Version française ci-dessous – For French and German versions, see below

Press release

Vulnerability in commercial quantum cryptography tackled by international collaboration

August 29, 2010

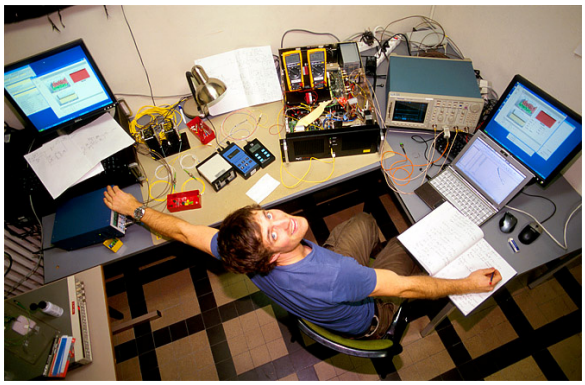
The Norwegian University of Science and Technology (NTNU) and the University of Erlangen-Nürnberg together with the Max Planck Institute for the Science of Light in Erlangen have recently developed and tested a technique exploiting imperfections in quantum cryptography systems to implement an attack. Countermeasures were also implemented within an ongoing collaboration with leading manufacturer ID Quantique.

Quantum cryptography is a technology that allows one to distribute a cryptographic key across an optical network and to exploit the laws of quantum physics to guarantee its secrecy. It makes use of the Heisenberg uncertainty principle – observation causes perturbation – to reveal eavesdropping on an optical fiber. The technology was invented in the mid-eighties, with first demonstration less than a decade later and the launch of commercial products during the first years of the century.

Although the security of quantum cryptography relies in principle only on the laws of quantum physics, it is also dependent on the lack of loopholes in specific implementations, just like any other security technology. “The security of quantum cryptography relies on quantum physics but not only… It must also be properly implemented. This fact was often overlooked in the past,” explains Prof. Gerd Leuchs of the University of Erlangen-Nürnberg and the Max Planck Institute for the Science of Light.

Recently, NTNU in collaboration with the team in Erlangen has found a technique to remotely control a key component of most of today’s quantum cryptography systems, the photon detector, which is reported today in Nature Photonics advance online publication doi:10.1038/nphoton.2010.214. “Unlike previously published attempts, this attack is implementable with current off-the-shelf components,” says Dr. Vadim Makarov, a researcher in the Quantum Hacking group at NTNU, who adds: “Our eavesdropping method worked both against MagiQ Technology's QPN 5505 and ID Quantique Clavis2 systems.”

In the framework of a collaboration initiated with ID Quantique, the researchers shared their results with the company prior to publication. ID Quantique has then, with a help of NTNU, developed and tested a countermeasure. Academic researchers of the two laboratories will continue testing security aspects of quantum cryptography solutions from ID Quantique. “Testing is a necessary step to validate a new security technology and the fact that this process is applied today to quantum cryptography is a sign of maturity for this technology,” explains Grégoire Ribordy, CEO of ID Quantique.



Hacking in progress:
A security researcher (PhD student Lars Lydersen) is testing a commercial quantum cryptography system in a laboratory, to confirm the security vulnerability.

For more pictures of experiments and equipment, visit
www.iet.ntnu.no/groups/optics/qcr/hacking-commercial-quantum-cryptography-2010/

About the Quantum Hacking group

The Quantum Hacking group at the Department of Electronics and Telecommunications, Norwegian University of Science and Technology, works in the field of quantum cryptography, with the main goal to make quantum cryptosystems secure in practice. This is done by playing the role of the evil eavesdropper, and hacking practical systems by exploiting imperfections. Using these results, we propose modifications to the systems and new security proofs which take imperfections into account.

About the QIV group

The Quantum Information Processing group in Erlangen represents a close collaboration in the field of quantum communication between the University of Erlangen-Nürnberg and the Max Planck Institute for the Science of Light. One of the group's research focuses is research in quantum key distribution and operating a free-space link transmitting continuous-variables quantum information.

About ID Quantique

ID Quantique is a global leader shaping the evolution of network security through the development and commercialization of Quantum Key Distribution and high-speed encryption products. In 2001, the company was the first to bring this new technology to the market. In 2007, it was able to announce the first public application of this technology to secure a network used for vote counting in an election in Geneva. In addition to its strong technology focus on Quantum Key Distribution, ID Quantique has also developed expertise in the area of high-speed encryption and has a broad portofolio of solutions for layer 2 encryption. A privately held company headquartered in Geneva, Switzerland, ID Quantique is a spin-off from the University of Geneva and has close ties with leading academic institutions.

For further information, contact:

Vadim Makarov, postdoctoral researcher, Department of Electronics and Telecommunications, Norwegian University of Science and Technology
Email: makarov@vad1.com, tel. +47 73592733, mobile: +47 46795898
Quantum Hacking group: www.iet.ntnu.no/groups/optics/qcr/

Christoffer Wittmann, Max Planck Institute for the Science of Light,
Günther-Scharowsky-Str. 1/Bau 24, 91058 Erlangen, Germany
Email: christoffer.wittmann@mpl.mpg.de, tel. +49 9131 6877129
QIV-group: mpl.mpg.de/mpf/php/abteilung1/index.php?lang=en

Grégoire Ribordy, CEO, ID Quantique SA
Tel. +41 22 301 83 71, Mobile: +41 79 784 70 79
Email: gregoire.ribordy@idquantique.com www.idquantique.com

Communiqué de presse

Une collaboration internationale permet de déjouer une vulnérabilité dans un système de cryptographie quantique

Genève, le 30 août 2010 – **L'Université de Science et Technologie (NTNU) de Trondheim en Norvège et celle d'Erlangen-Nuremberg en Allemagne, en collaboration avec le Max Planck Institute for the Science of Light d'Erlangen, ont récemment développé et testé une technique exploitant les imperfections des systèmes pratiques de cryptographie quantique, dans le but d'implémenter une attaque. Une collaboration avec la société genevoise ID Quantique SA, leader mondial de ce marché, a permis de mettre en place les contre-mesures.**

La technologie de cryptographie quantique permet de distribuer une clé de chiffrement au travers d'un réseau optique. Elle utilise le principe d'incertitude d'Heisenberg – toute observation cause la perturbation – pour révéler la présence d'un espion sur la ligne. Bien que garantie par les lois de la physique quantique, sa sécurité dépend aussi - et tout comme l'ensemble des technologies de sécurité - d'une absence de faille dans l'implémentation pratique. « *Fait qui a souvent été négligé par le passé* », affirme le professeur Gerd Leuchs de l'Université d'Erlangen-Nuremberg et de l'Institut Max Planck.

La NTNU, en collaboration avec l'équipe d'Erlangen, a récemment découvert une technique permettant de contrôler un composant clé - le compteur de photons - présent dans la plupart des systèmes de cryptographie quantique actuels. Cette découverte a été rapportée hier dans un article publié sur le site Nature Photonics (www.nature.com/nphoton). « *Contrairement aux autres attaques présentées jusqu'à maintenant, celle-ci peut être réalisée avec des composants standard* » explique le Dr. Vadim Makarov, chercheur au sein du groupe de Hacking Quantique de la NTNU. Le Dr. Makarov ajoute « *Notre approche fonctionne tant contre le système QPN 5505 de MagiQ Technologies que le Clavis2 d'ID Quantique* ».

Dans le cadre d'une collaboration avec ID Quantique, les chercheurs ont partagé leurs résultats avec l'entreprise genevoise avant leur publication. ID Quantique a ainsi pu développer et tester, avec l'assistance des chercheurs de la NTNU, une contre-mesure permettant de neutraliser cette attaque. Les chercheurs des deux laboratoires continueront désormais à tester la sécurité des solutions de cryptographie quantique d'ID Quantique. « *Des phases de tests sont évidemment nécessaires pour valider une nouvelle technologie de sécurité et le fait que ce processus soit aujourd'hui aussi appliqué à la cryptographie quantique est un signe de maturité pour cette technologie* » conclut Grégoire Ribordy, directeur d'ID Quantique.

A propos du Groupe de Hacking Quantique, Trondheim

Le Groupe de Hacking Quantique du département d'électronique et télécommunications de l'Université de Science et Technologie à Trondheim en Norvège est actif dans le domaine de la cryptographie quantique. Son principal but consiste à rendre les systèmes de cryptographie quantique fiables dans la pratique. Il agit en jouant le rôle d'un adversaire tentant d'exploiter les imperfections expérimentales présentes dans les systèmes. En fonction des résultats, le groupe propose aussi des améliorations des systèmes qui tiennent compte des imperfections découvertes.

A propos du Groupe de Traitement Quantique de l'Information, Erlangen

Le Groupe de Traitement Quantique de l'Information d'Erlangen en Allemagne réunit des chercheurs de l'Université d'Erlangen-Nuremberg et du Max Planck Institute for the Science of Light, actifs dans le domaine des communications quantiques. Le groupe étudie entre autres la cryptographie quantique et a développé un système d'échange de clés aérien utilisant une approche par variables continues.

A propos d'ID Quantique SA

Spécialisée dans la cryptographie quantique et le chiffrement conventionnel, ID Quantique commercialise ses produits et services de sécurité de l'information en Suisse et en Europe. Elle est présente sur le marché mondial dans les domaines de l'instrumentation scientifique (instruments de mesure pour les laboratoires de recherche académiques et industriels) et des générateurs de nombres aléatoires. Ses produits de chiffrement sont dotés d'une certification indépendante selon les Critères Communs de niveau EAL4+ qui reste également valable lorsque l'on y intègre la technologie de distribution quantique de clé. Lauréate du prix de la Jeune Industrie 2009 décerné par l'OPI (Office de Promotion des Industries et Technologies à Genève), ID Quantique participe à de nombreux projets d'innovation technologique, tel SwissQuantum de l'Université de Genève, initié en mars 2009, où elle y joue un rôle central avec le déploiement en environnement réel d'un réseau pilote de cryptographie quantique. Fondée en 2001, la société est établie à Genève et compte quatorze collaborateurs.

Lien vers l'article complet :
http://dx.doi.org/10.1038/nphoton.2010.214

Informations complémentaires :

ID Quantique SA
Grégoire Ribordy - CEO d'ID Quantique SA
gregoire.ribordy@idquantique.com
Mobile 079 784 70 79
www.idquantique.com

Agence de relations publiques
Chantal Béhar, Visinand Communications
c.behar@visinandcom.ch
Tél. 021 312 75 05

Pour obtenir plus d'informations sur l'attaque, ainsi que des illustrations et photographies de l'expérience en laboratoire :

Vadim Makarov, chercheur postdoctorant,
Université de Science et Technologie de Trondheim**,**
Département d'électronique et télécommunications,
Email: makarov@vad1.com,
Tel. +47 73592733
Mobile: +47 46795898
Groupe de Hacking Quantique : www.iet.ntnu.no/groups/optics/qcr/

Christoffer Wittmann,
Max Planck Institute for the Science of Light,
Günther-Scharowsky-Str. 1/Bau 24, 91058 Erlangen, Germany
Email: christoffer.wittmann@mpl.mpg.de,
Tel. +49 9131 6877129
QIV-group: mpl.mpg.de/mpf/php/abteilung1/index.php?lang=en

Deutsche Version (German version)

Pressemitteilung

Internationales Forscherteam behebt Sicherheitslücke in kommerzieller Quantenkryptographie

29. August 2010

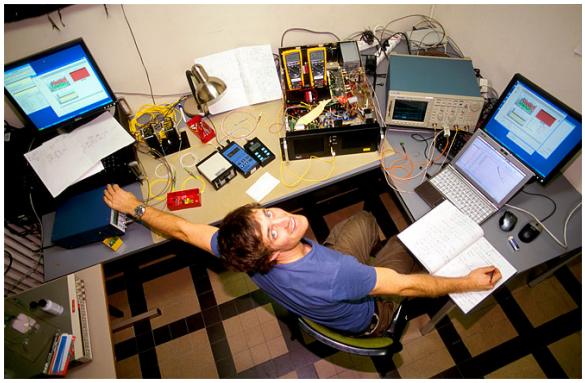
Die Universitäten Trondheim und Erlangen-Nürnberg haben zusammen mit dem Max-Planck-Institut für die Physik des Lichts eine Angriffsmethode gegen Quantenkryptographiesysteme entwickelt. Die Forscher konnten nachweisen, dass solche Systeme derzeit noch technische Unzulänglichkeiten aufweisen, die Abhörer ausnutzen könnten. Im Rahmen einer Kooperation mit dem führenden Hersteller ID Quantique wurden bereits Gegenmaßnahmen entwickelt.

Durch Quantenkryptographie kann eine Schlüsselsequenz über ein optisches Netzwerk verteilt werden. Dabei sorgen physikalische Gesetze für bisher unerreichte Geheimhaltung des Schlüssels. Unter Ausnutzung der Heisenbergschen Unschärferelation (eine Beobachtung erzeugt eine Störung) wird jeder Abhörer im optischen Kanal entdeckt. Die Prinzipien dieser Technologie wurden Mitte der achtziger Jahre erfunden, und bald darauf in ersten Versuchsaufbauten überprüft. Die Entwicklung ging soweit, dass kommerzielle Produkte nach der Jahrtausendwende eingeführt wurden.

In der Theorie ist die Sicherheit der Quantenkryptographie unumstößlich, da sie auf allgemeingültigen physikalischen Gesetzen beruht. Allerdings weichen Geräte in der Praxis oft vom theoretischen Modell ab, wodurch Sicherheitslücken entstehen können. Diese Sicherheitslücken zu identifizieren und zu beheben werden ist eine notwendige Vorgehensweise bei jeder neuen Verschlüsselungsmethode. „Die Sicherheit der Quantenkryptographie basiert an sich auf physikalischen Gesetzen … aber nicht ausschließlich. Die technische Umsetzung spielt auch eine wichtige Rolle, was in der Vergangenheit oft übersehen wurde“, erklärt Prof. Gerd Leuchs von der Universität Erlangen-Nürnberg, der geschäftsführender Direktor des Max-Planck-Instituts für die Physik des Lichts ist.

Die Forscher der Universitäten Trondheim und Erlangen haben jetzt eine Technik entwickelt, die es Abhörern ermöglicht, eine entscheidende Komponente der meisten derzeitigen Quantengeräte zu manipulieren: den Photodetektor. Eine Veröffentlichung dazu erscheint heute in der Fachzeitschrift *Nature Photonics*. “Im Gegensatz zu Arbeiten anderer Gruppen setzen wir diese Attacke mit serienmäßig produzierten Geräten um”, erläutert Dr. Vadim Makarov, Wissenschaftler in der Quanten-Hacking-Gruppe in Trondheim, und fügt hinzu: “Unsere Abhörmethode funktioniert sowohl gegen das Gerät QPN 5505 von MagiQ Technologies, als auch gegen ID Quantiques Clavis2-System.“

Im Rahmen einer Zusammenarbeit mit ID Quantique teilten die Wissenschaftler dem Unternehmen ihre Ergebnisse vor deren Veröffentlichung mit. ID Quantique hat daraufhin mit Hilfe der Norweger Forscher eine Gegenmaßnahme entwickelt und getestet. Wissenschaftler aller drei Labore werden auch weiterhin Sicherheitsaspekte verschiedener Quantenkryptographiesysteme von ID Quantique überprüfen. „Ab einem gewissen Entwicklungsgrad sind Tests ein notwendiger Schritt bei der Überprüfung neuer Sicherheitstechnologien. Daran, dass solche Tests mittlerweile in der Quantenkryptographie durchgeführt werden, erkennt man deren hohe technologische Ausgereiftheit“, erklärt Grégoire Ribordy, Geschäftsführer von ID Quantique.



Einblick ins Labor:
Der Doktorand Lars Lydersen untersucht gerade ein kommerzielles Quantenkryptographiesystem auf mögliche Sicherheitslücken.

Weitere Bilder des experimentellen Aufbaus und verwendeten Equipments finden Sie unter: www.iet.ntnu.no/groups/optics/qcr/hacking-commercial-quantum-cryptography-2010/

Über die Quanten-Hacking-Gruppe in Trondheim

Die Quanten-Hacking-Gruppe des Departments für Elektronik und Telekommunikation an der Norwegischen Universität für Wissenschaft und Technologie (NTNU) arbeitet im Bereich der Quantenkryptographie. Ihr Hauptziel ist es, praxistaugliche Quantenkryptographiesysteme mit höherer Sicherheit zu entwickeln. Die Forscher schlüpfen dabei in die Rolle eines böswilligen Abhörers, um existierende Systeme zu knacken. Dabei nutzen sie Modellabweichungen der Systeme aus. Als Abhilfe schlagen sie Änderungen und neue Sicherheitsbeweise vor, worin derartige Abweichungen berücksichtigt werden.

Über die QIV-Gruppe in Erlangen

Die QIV-Gruppe stellt eine enge Zusammenarbeit der Universität Erlangen-Nürnberg und des Max-Planck-Instituts für die Physik des Lichts dar. Die Gruppe beschäftigt sich mit vielfältigen Aspekten optischer Quanteninformationsverarbeitung. Unter anderem entwickeln die Forscher neue Methoden, um Quantenkommunikation immun gegenüber Störeinflüssen zu machen, so z.B. bei einer Freistrahlverbindung quer durch Erlangen.

Über ID Quantique in Genf

ID Quantique ist Weltmarkführer bei Quantenkryptographiesystemen in Verbindung mit Hochgeschwindigkeitsverschlüsselung. Das Unternehmen führte diese Technologie im Jahr 2001 ein. 2007 folgte der erste öffentliche Einsatz, wobei ein Netzwerk für die Stimmenzählung bei einer Wahl in Genf abgesichert wurde. Zusätzlich zur Quantenkryptographie hat ID Quantique Expertise im Bereich Hochgeschwindigkeitsverschlüsselung und bietet ein breites Spektrum an Layer-2-Verschlüsselung an. ID Quantique, das seinen Hauptsitz in Genf hat, ist ein Spin-Off der dortigen Universität, und pflegt Kontakte zu weltweit führenden Forschungsgruppen.

Weitere Informationen, Kontakt:

Die Veröffentlichung in der Fachzeitschrift *Nature Photonics* erscheint unter http://dx.doi.org/10.1038/nphoton.2010.214

Weitere Informationen über die Attacke, sowie Illustrationen und Bilder des Laborexperiments erhalten Sie von Dr. Makarov:

Vadim Makarov, Department of Electronics and Telecommunications, Norwegian University of Science and Technology (NTNU)
Email: makarov@vad1.com, Tel. +47 73592733, Mobil: +47 46795898
Quantum Hacking Group: www.iet.ntnu.no/groups/optics/qcr/

Christoffer Wittmann, Universität Erlangen-Nürnberg und Max-Planck-Institut für die Physik des Lichts, Günther-Scharowsky-Str. 1 / Bau 24, 91058 Erlangen
Email: christoffer.wittmann@mpl.mpg.de, Tel. +49 9131 6877129
QIV-Gruppe: mpl.mpg.de/mpf/php/abteilung1/index.php?lang=en

Grégoire Ribordy, Geschäftsführer von ID Quantique SA
Tel. +41 22 301 83 71, Mobil: +41 79 784 70 79
Email: gregoire.ribordy@idquantique.com www.idquantique.com