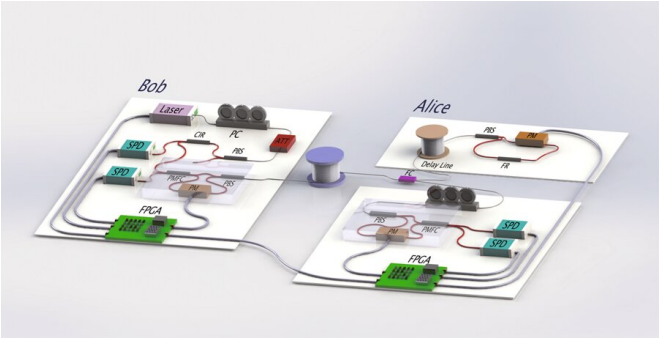
Implementing a practical quantum secure direct communication system

18 February 2019, by Thamarasee Jeewandara



Experiment setup. A strongly attenuated 1550 nm laser is used as an approximate single-photon source with a systematic pulse-repetition frequency of 1 MHz. In the experimental setup Bob sends the single photons to Alice in a superposition of two time-bins with a relative phase, and Alice randomly chooses one of two possible tasks, error-check or coding. Both sides are controlled by field programmable gate arrays (FPGAs), and the operation of the four single-photon states is realized with a commercial lithium niobate modulator. PM phase modulator. PC polarization controller. PBS polarization beam splitter. ATT attenuator. CIR optical circulator. FC fiber coupler. SPD superconducting nanowire single-photon detector with 70% detection efficiency, 100 Hz dark count rate and 50 ns reset time. PMFC polarization maintaining filter coupler. FR Faraday rotator. Credit: Light: Science & Applications, doi: https://doi.org/10.1038/s41377-019-0132-3

Quantum secure direct communication (QSDC) is an important branch of quantum communication, based on the principles of quantum mechanics for the direct transmission of classified information. While recent proof-of-principle experimental studies have made remarkable progress; QSDC systems remain to be implemented in practice. In a recent study, Ruoyang Qi and co-workers at the departments of low-dimensional quantum physics, information technology, electronics and information engineering, proposed and experimentally implemented a practical quantum secure communication system.

In the work, Qi et al. analyzed the security of the system using the Wyner wiretap channel theory. The scientists developed a coding scheme using concatenation (interconnected) low-density parity-check (LDPC) codes in a realistic environment of high noise and high losses. The system operated with a repetition rate of 1 MHz across a distance of 1.5 kilometers and maintained a secure communication rate of 50 bps to send text messages, reasonably sized images and sounds. The results are now published in *Light: Science & Applications*.

The work by Qi et al. highlighted a form of QSDC that can transfer direct information without a distribution key to prevent vulnerability to attacks. In the work, the team used a 1550 nm laser to generate single photons that carried secure quantum information, the scientists were able to successfully decode the information upon receipt. The method was reliable even in realistic environments caused by high photon loss or errors introduced due to noise. The standard LDPC code that they used in the study for better error-correction performance was implemented by the Consulate Committee for Space Data Systems (CCDS) for near-earth and deep-space applications.

Global security depends on secure communication infrastructures. At present, communication is secured via encryption techniques such as the RSA public key scheme. The secrecy capacity is defined as the supremum of all achievable transmission rates with security and reliability. In practice, it is difficult to estimate the secrecy capacity in classical communication systems due to the difficulty with eavesdropping detection. In quantum systems, single photons or entangled photon pairs can transmit digital information, giving rise to new features in quantum cryptography, unattainable in classical transmission media. In principle, it is

impossible to eavesdrop without disturbing the transmission so as to avoid detection in such a setup.

The first quantum communication protocol was proposed by Bennett and Brassard (BB84), based on exploiting quantum resources for secure key agreement. In 2000, QSDC was proposed to communicate information directly without a secret key and eliminate loopholes associated with key storage and ciphertext attacks. Subsequent proof-of-principle studies have demonstrated QSDC based single photons and entangled pairs, including studies where a fiber could communicate across a meaningful distance of 500 m using two-step QSDC protocols.

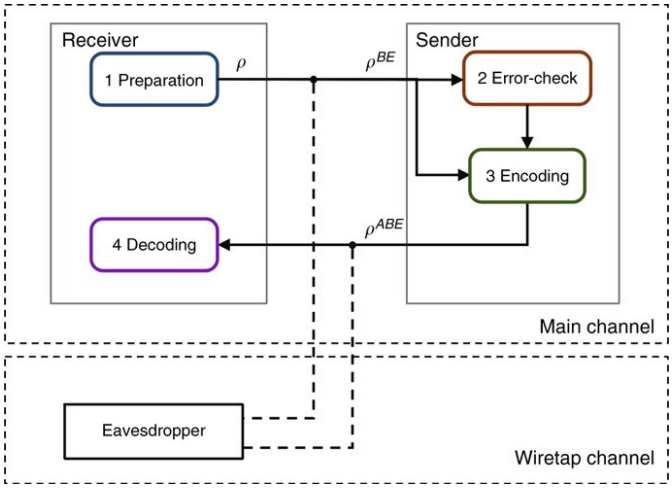


Illustration of the practical DL04-QSDC protocol. The “main channel” and the “wiretap channel” are discrete memoryless channels. The main channel represents a channel between the sender and the legitimate receiver, while the wiretap channel represents a channel between the sender and the eavesdropper. Credit: Light: Science & Applications, doi: https://doi.org/10.1038/s41377-019-0132-3

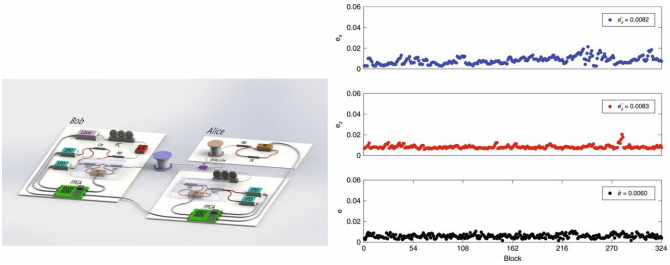
In the present study, Qi et al. implemented a practical quantum secure direct communication system using a procedure based on the DL04 protocol (without a key). According to the Wyner wiretap model, to implement the QSDC system in practice, the system should work below the secrecy capacity of the channel for secure information transmission. The scientists estimated the secrecy capacity of the system using interconnected low-density parity check (LDPC) codes. They designed the scheme to specifically operate in high loss and high error-rate regimes, unique for quantum communication. Qi et al. thus demonstrated the QSDC platform could effectively function in a realistic environment.

When implementing the DL04-QSDC protocol, the scientists included a discrete memoryless 'main channel' and a 'wiretap channel'. The main channel represented the network between the sender and the receiver. The wiretap channel represented the network between the legitimate users and the eavesdropper. The protocol contained four steps:

1. Hypothetically, Bob is a legitimate information receiver who prepares a sequence of qubits. Each qubit is randomly in one of the four states (|0>, |1>, |+> and |->). He then sends the sequence of states to the information sender Alice.
2. Upon receiving the single photon sequence, Alice randomly chooses some of them and measures them randomly. She publishes the positions, the measuring basis and measurement results of those single photons. Bob compares this information with his preparations of these states and estimates the bit-error rate of the Bob-to-Alice channel and informs Alice through a broadcast channel. Alice can then estimate the maximum secrecy capacity (Cs) of the Bob-to-Alice channel using the wiretap channel theory.
3. Alice chooses a coding sequence for the remaining qubits. This scheme is based on the interconnected LDPC codes. She constructs the code words and returns them back to Bob.
4. Bob decodes Alice's message from the signals he received after measuring the qubits in the same basis as he prepared. If the error rate is below the correcting capability of the LDPC code, the transmission is successful. They then start again from step 1 to send another part of the secret message until they completely transmit the entire message. If the error rate

is greater than the correcting capacity of the LDPC code, neither Bob nor the eavesdropper Eve can obtain information, in which case they terminate the process.

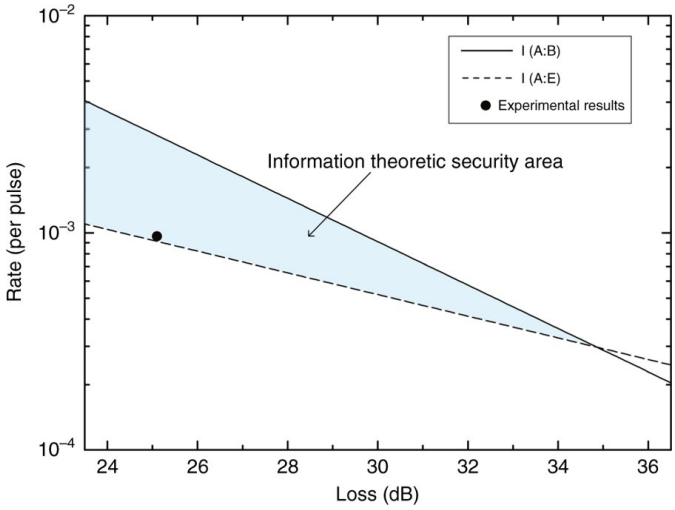
Qi et al. used highly attenuated lasers as an approximate single-photon source in the implementation. For better approximation of a single photon source to detect eavesdropping attacks, a decoy state quantum key distribution method can be used. If the secrecy capacity is non-zero for any wiretap channel, i.e. if the legitimate receiver has a better channel than the eavesdropper, there exists some coding scheme that achieves perfect secrecy according to the Wyner model. However, not all coding schemes can guarantee the security, which essentially depends on details of the coding.



Left: Experimental setup. Right: System stability with different message blocks. ex and ez are the error rates of measurements using the X-basis and Z-basis, respectively, at Alice's site. e is the error rate at Bob's site. The error rate was estimated block by block; each block contains 1312 × 830 pulses. The mean number of photons is 0.1. The inherent loss of a quantum channel is 14.5 dB, which includes the efficiency of the detector, ~70%, and the optical elements, ~13 dB. The total loss of the system is 25.1 dB at a distance of 1.5 km. Credit: Light: Science & Applications, doi: https://doi.org/10.1038/s41377-019-0132-3

The scientists then implemented the scheme in a fiber system with phase coding, for quantum communication across long distances. In this setup, Bob prepares a sequence of single-photon pulses, after polarization control and attenuation, the pulses are prepared as random qubits and sent to Alice's site through a 1.5 km-long fiber. On arrival at Alice's site, it's separated in to two parts, where one goes to the encoding module and the other to the control module for error-check, controlled by field programmable gate arrays (FPGAs) in the setup.

Simultaneously encoding occurs in the encoding module. If the error-rate is smaller than the threshold, the encoding part is allowed to send the single photons back to Bob via the same fiber, where they are guided to single photon detectors for measurement. The scientists controlled the setup consisting of three phase modulators (PM) and single photon detectors (SPD) to encode messages at the two sites using the FPGAs, which were further controlled by upper-position computers.



The solid line represents the mutual information between Alice and Bob; by the noisy-channel coding theorem that transmission rate cannot exceed the capacity of the main channel. The dotted line is the mutual information between Alice and Eve, the maximum information that an eavesdropper can obtain. Symbols represent experimental results. Together with the chosen LDPC code, the coding scheme yields a transmission rate of 0.00096 when the bit-error rate is under 10^?6. Because the rate is greater than the mutual information between Alice and Eve, both the security and reliability of the information transmission are assured. Credit: Light: Science & Applications, doi: https://doi.org/10.1038/s41377-019-0132-3

In the experimental results, the scientists represented the mutual information versus the loss of the system as two straight lines. The area

between these two lines formed the information theoretic secure area. As a result, for a coding scheme with an information rate within the specified area, the security could be reliably guaranteed. Using the experimental setup, Qi et al. attained a secure information rate of 50 bps, well within the defined secure area.

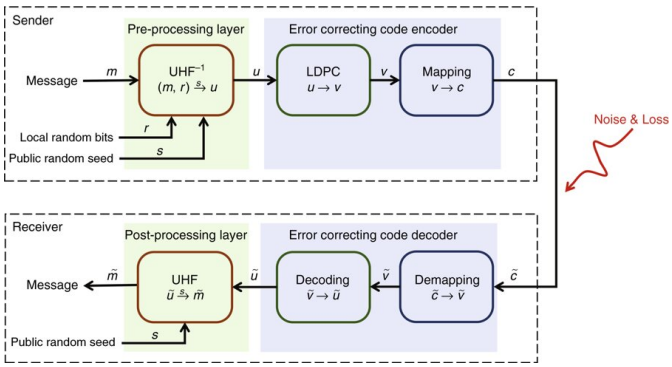


Illustration of the coding scheme. A message m together with a local random bits r and public random seed s are processed by the reverse universal hashing families UHF?1 to vector u, and then u is changed by LDPC code into v, which is mapped to codeword c and is then sent to the receiver's site. Because of loss and error, receiver Bob receives a degraded codeword, and then he demaps, decodes and obtains the message after performing universal hashing families UHF. Credit: Light: Science & Applications, doi: https://doi.org/10.1038/s41377-019-0132-3

The scientists illustrated a coding scheme to guarantee the reliability of transmission for QSDC based on interconnected LDPC codes. Preprocessing was based on universal hashing families (UHF). In the process, for each message (m), the sender Alice generates a local sequence of random bit (r) and public random seed (s). Next, she maps to a vector (u) by the inverse of an appropriately chosen UHF (UHF^{-1}), which is then changed by LDPC code into (v), mapped to codeword (c) and sent to the receiver's site.

In information theory, the noisy-channel coding theorem establishes reliable communication for any given degree of noise contamination of a communication channel. To ensure reliability of the information, Alice modulates the pulses that reach the legitimate receiver Bob, who makes measurements in the same basis as he prepared them. Due to loss and error, Bob receives a degraded codeword, which he demaps and decodes after postprocessing with UHF to obtain the message.

In this way, Qi et al. implemented a practical QSDC system in a realistic environment of high noise and high loss. Among other techniques, the scientists used an LDPC code to reduce error and loss in the system. They analyzed the security of the system in depth using the Wyner wiretap channel theory. When the secrecy capacity was non-zero; a coding scheme with an information rate less than the secrecy capacity ensured both security and reliability of the information transmission. In total, the scientists obtained a secure information rate of 50 bps at a practically meaningful distance of 1.5 km. Qi et al. imply these parameters are premature and envision an improved system that can integrate the existing technology for a higher rate of dozens of kbps information transmission in the future.

More information: Implementation and security analysis of practical quantum secure direct communication www.nature.com/articles/s41377-019-0132-3, Ruoyang Qi et al. 06 February 2019, *Light: Science & Applications*.

Secure direct communication with a quantum one-time pad journals.aps.org/pra/abstract/ … 3/PhysRevA.69.052319, Deng Fuo-Guo and Long Gui Li, May 2004, *Physical Review A*.

A method for obtaining digital signatures and public-key cryptosystems dl.acm.org/citation.cfm?id=359342 Rivest R.L. et al. February 1978, Communications of the Association for Computing Machinery.

A Mathematical Theory of Communication dl.acm.org/citation.cfm?id=584093, Shannon C.E. October 1948, The Bell System Technical Journal, IEEE Explore.