UNIVERSITÉ DE GENÈVE

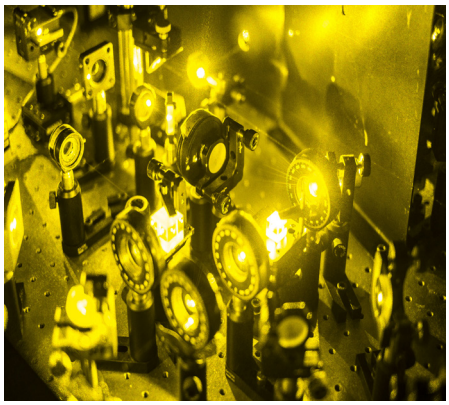
COMMUNIQUÉ DE PRESSE

Genève | 31 mai 2017

Nombres aléatoires: les espions vont se casser les dents

Des chercheurs de l'Université de Genève ont mis au point un nouveau procédé quantique pour générer des nombres aléatoires.

Lorsque l'on souhaite échanger des messages secrets, il faut utiliser une clé de cryptage. Pour que cette clé soit efficace, elle doit être constituée de nombres aléatoires, sans structure, à l'exact opposé de la date de naissance de notre animal de compagnie. Or, il est très difficile pour l'être humain de ne pas insérer de biais, même lorsqu'il pense taper des nombres au hasard. C'est pourquoi des physiciens de l'Université de Genève (UNIGE) ont mis au point un nouveau générateur de nombres aléatoires fonctionnant selon les principes de la physique quantique. Cette théorie physique, qui va généralement à l'encontre de notre sens commun, prédit en effet que certains phénomènes physiques sont parfaitement aléatoires, et donc totalement imprévisibles. Contrairement à ses prédécesseurs, ce nouveau système permet à l'utilisateur de contrôler en permanence la fiabilité des nombres aléatoires qui en résultent. Cette recherche, à découvrir dans la revue *Physical Review Applied*, va singulièrement compliquer la tâche des espions, qui ne pourront plus tabler sur les biais insérés par l'intelligence humaine ou d'éventuelles défaillances des machines actuelles.



En utilisant les propriétés quantiques de la lumières, les chercheurs génèrent des nombres parfaitement aléatoires.

Pour générer une bonne clé de cryptage, il faut alterner de manière aléatoire des 0 et des 1, dits bits, à savoir l'unité d'information qui sert de base à l'ordinateur. Toutefois, lorsque l'intelligence humaine génère une succession de nombres qu'elle pense aléatoire, une part reste malgré tout prédictible grâce aux études de comportement et surtout aux statistiques. En plus de cette mauvaise perception de l'aléatoire, le cerveau humain est bien plus lent qu'une machine capable de générer des millions de nombres à la seconde. Ceci ouvre la voie aux espions, qui ont la possibilité de craquer des mots de passe que l'on penserait inviolables.

La physique quantique comme clé de sûreté

Depuis vingt ans, les chercheurs se sont tournés vers la physique quantique, caractérisée par ses processus totalement aléatoires et imprévisibles, pour développer de nouvelles techniques de cryptage, et en particulier la génération de nombres aléatoires. «Il s'agit d'envoyer un photon (une particule de lumière) sur un miroir semi-transparent. Soit il passe au travers, soit il est réfléchi. Mais il est en principe impossible de prévoir quel cas de figure va se produire. C'est cette idée de base qui sert aux générateurs quantiques», explique Nicolas Brunner, professeur au Département de Physique Appliquée de la Faculté de sciences de l'UNIGE et responsable de l'aspect théorique de la

recherche. Ces générateurs quantiques performants sont aujourd'hui commercialisés. Toutefois, une limitation du système actuel est que l'utilisateur est dans l'impossibilité de vérifier que l'appareil génère bien des nombres aléatoires et non pas une séquence prédictible, composée par exemple des décimales de π. L'utilisateur doit donc se fier à l'appareil (et à son fabriquant) et supposer qu'il fonctionne correctement, ceci même après plusieurs années d'utilisation. Il est donc légitime de se demander si le système peut être améliorer de ce point de vue.

Un nouveau générateur de nombres aléatoires self-testing

«Nous voulions créer un appareil qui pourrait se tester en permanence afin d'assurer son bon fonctionnement au cours du temps et garantir la fiabilité des nombres aléatoires», précise Nicolas Brunner. Les physiciens de l'UNIGE ont ainsi mis au point un générateur quantique de nombres aléatoires «self–testing», dont l'utilisateur peut vérifier en temps réel qu'il fonctionne de manière optimale et délivre toujours des nombres aléatoires. «Le générateur doit résoudre un problème pour lequel nous l'avons calibré. S'il le résout de manière correcte, les nombres sont véritablement aléatoires. Si l'appareil ne trouve pas la bonne solution, le caractère aléatoire n'est plus assuré et l'utilisateur doit donc recalibrer son appareil. Ceci évite l'utilisation de nombres peu (ou pas) aléatoires pour générer par exemple des mots de passe qu'un espion pourrait par la suite craquer», s'enthousiasme le professeur Hugo Zbinden, responsable du volet expérimental de l'étude. L'appareil permet en effet de quantifier avec précision la qualité de nombres aléatoires générés. Ceux-ci seront ensuite distillés et utilisés pour des applications, comme par exemple la création de mots de passe indéchiffrables par des espions.

Ce générateur quantique de nombres aléatoires self-testing permettra d'augmenter encore d'un cran la sûreté des mots de passe et outils de cryptage actuels. Ici, la sécurité est garantie par les seules lois de la physique quantique, et non pas par des limitations technologiques de l'espion. Cette recherche, menée par les physiciens de l'UNIGE, permet de mieux comprendre l'aléa quantique, ainsi que son utilisation pour des applications dans les technologies de l'information.

contact

Nicolas Brunner
+41 22 379 43 68
Nicolas.Brunner@unige.ch

Hugo Zbinden
+41 22 379 05 04
Hugo.Zbinden@unige.ch

UNIVERSITÉ DE GENÈVE
Service de communication
24 rue du Général-Dufour
CH-1211 Genève 4

Tél. +41 22 379 77 17

media@unige.ch
www.unige.ch