Zeitschrift: Tracés : bulletin technique de la Suisse romande
Herausgeber: Société suisse des ingénieurs et des architectes
Band: 130 (2004)
Heft: 13: Ordinateur quantique

Artikel: La cryptographie quantique entre dans le commerce
Autor: Poritz, Jonathan / Hohler, Anna
DOI: https://doi.org/10.5169/seals-99324

Jonathan Poritz
Propos recueillis par Anna Hohler

La **cryptographie quantique** entre dans le commerce

Partenaire industriel des deux pôles de recherche nationaux qui touchent à l'informatique quantique (voir ci-contre), *IBM* s'intéresse aussi à la cryptographie, première branche du domaine qui a réussi son entrée dans le monde industriel et commercial. Car la cryptographie quantique sera à la base des technologies et des infrastructures de communication de demain (voir aussi pp. 20 à 22). Le laboratoire de recherche d'*IBM* de Zurich emploie plusieurs collaborateurs qui travaillent dans ce sens, dont Jonathan Poritz, professeur également à l'EPF de Zurich. Dans l'entretien téléphonique transcrit ci-dessous, réalisé sous le contrôle d'une responsable de la communication d'*IBM*, il apparaît en filigrane que les enjeux commerciaux de la cryptographie quantique sont considérables.

TRACÉS : Est-ce que IBM *a déjà lancé des produits utilisant la cryptographie quantique ?*

Jonathan Poritz : A ma connaissance, les seuls produits qui sont issus de la cryptographie quantique et qui se trouvent actuellement sur le marché sont ceux développés soit par *MagicQ Technologies*, à New York, soit par l'entreprise *id Quantique*, en collaboration avec Nicolas Gisin de l'Université de Genève. Ce sont des systèmes de cryptographie quantique basés sur des fibres optiques standard, des lasers et des détecteurs. En gros, on transmet des photons à l'aide d'un câble en fibre optique, ce qui permet d'échanger des clefs secrètes. *id Quantique* utilise le même principe que celui que nous sommes en train de développer dans notre centre de recherche d'Almaden, dans la Silicon Valley. Un groupe de chercheurs d'Almaden a d'ailleurs été parmi les premiers à démontrer l'aspect pratique des idées développées par C. H. Bennett et G. Brassard, qui ont inventé la cryptographie quantique[1]. C'est même étonnant qu'on ait déjà réussi à développer un produit dans ce domaine, qui est extrêmement complexe et délicat.

T. : Complexe mais, pour IBM, *d'une importance primordiale ?*

J. P. : C'est difficile à dire. Je crois que la cryptographie quantique joue un rôle important pour tous ceux qui travaillent dans le domaine de l'informatique. Pour l'instant, par exemple, personne ne sait construire un ordinateur quantique. On peut espérer que ce sera possible dans une dizaine d'années.

T. : Travaillez-vous également sur d'autres produits que celui cité ci-dessus ?

J. P. : Ici à Zurich, dans le domaine de la cryptographie quantique, nous nous consacrons à la recherche de base. Ce serait intéressant de réussir, dans l'avenir, à transmettre des photons à travers l'air, par exemple. Une expérience dans ce sens a été réalisée il y a un an environ, en Allemagne, je crois. Pour l'instant, les principales limites de la transmission de clefs secrètes sont la distance, et le fait d'avoir besoin du support d'un câble. Prenez une conversation téléphonique entre l'Europe et les Etats-Unis, par exemple : si à cause de la distance considérable les signaux à transmettre sont faibles, on arrive à les amplifier de manière artificielle. Ceci n'est pas réalisable dans le domaine quantique, et un câble trop long rend donc la transmission impossible.

T. : La cryptographie quantique entrera-t-elle dans notre vie quotidienne ? Peut-on imaginer par exemple des cartes bancaires qui fonctionneront selon ses lois ?

J. P. : C'est difficile à imaginer aujourd'hui, mais je suis plutôt optimiste. Ce sera probablement possible dans un avenir lointain, c'est-à-dire dans 20 à 25 ans. Pour l'instant, la recherche se concentre sur la transmission de clefs et les communications de haute sécurité.

Jonathan Poritz, Research Staff Member
IBM Zurich Research Laboratory
Säumerstrasse 4, CH - 8803 Rüschlikon

Propos recueillis par Anna Hohler

[1] Voir aussi p. 20