Forum

Stephan Wolf

Was nützen uns Quantengesetze? A quoi les lois quantiques peuvent-elles servir?

In der Mittagshitze eines sonnigen Tages der 1980er-Jahre treffen sich zwei Fremde beim Bad vor Puerto Rico, und der Ältere der beiden richtet sich an den Bärtigen mit einer eher ungewöhnlichen Frage: «Did you know that using Quantum Physics, you can make banknotes impossible to counterfeit?» («Wussten Sie, dass die Quantenmechanik, geschickt eingesetzt, es erlaubt, fälschungssichere Banknoten herzustellen?») Wohl zu seiner eigenen Überraschung stiess Charles Bennetts Frage auf grösstes Interesse bei Gilles Brassard, und die beiden entdeckten bald darauf, dass eine ähnliche Idee es auch möglich macht, Geheimnachrichten mit bisher unerreichter Sicherheit auszutauschen: Das war die Geburtsstunde der Quantenkryptografie.

Es muss purer Zufall sein, dass die «Quanten» den Kryptologen noch ein zweites Mal gehörig dreinfunken; diesmal, weil ein Rechenautomat, der quantenmechanische Effekte geschickt ausnützt, gängige Verschlüsselungsverfahren wie RSA völlig unsicher macht.

Während Geräte für Quantenverschlüsselung bereits auf dem Markt erhältlich sind, lässt die Realisierung von solchen Quantencomputern noch auf sich warten. Ob das eines Tages geschieht oder nicht, steht in den Sternen. Klar ist indes, dass die immer deutlicher werdende Verquickung von Information und Physik es uns erlaubt, in beiden Gebieten neue Fragen zu stellen und faszinierende Einsichten zu gewinnen. Wie passt es zum Beispiel in unser Weltbild, dass voneinander getrennte Photonen in ihrem Verhalten eine Korrelation zeigen, die eigentlich nur mit Kommunikation erklärbar wäre, ohne dass die Teilchen aber tatsächlich Information austauschen können? Können wir auch diese «Nichtlokalität» in der Informationsverarbeitung benützen, beispielsweise für sicherere Verschlüsselung oder effizientere Kommunikation?

Sous le soleil de midi d'une chaude journée des années 1980, deux hommes qui ne se connaissent pas se rencontrent durant une baignade devant Porto Rico, et le plus âgé des deux pose au barbu une question plutôt insolite: «Did you know that using Quantum Physics, you can make banknotes impossible to counterfeit?» («Saviez-vous que la mécanique des quanta, utilisée correctement, permet de fabriquer des billets de banque à l'épreuve de toute contrefaçon?») Charles Bennetts fut lui-même surpris de constater que sa question intéressait vivement Gilles Brassard, et tous deux s'aperçurent bientôt qu'une idée de ce genre permettrait aussi d'échanger des données avec une sécurité encore jamais atteinte: la cryptographie quantique était née.

Ce ne peut être qu'un hasard si les «quanta» ont encore une fois joué un tour aux cryptologues; cette fois-ci parce qu'un calculateur automatique exploite habilement la mécanique quantique pour désécuriser totalement les méthodes cryptologiques courantes comme RSA.

Tandis qu'il y a déjà dans le commerce des appareils de cryptographie quantique, la réalisation de tels ordinateurs quantiques se fait encore attendre. Et l'on ne saurait dire s'ils apparaîtront un jour ou pas. Une chose est cependant claire: l'amalgamation de plus en plus évidente de l'information et de la physique nous permet de poser de nouvelles questions dans les deux domaines et de faire de fascinantes découvertes. Comment concevoir par exemple que des photons séparés les uns des autres puissent présenter dans leur comportement une corrélation qui ne pourrait s'expliquer que par la communication, mais ceci sans que les particules puissent effectivement échanger l'information? Pouvons-nous exploiter ce caractère «antilocal» dans le traitement de l'information, en vue, par exemple, d'une cryptographique plus sûre ou d'une communication plus efficace?

Stephan Wolf ist Professor am Departement für Informatik der ETH Zürich
Stephan Wolf est professeur au département d'informatique de l'EPF Zurich