New Journal of Physics

The open access journal at the forefront of physics

PAPER

Implementation vulnerabilities in general quantum cryptography

Anqi Huang[1,2,3] ⬥, Stefanie Barz[4,5], Erika Andersson[6] and Vadim Makarov[7,8]

1 Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha 410073, People's Republic of China
2 Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada
3 Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1, Canada
4 Institute for Functional Matter and Quantum Technologies, University of Stuttgart, D-70569 Stuttgart, Germany
5 Center for Integrated Quantum Science and Technology, University of Stuttgart, IQST, D-70569 Stuttgart, Germany
6 Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh, Scotland, EH14 4AS, United Kingdom
7 Russian Quantum Center and MISIS University, Moscow, Russia
8 Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1, Canada

E-mail: angelhuang.hn@gmail.com

Abstract

Quantum cryptography is information-theoretically secure owing to its solid basis in quantum mechanics. However, generally, initial implementations with practical imperfections might open loopholes, allowing an eavesdropper to compromise the security of a quantum cryptographic system. This has been shown to happen for quantum key distribution (QKD). Here we apply experience from implementation security of QKD to several other quantum cryptographic primitives. We survey quantum digital signatures, quantum secret sharing, source-independent quantum random number generation, quantum secure direct communication, and blind quantum computing. We propose how the eavesdropper could in principle exploit the loopholes to violate assumptions in these protocols, breaking their security properties. Applicable countermeasures are also discussed. It is important to consider potential implementation security issues early in protocol design, to shorten the path to future applications.

1. General introduction

Common aims in cryptography are to guarantee confidentiality, integrity, and authentication of information. Some of the conventional cryptography based on computational complexity might be broken by a powerful quantum computer [1]. However, quantum cryptography, where security rests on the laws of quantum mechanics, is one way to achieve information-theoretic security. Among the quantum cryptographic protocols, quantum key distribution (QKD) has become theoretically mature and technically practical. Inspired by the idea of QKD and taking advantage of QKD implementations, other quantum cryptographic primitives have gradually been developed, such as quantum coin tossing, quantum secret sharing (QSS), and quantum digital signatures (QDS) [2–4]. For each primitive, different protocols have been proposed, and even realized by current technology [5–7].

However, there is a non-negligible gap between theory and practice in QKD: imperfections in devices create various loopholes that compromise the protocol's security [8–14]. Practical security issues might also occur in the realization of other quantum cryptographic protocols. In theory, the protocols are unconditionally secure, but the security might not be guaranteed in practice due to imperfections of devices. Investigating device imperfections and system loopholes in QKD has taken more than a decade, and is still in progress. The experience gained from QKD will be helpful in finding possible loopholes in other implementations of quantum cryptographic protocols, because they use similar optical components. This enhances the practical security of quantum cryptography.

Table 1. Summary of potential attacks in implementations of quantum cryptographic protocols. The table lists broken security properties for five primitives: two different protocols for quantum digital signatures (QDS), two different protocols for quantum secret sharing (QSS), source-independent quantum random number generation (SI QRNG), quantum secure direct communication (QSDC), and blind quantum computing (BQC). '—' means the attack is not applicable. See text for details.

Protocol	Attack			
	Source side channel	Wavelength-dependent attack	Detector control attack	Trojan-horse attack
QDS				
Identical-state-sharing [7]	Unforgeability	Unforgeability	Unforgeability	—
Different-state-sharing [6]	—	—	Unforgeability	Unforgeability
QSS				
Entanglement-based [15]	—	—	Confidentiality	—
Single-qubit [5]	—	—	—	Confidentiality
SI QRNG [16]	—	Randomness	Randomness	—
QSDC [17]	—	—	Confidentiality	Confidentiality
BQC [18]	Confidentiality	—	—	Confidentiality

The vulnerability of quantum coin-tossing and non-loophole-free Bell testing has previously been demonstrated [19, 20], using imperfections in their specific experimental implementations to remove the protocol's quantum advantages. In this Article, we survey five quantum cryptographic primitives as examples to investigate practical security threats in their implementation. The primitives are QDS, QSS, source-independent (SI) quantum random number generation, quantum secure direct communication (QSDC), and blind quantum computing (BQC). Based on attacks known to exist for QKD, we propose potential attacks on these primitives. The attacks may compromise the security of practical quantum cryptographic systems, without making the legitimate participants abort the cryptographic protocols. We summarize potential imperfections and broken security properties for all five primitives in table 1. Details for each primitive are explained in sections 2–6. Each of these sections contains two parts: in first subsection we recap the protocol, and in second subsection we propose the attacks on its implementation. Countermeasures are discussed in section 7. We conclude in section 8. Please note that this study is merely a starting point presenting a broad overview. Detailed analysis of each implementation imperfection should be done in the future, as technological implementations of the protocols mature.
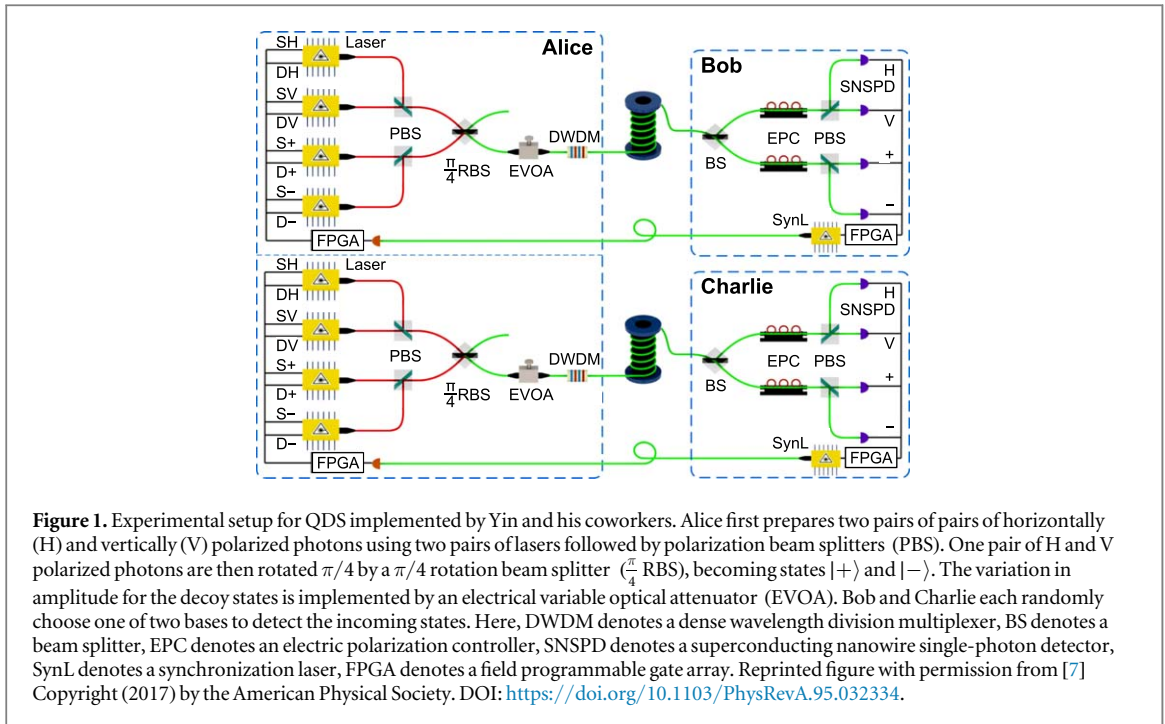
In this Article, we focus on the implementation security of the demonstrations. We also remark that while most of these quantum cryptographic schemes have advantages over 'classical' schemes, for some of these protocols, their practical usefulness is less clear, and strict security proofs may still be under development. For example, it is not always clear what practical advantage all protocols for QSS offer, over protocols based on secret shared keys followed by a 'classical' protocol for secret sharing. Similarly, for QSDC, one would need to motivate the usefulness of direct communication, as opposed to establishing secret shared keys using standard QKD, followed by encryption using these keys. Discussing these aspects is however outside the scope of our study.

2. Quantum digital signatures

Digital signatures are an important primitive in cryptography. Specifically, three security properties are required for signatures: unforgeability, nonrepudiation, and transferability [21]. Unforgeability guarantees a unique message signer, so no one else is able to forge a valid signature. Nonrepudiation requires that once a message is signed, the signer cannot deny the signature. Transferability means that a recipient who accepts a message can be sure that if the message is forwarded, another recipient will also accept the message, except with a probability that can be made arbitrarily low. QDS based on laws of quantum physics is able to satisfy these requirements, and achieve information-theoretic security [4]. Unconditionally secure signatures are also possible based on shared secret keys [21–24], and the scaling of secret key length with respect to message length can be more favorable than for quantum signatures. The secret shared key could be generated by QKD, but otherwise these schemes remain entirely 'classical'. On the other hand, the error rate threshold can be less strict for QDS than for QKD to distill shared secret keys [25].

References [26, 25] propose QDS protocols via insecure quantum channels, which later have been implemented [6, 7]. A significant difference between these two protocols is the stage of quantum state distribution. In [26], Alice sends the same quantum states to Bob and Charlie, while in [25], Bob and Charlie individually send different quantum states to Alice.

Both protocols are briefly introduced in the next subsection. A reader familiar with protocol implementation can, of course, skip to second subsection, where we discuss vulnerabilities.

Figure 1. Experimental setup for QDS implemented by Yin and his coworkers. Alice first prepares two pairs of pairs of horizontally (H) and vertically (V) polarized photons using two pairs of lasers followed by polarization beam splitters (PBS). One pair of H and V polarized photons are then rotated $\pi/4$ by a $\pi/4$ rotation beam splitter ($\frac{\pi}{4}$ RBS), becoming states $|+\rangle$ and $|-\rangle$. The variation in amplitude for the decoy states is implemented by an electrical variable optical attenuator (EVOA). Bob and Charlie each randomly choose one of two bases to detect the incoming states. Here, DWDM denotes a dense wavelength division multiplexer, BS denotes a beam splitter, EPC denotes an electric polarization controller, SNSPD denotes a superconducting nanowire single-photon detector, SynL denotes a synchronization laser, FPGA denotes a field programmable gate array. Reprinted figure with permission from [7] Copyright (2017) by the American Physical Society. DOI: https://doi.org/10.1103/PhysRevA.95.032334.

2.1. Protocol and implementation
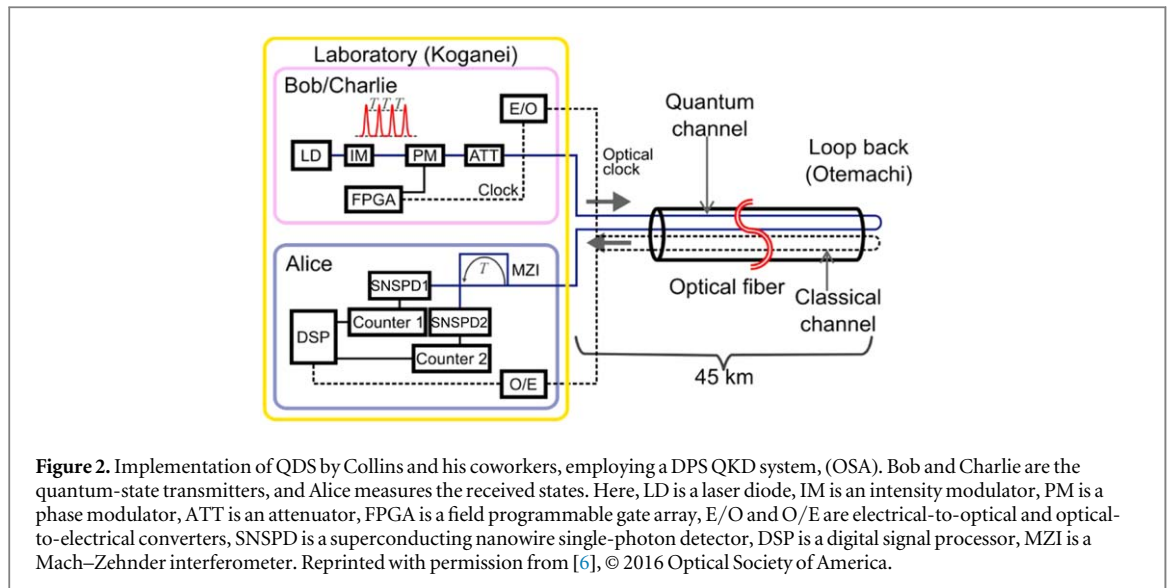
2.1.1. Identical-state-sharing

Reference [26] proposes a QDS protocol with a quantum-state sender, Alice, and two quantum-state receivers, Bob and Charlie. This protocol has been implemented over a distance of 102 km [7] as shown in figure 1. The protocol consists of two stages, a quantum stage, and a signing stage. In the quantum stage, for each future 1 bit message $m = 0$ or $m = 1$, Alice employs weak coherent states to randomly prepare two identical sequences of qubit states, and every individual state is in one of the Bennett–Brassard 1984 (BB84) polarization states $|H\rangle$, $|V\rangle$, $|+\rangle$ and $|-\rangle$ [2]. In addition, the decoy-state protocol [27] is used to randomly modulate the mean photon numbers of the weak coherent states, protecting the system from photon-number-splitting attacks [28]. Then one copy of the sequence is sent to Bob, and one copy to Charlie. A beam splitter is used to randomly and independently select the X or Z basis to measure the received states.

In a sifting phase, Bob and Charlie announce in which slots they obtain detections. For each detection slot, Alice then announces two nonorthogonal states from different bases, for example, $|H\rangle$ and $|+\rangle$. One of them is the real state she sent. If Bob (Charlie) obtains a measurement result corresponding to a state that is orthogonal to one of the states Alice announced, such as $|V\rangle$, then Bob (Charlie) conclusively knows that it is the other announced state, $|+\rangle$.

In the next stage, the signing stage, only classical processing takes place. It starts by announcing some of the states shared between Alice and Bob (Charlie) during the quantum stage to calculate an authentication threshold T_a (T_v) for Bob (Charlie). The unannounced states form strings denoted as S_{Am} for Alice, S_{Bm} for Bob and S_{Cm} for Charlie, and will be used for the digital signature. To send a signed 1 bit message m, Alice sends the message and the corresponding data string, (m, S_{Am}), to one of the recipients, say, Bob. Bob will accept this message if the mismatch rate of sifted bits between S_{Am} and S_{Bm} is less than T_a. If Bob wishes to forward the message to Charlie, he forwards (m, S_{Am}) to Charlie. Charlie will accept this message as well if the mismatch rate of the sifted bits between S_{Am} and S_{Cm} is less than T_v.

2.1.2. Different-state-sharing

Reference [25] proposes another QDS protocol that sends different quantum states from Bob and Charlie to Alice. This protocol has subsequently been implemented based on an installed differential-phase-shift (DPS) QKD system, as shown in figure 2 [6]. This protocol is also divided into two stages, a distribution stage and a messaging stage. In the distribution stage, Bob and Charlie randomly and independently select two different n-bit strings. Then, they encode the bits into quantum states according to the DPS QKD protocol [29]. For each future message $m = 0$ or $m = 1$, Bob (Charlie) applies a key-generating protocol (KGP) to share the bit string with Alice. The KGP can be treated as a partial QKD procedure without error correction and privacy amplification. Alice and Bob (Charlie) estimate the quantum bit error rate by announcing a small part of the shared bits. The remaining L-bit key is denoted by K_m^B (K_m^C) at Bob's (Charlie's) side. At Alice's side, she obtains a signature $Sig_m = (A_m^B, A_m^C)$ for a future message m. Then, to guarantee transferability, Bob and Charlie

Figure 2. Implementation of QDS by Collins and his coworkers, employing a DPS QKD system, (OSA). Bob and Charlie are the quantum-state transmitters, and Alice measures the received states. Here, LD is a laser diode, IM is an intensity modulator, PM is a phase modulator, ATT is an attenuator, FPGA is a field-programmable gate array, E/O and O/E are electrical-to-optical and optical-to-electrical converters, SNSPD is a superconducting nanowire single-photon detector, DSP is a digital signal processor, MZI is a Mach–Zehnder interferometer. Reprinted with permission from [6], © 2016 Optical Society of America.

randomly forward half of their keys, K_m^B and K_m^C, to each other. This classical bit exchange is encrypted by Bob and Charlie using a separate BB84 QKD system. This way, Alice receives no information on which bits have been forwarded and which bits have been kept. From her point of view, a bit she originally shared with Bob (Charlie) is now equally likely to be retained by Bob as by Charlie. Bob (Charlie) combine the non-exchanged part of K_m^B (K_m^C) and the received part of K_m^C (K_m^B) as a symmetric key, S_m^B (S_m^C).

In the messaging stage, Alice signs a message m by Sig_m, and then sends (m, Sig_m) to Bob. Bob checks the mismatch rate between Sig_m and S_m^B. If the mismatch rate is lower than the threshold s_a, Bob accepts the message. If Bob wishes to forward the message to Charlie, he forwards (m, Sig_m) to Charlie. Charlie also checks the mismatch rate between Sig_m and S_m^C, and accepts the message if the mismatch rate is lower than the threshold s_v. From Alices point of view, the situation is symmetric with respect to Bob and Charlie, so that if Bob accepts a signature, Charlie must accept it with high probability, provided acceptance thresholds are chosen correctly and differently for Bob and Charlie.

2.2. Hacking

Both protocols have been proven to be information-theoretically secure, based on different assumptions [25, 26]. In this section, we analyse the security assumptions for both protocols and illustrate how these assumptions might be broken. Since QDS realizations are based on QKD schemes with similar optical components, similar vulnerabilities exist. That is, some known attacks on QKD systems are applicable also to the realisations of QDS. In our analysis, we assume an external attacker Eve who is not a legitimate participant (Alice, Bob or Charlie) in the QDS protocol.

2.2.1. Identical-state-sharing protocol

The unforgeability of this protocol is based on the assumption that given two copies of quantum states, Eve cannot distinguish between all four states Alice might send without error before Alice's declaration [30]. However, in practice, if Eve were able to discriminate the states via a side channel, messages could be forged. Several side channels exist in the implementation [7], which could be exploited by Eve to hack it.

Source side channels are useful for Eve to learn the quantum state prepared by Alice. When quantum states are prepared by different laser diodes, side channels could exist both in time and frequency domains [31, 32]. In the implementation presented in [7], each laser diode prepares a specific state, and different laser diodes are used in a random order. To avoid the spectral side channel, the implementation controls the difference of the central wavelengths for all of these laser diodes in a narrow range (0.02 nm). Additionally, a dense wavelength division multiplexer with 100 GHz bandwidth is used as a filter before the states are sent out. However, a side channel might exist in another degree of freedom. For example, pulse emission time, pulse width and pulse shape may vary for different laser diodes. These mismatches give Eve a chance to distinguish different states [32]. If Eve is able to perfectly distinguish the quantum states, she could forge a copy of Alice's signature and send it to Bob and Charlie. However, usually, Eve can only partially distinguish the states. She may choose to perform different types of quantum measurements to maximize her distinguishability. For example, if Eve makes a measurement that sometimes gives her higher confidence in the result, such as an unambiguous quantum measurement, then she could forward a state only when her

measurement has succeeded. Thus, in this case, if losses are high enough, this strategy may not be noticed by the legitimate parties.

Measurements are usually more vulnerable than state preparation. One potential flaw hides in the beam splitter situated at the input of Bob's/Charlie's subsystem. The output ratio of the beam splitter might depend on the wavelength of the incoming light [33], which helps Eve during the intercept-resend attack. Eve first measures a state sent by Alice. According to the measurement result, Eve resends the measured state with a wavelength that makes the output ratio of the beam splitters become highly unbalanced, for example, 99:1 or 1:99. Then the resent state passes through Bob's/Charlie's beam splitter via one output with high probability, likely reaching the same measurement basis as Eve's. Thus, Eve, Bob and Charlie share almost the same detection results. At the sifting phase, Eve can wiretap the public announcement and follow the sifting rule described in the protocol, obtaining her signature string. After that, if the mismatch rate between Eve's and Bob's (Charlie's) strings is lower than T_a (T_v), Eve would be able to pretend to be Alice and send a signature to Bob (Charlie).

To force Bob and Charlie to obtain the same detection results as Eve during the intercept-resend attack, another possible tool is a detector blinding attack [9, 34, 35]. By applying this attack, Eve might be able to control all Bob's measurement results [9, 34, 35]. In this attack, Eve sends a strong laser to blind Bob's and Charlie's detectors such that they are no longer sensitive to single photons, but act as classical optical detectors. Then, during intercept-resend, Eve resends the measured states by energy-tailored pulses. The resent pulses trigger Bob's detections in the same basis and state as Eve's. If the detector blinding attack is possible in this QDS implementation, Eve could obtain a copy of the bits shared by Alice and Bob/Charlie after sifting. Thus, Eve could pretend to be Alice to sign a message. The detector blinding attack can maintain the normal detection statistics [36]. Furthermore, in a receiver that uses a beam splitter to passively choose bases and is vulnerable to the detector blinding attack, Eve can force a click with 100% probability [36]. If the digital signature scheme is built using detectors other than superconducting nanowire single-photon detectors used in the implementation shown in figure 1, other types of detector-control attacks may also apply, such as efficiency mismatch [37], after-gate [38], superlinearity [39], and deadtime [10].

2.2.2. Different-state-sharing protocol

In this protocol, unforgeability is based on the security of the KGP that guarantees $d(A_i^B, K_i^B) < d(E_{\text{guess}}, K_i^B)$ (with high probability), where d is the Hamming distance and E_{guess} is Eve's attempt at guessing K_i^B [25]. However, this property could be broken as well, if Eve can learn the states sent by Bob (Charlie) or forces Alice to detect the same result as hers. Similar to the previous protocol, the implementation might also contain several loopholes.

Alice's SNSPDs might be vulnerable to the detector blinding attack [9, 34, 35]. Similarly to the previous implementation, the SNSPDs might be blinded by a strong laser. Eve then does intercept-resend and sends Alice faked states whose power and phase are tailored [40]. Thus, Eve, Alice and Bob (Charlie) share the same bit string, which means $d(A_i^B, K_i^B) = d(E_{\text{guess}}, K_i^B)$.

At the source in Bob (Charlie), all the states are modulated by a phase modulator, which might open another loophole. The modulation information from the PM could be eavesdropped by a Trojan-horse attack [12, 19, 41, 42]. In this attack, Eve sends strong light to Bob (Charlie). The reflected light carries the modulation information, which could be measured from the phase difference between injected light and reflected light. It has been shown that around four reflected photons are sufficient to read out most of the information [12]. If the Trojan-horse attack is successful in the QDS system, Eve could get all Alice's information: $d(E_{\text{guess}}, K_i^B)$ could become equal to $d(A_i^B, K_i^B)$.
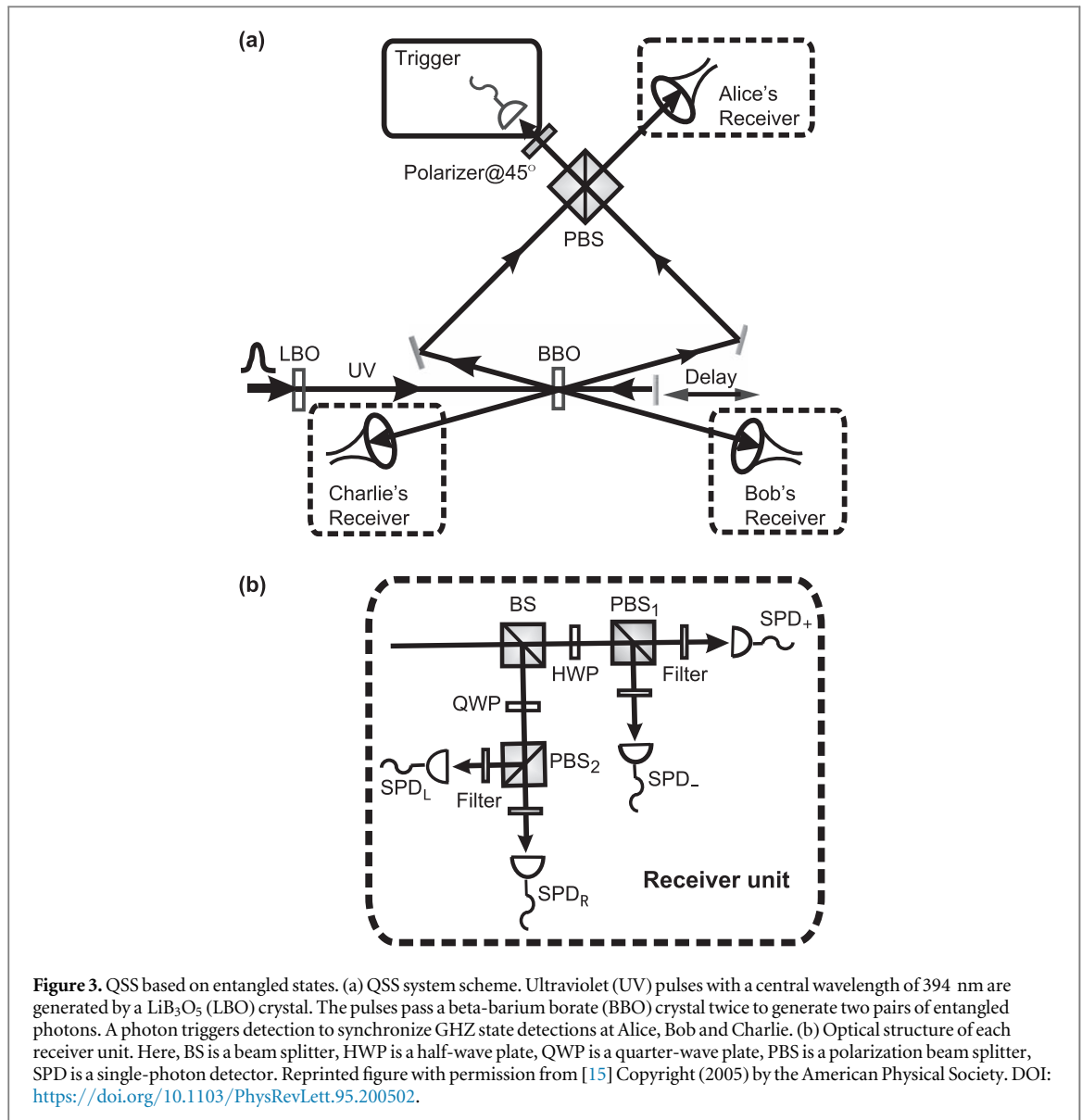
3. Quantum secret sharing

In secret sharing protocols, information is shared among many parties. The information can be reconstructed only if groups of parties collaborate. Information-theoretically secure secret sharing is possible not only using classical means (e.g., by pairwise shared keys), but also using quantum methods. Here, we focus on QSS [3]. Two types of QSS schemes, entanglement-based schemes [15] and single-qubit schemes [5], have been proposed for the sharing of classical messages. We survey both schemes.

3.1. Protocol and implementation

3.1.1. Entanglement-based protocol

In one scheme for entanglement-based QSS [15], Alice, Bob and Charlie first hold one photon each in a Greenberger–Horne–Zeilinger (GHZ) triplet, which is the state

Figure 3. QSS based on entangled states. (a) QSS system scheme. Ultraviolet (UV) pulses with a central wavelength of 394 nm are generated by a LiB$_3$O$_5$ (LBO) crystal. The pulses pass a beta-barium borate (BBO) crystal twice to generate two pairs of entangled photons. A photon triggers detection to synchronize GHZ state detections at Alice, Bob and Charlie. (b) Optical structure of each receiver unit. Here, BS is a beam splitter, HWP is a half-wave plate, QWP is a quarter-wave plate, PBS is a polarization beam splitter, SPD is a single-photon detector. Reprinted figure with permission from [15] Copyright (2005) by the American Physical Society. DOI: https://doi.org/10.1103/PhysRevLett.95.200502.

$$|\psi\rangle_{ABC} = \frac{1}{\sqrt{2}}(|H\rangle_A|H\rangle_B|H\rangle_C + |V\rangle_A|V\rangle_B|V\rangle_C). \tag{1}$$

Then, a projective measurement is performed on each photon randomly either in the X or Y basis, where the basis states are given by

$$|X_\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle), \quad |Y_\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm \mathrm{i}|V\rangle). \tag{2}$$

The GHZ states can be written as

$$|\psi\rangle_{ABC} = \frac{1}{2}[(|X_+\rangle_A|X_+\rangle_B + |X_-\rangle_A|X_-\rangle_B)|X_+\rangle_C + (|X_+\rangle_A|X_-\rangle_B + |X_-\rangle_A|X_+\rangle_B)|X_-\rangle_C]. \tag{3}$$

Thus, if each party measures in the X basis, the measurement results would show perfect correlations. Once any two measurement results are known, the third measurement result can be predicted with certainty. Similar correlation would be obtained for three other measurement combinations, $X_AY_BY_C$, $Y_AX_BY_C$, and $Y_AY_BX_C$. However, the remaining four basis combinations, $X_AX_BY_C$, $X_AY_BX_C$, $Y_AX_BX_C$, and $Y_AY_BY_C$, result in uncorrelated measurement results among the three parties. Thus, they could announce their basis choices to sift the basis combinations with perfect correlation. After that, Alice and Bob share their measurement results with each other to establish Charlie's key. Thus, a message encrypted by Charlie can be decrypted if Alice and Bob cooperate. The protocol implementation is shown in figure 3.

Figure 4. Single-qubit QSS. Alice randomly modulates the state, adding a phase of 0 or $\pi/2$. The rest of parties randomly choose a phase from $\{0, \pi/2, \pi, 3\pi/2\}$. Here, LD denotes a laser diode, ATT denotes an attenuator, SPD denotes a single-photon detector, CIR denotes a circulator, BS denotes a beam splitter, PBS denotes a polarization beam splitter, PM denotes a phase modulator, AM denotes an amplitude modulator, FM denotes a Faraday mirror. Reprinted figure with permission from [5] Copyright (2008) by the American Physical Society. DOI: https://doi.org/10.1103/PhysRevA.78.062307.

3.1.2. Single-qubit protocol

Instead of using entangled states, [43] proposed an N-party QSS protocol that uses a single qubit, which is easily realizable and scalable compared to the entanglement-based protocol. On the other hand, this protocol completely removes the possibility to share quantum information in terms of an entangled state. The information shared is necessarily classical. Reference [5] demonstrated this protocol. An initial qubit $|x\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ is prepared by party R_1, and sent from R_2 to R_N sequentially. Each party R_i ($i = 1, ...,$ $N - 1$) encodes information by applying a phase randomly chosen from two sets, $\{0, \pi\}$ and $\{\pi/2, 3\pi/2\}$, to the $|1\rangle$ component in the qubit $|x\rangle$. The party R_N randomly applies phase 0 or $\pi/2$ to the $|1\rangle$ component before measuring the state $|\pm x\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Thus, the detection probability of each detector is

$$P_{D1} = \frac{1}{2}\left[1 + \cos(\sum_{i=1}^{N} \phi_i)\right],$$

$$P_{D2} = \frac{1}{2}\left[1 - \cos(\sum_{i=1}^{N} \phi_i)\right]. \tag{4}$$

Half of the time, there is destructive or constructive interference, when $\cos(\phi_1 + \cdots + \phi_N) = \pm 1$. If all parties announce which set of phase values their choice belonged to, then every party knows which detection results are deterministic. Using the knowledge of which measurement results are deterministic, multiple parties can then share a secret as follows. If any $N - 1$ parties collaborate and share their modulating phases, they would be certain about the phase applied by the Nth party for one slot of the deterministic measurement. To maintain stability in the experiment, a bidirectional scheme is applied to implement a 5-party protocol [5] as shown in figure 4. Alice prepares the initial pulse without phase encoding and acts as R_5 to measure the final reflected state. The rest of parties encode their information on the way back from the Faraday mirror, after the pulse is attenuated to the single-photon level by the amplitude modulator. This idea is similar to the plug and play QKD system [44].

3.2. Hacking

We discuss one type of known attack that may work for the implementation of each aforementioned QSS protocol. An external Eve is assumed to be the attacker. If an external Eve can compromise the security, any inside attacker (a protocol participant) could also compromise security and obtain the secret without the cooperation of the other participants, because inside attackers have at least as much information as an outside attacker.

3.2.1. Blinding attack on entanglement-based implementation

In the entanglement-based QSS scheme mentioned above, three parties securely share a secret string using a GHZ state that has inherent correlations among the three photons. If Eve would like to perform an intercept-resend attack via a quantum channel, she would break the initial correlation between the three entangled photons, and thus introduce errors [45]. However, the detector blinding attack (see section 2.2.1) could help Eve steal the shared secret while introducing no error. Eve performs two independent detector blinding attacks on

Alice's and Bob's detectors. The blinded detectors only click when Alice/Bob chooses the same measurement bases as Eve during an intercept-resend attack. Thus, Alice's and Bob's secret strings could be obtained by Eve to let her learn Charlie's key. Alternatively, instead of hacking Alice and Bob, Eve can directly blind Charlie's detectors to control the secret key he obtains.

3.2.2. Trojan-horse attack on single-qubit implementation
The security of single-qubit QSS follows the proven BB84 QKD protocol [43]. Similarly to BB84 protocol, an intercept-resend attack on the QSS introduces 25% error in the final detection results. However, the implementation might have side channels that leak information about state preparation, allowing Eve to learn the shared secret without disturbing the normal QSS protocol.

In the implementation scheme of single-qubit QSS shown in figure 4, similar to QKD systems, the phase modulation is implemented by a phase modulator which may be vulnerable. Thus, the Trojan-horse attack (see section 2.2.2) appears to be a high risk, owing to the pass-through nature of every party except for Alice. Eve could send strong light to each party, excluding Alice, and then at the other side of each party receive the light modulated by the PM. By measuring the phase difference between Eve's original coherent light and the modulated light, she could read the phase modulation. In this way, Eve could know the secret shared among the four parties. In general, this hacking strategy works for N parties. An attack on Alice may also be attempted, however, it is more difficult owing to the presence of SPDs in Alice [46].

4. SI quantum random number generation

Quantum random number generation (QRNG) based on the uncertainty principle in quantum mechanics can be used to provide pure random numbers, a crucial resource in cryptography [47]. Similarly to QKD, a QRNG system also consists of quantum state preparation and measurement, however, the states are measured locally without long-distance transmission. SI QRNG protocols [16, 48, 49] assume that the state preparation setup is untrusted, while the measurement setup is trusted. We survey the protocol in [16] and its experimental demonstration.
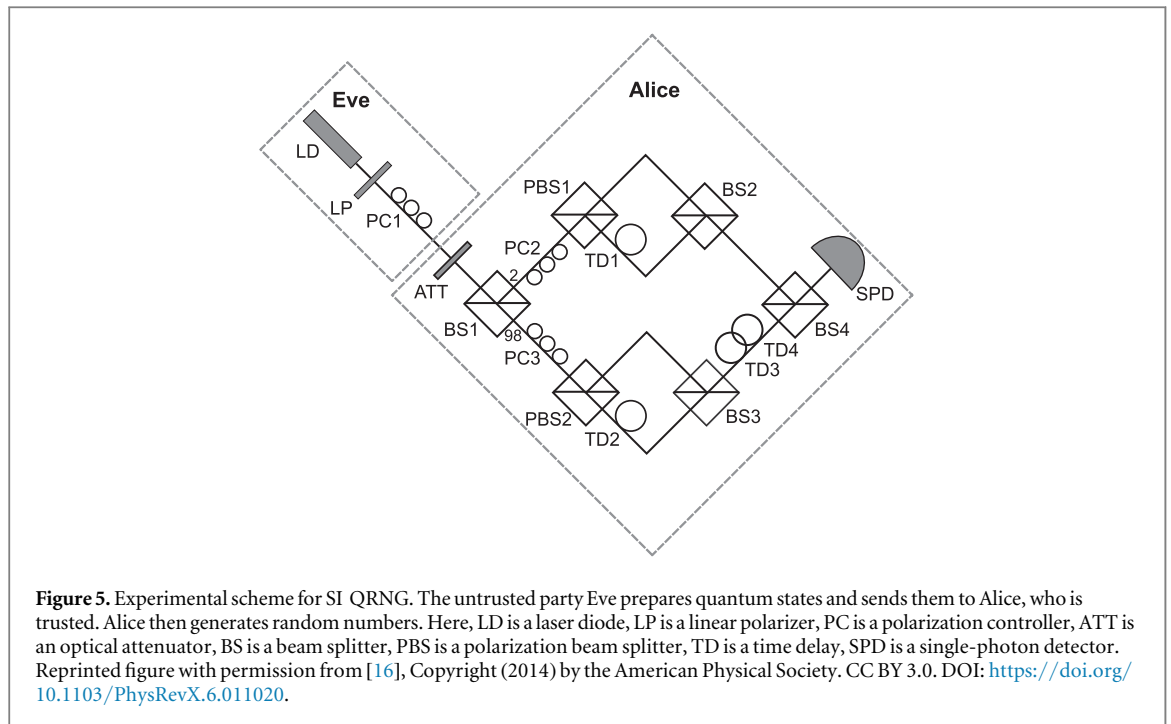
4.1. Protocol and implementation
In the SI QRNG protocol, an untrusted party Eve prepares single-qubit states $|+\rangle$ and sends them to Alice's measurement station [16]. Alice first projects the quantum states into qubits $|+\rangle$ and vacuum states, but it is unclear how to implement this operation in practice. Assume that n squashed qubits are obtained during the operation of the protocol. The resulting single qubits are then randomly measured either in the X basis, $\{|+\rangle, |-\rangle\}$, or the Z basis, $\{|H\rangle, |V\rangle\}$. If n_x out of the n squashed qubits are measured in the X basis, they should be detected as $|+\rangle$ ideally. The detection rate for $|-\rangle$ is treated as the estimated error rate e_{bx}. The remaining $n_z = n - n_x$ qubits are measured in the Z basis to generate n_z random bits. Alice then extracts the final secure random bits from n_z, which is equivalent to privacy amplification in QKD.

The experimental demonstration is shown in figure 5. Weak coherent pulses are prepared with $|+\rangle$ polarization by a linear polarizer and a polarization controller (PC1). At Alice's side, a beam splitter (BS1) with splitting ratio 2:98 is used to passively choose the X or Z basis. In figure 5, the upper and lower paths correspond to the X basis and Z basis respectively. A single-photon detector is time-division-multiplexed by using four time delays TD1–TD4. For each coherent state Eve sends, a click in the first detection slot indicates that Alice chooses the X basis and correctly detects the incoming pulse as $|+\rangle$, while a click in the second slot indicates a wrong detection, $|-\rangle$, which is used for the error estimation. Moreover, a click in the third slot indicates that Alice selects the Z basis and obtain the result $|H\rangle$, while a click in the fourth slot indicates the result $|V\rangle$.

4.2. Hacking
This SI QRNG protocol assumes that the source can be untrusted, but the measurement station is trusted and characterized [16]. However, it is not clear how to guarantee the latter requirement in practice. Therefore, Eve might be able to prepare fake states to generate nonrandom numbers. The detector blinding attack (see section 2.2.1) could force the SPD to work as a classical detector. Then Eve could send a strong bright pulse to trigger a detection in the first slot. Then she sends another bright pulse with either the state $|H\rangle$ or $|V\rangle$ to control the detection in the third or fourth slot. The attack can result in equal detection rates for $|H\rangle$ and $|V\rangle$, which looks like random clicks to Alice, while being precisely controlled by Eve. Eve actually thus controls the bit string.

Another potential issue is the wavelength-dependent attack, because the splitting ratio of a beam splitter might be sensitive to the wavelength of the incoming light (see section 2.2.1). All four beam splitters in the measurement station might be affected. By controlling the splitting ratio of BS1 and/or BS4, Eve can bias whether error checking or random bit generation happens. For BS2 and BS3, by manipulating the splitting ratio,

Figure 5. Experimental scheme for SI QRNG. The untrusted party Eve prepares quantum states and sends them to Alice, who is trusted. Alice then generates random numbers. Here, LD is a laser diode, LP is a linear polarizer, PC is a polarization controller, ATT is an optical attenuator, BS is a beam splitter, PBS is a polarization beam splitter, TD is a time delay, SPD is a single-photon detector. Reprinted figure with permission from [16], Copyright (2014) by the American Physical Society. CC BY 3.0. DOI: https://doi.org/10.1103/PhysRevX.6.011020.

Eve is able to partially control the results of error checking and bit generation. Please note that a wavelength filter alone will not protect the system from this attack, because Eve could send bright states to overcome the finite extinction ratio in the filter's stopband.

5. Quantum secure direct communication

QSDC transmits secret information directly through a quantum channel, instead of establishing a secret key first [50]. The initial QSDC protocol is based on entangled pairs [51–53]. However, entanglement is not a necessary condition for QSDC The first single-photon QSDC protocol, Deng-Long 2004 (DL04), was proposed in [54]. Recently, researchers started studying the strict security proof of this DL04 protocol [55]. However, regarding the practical security, the implementation of this protocol also needs to be investigated. Also, more attention may need to be paid to the motivation for secure direct communication.

5.1. Protocol and implementation

The DL04 protocol contains two phases of channel estimation and a phase of secret transmission. The first channel estimation checks the security of the channel from Alice to Bob. Alice prepares a sequence of photons randomly chosen from the set of states $|H\rangle$, $|V\rangle$, $|+\rangle$, and $|-\rangle$, and sends them to Bob. He randomly selects a portion of the received photons, and randomly measures them in the X or the Z basis. Then Bob announces the measurement results and compares them to Alice's prepared states to calculate an error rate. Only when the error rate is lower than a threshold, Alice and Bob trust the channel and continue to the next step. Bob randomly selects another small portion of the received photons, and applies one of two unitary operations to each of them: $U = |0\rangle\langle 1| - |1\rangle\langle 0|$ or $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, i.e., flipping a state or not. These photons are employed to check the security of the channel from Bob to Alice. The rest of the photons received by Bob are used to encode secret information by randomly applying the operator U or I to each photon. All these photons are then sent to Alice, who measures these photons in the preparation bases. Regarding the photons used for the security check, Alice checks if her measurement result is compatible with Bob's operation to estimate the error rate. Once the error rate is lower than a threshold, they trust the channel from Bob to Alice. The remaining photons measured in their preparation bases allow Alice to deterministically know Bob's operation, obtaining the secret information.

The protocol is implemented by the setup shown in figure 6 [17]. Alice prepares the initial photon string and measures the photons encoded by Bob. She first prepares $|H\rangle$ and $|V\rangle$ using two laser diodes. The preparation and measurement bases are selected by PC_1 and PC_2 respectively. Bob encodes his information by PC_3. All the basis choices are controlled by field programmable gate arrays. The channel from Alice to Bob is denoted forward channel, and the channel from Bob to Alice is denoted backward channel. A beamsplitter at Bob's side selects a small portion of the received photons, and then a control module is used to check the security of the forward channel. The control module's scheme is the same as the passive measurement station in BB84 QKD

Figure 6. QSDC implementation. Alice prepares and measures states, and Bob encodes the secret message by manipulating the states. Here, LD is a laser diode, PBS is a polarization beam splitter, ATT is an optical attenuator, PC is a polarization controller, BS is a beam splitter, CM is a control module, FPGA is a field programmable gate array, SPD is a single-photon detector. Reproduced from [17].

system. A delay line is used to store the photons during the forward-channel check. To tolerate photon loss during secret transmission, a special method named single-photon frequency encoding is used. Instead of encoding information on individual photons, this method encodes information on the spectrum of a sequence of photons. After Alice detects a sequence of photons and converts them to a binary bit string, the spectrum can be known by applying the Fourier transform to the bit string. During the detection, Alice might miss some photons due to channel loss and imperfect detection efficiency. Fortunately, because the information does not only rely on an individual photon, but is determined by the spectrum of the entire sequence, missing some photons just reduces the signal-to-noise ratio, but the feature of the spectrum still exists [17]. The calculated spectrum corresponds to the bit string that is the initial information Bob sent.

5.2. Hacking

The first phase of the DL04 QSDC protocol, the security check of the forward channel, is similar to the raw key exchange, sifting and error estimation phases in the BB84 QKD protocol [2]. The security check of the backward channel and secret direct transmission are quantum versions of the one-time pad, which randomly flips the bit information [54]. Just as for QKD, the implementation [17] may contain side channels.

The first potential side channel is that detectors may be attacked by the detector blinding attack (see section 2.2.1). During the check of the forward channel, Eve blinds the detectors in the control module and conducts an attack with fake states [56] to control Bob's detection results. Since this attack introduces no errors, the security check is passed. During the second check of the backward channel and information transmission, Eve uses classical optical detectors to measure her bright pulses modulated by Bob. Since these are states resent by Eve during the previous phase, Eve could apply the same basis as in the previous step to know with certainty what operation Bob performed. Then, she sends the same states with proper brightness to Alice's blinded detectors, such that only when Alice selects the same bases as Eve, Alice obtains detections. This attack results in full control of Alices measurement outcomes. Again, no extra errors are introduced. Furthermore, Eve learns the secret information between Alice and Bob. This breaks the security of QSDC. Please note that because this implementation uses an active basis choice (the basis is actively selected by the polarization controller), Eve's measurement basis can only match Alice's/Bob's measurement basis half the time. However, when the basis matches the click probability in Bob under attack can be unity, while his single-photon detection efficiency is typically much lower than unity [9]. This may compensate for the extra loss introduced by the attack.

The second possible side channel exists in the polarization controllers that might be vulnerable to the Trojan-horse attack (see section 2.2.2). In this QSDC implementation [17], Eve can conduct the Trojan-horse attack on PC_1 or PC_3. From an attack on PC_1, Eve would know Alice's basis choice in the state preparation and measurement, as PC_2 applies the same basis as PC_1. The difference between the prepared and the measured state is Bob's secret information (flip or not). On the other hand, Bob's encoded information could be directly known by hacking PC_3 (similarly to section 3.2.2). Once Eve knows the original states prepared by Alice or what Bobs modulation was, she could obtain the secret information.

6. Blind quantum computing

In the future, a quantum computer could be used as a server that provides quantum computation capability to remote users, who themselves do not have a quantum computer and only use simple technology. A key task is to

Figure 7. Proof-of-principle implementation of BQC. Entangled photon pairs are generated from non-collinear type-II spontaneous parametric down-conversion process in BBO crystal. The horizontal and vertical polarization represents $|0\rangle$ and $|1\rangle$. From [18]. Reprinted with permission from AAAS.
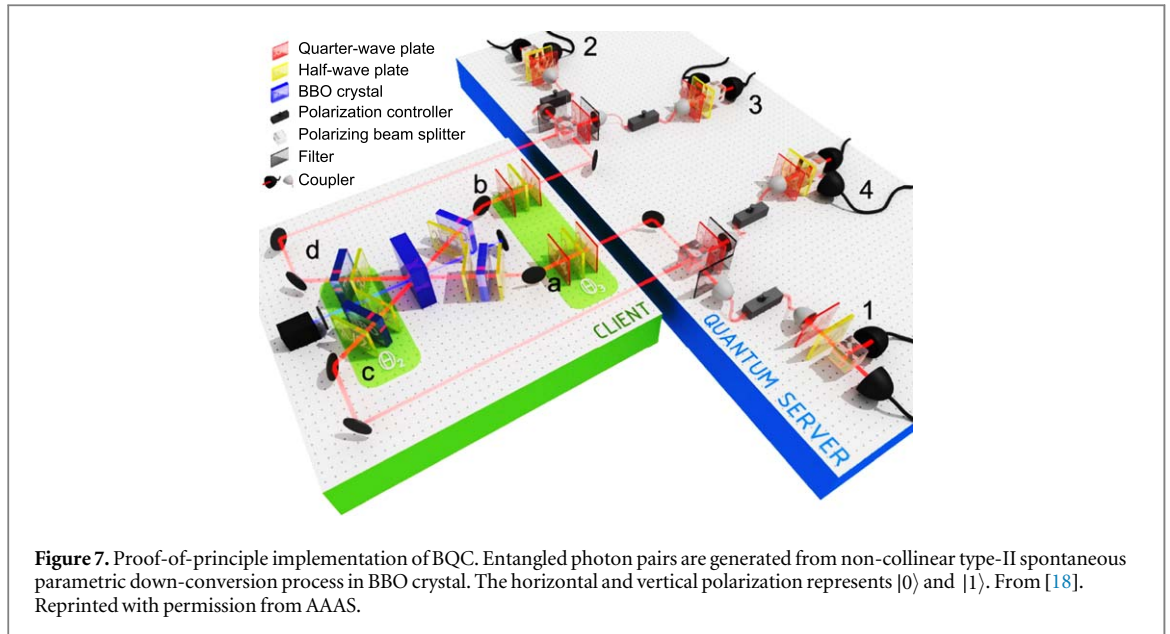
keep the client's data and program secret from the server. Classical blind computing protocols exist [57], but it can only guarantee computational security [18]. However, taking advantage of quantum mechanics, BQC is able to provide unconditional security for client's data and computation in the quantum computer server [58].

6.1. Protocol and implementation

BQC is based on entangled multiparticle cluster states [18]. In the BQC protocol, qubits are first prepared as $|\theta_j\rangle = (|0\rangle + e^{i\theta_j}|1\rangle)/\sqrt{2}$ by a client, where θ_j is randomly selected from $\{0, \pi/4, ..., 7\pi/4\}$. Then the single-photon qubits are sent to a quantum server that entangles them with each other by applying controlled-phase gates, so that the qubits form a cluster state. Then the cluster state is measured by the quantum server, which performs single-qubit measurements in the basis $|\pm_{\delta_j}\rangle = (|0\rangle + e^{i\delta_j}|1\rangle)/\sqrt{2}$. The measurement basis is instructed by the client: $\delta_j = \phi_j + \theta_j + \pi r_j$, where ϕ_j is the desired rotation and r_j is randomly chosen from $\{0, 1\}$. Since θ_j is the initial phase hidden from the quantum server, the server is not able to calculate the desired rotation ϕ_j from the measurement result. It is remarkable that for the cluster state, its shape, such as the dimension, also may leak information about the operation gates. Thus, also the shape of the cluster state is required to be hidden, which can be accomplished by choosing, for example, brickwork states [18]. The BQC protocol then completes a quantum computation while preserving the client's privacy.

Theoretically, the client only needs to have a single-photon source to generate a state $|\theta_j\rangle$ and send it to the server. However, implementing a single-photon source is challenging so far, as standard parametric down-conversion sources always also have higher-order emissions, meaning that instead of one pair, two or more pairs are emitted at the same time. An initial demonstration of the BQC protocol with current technology is shown in figure 7 [18]. Note that in the current implementation, entangled pairs are first prepared on the client's side, and the cluster state is generated on the server's side. The laser beam passes a BBO crystal to first generate the entangled pair traveling forwards. Then the beam is reflected and passes the BBO crystal again to generate the entangled pair traveling backwards. The initial phase θ_j is applied by rotating the angles of half-wave plates and quarter-wave plates, serving as modulators. Then the entangled states are sent to the quantum server's side, where a cluster state is generated. The states are measured in different bases, as instructed by the client. In this BQC protocol, the setup of the client is relatively simple, but the setup of the quantum server would have more capabilities once a real quantum computer is available. Here we take one type of BQC protocol as an example. There also exist other versions of BQC where the server generates entangled cluster states and the measurements are done by the client [59, 60].

6.2. Hacking

In the above subsection, a proof-of-principle implementation of BQC was introduced. Although in the future the technology available to implement the quantum server for BQC will be more mature and comprehensive, the client setup is already relatively clear. It is foreseeable that future client station will likely still consist of a photon source and modulators. Unfortunately, in practice, any kind of modulator is susceptible to the Trojan-horse attack [12, 19, 41, 42]. This vulnerability breaks an important assumption in BQC: the initial phase θ_j should be unknown to the untrusted quantum server. Specifically, regarding the implementation shown in figure 7, the
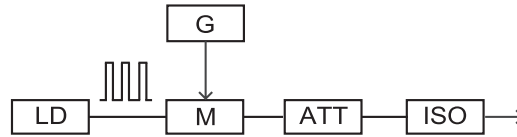
Figure 8. The scheme of countermeasures against source imperfections. To eliminate the mismatch among different laser diodes, a single laser diode LD followed by a modulator M can be used. The following attenuator ATT and isolator ISO provide sufficient isolation to prevent the Trojan-horse attack in a unidirectional system. Here, G denotes a modulation signal generator.

phase modulation is done by the wave plates. The reflected light from the wave plates may leak information about θ_j. Instead of wave plates, an advanced setup in the future could be using phase modulators to randomly modulate the phase θ_j, which is a technique widely used in quantum cryptography [5, 6, 61]. Unfortunately, the Trojan-horse attack might still be applied to phase modulators, as we have discussed in section 2.2.2.

Except for imperfect phase modulation, another possible issue is the photon source itself. For the current version of implementation, the entanglement source sometimes might simultaneously emit multiple pairs of entangled states. In this case, Eve could split off a copy of entangled states from the source. Then measuring her copy would give Eve information about the state itself. Even in future implementations, when ideal single-photon sources are available, one still needs to pay attention to state generation. For instance, the BQC protocol needs indistinguishable multiple photons [18]. Thus, careful source design is crucial to avoid any distinguishability in the generated photons (this can, in principle, occur in any degree of freedom, for example wavelength).

For other variations of BQC protocols, where the measurements are done on the client's side [59, 60], attacks that leak information about the measurement settings are applicable. So, in a setting where the client uses wave plates to choose a measurement basis [60], the Trojan-horse attack could be applied as well.

7. Countermeasures

An imperfect implementation compromises the security promised in theory, as we have argued in sections 2–6. To patch the practical loopholes, we should consider feasible countermeasures in implementations of quantum cryptographic protocols. Existing countermeasures for QKD and countermeasures under development may be adaptable to implementations of other cryptographic protocols. However, integrating these considerations into the relevant security proofs is an open challenge. We now recap countermeasures proposed in the literature for both the source and measurement parts of a quantum cryptographic system. We also discuss how they may be applied to the protocols surveyed in this Article.

7.1. Countermeasures against source imperfection

Properly implementing the quantum-state source in the above protocols requires that any other degrees of freedom are uncorrelated with the degree of freedom where information is encoded. However, for the states prepared by different laser diodes (see section 2.1.1), the laser diodes may show the inherent difference in the spectrum and emission time. These types of difference hint which laser diode is on, i.e., which state is prepared. The mismatch in a certain degree of freedom could be a side channel for Eve who tries to distinguish different quantum states [31, 32]. To avoid this inherent mismatch among different laser diodes, quantum state preparation could use only one laser diode followed by optical modulators (figure 8), as shown in many QKD implementations [62–64]. The laser diode generates identical pulses. Then different states are modulated by a phase modulator [62], intensity modulator [63], or polarization modulator [64].

The external modulation method could be applied to the implementation of double-receiver QDS (see section 2.1.1). However, this modification might open another loophole: the Trojan-horse attack on the modulators. Once a system uses a modulator, countermeasures against Trojan-horse attack are required. For a unidirectional system that only sends states from one party to another but never back, a possible countermeasure is adding enough isolation between the modulator and the output port connected to the quantum channel, as shown in figure 8. The amount of isolation is defined by the combination of bidirectional attenuation from attenuators, the unidirectional attenuation from isolators and total reflection probability from lasers and modulators. For example, in a BB84 QKD system, the isolation has been quantified as the following [65]. Suppose Eve injects pulsed light into the party preparing the state. The injected power is limited by the maximum power transmitted safely through standard single-mode fiber (assumed to be 12.8 W in [65]). The amount of reflection then is obtained after the injected light is attenuated by the system isolation. Taking this amount of reflection into account in the calculation of the key rate, one could obtain the final secure key rate. To

obtain a key rate under the Trojan-horse attack that is close to the rate without an attack, 170 dB isolation is required [65].

A similar methodology could be applied to single-receiver QDS, QSDC, and BQC, which may be vulnerable to the Trojan-horse attack. In each implementation, attenuators and isolators could be added between the modulators and system output, and the reflectivity of modulator and laser diodes should be quantified. Then the required amount of isolation should be calculated according to the security models of the corresponding protocol as has already been done for QKD [65]. The chosen amount of isolation should maintain the system's security properties. We notice that in the implementation of single-receiver QDS in [25], an attenuator is already included to weaken the output power to single-photon level. However, this amount of attenuation is probably not sufficient to provide isolation to counter the Trojan-horse attack.

For a bidirectional plug and play QSS system (see section 3.1.2) and pass-through QSDC (see section 5), the system's isolation in the previous countermeasure is not applicable, because it would block transmission of the states. In the bidirectional system, single-photon monitors would be needed to observe the incoming light [41]. It is not clear if implementing such countermeasure securely is realistic. Nevertheless, a patent by Trifonov and Vig [66] proposes a scheme against Trojan-horse attack with a single-photon watchdog detector. This countermeasure could be adapted for the single-qubit QSS implementation. Alice could employ a watchdog detector for the received light. The rest of parties in the scheme could use two watchdog detectors to observe two fiber connection ports at each side of the PM. Any alarm would abort the protocol. Please note that the single-photon detector might be vulnerable to the detector blinding attack. Thus, a corresponding countermeasure against detector control attacks is necessary, which is discussed in the next subsection.

7.2. Countermeasures against measurement imperfection

In a party that makes measurements, characteristics of passive optical components, such as beam splitters, might be sensitive to wavelength. That is, the component's behavior for unexpected wavelengths may deviate from what is assumed. To provide practical security, wavelength dependence should be eliminated. A possible method is using a wavelength filter to block unexpected wavelengths, and only pass a narrow range around the working wavelength [65]. In the implementation of double-receiver QDS (see section 2.1.1), this filter could be added before the beam splitter in Bob and Charlie, i.e., right at their input ports. The filter's transmission should be verified in a wide range of wavelengths. However, there is a limitation to this approach: Eve can simply increase her light power to pass through the stopband. Therefore, as a more robust countermeasure, we suggest utilizing active basis choice in the measurement station.

Another major vulnerability in measurement setups is imperfections in single-photon detectors (see section 2.2.1). A proposed countermeasure for QKD systems is calibrating the characteristics of detectors in real time, avoiding Eve's manipulation [67]. In this receiver design, a calibrated light source is locally included in the measurement unit, in combination with several other countermeasures. By randomly activating this local source to send photons to the detectors, the corresponding detection efficiency can be calibrated during the system operation. The characterized detection efficiency can then be used in the security proof to calculate the secure key rate. A similar design might be applicable to measurement stations in the other quantum cryptographic protocols. However, incorporating the calibration procedure into their security models should be studied in each case.

Another approach to entirely avoid the effect of imperfect detectors and other measurement imperfections are measurement-device-independent (MDI) quantum cryptographic protocols [68], such as MDI QKD [69], MDI QSS [70] and MDI QDS [71, 72]. In the MDI protocols, the party making measurements is untrusted: there are no security assumptions regarding the measurements. Even if Eve makes the measurements, the secret information (provided the protocol produces it) can still be distributed among the rest of the authenticated parties. This is a promising idea to avoid security loopholes related to the measurements. However, state preparation remains trusted and still needs to be carefully designed to avoid loopholes.

8. Conclusion

We have surveyed implementations of five types of quantum cryptographic primitives. As our analysis shows, these quantum cryptographic systems might have security loopholes similar to QKD systems, because they use similar optical components. These imperfections would compromise the security properties of each quantum cryptographic protocol (see summary in table 1). We discuss implementations of these protocols, showing that practical insecurity is a common issue in the implementation of quantum cryptography in general, not only in QKD. In other words, a gap between perfect theory and imperfect practice generally exists in quantum cryptography.

Our analysis of imperfections in this survey has been intended to reveal a broad picture. Detailed analysis of imperfections for each specific implementation should be done in the future. Once the existence of practical loopholes has been noticed, it becomes essential to bridge the gap between theory and practice. One should consider countermeasures when implementing existing protocols or designing new quantum cryptographic protocols that tolerate practical imperfections. Fortunately, these approaches appear to be feasible. However, integrating imperfections into security proofs [27, 65, 73] is a significant challenge, which should be addressed in future studies.

Acknowledgments

ORCID iDs

Anqi Huang ⓘ https://orcid.org/0000-0002-3989-000X

References

[1] Quantum safe cryptography and security, ETSI white paper no. 8 2015, http://etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf
[2] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore, India)* (New York: IEEE Press) pp 175–9
[3] Cleve R, Gottesman D and Lo H-K 1999 *Phys. Rev. Lett.* **83** 648
[4] Gottesman D and Chuang I 2001 arXiv:quant-ph/0105032
[5] Bogdanski J, Rafiei N and Bourennane M 2008 *Phys. Rev.* A **78** 062307
[6] Collins R J, Amiri R, Fujiwara M, Honjo T, Shimizu K, Tamaki K, Takeoka M, Andersson E, Buller G S and Sasaki M 2016 *Opt. Lett.* **41** 4883
[7] Yin H-L *et al* 2017 *Phys. Rev.* A **95** 032334
[8] Zhao Y, Fung C-H F, Qi B, Chen C and Lo H-K 2008 *Phys. Rev.* A **78** 042333
[9] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 *Nat. Photon.* **4** 686
[10] Weier H, Krauss H, Rau M, Fürst M, Nauerth S and Weinfurter H 2011 *New J. Phys.* **13** 073024
[11] Sun S-H, Jiang M-S and Liang L-M 2011 *Phys. Rev.* A **83** 062331
[12] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C and Leuchs G 2014 *New J. Phys.* **16** 123030
[13] Sajeed S, Chaiwongkhot P, Bourgoin J-P, Jennewein T, Lütkenhaus N and Makarov V 2015 *Phys. Rev.* A **91** 062301
[14] Makarov V, Bourgoin J-P, Chaiwongkhot P, Gagné M, Jennewein T, Kaiser S, Kashyap R, Legré M, Minshull C and Sajeed S 2016 *Phys. Rev.* A **94** 030302
[15] Chen Y-A, Zhang A-N, Zhao Z, Zhou X-Q, Lu C-Y, Peng C-Z, Yang T and Pan J-W 2005 *Phys. Rev. Lett.* **95** 200502
[16] Cao Z, Zhou H, Yuan X and Ma X 2016 *Phys. Rev.* X **6** 011020
[17] Hu J-Y, Yu B, Jing M-Y, Xiao L-T, Jia S-T, Qin G-Q and Long G-L 2016 *Light Sci. Appl.* **5** e16144
[18] Barz S, Kashefi E, Broadbent A, Fitzsimons J F, Zeilinger A and Walther P 2012 *Science* **335** 303
[19] Sajeed S, Radchenko I, Kaiser S, Bourgoin J-P, Pappa A, Monat L, Legré M and Makarov V 2015 *Phys. Rev.* A **91** 032326
[20] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Scarani V, Makarov V and Kurtsiefer C 2011 *Phys. Rev. Lett.* **107** 170404
[21] Swanson C M and Stinson D R 2011 *Int. Conf. on Information Theoretic Security* vol 6673 (Berlin: Springer) pp 100–16
[22] Chaum D and Roijakkers S 1990 *Conf. on the Theory and Application of Cryptography* (Berlin: Springer) pp 206–14
[23] Hanaoka G, Shikata J, Zheng Y and Imai H 2000 *International Conf. on the Theory and Application of Cryptology and Information Security* (Berlin: Springer) pp 130–42
[24] Amiri R, Abidin A, Wallden P and Andersson E 2016 *IACR Cryptology ePrint Archive* **2016** 739
[25] Amiri R, Wallden P, Kent A and Andersson E 2016 *Phys. Rev.* A **93** 032325
[26] Yin H-L, Fu Y and Chen Z-B 2016 *Phys. Rev.* A **93** 032316
[27] Ma X, Qi B, Zhao Y and Lo H-K 2005 *Phys. Rev.* A **72** 012326
[28] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[29] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[30] Chefles A 2001 *Phys. Rev.* A **64** 062305
[31] Nauerth S, Fürst M, Schmitt-Manderbach T, Weier H and Weinfurter H 2009 *New J. Phys.* **11** 065001
[32] Huang A, Sun S-H, Liu Z and Makarov V 2018 *Phys. Rev.* A **98** 012330
[33] Li H-W *et al* 2011 *Phys. Rev.* A **84** 062308
[34] Lydersen L, Akhlaghi M K, Majedi A H, Skaar J and Makarov V 2011 *New J. Phys.* **13** 113042
[35] Tanner M G, Makarov V and Hadfield R H 2014 *Opt. Express* **22** 6734
[36] Gerhardt I, Liu Q, Lamas-Linares A, Skaar J, Kurtsiefer C and Makarov V 2011 *Nat. Commun.* **2** 349
[37] Makarov V, Anisimov A and Skaar J 2006 *Phys. Rev.* A **74** 022313
    Makarov V, Anisimov A and Skaar J 2008 *Phys. Rev.* A **78** 019905
[38] Wiechers C, Lydersen L, Wittmann C, Elser D, Skaar J, Marquardt C, Makarov V and Leuchs G 2011 *New J. Phys.* **13** 013043
[39] Lydersen L, Jain N, Wittmann C, Marøy Ø, Skaar J, Marquardt C, Makarov V and Leuchs G 2011 *Phys. Rev.* A **84** 032320

[40] Lydersen L, Skaar J and Makarov V 2011 *J. Mod. Opt.* **58** 680

[41] Vakhitov A, Makarov V and Hjelme D R 2001 *J. Mod. Opt.* **48** 2023

[42] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev.* A **73** 022320

[43] Schmid C, Trojek P, Bourennane M, Kurtsiefer C, Żukowski M and Weinfurter H 2005 *Phys. Rev. Lett.* **95** 230505

[44] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H and Gisin N 1997 *Appl. Phys. Lett.* **70** 793

[45] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829

[46] Sajeed S, Minshull C, Jain N and Makarov V 2017 *Sci. Rep.* **7** 8403

[47] Herrero-Collantes M and Garcia-Escartin J C 2017 *Rev. Mod. Phys.* **89** 015004

[48] Vallone G, Marangon D G, Tomasin M and Villoresi P 2014 *Phys. Rev.* A **90** 052327

[49] Marangon D G, Vallone G and Villoresi P 2017 *Phys. Rev. Lett.* **118** 060503

[50] Deng F-G, Long G-L and Liu X-S 2003 *Phys. Rev.* A **68** 042317

[51] Wang C, Deng F-G, Li Y-S, Liu X-S and Long G-L 2005 *Phys. Rev.* A **71** 044305

[52] Wang C, Deng F-G and Long G-L 2005 *Opt. Commun.* **253** 15

[53] Wang T-J, Li T, Du F-F and Deng F-G 2011 *Chin. Phys. Lett.* **28** 040305

[54] Deng F-G and Long G-L 2004 *Phys. Rev.* A **69** 052319

[55] Hu J, Jing M, Zhang P, Zhang Q, Hou H, Xiao L and Jia S 2017 arXiv:1706.03234

[56] Makarov V and Hjelme D R 2005 *J. Mod. Opt.* **52** 691

[57] Rivest R L, Adleman L and Dertouzos M L 1978 *Foundations of Secure Computation* (Orlando, FL: Academic) pp 169–80

[58] Broadbent A, Fitzsimons J and Kashefi E 2009 *Proc. 50th Annual IEEE Symp. on Foundations of Computer Science* (Los Alamitos, CA: IEEE Computer Society) pp 517–26

[59] Morimae T and Fujii K 2013 *Phys. Rev.* A **87** 050301

[60] Greganti C, Roehsner M-C, Barz S, Morimae T and Walther P 2016 *New J. Phys.* **18** 013020

[61] Takesue H, Diamanti E, Honjo T, Langrock C, Fejer M M, Inoue K and Yamamoto Y 2005 *New J. Phys.* **7** 232

[62] Stucki D, Gisin N, Guinnard O, Ribordy G and Zbinden H 2002 *New J. Phys.* **4** 41

[63] Stucki D, Walenta N, Vannel F, Thew R T, Gisin N, Zbinden H, Gray S, Towery C R and Ten S 2009 *New J. Phys.* **11** 075003

[64] Tang Z, Liao Z, Xu F, Qi B, Qian L and Lo H-K 2014 *Phys. Rev. Lett.* **112** 190503

[65] Lucamarini M, Choi I, Ward M B, Dynes J F, Yuan Z and Shields A J 2015 *Phys. Rev.* X **5** 031030

[66] Trifonov A and Vig H 2007 Single-photon watch dog detector for folded quantum key distribution system *US patent* 7227955B2

[67] Marøy Ø, Makarov V and Skaar J 2017 *Quantum Sci. Technol.* **2** 044013

[68] Fu Y, Yin H-L, Chen T-Y and Chen Z-B 2015 *Phys. Rev. Lett.* **114** 090501

[69] Lo H-K, Curty M and Qi B 2012 *Phys. Rev. Lett.* **108** 130503

[70] Yang X, Wei K, Ma H, Sun S, Liu H, Li Z, Yin Z, Du Y and Wu L 2016 arXiv:1608.00114

[71] Puthoor I V, Amiri R, Wallden P, Curty M and Andersson E 2016 *Phys. Rev.* A **94** 022328

[72] Yin H-L *et al* 2017 *Phys. Rev.* A **95** 042338

[73] Tamaki K, Curty M and Lucamarini M 2016 *New J. Phys.* **18** 065008