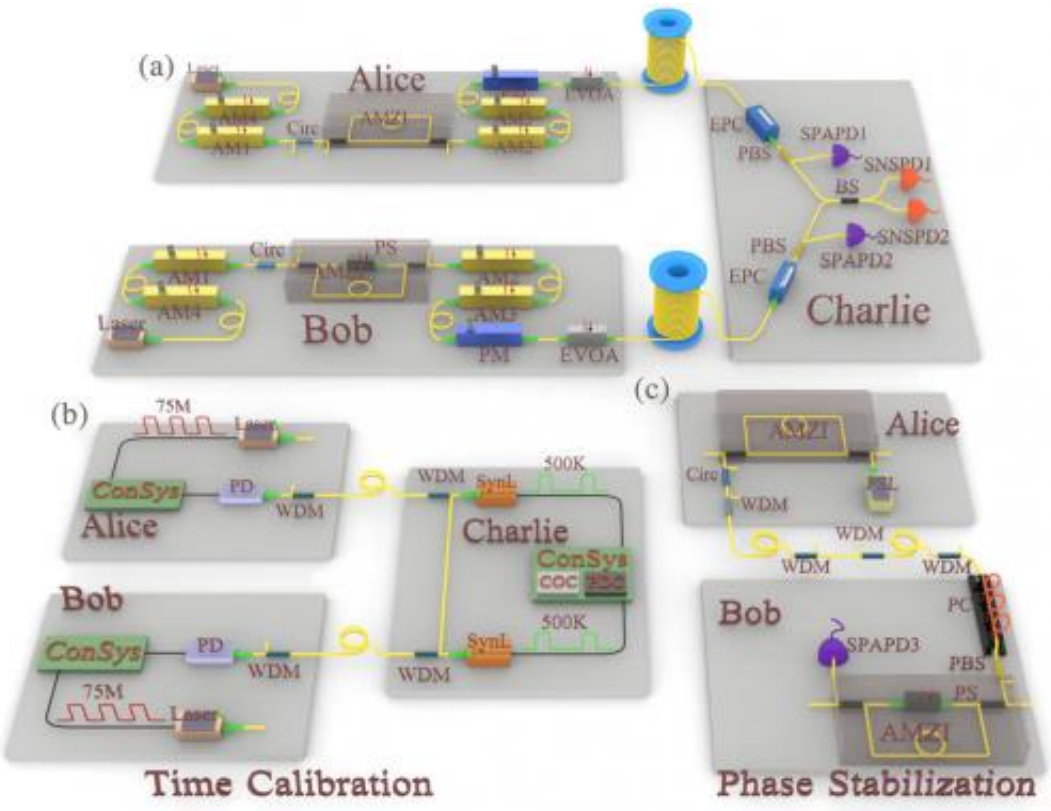
Hackers begone: Measurement-device-independent QKD increases clock rate and transmission distance while reducing failure

December 1 2014, by Stuart Mason Dambrot



(a) Schematic layout of our MDIQKD setup. Alice's (Bob's) signal laser pulses (1550 nm) are modulated into three decoy-state intensities by AM1. An AMZI, an AM2–4, and one PM are used to encode qubits. Charlie's setup consists of a polarization stabilization system and a BSM system. The polarization stabilization system in each link includes an EPC, a PBS, and a SPAPD. The BSM system includes an interference BS and two SNSPDs. (b) Time calibration system. Two SynLs (1570 nm) are adopted, with the 500 kHz shared time reference generated from a crystal oscillator circuit (COC) and with the time

delayed by a programmable delay chip (PDC). Alice (Bob) receives the SynL pulses with a PD and then regenerates a system clock of 75 MHz. WDM: wavelength division multiplexer, ConSys: control system. (c) Phase stabilization system. Circ: circulator, PC: polarization controller, PS: phase shifter. Credit: Tang, Yan-Lin et al. (2014) Measurement-Device-Independent Quantum Key Distribution over 200 km. *Phys. Rev. Lett.* 113:190501.

(Phys.org)—In the ongoing effort to make communications secure, Quantum Key Distribution (QKD) theoretically provides a solution – but to the delight of increasingly sophisticated hackers, falls short in real-world systems due to implementation deviating from mathematical models. A number of QKD variants – including Device-Independent Quantum Key Distribution (DIQKD) and the more recently introduced Measurement-Device-Independent Quantum Key Distribution (MDIQKD) – attempt to close the gap between theory and practice with varying degrees of success. These two variants differ in several ways, the most important being that DIQKD requires but unlike MDIQKD cannot easily achieve very high detection efficiency and low channel loss to yield secure keys, while MDIQKD, unlike DIQKD, does not rely on any ideal devices and can close the most vulnerable QKD security hole by removing all side-channels from the measurement unit. Nevertheless, previous MDIQKD systems have had limitations as well, such as limited distance and a low key rate of less than 0.1 bit/s.

Recently, however, scientists at the University of Science and Technology of China devised a *de novo* MDIQKD protocol and have developed a 75 MHz clock rate, fully automatic and highly stable system and superconducting nanowire single-photon detectors with detection efficiencies of more than 40%. By so doing, they have extended MDIQKD secure transmission distance to 200 km, and achieving a secure key rate three orders of magnitude higher – and an failure

probability six orders of magnitude lower – than those of previous MDIQKD attempts. The researchers state that their results pave the way towards a quantum network with measurement-device-independent security, and in fact have already demonstrate the feasibility of MDIQKD in an unstable environment by performing a field test in which their system was inserted into an installed fiber network.

Prof. Qiang Zhang discussed the three key accomplishments detailed in the paper that he, co-group lead Prof. Jian-Wei Pan, Researcher Yan-Lin Tang, and their co-authors published in *Physical Review Letters*. "Each of our main accomplishments – increasing system clock rate to 75 MHz and improving system stability, extending secure transmission distance to 200 km, and lowering failure probability by six orders of magnitude to 2×10^{-9} – had its unique challenges," Zhang tells *Phys.org*. "In terms of performance, this is the first time we've increased clock rate to 75 MHz, as well as improving system stability and using high efficiency – over 40% – superconducting nanowire single-photon detectors to develop a fully automatic system, in an MDIQKD approach."

Zhang points out that while a gigahertz clock rate in conventional QKD is easily achieved, this is not the case with MDIQKD. Specifically, unlike conventional QKD, MDIQKD relies on interference between two independent lasers – and increasing the clock rate to 75 MHz caused poor two-laser interference visibility. "The main challenge lies in high-speed laser modulation, including not only severe overshoot, ringing and chirp inside the laser pulse, but also a more subtle problem lying in the temperature fluctuation caused by random triggering signals to the internally-modulated laser source," Zhang explains. "These effects are observed for the first time simply because interference of two independent high clock-rate lasers could not be discovered in a low-speed system."

Regarding detector efficiency (DE), Zhang notes that superconducting

nanowire single-photon detectors (SNSPDs) have been demonstrated as a key tool for improving the QKD performance – but the challenge is to improve nanowire absorption. The scientists have addressed this issue by integrating an optical cavity structure in the detectors: SNSPDs are cooled down to 2.2 K by using a Gifford-McMahon cryocooler to guarantee high detector performance as well as 7´24 hour operation[†]. "Again," he stresses, "this is the first time high detector efficiency superconducting nanowire single-photon detectors have been applied in an MDIQKD system."

Extending the MDIQKD secure transmission distance to 200 km and achieving a secure key rate three orders of magnitude higher than previous results in recent MDIQKD experiments challenged the researchers in several aspects. "First was the signal-to-noise ratio," Zhang notes. "Because of the long distance, the signal arriving at the receiver's side will be very weak. "Secondly, system stability in a 200 km case is difficult since the fiber fluctuation is much severe, and a large attenuation will make it even harder with weak feedback signals. Thirdly, we required a better and stricter post-processing method to handle the greater distance results in a slower raw data rate and a stronger fluctuation."

Finally, to guarantee the safe usage of the secure key in practice, the failure probability must be controlled beneath the order of 10^{-9} – and the 2×10^{-9} failure probability they achieved is six orders of magnitude lower than previous results. The main reason that previous demonstrations used a higher failure probability of 10^{-3}, Zhang tells *Phys.org*, is that performing fluctuation analysis with a lower failure probability requires more data to be accumulated. However, this requirement could not be satisfied by the actual experimental systems operated at a slow system clock rate and without full automatic feedback system – especially in the 200 km case when signal attenuation is very large – so the arriving signal is weak.

Addressing these challenges was, in itself, a challenge. "For the current experiment," Zhang continues, "the first challenge was to increase the system clock rate to 75MHz with good laser modulation. To ensure a good waveform, we modulated the laser pulse with an amplitude modulator cutting off the tail, thereby eliminating the influence of the chirp, overshoot and ringing. To ensure robust two-laser interference, we modulated vacuum intensity – instead of not providing the triggering signal – to avoid the effect of temperature fluctuation."

For a long distance QKD experiment, a single-photon detector with high detection efficiency and low dark count rate (the average rate of registered counts without any incident light) is decisive. "A conventional semiconducting APD (avalanched photodiode) cannot fulfill this requirement because of its high dark count rate and low detection efficiency, which is why a superconducting nanowire single-photon detector – specifically, a cryocooler-based SNSPD technology providing over 40% detection efficiency at the dark count rate of 10 Hz – is the sole choice for 200 km MDIQKD." (In QKD protocols, an ideal single photon source rarely exists, and so is replaced by a weak coherent state laser source or other alternative. This causes a serious security problem that is minimized by using a weak laser source – but the latter results in low QKD speed. *Decoy state QKD* uses several different photon intensities rather than a single intensity to resolve the multi-photon issue. Moreover, the scientists optimized the decoy state MDIQKD protocol, including the decoy state scheme, intensity and probability distribution.

"Secondly," Zhang continues, "we adopted the high efficiency, low dark count superconducting nanowire single-photon detector to achieve the 200 km distance. Last but not least, to make the entire system stable for a long period of time, we developed several feedback systems to precisely calibrate the parameters of the system, such as a wavelength calibration system employing an optical spectrum analyzer with 1 pm precision." This is critical because extended system stability enables

continuous running for as long as an entire week.

The much lower failure probability of 10^{-9} requires not only an experimental setting capable of accumulating enough raw data, but also a more appropriate post-processing method to extract the secure key. "With this work, for the first time in the entire OKD community we adopt the Chernoff bound (which gives exponentially decreasing bounds on tail distributions of sums of independent random variables) with a failure probability of 10^{-9} to allow statistical fluctuation analyses six orders of magnitude lower than previously achieved," Zhang explains. "Furthermore, with the high loss that occurs in long-distance QKD, the Chernoff bound – believed to be a future standard post-processing method – provides better, stricter parameter estimation in the statistical fluctuation analysis."

Interestingly, in their paper the scientists point MDIQKD security is inspired by the time-reversed EPR-based QKD protocol. "This can be explained by a virtual qubit idea," Zhang says. "A sender first prepares an entangled state of the combined system of her virtual qubit and the qubit to be sent to the receiver. The sender then measures the virtual qubit, thereby preparing a BB84 state." *BB84* is a provably secure quantum key distribution scheme – in fact, the first quantum cryptography protocol – developed by Charles Bennett and Gilles Brassard in 1984 (hence its name) relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states we are trying to distinguish are not orthogonal. "After making a Bell state measurement (BSM) and obtaining a successful outcome, the receiver announces the results to the sender and the third party in the quantum system, resulting in their virtual qubits becoming entangled. (*Bell states* are maximally entangled quantum states of two qubits; the *Bell state measurement* is a joint quantum-mechanical measurement of two qubits that determines which of the four Bell states the two qubits are in.) "In this sense, the protocol is directly equivalent to

an entanglement based protocol, only with the time direction reversed."

In addition, the new MDIQKD protocol does not rely on any assumption on measurement. "In the virtual qubit idea, we can see that a sender prepares the BB84 state by measuring a virtual qubit. Since the sender could have delayed the measurement on this virtual qubit until *after* the receiver performs a Bell state measurement and announces its results, the receiver's BSM cannot affect the BB84 state preparation process, and so the receiver cannot obtain any information about the BB84 state. In other words, security does not rely on any assumption on measurement."

Another result described in the paper is that the novel MDIQKD system's techniques constitute a critical ingredient for a quantum repeater and long-distance quantum communication. "Performing a Bell-state measurement is an intrinsic element in these situations," Zhang points out, because it requires good interference of two independent laser sources. Again, in our work we for the first time have shown the feasibility of this kind of interference, especially at a distance 200 km. Besides the laser modulation techniques, the feedback systems developed for this purpose – for example, time calibration and wavelength calibration – are also of great importance to realizing a long-distance quantum repeater."

The researchers point out that their results have a range of implications for future quantum communication systems, one clearly being it paving the way towards a quantum network with measurement-device-independent security. "Our MDIQKD system includes two clients and one server. With the help of a system-wide feedback system, all users are time-synchronized and all independent laser sources have the same wavelength. All these techniques are definitely a solid foundation of building an MDIQKD network. In addition, to add more clients into the network, all that is needed is placing an active optical switch in the server's site – and with off-the-shelf optical switches, this MDIQKD

network can be built in the near future."

The novel MDIQKD protocol has a star-type structure in which the detection system placed in the Bell-state measurement site as a server, allowing it to be shared by all transmitters – a structure very suitable to a QKD network with a star-type structure, since all the end-node clients can share the entire measurement system of the center-node server. This means that, importantly, only laser sources and modulators are required when more clients are added to the network. Zhang notes that these devices are much smaller and cheaper than the complex, expensive detectors – a factor preferred for creating an economical network.

The scientists have also performed a field test in which their system has been inserted into an installed fiber network to demonstrate the feasibility of MDIQKD in an unstable environment. "Previously, an MDIQKD field test was performed over an 18.6 km deployed fiber by Wolfgang Tittel's group at the University of Calgary[1]," Zhang tells *Phys.org*. "However, a random modulated decoy state was not added in that experiment, so a secure key was not actually generated. Moreover, all other laboratory demonstrations are performed without perturbation of the field environment." Based on the technology developed in their experiment, the researchers have achieved a 16.9 bps secure key rate over a 30 km fiber network of total length[‡].

Zhang and his co-authors envision a number of future real-world applications that would be made feasible by using a single fiber to transmit both signal laser pulses and synchronization laser pulses, as well as by minimizing noise generated from Raman spontaneous scattering. "To make MDIQKD more attractive for potential users, our goal is to have only one single fiber required for each link. This would decrease the resources required by real-world applications, such as voice calls and file transfers, and would be especially useful in some particular situations." For example, a user having insufficient fiber link resources

could multiplex a single fiber link to do classical synchronization and single-photon transmission – or in the occasional situation when a user performs QKD tasks, it would be preferable to have one fiber link rather than two in order to conserve normally unused resources.

Zhang adds that a significant concern when adopting one single fiber is strong spontaneous Raman scattering of the synchronization light, which introduces additional noise to the signal and thus increases error rates. (*Spontaneous Raman scattering* is the inelastic scattering of photons – in which the kinetic energy of an incident particle is not conserved, but lost or increased – in random time intervals.) "Typically, the power of the synchronization light is at least five orders of magnitude higher than the signal light – so spontaneous Raman scattering could be disastrous. We therefore have to be careful when multiplexing these two kinds of light, because otherwise the resulting high noise and error rates would male all real world applications impossible."

Moving forward, Zhang says that the scientists plan to build a polarization-encoding MDIQKD system, which let them remove the phase stabilization that is currently required, as well as other possible innovations. "In our experiment, wavelength calibration is based on an optical spectrum analyzer. However, in addition to this simple and direct approach, we plan to develop an alternative way *without* an optical spectrum analyzer – but only with the evaluation of two independent laser sources. This can be realized by observing Hong-Ou-Mandel dip." (The Hong–Ou–Mandel effect is a two-photon interference effect in quantum optics that occurs when two identical single-photon waves enter a 50:50 beam splitter, one in each input port. When both photons are identical they will extinguish each other – but if they become more distinguishable the probability of detection will increase, allowing the interferometer to accurately measure bandwidth, path lengths and timing.) Moreover, Zhang adds, the researchers plan to build a three-layer architecture to generate, manage and use the secure key,

respectively, which will lead to a more complete and practical QKD network.

"Since the Bell state measurement is so common in quantum information," Zhang concludes, "our Bell state measurement techniques can be utilized in other quantum information tasks." "These tasks include the quantum repeater mentioned above, quantum fingerprinting and quantum teleportation."

More information: Measurement-Device-Independent Quantum Key Distribution over 200 km, *Physical Review Letters* (2014) **113:**190501, doi:10.1103/PhysRevLett.113.190501

Related:

[1]Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, *Physical Review Letters* (2013) 111:130501, doi:10.1103/PhysRevLett.111.130501

[†]Detectors and cryocooling systems developed by Shanghai Institute of Microsystem and Information Technology (SIMIT) and the Chinese Academy of Sciences (CAS)

[‡]Paper to be published in *IEEE Journal of Selected Topics of Quantum Electronics*