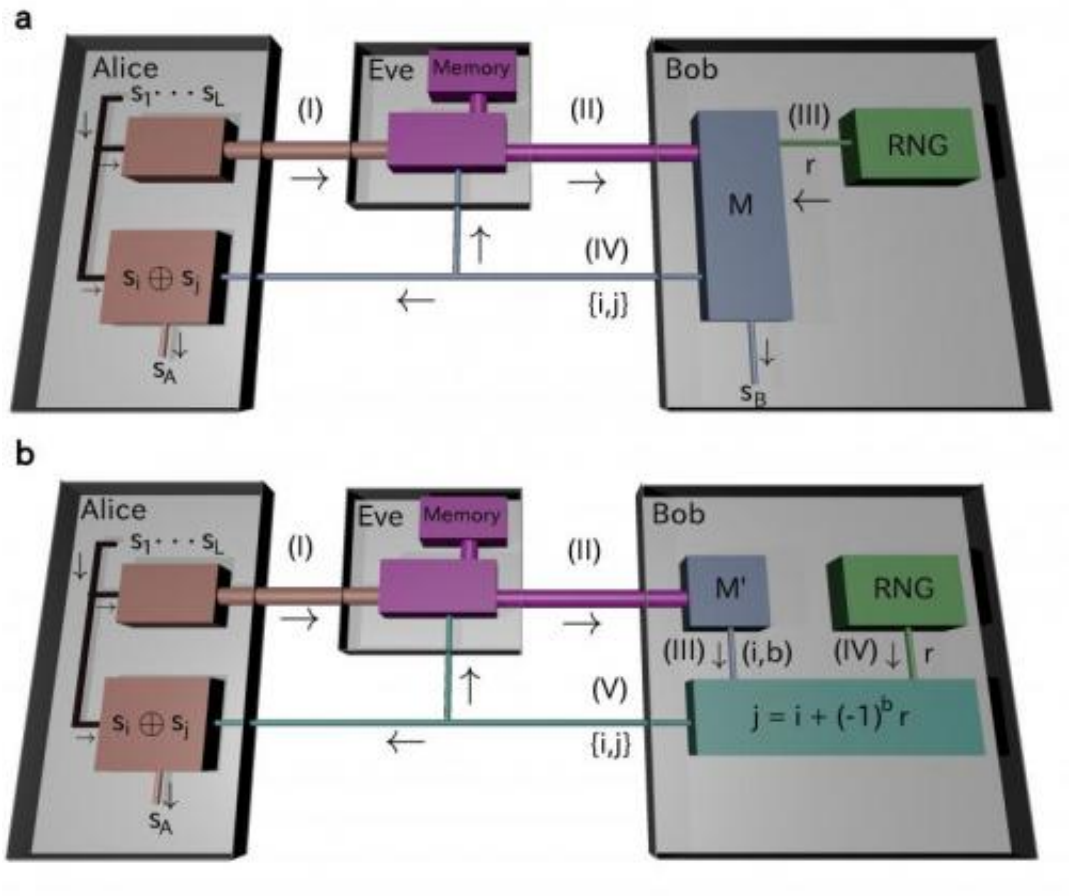
Eavesdroppers begone: New quantum key distribution technique is impervious to noise

June 11 2014, by Stuart Mason Dambrot



Principle behind the proposed quantum cryptography protocol. The final single bit value is calculated from many bits through a pair of numbers {i,j} announced by the receiver, Bob. The upper panel corresponds to the actual scheme, in which Bob measures the wave-like nature of the received light sent by Alice to learn the final bit value. Notice that the value of {i,j} might be controlled by an eavesdropper (Eve) through the signal (II) fed to Bob's measurement process M, so looking at this panel alone, the security is ambiguous. If Bob now measures

the particle-like nature of the received light, he no longer learns the final bit but can still exactly produce the same pair {i,j} Lower panel: Here it is seen that {i,j} is directly randomized by the random number generator. Therefore, the possibility that Bob could have measured the particle-like nature of the received light ensures that the randomness of {i,j} is not rigged by Eve. Credit: Toshihiko Sasaki

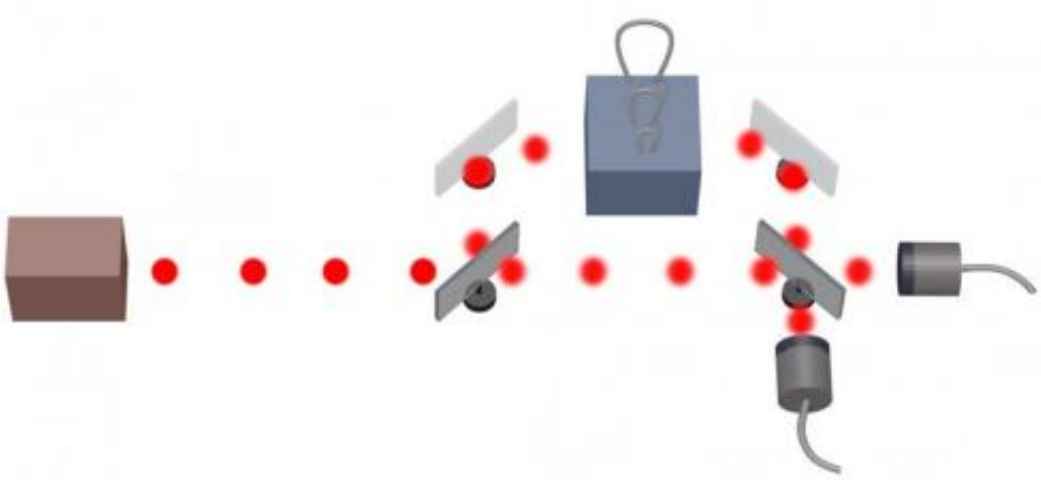
(Phys.org) —Cryptography – the art and science of providing secure communications – typically employs three methods to authenticate users and prevent data theft: *secret key* (symmetric) cryptography, which uses a single key for both encryption and decryption; *public key* (asymmetric) cryptography which uses different keys for encryption and decryption; and hash functions, which employs a mathematical transformation to irreversibly encrypt information. That being said, *quantum cryptography* relies on the laws of quantum mechanics to secure private information exchange, specifically through *quantum key distribution* (QKD) of a random bit sequence, in which an attempt to eavesdrop on the encoded quantum states causes a detectable disturbance in the communications signal. Historically, high-precision monitoring of the disturbance decreases efficiency – but recently, scientists at The University of Tokyo, Stanford University and National Institute of Informatics (Tokyo) proposed a QKD protocol based on an entirely different principle.

The new QKD scheme allows the sender to coherently encode a large number of random bits in such a way that only a small number of bits can be simultaneously read, and the receiver to determine how a single bit is to be calculated. Since an eavesdropper is unable to learn the entire sequence it is impossible to correctly guess the bit value. Moreover, the proposed QKD protocol demonstrated a novel way of utilizing it for secure communication by spreading quantum information coherently

over hundreds of quantum systems, such as optical pulses– and because the resulting quantum effect survives under significant noise, the researchers state that their results will facilitate the simple and efficient use of conventional lasers for QKD.

Prof. Masato Koashi discussed the paper that he, Prof. Yoshihisa Yamamoto and Dr. Toshihiko Sasaki published in *Nature*, first addressing the challenges of defining a quantum key distribution protocol in which non-orthogonal quantum states and random bit calculation to prevent an eavesdropper from correctly determining the bit value by independently bounding leaked information. "This is the point where our new QKD scheme differs from conventional QKD, which relies on the Heisenberg uncertainty principle and allows an eavesdropper to read the signal but leaves a trace that the legitimate users can counter by observing the trace," Koashi tells *Phys.org*. "Our new QKD protocol works on a different principle that prevents eavesdropping attempts rather than detecting them. The challenge was to conceive of a QKD based on such a different principle."

Koashi points out that encoding many raw key bits on quantum systems coherently such that only a few bits can be read out at the same time had some issues as well. "The idea of using a weak coherent pulse train instead of individual photons itself was introduced in 2003, in the form of a QKD scheme called differential phase shift (DPS) QKD. The problem was the lack of a security proof to show that DPS QKD achieves a good key rate."



Implementation of the proposed quantum cryptography scheme. The sender encodes using a pulse train of very weak laser pulses. The receiver superposes and measures arbitrary pairs of optical pulses using a variable delay. Credit: Toshihiko Sasaki

Another challenge was determining that a practical implementation using a laser pulse train achieves a key rate comparable to a *decoy-state QKD protocol*, in which several different photon intensities are used instead of one to compensate for the security loophole that arises when the sender uses multi-photon sources rather than a single-photon source to transmit quantum information. "The challenge here was to determine how to use a mundane laser, rather than more exotic light sources such as a single-photon source, for QKD," Koashi explains. "The laser is cheap and can emit pulses in a rapid sequence – for example, 10^9 pulses per second – but its drawback is the photon number randomness in a single pulse: a laser pulse sometimes includes two or more photons, so if we use laser pulses for a QKD scheme employing a photon as an information carrier, such multi-photon pulses are exploited by an eavesdropper because additional photons are available." He concludes that since the decoy-state QKD protocol incorporates additional monitoring steps to infer how much an eavesdropper may have exploited multi-photon pulses, it was

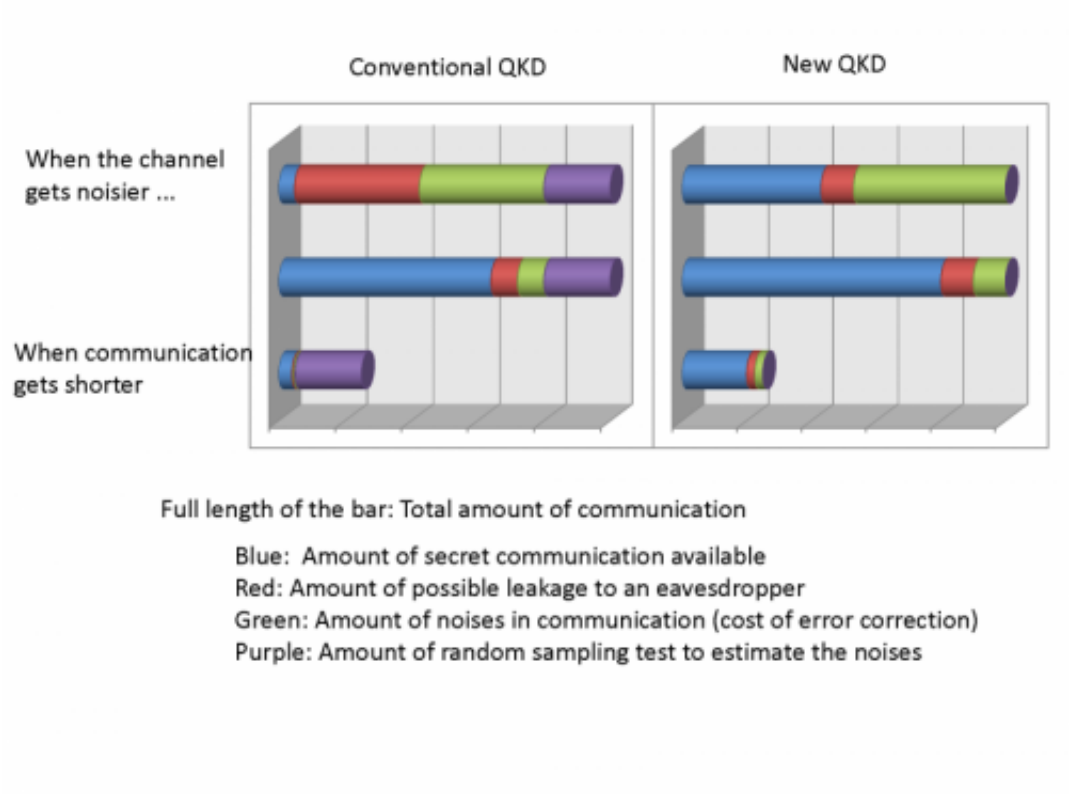
one of the best answers so far – but since the complicated monitoring steps in the decoy-state QKD is tedious, a QKD scheme which does not use a single photon as a carrier, but uses more of the wave-like property of light, would be preferable. "In that case, we wouldn't need to worry when the laser emits two or more photons. That said," he acknowledges "while DPS QKD – which utilizes a weak coherent pulse train instead of individual photons – is one example of such an attempt, there is no security proof showing that this scheme works well."

To address these challenges, the scientists tried variants of DPS QKD schemes. "The round robin, or RR, DPS QKD scheme we named and introduced in the paper is one such scheme," notes Koashi. (As described in the paper, the RR-DPS QKD setup is almost identical to the DPS QKD protocol, the difference being that the fixed delay line in the original is replaced by a variable delay line.) "The key insight is that we've been looking at QKD security in terms of one particular feature of quantum mechanics – that is, complementarity." Complementarity is the concept that two contrasted theories, such as the wave- and particle-like natures of light, may be able to explain a set of phenomena, although each separately only accounts for some aspects. "The two faces of light – photons and electromagnetic waves – are revealed not by a single measurement, but by separate measurements that cannot be performed simultaneously. You must choose either one or the other. The existence of the choice between two different measurements was the key to show that the RR-DPS QKD scheme is nothing like the conventional QKD. Without such a perspective, we wouldn't have noticed that we stumbled upon a gem when we tried the RR-DPS QKD scheme."

In the paper, the researchers state that their findings give new insight into how the probabilistic nature of quantum mechanics can be related to secure communication, and moreover will facilitate the simple and efficient use of conventional lasers for QKD. "I'm excited about the results because our discovery is an entirely different way of hiding

information that was somehow overlooked by researchers for the 30 years since they realized in 1984 that the quantum mechanics can be used for that purpose." Koashi tells *Phys.org*. "Moreover, it was even more surprising that the new idea can be implemented by a mundane interferometer with a conventional laser." Regarding the second benefit, Koashi says that when channel noise gets higher – that is, when the bit-error rate exceeds ~15% - conventional QKD schemes cease to work, while the new QKD method can still work and provide secret communication up to bit-error rate of ~35%.

"When the communication time is limited," Koashi adds, "the cost of monitoring channel disturbance, which is an almost constant number of bits, severely affects the efficiency in conventional QKD. For conventional QKD with lasers, typically 10^6 bits of communication is required for enabling even one bit of secret communication. The new method starts to produce secret communication from ~10^3 bits of communication – so I'd say our new QKD is more flexible in use and can be adapted to a wider variety of situations."



Credit: Toshihiko Sasaki

Koashi also elaborated on how spreading quantum information coherently over hundreds of quantum systems provides a novel way of utilizing such systems for secure communication. "In our proposed scheme, a train of ~100 very weak laser pulses are used. Every pulse is encoded with one-bit information, but there are only a few photons in total over the entire pulse train. This means that there are ~100 bits of candidates encoded on the pulse train, but only a few bits are retrievable, thereby lowering the chance that an eavesdropper might acquire the information on the pair of bits randomly specified by the receiver."

Moving forward, Koashi says, planned research is based on the scientists finding a new way to hide information in quantum signals. "Our proposed RR-DPS scheme is one particular example of implementing

that principle, so our next step is to seek a variety of ways in which the new principle can be implemented, such as using many different wavelengths of light instead of many pulses. In addition, and as mentioned, our scheme is much more robust against noise than is conventional QKD. Since fragility to noise is a weakness of quantum signals we frequently encounter in various applications of quantum information, I hope that the encoding technique used in our proposed scheme may be adapted to other applications to provide a better shield against noise."

Regarding the wider effect of their research, Koashi notes, "The principle of our new scheme has a close connection to the notion of information causality, which was proposed a few years back to answer the very fundamental question of why our universe is governed by quantum mechanics rather than other conceivable candidates. Therefore, our research will also give an insight into fundamental aspects of physics."

More information: Practical quantum key distribution protocol without monitoring signal disturbance, *Nature* 509, 475–478 (22 May 2014), doi:10.1038/nature13303