L’avenir des communications sécurisées passe-t-il par la distribution quantique de clés ?

La distribution quantique de clé (*Quantum Key Distribution* ou QKD) se présente comme un équivalent fonctionnel des mécanismes asymétriques usuels de négociation de clé utilisés dans la plupart des protocoles de communication sécurisée déployés sur Internet ou dans des réseaux privés. La particularité de la QKD serait de posséder un niveau de sécurité supérieur qui justifierait son déploiement pour les applications de haute sécurité. Toutefois, les contraintes inhérentes à cette technologie ne permettent pas d'en envisager un déploiement massif qui offrirait des garanties de sécurité élevées en pratique. De plus, même en tenant compte de l'émergence possible de nouvelles menaces sur les moyens cryptologiques actuels, au premier rang desquels figure l'ordinateur quantique universel, l'avenir des communications sécurisées peut être assuré sur la durée sans qu'il soit nécessaire d'utiliser la QKD. Ainsi, si cette technologie peut éventuellement être appelée à jouer un rôle dans des applications de niche, elle ne constitue pas pour autant le chemin d'évolution naturel des communications sécurisées.

Pour un point de vue complémentaire de celui de l’ANSSI, mais développant des arguments similaires, le lecteur pourra consulter l’avis du National Cyber Security Centre (Royaume-Uni) [3].

Cette prise de position technique ne vise pas à expliquer le fonctionnement de la QKD qui se décline en de nombreux protocoles, mais plutôt à explorer les fonctionnalités qu’elle offre et leurs propriétés de sécurité.

De même, cette prise de position ne concerne pas les communications quantiques en général, ni les réseaux visant à transporter des états quantiques. Ces sujets sont largement prospectifs, au contraire de la QKD.

Enfin, il ne s’agit pas ici de se prononcer sur l’opportunité d’investir dans la recherche et l’innovation dans les domaines de la QKD ou des communications quantiques, qui présentent une porosité avec d’autres sujets tels que le calcul quantique. De tels investissements sont susceptibles d’être porteurs de ruptures ; ils sont essentiels au soutien de l’excellence scientifique et technique européenne et au concourent au développement de son autonomie stratégique.

Qu'est-ce que la distribution quantique de clé (« Quantum Key Distribution » ou QKD) ?

La distribution quantique de clé est une famille de méthodes se fondant sur des principes physiques, et non mathématiques (comme c'est le cas pour la cryptographie usuelle), pour permettre à deux correspondants de construire un secret commun (une clé) en dialoguant sur des canaux publics. Deux canaux sont nécessaires :
- un canal aux propriétés physiques contrôlées, généralement une fibre optique ou une liaison directe à l'air libre, sans trop de pertes ou de perturbations, *et surtout sans dispositif interagissant avec l'information transportée* ;
- une liaison réseau classique.

Comme dans toute méthode visant à produire un secret commun entre deux correspondants, chaque participant doit s'assurer qu'il dialogue avec son homologue et non avec un tiers qui chercherait à s'immiscer dans la négociation pour obtenir séparément un secret commun avec chaque correspondant. Cela se traduit concrètement par la nécessité d'authentifier les communications sur la liaison réseau qui est utilisée.

Lorsqu'un système de QKD est déployé entre deux points, il produit continuellement des secrets communs en ces deux points, avec un débit variable, généralement de l'ordre de quelques kilobits / sec. jusqu'à quelques mégabits / sec.

L'aptitude de la QKD à produire du secret résulte en fait de sa capacité à détecter grâce à des effets quantiques la présence d'un « espion » sur le canal physique (pour comprendre comment cela est possible, voir par exemple une description vulgarisée du protocole BB84 [7]), de quantifier la quantité d'information que celui-ci a pu obtenir concernant les données ayant transité sur ce canal, et d'adapter le taux de secret en conséquence. En cas de présence d'un dispositif actif en coupure, le taux de secret est nul. Tout dispositif de régénération du signal transmis est donc incompatible avec le fonctionnement d'un lien QKD. Cela inclut tout dispositif réseau actif (switch, routeur, ...) et les amplificateurs optiques. *C'est pourquoi la QKD nécessite des liens directs (point à point)*.

La limitation en pertes se traduit quant à elle par une limitation de distance. Ainsi par exemple, sur une fibre optique, une limitation à 20dB de pertes, typique d'un équipement QKD, correspond à une distance de 100Km sur une fibre optique en parfait état et sans connexion intermédiaire, mais ce niveau de pertes peut être atteint sur un lien réel à une distance bien plus faible. Des distances plus grandes peuvent être parcourues avec des liens atmosphériques en utilisant des satellites.

Quels sont les usages proposés pour la QKD ?

La QKD est généralement mise en avant pour permettre d'établir des communications sécurisées, c'est à dire confidentielles et intègres (non modifiables par un attaquant).

Les communications sécurisées sont aujourd'hui utilisées massivement, aussi bien dans des contextes grand public sur internet, que pour relier des sites d'entreprise, permettre via un réseau privé virtuel ou VPN la connexion de machines nomades à des ressources d'entreprise, ou même cloisonner les communications de machine à machine, ou de service à service, dans un réseau informatique.

Ces communications sont aujourd'hui établies en deux temps : dans une première phase, une négociation qui utilise des algorithmes cryptographiques *asymétriques* (à base de RSA ou Diffie-Hellman) permet d'authentifier les participants de la connexion et de construire un secret commun à ces participants ; dans un second temps, ce secret commun ou *clé* est utilisé pour assurer l'intégrité et la confidentialité des messages échangés via des mécanismes issus de la cryptographie *symétrique* (à base par exemple de l'algorithme standardisé de chiffrement par bloc AES).

La QKD peut être employée à la place des mécanismes cryptographiques asymétriques pour produire la clé, qui est ensuite utilisée normalement dans des mécanismes cryptographiques symétriques. Dans cet usage, le débit de secret atteint par la QKD ne limite pas le débit des communications, car une clé courte (typiquement 128 ou 256 bits) permet d'échanger de façon

protégée un très grand volume d'informations. Cette combinaison dépend cependant toujours de mécanismes cryptographiques calculatoires (dont la sécurité dépend en principe de la puissance de calcul d'un attaquant).

La QKD peut aussi être utilisée sans cryptographie symétrique, pour protéger les communications par des mécanismes à la sécurité non calculatoire. Pour assurer la confidentialité de messages, on utilise dans ce cas un masque jetable ou *one-time pad*, qui nécessite un bit de clé par bit de message transmis. Le débit utile atteignable est alors limité par le débit de secret produit par la QKD, à des valeurs qui sont typiquement entre 1.000 et 1.000.000 fois inférieures à ce qui peut être obtenu par du chiffrement symétrique. Ce débit utile très faible est rédhibitoire pour la plupart des applications.

Enfin la QKD est parfois décrite comme permettant d'assurer la sécurité du stockage de données. Cela consiste en fait à chiffrer des données par un moyen sans lien avec la QKD, puis à transporter la clé à l'aide de QKD en un lieu de stockage distinct de celui des données, éventuellement après l'avoir divisée en plusieurs parties à l'aide d'un mécanisme de partage de secrets. Il s'agit donc plus d'une application des communications sécurisées qu'une fonctionnalité véritablement distincte.

La QKD fournit-elle un nouveau service, ou vise-t-elle à remplacer des technologies existantes ? Quel est son champ d'application potentiel ?

On le voit, *la QKD fournit un service qui peut déjà être rendu par des primitives cryptographiques existantes*, avec de plus des limitations pratiques importantes concernant son applicabilité. Si l'on met provisoirement de côté ses propriétés de sécurité spécifiques, la question pertinente concernant les usages de la QKD est celle du sous-ensemble des usages actuels des communications sécurisées pour lesquels elle peut être utilisée, étant données ses limitations.

Au-delà des limites qui concernent le canal de communication employé (portée, incompatibilité avec des équipements actifs), le simple fait qu'il s'agisse d'une technologie nécessitant un matériel spécifique la désavantage nettement dans tous les cas d'usage où la cryptographie est aujourd'hui implémentée de façon logicielle, et l'empêche de fournir une sécurité de bout en bout dans une telle situation. Ainsi, elle ne peut être utilisée dans les environnements virtualisés ou pour protéger des communications entre des services.

L'utilisation la plus naturelle de la QKD consiste en la liaison sécurisée de deux sites terrestres fixes, suffisamment proches l'un de l'autre et reliés par une fibre optique.

Contre quelles menaces la QKD protège-t-elle spécifiquement ? Pourquoi est-ce un sujet d'actualité ?

L'intérêt de la QKD est d'offrir une immunité aux attaques mathématiques visant à obtenir les secrets produits. Dans les méthodes de négociation de clé employées aujourd'hui, à base de cryptographie asymétrique, l'attaquant cherchant à obtenir la clé commune possède toutes les informations nécessaires pour le faire, mais doit pour cela résoudre un problème mathématique. La résolution de ce problème nécessite d'effectuer une quantité de calculs parfaitement irréaliste avec les meilleures méthodes connues, et ce même en prenant en compte de façon optimiste l'évolution de la puissance de calcul sur plusieurs décennies. Cependant, il n'existe pas de *preuve d'absence* de méthodes sensiblement meilleures que les méthodes actuelles, qui permettraient de

rendre cette résolution faisable ; autrement dit, il n'existe pas de preuve absolue de la robustesse des méthodes de négociation de clé utilisées actuellement.

Ce problème, ancien à l'échelle de l'informatique et de la cryptographie moderne, a pris un tour nouveau avec les interrogations actuelles concernant la faisabilité d'un *ordinateur quantique universel*. Il est en effet prouvé qu'une telle machine, si elle venait à être construite, permettrait de résoudre bien plus efficacement que les ordinateurs actuels les problèmes mathématiques associés aux méthodes asymétriques de négociation de clé employées aujourd'hui (la factorisation de grands entiers pour RSA, le problème du logarithme discret pour Diffie-Hellman), au point de faire perdre toute sécurité à ces dernières. A l'inverse, l'ordinateur quantique universel n'altère pas significativement la sécurité de la cryptographie symétrique. C'est ce qui motive le discours légitimant le basculement de la négociation de clé asymétrique vers la QKD ; et ce d'autant plus si l'on se préoccupe de la sécurité dans la durée de données échangées aujourd'hui, ce qui nécessite de prendre en compte la menace de l'ordinateur quantique *avant* qu'elle devienne une réalité.

Nous le verrons plus loin, prendre en compte cette menace sans avoir recours à la QKD est possible. A ce stade, remarquons simplement que la résistance de la QKD aux attaques n'est pas absolue :

- Si théoriquement les protocoles QKD ne sont pas vulnérables aux attaques mathématiques, il est en pratique très difficile de les mettre en œuvre parfaitement. Un attaquant peut de plus parvenir à provoquer un fonctionnement anormal des équipements. Les écarts, provoqués ou non, vis-à-vis du protocole théorique sont alors susceptibles de compromettre la sécurité au point de conduire à des attaques pratiques. Ce problème, s'il est analogue au problème des canaux auxiliaires pour la cryptographie classique, est néanmoins spécifique à la QKD et a conduit à plusieurs cryptanalyses d'équipements QKD commerciaux (voir par exemple [5] pour l'un des premiers articles sur le sujet ou [6] pour une publication plus récente) ;
- Par ailleurs, les dispositifs de QKD peuvent posséder des faiblesses non liées au protocole quantique mise en œuvre : par exemple, des vulnérabilités logicielles ou une fuite de secrets par rayonnement électromagnétique. Ces problématiques, classiques pour des équipements cryptographiques, ont été peu examinées jusqu'à présent dans le cas des équipements QKD ; une analyse approfondie et normalisée de ceux-ci, par exemple au sens des critères communs [4], est nécessaire avant de pouvoir envisager leur emploi pour la protection de données sensibles.

Le déploiement de la QKD à grande échelle induit des problèmes de sécurité supplémentaires.

Un déploiement de la QKD à grande échelle est-il envisageable ? quel niveau de protection offrirait-il ?

Les limitations de portée de la QKD (ou la nécessité d'utiliser des satellites pour les dépasser), sa nature point-à-point, sa dépendance vis-à-vis des caractéristiques physiques des canaux qu'elle emprunte, rendent extrêmement complexe et coûteux son déploiement à grande échelle. Mais surtout, en l'absence de ligne directe reliant deux points désirant négocier une clé commune, les utilisateurs sont conduits à négocier des clés par tronçons sur un chemin composé de plusieurs liens QKD, *ce qui nécessite d'avoir confiance en les nœuds intermédiaires de la communication et constitue une régression majeure par rapport aux méthodes de négociation de clé de bout en bout*

actuelles. L'alternative qui consiste à relier directement tous les nœuds devant communiquer n'est pas réalisable en pratique sauf pour les réseaux de petite taille, tant en termes de nombre de terminaisons que d'extension géographique.

Si l'emploi de satellites permet de repousser les limites de portée de la QKD, il ne permet généralement pas la protection des informations de bout en bout, sauf si les deux extrémités de la communication disposent de leur propre infrastructure sol pour le lien spatial ; il repose par ailleurs sur l'hypothèse que chaque satellite est lui-même un nœud de confiance, ce qui suppose que le risque d'intrusion informatique soit parfaitement maîtrisé.

Quelles sont les alternatives aux méthodes de négociation de clé asymétriques actuelles autres que la QKD ?

La menace de l'ordinateur quantique est prise au sérieux par la communauté cryptographique depuis de nombreuses années. De nouveaux algorithmes asymétriques sont en cours de standardisation (principalement à travers la compétition organisée par le NIST [1]) en vue de remplacer les algorithmes vulnérables à l'ordinateur quantique. Des candidats sont déjà disponibles aujourd'hui, et un effort de développement conséquent aboutira à leur déploiement progressif dans les produits et les librairies logicielles de communications sécurisées dans la décennie à venir. Ce déploiement aura lieu sans modification fonctionnelle significative des services qui utilisent ces algorithmes.

Comme pour les mécanismes asymétriques actuels et sauf progrès théorique majeur, nous ne disposerons pas de preuve de robustesse absolue pour ces nouveaux mécanismes. La confiance que nous pourrons leur apporter viendra plutôt de l'intensité des efforts qui auront été consentis pour trouver leurs faiblesses et étudier les problèmes mathématiques sous-jacents.

En ce qui concerne la négociation de clé et le chiffrement asymétrique, l'ANSSI recommande l'emploi de ces nouveaux mécanismes dès que possible en cas de besoin de sécurité à long terme (plus de dix ans). Dans un tel cas de figure, pendant une période intermédiaire qui durera plusieurs années et qui pourra s'étendre au-delà de la conclusion de la compétition du NIST, l'ANSSI préconise de ne pas utiliser seuls les nouveaux mécanismes devant apporter la résistance à l'ordinateur quantique, mais plutôt de les combiner avec les mécanismes actuels de façon à écarter tout risque de régression sécuritaire liée à des mécanismes immatures.

Pour ce qui concerne la signature asymétrique, la nécessité de remplacer les algorithmes actuels est moins pressante, car la durée de validité d'une signature peut être bornée dans le temps ; par ailleurs, des mécanismes fondés sur des primitives éprouvées et peu affectées par l'ordinateur quantique peuvent convenir pour certains usages (voir par exemple [8]).

Les détails de ces recommandations, dont la mise en œuvre nécessite une expertise cryptographique, sortent du cadre du présent avis technique.

Dans un univers hypothétique sans négociation asymétrique de clé, une fonctionnalité équivalente à la QKD pourrait par ailleurs être obtenue par des mécanismes purement symétriques peu affectés par l'ordinateur quantique (la publication [2] fournit un exemple du type de protocole qui pourrait être employé). L'utilisation à grande échelle de ce type de solution ferait revenir les produits de communication sécurisée à ce qu'ils étaient avant la généralisation des mécanismes asymétriques : complexes et coûteux, nécessitant une gestion centralisée des secrets, et donc

réservés aux États et aux grandes organisations. Mais étant compatibles avec les réseaux actuels, ils demeureraient néanmoins plus simples à déployer que leurs équivalents à base de QKD.

Avis de l'ANSSI

Les garanties de sécurité apportées en principe par la QKD le sont aux au prix de contraintes d'emploi lourdes qui réduisent la portée des services offerts et compromettent le niveau de sécurité qui peut être atteint en pratique, en particulier dans les scénarios où les communications transitent par un réseau de liens QKD connectés entre eux. Si l'emploi de QKD sur des liaisons point à point peut malgré tout être envisagé comme une mesure complémentaire aux moyens cryptographiques classiques dans une logique de défense en profondeur, les dépenses qu'un tel choix occasionne ne doivent pas être faites au détriment de la lutte contre les menaces actuelles sur les systèmes d'information.

Références

- [1] Post-Quantum Cryptography Standardization, NIST, USA
- [2] "Symmetric Authenticated Key-Exchange (SAKE) with Perfect Forward Secrecy", 2019
- [3] White paper – Quantum Security Technologies, NCSC, Royaume-Uni, 24 mars 2020
- [4] Certification critères communs - ANSSI
- [5] "Hacking commercial quantum cryptography systems by tailored bright illumination", 2010
- [6] "Laser seeding attack in quantum key distribution", 2019
- [7] La communication quantique et le protocole BB84, 2019
- [8] "XMSS – A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions", 2011