datanews

Une thèse belge fait grand cas de la cryptographie 'à résistance quantique'

12/12/18 à 14:00 - Mise à jour à 14:00 Source: Datanews

CLUSIB, le Club de la Sécurité Informatique Belge, a loué la thèse de l'étudiant de la KU Leuven, Ward Beullens, en tant que meilleure thèse de master apportant une contribution à la sécurité des systèmes d'information. Son travail est du reste en course pour devenir une norme post-quantique.

© ISTOCK

Le jury de CLUSIB a récompensé d'un prix de 2.000 euros la thèse de master intitulée 'New Signature Schemes based on UOV with smaller public keys' de Ward Beullens. Ward a rédigé sa thèse dans le cadre de son Master en Mathématiques à la KU Leuven, sous la direction du professeur et expert en cryptographie Bart Preneel. CLUSIB attribue ce prix pour la quatrième fois.

Qu'en sera-t-il avec l'arrivée de l'ordinateur quantique?

Sa thèse porte sur la migration vers une nouvelle cryptographie résistant à de possibles attaques de la part d'ordinateurs quantiques. Ce genre d'ordinateur quantique pourrait en théorie être utilisé pour 'craquer' toute cryptographie à clé publique utilisée aujourd'hui. Nombre d'organisations telles Google, Intel, IBM, mais aussi la NSA ont déjà investi des centaines de millions dans la recherche sur les ordinateurs quantiques et tentent d'en construire un. Ce type d'ordinateur quantique se caractérise par une puissance de calcul exponentielle, qui pourrait aussi 'craquer' la cryptographie existante. Cela sous-entend le décryptage des communications secrètes, mais tout aussi bien le transfert forcé de mises à jour infectées vers des ordinateurs et des smartphones en vue d'en prendre le contrôle.

Nouvelle cryptographie

"Pour empêcher cela, nous devrons migrer à temps vers une nouvelle cryptographie qui résiste aux attaques des ordinateurs quantiques, ce qu'on appelle la cryptographie Post-Quantique. Ma thèse porte sur l'amélioration de ce genre d'algorithme Post-Quantique", précise Ward Beullens. Concrètement, il a développé deux méthodes en vue de réduire considérablement (jusqu'à 15x) la taille de la clé publique. Cela a pour but de rendre ce type d'algorithme nettement plus attractif, car la taille de la clé était jusqu'à présent le principal inconvénient de l'algorithme.

Base d'une nouvelle norme?

Il est possible qu'il y ait une suite pour Ward Beullens. En effet, sa thèse a entre-temps aussi été envoyée au National Institute of Standards and Technology (NIST) américain, qui organise actuellement un concours axé sur les algorithmes cryptographiques post-quantiques de valeur. Si Ward Beullens remporte ce concours, il est possible que son travail devienne une norme post-quantique. Ce ne serait du reste pas une primeur pour la Belgique. Précédemment en effet, le NIST avait organisé un concours similaire pour standardiser AES: l'Advanced Encryption Standard tel qu'il est actuellement utilisé au niveau mondial. Ce concours avait été remporté en 2001 par le 'Rijndael' belge: un algorithme cryptographique inventé par Joan Daemen et Vincent Rijmen. L'appellation Rijndael est une dérivée de leurs noms de famille.