Press release

Making quantum cryptography truly secure: Researchers in Singapore and Norway implement a perfect eavesdropper that illustrates an overlooked loophole in secure communications technology.

(14 June 2011) Singapore and Trondheim, Norway: Quantum key distribution (QKD) is an advanced tool for secure computer-based interactions, providing confidential communication between two remote parties by enabling them to construct a shared secret key during the course of their conversation.

QKD is perfectly secure in principle, but researchers have long been aware that loopholes may arise when QKD is put into practice. Now, for the first time, a team of researchers at the Centre for Quantum Technologies (CQT) at the National University of Singapore, the Norwegian University of Science and Technology (NTNU) and the University Graduate Center (UNIK) in Norway have created and operated a "perfect eavesdropper" for QKD that exploits just such a loophole in a typical QKD setup. As reported in the most recent issue of Nature Communications, this eavesdropper enabled researchers to obtain an entire shared secret key without alerting either of the legitimate parties that there had been a security breach. The results highlight the importance of identifying imperfections in the implementation of QKD as a first step towards fixing them.

Cryptography has traditionally relied on mathematical conjectures and thus may always be prone to being "cracked" by a clever mathematician who can figure out how to efficiently solve a mathematical puzzle, aided by the continual development of ever-faster computers. Quantum cryptography, however, relies on the laws of physics and should be infinitely more difficult to crack than traditional approaches. While there has been much discussion of the technological vulnerabilities in quantum cryptography that might jeopardize this promise, there have been no successful full field-implemented hacks of QKD security – until now.

"Quantum key distribution has matured into a true competitor to classical key distribution. This attack highlights where we need to pay attention to ensure the security of this technology," says Christian Kurtsiefer, a professor at the Centre for Quantum Technologies at the National University of Singapore.

In the setup that was tested, researchers at the three institutions demonstrated their eavesdropping attack in realistic conditions over a 290-m fibre link between a transmitter called "Alice" and a receiver called "Bob". Alice transmits light to Bob one photon at a time, and the two build up their secret key by measuring properties of the photons. During multiple QKD sessions over a few hours, the perfect eavesdropper "Eve" obtained the same "secret" key as Bob, while the usual parameters monitored in the QKD exchange were not disturbed – meaning that Eve remained undetected.

The researchers were able to circumvent the quantum principles that in theory provide QKD its strong security by making the photon detectors in Bob behave in a classical way. The detectors were blinded, essentially overriding the system's ability to detect a breach of security. Furthermore, this technological imperfection in QKD security was breached using off-the-shelf components.

"This confirms that non-idealities in the physical implementations of QKD can be fully and practically exploitable, and must be given increased scrutiny if quantum cryptography is to become highly secure," says Vadim Makarov, a postdoctoral researcher at the University Graduate Center in Kjeller, Norway. "We can not simply delegate the burden of keeping a secret to the laws of quantum physics; we need to carefully investigate the specific devices involved," says Kurtsiefer.

The open publication of how the "perfect eavesdropper" was built has already enabled this particular loophole in QKD to be closed. "I am sure there are other problems that might show that a theoretical security analysis is not necessarily exactly the same as a real-world situation," says Ilja Gerhardt, currently a visiting scholar at the University of British Columbia in Vancouver, Canada. "But this is the usual game in cryptography – a secure communications system is created and others try to break into it. In the end this makes the different approaches better."

For further information, contact:

Dr. Vadim Makarov, postdoctoral researcher, University Graduate Center in Kjeller, Norway
Email: makarov@vad1.com, tel. +47 4679 5898, skype: vadim_makarov
Quantum Hacking group: www.iet.ntnu.no/groups/optics/qcr

Dr. Christian Kurtsiefer, professor, Centre for Quantum Technologies, National University of Singapore
Email: phyck@nus.edu.sg, tel. +65 6516 1250
Centre for Quantum Technologies: www.quantumlah.org

Qin Liu, PhD candidate, Department of Electronics and Telecommunications, Norwegian University of Science and Technology, Trondheim, Norway
Email: qin.liu@iet.ntnu.no, tel. +47 4621 1297

Dr. Ilja Gerhardt, visiting scholar, University of British Columbia, Vancouver, Canada
Email: ilja@quantumlah.org, tel: +1 604 822 5265

Journal reference: Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," Nature Communications **2**, 349 (2011). Article is available at http://dx.doi.org/10.1038/ncomms1348

A free preprint is available at http://arxiv.org/abs/1011.0105

Quantum Hacking group
The Quantum Hacking group at the 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, the group proposes modifications to the systems and new security proofs which take imperfections into account. Learn more at www.iet.ntnu.no/groups/optics/qcr

Norwegian University of Science and Technology
The Norwegian University of Science and Technology (NTNU) is Norway's primary institution for educating the nation's future engineers and scientists. The university also has strong programmes in the social sciences, teacher education, the arts and humanities, medicine, architecture and fine art. NTNU's cross-disciplinary research delivers creative innovations that have far-reaching social and economic impact. Learn more at www.ntnu.edu

National University of Singapore
A leading global university centred in Asia, the National University of Singapore (NUS) offers a global approach to education and research, with a focus on Asian perspectives and expertise. The University has 15 faculties and schools, with over 36,000 students from about 100 countries. NUS has three Research Centres of Excellence (RCE), 22 university-level research institutes and centres, and it is also a partner for Singapore's 5th RCE. The University is well known for its research strengths in engineering, life sciences, medicine, social sciences and natural sciences. More at www.nus.edu.sg

Centre for Quantum Technologies at the National University of Singapore
The Centre for Quantum Technologies (CQT) was established as Singapore's inaugural Research Centre of Excellence in December 2007. It brings together quantum physicists and computer scientists to explore the quantum nature of reality and quantum possibilities in information processing. CQT is funded by Singapore's National Research Foundation and Ministry of Education and is hosted by the National University of Singapore (NUS). The CQT's Quantum Optics group has developed a complete quantum key distribution system based on entangled photon pairs, which has resulted in a few firsts in the field, including providing complete open source information for the hard- and software involved in this research. More at www.quantumlah.org

University Graduate Center in Kjeller, Norway
The University Graduate Center in Kjeller (UNIK) educates master's and PhD candidates in selected technological subjects. UNIK students are usually enrolled at the University of Oslo or NTNU, but other students are also welcome. UNIK was founded in 1987 and collaborates with special and highly qualified research communities in the Kjeller area.

Hacker's suitcase:
Mobile toolkit for eavesdropping on a quantum cryptography link, containing optical and electronic equipment.

Researchers at work:
Dr. Ilja Gerhardt, Prof. Antía Lamas-Linares and Prof. Christian Kurtsiefer set up quantum cryptography system.

For more pictures of experiments and equipment, please visit
http://www.iet.ntnu.no/groups/optics/qcr/full-eavesdropping-2011/

Pressemelding

Sikker kvantekryptografi: Forskere i Norge og Singapore oppretter en perfekt eavesdropper, avlytter, for å vise et sikkerhetshull som til nå har vært oversett i sikker kommunikasjonsteknologi.

(14. juni 2011) Trondheim og Singapore:

Quantum key distribution (QKD) er et avansert verktøy for sikker databasert samhandling der to eksterne parter kan lage en felles hemmelig nøkkel i løpet av samtalen slik at de kan holde kommunikasjonen trygg.

QKD er i prinsippet helt sikkert, men forskerne har lenge vært klar over at i praksis kan det likevel oppstå sikkerhetshull. For første gang har forskere ved Norges teknisk-naturvitenskapelige universitet (NTNU), Universitetssenteret på Kjeller (UNIK) og National University of Singapore laget og styrt en «perfekt eavesdropper» for QKD som utnytter sikkerhetshull i et typisk QKD-oppsett.

Nature Communications skrev i siste utgave at eavesdropperen lot forskerne skaffe seg en felles hemmelig nøkkel uten å varsle noen av dem om at det hadde vært et sikkerhetsbrudd. Resultatene viser hvor viktig det er å identifisere feil når QKD blir etablert slik at feilene kan bli rettet opp.

Kryptografi er tradisjonelt basert på matematiske beregninger. Kryptografi er derfor alltid utsatt for å bli knekket av en smart matematiker som godt hjulpet av stadig raskere datamaskiner kan løse en matematisk gåte.

Kvantekryptografi hviler derimot på fysikkens lover og er derfor uendelig mye vanskeligere å knekke enn ved tradisjonelle tilnærminger. Selv om denne sannheten er utfordret i mye diskusjon om teknologisk sårbarhet i kvantekryptografi, har det til nå ikke vært mulig med fullstendig hacking av sikkerheten i QKD.

– Quantum key distribution har modnet og blitt en konkurrent til klassisk nøkkeldistribusjon. Dette angrepet markerer nå hva vi må rette oppmerksomheten mot fremover for å garantere sikkerheten for denne type teknologi, sier Christian Kurtsiefer, professor ved Centre for Quantum Technologies (CQT), National University of Singapore.

Forskerne ved de tre institusjonene har testet avlyttingsangrep under realistiske betingelser over en 290-m fiberlink mellom en sender kalt «Alice» og en mottaker kalt «Bob». Alice sender lys til Bob, ett og ett foton av gangen. Alice og Bob lager så en hemmelig nøkkel ved å måle egenskapene ved fotonene. I løpet av mange QKD-økter over noen timer, fikk den perfekte eavesdropperen kalt «Eve» samme hemmelige nøkkel som Bob. De vanlige parametrene som overvåkes i QKD-utvekslingen ble ikke forstyrret og det betyr at Eve ikke ble oppdaget.

Fordi forskerne fikk fotonene i Bob til å oppføre seg som i klassisk fysikk, kunne de dermed villede kvanteprinsipper som i teorien gir QKD den sterke sikkerheten. Detektorene var blendet, og overstyrte hovedsakelig systemets evne til å avdekke brudd på sikkerheten. Avlytteren var dessuten bygget av standardkomponenter som er lett tilgjengelig og enkelt kan kjøpes.

– Ikke-idealet i fysisk bruk av QKD kan dermed være fullt og praktisk mulig å utnytte. For å få garantert sikker kvantekryptografi, må imidlertid dette granskes ytterligere, sier Vadim Makarv, post doktor ved Universitetssenteret på Kjeller.

– Vi kan ikke enkelt overdra forpliktelsen med å holde på en hemmelighet om kvantefysikkens lover. De enkelte komponentene som er involvert må undersøkes nøye, sier Kurtsiefer.

Publiseringen av hvordan den perfekte eavesdropper ble laget har allerede ført til at det spesielle sikkerhetshullet i QKD er stengt.

– Jeg er sikker på at det er andre problemer som kan vise at teoretisk sikkerhetsanalyse ikke nødvendigvis er det samme som en virkelig situasjon. Det vanlige spillet i kryptografi er at noen lager et sikkert kommunikasjonssystem og at noen andre prøver å bryte seg inn i det. Resultatet er at metodene for å gjøre det sikkert blir bedre, sier Ilja Gerhardt, gjesteforsker ved University of British Columbia i Vancouver.

Kontakt

Qin Liu, stipendiat
Institutt for elektronikk og telekommunikasjon,
Norges teknisk-naturvitenskapelige universitet, Trondheim, Norge
Epost: qin.liu@iet.ntnu.no, mobil +47 462 11 297

Vadim Makarov, post doktor
Universitetssenteret på Kjeller, Kjeller, Norge
Email: makarov@vad1.com, mobil +47 467 95 898, skype: vadim_makarov
Quantum Hacking group: www.iet.ntnu.no/groups/optics/qcr

Christian Kurtsiefer, professor
Centre for Quantum Technologies, National University of Singapore
Email: phyck@nus.edu.sg, telefon +65 6516 1250
Centre for Quantum Technologies: www.quantumlah.org

Ilja Gerhardt, gjesteforsker
University of British Columbia, Vancouver, Canada
Email: ilja@quantumlah.org, telefon +1 604 822 5265

Artikkel

Qin Liu og Johannes Skaar (NTNU), Vadim Makarov (Universitetssenteret på Kjeller), Ilja Gerhardt (University of British Columbia), Antía Lamas-Linares og Christian Kurtsiefer (National University of Singapore):

«Full-field implementation of a perfect eavesdropper on a quantum cryptography system», Nature Communications **2**, 349 (2011):

http://dx.doi.org/10.1038/ncomms1348