Les clÃ©s de la Cryptographie Post-Quantique
Internet
PostÃ© par : JulieM
PubliÃ©e le : 21/9/2022 13:00:00

La technologie des ordinateurs quantiques nâ□□en est quâ□□Ã ses dÃ©buts quâ□□on parle dÃ©jÃ de cryptographie post-quantique. Loin du buzzword, cette discipline est en passe de devenir un vrai casse-tÃªte dans les secteurs de la cybersÃ©curitÃ©, des tÃ©lÃ©communications, des banques ou encore des renseignements dixit MichÃ¨le Colly â□□ SCC France .

La disruption de lâ□□informatique quantique, avant dâ□□Ãªtre une opportunitÃ© et une source de progrÃ¨s dans de nombreux domaines, sera une menace sÃ©rieuse pour la sÃ©curitÃ© des donnÃ©es.

Deux disciplines distinctes : la cryptographie quantique vs la cryptographie post-quantique.

DÃ©cryptage

La cryptographie quantique

La cryptographie quantique est sortie du domaine thÃ©orique depuis quelques annÃ©es. Si on ignore depuis quand les Ã©tats-majors militaires ou les services de renseignement la testent, on sait quâ□□elle a Ã©tÃ© utilisÃ©e avec succÃ¨s dÃ¨s 2004 lors dâ□□une importante transaction financiÃ¨re, puis en 2007 avec ID Quantique, spin-off de lâ□□UniversitÃ© de GenÃ¨ve pour transmettre les rÃ©sultats des Ã©lections suisses.

La cryptographie quantique utilise les propriÃ©tÃ©s de la physique quantique pour Ã©tablir des protocoles de cryptographie. Le porteur dâ□□information est alors le photon â□□ encodÃ© via la polarisation, sa phase ou encore son amplitude. Lâ□□exemple le plus connu est la distribution quantique de clÃ©s secrÃ¨tes, appelÃ©e QKD (Quantum Key Distribution) fournissant un canal de communication sÃ©curisÃ© entre deux utilisateurs distants pour gÃ©nÃ©rer une clÃ© privÃ©e.

La clÃ© ainsi distribuÃ©e peut alors Ãªtre utilisÃ©e pour chiffrer et dÃ©chiffrer de maniÃ¨re symÃ©trique un message via la technique du masque jetable (somme modulo deux entre le message et la clÃ©), garantissant un niveau de sÃ©curitÃ© inconditionnel de bout en bout. Et ce, mÃªme face Ã un adversaire en possession dâ□□un ordinateur quantique.

Cette technique repose sur le fait quâ□□il est impossible de copier lâ□□Ã©tat dâ□□un systÃ¨me quantique (thÃ©orÃ¨me de non-clonage) et que toute mesure sur un systÃ¨me quantique perturbe en gÃ©nÃ©ral ce dernier, de sorte que la prÃ©sence dâ□□un espion cherchant Ã acquÃ©rir de lâ□□information sur la clÃ© Ã©changÃ©e est alors dÃ©celable.

La cryptographie post-quantique

La cryptographie post-quantique dÃ©signe des algorithmes de chiffrement conventionnel robustes, face Ã un attaquant disposant dâ□□un hypothÃ©tique ordinateur quantique de grande Ã©chelle, avec plusieurs milliers, voire centaines de milliers de qubits logiques.

Pour ce dernier, câ□□est un peu lâ□□histoire du pompier pyromane. Dâ□□un cÃ´tÃ© les pompiers cherchant Ã protÃ©ger les communications numÃ©riques avec des algorithmes rÃ©sistants. De lâ□□autre, les pyromanes, espÃ©rant casser les clÃ©s de sÃ©curitÃ© publique de type RSA.

Lâ□□Algorithme de Shor

En 1994, Peter Shor, un mathÃ©maticien amÃ©ricain crÃ©e un algorithme capable de factoriser rapidement des nombres entiers. Ã□ lâ□□Ã©poque, les chercheurs nâ□□avaient pas rÃ©ussi Ã crÃ©er un seul qubit contrÃ´lable, que lâ□□algorithme provoquait dÃ©jÃ un vif intÃ©rÃªt pour le calcul quantique.

Lâ□□algorithme de Shor permet de casser de nombreux systÃ¨mes de cryptographie utilisant des clÃ©s publiques, tel que le protocole RSA massivement utilisÃ© dans le e-commerce. Lâ□□industrie des tÃ©lÃ©coms et de lâ□□informatique seront les premiers impactÃ©s. Cet algorithme ne peut toutefois tourner que sur des ordinateurs quantiques universels avec correction dâ□□erreurs, nÃ©cessitant un nombre non nÃ©gligeable de qubits physiques.

Les consÃ©quences

Lâ□□avÃ¨nement de lâ□□ordinateur quantique devrait avoir un rÃ©el impact sur la cryptographie asymÃ©trique Ã clÃ© publique, rendant les protections des infrastructures et des applications obsolÃ¨tes, si le risque nâ□□est pas anticipÃ©. Les entreprises devront fournir un Ã©norme effort de gestion du changement pouvant aller de 2 Ã 4 ans.

Lâ□□ordinateur quantique constitue un risque potentiel qui peut Ãªtre anticipÃ© via une migration vers des algorithmes de chiffrement post-quantiques, dont il reste Ã dÃ©finir les standards.

Les systÃ¨mes de cryptographie symÃ©triques Ã clÃ© privÃ©e sont Ã lâ□□abri de la menace Shor, car la cryptographie quantique est Ã mÃªme dâ□□apporter une rÃ©ponse Ã cette problÃ©matique et porte la promesse dâ□□une sÃ©curitÃ© inconditionnelle.

La Cryptographie Post-Quantique, câ□□est pour tout de suite ?

Lâ□□ordinateur quantique parfait nâ□□existe pas encore que dÃ©jÃ , bon nombre dâ□□algorithmes sont prÃªts Ã y Ãªtre implÃ©mentÃ©s. Jusquâ□□Ã prÃ©sent, aucune implÃ©mentation de ce cÃ©lÃ¨bre algorithme nâ□□avait pu Ãªtre vÃ©rifiÃ©e, faute dâ□□outils adaptÃ©s. Mais des solutions de cryptographies robustes Ã lâ□□algorithme de Shor fleurissent dÃ©jÃ , comme CryptoNext Security, spin-off de lâ□□Inria Paris et de la Sorbonne.

Par ailleurs, les premiÃ¨res gÃ©nÃ©rations dâ□□ordinateurs quantiques ne supporteront probablement pas une implÃ©mentation Â« efficace Â» de lâ□□algorithme de Shor. Lâ□□algorithme reste toutefois un Ã©tendard symbolique pour le logiciel quantique, ainsi quâ□□un Ã©talon pour prouver le passage Ã lâ□□Ã©chelle des diffÃ©rentes solutions.