé *Quantum Computational Timelock*, permet en outre de réaliser, avec une sécurité *everlasting*, un échange de clé quantique entre Alice et Bob en s'envoyant un grand nombre de copies du même état $|\psi\rangle$, ce qui en renforce la praticité par rapport à la cryptographie quantique standard, qui n'est sûre que si une seule copie de l'état quantique est envoyée [3].

CONCLUSION

Comme récemment illustré par les recommandations de la Commission Européenne [5], combiner les approches quantiques et post-quantiques est une voie d'avenir pour garantir la sécurité des échanges numériques y compris vis à vis d'attaques par un ordinateur quantique. C'est aussi une approche féconde, qui reposera en particulier – tout comme le calcul quantique photonique – sur la capacité à créer et détecter des états quantiques de grande dimension, pour augmenter les performances et la praticité de la cryptographie quantique.

RÉFÉRENCES

[1] Y.-A. Chen *et al.* Nature **589**, 214 (2021)

[2] B. Dowling *et al.*, In International Conference on Post-Quantum Cryptography (pp. 483-502). Cham: Springer International Publishing (2020)

[3] F. Mazzoncini *et al.*, arXiv:2311.09164 (2023)

[4] R. Impagliazzo, Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference (1995)

[5] European Commission, Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography (2024)