Publié sur le site de l'INRIA le 7/10/2019 :

https://www.inria.fr/centre/paris/actualites/cryptonext-security-un-logiciel-de-chiffrement-a-l-epreuve-des-futurs-ordinateurs-quantiques

Cryptonext Security : un logiciel de chiffrement à l'épreuve des futurs ordinateurs quantiques

La startup *Cryptonext Security* a été créée en juin 2019 par Ludovic Perret et Jean-Charles Faugère. Cette *spin-off* d'Inria et de Sorbonne Université propose des logiciels capables de résister à la prochaine menace de sécurité : la puissance de calcul phénoménale des ordinateurs quantiques permettra de "casser" facilement la plupart des codes de cryptographie actuellement utilisés ! Leur logiciel BtoB veut donc devenir l'un des outils incontournables de la cybersécurité.

La sécurité de nombreux logiciels et d'innombrables données repose sur le fait qu'ils sont chiffrés : les contenus sont chiffrés grâce à une clé publique, une clé secrète permet le déchiffrement. Faute de connaître cette clé, un "indiscret" doit la deviner, ce qui est un processus long et fastidieux avec nos ordinateurs actuels. Or, le temps passé à accéder à l'information la rend caduque ou moins intéressante à détenir, qu'il s'agisse d'un code temporaire pour un achat par carte bleue sur Internet ou de la communication entre un état-major et un soldat sur le terrain par exemple. Un bon chiffrement est donc un chiffrement qui bloque l'intrus suffisamment longtemps.

Mais la puissance de calcul des ordinateurs quantiques rendra dérisoires les temps de calcul nécessaires à outrepasser des chiffrements actuellement considérés parfaitement sûrs. Étant donnée l'imminence de l'arrivée des ordinateurs quantiques, qui devraient atteindre une puissance suffisante pour compromette la sécurité des communications d'ici une dizaine d'années, élaborer une nouvelle cryptographie et l'incorporer aux différents protocoles de communications est donc devenu un enjeu majeur. Et c'est un enjeu d'aujourd'hui : certaines données diffusées maintenant doivent pouvoir résister à une lecture facile demain...

Proposer des clés de chiffrement "postquantique"

C'est pour proposer des dispositifs résistants à ces capacités de calcul "postquantiques" que la startup *Cryptonext Security* a été créée à Paris en juin 2019, après trois ans de préparation. Ses deux fondateurs, Ludovic Perret et Jean-Charles Faugère, sont issus de l'équipe Polsys, commune à Inria et Sorbonne Université. Celle-ci est reconnue internationalement comme l'une des meilleures dans le domaine de la résolution de systèmes non

linéaires par des méthodes exactes. Elle développe des algorithmes très efficaces pour déterminer les solutions de systèmes d'équations polynomiales ou algébriques.

L'une des applications pratiques de ces algorithmes est leur utilisation en cryptologie : cela permet de définir des clés de chiffrement allant au-delà de toutes les possibilités de calcul (y compris celles de l'ordinateur quantique) en imposant de résoudre des systèmes d'équations algébriques ou linéaires ayant énormément de solutions, en y ajoutant des contraintes sur la "bonne solution" permettant le décryptage.

« La cryptographie à clé publique classique repose, mathématiquement, sur le concept de factorisation de grands entiers , explique Jean-Charles Faugère, directeur général de *Cryptonex Security*. *Il faut donc trouver maintenant de nouveaux problèmes extrêmement compliqués à résoudre et cela peut passer, par exemple par des systèmes d'équations non linéaires de grandes tailles. »*

Une "course aux standards"

Mais, dans la technologie qui sera effectivement appliquée à l'avenir pour le chiffrement à clé publique, plusieurs méthodologies sont possibles. Et il faut les normaliser. C'est un processus en cours, *via* un concours lancé par le NIST (*National Institute of Standards and Technology* , aux États-Unis) qui définira les technologies les plus performantes et, ainsi, celles qui seront les normes de demain. 80 solutions étaient sur les rangs au départ, il en reste 26 à ce jour.

Dans cette "course aux normes", *Cryptonext Security* est bien placée : son logiciel reste en lice pour les demi-finales, avec un logiciel basé sur la résolution d'équations algébriques.

> *« Avoir un algorithme qui figure parmi les finalistes est une reconnaissance de la qualité de notre travail,* se félicite LudovicPerret, président de *Cryptonext Security.Et, en participant à la définition des standards, nous pouvons anticiper et être en avance de phase avec notre logiciel. »*

Aujourd'hui, sans attendre demain !

Or, il ne faut effectivement pas attendre que les normes soient adoptées pour intégrer les solutions du futur : le jour J, de l'ampoule de salon à l'informatique embarquée des véhicules, en passant par les téléphones portables, ce seront des milliards d'objets connectés à mettre à jour pour qu'ils passent "le cap du quantique" ! Et pour certains acteurs, voir très loin est primordial : les systèmes embarqués des avions par exemple ne sont pas *a priori* recertifiés après autorisation.

« Nous avons donc intégré dans notre logiciel différentes solutions techniques, compatibles avec les standards actuels mais aussi avec ceux qui seront la norme à l'avenir, indique Jean-Charles Faugère. *Ce que nous proposons peut être vu comme une couche de sécurité supplémentaire aujourd'hui. Avec l'avènement de l'ordinateur quantique, la première, celle que nous considérons sûre actuellement, sera dérisoire ! »*

> *« L'utilisateur final n'a pas conscience des solutions de cryptage qui interviennent lorsqu'il utilise des dispositifs connectés et la complexité croissante du cryptage n'y changera rien* , souligne Ludovic Perret. *Nous proposons déjà nos solutions à des entreprises soucieuses de la confidentialité et de la sécurité lors d'échanges de données via internet, comme les banques par exemple, ou, pour la Défense, lors d'envoi de données chiffrées pour communiquer avec l'un de ses avions. »*

La levée de fonds que finalise *Cryptonext Security* en ce moment devrait lui ouvrir en grand les portes du marché de la cryptographie du futur : elle lui permettra d'étoffer l'équipe de R&D pour accélérer le développement de son produit... avant d'en envisager une deuxième pour le développement commercial.