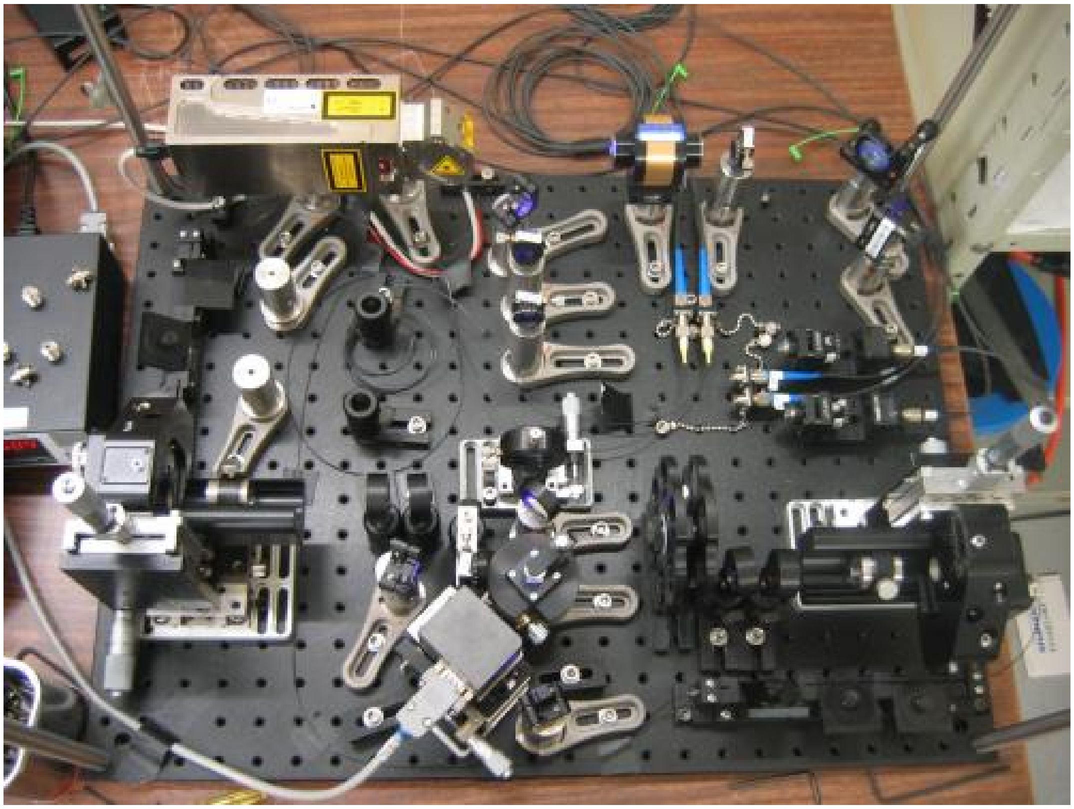
Quantum physics secures new cryptography scheme

March 12 2014



The experiment's Alice and Bob communicated with entangled photons produced in this setup. Such apparatus could be miniaturized using techniques from integrated optics. Credit: IQC, University of Waterloo

The way we secure digital transactions could soon change. An international team has demonstrated a form of quantum cryptography that can protect people doing business with others they may not know or trust – a situation encountered often on the internet and in everyday life, for example at a bank's ATM.

"Having quantum cryptography to hand is a realistic prospect, I think. I expect that quantum technologies will gradually become integrated with existing devices such as smartphones, allowing us to do things like identify ourselves securely or generate encryption keys," says Stephanie Wehner, a Principal Investigator at the Centre for Quantum Technologies (CQT) at the National University of Singapore, and co-author on the paper.

In cryptography, the problem of providing a secure way for two mutually distrustful parties to interact is known as 'two-party secure computation'. The new work, published in *Nature Communications*, describes the implementation using quantum technology of an important building block for such schemes.

CQT theorists Wehner and Nelly Ng teamed up with researchers at the Institute for Quantum Computing (IQC) at the University of Waterloo, Canada, for the demonstration.

"Research partnerships such as this one between IQC and CQT are critical in moving the field forward," says Raymond Laflamme, Executive Director at the Institute for Quantum Computing. "The infrastructure that we've built here at IQC is enabling exciting progress on quantum technologies."

"CQT and IQC are two of the world's largest, leading research centres in quantum technologies. Great things can happen when we combine our powers," says Artur Ekert, Director of CQT.

In the future, quantum cryptography might secure transactions such as identification at ATMs. (This is an artist's impression.) Researchers have demonstrated a proof-of-principle protocol known as 1-2 random oblivious transfer. Credit: CQT, National University of Singapore

The experiments performed at IQC deployed quantum-entangled photons in such a way that one party, dubbed Alice, could share information with a second party, dubbed Bob, while meeting stringent restrictions. Specifically, Alice has two sets of information. Bob requests access to one or the other, and Alice must be able to send it to him without knowing which set he's asked for. Bob must also learn nothing about the unrequested set. This is a protocol known as 1-2 random oblivious transfer (ROT).

ROT is a starting point for more complicated schemes that have applications, for example, in secure identification. "Oblivious transfer is a basic building block that you can stack together, like lego, to make something more fantastic," says Wehner.

Today, taking money out of an ATM requires that you put in a card and type in your PIN. You trust the bank's machine with your personal data. But what if you don't trust the machine? You might instead type your PIN into your trusted phone, then let your phone do secure quantum identification with the ATM (see artist's impression). Ultimately, the aim is to implement a scheme that can check if your account number and PIN matches the bank's records without either you or the bank having to disclose the login details to each other.

Unlike protocols for ROT that use only classical physics, the security of the quantum protocol cannot be broken by computational power. Even if the attacker had a quantum computer, the protocol would remain secure.

Its security depends only on Alice and Bob not being able to store much quantum information for long. This is a reasonable physical assumption, given today's best quantum memories are able to store information for minutes at most. Moreover, any improvements in memory can be matched by changes in the protocol: a bigger storage device simply means more signals have to be sent in order to achieve security. (The idea of 'noisy storage' securing quantum cryptography was developed by Wehner in earlier papers.)

To start the ROT protocol, Alice creates pairs of entangled photons. She measures one of each pair and sends the other to Bob to measure. Bob chooses which photons he wants to learn about, dividing his data accordingly without revealing his picks to Alice. Both then wait for a length of time chosen such that any attempt to store quantum information about the photons is likely to fail. To complete the oblivious transfer, Alice then tells Bob which measurements she made, and they both process their data in set ways that ensure the result is correct and secure within a pre-agreed margin of error.

In the demonstration performed at IQC, Alice and Bob achieved a random oblivious transfer of 1,366 bits. The whole process took about three minutes.

The experiment adapted devices built to do a more standard form of quantum cryptography known as quantum key distribution (QKD), a scheme that generates random numbers for scrambling communication. Devices for QKD are already commercially available, and miniaturised versions of this experiment are in principle possible using integrated optics. In the future, people might carry hand-held quantum devices that can perform this kind of feat.

"We did the experiment with big and bulky optics taking metres of space, but you can well imagine this technology being shrunk down to sit happily next to classical processing circuits on a small little microchip. The field of integrated quantum optics has been progressing in leaps and bounds, and most of the key pieces required to implement ROT have already been successfully demonstrated in integrated setups a few millimetres in size," says Chris Erven, who performed the experiments at IQC as a PhD student under the supervision of Raymond Laflamme and Gregor Weihs. Weihs is now at the University of Innsbruck, Austria. Erven is now a postdoctoral fellow at the University of Bristol, UK.

More information: "An Experimental Implementation of Oblivious Transfer in the Noisy Storage Model", *Nature Communications* DOI: 10.1038/ncomms4418 (2014) A preprint is available at arxiv.org/abs/1308.5098

Provided by National University of Singapore

Citation: Quantum physics secures new cryptography scheme (2014, March 12) retrieved 23 April 2024 from https://phys.org/news/2014-03-quantum-physics-cryptography-scheme.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.