3

Traquer les failles des algorithmes

Léo Ducas, Centrum Wiskunde & Informatica, Amsterdam

Les spécialistes des attaques des protocoles cryptographiques – les cryptanalystes – évaluent la confiance que l'on peut avoir dans les schémas post-quantiques, en cherchant continuellement des vulnérabilités dans les systèmes, protocoles et algorithmes, proposés. Dans ce domaine, les chercheurs français sont à la pointe.

Le scénario de la « cryptocalypse quantique » est pris au sérieux par les agences gouvernementales, mais aussi par les géants du Net. C'est que l'enjeu est massif ! Une telle catastrophe mettrait à nu toutes les données sécurisées : identifiants bancaires, communications militaires, plus rien ne pourrait rester secret. Sur Internet, ce n'est pas uniquement la confidentialité de vos e-mails et de vos visites qui serait en proie aux hackers, mais l'infrastructure du réseau elle-même. Il deviendrait aussi possible de falsifier un passeport électronique.

Face à cette menace, Google a lancé, dès 2016, une expérience grandeur nature en incluant, dans son navigateur, le schéma post-quantique New Hope censé résister à l'ordinateur quantique (1). En 2017, c'est le NIST, l'institut américain des standards et de la technologie, qui a ouvert une compétition pour définir les futures normes de la cryptographie post-quantique, dont New Hope, algorithme fondé sur les réseaux, est un candidat (lire p. 44).

Parmi les candidatures proposées et soumises à la sagacité de la communauté, certaines, pas très sérieuses, ont été très rapidement cassées, des attaques dévastatrices ayant été découvertes quelques semaines après leur publication. C'est en effet aux cryptanalystes, dont la spécialité est de trouver les points faibles dans les protocoles et algorithmes, que revient la charge d'éprouver les systèmes proposés.

Dans ce domaine, la recherche française est bien lotie, sans doute parce que l'école française de mathématiques est forte et que, in fine, pour attaquer des protocoles cryptographiques, il faut faire appel à de l'algèbre et à une théorie des nombres avancée. En Allemagne, la recherche cryptographique collabore étroitement avec l'industrie de la carte à puce ; et les Pays-Bas ont de nombreux experts en algèbre, en cryptographie, mais aussi en calcul quantique. La recherche publique aux États-Unis est, quant à elle, souvent bien plus théorique. Les mauvaises langues diront que la cryptanalyse y est la chasse gardée de la NSA, l'agence de sécurité américaine…

DR

CRYPTANALYSTE
Léo Ducas est chercheur au Centrum Wiskunde & Informatica (CWI), l'institut national de recherche en mathématiques et informatique, à Amsterdam, aux Pays-Bas.

Contexte **Alors que les progrès en matière de calcul quantique menacent la plupart des cryptosystèmes asymétriques (ou à clé publique) actuellement déployés, de nombreuses alternatives sont à l'étude depuis plus d'une décennie et demandent à être testées.**

Un énoncé non interactif

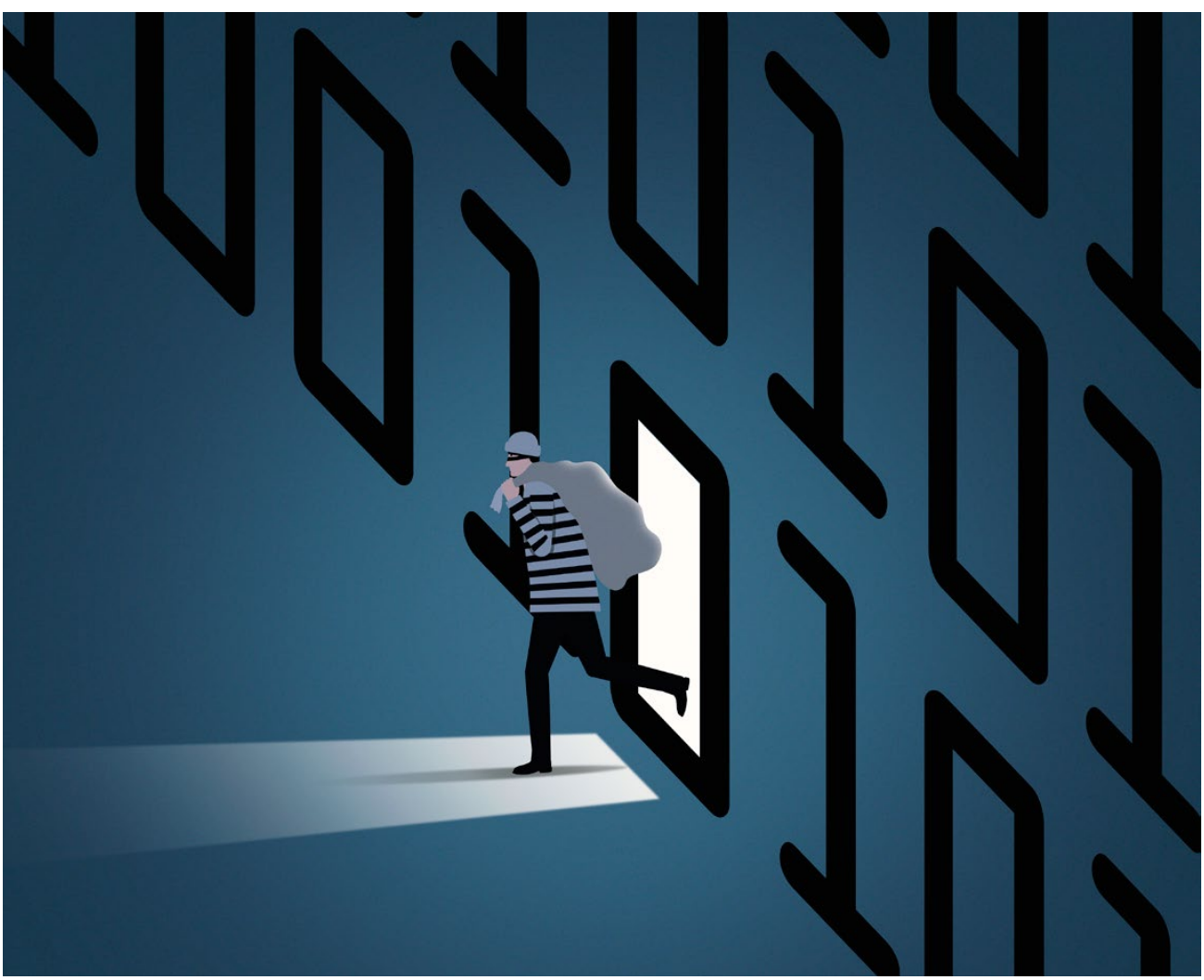
Comment procède le cryptanalyste face à un nouveau schéma ? Les protocoles sont compliqués, interactifs, ce qui offre une large panoplie d'attaques ; il est ainsi difficile a priori de se convaincre que tel ou tel protocole est incassable. Par exemple, pour un schéma de chiffrement, un attaquant dit actif – c'est-à-dire qui injecterait lui-même des messages durant le protocole – pourrait forcer les participants légitimes à laisser échapper des informations secrètes. Pour être plus convaincants, les concepteurs de schémas cryptographiques sérieux fournissent une « réduction », sorte de preuve de sécurité :

on prouve mathématiquement que la sécurité du schéma est fondée sur une hypothèse dont l'énoncé est plus simple, non interactif. Ainsi, pour éprouver le schéma, le cryptanalyste peut concentrer ses efforts sur cette hypothèse, cette clé de voûte, plutôt que sur l'ensemble de l'édifice. S'il y a une faiblesse, elle est forcément ici.

Mais, bien que ces réductions simplifient la tâche de cryptanalyse, ce travail nécessite un effort prolongé: en l'absence de garanties mathématiquement infaillibles, une longue durée d'invulnérabilité finit par convaincre qu'une hypothèse est solide. Lorsque toutes les approches crédibles ont été explorées et que toutes les attaques connues n'ont pas subi d'améliorations significatives pendant plusieurs années, alors seulement le cryptographe est rassuré. C'est pour cette raison que les processus de sélection de standards cryptographiques sont si longs.

Il faut combiner toute une branche des sciences, avec l'algèbre et l'algorithmique

L'analyse de sécurité post-quantique offre de nouveaux défis. En effet, bien que les algorithmes puissent souvent être analysés mathématiquement, l'expérimentation est un outil essentiel au travail du cryptanalyste. Mais difficile de tester des algorithmes conçus pour l'ordinateur quantique, qui n'existe pas encore… De surcroît, maîtriser les arcanes mathématiques de l'ordinateur quantique n'est pas une mince affaire, tant la mécanique quantique échappe à l'intuition (lire p. 53). C'est toute une branche des sciences qu'il faut combiner avec l'algèbre et l'algorithmique, ne serait-ce que pour appréhender l'état de l'art. À cela s'ajoutent des défis classiques, •••



MARK AIRS/GETTY IMAGES

▲ *Requérant davantage de puissance informatique, la sécurité des données numériques pourrait avoir un coût de plus en plus important.*

••• car le comportement des algorithmes est parfois meilleur en pratique qu'en théorie. C'est le cas, par exemple, des algorithmes de calcul de bases de Gröbner, des outils issus de l'algèbre qui permettent d'attaquer efficacement la cryptographie multivariable. De même, l'étude rigoureuse des algorithmes de cryptanalyse pour les réseaux euclidiens ne donne que des résultats très imprécis, et des analyses plus fines ne semblent pas possibles sans recours à des modèles heuristiques (Fig. 1). Cependant, de telles différences entre la théorie et la pratique ne sont que quantitatives, et non qualitatives : le problème est certes peut-être un peu moins ardu que prévu, mais reste quand même difficile à mesure que la taille du problème augmente.

Parmi les schémas soumis au NIST, certains ont été attaqués dans ce sens quantitatif : le coût en temps de calcul pour les casser avait été un peu sous-évalué. Toutefois, de telles attaques ne sont pas forcément problématiques, tant les objectifs initiaux de résistance sont élevés. Au lieu d'un million d'années de calcul, sur un million d'ordinateurs, il n'en faudra peut-être « que » 20 000 pour casser le système. Cette perte relative de sécurité est alors compensée par une petite augmentation de la taille des clés – qui permettent de chiffrer le message – car, à moins d'une attaque dévastatrice, la sécurité de ces schémas varie de façon exponentielle avec la taille des clés : ajoutez quelques octets à celles-ci, et le temps de calcul pour une attaque sera doublé.

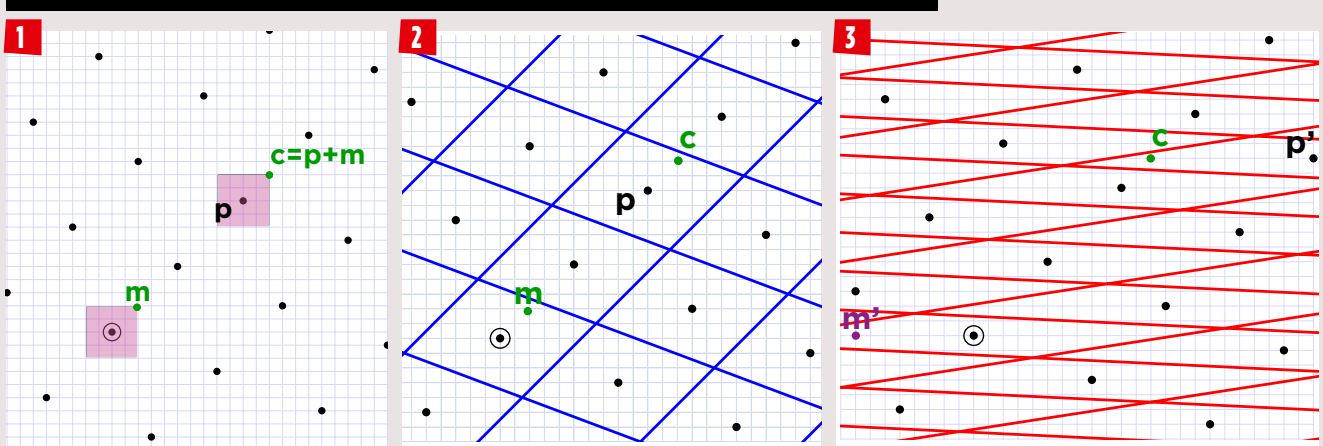
▲ *En 2014, l'agence de renseignement britannique GCHQ a alerté la communauté sur une vulnérabilité potentielle des réseaux aux attaques quantiques.*

MINISTRY OF DEFENCE/DEFENCEIMAGERY.MOD.UK - LÉO DUCAS

Une approche différente

Reste que la menace de nouvelles attaques dévastatrices plane sur tous ces candidats. Pour reprendre la maxime du cryptographe italien Silvio Micali – Prix Gödel et Prix Turing –, « *les cryptographes dorment rarement sur leurs deux oreilles* ». Ainsi, en 2014, alors que l'on pensait les réseaux complètement invulnérables aux attaques quantiques, le Quartier général des communications du gouvernement britannique (GCHQ) a alerté la communauté en montrant que nous avions oublié de nous poser certaines questions.

Fig. 1 Chiffrer un message grâce aux réseaux euclidiens



Un réseau euclidien est une grille régulière et infinie dans le plan, l'espace tridimensionnel ou même dans des dimensions supérieures. Pour chiffrer un message *m*, on lui ajoute un petit bruit sous la forme d'un point *p* aléatoire du réseau. Le message crypté (le chiffré) est donc *c* = *p* + *m* 1. On le déchiffre en retrouvant le centre du pavé 2. Si le pavage choisi – qui définit la base du réseau – est trop allongé, il est difficile de retrouver le bon centre 3. La bonne base (en bleu) constitue la clé secrète qui sert à déchiffrer le message, tandis que la mauvaise base (en rouge) est la clé publique. Si, visuellement, il peut sembler aisé de casser un tel cryptosystème sur le dessin (en dimension 2), les choses se compliquent en grande dimension. En dimension 1000, par exemple, il est extrêmement coûteux en temps de calcul de retrouver la clé secrète à partir de la clé publique.

Cette approche était tellement différente de celles qui sont usuellement considérées pour attaquer les réseaux que certains ont cru qu'elles pourraient mener à des attaques dévastatrices. En explorant cette piste, les méthodes de théorie analytique des nombres – cette branche des mathématiques qui s'intéresse en particulier à l'hypothèse de Riemann – se sont invitées, ce qui a permis de confirmer un début de brèche (2). Nous avons ainsi pu conclure que certains réseaux, cycliques ou cyclotomiques – possédant certaines symétries de rotation –, étaient partiellement vulnérables à des attaques quantiques (3). Bien qu'il s'agisse d'un cas particulier, il était préoccupant, car il se rapprochait de certaines structures de réseaux proposés dès 1998 pour améliorer l'efficacité des cryptosystèmes, et toujours très en vogue (4). A posteriori, cette brèche nous semble en fait limitée et n'affecte, à notre connaissance, aucun des schémas soumis au NIST.

Enjeux économiques

Mais alors, à quel point faut-il craindre de futurs progrès de la cryptanalyse ? La maturité de l'état des connaissances pousse certainement à la prudence, mais pas à la paranoïa. En effet, il est possible de prendre suffisamment de marge, en termes de taille des clés, pour contrer des avancées à venir ; il est même possible de combiner plusieurs schémas de telle sorte que l'édifice tienne, même si l'une des voûtes s'effondre.

Mais ces marges supplémentaires ont un coût : davantage de communications, et donc un délai accru pour l'affichage de nos pages internet ; davantage de calcul, et donc des puces plus puissantes et plus chères dans nos cartes bleues et nos passeports. Ainsi, l'effort de cryptanalyse est motivé par des enjeux économiques et industriels : raffiner notre compréhension des attaques permet de diminuer les marges, et donc les coûts de la sécurité. Plus ces derniers sont élevés, plus l'adoption de cette cryptographie sera freinée, nous laissant donc en proie à la menace de l'ordinateur quantique… C'est ce dilemme que seule la cryptanalyse peut résoudre. ■

(1) tinyurl.com/Post-Quantum-Cryptography

(2) R. Cramer *et al.*, *IACR-EUROCRYPT*, rapport 2015/313, 2015 (eprint.iacr.org/2015/313).

(3) R. Cramer *et al.*, *IACR-EUROCRYPT*, rapport 2016/885, 2016 (eprint.iacr.org/2016/885).

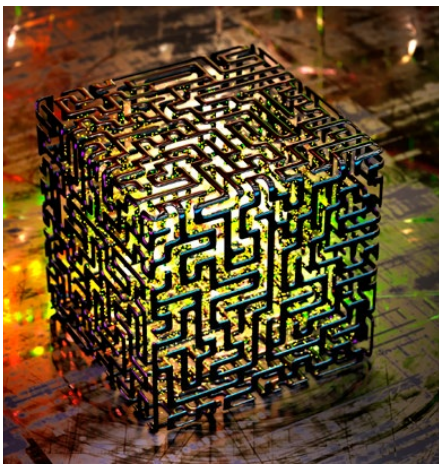
(4) J. Hoffstein *et al.*, *Algorithmic Number Theory*, ANTS 1998, 267, 1998.

L'ORDINATEUR QUANTIQUE ET SON OREILLE ABSOLUE

Le calcul quantique sans formalisme mathématique mène trop souvent à une compréhension erronée ou incomplète. Le qubit, cousin quantique du bit manipulé par nos ordinateurs classiques, peut être dans un état de superposition, à la fois 0 et 1. Cette notion pourrait laisser croire que l'ordinateur quantique serait capable de tester en parallèle toutes les combinaisons. Or, si c'était le cas, il serait en mesure de résoudre tous les problèmes de complexité dite NP (non déterministe polynomial). En particulier, il n'y aurait aucun espoir de faire de la cryptographie post-quantique, puisque tous les problèmes cryptographiques connus ont une complexité NP. Certes, l'ordinateur quantique peut considérer en parallèle un nombre exponentiel de combinaisons mais, pour autant, il ne peut pas facilement extraire, de cette immense superposition, la combinaison qui nous intéresse, hormis dans quelques cas particuliers. L'un d'eux, la recherche de période, correspond à l'algorithme de Shor, qui permet notamment la factorisation des nombres entiers.

Imaginez un livre immense, si gros que vous n'aurez, en une vie, pas le temps d'en feuilleter toutes les pages. Ce livre a une particularité : il est périodique. Toutes les *n* pages, il recommence au début pour raconter la même histoire. Comment trouver ce nombre ? La meilleure stratégie consiste, de manière classique, à en tourner les pages une par une jusqu'à en trouver deux identiques. L'ordinateur quantique, lui, n'ouvrirait même pas le livre, mais tapoterait simplement dessus et écouterait le son qui en sort par résonance. Tout comme un diapason possède une note bien précise, la structure périodique du livre correspond à une fréquence, que l'ordinateur quantique est capable de repérer très efficacement.

Cette métaphore se fonde sur la transformation de Fourier, opération mathématique qui décompose un signal en un ensemble de fréquences. C'est pour une telle opération que l'ordinateur quantique est particulièrement efficace : s'il existe une fréquence prédominante, alors ce dernier saura la trouver facilement. Un tel mécanisme quantique n'est pas si mystérieux : c'est le même qui permet, par exemple, d'étudier la structure régulière des cristaux à l'aide d'un laser. Reste que le calcul de périodes est un problème calculatoire spécifique. L'ordinateur quantique ne sera donc pas une machine à tout résoudre. En fait, il y a même assez peu de calculs utiles que l'on résoudrait mieux avec l'ordinateur quantique qu'avec l'ordinateur classique. Coup du sort, il a fallu que la factorisation et le logarithme discret, les deux piliers actuels de la cryptographie asymétrique, en fassent partie…



▲ *L'ordinateur quantique est efficace pour trouver une fréquence prédominante dans un signal.*

PLOTPLOT/SHUTTERSTOCK