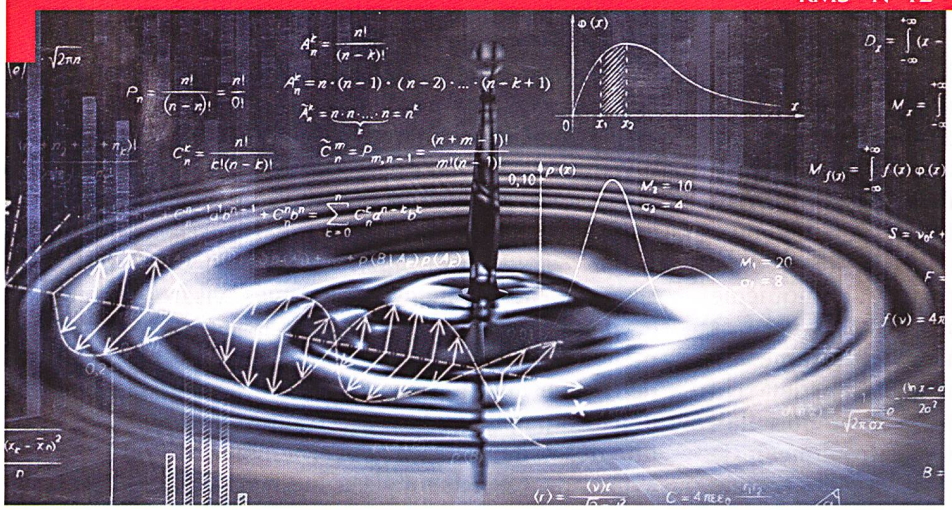
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: Evolution vers la cryptographie quantique
Autor: Verderosa, Mauro
DOI: https://doi.org/10.5169/seals-823454



Cyber

Evolution vers la cryptographie quantique

Mauro Verderosa
CISSP, IT Security Specialist chez PSYND

A travers des réseaux sociaux et des applications mobiles, la société moderne fait un usage intensif de la communication. Le canal utilisé pour transmettre ces communications n'est pas toujours sécurisé, et les informations qui y sont souvent échangées, bien que cryptées, ne peuvent plus être considérées comme confidentielles car les normes que nous utilisons pour la cryptographie doivent être repensées.

Comment la cryptographie fonctionne aujourd'hui?

Chiffrer un message, connu sous le nom de plain-text, signifie le transformer en un nouveau message, un texte chiffré, qui n'aura aucun sens pour quiconque le lirait et ne connaîtrait pas la clé de déchiffrement nécessaire pour le re-transformer en plain-text original. Ce modèle est appelé cryptographie à clé secrète, ce qui signifie que la puissance du secret est cachée dans les clés utilisées.

La cryptographie classique repose sur deux transformations: la permutation et la substitution.

La permutation est la transformation qui va déplacer chaque lettre du texte brut dans une position différente par rapport à l'endroit où elle était à l'origine. Par exemple, on pourrait imaginer que la première lettre d'un texte brut soit déplacée au milieu du texte chiffré, la seconde à la fin du texte chiffré, etc.

La substitution est la transformation qui remplacera dans le plain-text une lettre par une autre. Chaque lettre conservera sa position d'origine également dans le texte chiffré, tandis que sa valeur sera modifiée.

Ces deux concepts peuvent être fusionnés pour obtenir un mélange des deux systèmes:
Avec l'introduction des ordinateurs, ces principes ont évolué en quelque chose d'extrêmement complexe et

Figure 1: Transformation par permutation

Figure 2: Transformation par substitution

Figure 3: Transformation par permutation et par substitution

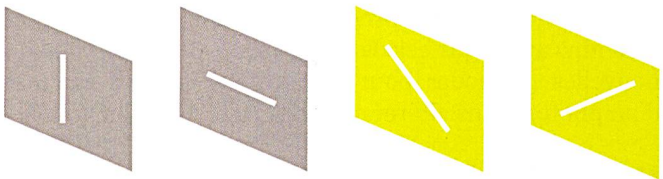


Figure 4: Filtres orthogonaux et diagonaux

Figure 5: Filtres pour la valeur 1

Figure 6: Filtres pour la valeur 0

sophistiqué, rendant le message incompréhensible pour quiconque ayant l'intention de le lire sans posséder la clé de déchiffrement.

Ces modèles sont appelés «sécurisés», ce qui signifie qu'ils sont considérés comme incassables uniquement parce que les cryptographes parient sur le fait que les efforts nécessaires pour déchiffrer les messages, en utilisant une attaque par force brute, seront trop chers, décourageant toute personne désireuse de rompre la clé de décryptage. En effet cela prendrait plusieurs années: un délai raisonnable pour décourager l'attaquant de casser la clé de cryptage et de décoder le message.

Malheureusement, il n'est pas toujours tenu compte du fait que chaque année la puissance de calcul des machines augmente de façon exponentielle. À titre d'exemple, l'un des standards les plus utilisés jusqu'à il y a 15 ans, le *Data Encryption Standard* (mieux connu sous le nom de DES) exigeait entre 6 mois et 2 ans pour être déchiffré, alors qu'aujourd'hui ce code pourrait être brisé en quelques minutes.

Les algorithmes cryptographiques les plus modernes nous donnent la certitude que ce qui est crypté aujourd'hui sera protégé pendant des milliers d'années, mais si une oreille indiscrète peut entrer dans le canal de communication alors que la clé, ou une partie de celle-ci, est en cours de transmission, notre sécurité pourrait être considérablement réduite (de plusieurs milliers d'années pour calculer la clé complète, à quelques mois). Cela pourrait être considéré comme bien si nous protégeons une communication entre deux amis qui acceptent un rendez-vous le lendemain, mais que se passerai-t-il si un autre gouvernement pouvait entrer en possession de nos secrets militaires aujourd'hui et les décrypter six mois après? Bien qu'ils puissent avoir besoin de mois, voire d'années, pour les décrypter, la sécurité nationale pourrait être encore exposée à des dangers. Aucun secret ne serait en sécurité.

Ces messages peuvent être cassés car, bien que cryptés, lorsque l'expéditeur enverra un bit représentant un 0, ce sera 0, et lorsque l'expéditeur enverra un bit représentant un 1, ce sera toujours un 1. Voyons voir comment, avec l'aide de la physique, nous pouvons transformer ce modèle en quelque chose d'incassable.

La cryptographie quantique

Le modèle de cryptographie quantique ne s'appuie pas sur les modèles mathématiques, mais sur ceux de la physique, le principe d'incertitude de Heisenberg. Ce principe dit que l'on ne peut pas absolument tout savoir sur le statut d'une particule quantique.

Dans la cryptographie quantique, la clé est un flux de photons qui ont une propriété appelée spin. C'est un état qui change quand il traverse un filtre qui pourrait être horizontal, vertical ou diagonale.

En utilisant les mêmes principes que le polariseur installé dans la plupart des caméras que nous utilisons tous les jours, en filtrant la lumière qui pénètre dans la lentille, nous pouvons filtrer les particules de lumière que nous faisons passer à travers les filtres.

Lorsque notre photon passera à travers un filtre horizontal ou à travers un filtre vertical, sa valeur ne changera pas, alors qu'il le fera quand il passera à travers une diagonale. Cela signifie qu'au moment où l'expéditeur transmettra un «1», basé sur le filtre utilisé, il pourrait apparaître comme un 1 ou un 0, bien que sa valeur reste inchangée: il gardera la valeur 1 pour le récepteur.

Pour la même raison un «0» sera toujours un 0 ou il sera transformé en 1 s'il passe par un filtre diagonal:

L'expéditeur communiquera avec le récepteur en utilisant un canal sécurisé uniquement le masque utilisé pour configurer les filtres, puis transmettra la clé.

Le récepteur appliquera le masque au flux de photons reçu. Parce qu'il ne connaîtra pas le flux exact utilisé par l'expéditeur, les informations en sa possession lui permettront de deviner correctement approximativement seulement 50% du flux original contenant la clé. Cette valeur sera la clé utilisée pour protéger la communication.

Si l'espion peut être en mesure d'intercepter la transmission, il pourra voir un 0 ou un 1 traversant le canal, mais il ne saura pas s'il s'agit d'une valeur originale ou transformée. Cela signifie que l'indiscret ne pourra utiliser aucun bit de la transmission. De plus, la cryptographie quantique est la première cryptographie qui protège contre l'interception passive. Puisque nous ne pouvons pas mesurer un photon sans affecter son comportement, le principe d'incertitude de Heisenberg

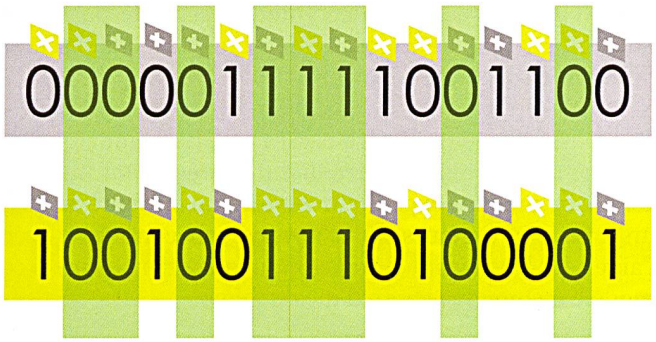


Figure 7: Choix de la clé dans la cryptographie quantique

émerge lorsque l'oreille indiscrète fait les premières mesures d'écoute. Cette mesure va modifier le contenu de la transmission et, au moment où la quantité d'erreurs accumulées par le récepteur dépassera un seuil, une toute nouvelle clé sera générée.

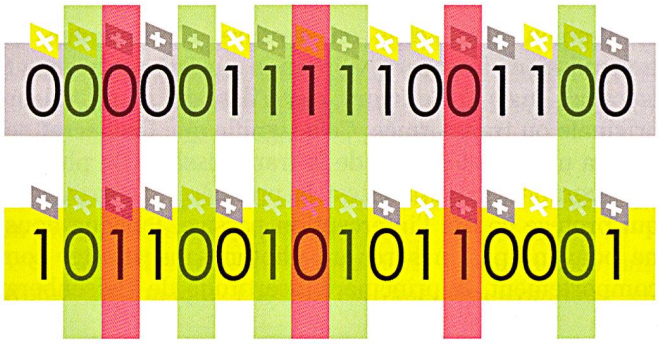
Où sommes-nous aujourd'hui?

Ce modèle de cryptographie présente encore quelques faiblesses, tout d'abord la distance qui pourrait être utilisée pour l'implémenter.

Le système original de cryptographie quantique, construit en 1989, a pu atteindre jusqu'à 36 centimètres, alors que nous sommes arrivés il y a quelques années pour couvrir des distances de 150 kilomètres. De plus, cette distance, si on la compare à la taille du réseau informatique moderne, est trop courte pour répondre à la plupart des besoins dont nous pourrions avoir besoin aujourd'hui.

Le problème principal est lié à l'interférence générée par le canal utilisé pour la transmission: le spin d'un photon peut être modifié lorsqu'il rebondit sur d'autres particules, et donc lorsqu'il est reçu il peut ne plus être polarisé comme il était initialement prévu. Cela signifie qu'un 1 peut apparaître comme un 0, et vice versa. Plus la distance parcourue par le photon augmentera, plus la probabilité de rencontrer d'autres particules et d'être influencé par elles augmentera.

Figure 8: Détection d'erreur pour l'interception d'attaque



Comme la technologie progresse, c'est juste une question de temps avant que ces défis ne soient résolus, ou que de nouvelles méthodes pour comprendre le spin original d'un photon, sans altérer son statut, soient découvertes.

Mais cela ne doit pas nous décourager: la première mise en œuvre publique d'une cryptographie quantique s'est déroulée en Suisse, dans le canton de Genève pour les élections parlementaires de 2007. À Genève, les votes sont cryptés dans une centrale de dépouillement. Ensuite, les résultats sont transmis sur une ligne de fibre optique dédiée à une installation de stockage de données à distance. Les résultats du vote sont sécurisés par cryptographie quantique, et la partie la plus vulnérable de la transaction de données (lorsque le vote passe de la station de comptage au référentiel central) est ininterrompue. Cette technologie se répandra bientôt dans le monde entier, car de nombreux autres pays font face au spectre des élections frauduleuses.

Autres usages, extrêmement délicats, qui pourraient être la communication avec l'espace, où il serait clairement impossible d'utiliser n'importe quel type de connexion filaire pour sécuriser la communication entre la Terre et les astronautes. Les informations sur le site et en transit pourraient être constamment protégées.

Il pourrait aussi être facile d'imaginer que les pays utilisant l'énergie nucléaire puissent être disposés à faire respecter leurs défenses. Un attaquant pourrait être prêt à prendre le contrôle ou à perturber les mesures de sécurité en bloquant l'approvisionnement en électricité de tout un pays. Nous pourrions avoir besoin de niveaux de sécurité plus élevés pour pouvoir défendre et garantir la sécurité de notre infrastructure contre les attaques.

Et qu'en est-il de nos communications privées? Nous devrions toujours être conscients que dans un proche avenir, cette technologie pourrait entrer dans toutes les maisons ou être utilisée par les téléphones mobiles. Aujourd'hui, Internet est relativement rapide, mais le niveau de sécurité mis en œuvre est loin de ce qui pourrait être obtenu en utilisant la cryptographie quantique. Alors pourquoi ne pas tout transmettre en l'utilisant? Le cryptage quantique ralentirait considérablement Internet, bien que l'on puisse imaginer un avenir où il serait possible d'utiliser un Internet plus classique ou un Internet confidentiel lent. Une utilisation civile importante, par exemple, pourrait être autour des nouveaux smartphones et des objets portables que nous avons, qui contiennent plusieurs informations sur nous, en commençant par les identificateurs biométriques (nous utilisons les empreintes digitales pour débloquer nos nouveaux téléphones, ou smartwatch pour contrôler nos battements de cœur). Ces informations ne devraient être transmises que par des canaux protégés.

La cryptographie quantique sera le bon pas dans la bonne direction, comblant les lacunes créées au cours des dernières décennies par les informations que nous partageons aujourd'hui.

M. V.