Les ordinateurs quantiques, la fin du RSA ?

- Informatique - Sécurité Informatique -

Date de mise en ligne : mardi 25 novembre 2008

Les ordinateurs quantiques, bien qu'encore fictifs, pourraient remettre en cause les méthodes de cryptographie actuelles. Les deux plus utilisées sont le RSA, basé sur la difficulté de factoriser de grands nombres, et la cryptographie reposant sur les courbes elliptiques. Cependant un ordinateur quantique, pourrait selon les chercheurs, facilement contourner ces méthodes. Le mois dernier une conférence internationale s'est tenue à Cincinnati, avec des industriels et des membres du gouvernement pour se pencher sur ce problème.

A l'heure actuelle le RSA est utilisé pour coder un grand nombre de transmissions informatiques comme les informations bancaires, les e-mails ou les identifications via internet. Pouvoir décoder le RSA de l'extérieur se révèle donc être une menace sérieuse dans notre société. Pour Jintai Ding professeur de mathématiques à l'université de Cincinnati, une des failles les plus préoccupantes serait alors la mise à jour des logiciels : "si quelqu'un pouvait briser le RSA il pourrait alors installer un logiciel en le faisant passer pour une mise à jour de Microsoft par exemple, et ainsi prendre le contrôle d'un ordinateur".

Face à cette menace, les chercheurs tentent de développer de nouveaux modèles de cryptographie. Plusieurs pistes semblent être intéressantes : la théorie d' "Error Correcting Code (ECC)", la théorie des réseaux et la problématique du "plus court vecteur", la cryptographie multivariable ou encore la "signature scheme". Cependant pour le moment l'efficacité et de la fiabilité de ces modèles n'ont pu être entièrement démontré et il est encore difficile d'en privilégier un en particulier. Enfin une autre perspective plus lointaine est la cryptographie quantique, mais la technologie est encore mal maîtrisée et reste très chère à mettre en place.

Mais pour le moment les recherches sur la conception de l'ordinateur quantique sont encore loin de permettre sa fabrication. Les prédictions les plus optimistes annoncent son apparition dans 10 ans voire 20 ans. Le RSA et la cryptologie actuelle ont encore de beaux jours devant eux.

Post-scriptum :

http://www.bulletins-electroniques....