« Les technologies quantiques et post-quantiques sont complémentaires »

GRÉGOIRE RIBORDY,
cofondateur et dirigeant de la société ID Quantique, à Genève.

La compétition lancée par le NIST sur la recherche d'une technologie post-quantique pour la cryptographie pourrait laisser croire que les mathématiques suffisent et que les technologies utilisant directement la physique quantique, sur lesquelles nous travaillons à ID Quantique, deviendraient obsolètes. À mon avis, les deux approches sont utiles et complémentaires. En un sens, nous n'avons jamais disposé de cryptographie classique fiable : avec le temps, les protocoles cryptographiques ont toujours fini par être cassés et il a fallu continuer à chercher pour en trouver d'autres. Et, même si les cryptographes découvrent de très puissants outils mathématiques, il n'y a pas de raison de penser qu'ils seront complètement fiables. En tout cas, pas indéfiniment.

Par conséquent, l'approche de cryptographie quantique, où la sécurité est assurée par des lois immuables de la physique – par exemple, le fait que l'on ne puisse pas dupliquer une information quantique (*) –, me semble importante. Bien entendu, la cryptographie quantique ne peut pas être partout, car elle nécessite des infrastructures spécifiques, comme des réseaux de fibres optiques, des appareillages dédiés… À l'inverse, la cryptographie post-quantique peut être déployée sans changement dans l'infrastructure des réseaux numériques, et indépendamment du médium de communication (filaire, optique ou radio). Cette nécessité d'une infrastructure spécifique implique des coûts encore élevés. Il est probable que vous n'aurez pas de cryptographie quantique sur votre téléphone portable. C'est pourquoi je pense que ces deux approches doivent fonctionner dans une logique complémentaire. Pour certains usages, on utilisera la cryptographie quantique, soit parce que les données y sont très critiques, soit parce qu'on veut une sécurisation à très long terme. Et pour d'autres, les méthodes de cryptographie post-quantique, fondées sur des problèmes mathématiques, seront suffisantes.

Dans la compétition NIST, il y a deux familles de protocoles : pour les signatures et pour l'échange de clés (ou le chiffrement). Pour les signatures, la sécurité est liée à des problèmes fondamentaux de l'informatique théorique, comme *P = NP* (*). Et cela me surprendrait que l'on trouve des failles. Pour le chiffrement, les choses me semblent moins assurées. Du coup, on peut imaginer une solution hybride où la signature et l'authentification se feront à l'aide d'algorithmes post-quantiques, mais où l'échange des clés utilisera des méthodes physiques de la cryptographie quantique.

Nous visons à mettre en place une infrastructure cryptographique qui serait une combinaison de ces solutions. Il faut sortir de cette opposition entre communautés – qui résulte historiquement d'une opposition entre physiciens et mathématiciens – car, pour les applications, je suis persuadé qu'il va falloir combiner les différentes approches. En partenariat avec le plus gros opérateur coréen, SK Telecom, nous sommes d'ailleurs en train de réfléchir au déploiement de la prochaine génération de réseau, la 5G. Utilisé comme passerelle entre le monde des télécommunications et le monde physique, ce réseau sera utilisé pour l'Internet des objets, dont la voiture connectée. Or il doit être hautement sécurisé. Il sera entièrement maillé, pour la partie « réseaux sol », par des méthodes quantiques. Cela sera le plus grand déploiement de cryptographie quantique au monde. Mais il va falloir quelques années, car il s'agit de s'intégrer à l'écosystème existant et donc de mettre en place l'interopérabilité des équipements. »

(*) **L'impossibilité** de dupliquer des informations quantiques résulte du théorème d'impossibilité du clonage quantique selon lequel on ne peut pas dupliquer à l'identique un état quantique inconnu.

(*) **Le problème d'informatique** théorique *P = NP* est une conjecture qui porte sur les classes de complexité et qui permettrait de déterminer si le fait de pouvoir vérifier rapidement une solution à un problème implique de pouvoir trouver cette solution rapidement. En majorité, les théoriciens pensent que *P ≠ NP*, mais c'est encore ouvert.

Cette puce quantique génère des nombres aléatoires utilisés pour le chiffrement.