La cryptographie post-quantique anticipe les ordinateurs quantiques

Description

Quand lâ€™ordinateur quantique nâ€™existe pas, quand les calculateurs quantiques font rÃ©guliÃ¨rement lâ€™objet dâ€™effets dâ€™annonce de la part de ceux qui les financent, la cryptographie post-quantique, elle, existe bel et bien, et dÃ©signe les algorithmes cryptographiques qui seront capables de rÃ©sister Ã la puissance de calcul de ces futurs ordinateurs.

Si nos ordinateurs contemporains fonctionnent avec des bits, 0 et 1, les ordinateurs quantiques (voir *La rem* nÂ°53, p.74), remplacent les bits par des qbits dont lâ€™une des propriÃ©tÃ©s, issues des principes de la physique quantique, est de pouvoir reprÃ©senter 0 et 1 en mÃªme temps, en Â« superÂposition Â». La puissance de calcul qui dÃ©coule de ces nouvelles lois de la physique bouleverse en profondeur les fondements de la cryptographie dite Â« classique Â», qui repose sur la difficultÃ© des ordinateurs actuels Ã rÃ©aliser certains calculs. UtilisÃ©e jusquâ€™Ã prÃ©sent, la cryptographie asymÃ©trique, ou Ã clef publique, est basÃ©e sur des problÃ¨mes mathÃ©matiques de factoÂriÂsation dâ€™entiers ou du logarithme discret, afin dâ€™Ã©tablir un canal chiffrÃ© entre deux parties pour sâ€™authentifier, ou encore signer Ã©lectroniquement. Prenons lâ€™exemple de la factoriÂsation dâ€™entiers. En octobre 1977, les lecteurs du magazine *Pour la Science*Â furent mis au dÃ©fi de rÃ©pondre Ã cette questionÂ :Â *Â«Â le nombreÂ 114 381Â 625 757Â 888 867Â 669 235Â 779 976Â 146 612Â 010 218Â 296 721Â 242 362Â 562 561Â 842 935Â 706 935Â 245 733Â 897 830Â 597 123Â 563 958Â 705 058Â 989 075Â 147 599Â 290 026Â 879 543Â 541 est le produit de deux nombres premiersÂ ; lesquels ?Â Â»*Â Avec un ordinateur classique, il est trÃ¨s difficileÂ de factoriser les grands nombres entiers et câ€™est le fondement mÃªme de la cryptographie asymÃ©trique que de reposer sur cette difficultÃ©. Le chiffrement RSA, dÃ©crit en 1977 par Ronald Rivest, Adi Shamir et Leonard Adleman, est un algorithme de cryptographie asymÃ©trique qui sert aujourdâ€™hui Ã sÃ©curiser les transactions bancaires, les transactions de commerce Ã©lectronique ou encore lâ€™Ã©change de donnÃ©es confidentiellesÂ *viaÂ* internet. Cet algorithme utilise une paire de clÃ©s (des nombres entiers) composÃ©e dâ€™une clÃ© publique pour chiffrer, et dâ€™une clÃ© privÃ©e pour dÃ©chiffrer des donnÃ©es confidentielles. Or, si ce calcul rÃ©siste Ã la puissance des ordinateurs classiques, ce ne sera plus le cas avec un ordinateur quantique.

Comme lâ€™explique le journaliste scientifique Julien Bourdet,Â *Â«Â un ordinateurÂ quantiqueÂ peut en thÃ©orie avoir accÃ¨s Ã la totalitÃ© des rÃ©sultatsÂ possibles dâ€™un calcul en une seule Ã©tape, lÃ oÃ¹Â unÂ ordinateurÂ classique doit traiter lâ€™information deÂ faÃ§onÂ sÃ©quentielle, un rÃ©sultat aprÃ¨s lâ€™autreÂ Â»*.Â Si bien que le jour oÃ¹ un Ã‰tat ou une entreprise parviendra Ã mettre au point un ordinateur quantique, il lui sera facile de casser les systÃ¨mes de cryptographie actuels.

Câ€™est ainsi quâ€™est nÃ©e la cryptographie post-quantique. Elle a non seulement pour objectif de se

prÃ©munir dâ€™attaques provenant dâ€™un futur ordinateur quantique, mais Ã©galement de pouvoir interagir avec les protocoles de rÃ©seaux de communication actuels.

En 2016, le National Institute of Standards and Technology (NIST), une agence fÃ©dÃ©rale non rÃ©glementaire rattachÃ©e au dÃ©partement amÃ©ricain du commerce, a organisÃ© une compÃ©tition mondiale et publique pour dÃ©finir les futurs standards des algorithmes de cryptographie post-quantique. Le 5Â juillet 2022, le NIST a prÃ©sentÃ© les quatre algorithmes sÃ©lectionnÃ©s, dont la standardisation sera finalisÃ©e en 2024. Il sâ€™agitÂ *Â«Â dâ€™un algorithme dâ€™Ã©tablissement de clÃ© nommÃ© CRYSTALS-Kyber ; et de trois algorithmes de signaÂture nommÃ©s CRYSTALS-Dilithium, FALCON et SPHINCS+. Les trois premiers de ces algorithmes sont fondÃ©s sur les rÃ©seaux euclidiens structurÃ©s ; leÂ dernier, SPHINCS+, est fondÃ© sur des constructions enÂ arbres de hachageÂ Â»*Â prÃ©cise lâ€™Agence nationale de la sÃ©cuÂritÃ© des systÃ¨mes dâ€™information (Anssi). Ce quâ€™il faut comprendre est que ces algorithmes dÃ©signent des problÃ¨mes mathÃ©matiques parmi les plus difficiles Ã rÃ©soudre, y compris pour un ordinateur quantique.

Si ces algorithmes deviennent les normes fÃ©dÃ©rales amÃ©ricaines, celles-ci seront probablement Ã©galement utilisÃ©es comme standards industriels internationaux. Dans une tribune publiÃ©e parÂ *Le Monde*, Ludovic Perret, maÃ®tre de confÃ©rences Ã Sorbonne UniversitÃ© et cofondateur de lâ€™entreprise Cryptonext, explique queÂ *Â«Â cette course Ã la norme doit aussi se comprendre comme unÂ outil de conquÃªte Ã©conomiqueÂ : qui contrÃ´le laÂ norme contrÃ´le le marchÃ©.Â Or, la normalisation post-ÂquantiqueÂ reste un point faible dans les ambitions industrielles et de souverainetÃ© technologique europÃ©ennesÂ Â»*.

Ironie du sortÂ : parmi ces quatre algorithmes, trois ont reÃ§u des contributions de laboratoires de recherche franÃ§ais, rattachÃ©s Ã lâ€™Institut des sciences de lâ€™information et de leurs interactions (INS2I) qui, depuis 2009, coordonne notamment les recherches menÃ©es au CNRS sur le sujet. Lâ€™INS2I explique ainsi queÂ *Â«Â pour le chiffrement Ã clÃ© publique et les algorithmes dâ€™Ã©tablissement de clÃ©, le seul algorithme retenu est CRYSTALS-Kyber qui implique un consortium dont fait partie Damien StehlÃ©, professeur Ã lâ€™ENS de Lyon et membre du Laboratoire de lâ€™informatique du parallÃ©lisme (LIP â€“ CNRS/ENS de Lyon/UniversitÃ© Claude Bernard Lyon 1). Le mÃªme enseignant-chercheur est impliquÃ© dans CRYSTALS-Dilithium, algorithme qui doit servir cette fois-ci Ã la gÃ©nÃ©ration de signatures Ã©lectroniques. Dans cette mÃªme catÃ©gorie, deux autres algorithmes ont Ã©tÃ© retenus, dont FALCON auquel a participÃ© Pierre-AlainÂ Fouque, professeur Ã lâ€™UniversitÃ© de Rennes 1 et membre deÂ lâ€™Institut de recherche en informatique et systÃ¨mes alÃ©atoires (IRISA â€“ CNRS/UniversitÃ© de Rennes 1). UneÂ reconnaissance de plus pour cet enseignant-chercheur Ã la tÃªte du projet PQ-TLS sur la cryptographie post-quantique dans le PEPR Quantique qui vient dâ€™Ãªtre lancÃ©Â Â»*.

Alors que des problÃ©matiques de souverainetÃ© taraudent les EuropÃ©ens dans de nombreux domaines, il sâ€™avÃ¨re queÂ les Ã‰tats-Unis vont probablement imposer leurs propres normes tout en sâ€™appuyant sur les travaux issus de chercheurs franÃ§ais.Â Lâ€™European Telecommunications

Standards Institute (ETSI), situÃ© Ã Sophia-Antipolis, a Ã©tÃ© crÃ©Ã© en 1988 parÂ laÂ ConfÃ©rence europÃ©enne des Postes et TÃ©lÃ©comÂmunications, Ã laÂ demande de la Commission europÃ©enne. Câ€™est aujourdâ€™hui lâ€™un des trois organismes europÃ©ens officiellement responsables de la normalisation des technologies de lâ€™information et de la commuÂniÂ-cation. Comble de lâ€™ironie, et toujours selon Ludovic Perret,Â *Â«Â le responsable du groupe post-Â-quantique de lâ€™ETSI est amÃ©ricain, et salariÃ© dâ€™Amazon, et les coresponsablesÂ travaillent pour une start-up canadienne dans le post-quantique et une agence gouvernementale (NCSC) britanniqueÂ Â»*. Difficile dâ€™imaginer plus mauvaise configuration pour que lâ€™Europe prenne la mainÂ surÂ les futurs standards de la cryptographie post-quantique.

SourcesÂ :

- Â« National Institute of Standards and Technology Â», nist.gov
- Â« La factorisation dâ€™entiers Â», FranÃ§ois Morain, pourlascience.fr, 1er juillet 2002.
- Â«Â OrdinateurÂ : les promesses de lâ€™aube quantiqueÂ Â», JulienÂ Bourdet,Â *CNRS Le journal*, lejournal.cnrs.fr, 15 avril 2019, MAJ le 27 janvier 2021.
- Â« Lâ€™Europe doit se prÃ©parer Ã la rÃ©volution postquantique Â», Ludovic Perret, lemonde.fr, 13 avril 2022.
- Â« Avis scientifique et technique de lâ€™ANSSI sur la migration vers la cryptographie post-quantique Â», ANSSI, ssi.gouv.fr, 14 avril 2022.
- Â« Plusieurs laboratoires franÃ§ais impliquÃ©s dans les algorithmes sÃ©lectionnÃ©s par le concours NIST sur la cryptographie post-quantique Â», INS2I, ins2i.cnrs.fr, 6 juillet 2022.
- Â« Lâ€™algorithme de Thales et IBM retenu par Washington pour rÃ©sister Ã la menace quantique Â», Alice Vitard, usine-digitale.fr, 13 juillet 2022.Â

Categorie

1. Techniques

date crÃ©Ã©e
2 fÃ©vrier 2023
Auteur
jacquesandrefines