REVIEWS OF MODERN PHYSICS, VOLUME 92, APRIL–JUNE 2020

Secure quantum key distribution with realistic devices

Feihu Xu

Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China and Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China

Xiongfeng Ma

Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China

Qiang Zhang

Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China and Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China

Hoi-Kwong Lo[*]

Center for Quantum Information and Quantum Control,
Department of Physics and Department of Electrical and Computer Engineering,
University of Toronto, Toronto, Ontario M5S 3G4, Canada

Jian-Wei Pan[†]

Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China and Shanghai Branch, CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, China

(published 26 May 2020)

In principle, quantum key distribution (QKD) offers information-theoretic security based on the laws of physics. In practice, however, the imperfections of realistic devices might introduce deviations from the idealized models used in security analyses. Can quantum code breakers successfully hack real systems by exploiting the side channels? Can quantum code makers design innovative countermeasures to foil quantum code breakers? Theoretical and experimental progress in the practical security aspects of quantum code making and quantum code breaking is reviewed. After numerous attempts, researchers now thoroughly understand and are able to manage the practical imperfections. Recent advances, such as the measurement-device-independent protocol, have closed critical side channels in the physical implementations, paving the way for secure QKD with realistic devices.

DOI: 10.1103/RevModPhys.92.025002

CONTENTS

[*] hklo@ece.utoronto.ca
[†] pan@ustc.edu.cn

I. INTRODUCTION

A. Secure communication

For thousands of years, code makers and code breakers have been fighting for supremacy. With the recent rise of the Internet of things, cybersecurity has become a hot topic. Cyber warfare that can undermine the security of critical infrastructures, such as smart power grids and financial systems, threatens the well-being of individual countries and the global economy.

In conventional cryptography, two distant parties, traditionally called Alice and Bob, share a communication channel, and they want to communicate privately in the presence of an eavesdropper Eve. The holy grail of secure communication is information-theoretical security. It is known that one could achieve information-theoretically secure communication via the one-time-pad (OTP) method (Vernam, 1926) if the two users Alice and Bob share a long random string that is kept secret from Eve. Note that for the OTP scheme to be information-theoretically secure, it is important not to reuse the key (Shannon, 1949); that is, that the key has to be as long as the message itself and can be used only once. Determining how to distribute such a long key in the presence of Eve is called the key distribution problem. In fact, the key distribution problem is a central challenge in all kinds of encryption methods.

In principle, *all* conventional key distribution schemes that rely on classical physics and mathematics can provide only computational security, because in classical physics there is nothing to prevent an eavesdropper from copying the key during the key distribution process. Now if Eve and Bob have the same key, whatever Bob can decrypt, Eve can decrypt too.

Currently, the key distribution problem is often solved by public-key cryptography. In public-key cryptography, there are a pair of keys: a public key and a private key. An intended recipient Bob will publish the public key so that anyone, including the intended sender Alice, can encrypt a message, called a plain text, with the public key and send the encrypted message, a cipher text, to Bob. On the other hand, only Bob with the private key can decrypt the cipher text to recover the plain text efficiently. The security of public-key cryptography is based on computational assumptions. Given the public key, there is no efficient known algorithm for Eve to work out the private key or to recover the plain text from the cipher text. For instance, the security of the best-known public-key cryptosystem RSA (Rivest, Shamir, and Adleman, 1978) is based on the presumed difficulty of factoring large integers. Unfortunately, public-key cryptography is vulnerable to unanticipated advances in hardware and software. Moreover, in 1994, Peter Shor (then at AT&T) invented an efficient quantum algorithm for factorization (Shor, 1997). For this reason, if a large-scale quantum computer is ever constructed, much of conventional cryptography will fall apart.

After more than two decades of intense theoretical and experimental efforts, primitive small-scale quantum computers have been built to date. Several big companies and a number of labs and start-ups are racing to build the world's first practical quantum computer. For instance, Google AI Quantum Laboratory[1] has realized a quantum advantage (or supremacy) over a state-of-the-art classical supercomputer for a specific computational task (Arute *et al.*, 2019) and plans to commercialize quantum computers within a few years (Mohseni *et al.*, 2017). IBM Q has already put its 16-qubit quantum processor online for client use.[2] Rigetti has also provided quantum cloud service.[3] The Chinese Academy of Sciences (CAS) and Alibaba have established the Quantum Computing Laboratory to advance the research of quantum computing.[4] Other companies, such as Intel, Microsoft, Baidu, Tencent, IonQ, Xanadu, and Zapata, have also joined the international race to build a quantum computer. Moreover, China is building the National Laboratory for Quantum Information Science to support revolutionary research in quantum information. The European Commission has launched the flagship initiative on quantum technologies.[5] The United States launched the National Quantum Initiative Act in 2018.[6] All in all, the possibility of successful construction of a quantum computer in the next decade can no longer be discounted.

Note that some data, such as our DNA data and health data, need to kept secret for decades. This is called *long-term security*. However, cryptographic standards could take many years to change. An eavesdropper intercepting encrypted data sent in 2019 may save them for decades as they wait for the future successful construction of a quantum computer. The eavesdropper could then retroactively successfully crack an encryption scheme; therefore, cryptographic standards need to consider the potential future technological advances of the next few decades. For instance, Canadian census data must be kept confidential for 92 years.[7] To ensure such security, we need to predict the technology of the next century. Note that the first general-purpose electronic computer ENIAC was formally dedicated in 1946, which was less than 92 years ago. This means that general-purpose electronic computers did not even exist 92 years ago. Therefore, if history is any guide, it is not realistic for one to predict with any confidence what types of technology will exist 92 years from now.

In 2015, the U.S. National Security Agency announced a plan for transition to quantum-safe cryptographic systems. For instance, the U.S. National Institute of Standards and Technology has made a call for quantum-safe candidate algorithm nominations that was due on November 30, 2017.[8] Over the next few years, those candidate algorithms will be evaluated.

Broadly speaking, there are two approaches to a quantum-safe encryption scheme. The first approach is to use conventional cryptography and to develop alternative public-key encryption schemes, such as hash-based or code-based encryption schemes, in which known quantum attacks such as Shor's algorithm (Shor, 1997) do not apply. This approach is called *postquantum cryptography*, and it has the advantage of being compatible with existing crypto infrastructure while having high key rates that are available over long distances. Recently, Google performed a test deployment of a postquantum crypto algorithm in transport layer security.[9] One drawback of postquantum algorithms is that those conventional algorithms have been shown to be secure only against *known* quantum attacks. There is always the possibility that a conventional or quantum physicist or computer scientist might one day come up with algorithms for breaking the postquantum cryptography efficiently. As mentioned, this would lead to a retroactive security breach in the future for data transmitted today, with potentially disastrous consequences.

The second approach is to use quantum cryptography (Bennett and Brassard, 1984; Ekert, 1991), particularly quantum key distribution (QKD). It has the advantage of promising information-theoretical security based on the fundamental laws of quantum physics; i.e., the security is independent of all future advances of algorithm or computational power.

Note, however, that quantum cryptography cannot replicate all functionalities of public-key cryptography. In the future, quantum cryptography is likely to be combined with postquantum cryptography to form the infrastructure of a quantum-safe encryption scheme. For instance, postquantum cryptography can be used to perform the initial authentication. This authentication is required only for a short time, and once it is done, the generated QKD key is secure. Therefore, the two approaches, postquantum cryptography and quantum cryptography, are *complementary* with each other rather than mutually exclusive.

B. QKD

The main goal of QKD is to achieve information-theoretical security by harnessing the laws of physics (Bennett and Brassard, 1984; Ekert, 1991). The quantum no-cloning theorem dictates that an unknown quantum state cannot be cloned reliably (Dieks, 1982; Wootters and Zurek, 1982). If Alice distributes a key via quantum (e.g., single-photon) signals, because there is only a single copy of the key to begin with, there is no way for Eve to clone the quantum state reliably to produce two copies of the same quantum state. Therefore, if Eve tries to eavesdrop in QKD, she unavoidably introduces disturbance to the quantum signals, which will then be detected by the users Alice and Bob. Alice and Bob can

[1] See http://research.google/teams/applied-science/quantum.

[2] See http://www.research.ibm.com/ibm-q.

[3] See http://www.rigetti.com.

[4] See http://quantumcomputer.ac.cn/index.html.

[5] See http://ec.europa.eu/digital-single-market/en/news/quantum-europe-2017-towards-quantum-technology-flagship.

[6] See http://www.congress.gov/bill/115th-congress/house-bill/6227.

[7] See http://www12.statcan.ca/English/census01/Info/chief.cfm.

[8] See http://csrc.nist.gov/Projects/Post-Quantum-Cryptography.

[9] See http://security.googleblog.com/2016/07/experimenting-with-post-quantum.

then simply discard such a key[10] and try the key distribution process again.

Note that an important advantage of QKD is that, once a QKD session is over, there is no classical transcript for Eve to keep since the communication is quantum. Therefore, an eavesdropper has to break a QKD session in real time or it will be secure forever. This differs significantly from conventional key distribution schemes.

1. Bennett-Brassard 1984 protocol

The best-known QKD scheme is the Bennett-Brassard 1984 (BB84) protocol (Bennett and Brassard, 1984). The BB84 protocol allows two users Alice and Bob, who share a quantum channel (e.g., an optical fiber or free space) and an authenticated conventional classical channel, to generate a secure key in the presence of an eavesdropper with unlimited quantum computing powers. In the BB84 protocol, a sequence of single photons carrying qubit states is sent by Alice to Bob through a quantum channel. A schematic diagram of the BB84 protocol is illustrated in Fig. 1, and the steps of the protocol are listed in Box I.B.1.

Box I.B.1: BB84 protocol.

(1) For each signal, Alice randomly encodes a single photon with one of the four polarization states, namely, vertical, horizontal, 45°, and 135°, and sends the photon through a quantum channel to Bob.
(2) For each signal, Bob chooses one of the two bases, rectilinear or diagonal, to perform a measurement on the polarization of a received photon. After detection, Alice and Bob publicly announce their basis choices through an authenticated conventional channel.
(3) Alice and Bob discard the polarization data that have been encoded and detected in different bases. They keep only those polarization data in the same basis. These remaining data form the sifted key. Alice and Bob can choose a random sample of the sifted key bits and compare them to compute the quantum bit error rate (QBER).
(4) If the computed QBER is too high, Alice and Bob abort. Otherwise, they proceed with classical postprocessing such as error correction and privacy amplification to generate a secret key.

2. Intuition of security

The quantum no-cloning theorem guarantees that Eve cannot copy the unknown quantum state sent by Alice reliably (Dieks, 1982; Wootters and Zurek, 1982). Furthermore, a key feature in quantum mechanics is the complementarity between the two conjugate bases, rectilinear and diagonal. Since the two measurements corresponding to the two bases do not commute with each other, there is no way to measure the two observables simultaneously without disturbing the state. Therefore, Eve, who tries to eavesdrop and extract information on the polarization data, inevitably introduces disturbance to the state. Bob, on the other hand, with the authenticated classical channel, has a fundamental advantage over Eve because he can compare his basis choice with Alice's and determine the QBER for data that are encoded and detected in the same basis.

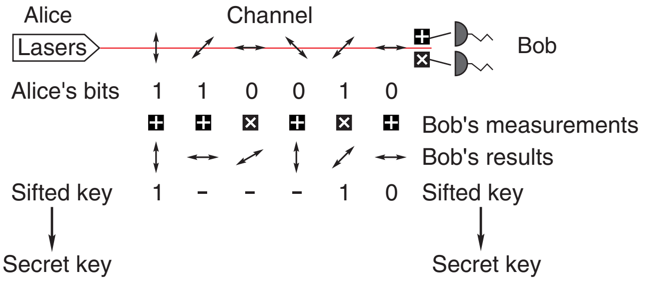

FIG. 1. Schematic diagram of the BB84 protocol. Alice encodes random bits on the polarization states of single photons. Bob randomly selects measurement bases, rectilinear ($+$) or diagonal ($\times$), to perform measurements using two detectors. They keep only those polarization data that have been encoded and detected in the same basis as the sifted key and perform additional classical postprocessing on the sifted key to produce the final secret key.

What happens if Eve attacks the quantum channel? A simple example of an eavesdropping strategy is the *intercept-and-resend attack* (Bennett and Brassard, 1984). In this attack, for each photon sent from Alice, Eve performs a measurement in a randomly chosen basis and resends a new photon to Bob according to her measurement result. Let us focus on those cases when Alice and Bob happen to use the same basis since they will throw away the rest. If Eve happens to use the correct basis (50%), then both she and Bob will decode Alice's bit value correctly. No error is introduced by Eve. On the other hand, if Eve uses the wrong basis (50%), then both she and Bob will have random measurement results. This suggests that if Alice and Bob compare a subset of the sifted key, they will see a significant amount of errors. For these bits, the photons will be passed on to Bob in the wrong basis, so regardless of Eve's measurement result Bob will have a 50% probability of measuring the opposite of Alice's bit value. In other words, Eve's attack will introduce 50% QBER for half of the total bits, and thus a total of 25% QBER. This example illustrates the basic principle behind QKD: Eve can gain information only at the cost of introducing disturbance, which will expose her interference.

3. Overview of recent developments

Theoretical developments.—On the theoretical side, the first security proof of QKD was based on the uncertainty principle by Mayers (2001). Mayers's proof was put into a conceptually simple framework based on entanglement distillation by Lo and Chau (1999), building on the earlier work of quantum privacy amplification (Deutsch *et al.*, 1996) and entanglement distillation (Bennett *et al.*, 1996). Later on, Shor and Preskill employed the idea of the Calderbank-Shor-Steane (CSS) quantum error correcting code (Calderbank and Shor, 1996; Steane, 1996) to simplify the entanglement-based proof of a prepare-and-measure protocol (Shor and Preskill, 2000); see also Biham *et al.* (2000), Devetak and Winter (2005), and Koashi (2009) for security proofs of QKD.

A rigorous definition of secure keys was presented afterward in the 2000s (Ben-Or *et al.*, 2005; Renner and König, 2005), where the composable security definition in conventional cryptography (Canetti, 2001) was introduced to

[10] Note that a key is simply a random string of numbers and that if a key is aborted, it will not be used. There is no loss in security in aborting.

quantum cryptography (Ben-Or *et al.*, 2005). A further development was the security proof for the consideration of finite-key effects in a more rigorous manner (Renner, 2008; Scarani and Renner, 2008; Tomamichel *et al.*, 2012).

Device imperfections in practical systems were investigated in security analyses (Lütkenhaus, 2000; Inamori, Lütkenhaus, and Mayers, 2007), and a remarkable framework for a security analysis of realistic devices was established by Gottesman *et al.* (2004). Moreover, new protocols such as the decoy state (Hwang, 2003; Lo, Ma, and Chen, 2005; Wang, 2005), differential phase shift (DPS) (Inoue, Waks, and Yamamoto, 2002), the Scarani-Acín-Ribordy-Gisin protocol (Scarani *et al.*, 2004), coherent one way (COW) (Stucki *et al.*, 2005), measurement-device independent (MDI) (Lo, Curty, and Qi, 2012) [see also Braunstein and Pirandola (2012)], and round-robin DPS (Sasaki, Yamamoto, and Koashi, 2014) were proposed to address the issues of device imperfections. In particular, the decoy-state protocol enables secure QKD with weak coherent pulses, and the MDI protocol removes all side channels in the detection. Furthermore, device-independent QKD was proposed by Mayers and Yao (1998), Barrett, Hardy, and Kent (2005), and Acín *et al.* (2007) to allow QKD with uncharacterized devices. Its security was proven effective against collective attacks (Pironio *et al.*, 2009; Masanes, Pironio, and Acín, 2011) [see also Hänggi, Renner, and Wolf (2010)], and later against general attacks (Vazirani and Vidick, 2014; Arnon-Friedman *et al.*, 2018).

Experimental developments.—After more than two decades of effort (Gisin *et al.*, 2002; Lo, Curty, and Tamaki, 2014), QKD developments have included the first laboratory demonstration performed in 1992 over 32.5 cm of free space (Bennett, Bessette *et al.*, 1992) and the recent landmark accomplishment of quantum satellite QKD experiment in 2017 over 1200 km by China (Liao *et al.*, 2017a), and 7600 km in 2018 between China and Austria (Liao *et al.*, 2018). Note that this is 7 orders of magnitude improvement in terms of the distance of QKD. There are also ongoing efforts on satellite-based quantum communications by Europe, the U.S., Canada, Japan, and Singapore (Joshi *et al.*, 2018). In fiber, the distance has been pushed to 500-km ultra-low-loss fiber (J.-P. Chen *et al.*, 2020; Fang *et al.*, 2019).

In addition to long distances, a high secret key rate is important for practical applications. Researchers have recently pushed the secret key rate of QKD from 1 Mbits/s over 50-km fiber (Lucamarini *et al.*, 2013) to more than 10 Mbits/s (Islam *et al.*, 2017; Yuan *et al.*, 2018). Commercial QKD systems are currently available on the market from several companies, such as ID Quantique, Quantum CTek, Qasky, and Toshiba Europe. Several institutes, e.g., the European Telecommunications Standards Institute (ETSI), the International Organization for Standardization (ISO), and the International Telecommunication Union (ITU), have made great efforts to address the standardization issues in QKD.

Besides the point-to-point link, a number of field-test QKD networks have been conducted in the U.S. (Elliott *et al.*, 2005), Europe (Peev *et al.*, 2009; Stucki *et al.*, 2011), Japan (Sasaki *et al.*, 2011), China (Chen *et al.*, 2009, 2010; Wang *et al.*, 2010), the U.K. (Dynes *et al.*, 2019), etc. Based on trusted relays,[11] remote users can be connected beyond point-to-point links. Recently, China successfully completed the 2000-km-long fiber-optic backbone link between Beijing and Shanghai (Y.-A. Chen *et al.*, 2020). The U.K. has launched the Quantum Communications Hub project, which aims to build quantum networks in England.[12]The U.S. is deploying its first dark fiber quantum network connecting Washington, D.C., with Boston, Massachusetts, over 800 km.[13]

Overall, QKD is already mature for several real-life applications (Qiu, 2014). For instance, QKD was used to encrypt security communications in the 2007 Swiss election and the 2010 World Cup. In China, QKD is being widely used to ensure long-term security for numerous users in government and the financial and energy industries (Y.-A. Chen *et al.*, 2020), including the People's Bank of China, the China Banking Regulatory Commission, and the Industrial and Commercial Bank of China. Figure 2 shows a schematic diagram of the space-ground integrated quantum network (Y.-A. Chen *et al.*, 2020), already constructed in China, which spans more than 2000 km of coverage area and has more than 600 QKD links.

C. Focus of this review

In the codebook by Singh (2000), he proclaimed that quantum cryptography achieves the holy grail of cryptography by offering unconditional security. Therefore, quantum cryptography presents the final stage of evolution of cryptography. After quantum cryptography, cryptography will no longer continue to evolve. Is this really true?

In principle, QKD promises unconditional security based on the laws of physics. In practice, however, realistic devices display imperfections, which might seldom conform to idealized theoretical models used in the security analysis by theorists. The deviations might also be vulnerable to some special attacks, i.e., quantum hacking. For this reason, an arms race has been going on in quantum cryptography among quantum code makers and quantum code breakers. The main goal is to assess the deviations between the system and the ideal, thus establishing the *practical security* for real QKD systems.

Table I summarizes the quantum hacking strategies developed in the last two decades; see also Jain *et al.* (2016) for an earlier review on the subject. Right after the QKD security proofs, in which ideal devices were presented, a well-known hacking strategy was proposed, the photon-number-splitting (PNS) attack (Brassard *et al.*, 2000; Lütkenhaus, 2000), which targets a practical QKD source. The source device

[11] In the trusted-relay scenario, Alice and Bob, respectively, share a secret key with a relay in the middle, and the relay then announces the exclusive-OR (XOR) results of both keys publicly. With the announced result, Alice and Bob can get each other's key via the XOR results with her or his own key. The negative side for this method is that the relay must be trusted. However, the positive side is reducing the cost and complexity as compared to the all-connected point-to-point links and extending the transmission distance.

[12] See http://www.quantumcommshub.net/about-us/.

[13] See http://techcrunch.com/2018/10/25/new-plans-aim-to-deploy-the-first-u-s-quantum-network-from-boston-to-washington-dc/.

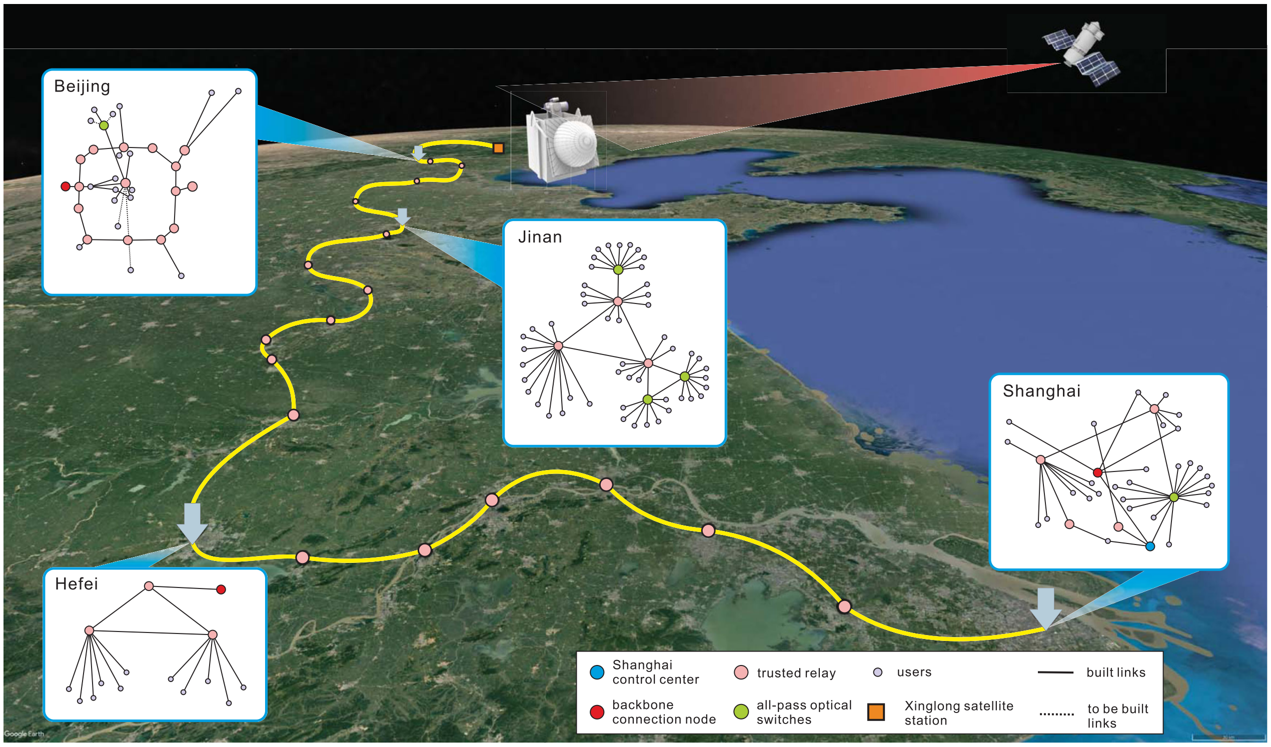

FIG. 2. Schematic diagram of the space-ground integrated quantum network in China (Chen *et al.*, 2020), consisting of four quantum metropolitan area networks in the cities of Beijing, Jinan, Shanghai, and Heifei, a backbone network extending over 2000 km, and ground-satellite links. There are three types of nodes in the network: user nodes, all-pass optical switches, and trusted relays. The backbone network is connected by trusted intermediate relays. The satellite is connected to a ground-satellite station near Beijing, which can provide ultra-long-distance communications (Liao *et al.*, 2018).

imperfection severely undermines the performance of a QKD system, typically below a 30-km fiber (Lütkenhaus, 2000; Gottesman *et al.*, 2004; Ma, 2006). To close this side channel for a QKD source, the decoy-state method was proposed by quantum code makers to make QKD practical with standard weak coherent pulses (WCPs) that are generated by attenuated lasers (Hwang, 2003; Lo, Ma, and Chen, 2005; Wang, 2005). Decoy-state QKD represents a dramatic performance improvement over conventional security proofs (Gottesman *et al.*, 2004), and it has become a standard technique in current QKD experiments. Table II provides a list of decoy-state QKD experiments.

After the decoy-state method, however, various quantum hacking attacks have been performed by quantum code breakers against other components in practical QKD systems; see Table I. To counter those attacks, a few important concepts have been proposed by quantum code makers. One practical countermeasure against quantum hacking is the measurement-device-independent quantum key distribution (MDI-QKD) (Lo, Curty, and Qi, 2012); see also Braunstein and Pirandola (2012). MDI-QKD completely removes all security loopholes in the detection system and ensures a QKD network security with *untrusted* relays. It is practical with current technology. Table III summarizes the MDI-QKD experiments after its invention.

In addition, an efficient version of MDI-QKD, twin-field (TF)-QKD, has the potential to greatly extend the secure distance. Table IV summarizes recent TF-QKD experiments. We note some of the recent developments of continuous-variable (CV)-QKD (see Table V), chip-based QKD (see Table VI), and other QKD protocols and implementations (see Table VII). We also summarize a list of some developments of recent quantum-cryptographic protocols besides QKD; see Table VIII.

Note that the side channels are common problems to any cryptosystems, i.e., not only to quantum cryptography but also to conventional cryptographic systems. For instance, the power consumption of the CPU performing encryption and decryption and the timing of the signals are common side channels that can threaten implementations of both quantum and conventional cryptographic systems (Kocher, Jaffe, and Jun, 1999; Brumley and Boneh, 2005). Therefore, closing the side channels is required in all cryptographic technologies. It is only through painstaking battle testing that the security of a practical cryptosystem could be established with confidence. The arms race between code makers and code breakers will continue in cryptographic systems.

Nonetheless, QKD is a physics-based cryptosystem, and its security is working on the physical layer. Compared to the conventional mathematical-based cryptography, QKD can provide an accurate description of the physical realization of a cryptographic system, and the security can be proved based on this description. QKD has the fundamental advantage of promising information-theoretical security, which is independent of all future advances of computational power. Furthermore, the recent advances, such as MDI-QKD, have

TABLE I. List of quantum hacking strategies.

Attack	Source or detection	Target component	Manner	Year
Photon number splitting (Brassard *et al.*, 2000; Lütkenhaus, 2000)	Source	WCP (multiphotons)	Theory	2000
Detector fluorescence (Kurtsiefer *et al.*, 2001)	Detection	Detector	Theory	2001
Faked state (Makarov and Hjelme, 2005; Makarov, Anisimov, and Skaar, 2006)	Detection	Detector	Theory	2005
Trojan horse (Vakhitov, Makarov, and Hjelme, 2001; Gisin *et al.*, 2006)	Source and detection	Backreflection light	Theory	2006
Time shift (Qi, Fung *et al.*, 2007; Zhao *et al.*, 2008)	Detection	Detector	Experiment[a]	2007
Time side channel (Lamas-Linares and Kurtsiefer, 2007)	Detection	Timing information	Experiment	2007
Phase remapping (Fung *et al.*, 2007; Xu, Qi, and Lo, 2010)	Source	Phase modulator	Experiment[a]	2010
Detector blinding (Makarov, 2009; Lydersen *et al.*, 2010)	Detection	Detector	Experiment[a]	2010
Detector blinding (Gerhardt *et al.*, 2011a; Gerhardt *et al.*, 2011b)	Detection	Detector	Experiment	2011
Detector control (Lydersen, Akhlaghi *et al.*, 2011; Wiechers *et al.*, 2011)	Detection	Detector	Experiment	2011
Faraday mirror (Sun, Jiang, and Liang, 2011)	Source	Faraday mirror	Theory	2011
Wavelength (Li *et al.*, 2011; Huang *et al.*, 2013)	Detection	Beam splitter	Experiment	2011
Dead time (Henning *et al.*, 2011)	Detection	Detector	Experiment	2011
Channel calibration (Jain *et al.*, 2011)	Detection	Detector	Experiment[a]	2011
Intensity (Jiang *et al.*, 2012; Sajeed, Radchenko *et al.*, 2015)	Source	Intensity modulator	Experiment	2012
Phase information (Sun *et al.*, 2012, 2015; Tang *et al.*, 2013)	Source	Phase randomization	Experiment	2012
Memory attacks (Barrett, Colbeck, and Kent, 2013)	Detection	Classical memory	Theory	2013
Local oscillator (Jouguet, Kunz-Jacques, and Diamanti, 2013; Ma *et al.*, 2013a)[b]	Detection	Local oscillator	Experiment	2013
Trojan horse (Jain *et al.*, 2014, 2015)	Source and detection	Backreflection light	Experiment	2014
Laser damage (Bugge *et al.*, 2014; Makarov *et al.*, 2016)	Detection	Detector	Experiment	2014
Laser seeding (Sun *et al.*, 2015)	Source	Laser phase or intensity	Experiment	2015
Spatial mismatch (Sajeed, Chaiwongkhot *et al.*, 2015; Chaiwongkhot *et al.*, 2019)	Detection	Detector	Experiment	2015
Detector saturation (Qin, Kumar, and Alléaume, 2016)[b]	Detection	Homodyne detector	Experiment	2016
Covert channels (Curty and Lo, 2019)	Detection	Classical memory	Theory	2017
Pattern effect (Yoshino *et al.*, 2018)	Source	Intensity modulator	Experiment	2018
Detector control (Qian *et al.*, 2018)	Detection	Detector	Experiment	2018
Laser seeding (Sun *et al.*, 2015; Huang *et al.*, 2019; Pang *et al.*, 2019)	Source	Laser	Experiment	2019
Polarization shift (Wei, Zhang *et al.*, 2019)	Detection	SNSPD	Experiment	2019

[a] Demonstration on a commercial QKD system.
[b] Continuous-variable QKD.

closed the critical side channels in the detection of physical implementations, paving the way for secure QKD with realistic devices. Therefore, we believe that QKD does represent an important chapter in the history of code making. We hope that QKD will play an important role in the quantum-safe encryption infrastructure for real applications, and it will bring us one step closer to the dream of information-theoretical security.

D. Outline of this review

This review will focus mainly on the practical security of realistic QKD systems. We begin with a discussion of security analysis in Sec. II and the basic implementation of QKD in Sec. III. In Sec. IV, we review various quantum hacking attacks against QKD implementations. In Sec. V, we review the security of a practical QKD source. In particular, we focus on the decoy-state protocol, which is a standard method for secure QKD with attenuated lasers. In Sec. VI, we turn to detector security. We primarily review the MDI-QKD protocol and how it automatically foils all attacks on the detection system. In Sec. VII, we review the developments of CV-QKD schemes and their practical security aspects. Section VIII contains a review of other quantum-cryptographic protocols. In Sec. IX, we present some concluding remarks.

For those wanting to learn further basics of QKD, we refer to two earlier reviews: Gisin *et al.* (2002), which introduces basic experimental elements and systems, and Scarani *et al.*

TABLE II. List of decoy-state QKD experiments and their performance.

Reference	Clock rate	Encoding	Channel	Maximal distance	Key rate (bits/s)	Year
Zhao *et al.* (2006a, 2006b)	5 MHz	Phase	Fiber	60 km	422.5	2006
Peng *et al.* (2007)	2.5 MHz	Polarization	Fiber	102 km	8.1	2007
Rosenberg *et al.* (2007)	2.5 MHz	Phase	Fiber	107 km	14.5	2007
Schmitt-Manderbach *et al.* (2007)	10 MHz	Polarization	Free space	144 km	12.8[a]	2007
Yuan, Sharpe, and Shields (2007)	7.1 MHz	Phase	Fiber	25.3 km	5.5 K	2007
Yin *et al.* (2008)	1 MHz	Phase	Fiber	123.6 km	1.0	2008
Wang *et al.* (2008)[b]	0.65 MHz	Phase	Fiber	25 km	0.9	2008
Dixon *et al.* (2008)	1 GHz	Phase	Fiber	100.8 km	10.1 K	2008
Peev *et al.* (2009)	7 MHz	Phase	Fiber network	33 km	3.1 K	2009
Rosenberg *et al.* (2009)	10 MHz	Phase	Fiber	135 km	0.2	2009
Yuan *et al.* (2009)	1.036 GHz	Phase	Fiber	100 km	10.1 K	2009
Chen *et al.* (2009)	4 MHz	Phase	Fiber network	20 km	1.5 K	2009
Liu *et al.* (2010)	320 MHz	Polarization	Fiber	200 km	15.0	2010
Chen *et al.* (2010)	320 MHz	Polarization	Fiber network	130 km	0.2 K	2010
Sasaki *et al.* (2011)	1 GHz	Phase	Fiber network	45 km	304.0 K	2011
Wang *et al.* (2013)	100 MHz	Polarization	Free space	96 km	48.0	2013
Fröhlich *et al.* (2013)	125 MHz	Phase	Fiber network	19.9 km	43.1 K	2013
Lucamarini *et al.* (2013)	1 GHz	Phase	Fiber	80 km	120.0 K	2013
Fröhlich *et al.* (2017)	1 GHz	Phase	Fiber	240 km[c]	8.4	2017
Liao *et al.* (2017a)	100 MHz	Polarization	Free space	1200 km	1.1 K	2017
Yuan *et al.* (2018)	1 GHz	Phase	Fiber	2 dB	13.7 M	2018
Boaron *et al.* (2018)	2.5 GHz	Time bin	Fiber	421 km[c]	6.5	2018

[a] Asymptotic key rate.
[b] Heralded single-photon source.
[c] Ultra-low-loss fiber.

TABLE III. List of MDI-QKD experiments and their performance.

Reference	Clock rate	Encoding	Distance or loss	Key rate (bits/s)	Year	Notes
Rubenok *et al.* (2013)[a]	2 MHz	Time bin	81.6 km	0.24[b]	2013	Field-installed fiber
Liu *et al.* (2013)	1 MHz	Time bin	50 km	0.12	2013	First complete demonstration
Ferreira da Silva *et al.* (2013)[a]	1 MHz	Polarization	17 km	1.04[b]	2013	Multiplexed synchronization
Z. Tang *et al.* (2014)	0.5 MHz	Polarization	10 km	4.7×10^{-3}	2014	Active phase randomization
Y.-L. Tang *et al.* (2014)	75 MHz	Time bin	200 km	0.02	2014	Fully automatic system
Tang *et al.* (2015)	75 MHz	Time bin	30 km	16.9	2015	Field-installed fiber
C. Wang *et al.* (2015)	1 MHz	Time bin	20 km	8.3[b]	2015	Phase reference free
Valivarthi *et al.* (2015)	250 MHz	Time bin	60 dB	5×10^{-2}	2015	Test in various configurations
Pirandola *et al.* (2015)[a]	10.5 MHz	Phase	4 dB	0.1	2015	Continuous variable
Y.-L. Tang *et al.* (2016)	75 MHz	Time bin	55 km	16.5	2016	First fiber network
Yin *et al.* (2016)	75 MHz	Time bin	404 km	3.2×10^{-4}	2016	Longest distance
G.-Z. Tang *et al.* (2016)	10 MHz	Polarization	40 km	10	2016	Include modulation errors
Comandar *et al.* (2016)[a]	1 GHz	Polarization	102 km	4.6 K	2016	High repetition rate
Kaneda *et al.* (2017)[a]	1 MHz	Time bin	14 dB	0.85	2017	Heralded single-photon source
C. Wang *et al.* (2017)	1 MHz	Time bin	20 km	6.3×10^{-3}	2017	Stable against polarization change
Valivarthi *et al.* (2017)	20 MHz	Time bin	80 km	100	2017	Cost-effective implementation
H. Liu *et al.* (2018)	50 MHz	Time bin	160 km	2.6[b]	2018	Phase reference free
H. Liu *et al.* (2019)	75 MHz	Time bin	100 km	14.5	2019	Asymmetric channels
Wei *et al.* (2019)	1.25 GHz	Polarization	20.4 dB	6.2 K	2019	Highest repetition or key rate

[a] No random modulations.
[b] Asymptotic key rate.

(2009), which discusses the basic security analysis tools of various QKD protocols. An early review on the first stage of development of QKD can be found in Sergienko (2018). An earlier review on quantum attacks can be seen in Jain *et al.* (2016). A brief overview of the implementation security of QKD can be found in a survey article by Lo, Curty, and Tamaki (2014) and in a ETSI white paper by Lucamarini *et al.*[14] A short overview of the practical challenges associated with QKD can be found in Diamanti *et al.* (2016) and Zhang *et al.* (2018). Moreover, the entropy uncertainty relation, an important

[14] See https://www.etsi.org/images/files/ETSIWhitePapers/.

TABLE IV. List of TF-QKD experiments.

Reference	Distance or loss	Key rate (bits/s)	Year
Minder *et al.* (2019)	90.8 dB	0.045[a]	2019
Wang, He *et al.* (2019)	300 km	2.01×10^3 [a]	2019
Y. Liu *et al.* (2019)	300 km	39.2	2019
Zhong *et al.* (2019)	55.1 dB	25.6[a]	2019
Fang *et al.* (2019)	502 km[b]	0.118	2019
J.-P. Chen *et al.* (2020)	509 km[b]	0.269	2019

[a] Asymptotic key rate.
[b] Ultra-low-loss fiber.

tool for analyzing the security of QKD, can be seen in Coles *et al.* (2017), and the quantum random number generator, a basic element in a practical QKD system, can be found in X. Ma *et al.* (2016) and in Herrero-Collantes and Garcia-Escartin (2017). A review on various techniques of single-photon detectors can be seen in Hadfield (2009) and Zhang *et al.* (2015). Furthermore, we may not cover certain important topics too thoroughly, but we refer the interested reader to other review articles on the topics of CV-QKD (Weedbrook *et al.*, 2012; Diamanti and Leverrier, 2015; Laudenbach *et al.*, 2018), high-dimensional QKD (Xavier and Lima, 2020), quantum repeaters (Sangouard *et al.*, 2011; Pan *et al.*, 2012; Munro *et al.*, 2015), quantum Internet (Kimble, 2008; Wehner, Elkouss, and Hanson, 2018), Bell nonlocality and device-independent protocols (Brunner *et al.*, 2014), and blind quantum computing (Fitzsimons, 2017). These related review articles are summarized in Table IX.

TABLE V. List of some recent CV-QKD experiments and their performance.

Reference	Clock rate	Distance or loss	Key rate (bits/s)	Year	Notes
Jouguet *et al.* (2013)	1 MHz	80.5 km	~250	2013	Full implementation
Qi *et al.* (2015)	25 MHz	⋯	⋯	2015	Local LO
Soh *et al.* (2015)	250 kHz	⋯	⋯	2015	Local LO
Huang, Huang *et al.* (2015)	100 MHz	25 km	100 K	2015	Local LO
Pirandola *et al.* (2015)	10.5 MHz	4 dB	0.1	2015	CV MDI-QKD
Huang, Lin *et al.* (2015)	50 MHz	25 km	~1 M	2015	High key rate
Kumar, Qin, and Alléaume (2015)	1 MHz	75 km	490	2015	Coexistence with classical
Zhang *et al.* (2020)	5 MHz	202.8 km[a]	6.2	2020	Long distance

[a] Ultra-low-loss fiber.

TABLE VI. List of chip-based QKD experiments.

Reference	Clock rate	Distance or loss	Key rate (bits/s)	Year	Notes
C. Ma *et al.* (2016)	10 MHz	5 km	0.95 K	2016	Silicon, decoy BB84
Sibson *et al.* (2017)	1.72 GHz	4 dB	565 K	2017	InP, DPS
Sibson, Kennard *et al.* (2017)	1.72 GHz	20 km	916 K	2017	Silicon, COW
Bunandar *et al.* (2018)	625 MHz	43 km	157 K	2018	Silicon, decoy BB84
Ding *et al.* (2017)	5 kHz	4 dB	~7.5	2018	Silicon, high dimension
G. Zhang *et al.* (2019)	1 MHz	16 dB	0.14 K	2019	Silicon, CV-QKD
Paraïso *et al.* (2019)	1 GHz	20 dB	270 K	2019	InP, modulator free
Wei *et al.* (2019)	1.25 GHz	140 km	497	2019	Silicon, MDI-QKD

TABLE VII. List of recent experiments of other QKD protocols.

Reference	Clock rate	Distance or loss	Key rate (bits/s)	Year
Quantum access network (Fröhlich *et al.*, 2013)	125 MHz	19.9 km	259	2013
Centric network (Hughes *et al.*, 2013)	10 MHz	50 km	⋯	2013
RRDPS (Guan *et al.*, 2015)	500 MHz	53 km	~118.0	2015
RRDPS (Takesue *et al.*, 2015)	2 GHz	20 km	2.0 K	2015
RRDPS (S. Wang *et al.*, 2015)	1 GHz	90 km	~800	2015
RRDPS (Li *et al.*, 2016)	10 kHz	18 dB	15.5	2016
High dimension (Lee *et al.*, 2014)	8.3 MHz	⋯	456	2014
High dimension (Zhong *et al.*, 2015)	cw	20 km	2.7 M	2015
High dimension (Mirhosseini *et al.*, 2015)	4 kHz	⋯	6.5	2015
High dimension (Sit *et al.*, 2017)	⋯	0.3 km	~30 K	2017
High-dimension (Islam *et al.*, 2017)	2.5 GHz	16.6 dB	1.07 M	2017
Coherent one way (Korzh *et al.*, 2015)	625 MHz	307 km	3.2	2015
Modulator free (Yuan *et al.*, 2016)	1 GHz	40 dB	~10	2016

TABLE VIII. List of recent developments of other quantum-cryptographic protocols beyond QKD.

Protocol	Theory or experiment	Notes
Noisy quantum storage (Damgård *et al.*, 2008; Wehner, Schaffner, and Terhal, 2008; Konig, Wehner, and Wullschleger, 2012)	Theory	Unconditional security
Oblivious transfer (Erven *et al.*, 2014)	Experiment	Noisy-storage model
Bit commitment (Ng *et al.*, 2012)	Experiment	Noisy-storage model
Bit commitment (Kent, 2012)	Theory	Relativistic assumption
Bit commitment (Lunghi *et al.*, 2013; Liu *et al.*, 2014)	Experiment	Relativistic assumption
Bit commitment (Chakraborty, Chailloux, and Leverrier, 2015; Lunghi *et al.*, 2015; Verbanis *et al.*, 2016)	Experiment	Long commitment time
Digital signature (Clarke *et al.*, 2012)	Experiment	First demonstration
Digital signature (Collins *et al.*, 2014; Dunjko, Wallden, and Andersson, 2014)	Experiment	No quantum memory
Digital signature (Donaldson *et al.*, 2016; Yin *et al.*, 2017a)	Experiment	Insecure channel
Coin flipping (Berlín *et al.*, 2011; Pappa *et al.*, 2014)	Experiment	Loss tolerance
Data locking (Fawzi, Hayden, and Sen, 2013; Lloyd, 2013; Lupo, Wilde, and Lloyd, 2014)	Theory	Loss tolerance
Data locking (Liu *et al.*, 2016; Lum *et al.*, 2016)	Experiment	Loss tolerance
Blind quantum computing (Broadbent, Fitzsimons, and Kashefi, 2009; Barz *et al.*, 2012)	Theory and experiment	No quantum memory
Blind quantum computing (Reichardt, Unger, and Vazirani, 2013; Huang *et al.*, 2017)	Theory and experiment	Classical clients

TABLE IX. List of reviews related to QKD.

Reference	Subject
Gisin *et al.* (2002)	Experimental basics of QKD
Scarani *et al.* (2009)	Theoretical basics of QKD
Lo, Curty, and Tamaki (2014), Diamanti *et al.* (2016), and Zhang *et al.* (2018)	Practical challenges of QKD
Jain *et al.* (2016))	Quantum hacking attacks
Xu, Curty, Qi, and Lo *et al.* (2015)	Measurement-device-independent QKD
Hadfield (2009) and Zhang *et al.* (2015)	Single-photon detector
X. Ma *et al.* (2016) and Herrero-Collantes and Garcia-Escartin (2017)	Quantum random number generator
Coles *et al.* (2017)	Entropy uncertainty relation
Weedbrook *et al.* (2012), Diamanti and Leverrier (2015), and Laudenbach *et al.* (2018)	Continuous-variable QKD
Sangouard *et al.* (2011), Pan *et al.* (2012), and Munro *et al.* (2015)	Quantum repeaters
Kimble (2008) and Wehner, Elkouss, and Hanson (2018)	Quantum internet
Brunner *et al.* (2014)	Bell nonlocality or device-independent QKD
Fitzsimons (2017)	Blind quantum computing
Xavier and Lima (2020)	High-dimensional QKD

II. SECURITY ANALYSIS

We review the security aspects of QKD, including the security definition, various security proofs, and implementation assumptions. We present a general framework to address device imperfections in security analysis. While we focus mainly on the widely implemented BB84 protocol, most of the results can be extended to other QKD protocols. We leave the MDI-QKD case for Sec. VI.B and the DI-QKD case for Sec. VIII.A.

A. Security definition

To prove the security of QKD, one needs to define the security criteria first. Ideally, a secure key satisfies two requirements. First, the key bit strings possessed by Alice and Bob need to be identical, i.e., be *correct*. Second, the key bit string should be uniformly distributed to anyone (say Eve) other than Alice and Bob, i.e., be *secret*. Owing to practical issues such as the finite data size and nonideal error correction, Alice and Bob cannot generate an ideal key. In reality, it is reasonable to allow the key to have a small failure probability ϵ. For some ϵ_{cor} and ϵ_{sec}, we say that the QKD protocol is ϵ secure with $\epsilon = \epsilon_{\mathrm{cor}} + \epsilon_{\mathrm{sec}}$ if it is ϵ_{cor} correct and ϵ_{sec} secret (Ben-Or *et al.*, 2005; Renner and König, 2005).

We define K_A and K_B (with the same length m) to be the key bit strings obtained by Alice and Bob, respectively. The secret key can be correlated to a quantum state ρ_E held by Eve. The joint state ρ_{ABE} is a classical-classical-quantum (c-c-q) state

$$\rho_{ABE} = \sum_{k_A,k_B} \Pr(k_A,k_B)|k_A\rangle\langle k_A| \otimes |k_B\rangle\langle k_B| \otimes \rho_E^{(k_A,k_B)}, \tag{1}$$

where $k_A, k_B \in \{0,1\}^m$ are the bit values. In particular, an ideal key state held by Alice and Bob is described by the private state

$$\rho_{ABE}^{\mathrm{ideal}} = 2^{-m}\sum_{k} |k\rangle_A\langle k| \otimes |k\rangle_B\langle k| \otimes \rho_E, \tag{2}$$

where $k_A = k_B = k$ implies that Alice and Bob hold the same string and ρ_E is independent of k; i.e., Eve has no information on the key string variable K.

A QKD protocol is defined as ϵ_{cor} correct if the probability distribution $\Pr(k_A, k_B)$ of the final state ρ_{ABE} in Eq. (1) satisfies

$$\Pr(k_A \neq k_B) \le \epsilon_{\mathrm{cor}}. \tag{3}$$

A QKD protocol is defined as ϵ_{sec} secret (Renner and König, 2005) if the state ρ_{AE} is close in trace distance to the single-party private state $\rho_{AE}^{\mathrm{ideal}}$,

$$\min_{\rho_E}\tfrac{1}{2}(1-p_{\mathrm{abort}})||\rho_{AE}-\rho_{AE}^{\mathrm{ideal}}||_1 \le \epsilon_{\mathrm{sec}}, \tag{4}$$

where p_{abort} is the probability that the protocol aborts, $\rho_{AE}^{\mathrm{ideal}} \equiv 2^{-m}\sum_s |s\rangle_A\langle s| \otimes \rho_E$, and $\|A\|_1 \equiv \mathrm{Tr}[\sqrt{A^\dagger A}]$ is the trace norm. It turns out that the security definition from the trace-distance metric owns a composable security property (Ben-Or *et al.*, 2005; Renner and König, 2005).

In general, following the definition of Ben-Or *et al.* (2005), a QKD protocol can be defined as ϵ secure if the final distilled *c-c-q* state ρ_{ABE} is ϵ close to the ideal key state $\rho_{ABE}^{\mathrm{ideal}}$ given in Eq. (2) with a proper chosen ρ_E:

$$\min_{\rho_E}\tfrac{1}{2}(1-p_{\mathrm{abort}})||\rho_{ABE}-\rho_{ABE}^{\mathrm{ideal}}||_1 \le \epsilon. \tag{5}$$

Note that if a distilled state is ϵ close to the ideal key state, then the guessing probability for Eve for the final key is also bounded by ϵ. Here we want to emphasize that one should not interpret the security parameter ϵ used in the previous definition as the guessing probability. In fact, the statement a key is ϵ close to the ideal key is much stronger than the statement Eve's guessing probability on a key is bounded by ϵ. Let us give a simple example. Denote $l = -\log\epsilon$ and $l < m$. We consider an m-bit key K_{bad}, which concatenates a uniformly distributed l-bit string with $m-l$ bits of 0s. The key K_{bad} does not satisfy the trance-distance (statistical distance in this case since everything is classical here) ϵ-security definition used in Eq. (5), because the statistical distance between K_{bad} and K_{ideal} is close to 1 when $m \gg l$. However, the guessing probability of Eve on the key K_{bad} is bounded by ϵ. The guessing probability alone is not a proper security parameter definition. This is a common mistake for those who are confused about the security foundation of quantum cryptography; see, for example, Yuen (2016). This common mistake was also pointed out and explained by Renner (2012).

B. Security proofs

1. Lo-Chau security proof

In the Lo-Chau security proof (Lo and Chau, 1999), the joint quantum state shared by Alice and Bob before the final key measurement is one of the Bell states,

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle),$$
$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \tag{6}$$

To see how the security of QKD is related to entanglement, consider the case where Alice and Bob share m pairs of perfect Einstein-Podolsky-Rosen (EPR) pairs $|\Phi^+\rangle^{\otimes m}$. It is not hard to verify that if both of them perform the local Z measurement M_{zz} on their halves of the m pairs, they share the ideal key state $\rho_{ABE}^{\mathrm{ideal}}$ in Eq. (2). In other words, the amount of distillable entanglement from quantum transmission gives a lower bound on the key-generation rate.

The main idea of the Lo-Chau security proof is that Alice and Bob can apply quantum error correction to distill entanglement, after which Alice and Bob share a quantum state ρ_{AB}, which ideally should be EPR pairs with the form of $|\Phi^+\rangle^{\otimes m}$. In reality, when the data size is finite, the entanglement distillation might fail with a small failure probability ε_f, which can be understood as the failure probability of quantum error correction,

$$\langle\Phi^+|^{\otimes m}\rho_{AB}|\Phi^+\rangle^{\otimes m} \ge 1-\varepsilon_f. \tag{7}$$

After considering Eve's system E, one can show the fidelity as [see Appendix A in Fung, Ma, and Chau (2010)]

$$F(\rho_{ABE}, (|\Phi^+\rangle\langle\Phi^+|)^{\otimes m} \otimes \rho_E) \ge 1-\varepsilon_f. \tag{8}$$

Then after the local Z measurement on system A and B, M_{zz}, for key generation the trace distance of the key state ρ_{ABE} to the ideal state $\rho_{ABE}^{\mathrm{ideal}}$ is bounded by

$$\begin{aligned}\frac{1}{2}||\rho_{ABE}-\rho_{ABE}^{\mathrm{ideal}}||_1 &= \frac{1}{2}||M_{zz}(\rho_{ABE})-M_{zz}(|\Phi^+\rangle\langle\Phi^+|^{\otimes m}\otimes\rho_E)||_1\\ &\le \frac{1}{2}||\rho_{ABE}(|\Phi^+\rangle\langle\Phi^+|)^{\otimes m}\otimes\rho_E||_1\\ &\le \sqrt{1-F(\rho_{ABE},|\Phi^+\rangle\langle\Phi^+|^{\otimes m}\otimes\rho_E)^2}\\ &\le \sqrt{\epsilon_f(2-\epsilon_f)}.\end{aligned} \tag{9}$$

In the literature, fidelity is widely used for security parameter quantification in QKD security proofs (Lo and Chau, 1999; Shor and Preskill, 2000; Koashi, 2009). To make the security parameter composable (Ben-Or *et al.*, 2005; Renner and König, 2005), one can apply Eq. (9) to bound the trace distance.[15]

The main job of a security analysis is to make sure that Alice and Bob eventually share almost perfect EPR pairs before they make the final ZZ measurement to obtain secure key bits. The procedure to extract perfect EPR pairs from imperfect ones is called entanglement distillation (Bennett *et al.*, 1996). The main idea of the Lo-Chau security proof lies in *quantum error correction* (Lo and Chau, 1999), which proves the security of an entanglement-based QKD protocol. Let us recap the Bennett-Brassard-Mermin 1992 (BBM92) (Bennett, Brassard, and Mermin, 1992) protocol, an entanglement version of BB84 in Box II.B.1. For simplicity of description, we assume that Alice and Bob own quantum

[15] It is interesting to note that in the original Lo-Chau and Shor-Preskill security proofs, fidelity is used as an intermediate measure to finally bound the mutual information between the final key and Eve's system. In fact, this mutual information definition is not composable.

memories, which will be removed shortly in the Shor-Preskill security proof (Shor and Preskill, 2000).

Box II.B.1: BBM92 protocol with quantum memorie. An entanglement version of BB84.

(1) Alice prepares an EPR pair $|\Phi^+\rangle$, stores one half of it locally, and sends the other half to Bob.
(2) Upon receiving a qubit, Bob stores half of the EPR pair in a quantum memory. If the qubit is lost in the channel or the quantum storage fails, Alice and Bob discard the pair.
(3) Repeat the first two steps many times until Alice and Bob store N pairs of qubits.
(4) With the help of preshared perfect EPR pairs, Alice and Bob apply a quantum error correcting code to correct all of the errors in the N pairs.
(5) After a random hashing test, Alice and Bob share almost perfect EPR pairs. They return the cost of pairs in the previous step and measure the rest in the local Z basis to obtain the final key.

The quantum random hashing test happens in the two conjugate bases separately. In each basis, Alice and Bob can compare the parities of the qubits. Comparison of each parity will cost Alice and Bob an EPR pair. Once they agree on enough numbers of parities, the states are stabilized by the operations $X \otimes X$ and $Z \otimes Z$, with a small failure probability. This step comes from the error verification in classical error correction (Fung, Ma, and Chau, 2010). There are a few notes on this scheme.

(1) This scheme is source device independent, which means that the source cannot be fully trusted (Koashi and Preskill, 2003). In the first step, the state preparation can be done by Eve. Then Eve prepares qubit pairs (designed to be EPR pairs) and sends them to Alice and Bob, who store the quantum states in memories. Remaining steps 4 and 5 are the same.
(2) After quantum transmission, Alice and Bob share N EPR pairs. Owing to channel disturbance or Eve's interference, these N EPR pairs are generally imperfect and might be entangled with each other and Eve's system. Here we consider the most general coherent attacks.
(3) In a security proof, it is crucial to evaluate the number of EPR pairs that are cost in step 4.

When Alice and Bob are both measured in the local Z basis, an error occurs when the outcomes are different. We call it a *bit error*. Similarly, when they are both measured in the X basis, a *phase error* occurs when the outcomes are different. Denote the bit and phase error rates as e_b and e_p, respectively:

$$e_b = \frac{\text{No. of bit errors}}{N},$$
$$e_p = \frac{\text{No. of phase errors}}{N}. \tag{10}$$

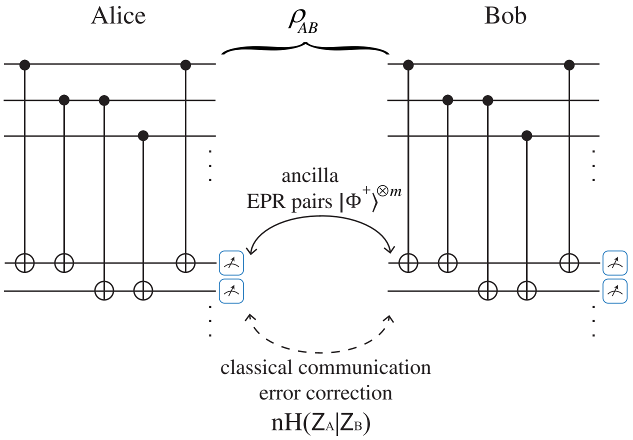

FIG. 3. Illustration of bit error correction. By adding Hadamard gates, the circuit can also be used for phase error correction.

Since we are considering the most general coherent attacks, the errors are in general not independent but correlated. Note that bit and phase errors can be defined in any two complementary bases in the qubit case. For quantum signals measured in a particular basis where the bit error is defined, the phase error denotes the hypothetical error if these signals are measured in its complementary basis. For higher-dimension cases, such definitions become slightly trickier with more than one type of phase error.

To distill perfect EPR pairs from imperfect ones with errors defined in Eq. (10), Alice and Bob can employ quantum error correction. Entanglement distillation can be done in two steps via bit and phase error correction. In bit error correction, Alice hashes her qubits in the Z basis by applying the controlled-NOT (CNOT) gate to ancillary perfect EPR pairs, as shown in Fig. 3. Alice sends the measurement results of ancillary qubits to Bob, which serves as the error syndrome in error correction. In the infinite data size limit, the number of perfect EPR pairs cost in this procedure is given by the Shannon entropy $NH(e_b)$. By applying Hadamard gates, one can switch between bit and phase spaces. Then, similarly, the phase error correction costs additional $NH(e_p)$ EPR pairs.

Finally, the net rate of EPR pairs generated is given by

$$r \geq 1 - H(e_b) - H(e_p), \tag{11}$$

where $H(e) = -e \log e - (1-e) \log(1-e)$ is the binary Shannon entropy function. Note that Eq. (11) is not tight, in general. If two-way classical communication is allowed in quantum error correction, more keys can be distilled (Chau, 2002; Gottesman and Lo, 2003).

In reality, when the data size is finite, the entanglement distillation might fail with a small failure probability, which can be understood as the failure probability of quantum error correction. In original security proofs (Lo and Chau, 1999; Shor and Preskill, 2000; Koashi, 2009), the fidelity between the key state ρ_{ABE} to the ideal state $\rho_{ABE}^{\text{ideal}}$ is often used as an intermediate measure to finally bound the mutual information between the final key and Eve's system. In fact, this definition is not composable. To make the security parameter composable (Ben-Or *et al.*, 2005; Renner and König, 2005), one can apply the connections between fidelity and trace distance using a general inequality relating them; see Sec. III of Fung, Ma, and Chau (2010).

2. Shor-Preskill proof: Reduction to prepare-and-measure schemes

In general, this quantum error correction–based entanglement distillation procedure, which is the essence of the

Lo-Chau security proof, requires quantum memories and quantum computers. However, these quantum memories and quantum computers are not available with the current technology (Lo and Chau, 1999). To remove this quantum memory or quantum computer requirement, one can move the final measurement ahead of the two error correction steps. The bit error correction becomes classical error correction, and the phase error correction becomes privacy amplification (Shor and Preskill, 2000). There are a few steps for this permutation of operations to work.

(1) Quantum bit and phase error correction operations commute, as shown in Fig. 3. This is due to the fact that Alice and Bob use EPR pairs as ancillary qubits.

(2) The Z-basis measurement on the ancillary EPR qubits commutes with all operations for error correction. This is straightforward to see since there are only two possible operations on ancillary qubits I and X (from the CNOT operation), both of which commute with the Z measurement.

(3) The Z-basis measurement on the Alice and Bob qubits commutes with the bit error correction. This is true since the $Z \otimes Z$ measurement commutes with CNOT operation. After moving the Z measurement ahead, the CNOT operation becomes a regular XOR operation on the two outcome bits.

(4) The Z-basis measurement on the Alice and Bob qubits commutes with the phase error correction. This relies on the use of EPR pair ancillary states.

(5) In phase error correction, after locating the errors phase error correction does not affect the values of the final key measurement in the Z basis. Thus, no "correction" operation is needed. Of course, the EPR pairs are still a cost in this step.

(6) Then all quantum operations become classical bit operations, essentially hashing.

(7) To perform privacy amplification, one still needs to estimate the phase error rate e_p. Now let us focus on the case in which the key bits are measured in the Z basis. The phase error rate can be estimated by measuring the key bits in the X basis. Of course, for this estimation to work one needs to make sure that the sampling is fair, which raises the critical assumptions in the security proof discussed in Sec. II.C.

After considering the permutation of quantum error correction and measurement, Alice and Bob can directly measure the EPR pairs once they receive them. Suppose that Alice prepares the original EPR pairs, measures halves of the pairs, and sends the remaining halves to Bob. Conditional to Alice's measurement outcomes, the states sent from Alice to Bob are pure. It is equivalent for Alice to prepare these states directly and send them to Bob. Now the entanglement-based protocol is reduced to a prepare-and-measure one.

The reduction from quantum bit error correction to classical error correction is easy to understand. Take Fig. 3, for example. Alice and Bob need to compare the ancillary qubit measurement results. Since the final $Z \otimes Z$ measurement commutes with the CNOT operation, one can measure all qubits in the Z basis first and in the XOR operation the bit values of all measurement outcomes of the control qubits to the target qubits. The CNOT links shown in Fig. 3 can be understood as a hashing matrix, meaning that the situation is equivalent to constructing a matrix and multiplying it by the raw bit string. Of course, such an error correction is linear. In general, any error correcting code can be applied once the bit and phase error corrections can be decoupled.

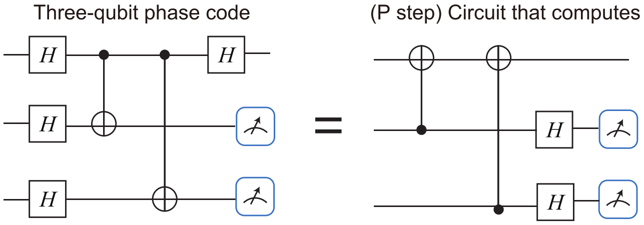

FIG. 4. Equivalence between the phase error correction and privacy amplification. The outcome of a simple three-qubit repetition phase error correcting code is the same as the hashing of the three bit values.

The reduction from quantum phase error correction to privacy amplification is trickier. In general, after Hadamard gates CNOT operation does not commute the Z measurement any more. In fact, those two operations anticommute. In this case, Alice and Bob can design a phase error correcting code such that it commutes with the Z measurement. Again, let us take the linear code as an example. A certain number of parity bits needs to be exchanged for error correction. Assuming universal hashing, Alice sends $NH(e_p)$ bits to Bob, and Bob corrects the phase errors. Note that the final key measurement must commute with this hashing. Then they can use the null space of the hashing matrix as with the final key space. The equivalence between phase error correction and privacy amplification is illustrated in Fig. 4. This can also be understood as a random number extraction. Alice and Bob use the phase error rate to estimate the randomness in the key and apply universal hashing to extract true randomness.

In quantum error correction, we assume that Alice and Bob use ancillary EPR pairs. As shown in Fig. 3, with EPR pairs bit and phase error correction operations commute with each other. That is, one can decouple these two error correction steps (Lo, 2003). In the Shor-Preskill security proof (Shor and Preskill, 2000), no ancillary EPR pairs are employed. Instead, the CSS quantum error correcting code (Calderbank and Shor, 1996; Steane, 1996) is used to decouple these two steps.

After the reduction to prepare-and-measure schemes, the data postprocessing can be divided into two steps: error correction and privacy amplification. Error correction is a step to reconciliate Alice's and Bob's sifted key. If we allow one-way key reconciliation, the cost in this step is $H(A|B)$, where A and B represent the random variables of Alice's and Bob's sifted key, respectively. In a symmetric channel where the detected numbers of 0 and 1 bits are the same, the cost per bit is given by $H(e_b)$, as shown in Eq. (11). It turns out that the cost can be reduced if we allow two-way key reconciliation. The optimal key rate is an open question even in the classical key agreement case (Maurer and Wolf, 1999).

Privacy amplification is a procedure for Alice and Bob to distill a common private key from a raw key about which Eve might have partial information (Bennett *et al.*, 1995). The concept of privacy amplification is closely related to the

TABLE X. List of tolerable error rate bounds for different schemes and proofs. The upper bounds are evaluated by simple individual (intercept-and-resend) attacks (Gottesman and Lo, 2003).

Scheme	One way	Two way	Upper bound
BB84	11.0%	20.0%	1/4
Six state	12.7%	27.6%	1/3

randomness extraction problem (De *et al.*, 2012; X. Ma *et al.*, 2013). The difference is that in privacy amplification local randomness is a free resource, whereas in randomness extraction any randomness is valuable. Note that initially the classical treatment on privacy amplification (Bennett *et al.*, 1995) is applicable to QKD only under restrictive assumptions, i.e., the adversary has no quantum memory. Later, however, this treatment was generalized to the case where the adversary has quantum memory (Renner, 2008). Details of data postprocessing, which distills a secure key from the raw data measured in quantum transmission (see Fig. 6), are presented in Sec. III.E.

In the end, Eq. (11) gives the key rate of the BB84 protocol. Considering the symmetric case where the bit and phase error rates are the same, it is not hard to see that the tolerable error rate of Eq. (11) is 11%, compared to 7% in the Mayers proof (Mayers, 2001). Similar to the entanglement distillation case, this formula is not tight. With two-way classical communication, one can achieve advantage distillation (Gottesman and Lo, 2003) using bit-flip error *detection*. Nonetheless, phase error detection remains forbidden in the absence of quantum computers. From the QKD postprocessing point of view, the bit and phase errors might be correlated. Alice and Bob can perform some preprocessing to reduce the total amount of key cost in error correction and privacy amplification. For example, they can group bits into pairs, compare parities, and discard the ones with different parities. In this way, one can reduce the errors in the remaining bits. This is called the B step (Gottesman and Lo, 2003). It turns out that such prepossessing is useful in practical QKD processing (Ma *et al.*, 2006). With two-way classical communication, one can also increase the tolerable error rates (Chau, 2002; Gottesman and Lo, 2003). In addition, with the six-state protocol (Bruß, 1998; Lo, 2001) it has been shown that the tolerable error rate is higher. We list all of the tolerable error rates in Table X. Apparently, there are gaps between the lower (tolerable) and upper error rate bounds. This has been an open question in QKD as well as in entanglement distillation for many years that is related to the key agreement problem in the classical communication case (Maurer and Wolf, 1999).

3. Koashi's complementarity approach

The aforementioned security analyses by Lo and Chau and Shor and Presill based on quantum error correction complications certainly benefit from strong intuition from entanglement to privacy. In fact, it turns out that entanglement (or a quantum channel that is capable of transmitting an entangled state) is a precondition for secure QKD (Curty, Lewenstein, and Lütkenhaus, 2004). The main drawback of this approach is the complication of introducing a virtual entanglement-based protocol. Although the bit and phase error correction can be decoupled in postprocessing by employing the CSS quantum error correcting code (Shor and Preskill, 2000) or ancillary EPR pairs (Lo, 2003), these two steps always mix together in security proofs. Sometimes constructing a virtual entanglement protocol can be highly nontrivial (Tamaki, Koashi, and Imoto, 2003; Tamaki and Lütkenhaus, 2004; Fung *et al.*, 2009). Error correction and privacy amplification are significantly different procedures in conventional cryptography. The former is to guarantee that Alice and Bob share an identical key, while the latter is to make sure that they share a private key. One key observation is that the error correction step is not directly related to quantum laws in the security analysis. That is, if Alice and Bob want to share an identical key only, they can just transmit classical states to do the job. From this observation, Koashi (2009) developed a simplified security proof framework based on *complementarity.*

In Koashi's approach, error correction and privacy amplification are decoupled from the beginning. Alice and Bob perform error correction first to make sure that the two bit strings are the same. Now the problem becomes, how many private key bits can be distilled from Alice's (same as Bob's) error corrected key? In this case, we need to deal with only two parties Alice and Eve. Denote the length of Alice's key string as N. Alice's N-bit string can be regarded as the Z-basis measurement outcome of N qubits $\rho_A \in \mathcal{H}_{2^N}$. Note that under the most general coherent attacks these N qubits are correlated (or even entangled) with each other. The key idea is that in a virtual protocol if each qubit of ρ_A is measured in the complementary X-basis measurement and only $+1$ results are obtained, then $\rho_A = |+\rangle^N$, where $|+\rangle$ is the eigenstate of X with the eigenvalue $+1$. In this ideal scenario, no one (including Eve) can predict Alice's key bits without accessing the measurement results directly. Like the EPR pairs discussed in the Lo-Chau security proof, this ideal case renders perfect privacy. This unpredictability in the computational Z basis is quantified by the coherence measure in resource theory (Yuan *et al.*, 2015), which was recently connected to the security of QKD (Ma *et al.*, 2019).

In general, ρ_A is not a product of $|+\rangle$ states. In this framework, the phase error rate e_p is defined as the ratio of getting -1 eigenstates of the complementary X-basis measurement for ρ_A. The parameter e_p can be estimated differently in different QKD protocols. For instance, in BB84 Alice essentially randomly chooses some qubits to be measured in the X basis and uses random sampling to estimate e_p. Details of random sampling for parameter estimation are discussed in Sec. III.E. Now, Alice can perform a virtual phase error correction on her N qubits by means similar to that discussed for the Lo-Chau phase error correction. Alice can hash the X-basis measurement outcomes and find the error syndrome. After phase error correction, Alice's state becomes close to $|+\rangle^N$, again, measured by fidelity or trace distance.

The key difference between the Lo-Chau and Koashi security proofs lies in the definition of the phase error rate e_p. In the Lo-Chau security proof, e_p is defined in Bob's system relative to Alice's, while in the Koashi proof it is defined on Alice's or Bob's side locally depending on protocols, and Bob or Alice can have an arbitrary system (irrelevant for security). In Koashi's approach, the complementary basis can be chosen arbitrarily as long as e_p can be estimated accurately. Meanwhile, along the lines of the complementarity approach, security proofs based on entropic uncertainty relations (Coles *et al.*, 2017) have been developed (Koashi, 2006; Berta *et al.*, 2010).

In summary, the Lo-Chau, Shor-Preskill, and Koashi security proofs are all based on phase error correction. Note that in this line of approach the estimation of e_p is at the core of the security analysis. Sometimes more sophisticated tools like semidefinite programming are employed to upper bound the phase error rate (Y. Wang *et al.*, 2019). Recently, there has been an effort to make a connection between the Shor-Preskill type of security proof (Shor and Preskill, 2000; Koashi, 2009) and the entropic approach (Renner, 2008) by Tsurumaru (2018).

Thus far the security proof reviewed here has focused on the BB84 protocol. The security proof based on phase error correction can be extended to other protocols, like Bennett 1992 (B92) (Bennett, 1992; Tamaki, Koashi, and Imoto, 2003) and six-state protocols (Bruß, 1998; Lo, 2001). Meanwhile, this technique can also be employed in general qudit systems (Chau, 2005). Note that there is a security proof based on the idea of twisted states (Horodecki *et al.*, 2008a, 2008b). Intuitively twisted states include shields. This allows the phase error correction syndrome to be hidden in the shield and thus become inaccessible to Eve. In principle, a virtual conceptual measurement on the joint state of Alice and Bob's shield would allow them to extract the missing phase error correction syndrome to complete the quantum error correction process. In practice, Alice and Bob do not need to perform such a virtual measurement.

4. Entropic approach

There is another line of security analysis (Renner, Gisin, and Kraus, 2005; Renner, 2008; Scarani and Renner, 2008; Tomamichel *et al.*, 2012; Coles *et al.*, 2017) that originates from the communication complexity and quantum memory approach (Ben-Or, 2002; Renner, 2008). Based on the entanglement distillation idea, a framework was established for a general ρ_{AB} by Devetak and Winter (2005). In this quantum-entropy based framework, Alice and Bob share many independent and identically distributed (i.i.d.) copies of ρ_{AB}, on which they perform measurements to obtain key bits. The Devetak-Winter key-rate formula is given by

$$\begin{aligned} r &= S(A|E) - H(A|B), \\ S(A|E) &= S(\rho_{AE}) - S(\rho_E) \\ &= S(\rho_B) - S(\rho_{AB}), \end{aligned} \tag{12}$$

where $S(A|E)$ is conditional quantum entropy and $S(A) = -\mathrm{Tr}(\rho_A \log \rho_A)$ is the von Neumann entropy. In the derivation, we assume the worst-case scenario in which ρ_{ABE} is pure. In fact, the privacy amplification term can also be written in a relative entropy form (Coles, Metodiev, and Lütkenhaus, 2016)

$$S(A|E) = D[\rho_{AB}||\Delta_z(\rho_{AB})], \tag{13}$$

where $\Delta_z(\rho_{AB}) = \sum_i |i\rangle\langle i|_A \rho_{AB} |i\rangle\langle i|_A$ is the partial dephasing operation on system A in the Z basis and the relative entropy function $D(\rho||\sigma) = \mathrm{Tr}\rho \log \rho - \mathrm{Tr}\rho \log \sigma$. This allows us to give an operational interpretation of coherence in QKD (Ma *et al.*, 2019).

The density matrix information ρ_{AB} is unknown to Alice and Bob due to Eve's interference. They have to monitor ρ_{AB} in real time, say, via tomography. Thus, the Devetak-Winter analysis is normally applied in the i.i.d. case, where Eve interferes with all rounds of QKD identically and independently, i.e., a collective attack (Renner, 2008; Scarani and Renner, 2008). Nonetheless, the security analysis can be extended to the case of a coherent attack by further analysis (Tomamichel *et al.*, 2012; Coles *et al.*, 2017), such as the de Finetti theorem (Renner, 2007), the postselection technique (Christandl, König, and Renner, 2009), and the uncertainty relation for smooth entropies (Tomamichel and Renner, 2011). Another advantage of this approach is that the security of a complicated QKD scheme can be analyzed numerically (Coles, Metodiev, and Lütkenhaus, 2016; Winick, Lütkenhaus, and Coles, 2018).

C. Security assumptions

We now discuss the security assumptions made in general security proofs. We focus on the BB84 protocol, but most of the discussions can be applied to other protocols, such as B92, BBM92, and the six-state protocols. In security proofs (Lo and Chau, 1999; Shor and Preskill, 2000; Koashi, 2009), as shown in Sec. II.B, we assume that Alice sends ideal qubit states in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ and Bob performs ideal qubit Z-basis and X-basis measurements. The channel, on the other hand, is assumed to be under the full control of Eve.

Nevertheless, in actual experiments these assumptions can be problematic. Table XI summarizes the main differences between the security assumptions of security proofs and typical experimental setups. These differences, if unnoticed, might essentially open the security issue of *basis dependency* between the Z basis and the X basis, thus causing the problem of quantum hacking attacks; see Table I.

1. Source

First, let us relax the requirement for sources by considering a more general source. In a prepare-and-measure QKD protocol, Alice randomly prepares system B on one of the four states $\{\rho_{x0}, \rho_{x1}, \rho_{z0}, \rho_{z1}\}$ and sends it to Bob. These four states can be denoted as $\rho_{\beta\kappa}$, where $\beta \in \{X, Z\}$ represents the encoding basis and $\kappa \in \{0, 1\}$ represents the encoding key bit. Here we consider four states with two bases, but such a scenario can

TABLE XI. Security assumptions and actual setup for BB84.

Component	Security assumption	Practical setup
Photon source	Ideal single photon	Coherent laser
Encoding state	Two dimension	Arbitrary dimension
Encoding state	Basis independent	Source flaws
Measurement	Two dimension	Arbitrary dimension
Measurement	Basis-independent	Measurement flaws
Photon detection	Ideal SPD	Threshold detector

be easily extended to more general cases with an arbitrary number of states and bases.

The prepare-and-measure protocol can be linked to the entanglement-based one as follows. Define the purification of state $\rho_{\beta\kappa}$ as $|\psi_{\beta\kappa}\rangle_{A_0B}$, where system A_0 is an ancillary system. From an entanglement-based view of the protocol, Alice sending out state $\rho_{\beta\kappa}$ is equivalent to her preparing

$$|\Psi_{\beta}\rangle_{AA_0B} = \frac{1}{\sqrt{2}}\sum_{\kappa}|\beta_{\kappa}\rangle_{A}|\psi_{\beta\kappa}\rangle_{A_0B}, \tag{14}$$

measuring system A in the β basis, and sending out system B according to the measurement result κ. Here system A is a qubit system and $|\beta_{\kappa}\rangle_{A}$ is the β-basis eigenstate whose eigenvalue is κ. For the ideal BB84 protocol, there is no ancillary system A_0 (or A_0 is just a detached trivial system) since all encoding states $\rho_{\beta\kappa}$ are pure. Then the states sent by Alice are

$$\rho_{\beta\kappa} = \mathrm{Tr}_{A_0}(|\psi_{\beta\kappa}\rangle\langle\psi_{\beta\kappa}|_{A_0B}), \tag{15}$$

the four BB84 states.

To send out $\rho_{x\kappa}$, in the entanglement-based equivalent protocol, Alice prepares

$$|\Phi^{+}\rangle_{AB} = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)_{AB}\,,$$

measures system A on the X basis, and obtains the measurement result κ. Similarly, to send out $\rho_{z\kappa}$, Alice first prepares

$$|\Phi^{+}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}\,,$$

measures A on the Z basis, and obtains the measurement result κ. No matter which basis Alice wants to send, the initial entangled states prepared are the same. Denote the X-basis state and Z-basis state as

$$\begin{aligned}\rho_x &= \tfrac{1}{2}(\rho_{x0} + \rho_{x1}),\\ \rho_z &= \tfrac{1}{2}(\rho_{z0} + \rho_{z1}),\end{aligned} \tag{16}$$

which are the quantum states transmitted when Alice and Bob choose the X and Z bases, respectively. Thus, in the ideal BB84 source case the state sent out by Alice is independent of the basis choice

$$\rho_x = \rho_z. \tag{17}$$

We call this kind of source *basis independent* (Koashi and Preskill, 2003; Ma, Fung, and Lo, 2007).

In the original proposal of the BB84 protocol, the basis choice was assumed to be unknown to Eve. This is also a crucial assumption in security proofs (Lo and Chau, 1999; Shor and Preskill, 2000), as shown in Sec. II.B. This is important for phase error estimation. If the source is basis dependent, one cannot simply use one basis information to estimate the other. This is guaranteed by Eq. (17). In fact, as long as the source is basis independent, it can be in an arbitrary dimension or state. It can even be assumed to be under the control of Eve.

In practice, it is hard to construct single-qubit sources. Instead, entangled-photon sources are widely used as a basis-independent source. For entangled-photon sources to work as a basis-independent source, note that the measurement for heralding has to be basis independent. In Sec. II.D.1, we show that the security can be guaranteed once the source contains a certain amount of basis-independent components.

In some QKD schemes, such as BBM92 (Bennett, Brassard, and Mermin, 1992), Alice and Bob choose bases after the quantum signals transmitted through the channel. In the BBM92 protocol, Alice prepares an entangled source, holds one part by herself, and sends another to Bob. Alice measures her own part in some basis to realize the basis choice and encoding. In these schemes, the quantum source can even be assumed to be in the possession of Eve. Then for these schemes, Eq. (17) can be guaranteed by the experimental setting.

2. Measurement

The measurement requirement is similar. Again, take the BB84 protocol as an example. There are four measurement outcomes labeled by two bits, β and κ. The corresponding four positive operator-valued measurement (POVM) elements are $M_{\beta\kappa}$,

$$\begin{aligned}M_x &= M_{x0} + M_{x1},\\ M_z &= M_{z0} + M_{z1}.\end{aligned} \tag{18}$$

Here $\{M_{x0}, M_{x1}\}$ form the X-basis measurement, while $\{M_{z0}, M_{z1}\}$ form the Z-basis measurement. We also require the measurement to be basis independent,

$$M_x = M_z. \tag{19}$$

On the measurement side, the requirement is more strict. For the security proof presented in Sec. II.B, we must have qubit measurements in the X and Z bases. Such a requirement can be extended to more general projection measurements.

In practice, a *squashing model* is widely employed (Gottesman *et al.*, 2004; Beaudry, Moroder, and Lütkenhaus, 2008; Fung, Chau, and Lo, 2011). In a squashing model, an arbitrary quantum state from the channel is projected to a qubit or vacuum. Then the X or Z measurement is performed. It has been proven that a typical threshold detector model adapts to the squashing model (Beaudry, Moroder, and Lütkenhaus, 2008; Tsurumaru and Tamaki, 2008).

Now one can see that the assumptions on the source and measurement are quite different. For the source, one needs only to guarantee its basis-independent property in Eq. (17). It must be a specific projection measurement. In practice, the source requirement is easier to meet than the measurement requirement. Hence, there are more practical security issues with measurement than with source. A full security analysis needs to take these measurement deviations into account. We present this in Sec. II.D.1. This problem is finally resolved by MDI-QKD (see Sec. VI.B).

3. Channel

In security proofs, the channel is assumed to be under the full control of Eve. Thus, in principle, we do not put any requirements on the channel. In fact, if any implementation deviation from the ideal QKD protocol can be put into the channel, it will not cause any security problems. For example, detectors normally have a finite efficiency. The loss caused by detectors can be moved to the channel. Then a detector can be replaced by a 100% efficient one in the security analysis.

The question now is, what kind of implementation deviations can be moved to the channel? The implementation deviation can be regarded as some deviation operation acting on an ideal implementation. The key requirement is that the deviation operation must commute with the basis switch operation. Alice and Bob each use a basis switching device (say, a phase modulator in phase-encoding schemes). The channel is defined as the operation on the quantum signals between the two basis switching devices.

D. Practical security analysis

In practice, there are two issues that need to be addressed: device imperfection and statistical fluctuation. In Sec. II.C, we review the assumptions in the security proofs. In reality, these assumptions might be fully satisfied. Implementation devices may deviate slightly from the ideal case used in the security proofs. When the deviation is small enough, we expect a secure key still to be generated. In Sec. II.D.1, we review the quantification of device imperfections and its effects on the security analysis.

In principle, the error rates defined in Eq. (10) cannot be obtained accurately since they are measured in complementary bases. In the security proofs reviewed in Sec. II.B, we employ random sampling to estimate the error rates. When the data size goes to infinity, the error rates approach error probabilities, which can be estimated accurately. In a finite data size, such a parameter estimation would render a finite confidence interval. In Sec. II.D.2, we review the parameter estimation with random sampling by calculating the failure probabilities and parameter bounds.

In Sec. III.E, we review the classical postprocessing of QKD and explain how Alice and Bob can distill secure keys in the raw bit strings from quantum measurement to final secure keys with the help of public discussions. Note that some of the discussions need to be encrypted and/or authenticated.

1. Gottesman-Lo-Lütkenhaus-Preskill (GLLP) framework

There exist deviations between realistic QKD systems and the ideal QKD protocol. To achieve practical security of a QKD system, Alice and Bob need to characterize these device deviations or imperfections carefully and take them into account in the security analysis. Based on previous work on the topic (Lütkenhaus, 2000; Inamori, Lütkenhaus, and Mayers, 2007), Gottesman *et al.* (2004) established a general framework for security analysis with realistic devices.

First, Alice and Bob need to characterize their devices to see how much deviation there is from the ideal ones used in the security proofs. One can employ typical distance measures, like fidelity and trace distance, to quantify the deviation. In principle, Alice and Bob can perform a virtual measurement on the devices for each run in real time to see whether it works the same as the "ideal device" or its "orthogonal case." Then they can tag the sifted key bit as "good" if the virtual measurement projects to the ideal case, and "bad" if it is the orthogonal case. Of course, in reality Alice and Bob do not know the virtual measurement result. Instead, they know the ratio of these two cases. Both source and measurement imperfections can fit into this scenario. The GLLP security analysis essentially tells us how to extract secure bits when the good bits are mixed with bad ones. Thus far the discussion has been rather abstract. In the following, we take the source imperfection as an example.

The framework is generic. Here let us take the BB84 protocol as an example. In reality, a weak coherent-state photon source is widely used as an approximate single-photon source. With phase randomization, one can treat the weak coherent-state photon source as a mixture of Fock states (Lo, Ma, and Chen, 2005). The vacuum and single-photon components are basis independent, whereas the multiphoton components are not. In principle, Alice can measure the photon number to tag each encoded state as basis independent or not (this is the aforementioned virtual measurement part). Denote the ratio of Bob's detected bits from the basis-independent source (the good part, e.g., the vacuum and single-photon component in the BB84 protocol) as $1-\Delta$, and the rest (the bad part, e.g., the multiphoton components in the BB84 protocol) as Δ. Details of the source model and its security analysis are presented in Sec. III.B.

With Alice's tagging information (photon number, in this example), she can sort the sifted key bit string k_A into two substrings k_{good} and k_{bad}, where

$$\begin{aligned} |k_{\text{good}}| &= (1-\Delta)N, \\ |k_{\text{bad}}| &= \Delta N. \end{aligned} \tag{20}$$

Following the phase error correction security proof, the underlying phase error rate of k_{good} is e_p, which can be estimated accurately via complementary measurements. The phase error rate of k_{bad} is unknown. In the worst-case scenario, the phase error rate of the string k_{bad} could be as high as $1/2$. The main idea of the GLLP security analysis is that if Alice and Bob employ linear privacy amplification, such as the matrix hashing introduced in Sec. III.E, they can still distill secure keys from k_{good} by accessing k_A only.

Denote k'_{good} as the bit string if Alice modifies the sifted key bit string by setting the bad bit positions to 0. Similarly, denote k'_{bad} as the bit string if Alice sets the good bit positions at 0. Then

$$\begin{aligned} |k'_{\text{good}}| = |k'_{\text{bad}}| &= |k_A|, \\ k'_{\text{good}} \oplus k'_{\text{bad}} &= k_A. \end{aligned} \tag{21}$$

Suppose that a hashing matrix T can distill secure bits from k_{good}. That is, Tk_{good} is a secure key. It is then not hard to show that $T'k'_{\text{good}}$ results in the same secure key if one extends the matrix T to T' by inserting new columns corresponding to the bad positions of k'_{good}. That is, T is determined as a submatrix of T' by taking certain column vectors. Here comes the clever trick of the GLLP security analysis: since $T'k'_{\mathrm{good}}$ is private, the XOR result

$$T'k'_{\mathrm{good}} \oplus T'k'_{\mathrm{bad}} = T'(k'_{\mathrm{good}} \oplus k'_{\mathrm{bad}}) = T'k_A \qquad (22)$$

is also private even though Eve knows everything about $T'k'_{\mathrm{bad}}$. Note that the new added columns from T to T' can be arbitrary. In practice, Alice can just pick up a universal hashing matrix T' to do privacy amplification and its submatrix T will automatically be a smaller universal hashing matrix.

Therefore, the secure key-rate formula of Gottesman, Lo, Lütkenhaus, and Preskill is given by

$$r \geq -H(E) + (1-\Delta)[1 - H(e_p)], \qquad (23)$$

where E is the total QBER. This key-rate formula can be viewed as an extension to Eq. (11). Furthermore, we need not restrict ourselves to two tag cases, good and bad. In principle, Alice and Bob can label sifted key bits with an arbitrary dimensional tag g, and for each g they can derive its corresponding phase error rate e_p^g. With the same argument as before, we can extend the GLLP formula (Ma, 2008),

$$r \geq -H(E) + \sum_g q_g[1 - H(e_p^g)], \qquad (24)$$

where q_g is the ratio of sifted key bits with the tag g and $\sum_g q_g = 1$. Here we assume that Alice and Bob cannot access the tag g in reality, and hence they have to do the error correction part for all bits together. If they can really read out tags for each run, they can divide this error correction part as well.

2. Random sampling and finite data size

The infinite data size limit ($N \to \infty$) is used for the key-rate formula, Eqs. (11) and (24). When the data size is finite, the phase error rate e_p used to evaluate the amount of privacy amplification cannot be measured accurately. Instead, Alice and Bob can bound e_p via certain complementary measurements.

In the BB84 protocol, the phase error probability in the Z basis is the same as the bit error probability in the X basis. In the following discussion, we assume that Alice and Bob have obtained the sifted key in the Z-basis measurement and want to estimate the underlying phase error rate e_p. Thus, by sampling the qubits in the X basis, Alice and Bob can bound e_p. This is a typical *random sampling* problem. Given a certain number of phase error rates in $n_x + n_z$ positions, Alice and Bob randomly sample n_x positions for phase error testing and find $n_x e_{bx}$ errors. The sampling problem lies in bounding the phase error rate e_{pz} in the remaining n_z positions. The upper bound is related to the failure probability by a hypergeometric function (Fung, Ma, and Chau, 2010).

Specifically, the main objective is to evaluate the deviation θ of the phase error rate from the tested value, the bit error rate in the complementary basis, due to the finite-size effect. Here we recap the results from Sec. IX of Fung, Ma, and Chau (2010) and list the variables in Table XII. The phase error rate e_{pz} is bounded by

TABLE XII. List of notations in phase error estimation.

Notation	Definition
n_z	Number of bits measured in the Z basis
n_x	Number of bits measured in the X basis
e_{bx}	Bit error rate in the X basis
e_{pz}	Phase error rate in the Z basis
q_x	Sampling ratio $n_x/(n_x+n_z)$
θ	Deviation of the phase error rate
ε_{ph}	Failure probability of phase error estimation

$$e_{pz} \leq e_{bx} + \theta, \qquad (25)$$

with a failure probability of

$$\varepsilon_{\mathrm{ph}} \leq \frac{\sqrt{n_x + n_z}}{\sqrt{e_{bx}(1-e_{bx})n_x n_z}} 2^{-(n_x+n_z)\xi(\theta)}, \qquad (26)$$

where $\xi(\theta) = H(e_{bx}+\theta-q_x\theta) - q_x H(e_{bx}) - (1-q_x)H(e_{bx}+\theta)$. If we take the Taylor expansion of Eq. (26), one can obtain the first order approximation essentially the same as the Gaussian limit used in the Shor-Preskill security proof (Shor and Preskill, 2000).

Another approach to deal with the problem of the finite-size effect is by employing the *smooth min-entropy* model (Renner, 2008), which is a valid measure of randomness in the nonasymptotic cases and degenerates to Shannon entropy in the i.i.d. limit. This approach has been applied to QKD to prove the finite-key security with almost tight bounds (Tomamichel and Renner, 2011; Tomamichel *et al.*, 2012). Moreover, the smooth min-entropy approach generally deals with non-i.i.d. cases and can be applied to other quantum information processing protocols, such as one-shot coherence resource theory (Zhao *et al.*, 2018) and device-independent QKD (Arnon-Friedman *et al.*, 2018). Note that for the security analysis of QKD systems with realistic devices, the finite data size effects are much more complicated. We review them in Sec. V.A.

III. QKD IMPLEMENTATION

In practice, security of a QKD system is often related to its implementation. A QKD implementation is composed of three parts: source, channel, and detection. In a rigorous security proof, the channel is assumed to be under the full control of Eve, who can replace the channel with any quantum operation she desires. In the security proof model, no implementation assumption is required for the channel. As a result, the security of the system does not depend on the physical realization of the quantum channel. Therefore, the practical security for the channel is not an issue. For the quantum source and detection, on the other hand, a security proof normally requires some assumptions on practical realization.

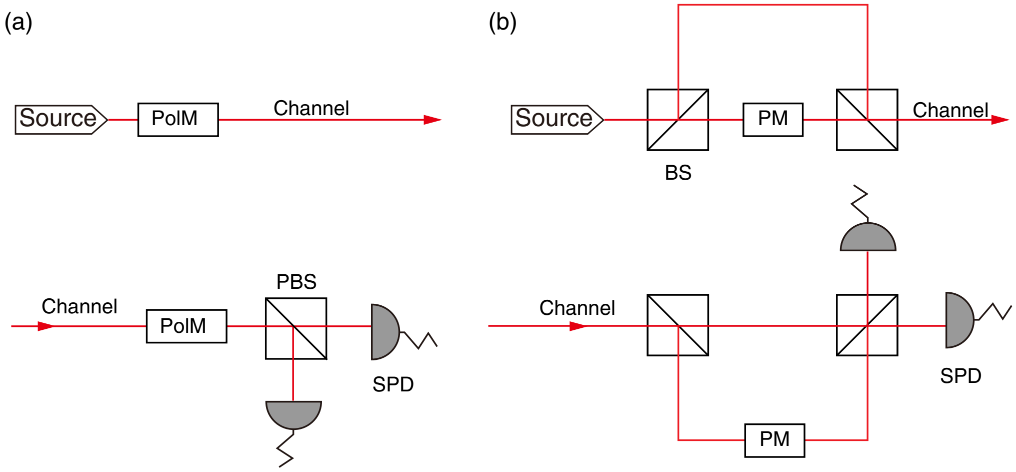

FIG. 5. Illustration of an optical device with (a) polarization encoding and (b) relative phase encoding. The top panels show the encoding, while the bottom panels show the decoding. PolM, polarization modulator; PM, phase modulator; PBS, polarization beam splitter; SPD, single-photon detector; BS, beam splitter.

Photons are most widely used for communication due to their robustness against decoherence due to the noisy environment and fast traveling speed. Hence, we focus mainly on the quantum optical realization of QKD systems. We first discuss the encoding and decoding methods, then briefly introduce the practical source, channel, and detection devices, and finally the classical postprocessing. Here we primarily review the practical components of a discrete-variable (DV-) QKD system, while the discussions for CV-QKD can be found in Sec. VII.

A. Encoding and decoding

Different encoding and decoding methods are reflected for source, channel, and detection. For discrete-variable QKD schemes, Alice needs to figure out an efficient method to encode her qubit or qudit in the quantum states. Accordingly, Bob needs to develop an efficient method to read out the quantum information encoded by Alice.

In general, for qubit-based QKD, quantum information can be encoded in two quantum modes s and r and their relative phases. Normally, the two modes are assumed to be orthogonal, say, using orthogonal polarizations or distinct time bins. Then for a photon, the states $\{|10\rangle_{sr}, |01\rangle_{sr}\}$ form a Hilbert space named the Z basis. Here, 0 and 1 refer to the photon number in a mode. Two complementary bases X and Y are defined with the relative phases. The X and Y basis states can be written as $\{|10\rangle_{sr} \pm |01\rangle_{sr}\}$ and $\{|10\rangle_{sr} \pm i|01\rangle_{sr}\}$.

In reality, a widely applied method is polarization encoding, which utilizes the polarization modes. The horizontal and vertical polarizations of a photon, denoted by $|10\rangle_{HV}$ and $|01\rangle_{HV}$, are used for the Z-basis encoding. Then the X-basis states $\{|10\rangle_{HV} \pm |01\rangle_{HV}\}$ denote the linear polarization modes along the directions of $\pm 45°$, respectively. The Y-basis states $\{|10\rangle_{HV} \pm i|01\rangle_{HV}\}$ denote the left- and right-handed circular polarizations. In the decoding process, the basis choice is realized by a polarization controller (Fig. 5), and the polarization measurement is realized with a polarization beam splitter (PBS) connected with single-photon detectors.

Another common method is time-bin phase encoding, where Alice chooses two pulses, a signal pulse and a reference pulse, for two encoding modes, denoted by s and r, respectively. Similar to polarization encoding, for a single photon, the two time-bin modes form the Z basis, $\{|10\rangle_{sr}, |01\rangle_{sr}\}$. Here the qubit in the Z basis determines whether the photon stays in the signal time bin or the reference time bin. The X- and Y-basis states $\{|10\rangle_{sr} \pm |01\rangle_{sr}\}$ and $\{|10\rangle_{sr} \pm i|01\rangle_{sr}\}$ denote the photons with a relative phase $0, \pi$ and $\pi/2, 3\pi/2$ between the signal and reference pulses, respectively. In the decoding process, an interferometer (Fig. 5) is employed to extract the phase information.

For qudit-based QKD, Alice and Bob need to find d orthogonal modes, and the encoding and decoding are similar. For example, the orbital angular momentum is the freedom of photons in the spatial distribution, which contains a large Hilbert space. By encoding the high-dimensional key information into the orbital angular momentum, one can enhance the performance of QKD (Cerf *et al.*, 2002; Gröblacher *et al.*, 2006). Another example is encoding with multiple time bins. In DPS QKD, the relative phase or each time-bin pulse is only 0 or π, and the key is encoded in the relative phases of two neighboring pulses. Round-robin-DPS QKD (Sasaki, Yamamoto, and Koashi, 2014) encode and decode the phase difference circularly.

B. Photon sources

Here we mainly discuss various practical photon sources for QKD: weak coherent-state source, thermal source, heralded single-photon source, and entangled-photon source. For most prepare-and-measure QKD protocols, a single-photon source is preferred. However, it is experimentally challenging to realize a high-quality and high-performance single-photon source. We now discuss the photon sources according to different QKD schemes.

1. Prepare-and-measure scheme

In a standard prepare-and-measure scheme like BB84, the common way is to employ other practical weak light sources to approximate the single-photon source. In general, they are modulated to be a Fock state mixture

$$\rho = \sum_{n=0}^{\infty} P(n)|n\rangle\langle n|, \tag{27}$$

where $P(n)$ is the photon-number distribution and $|n\rangle$ is the n-photon-number state. For different types of sources, the photon-number distribution is also different. Normally, the single-photon component $|1\rangle\langle 1|$ is required to be dominant compared to higher-order components.

The weak coherent-state source is the most widely employed in QKD, which can be easily realized by attenuating laser lights. The light generated by a laser can be regarded as a coherent pulse $|\alpha\rangle$ within the coherence time, where α is a complex number and $\mu = |\alpha|^2$ is the average photon number. The coherent state can be expanded in the Fock basis as

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle. \tag{28}$$

The phase of α reflects the relative phase between different photon-number components. To realize a photon source in the form of Eq. (27), Alice can randomize the phase of coherent pulses and make it a mixture of photon-number states (Lo, Ma, and Chen, 2005),

$$\rho_\mu = \frac{1}{2\pi} \int_0^{2\pi} d\phi |\alpha e^{i\phi}\rangle\langle \alpha e^{i\phi}| = \sum_{n=0}^{\infty} P_\mu(n)|n\rangle\langle n|, \tag{29}$$

where the photon number follows a Poisson distribution $P_\mu(n) = e^{-\mu}\mu^n/n!$. In many QKD protocols, such as BB84, only the single-photon component is secure for key distribution. Thus, the light intensity μ is typically on the single-photon level, $\mu = O(1)$.

The thermal source is a Fock state mixture, expanded by

$$\begin{aligned} \rho_{\mathrm{th}} &= \sum_{n=0}^{\infty} P_{th}(n)|n\rangle\langle n| \\ &= \sum_{n=0}^{\infty} \frac{\mu^n}{(\mu+1)^{n+1}} |n\rangle\langle n|, \end{aligned} \tag{30}$$

where μ is the average photon number and the photon number follows a thermal distribution $P_{\mathrm{th}}(n)$. Note that for a small average photon number $\mu \leq 2$, the single-photon component ratio is bigger in a Poisson distribution than in a thermal distribution. This is the reason why the weak coherent-state source normally can outperform the thermal one in QKD (Curty *et al.*, 2010).

2. Entanglement-based protocol

For entanglement-based QKD protocols such as BBM92 (Bennett, Brassard, and Mermin, 1992), an entangled-photon source via parametric down-conversion (PDC) process is normally adopted. In a PDC process, a high frequency photon is converted to a pair of low frequency photons. A PDC source emits a superposition state of different numbers of photon pairs (Ma and Lo, 2008; Walls and Milburn, 2008),

$$|\Psi\rangle = (\cosh\chi)^{-1} \sum_{n=0}^{\infty} (\tanh\chi)^n |n,n\rangle, \tag{31}$$

where χ is the nonlinear parameter for the down-conversion process, $\mu = \sinh^2\chi$ is the average photon pair number, and $|n,n\rangle$ represents n photon pairs in two optical modes.

The PDC process is widely used to generate photon pairs. In this case, four optical modes are used. For example, a typical PDC photon source emits photon pairs in two directions. In each direction, the photon can be in H or V polarization. The two optical modes are entangled in polarization. Compared to Eq. (31), due to different collection means, the amplitudes of photon pair numbers are slightly different from the one in Eq. (31) (Kok and Braunstein, 2000; Ma, Fung, and Lo, 2007),

$$|\Psi\rangle = (\cosh\chi)^{-2} \sum_{n=0}^{\infty} \sqrt{n+1} \tanh^n\chi |\Phi_n\rangle, \tag{32}$$

where χ is the nonlinear parameter for the down-conversion process, $\mu = 2\sinh^2\chi$ is the average number of entangled-photon pairs, and $|\Phi_n\rangle$ is the state of an n-entangled-photon pair,

$$|\Phi_n\rangle = \frac{1}{\sqrt{n+1}} \sum_{m=0}^{n} (-1)^m |n-m, m\rangle_a |m, n-m\rangle_b. \tag{33}$$

In the aforementioned example, a and b represent two directions of the light, and $|n-m, m\rangle_a$ represents $n-m$ photons in the H polarization and m photons in the V polarization. The number of entangled-photon pairs follows a super-Poissonian distribution, slightly different from the thermal distribution,

$$P(n) = \frac{(n+1)(\mu/2)^n}{(1+\mu/2)^{n+2}}. \tag{34}$$

Notice that the PDC source can also be used as a heralded photon source in the prepare-and-measure scheme. If we focus only on one of the optical modes (normally called the signal mode), tracing out the other (normally called the idle mode) the photon number follows the thermal distribution $P_{th}(n)$ given in Eq. (30). A typical usage of a PDC source for a heralded photon involves measuring the idle optical mode locally as a trigger and encoding the signal mode for QKD. In this case, once Alice obtains a trigger locally, she can largely rule out the vacuum component in the signal mode. In fact, conditional on whether or not a detection clicks on the idle mode, the photon-number distribution differs in the signal mode. Such a source can be used as a passive decoy-state source (Adachi *et al.*, 2007; Ma and Lo, 2008; Sun *et al.*, 2014). Note that when μ is extremely small, such a heralded photon source can well approximate a single-photon source, which is widely used in multiphoton processing (Pan *et al.*, 2000).

C. Channel

Theoretically, we put no assumption on the quantum channel used for QKD. However, in the real-world implementation, we build the QKD channel with mature optical communication technology to enhance the performance of the QKD protocol. There are two widely adopted channels for QKD: fiber and free space. The most common channel used in QKD is built with commercial optical fiber. For a standard commercial single-mode fiber, losses depend exponentially on the channel distance l as $10^{-\alpha l/10}$, where the loss rate α is roughly 0.2 dB/km for a telecommunication wavelength of around 1550 nm. The loss rate can be remarkable if we extend the transmission distance to more than 300 km of standard commercial fiber (Yin *et al.*, 2016; J.-P. Chen *et al.*, 2020; Fang *et al.*, 2019). Besides loss, a fiber-based QKD implementation should solve several other problems, such as chromatic dispersion, polarization mode dispersion, birefringence, etc. (Gisin *et al.*, 2002).

The free-space channel features some advantages over optical fiber. There are several atmospheric transmission windows, including 780–850 and 1520–1600 nm, which have a low loss and an attenuation less than 0.1 dB/km in clear weather (Bloom *et al.*, 2003). The attenuation is negligible even in the outer space above Earth's atmosphere, which enables long-distance QKD of over 1000 km between ground and satellite (Liao *et al.*, 2017a). Furthermore, the decoherence of polarization or of any other degree of freedom is practically negligible. However, there are also some drawbacks with free space. For instance, weather conditions influence the loss of free space heavily. The effective apertures of the sending and receiving telescopes, influenced by alignment, movements, and atmospheric turbulence, contribute coupling losses and affect the performance of free-space QKD.

D. Detection

For DV-QKD schemes, single-photon detection is realized with threshold detectors that can distinguish the vacuum (zero photon) from single-photon or multiphoton cases only. Besides, some imperfections may exist in the single-photon detector (SPD): the detector efficiency η is not 100%, which means that some nonvacuum signals will not cause a click on the SPD; there exists a dark count factor p_d, which means that some vacuum signals will incorrectly cause a click. This will affect the performance of QKD systems.

The measurement model is based on the threshold SPDs mentioned previously. For the single-photon subspace, the detection here can be regarded as an X/Y–basis qubit measurement. However, there is a multiphoton component in the final signal, and the behavior of the measurement device differs from the required Z-basis and X-basis measurements in DV-QKD. For example, there are double-click signals caused by the multiphoton component, which does not happen in the ideal X/Y–basis detection. To address this issue, the squashing model of the measurement is proposed, combined with the random assignment of double-click signals (Beaudry, Moroder, and Lütkenhaus, 2008; Fung, Chau, and Lo, 2011).

In 2012, the MDI-QKD scheme (Lo, Curty, and Qi, 2012) was proposed to fill the detection loophole. The design of measurement devices in MDI-QKD is similar to the one in point-to-point QKD protocol. In the discrete-variable MDI-QKD scheme, the measurement device, assumed to be manipulated by the adversary, can be divided into two categories, single detection and coincidence detection. The coincident detection MDI-QKD schemes (Ma and Razavi, 2012) are based on the schemes in which the two communication parties Alice and Bob encode their key information into a single photon and build correlation between their key value using a Bell state projection. The single detection MDI-QKD scheme (Lucamarini *et al.*, 2018; Ma, Zeng, and Zhou, 2018) can be regarded as the detection of the coherent states rather than the single photon. They both build correlations between Alice's and Bob's bit values by Bell state projections.

E. Postprocessing

Postprocessing is a procedure for Alice and Bob to distill a secure key from the raw data measured in quantum transmission with the help of public discussions. The flow chart of QKD postprocessing is shown in Fig. 6.

There are a few practical aspects to take into consideration when the number of signals are finite, i.e., the finite-key effect. For example, the error correction efficiency may not reach the Shannon limit; depending on the data size, a factor may be applied. On the privacy amplification side, there is a small failure probability. Some public communication between Alice and Bob need to be authenticated and/or encrypted. Table XIII summarizes the resource cost and the failure probabilities for the various steps.

The first step is the raw key assignment, which depends on different schemes. For example, in the commercial BB84 implementation, Alice and Bob discard all no clicks and randomly assign double clicks. In the MDI-QKD scheme, this

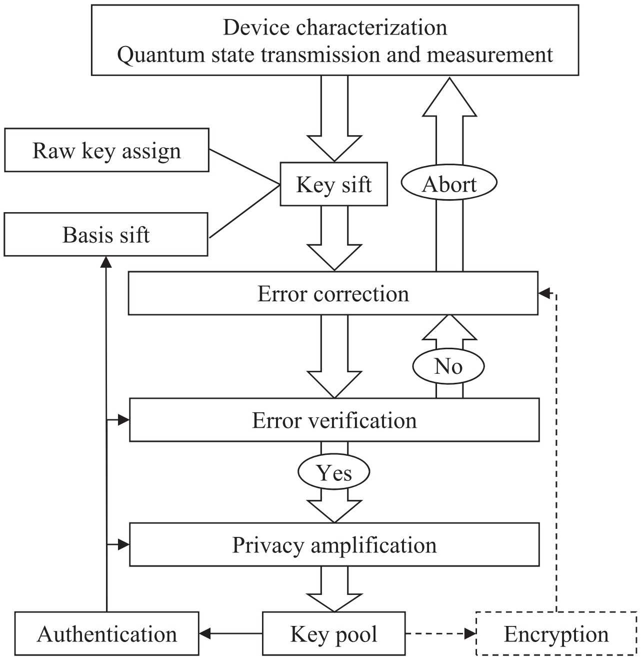

FIG. 6. Flow chart of data postprocessing procedures. The resource cost and the failure probabilities in encryption and authentication is listed in Table XIII. The encryption is optional for error correction depending on whether more privacy application is performed later. Adapted from Fung, Ma, and Chau, 2010.

TABLE XIII. List of resource cost and failure probabilities in the various steps. The numbers of consumed secret key bits are denoted as k, while the failure probabilities are denoted as ε. Alice sends out N signals, and Bob detects n of them in the Z-basis measurement. The final key output length is l. The tag length refers to authentication tag and the ellipses indicate that no authentication is required. In error verification, no message aside from an encrypted authentication tag is transmitted. The cost of error correction k_{ec} is given by $nfH(E)$. No communication is required in phase error estimation. Adapted from Fung, Ma, and Chau, 2010.

Procedure	Message	Tag	Failure probability
1. Raw key assignment	N	$\cdots$	$\cdots$
2. Basis sift	n	k_{bs}	ε_{bs} [Eq. (35)]
3. Bit error correction	k_{ec}	$\cdots$	$\cdots$
4. Error verification	$\cdots$	k_{ev}	ε_{ev} [Eq. (35)]
5. Phase error estimation	$\cdots$	$\cdots$	ε_{ph} [Eq. (26)]
6. Privacy amplification	$(n+l-1)$	k_{pa}	ε_{pa} [Eq. (37)]

step is based on the announcement of the measurement site. In device-independent (DI) QKD, Alice and Bob can perform arbitrary assignments. Of course, any improper assignment will reduce the key rate.

During the public discussions, some of the classical communication needs to be authenticated, as indicated in Table XIII. In the security proofs that we reviewed, we assume the encryption of classical communication in error correction. Such encryption can be avoided in other security proofs. In this case, there may be some restriction on the error correction procedure, and more follow-up privacy amplification is required. For example, in the original Shor-Preskill security proof, such encryption is not necessary when the CSS code is employed. In practice, there is an advantage to using error correction without encryption, since if Alice and Bob abort the QKD procedure after error correction, no preshared secret bits are lost due to encryption. In the following discussion, we assume that the number of bits communicated in error correction is counted for later privacy amplification. Thus, in privacy amplification the extraction ratio will be the r given in Eq. (24) without considering the finite data size effects. If the one-time pad encryption is used for error correction, the privacy amplification ratio will be higher by removing the error correction term in Eq. (24). After that, a certain amount of secure key bits needs to return to the keep pool for encryption consumption. In the end, the final key rate is still the same in the encryption and nonencryption cases.

1. Error correction

For practical error correction, an efficiency factor $f > 1$ is put normally before the $H(E)$ term Eq. (24), which means that the actual cost is larger than the theoretical Shannon limit. Previously, a widely used error correction protocol for QKD was Cascade (Brassard and Salvail, 1994). The Cascade protocol is simple and highly efficient, able to achieve an error correction factor of around 1.1–1.2 for a large QBER range extending from 0% to beyond 11%. In the Cascade protocol, Alice and Bob divide their sift key bit strings into blocks and compare parities of each block to look for errors. They perform a binary search to locate the error when the parity of a block is different. The process repeats a few times with different block sizes and permutations to ensure that all error bits are corrected. The Cascade protocol is highly interactive because the binary search requires $1+\log_2(n)$ communications, and successful error correction often requires several passes. Later, several improved protocols were proposed to reduce the interaction rounds (Buttler *et al.*, 2003; Nakassis, Bienfang, and Williams, 2004; Elliott *et al.*, 2005).

Another family of error correcting codes is forward error correction, which needs to send only one syndrome from Alice to Bob. Because of its light classical communication load, the forward error correction is widely implemented in commercial QKD systems. One outstanding example is the low-density parity-check (LDPC) code (MacKay and Neal, 1996). The LDPC code works well for QKD due to its high error correction efficiency and limited communication requirements. The design and optimization of LDPC codes in QKD postprocessing is similar to the classical case, which can be divided into three steps.

(1) The first step is to find a good degree distribution (MacKay, Wilson, and Davey, 1999; Richardson and Urbanke, 2001) for the target error rate.

(2) The second step is to generate a good parity-check matrix. As in classical communication, small cycles may contribute to localized information transmitted in decoding. Thus, a good parity-check matrix generation algorithm should yield a relatively large girth. Progressive edge growth is one of the most successful algorithms to generate parity-check matrix eliminating small cycles (Hu, Eleftheriou, and Arnold, 2005).

(3) The third step is to decode using Bob's key string and the received syndrome. The brief-propagation algorithm (Fossorier, Mihaljevic, and Imai, 1999), also known as the sum-product algorithm, is highly efficient in decoding.

The standard LDPC algorithm is optimum at its designed rate only for the designed QBER. But the actual QBER is fluctuating from round to round. The rate compatible LDPC can solve this problem with puncturing and shorting (Ha *et al.*, 2006). The main technology here is to select a mother code close to the target rate, then to adjust the code rate with puncturing. The puncturing operation can be done multiple times to find the best code rate for the actual error rate. This method has been employed in QKD (Elkouss *et al.*, 2009; Martinez-Mateo, Elkouss, and Martin, 2010). Besides efficiency, another important factor of error correction is the throughput. The limitation of the Cascade code is highly interactive communication, and that of LDPC is the computational cost in iterative decoding. It was reported that the throughput with both the Cascade (Pedersen and Toyran, 2013) and LDPC (Dixon and Sato, 2015) codes can be higher than 10 Mbits/s. Note that the computing in decoding LDPC is always assisted with graphics processing unit acceleration.

2. Error verification and authentication

Before error correction, Alice and Bob sample the sifted key bits to roughly estimate the error rates. Then they perform error correction. After error correction, Alice and Bob can perform error verification to make sure that they share the same key (Lütkenhaus, 1999; Ma *et al.*, 2011). Then, the failure probability for the error correction is reflected in an error verification step in which finite data size is considered. It is not hard to see that error verification and message authentication are similar. In both cases, Alice and Bob want to make sure the bit strings on the two ends are the same. The only difference is that the authentication tag might reveal information about the message, but error verification should not. This difference can be overcome by encrypting the tag, which has already been done in most information-theoretically secure authentication schemes. If we employ the linear-feedback-shift-register-based Toeplitz matrix construction, the relation between the tag length (the same as the key cost) and the failure probability is given by

$$\varepsilon = n2^{-k+1}, \tag{35}$$

where n is the message length and k is the key cost.

After error correction and error verification, Alice and Bob are almost sure that they have located all of the errors. Then they can accurately count the number of bit errors and hence the rate e_b defined in Eq. (10). If Alice and Bob choose not to encrypt error correction, they can count the amount of classical communication used in the error correction k_{ec}. Then they perform an additional amount of privacy amplification. For example, in the ideal device case of Eq. (11) and the infinite data limit, $k_{ec} = nH(e_b)$. The final key output length is given by $l = rn$.

3. Privacy amplification

Practical privacy amplification turns out to be extremely efficient in terms of finite data size effect once the necessary parameters, such as the phase error rates, are estimated as reviewed in Sec. II.D.2. Denote the error corrected bit strings for Alice and Bob as $k_A = k_B$ with a length of n, and denote the output length as l. In the infinite key limit, use $l/n = r$ as given in Eq. (24) if the error correction is not encrypted. In the privacy amplification procedure, Alice randomly chooses a universal hashing matrix $T \in \{0,1\}^{l\times n}$ and sends it to Bob via a public classical channel. The final key is given by $Tk_A = Tk_B$, with a small failure probability.

Privacy amplification works for general classes of two-universal hash functions (Tomamichel *et al.*, 2011). In particular, the universal hashing function based on Toeplitz matrices is widely used for privacy amplification. An $l \times n$ Toeplitz matrix is a Boolean matrix with a structure

$$T = \begin{pmatrix} a_0 & a_{-1} & a_{-2} & \cdots & a_{-n+1} \\ a_1 & a_0 & a_{-1} & \ddots & \\ a_2 & a_1 & \ddots & & \vdots \\ \vdots & \ddots & & & \\ a_{l-1} & & \cdots & & a_{l-n} \end{pmatrix}, \tag{36}$$

where $a_i \in \{0,1\}$ for $-n+1 \le i \le l-1$. The Toeplitz matrix can also be concisely written as $T_{(i,j)} = a_{i-j}$, where $T_{(i,j)}$ is the (i,j) element of T. Apparently, an $l \times n$ Toeplitz matrix can be specified by $N + K - 1$ bits, as opposed to $N \times K$ bits for completely random matrices. The main advantage of Toeplitz matrix hashing is that the computational complexity for Tk_A is $O(n \log n)$ when using the fast Fourier transform.

Following the security proofs reviewed in Sec. II.B, the matrix T should be related to the phase error correction. To ensure that the phase error correction commutes with the final key measurement, we require the null space of H to be capable of correcting the underlying phase errors. For universal hashing functions, such an error correcting capability can be evaluated with certain failure probabilities. Details of the derivation can be found in Sec. X of Fung, Ma, and Chau (2010). The failure probability for privacy amplification with Toeplitz hashing is given by

$$\begin{aligned} \varepsilon_{pa} &= 2^{-t_{pa}}, \\ t_{pa} &= nr - l. \end{aligned} \tag{37}$$

If Alice transmits the Toeplitz matrix to Bob, then she needs to authenticate that communication as well, which would add an extra term of Eq. (35) to ε_{pa}. In privacy amplification, by sacrificing t_{pa} extra bits in privacy amplification one can obtain a failure probability of $2^{-t_{pa}}$. More general discussions for hash functions besides Toeplitz hashing can be seen in Tomamichel *et al.* (2011).

Note that message authentication can be done more efficiently by piling up classical communication data and authenticating them at once. That is, the authentication terms listed in Table XIII can be done once with one authenticated tag and one failure probability. The main drawback of this saving data and authenticating approach is that it might require a lot of local data storage. In QKD system design, it is normally preferred that each procedure of postprocessing is isolated.

From the simulation results (Fung, Ma, and Chau, 2010), we learn that the failure probabilities for authentication, error verification, and privacy amplification are not the main contributions to the total system one. In fact, the one in phase error rate estimation, Eq. (26), is the dominate term. The summation of failure probabilities evaluated here can be converted to the trace-distance measure in Eq. (5).

4. Finite-key length

When the failure probability of the postprocessing procedure is ϵ, the final key is $\sqrt{\epsilon(2-\epsilon)}$ secure, in accordance with the composable security definition given in Eq. (5). Finally, by including the finite data statistics for parameter estimation (see Sec. II.D.2) and the postprocessing costs (see Table XIII), we have the finite-key length NR for the finite-size security of QKD, which can be written as (Fung, Ma, and Chau, 2010)

$$NR \ge l - k_{bs} - k_{ec} - k_{ev} - k_{pa}, \tag{38}$$

with a failure probability of

$$\varepsilon \le \varepsilon_{bs} + \varepsilon_{ev} + \varepsilon_{ph} + \varepsilon_{pa}, \tag{39}$$

where l is given by

$$l = n_x[1 - H(e_{bz} + \theta_z)] + n_z[1 - H(e_{bx} + \theta_x)], \quad (40)$$

and the variables can be found in Table XII.

Notice that one can also utilize the smooth min-entropy approach to obtain the finite-key length (Renner, 2008; Scarani and Renner, 2008) or the tight bounds (Tomamichel *et al.*, 2012). For QKD systems with realistic devices, the finite-key length is slightly complicated; we refer the interested reader to Lim *et al.* (2014) for decoy-state QKD, Curty *et al.* (2014) for measurement-device-independent QKD, Lorenzo *et al.* (2019) for twin-field QKD, Arnon-Friedman *et al.* (2018) for device-independent QKD, and Furrer *et al.* (2012) and Leverrier *et al.* (2013) for continuous-variable QKD.

IV. QUANTUM HACKING

In theory, it is traditional to divide Eve's hacking strategy into three main classes: *individual*, *collective*, and *coherent* (or general) attacks. In an individual attack, Eve interacts with each secure qubit in the channel separately and independently; in a collective attack, Eve prepares independent ancilla and interacts with each qubit independently but can perform a joint measurement on all ancilla; and in a coherent attack, Eve can prepare an arbitrary joint entangled state of the ancilla, which then interact with the qubits in the channel before being measured jointly. The last one does not limit Eve's capabilities beyond what is physically possible. Any QKD system aiming to implement an informational-theoretically secure protocol, therefore, has to be proven secure against coherent attacks. Another aspect that cannot be neglected is security in a finite-size scenario. No key transmission session is endless, and the resulting statistical fluctuations have to be taken into account (Scarani *et al.*, 2009).

In this section, putting theory attacks aside we focus on the practical attacks that exploit the device imperfections in QKD systems. Specifically, Eve may try to exploit the imperfections in real QKD systems and launch the so-called quantum hacking not covered by the original security proofs. Researchers have demonstrated several quantum hacking attacks in practical QKD systems. An earlier review on quantum hacking attacks can be seen in Jain *et al.* (2016). Here we provide a review of the quantum attacks for both the source and the detection. The detection attacks are similar to those reviewed in Jain *et al.* (2016), but we provide more details on the attacks at source that exploit the multiple photons, timing, or phase information of the laser source. Some new attacks that followed Jain *et al.* (2016) are also mentioned. Table I summarizes a list of the attacks developed from early 2000 to the present.

A. Attacks at the source

In the standard QKD scheme, it is assumed that Alice (state preparation) is placed in a protected laboratory and that she prepares the required quantum state correctly. Unfortunately, imperfect state preparation may leak information about the secret key. Indeed, practical preparation may introduce some errors due to imperfect devices or Eve's disturbance (Brassard *et al.*, 2000; Lütkenhaus, 2000; Fung *et al.*, 2007; Xu, Qi, and Lo, 2010; Sun *et al.*, 2012, 2015; Tang *et al.*, 2013). To steal information about the states, Eve can also actively perform the Trojan-horse attack (Gisin *et al.*, 2006; Jain *et al.*, 2014, 2015) on intensity modulators and phase modulators. This section reviews some examples of attacks at the source.

1. Photon-number-splitting attack

The first well-known hacking strategy that was considered was the PNS attack (Brassard *et al.*, 2000; Lütkenhaus, 2000) aiming at an imperfect photon source. As described in Sec. III.B, because of technological challenges WCPs generated by highly attenuated lasers are widely used in QKD implementations. Since the photon number of a phase-randomized WCP follows the Poisson distribution [Eq. (29)], there is a nonzero probability for multiple-photon pulses, i.e., those pulses containing two or more photons. Consequently, Eve may exploit the multiple-photon pulses and launch the PNS attack. In this attack, for each WCP Eve first utilizes a quantum nondemolition (QND) measurement to obtain the photon-number information. Conditional on the QND measurement result, Eve either blocks the one-photon pulse or splits the multiple-photon pulse in two. She stores one part of the multiple-photon pulse and sends the other part to Bob. Later during the basis-reconciliation process of the BB84 protocol Eve can get the secret key information for the multiple-photon pulse without introducing any errors. By doing so, Alice and Bob cannot notice Eve's attack.

The PNS attack restricts the secure transmission distance of QKD typically below 30 km (Gottesman *et al.*, 2004). Actually, in the early 2000s there were not many research groups working on QKD experiments (Hughes, Morgan, and Peterson, 2000; Ribordy *et al.*, 2000; Gobby, Yuan, and Shields, 2004). Researchers in the field had doubts about the future of QKD, and they generally thought that QKD may be impractical with WCP sources. This concern severely limited the development of QKD at that time. Fortunately, the discovery of the decoy-state method perfectly resolved the problem of PNS attacks and made QKD practical with standard WCP sources (Hwang, 2003; Lo, Ma, and Chen, 2005; Wang, 2005). More details on the decoy-state method are discussed in Sec. V.

2. Phase-remapping attack

Phase modulators are commonly used to encode random bits in the source of phase-coding QKD systems (Gisin *et al.*, 2002). In practice, a phase modulator has finite response time, as shown in Fig. 7(a). Ideally, the pulse will pass through the phase modulator in the middle of the modulation signal and undergo a proper modulation [time t_0 in Fig. 7(a)]. However, if Eve can change the arrival time of the pulse, then the pulse passes through the phase modulator at a different time [time t_1 in Fig. 7(a)], and the encoded phase is different. This phase-remapping process allows Eve to launch an intercept-and-resend attack, i.e., a phase-remapping attack (Fung *et al.*, 2007). The phase-remapping attack is a particular threat for bidirectional QKD schemes such as the plug-and-play QKD structure (Stucki *et al.*, 2002).

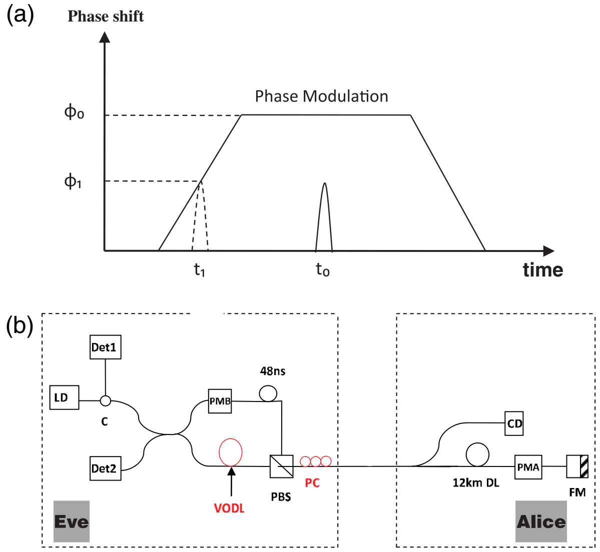

FIG. 7. Phase-remapping attack. (a) Diagram of a phase modulation signal. t_0 is the original time location where the signal pulse is properly modulated to have phase ϕ_0. Eve can time shift the signal pulse from t_0 to t_1, where the pulse will undergo a new modulated phase ϕ_1. (b) Implementation of a phase-remapping attack in a commercial IDQ QKD system. Original QKD system. LD, laser diode; Det1 and Det2, single-photon detector; PMB and PMA, phase modulator; C, circulator; PBS, polarization beam splitter; FM, Faraday mirror; CD, classical detector; DL, delay line. Eve's modifications. VODL, variable optical delay line; PC, polarization controller. From Xu, Qi, and Lo, 2010.

In 2010, the phase-remapping attack was successfully demonstrated in a commercial ID-500 plug-and-play QKD system (manufactured by ID Quantique[16]) (Xu, Qi, and Lo, 2010), as shown in Fig. 7(b). In that experiment, Eve utilized the same setup as Bob to launch her attack. Eve modified the length of the short arm of her Mach-Zehnder interferometer by adding a variable optical delay line (VODL) to shift the time delay between the reference pulse and the signal pulse. To remap the phase small enough into the low QBER range, Eve shifted the forward signal pulse out and only the backward signal pulse in the phase modulation range by using VODL, and she properly aligned the polarization direction of the backward signal pulse orthogonal to the principal axis of the phase modulator by using a polarization controller (PC). The experiment demonstrates that Eve can get full information and introduce a QBER of only 19.7%, which is much lower than the well-known 25% error rate for an intercept-and-resend attack in BB84.

3. Nonrandom-phase attack

Phase randomization is a basic assumption in most security proofs of QKD (Hwang, 2003; Gottesman *et al.*, 2004; Lo, Ma, and Chen, 2005; Wang, 2005). Although the security of QKD with a nonrandom phase had been proven (Lo and Preskill, 2007), the performance is limited in distance and key rate. By assuming that the overall phase is uniformly distributed in $[0, 2\pi]$, a coherent state with intensity can be reduced to a classical mixture of photon-number states, i.e., Eq. (29). This can greatly simplify the security proofs and allow one to apply classical statistics theory to analyze quantum mechanics. In practice, however, the phase-randomization assumption may be violated in practice, thus resulting in various attacks (Sun *et al.*, 2012, 2015; Tang *et al.*, 2013).

The first example is the unambiguous state discrimination (USD) attack demonstrated by Tang *et al.* (2013). When the phase of the WCPs is not properly randomized, the quantum state is a pure state. Then in decoy-state QKD (Hwang, 2003; Lo, Ma, and Chen, 2005; Wang, 2005), it is possible for Eve to distinguish the signal state and decoy state with an USD measurement. Hence, Eve first measures each of Alice's WCPs to distinguish between the signal state and decoy state by performing an USD measurement, which is combined with POVM operators without disturbing the quantum state sent by Alice. After the USD, Eve performs the PNS attack. Since Eve knows which state the pulse belongs to (signal or decoy), she could use different strategies for the signal state and decoy state. As a result, the key assumption in decoy-state QKD (Lo, Ma, and Chen, 2005), that a decoy state and a signal state have the same characteristics, is violated.

The second example is the laser seed-control attack that was proposed and demonstrated by Sun *et al.* (2015). A semiconductor laser diode (SLD) is normally used as a single-photon source in most commercial and research QKD systems. In the interdriven mode, the semiconductor medium of the SLD is excited from loss to gain by each driving current pulse. A laser pulse is generated from seed photons originating from spontaneous emission. The phase of the laser pulse is determined by the seed photons. Since the phase of the seed photons is random, the phase of each laser pulse is inherently random. However, if a certain number of photons are injected from an external source into the semiconductor medium, these photons will also be amplified to generate laser pulses. Consequently, the seed photons consist of two parts: one from spontaneous emission and the other from the external source. Both parts will affect the phase of the resulting laser pulse. If the injected photons greatly outnumber the photons from spontaneous emission, the phase of the output laser pulse is largely determined by the phase of the injected photons. Therefore, Eve can control the phase of Alice's signal laser by illuminating the SLD from an external control source and can successfully violate the phase-randomization assumption (Gottesman *et al.*, 2004).

B. Attacks at detection

The detection component is much more vulnerable to quantum hacking attacks than the source. Since Eve controls the channel and can send any signals (e.g., strong optical pulses combined with an x ray and neutrinos) to Bob, Bob has no choice but to receive Eve's signal, and any filters used by Bob may be imperfect, it may be hard for Bob to isolate his lab and avoid side channels or detector control from or by Eve. For instance, a significant number of attacks have been proposed to hack SPDs (Makarov, 2009; Lydersen *et al.*, 2010; Gerhardt *et al.*, 2011a, 2011b; Sauge *et al.*, 2011;

[16] See https://www.idquantique.com/.

Wiechers *et al.*, 2011).[17] SPDs were regarded as the “Achilles heel” of QKD by Bennett.[18] In this section, we review some examples of attacks at detection. The first two examples, the double-click attack and the fake-state attack, were proposed only in theory. The last two examples, the time-shift attack and the detector-blinding attack, were successfully demonstrated in experiment.

1. Double-click attack

Since QKD systems require the detection of two different bit values, bit 0 and bit 1, they require at least two SPDs. The double-click event refers to the case where both SPDs detect signals. The double-click event will introduce a QBER of 50% when either of the two bits is selected. A naive strategy is to determine double-click events as abnormal events and discards these events to minimize the QBER. However, this strategy results in the problem of a double-click attack. In this attack, Eve simply floods Bob’s polarization beam splitter with multiple photons or a strong pulse of the same polarization. Then, when Bob makes a measurement using a conjugate basis different from that of Eve, a double-click event occurs and is discarded; when the receiver makes a measurement using the same basis as Eve’s, a normal event is detected. Consequently, Alice and Bob finally share the same information with Eve. To solve this problem, Lütkenhaus (1999, 2000) proposed that double-click events are not discarded and that bit 0 or bit 1 is randomly allocated by Bob whenever a double-click event occurs.

2. Fake-state attack

In 2005, Makarov *et al.* proposed a faked-state attack, which exploits the efficiency mismatch of two detectors in a practical QKD system (Makarov and Hjelme, 2005; Makarov, Anisimov, and Skaar, 2006). In practice, standard SPDs such as Si/InGaAs avalanche photodiodes (APDs) are often operated in a gated mode. Therefore, the detection efficiency of each detector is time dependent. Since QKD systems require the detection of two different bit values, 0 and 1, they often employ at least two SPDs. It is inevitable that finite manufacturing precision in the detector and the electronics and the difference in the optical path length will slightly misalign the two detector gates and cause a detector-efficiency mismatch. This is illustrated in Fig. 8(a). At the expected arrival time T, the detection efficiencies of the two detectors are identical. However, if the signal is chosen to arrive at some unexpected times [such as t_1 and t_2 in Fig. 8(a)], it is possible that the detector efficiencies of the two detectors η_0 and η_1 will differ greatly. This problem often exists in practical QKD systems, and it leaves a back door for Eve to attack the system.

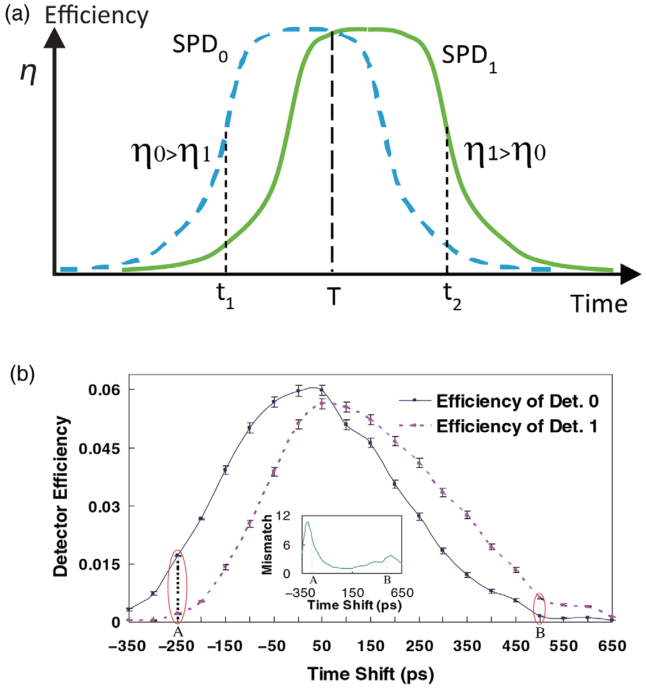

FIG. 8. Schematic of the detection-efficiency mismatch (Makarov, Anisimov, and Skaar, 2006) and time-shift attack (Qi, Fung *et al.*, 2007; Zhao *et al.*, 2008). (a) Single-photon detector (SPD). At the expected arrival time T, the detection efficiencies of SPD$_0$, η_0 for the event of bit 0, and SPD$_1$, η_1 for the event of bit 1 are the same. However, at time t_1 SPD$_0$ is more sensitive to the incoming photon than SPD$_1$, while at time t_2 SPD$_1$ is more sensitive to the incoming photon than SPD$_0$. (b) Real detector efficiencies of the two SPDs characterized on a commercial QKD system manufactured by IDQ. From Zhao *et al.*, 2008.

The fake-state attack is an intercept-and-resend attack. For each signal, Eve randomly chooses one of the two BB84 bases to perform a measurement and obtain a measurement result. Then, she resends the opposite bit value from her measurement result in the opposite basis at a time when the detector for the opposite bit has a lower detection efficiency than the other detector. As analyzed by Makarov, Anisimov, and Skaar (2006), Eve introduces less than 11% QBER if the detection efficiency $\eta \leq 6.6\%$. The fake-state attack, while conceptually interesting, is hard to implement in a real-life QKD system. This is because it is an intercept-and-resend attack and as such involves finite detection efficiency in Eve’s detectors and precise synchronization between Eve’s and Alice and Bob’s systems. A typical countermeasure against detector-efficiency mismatch is the four-state QKD protocol (Makarov, Anisimov, and Skaar, 2006).

3. Time-shift attack

Motivated by the fake-state attack, in 2007 Qi, Fung *et al.* (2007) proposed the time-shift attack. This is also based on the detection-efficiency mismatch for gated SPDs in the time domain but is much easier to implement. Let Fig. 8(a) illustrate the detection efficiencies of the two gated SPDs in a real-life QKD system. Eve can simply shift the arrival

[17] The vulnerabilities of SPDs are due mainly to their complex working mechanism: the detection is affected by incoming light and the control electronic circuits. Therefore, Eve can manipulate the intensity, the time, or the wavelength of the incoming light to control the responses of the SPDs.

[18] C. H. Bennett, “Let Eve do the heavy lifting, while John and Won-Young keep her honest,” http://dabacon.org/pontiff/?p=5340.

time of each pulse sent from Alice by employing a variable optical delay line. For example, Eve randomly shifts the pulse from Alice to arrive at t_1 or t_2 through a shorter path or a longer path of optical line. This shifting process can partially reveal the bit value of Bob: if the pulse arrives at t_1 (t_2) and Bob announces receipt, the bit value is more likely to be 0 (1). Moreover, Eve can carefully determine how many bits should be shifted forward and how many should be shifted backward to ensure that the distribution of bit 0 and bit 1 received by Bob is balanced. Hence, the time-shift attack does not make any measurements on the quantum state, and quantum information is not destroyed.

Since Eve does not need to make any measurements or state preparation, the time-shift attack is practically feasible with current technology. In 2008, it was successfully implemented on a commercial QKD system by Zhao *et al.* (2008), as shown in Fig. 8(b). This was one of the first successful demonstrations of quantum hacking on a widely used commercial QKD system. In their experiment (Zhao *et al.*, 2008), Eve got an information-theoretical advantage in around 4% of her attempts. The successful implementation of the quantum attack shows that a practical QKD system has non-negligible probability to be vulnerable to the time-shift attack.

4. Detector-control attack

The detector-control attack is the most powerful attack, and it has been successfully demonstrated on several types of practical QKD systems (Makarov, 2009; Lydersen *et al.*, 2010). In general, detector-control attacks can be divided into three categories: (i) detector-blinding attack (Makarov, 2009; Lydersen *et al.*, 2010; Lydersen, Akhlaghi *et al.*, 2011; A. Huang *et al.*, 2016), where Eve illuminates bright light to control detectors; (ii) detector-after-gate attack (Wiechers *et al.*, 2011), where Eve just sends multiphoton pulses at the position after the detector gate; and (iii) detector-superlinear attack (Lydersen, Jain *et al.*, 2011; Qian *et al.*, 2018), where Eve exploits the superlinear response of single-photon detectors during the rising edge of the gate.

Most available SPDs are InGaAs/InP APDs operating in a Geiger mode (Hadfield, 2009) in which they are sensitive to a single photon. The working principle of this type of APD is shown in Fig. 9(a). In the detector-blinding attack, by sending a strong light to Bob Eve can force Bob's SPDs to work in a linear mode instead of a Geiger mode, as shown in Fig. 9(a). In the linear mode, a SPD such as the one based on InGaAs APD is sensitive only to bright illumination. This detector operation mode is called *detector blinding*. After blinding the detectors, Eve sends a bright pulse with tailored optical power such that Bob's detector always reports a detection event from the bright pulse but never reports a detection event from a pulse with half power. This is illustrated in Fig. 9(b). Consequently, Eve can successfully launch an intercept-and-resend attack without increasing the QBER. For example, when Eve uses the same basis as Bob to measure the quantum state from Alice, Bob gets a detection event as if there were no eavesdropper. But if Eve uses the opposite basis of Bob's to measure the quantum state from Alice, her bright pulse will strike each of Bob's detectors with half power, and neither detector will report a detection event. In practice, a simple detector-blinding attack will introduces a 50% total loss. However, Eve can place her intercept unit close to Alice's laboratory while compensating for the loss in the remaining fiber by resending brighter states.

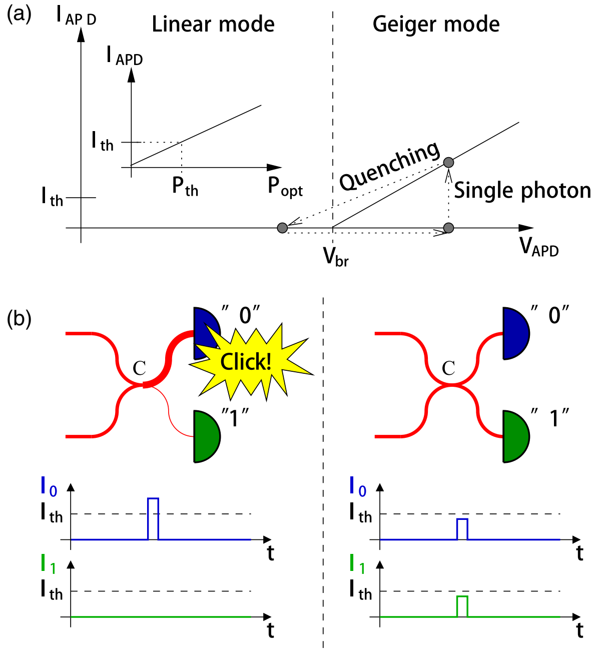

FIG. 9. Schematic illustration of the detector-blinding attack. (a) Linear-mode and Geiger-mode APD operation. When the APD is reverse biased above its breakdown voltage $V_{\rm br}$, a single photon can cause a large current $I_{\rm APD}$ to flow and register this as photon detection (a "click"). After that, an external circuit quenches the avalanche by lowering the bias voltage below $V_{\rm br}$, and the APD then goes into a linear mode. In the linear mode, $I_{\rm APD}$ is proportional to the incident bright optical power $P_{\rm opt}$. (b) Eve sends Bob a tailored light pulse that produces a click in one of his detectors only when Bob uses the same measurement basis as Eve. Otherwise, there are no detector clicks. From Lydersen *et al.*, 2010.

The detector-control attack is applicable to various types of SPDs, such as gated APDs (Lydersen *et al.*, 2010; A. Huang *et al.*, 2016), passively or actively quenched APDs (Makarov, 2009; Sauge *et al.*, 2011), superconducting nanowire single-photon detectors (SNSPDs) (Lydersen, Akhlaghi *et al.*, 2011), etc. A full field implementation of the attacking strategy was investigated by Gerhardt *et al.* (2011a). The blinding attack was also demonstrated to fake the violation of Bell's inequality (Gerhardt *et al.*, 2011b). How to remove the detector-control attacks is a challenge in the field of QKD. One proposed countermeasure is carefully operating the single-photon detectors inside Bob's system and monitoring the photocurrent for anomalously high values (Yuan, Dynes, and Shields, 2010, 2011). This work also highlights that the misoperation of QKD devices allows the loophole to be exploited, which is related to the best-practice criteria for all QKD devices in QKD implementations (Koehler-Sidki *et al.*, 2018). Recently, Qian *et al.* (2019) proposed another countermeasure against the detector-control attacks by introducing a variable attenuator in front of the detector. However, these countermeasures may seem to be *ad hoc*, may lead away from provable security models of QKD, and can often be defeated by advanced hacking technologies. A practical and promising solution is the MDI-QKD protocol, which is reviewed in Sec. VI.B.

C. Other attacks

Another well-known hacking strategy is the Trojan-horse attack (THA), in which Eve sends a probe light to Alice or Bob and reads his or her information from the backscattered probe light. In 2001, Vakhitov, Makarov, and Hjelme (2001) proposed the large pulse attack and Kurtsiefer *et al.* (2001) analyzed the possibility of THA by detecting the detector fluorescence of Si-based avalanche photodiodes. Gisin *et al.* (2006) studied the problem of THA in QKD implementations in which light goes two ways. Later, Jain *et al.* (2014, 2015) performed a comprehensive analysis of the risk of THA against typical components in standard QKD systems. Recently, backflash photons caused by detection events in single-photon detectors were exploited to realize the detector-backflash attack (Pinheiro *et al.*, 2018). A countermeasure against the THA is to add proper isolation and consider the leaking information in the privacy amplification, which is reviewed in Sec. V.C.

Besides the previously mentioned attacks, Lamas-Linares and Kurtsiefer (2007) demonstrated that the timing information revealed during public communicating can be exploited to attack the entanglement-based QKD system. In a two-way QKD system such as the “plug-and-play” structure, Sun, Jiang, and Liang (2011) studied the imperfections of Faraday mirrors and proposed the Faraday-mirror attack; Jain *et al.* (2011) experimentally demonstrated that the calibration routine of a commercial plug-and-play system can be tricked into setting a large detector-efficiency mismatch, and they proposed an attack strategy on such a compromised system with a QBER of less than 7%. Moreover, Li *et al.* (2011) studied the imperfection of a practical beam splitter and demonstrated a wavelength-dependent beam-splitter attack on top of a polarization-coding QKD system. The detector dead-time issue was widely studied by Rogers *et al.* (2007) and demonstrated by Henning *et al.* (2011). Bugge *et al.* (2014) and Makarov *et al.* (2016) demonstrated the laser damage attack by using a high-power laser to damage the SPDs. Recently, Huang *et al.* (2018) showed that the decoy states are distinguishable if they are generated by modulating the pump current of a semiconductor laser diode, and Wei, Zhang *et al.* (2019) exploited the efficiency mismatch in the polarization degree of freedom to hack SNSPD.

Most of the imperfections that have been reviewed so far are in fiber-based QKD systems. There are also quantum attacks reported for free-space QKD systems (Nauerth *et al.*, 2009; Sajeed, Chaiwongkhot *et al.*, 2015; Chaiwongkhot *et al.*, 2019). For instance, imperfect encoding methods result in side channels from which encoded states are partially distinguishable (Nauerth *et al.*, 2009). The imperfection due to non-single-mode quantum signals is a crucial issue in free-space QKD. Eve can exploit this imperfection and launch the spatial-mode attack against a free-space QKD system. This problem was carefully studied by Sajeed, Chaiwongkhot *et al.* (2015) and Chaiwongkhot *et al.* (2019) following an earlier discussion on the origins of the detection-efficiency mismatch by Fung *et al.* (2009). Besides DV-QKD, the practical security of CV-QKD also deserves future investigation, and it is reviewed in Sec. VII.C.

More generally, as noted by Curty and Lo (2019), in principle, there are simply too many side channels for Alice and Bob to close. This is because Eve might, in principle, attack Alice’s and Bob’s system via x rays, neutrons, neutrinos, or even gravitational waves. Whatever detection systems Alice and Bob have will probably have limited ranges of response. Moreover, classical postprocessing units pose a serious threat to the security of QKD. Most QKD security frameworks assume without proof that classical postprocessing units are secure. However, in conventional security it is well known that hardware Trojan-horse attacks and software Trojan-horse attacks are commonly used to compromise the security of conventional cryptographic systems. Curty and Lo (2019) proposed using redundancies in QKD units and classical postprocessing units to achieve security through verifiable secret sharing.

V. SOURCE SECURITY

In this section, we review various approaches for resolving the security issues of practical sources. On the one hand, imperfections in quantum-state preparation, including multiphoton components of laser, nonrandomized phases, encoding flaws, etc., need to be carefully quantified and taken into account in security analysis. In particular, we discuss the decoy-state QKD protocol in more detail. On the other hand, practical countermeasures are required to prevent Trojan-horse attacks on the source. Note that we focus on the BB84 protocol, but most techniques can be extended to other protocols.

A. Decoy-state method

The decoy-state method is a common way to combat source imperfection by introducing extra sources for better channel characterization. In the decoy-state method, the user randomly modifies the source states during the quantum stage; after that, he or she reveals which state is used in each turn. Eve cannot modify her attack to different source states, but in postprocessing the users can estimate their parameters conditioned on that knowledge. The decoy-state method is used mostly to bound the multiphoton components in a practical photon source.

In practical photon sources, multiphoton components are inevitable. As reviewed in Sec. IV.A.1, Eve can split a multiphoton pulse and save one photon from it for later hacking. Since Alice and Bob cannot tell whether a detection comes from a single-photon or multiphoton component and Eve controls the channel, they have to pessimistically assume that all multiphoton states cause clicks with 100% efficiency. All losses come from the single-photon states. To reduce the effects of the multiphoton components, Alice has to use low intensity optical pulses. In the case of a coherent-state photon source, it has been shown that the optimal intensity used is close to the channel transmittance η (Lütkenhaus, 2000; Ma, 2006),

$$\mu_{\text{opt}} \approx \eta, \tag{41}$$

where η includes the channel transmission and detection efficiency. The final key rate will then quadratically depend on the transmittance η, $R = O(\eta^2)$.

Various protocols have been proposed (Inoue, Waks, and Yamamoto, 2002; Hwang, 2003; Scarani *et al.*, 2004)over the key-rate limit caused by PNS attacks, the most effective of which is the decoy-state method (Hwang, 2003; Lo, Ma, and Chen, 2005; Wang, 2005). In the decoy-state QKD scheme, instead of using one intensity for encoding Alice employs a few additional intensities of optical pulses as decoy states to monitor the transmittance of different photon-number components. After Bob detects the signals, Alice announces the intensities she uses for each pulse. With detection rates for decoy states, Alice and Bob can bound tightly the number of detections from single-photon components. If Eve simply changes the transmittance for different photon-number states as adopted in the PNS attacks, she will inevitably change the detection rates for signal and decoy states differently. Without Alice's intensity information ahead, Eve has to let a significant amount of single-photon states pass to maintain the ratio of detection rates among signal and decoy states. The decoy-state idea was first proposed by Hwang (2003), who considered using a strong decoy signal with an intensity of around two photons as a decoy state.

The security proof of the decoy-state method was given later by Lo, Ma, and Chen (2005), where a photon-number channel model (Ma, 2008) is employed. With an infinite number of decoy states, Alice and Bob can estimate the detections from all photon-number components accurately. After adopting the GLLP security analysis reviewed in Sec. II.D.1, one can show that the optimal intensity of optical pulses can be increased to $O(1)$, which results in a key rate having a linear dependence of transmittance $O(\eta)$ (Lo, Ma, and Chen, 2005). The decoy-state method significantly increases the performance of practical QKD. The schematic diagram of the decoy-state method is shown in Fig. 10.

In the meantime, practical decoy-state methods with only a vacuum and weak decoy states were proposed (Lo, 2004; Ma, 2004), and tight bounds were derived later (Ma *et al.*, 2005; Wang, 2005). In the original security proof, continuous phase randomization is assumed to decohere phases between different photon-number components. As discussed in Sec. V.B.2, phase randomization is necessary but can be relaxed to discrete phase randomization (Cao *et al.*, 2015). In fact, the uniformly discrete phase randomization with discrete phase number $m = 10$ can already achieve a good approximation of continuous phase randomization.

1. Theory

For the source with different photon-number components, one can assume a photon-number channel model (Ma, 2008). The decoy-state method is a tomography to the photon-number channel model, providing tighter estimations on the single-photon component (Lo, Ma, and Chen, 2005). In the decoy-state method, the source is operated at different photon-number distributions, leading to different measurement outcome statistics. The communication partners can estimate the channel parameters of yield Y_n and QBER e_n for each photon-number component. One crucial assumption in the decoy-state QKD is that the signal state and decoy states are identical except for their average photon numbers. This means that after Eve's photon-number measurement, she has no way of telling whether the resulting photon-number state originated from the signal state or the decoy state. Hence, the yield Y_n and QBER e_n can depend on only the photon number n, not which distribution (decoy or signal) the state is from. That is,

$$\begin{aligned} Y_n(\text{signal}) &= Y_n(\text{decoy}), \\ e_n(\text{signal}) &= e_n(\text{decoy}). \end{aligned} \tag{42}$$

The implementations of the decoy-state method can be divided into active ones and passive ones. In the active decoy-state method, the user prepares the source signals with different intensities to change the probability distributions of each photon-number component. A simple solution for decoy-state preparation, as shown in Fig. 10, is to use an amplitude modulator (AM) to modulate the intensities of each WCP to the desired intensity level. This is indeed the implementation reported in most decoy-state QKD experiments. Another solution for decoy-state implementation is to use multiple laser diodes of different intensities to generate different states (Peng *et al.*, 2007). In the passive decoy-state method, heralded single-photon sources are often applied (Adachi *et al.*, 2007; Mauerer and Silberhorn, 2007; Ma and Lo, 2008). The probability distribution is changed by observing different measurement outcomes of the heralded photons.

A popular source for the decoy-state method is the phase-randomized weak coherent-state source, as shown in Eq. (29). To apply the active decoy method, Alice randomly adjusts the intensity μ of the coherent state, which is related to different Poisson distributions $P_\mu(n)$. Alice estimates the

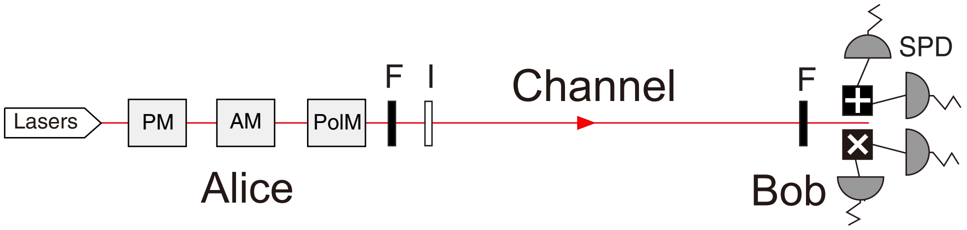

FIG. 10. Schematic diagram of decoy-state QKD. In a decoy-state BB84 transmitter, the optical pulses are normally generated with phase-randomized laser pulses. Decoy states are prepared using an amplitude modulator (AM). PM, phase modulator for phase randomization; PolM, polarization modulation for encoding; *F*, optical filter; *I*, optical isolator.

single-photon yield Y_1 and error e_1 by solving the equation provided by the observed gain Q_μ and QBER E_μ related to different intensities μ,

$$
\begin{aligned}
Q_\mu &= \sum_{n=0}^{\infty} P_\mu(n) Y_n, \\
E_\mu Q_\mu &= \sum_{n=0}^{\infty} P_\mu(n) e_n Y_n,
\end{aligned}
\tag{43}
$$

where $P_\mu(n) = \mu^n e^{-\mu}/n!$ for the coherent-state case.

Following the GLLP security analysis, Eq. (23), the key rate is given by

$$
R \geq -Q_\mu H(E_\mu) + Q_1[1 - H(e_1)], \tag{44}
$$

where $Q_1 = Y_1 \mu e^{-\mu}$. Here the gain Q_μ and QBER E_μ can be directly obtained from experiment, and the signal intensity μ is set by Alice. Making a tight estimation on Y_1 and e_1 by solving the linear equations in the form of Eq. (43), the key rate can be improved from $O(\eta^2)$ to $O(\eta)$.

In practice, only several different intensities are enough to make an accurate estimation. The most popular practical decoy-state method is the vacuum and weak decoy-state method (Lo, 2004; Ma, 2004). That is, Alice randomly generates coherent states with three different intensities $\{0, \nu, \mu\}$, where states with intensity μ are the signal states for key generation, and states with intensity $\nu < \mu$ and vacuum states with intensity 0 are for parameter estimation. The two parameters that we need to estimate in Eq. (44) can be bounded by (Ma *et al.*, 2005)

$$
\begin{aligned}
&Y_1 \geq Y_1^L = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right), \\
&e_1 \leq e_1^U = \frac{E_\nu Q_\nu e^\nu - e_0 Y_0}{Y_1^L \nu}.
\end{aligned}
\tag{45}
$$

A similar result was also derived by Wang (2005).

For the finite data size effect, Ma *et al.* (2005) took the first step to analyze the statistical fluctuations using standard error analysis, which essentially assumes i.i.d. channel behavior. The idea is that, instead of using Q_μ and E_μ obtained from the experiment directly, one assumes that these parameters fluctuate according to a normal distribution. Then in Eq. (45), one can substitute the upper and lower bounds of Q_μ and E_μ. The failure probability for this estimation would link to the number of standard deviations used for bounds.

The finite data size effect was discussed in a more rigorous manner by Lim *et al.* (2014) and Zhang *et al.* (2017). It turns out that the formulas used in the standard error analysis approach (Ma *et al.*, 2005) can be directly applied with a different value of failure probabilities in parameter estimation, as presented in Table XIV.

TABLE XIV. The failure probability as a function of the fluctuation deviations, measured by the number of standard deviations $(\chi - \mathbb{E}^L[\chi])/\mathbb{E}^L[\chi] = (\mathbb{E}^U[\chi] - \chi)/\mathbb{E}^L[\chi] = n\sigma$, where χ is counted in experiment. Here ε_G, ε_∞, $\varepsilon_{10\,000}$, and ε_{70}, respectively, denote failure probabilities for the bounds in the Gaussian approximate analysis, the rigorous method with a large data size limit, and a data size of 10 000 and 70. A similar table was presented in Zhang *et al.* (2017).

Deviation	ε_G	ε_∞	$\varepsilon_{10\,000}$	ε_{70}
2σ	$10^{-1.34}$	$10^{-0.57}$	$10^{-0.57}$	$10^{-0.57}$
3σ	$10^{-2.57}$	$10^{-1.65}$	$10^{-1.65}$	$10^{-1.54}$
4σ	$10^{-4.20}$	$10^{-3.17}$	$10^{-3.17}$	$10^{-2.65}$
5σ	$10^{-6.24}$	$10^{-5.13}$	$10^{-5.09}$	$10^{-3.92}$
6σ	$10^{-8.70}$	$10^{-7.52}$	$10^{-7.43}$	$10^{-5.36}$
7σ	$10^{-11.59}$	$10^{-10.34}$	$10^{-10.13}$	$10^{-6.95}$
8σ	$10^{-14.91}$	$10^{-13.60}$	$10^{-13.18}$	$10^{-8.67}$
9σ	$10^{-18.65}$	$10^{-17.29}$	$10^{-16.60}$	$10^{-10.50}$
10σ	$10^{-22.82}$	$10^{-21.41}$	$10^{-20.36}$	$10^{-12.38}$

In addition to weak coherent-state photon sources, one can use a PDC source or a thermal source, as reviewed in Sec. III.B. As long as the photon-number distribution of the source is different than the Poisson distribution, one can employ the passive decoy-state scheme (Adachi *et al.*, 2007; Ma and Lo, 2008), where Alice splits the pulses with a beam splitter, detects one arm as a trigger, and uses the other arm for QKD encoding. Depending upon the detection of the triggering signals, the photon-number distribution of the encoding arm is different. Alice can announce her local detection after Bob's detection. Then they can have linear gains for photon pulses with different conditional photon-number distributions for the decoy-state method analysis. It turns out that one can employ the passive decoy-state method even with phase-randomized coherent states (Curty *et al.*, 2010).

2. Experiment

Decoy-state methods have been widely implemented in different QKD systems. The decoy-state experiments are summarized in Table II. Figure 11 shows the four initial decoy-state QKD experiments. Zhao *et al.* (2006a, 2006b) reported decoy-state experiments on up to 60-km fiber on top of a commercial plug-and-play QKD system; Peng *et al.* (2007) implemented decoy-state QKD over 102-km fiber using a one-way polarization-encoding QKD system; Rosenberg *et al.* (2007) implemented decoy-state QKD over 107-km fiber using a one-way phase-encoding QKD system; and Schmitt-Manderbach *et al.* (2007) achieved 144-km decoy-state QKD in free space. These experiments demonstrated that decoy-state BB84 was secure and feasible under real-world conditions.

Since then, more experimental effort has been devoted to QKD deployments in labs and field tests. In 2007, Yuan, Sharpe, and Shields (2007) realized a stabilized one-way, phase-encoding, decoy-state QKD system. Later, Dixon *et al.* (2008) implemented decoy-state QKD with a high clock rate of 1 GHz, and Liu *et al.* (2010) extended decoy-state QKD to a long-distance 200-km fiber. A number of field QKD networks with the decoy-state implementation have been built in Europe (Peev *et al.*, 2009), Japan (Sasaki *et al.*, 2011), China (Chen *et al.*, 2009, 2010; Wang *et al.*, 2010), etc. An illustration of the Tokyo QKD network is shown in Fig. 12.

In the meantime, Wang *et al.* (2008) experimentally implemented a decoy state with a PDC source. The passive decoy-state method has also been demonstrated (Sun *et al.*, 2014). Recently, the decoy-state experiment was extended to a record-breaking distance of 1200 km in free space

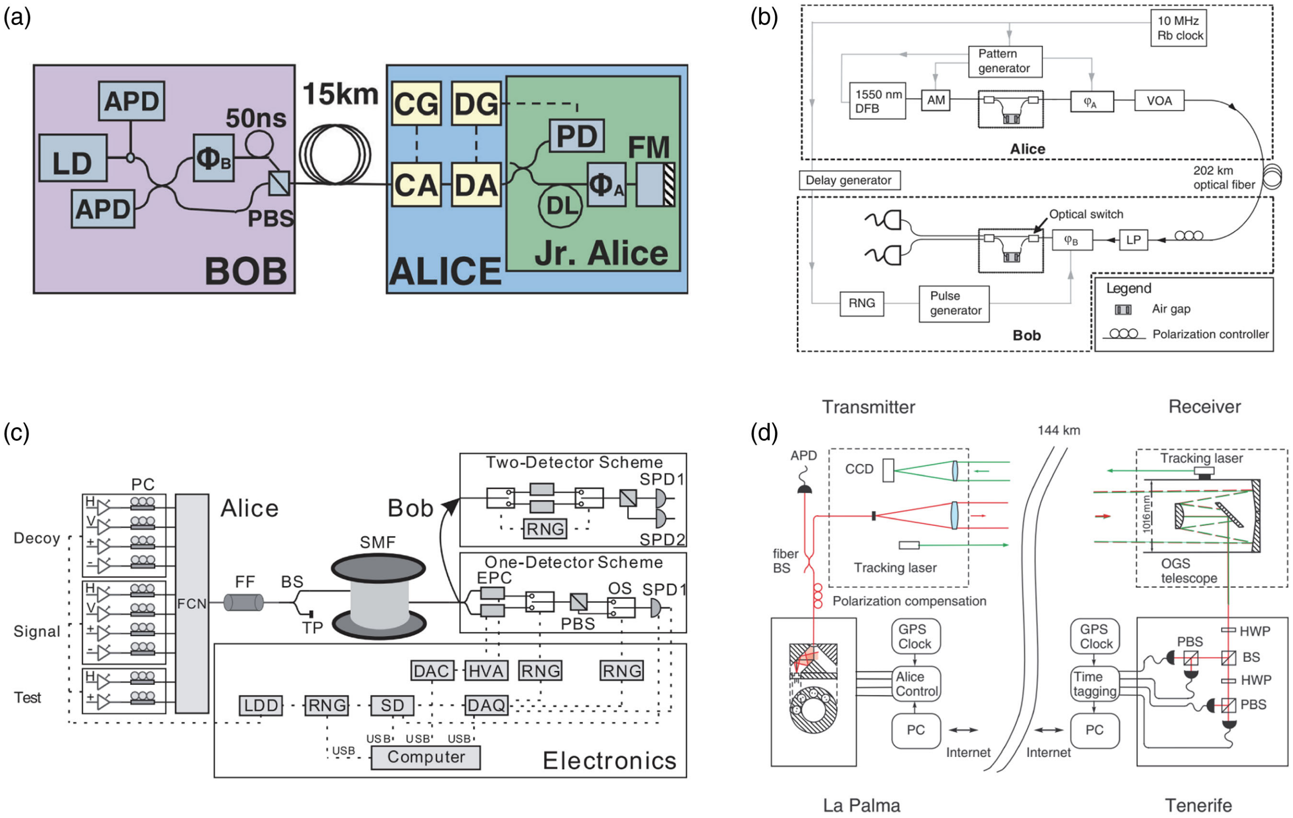

FIG. 11. Decoy-state QKD experiments. (a) Experiment on a commercial plug-and-play QKD system (Zhao *et al.*, 2006b). CA, compensating acousto-optic modulator (AOM); CG, compensating generator; DA, decoy AOM; DG, decoy generator; LD, laser diode; ϕ, phase modulator; PD, classical photodetector; DL, delay line; FM, Faraday mirror. (b) Phase-encoding experiment (Rosenberg *et al.*, 2007). DFB, distributed feedback laser; VOA, variable optical attenuator; AM, amplitude modulator; LP, linear polarizer. (c) Polarization-encoding experiment (Peng *et al.*, 2007). FCN, fiber coupling network; FF, fiber filter; EPC, electric polarization controller; DAC, digital-to-analog converter. (d) Free-space experiment (Schmitt-Manderbach *et al.*, 2007). BS, beam splitter; PBS, polarizing beam splitter; HWP, half-wave plate; APD, avalanche photodiode. From Zhao *et al.*, 2006b, Peng *et al.*, 2007, Rosenberg *et al.*, 2007, and Schmitt-Manderbach *et al.*, 2007.

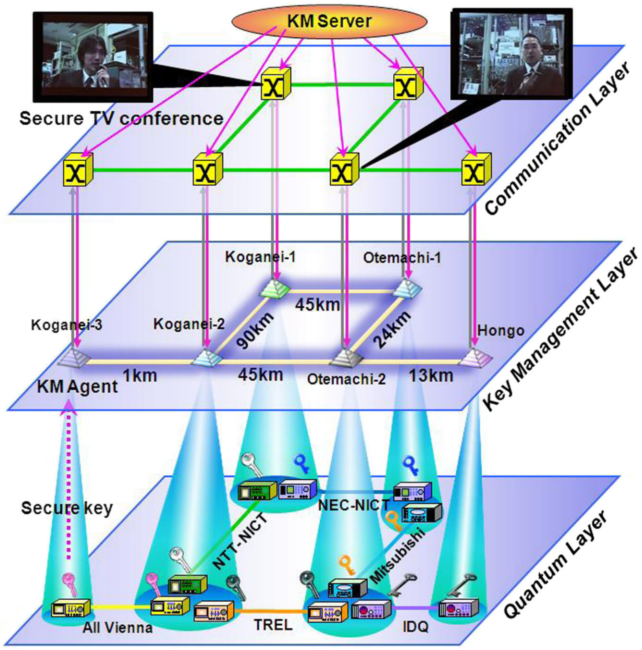

FIG. 12. Architecture of the Tokyo QKD Network. From Sasaki *et al.*, 2011.

(Liao *et al.*, 2017a) and 421 km in an ultra-low-loss optical fiber (Boaron *et al.*, 2018). Because of its convenient implementation and remarkable enhancement of performance, the decoy-state method has become a standard technique in current QKD implementations. A large-scale decoy-state QKD network was constructed recently that spans more than 2000 km of coverage area; see Fig. 2.

B. Source flaws

1. Basis-dependent source

In practice, there is often some difference between ρ_x and ρ_z; i.e., Eq. (17) might not be fulfilled. Then, in the worst-case scenario, we should assume that Eve is capable of distinguishing the basis choice and hence that she can attack two basis states separately. This kind of source is called a basis-dependent source. Obviously, the more state dependence there is on the basis, the easier it is for Eve to distinguish the bases and hence the lower the key rate.

Without loss of generality, we take the Z basis as an example. The general Shor-Preskill key-rate formula is (Shor and Preskill, 2000)

$$r \geq 1 - H(e_Z) - H(e_Z^p), \tag{46}$$

where e_Z^p is the Z-basis phase error rate defined in Eq. (10).

For a basis-dependent source, $e_Z^p \neq e_X$ since $\rho_Z \neq \rho_X$. However, if ρ_X is close to ρ_Z, we can still bound e_Z^p from the measured e_X. In the GLLP security analysis framework (Gottesman *et al.*, 2004), the basis dependence is quantified by a bias

$$\Delta = \frac{1 - F(\rho_X, \rho_Z)}{2}, \tag{47}$$

where $F(\rho_X, \rho_Z) = \sqrt{\sqrt{\rho_Z}\rho_X\sqrt{\rho_Z}}$ is the fidelity between the two states. Given this bias, the phase error rate used in the key-rate formula can be bounded by (Lo and Preskill, 2007; Koashi, 2009)

$$\begin{aligned} e_z^p \leq{} & e_j^b + 4\Delta(1-\Delta)(1-2e_x^b) \\ & + 4(1-2\Delta)\sqrt{\Delta(1-\Delta)e_x^b(1-e_x^b)}. \end{aligned} \tag{48}$$

For the practical photon sources presented in Sec. III.B, Alice and Bob have more information than the bias in Eq. (47) provides. For example, in principle, they can measure the photon number n, with which they can tag each quantum signal. Then, using the phase error correction of the entanglement distillation process, which would be reduced to privacy amplification for prepare-and-measure schemes, they could take advantage of this tagging. With the tagging, the GLLP key-rate formula can be written as (Gottesman *et al.*, 2004)

$$r \geq -H(E) + (1-\Delta)[1 - H(e_z^p)], \tag{49}$$

where E is the total QBER, Δ is the ratio of tagged signals, and e_z^p is the phase error rate of the untagged signals. Here we use the same notation of the bias Δ found in Eq. (47).

2. Nonrandom phase

A general example of a source flaw involves the use of weak coherent states with nonrandom phases to encode the basis and key information (Lo and Preskill, 2007). Their difference is treated as a source flaw, i.e, a basis dependence of the source. The encoded state $|\psi_{\beta\kappa}\rangle_B$ is

$$|\psi_{\beta\kappa}\rangle_B = |\alpha\rangle_R |\alpha e^{i\pi[\kappa + (1/2)\beta]}\rangle_S, \tag{50}$$

where α is a constant and $\mu = 2|\alpha|^2$ is the intensity. In this case, the basis dependence Δ is

$$\Delta = \tfrac{1}{2}\{1 - e^{\mu/2}[\cos(\mu/2) + \sin(\mu/2)]\} = \mu/8 + O(\mu^3). \tag{51}$$

Note that in the practical QKD experiment we will post-select the clicked signals. In this case, to calculate the basis dependence we have to take the channel transmittance η into account. In the worst-case scenario, the channel loss is caused by Eve's selection on the transmitted signals. To clarify this, we can consider Eve performing an USD attack (Dušek, Jahma, and Lütkenhaus, 2000), where Eve performs an USD to discriminate ρ_X from ρ_Z. If the discrimination is successful, then Eve can learn the basis and key, she generates the same state $\rho_{\beta\kappa}$, and she sends it to Bob. If the discrimination fails, Eve partially blocks the signal as loss. In this case, the basis dependence Δ' of left signals is amplified by η:

$$\Delta' = \Delta/(\eta\mu) \approx \mu/(8\eta). \tag{52}$$

From Eqs. (46), (48), and (52), we can calculate the key rate. However, the achievable key-generation rate scales only quadratically with the transmittance η in the channel, i.e., $r = O(\eta^2)$. This question can be potentially solved using the scheme of discrete phase randomization (Cao *et al.*, 2015).

3. Encoding flaws

Another example of a source flaw is the encoding flaws in the phase and the polarization encoding due to the device imperfections in the encoding devices. This also makes the source basis dependent. Although Gottesman *et al.* (2004) allow the security proof to consider encoding flaws, the key rate drops dramatically. This is because Gottesman *et al.* have a pessimistic viewpoint when assuming that the encoding flaws are in arbitrary dimensions. To address this issue, a loss-tolerant protocol was proposed by Tamaki *et al.* (2014) that makes QKD tolerable of channel loss in the presence of source flaws (Yin *et al.*, 2014).

On the basis of the assumption that the single-photon components of the states prepared by Alice remain inside a two-dimensional Hilbert space, it was shown that Eve cannot enhance state preparation flaws by exploiting the channel loss, and Eve's information can be bounded by the rejected data analysis. The intuition for the security of the loss-tolerant QKD protocol (Tamaki *et al.*, 2014) can be understood in the following manner. By assuming that the state prepared by Alice is a qubit, it becomes impossible for Eve to perform an USD attack. Indeed, for Eve to perform an USD attack, the states prepared by Alice must be linearly independent, but by having three or more states in a two-dimensional space, the set of states prepared by Alice is, in general, linearly dependent, thus making USD impossible. The previous loss-tolerant protocol was further developed and demonstrated experimentally for decoy-state BB84 (Xu, Wei *et al.*, 2015; Boaron *et al.*, 2018) and MDI-QKD (G.-Z. Tang *et al.*, 2016).

C. Leaky source

As discussed in Sec. IV.C, the source is vulnerable to a THA. In particular, Eve could inject bright light pulses into Alice's transmitter and then measure the backreflected light to extract information about Alice's state preparation process. This problem was analyzed by Lucamarini *et al.* (2015). They evaluated the security of a QKD system in the presence of information leakage from Alice's phase modulator (PM), which was used to encode the bit and basis information of the generated signals. A key observation was that the joint state of Alice's transmitted signals and Eve's backreflected light from her THA is not basis independent but instead depends on Alice's basis choice. The security of the system can be analyzed by quantifying Eve's information and considering this information in privacy amplification, based on the techniques introduced by Lo and Preskill (2007). Recently, these seminal results were generalized to prove the security of decoy-state QKD in the presence of arbitrary information leakage from both the PM and the intensity modulator (IM) (Tamaki, Curty, and Lucamarini, 2016; Wang, Tamaki, and Curty, 2018). Here the IM is normally used to select the intensity setting for each emitted signal. Consequently, it is possible to quantify the amount of device isolation against THA to achieve a certain performance with a realistic leaky QKD system.

VI. DETECTION SECURITY

In this section, we review the various approaches that address the detection security of practical QKD. We then review the MDI-QKD protocol and its extensions in more detail.

A. Countermeasures against detection attacks

Many approaches have been proposed to defeat the attacks at detection. The first one is the *security patch*. That is, once one discovers a new type of attack, a corresponding countermeasure against this attack can be proposed and realized in an existing QKD system. This approach usually requires only modifying the software or the hardware of a current system. For instance, the time-shift attack introduced in Sec. V can be avoided by simply shifting the gating window of the detectors at random (Qi, Fung *et al.*, 2007). The detector-blinding attack could, in principle, be avoided by monitoring the detector's photocurrent for anomalously high values (Yuan, Dynes, and Shields, 2011; da Silva *et al.*, 2012) or by randomly varying the detector efficiency (Lim *et al.*, 2015). Although a security patch could defeat certain attacks, patched countermeasures themselves might open other loopholes. This could, as a result, introduce one more layer of security risk (Sajeed, Radchenko *et al.*, 2015; A. Huang *et al.*, 2016; Qian *et al.*, 2019). Furthermore, a major issue associated with security patches is that they prevent the known attacks only. For potential and unknown attacks, the countermeasures may fail. Therefore, security patch is only *ad hoc*, which abandons the information-theoretic security framework of QKD.

The second approach is to fully characterize the devices used in a QKD system and precisely describe the devices in mathematical models. Then the models can be included in the security proof to estimate the real secure key rate based on an imperfect setup. A well-known example is the GLLP security proof (Gottesman *et al.*, 2004). While this approach seems to be straightforward, developing models to fully match the practical behavior of various QKD devices is rarely possible because the components are complex. Even so, there are several ongoing theoretical efforts to consider as many imperfections as possible in the security proof (Fung *et al.*, 2009; Marøy, Lydersen, and Skaar, 2010; Tamaki *et al.*, 2014; Lucamarini *et al.*, 2015; Tamaki, Curty, and Lucamarini, 2016). Nevertheless, this approach is limited by our understanding of the devices, and a complete knowledge of the devices is rather challenging. Hence, full characterization is still *ad hoc*.

The third approach is DI-QKD, which is reviewed in Sec. VIII.A. Note that there are also proposals for a semi-device-independent QKD, where one party's measurements are fully characterized while the other's are unknown (Pawłowski and Brunner, 2011; Branciard *et al.*, 2012; Smith *et al.*, 2012).

The final approach is the MDI-QKD protocol, which closes all detection attacks and works practically with current technology. We next review MDI-QKD in detail.

B. Measurement-device-independent scheme

MDI-QKD generates secret keys based on the "time-reversed" entanglement protocol and leaves all single-photon detections to a public, untrusted relay Eve.

1. Time-reversed EPR QKD

The MDI idea was inspired by the EPR-based QKD protocol (Ekert, 1991; Bennett, Brassard, and Mermin, 1992). This is illustrated in Fig. 13 (Biham, Huttner, and Mor, 1996). In the initial EPR-based protocol [Fig. 13(a)], Alice and Bob individually prepare an EPR pair at each side and send one photon from each pair to an untrusted center party Charles. Charles then performs a Bell state measurement (BSM) for entanglement swapping. The measurement result is

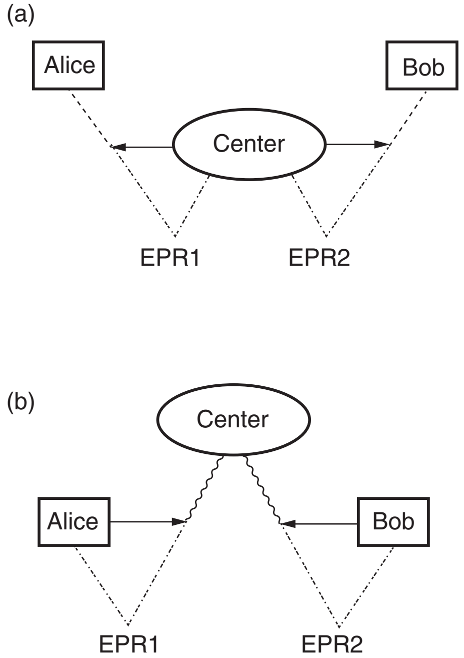

FIG. 13. EPR-based QKD protocol. One particle of each EPR correlated pair, denoted by dashed lines, is sent to the center, and a Bell state measurement (BSM) is performed. The second particles are sent to Alice and Bob, respectively, who project them onto the BB84 states. (a) Original EPR QKD. The first measurement is done at the center, and the particles arriving at Alice and Bob are therefore in the Bell state, which can be used to perform the QKD as in the EPR-based protocol (Ekert, 1991). (b) Time-reversed EPR QKD. The first measurement is performed by Alice and Bob and each particle sent to the center is therefore in one of the BB84 states, which forms the concept behind MDI-QKD (Lo, Curty, and Qi, 2012). From Biham, Huttner, and Mor, 1996.

announced. Once the BSM is finished, Alice and Bob measure the other photon of the EPR pairs locally by choosing between the X and Z bases randomly. Comparing a subset of their measurement results allows Alice and Bob to know whether Charles is honest. Then Alice and Bob can generate the secret using the BBM92 protocol (Bennett, Brassard, and Mermin, 1992).

Note that the EPR protocol can also work in a *time-reversal* version, as shown in Fig. 13(b). That is, Alice and Bob can measure their local photons first, instead of waiting for Charles's measurement results. This order of preparation and measurement is equivalent to that of the prepare-and-measurement QKD scheme, in which Alice and Bob prepare BB84 states and send them to Charles to perform the BSM. After that, Charles's honesty can be checked by comparing parts of Alice's and Bob's results. Charles's BSM is used only to check the *parity* of Alice's and Bob's bits; thus, it does not reveal any information about the individual bit values. This time-reversal EPR protocol forms the main concept behind MDI-QKD.

This time-reversed EPR QKD protocol was first proposed by Biham, Huttner, and Mor (1996). Later, Inamori (2002) provided a security proof. Nevertheless, these two important works offered limited performance, and therefore they have been largely forgotten by the QKD community. For instance, the scheme in Biham, Huttner, and Mor (1996) requires perfect single-photon sources and long-term quantum memories, which renders it unpractical with current technology. The scheme of Inamori (2002) uses practical WCPs but does not include decoy states, since it was proposed long before the advent of the decoy-state protocol. Moreover, two early papers (Biham, Huttner, and Mor, 1996; Inamori, 2002) did not specifically consider the side-channel problem in QKD. Braunstein and Pirandola (2012) performed a general security analysis of the time-reversed EPR QKD approach and proved that detector side-channel attacks can be eliminated by using teleportation in which any incoming quantum signals are excluded from accessing the detectors. Note that the idea of using teleportation for the specific purpose of removing side channels was first discussed in footnote 21 of Lo and Chau (1999).

2. MDI-QKD protocol

The MDI-QKD proposal (Lo, Curty, and Qi, 2012) [see also Braunstein and Pirandola (2012)] builds on the time-reversed EPR QKD. In particular, the main merits of the proposal, introduced by Lo, Curty, and Qi (2012), are twofold: First, it identifies the importance of the results in Biham, Huttner, and Mor (1996) and Inamori (2002) to remove all detector side channels from QKD implementations. Second, it significantly improves the system performance with practical signals by including decoy states. The protocol can be summarized in four steps.

(1) Alice and Bob randomly and individually prepare one of four BB84 states using phase-randomized WCPs together with decoy signals. Then they send the states to an untrusted party Charles.

(2) An honest Charles performs a BSM that makes Alice's and Bob's states interfere with each other, generating a Bell state. An example of a BSM implementation with linear optics in shown in Fig. 14: Charles interferes the incoming pulses at a 50:50 beam splitter (BS), which has on each end a PBS that projects the photons into either horizontal (H) or vertical (V) polarization states. A click in the single-photon detectors D_{1H} and D_{2V} or in D_{1V} and D_{2H} indicates a projection into the singlet state $|\psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$, while a click in D_{1H} and D_{1V} or in D_{2H} and D_{2V} implies a projection into the triplet state $|\psi^+\rangle = (|HV\rangle + |VH\rangle)/\sqrt{2}$. Other detection patterns are considered unsuccessful.

(3) Whether Charles is honest or not, he announces the outcome of his claimed BSM using a classical public channel when he claims to obtain a successful measurement.

(4) Alice and Bob keep the data that correspond to Charles's successful measurement events and discard the rest. Next, similar to the sifting in the BB84 protocol, Alice and Bob announce their basis choices for sifting the events and keep the events using the same bases. Based on Charles's measurement result, Alice flips some of her bits to guarantee the correct correlation with those of Bob. The postselection strategy is illustrated in Table XV. Finally, they use the decoy-state method to estimate the gain and QBER of the single-photon contributions.

In MDI-QKD, both Alice and Bob are senders, and they transmit signals to an untrusted third party Eve, who is supposed to perform a BSM. Since the BSM is used only to postselect entanglement, it can be treated as an entirely

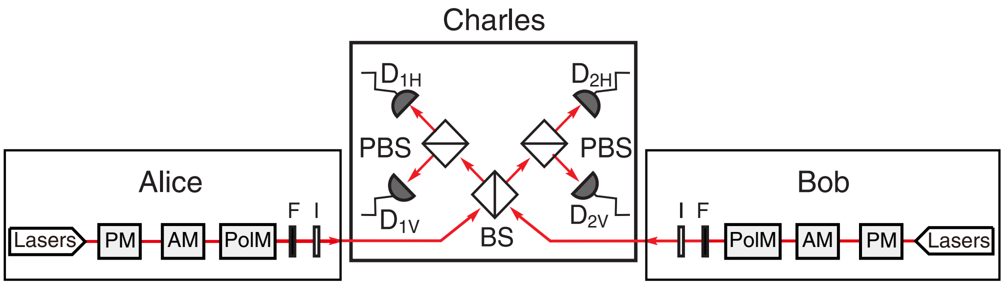

FIG. 14. Schematic diagram of MDI-QKD proposed by Lo, Curty, and Qi (2012). Alice and Bob prepare BB84 polarization states using a decoy-state BB84 transmitter that is the same as the one illustrated in Fig. 10. They send BB84 states to an untrusted relay from Charles to Eve. The relay is supposed to perform a BSM that projects Alice's and Bob's signals into a Bell state.

TABLE XV. Postselection for MDI-QKD (Lo, Curty, and Qi, 2012). Alice and Bob postselect the events where the relay outputs a successful result and use the same basis in their transmission. Moreover, either Alice or Bob flips her or his bits, except in the cases where both of them select the diagonal basis and the relay outputs a triplet

	Singlet state $\lvert\psi^-\rangle$	Triplet state $\lvert\psi^+\rangle$
Coincident clicks	D_{1H} and D_{2V} or D_{2H} and D_{1V}	D_{1H} and D_{1V} or D_{2H} and D_{2V}
Rectilinear basis	Bit flip	Bit flip
Diagonal basis	Bit flip	⋯

TABLE XVI. Security assumptions in DI-QKD and MDI-QKD. While DI-QKD has the advantage of being applicable to an uncharacterized source, it demands no unwanted information leakage from the measurement unit. MDI-QKD applies to any measurement units. This means that the measurement unit in MDI-QKD can be an entire black box, purchased from untrusted vendors.

	DI-QKD	MDI-QKD
True random number generators	Yes	Yes
Trusted classical postprocessing	Yes	Yes
Authenticated classical channel	Yes	Yes
No unwanted information leakage from the measurement unit	Yes	No
Characterized source	No	Yes

black box. Hence, MDI-QKD can remove all detection side channels. The assumption in MDI-QKD is that the source should be trusted. The security assumptions of MDI-QKD, together with those of DI-QKD (see Sec. VIII.A), are summarized in Table XVI. A comparison of practical security between MDI-QKD and DI-QKD, as commented upon by Bennett,[19] is summarized in Box VI.B.2.

Box VI.B.2: A security remark about MDI-QKD and DI-QKD by Charles H. Bennett.

MDI-QKD at first sounds weaker than DI-QKD, but in fact it is stronger. In MDI-QKD, Eve's untrusted device remains outside Alice's and Bob's trusted enclosures. They need only trust themselves not to have inadvertently created a side channel to Eve through incompetent design of their do-it-yourself light sources. By contrast, in DI-QKD they must trust Eve not to have deliberately created side channels from the untrusted devices to herself.

3. Theoretical developments

The decoy-state analysis is essential for MDI-QKD. The analysis is different from that of conventional decoy-state BB84 in that now both Alice and Bob send decoy signals to a common receiver (instead of only Alice sending decoy signals to Bob), which makes the mathematics slightly more complex. Fortunately, it has been shown that it is enough to obtain a tight estimation if Alice and Bob employ just a few decoy settings each. Ma, Fung, and Razavi (2012) and Wang (2013), respectively, proposed a numerical method based on linear programming and an analytical approach based on Gaussian elimination. Both approaches assume that Alice and Bob can prepare a vacuum intensity. Following a similar analytical line, Xu, Curty *et al.* (2013) studied the situation in which none of the two decoy intensities are vacuum ones.[20] A full parameter optimization method was proposed by Xu, Xu, and Lo (2014). Soon thereafter, Yu, Zhou, and Wang (2015) proposed using joint constraints for a better key rate, and Zhou, Yu, and Wang (2016) proposed a four-intensity method in which the key generation is conducted in the Z basis and the decoy analysis is performed only in the X basis. By doing so, the four-intensity method is efficient in the case of short data size. Recently, the four-intensity method was extended to a seven-intensity method that can substantially enhance the key rate for MDI-QKD over asymmetric channels (Wang, Xu, and Lo, 2019). All of these results provide experimentalists with a clear path to implement MDI-QKD with a finite number of decoy states.

For finite-key analysis, Ma, Fung, and Razavi (2012) provided an analysis that assumes a Gaussian distribution for the statistical fluctuations. Curty *et al.* (2014) presented a rigorous finite-key security proof against general attacks by using min-entropy analysis and the Chernoff bound. In addition, this result satisfies the composable security definition. All of these results confirm the feasibility of long-distance implementations of MDI-QKD within a reasonable time frame of signal transmission. Simulations of the secret key rates with different kinds of decoy-state methods and finite-key analysis methods are shown in Fig. 15.

Other practical aspects have also been extensively analyzed in theory. Besides polarization encoding in the original MDI-QKD protocol (Lo, Curty, and Qi, 2012), alternative schemes including phase encoding (Tamaki *et al.*, 2012) and time-bin encoding (Ma and Razavi, 2012) have been proposed and analyzed. To extend the transmission distance further, one could include quantum memories (Abruzzo, Kampermann, and Bruß, 2014; Panayi *et al.*, 2014), entanglement sources (Xu, Qi *et al.*, 2013), or adaptive operations (Azuma, Tamaki, and Munro, 2015). Moreover, a key security assumption in MDI-QKD is that the source should be trusted. Recently, there has been an effort to prove the security of MDI-QKD when Alice's and Bob's encoding devices are flawed (Tamaki *et al.*, 2014; Xu, Wei *et al.*, 2015) or when their apparatuses are not fully characterized (Yin *et al.*, 2014). Furthermore, a plug-and-play type of MDI-QKD was proposed by Xu (2015) and Choi *et al.* (2016) and experimentally demonstrated by G.-Z. Tang *et al.* (2016).

4. Experimental developments

Table III summarizes the MDI-QKD experiments after its invention. The main experimental challenge of MDI-QKD is to perform a high-visibility two-photon interference between photons from two independent laser sources (Alice's and Bob's) (Lo, Curty, and Qi, 2012), which is not required in conventional QKD schemes. To do so, Alice's photons should be indistinguishable from those of Bob. If one implements MDI-QKD over telecom fibers, it is necessary to include

[19] See slide 6 of Charles H. Bennett's talk in the Lightning Talks session of QCrypt 2018: http://2018.qcrypt.net/.

[20] A vacuum state is normally hard to realize in practice due to the finite extinction ratio of a practical intensity modulator.

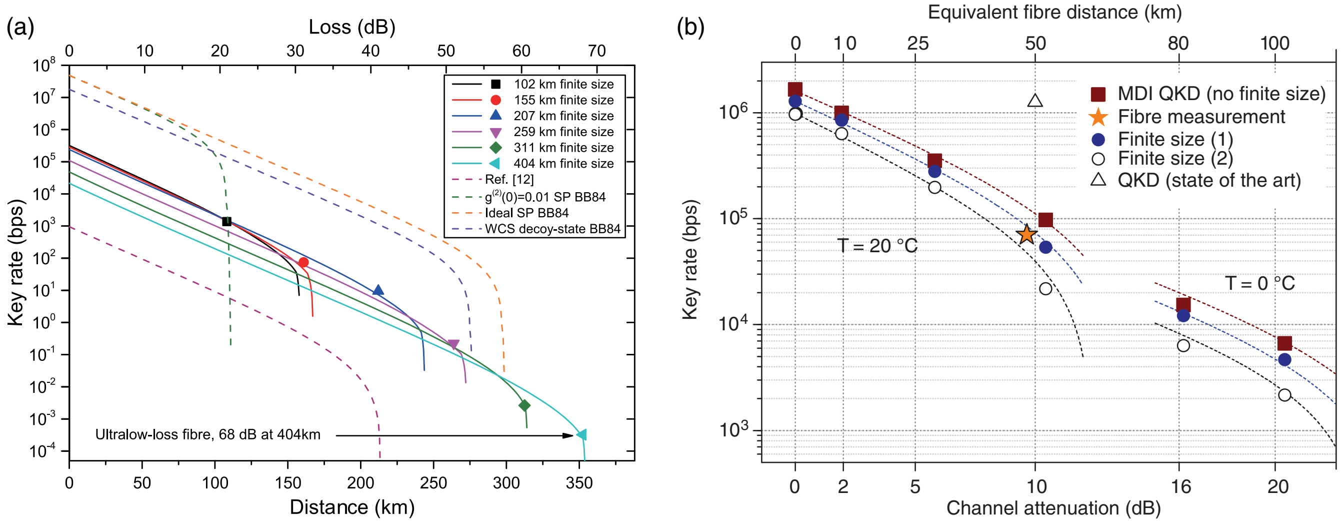

FIG. 15. Simulation and experimental secret rates of MDI-QKD. (a) 404-km MDI-QKD (Yin *et al.*, 2016). The experimental results (symbols) agree well with the theoretical simulations (solid lines). The dotted lines from upper to bottom show, respectively, the simulations for the balanced-basis passive BB84 protocol using ideal single-photon (SP) sources, the practical SP without the decoy-state method, the WCS with the decoy-state method, and the results of Y.-L. Tang *et al.* (2014). (b) 1-GHz MDI-QKD (Comandar *et al.*, 2016). Filled squares refer to key rates without the finite-size analysis. The star is the key rate obtained using two 25-km spools of fiber. The filled and open dots represent key rates with the finite-size analysis. The finite-size distillation methods are (1) standard error analysis (Ma, Fung, and Razavi, 2012) and (2) composable security analysis (Curty *et al.*, 2014). The dashed lines are simulations of the key rate for two different detector temperatures. From Comandar *et al.*, 2016, and Yin *et al.*, 2016.

feedback controls to compensate for the time-dependent polarization rotations and propagation delays caused by the two separated fibers. Note that in standard BB84 QKD systems the requirement of compensating for polarization rotations and propagation delays can be relaxed by using phase encoding because the two optical pulses, which interfere with each other at the receiver's end, pass through the same optical fiber and thus experience the same polarization rotation and phase change. Therefore, one can achieve high interference visibility without performing any polarization control. Nevertheless, this advantage of phase encoding (in comparison to other encoding schemes) cannot be directly translated to MDI-QKD because the two pulses pass through two *independent* quantum channels.

In 2013, several groups performed independent experimental study for MDI-QKD. Liu *et al.* (2013) reported the first demonstration of MDI-QKD with random modulation for encoding states and decoy states over 50-km fiber. Simultaneously, Rubenok *et al.* (2013) were the first to demonstrate the feasibility of high-visibility two-photon interference between two independent lasers, passing through separate field-deployed fibers in a real-world environment. Later, Ferreira da Silva *et al.* (2013) observed similar interference using polarization encoding in the lab, and Z. Tang *et al.* (2014) reported a full demonstration of polarization encoding MDI-QKD with random modulation of encoding states and decoy states. All four of these initial experiments, when taken together, complete the cycle needed to demonstrate the feasibility of MDI-QKD using off-the-shelf optoelectronic devices. Their experiment diagrams are illustrated in Fig. 16.

MDI-QKD is attractive not only because of its security against detection attacks but also due to its practicality. It can resist high channel loss and reach a long distance. Tang *et al.* implemented MDI-QKD over 200-km fiber (Y.-L. Tang *et al.*, 2014) and in a field environment (Tang *et al.*, 2015) by increasing the system clock rate from 1 to 75 MHz, developing an automatic feedback system, and utilizing SNSPDs.

In 2016, two millstone MDI-QKD experiments were reported. In the first, Yin *et al.* (2016) extended the MDI-QKD to a record-breaking distance of 404 km by optimizing the implementation parameters and using a ultra-low-loss fiber (0.16 dB/km). The key rate achieved in the experiment at 100 km is around 3 kbits/s, which is sufficient for one-time-pad encoding of a voice message. The results demonstrated by Yin *et al.* (2016) are shown in Fig. 15(a). In the second experiment, Comandar *et al.* (2016) increased the system clock rate of MDI-QKD to 1 GHz by exploiting the technique of optical seed lasers. The 1-GHz system demonstrated the feasibility of MDI-QKD reaching a 1-Mbits/s key rate. The achieved secret rates of Comandar *et al.* (2016) are shown in Fig. 15(b).

Besides a long distance and high rate, several research groups have analyzed the practical aspects in the implementation of MDI-QKD. For instance, Valivarthi *et al.* (2015, 2017) analyzed the trade-offs among complexity, cost, and system performance associated with the implementation of MDI-QKD and implemented a cost-effective system. C. Wang *et al.* (2015, 2017) demonstrated a reference-frame-independent MDI-QKD that requires no phase reference between Alice and Bob, and this scheme was recently improved to a clock rate of 50 MHz by H. Liu *et al.* (2018). G.-Z. Tang *et al.* (2016) demonstrated MDI-QKD with source flaws. Roberts *et al.* (2017) reported a reconfigurable system to switch between QKD and MDI-QKD. Instead of giving a MDI-QKD demonstration with WCP sources, Kaneda *et al.*

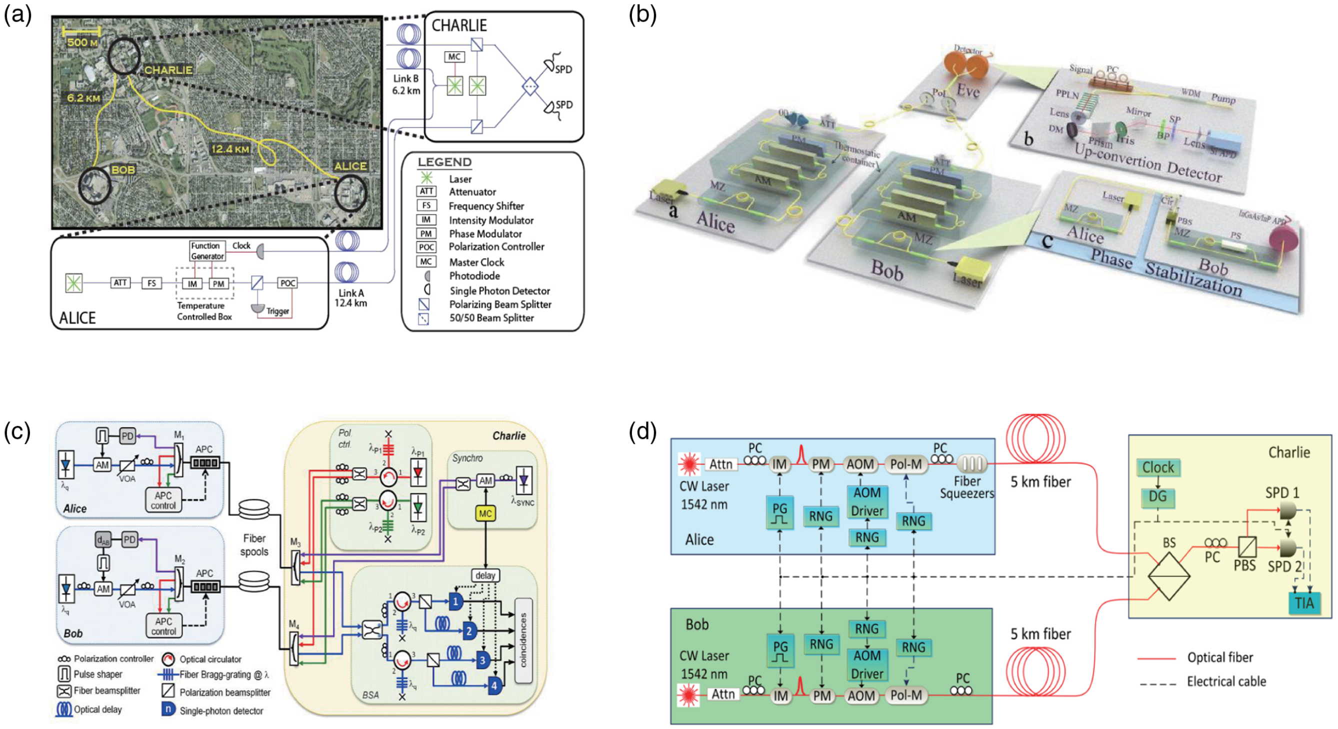

FIG. 16. The four initial MDI-QKD experiments. (a) Proof-of-principle MDI-QKD with time-bin encoding. From Rubenok *et al.*, 2013. (b) Full MDI-QKD implementation with random modulations of states and decoy intensities based on time-bin encoding. From Liu *et al.*, 2013. (c) Proof-of-principle MDI-QKD with polarization encoding. From Ferreira da Silva *et al.*, 2013. (d) Full MDI-QKD with random modulations of states and decoy intensities based on polarization encoding. From Z. Tang *et al.*, 2014.

(2017) demonstrated MDI-QKD using heralded single-photon source. Furthermore, a continuous-variable version of MDI-QKD was also proposed and studied (Pirandola *et al.*, 2015); it is reviewed in Sec. VII.

With all of the previously mentioned experimental efforts, MDI-QKD is ready for applications in future quantum networks. MDI-QKD is particularly well suited to constructing a centric star-type QKD network even with untrusted relays. Indeed, Y.-L. Tang *et al.* (2016) performed the first implementation of a field MDI-QKD network, which has four nodes with one untrusted relay node and three user nodes. Note that if the central relay is trusted, one can reconfigure the MDI-QKD network to allow many quantum communication protocols (Roberts *et al.*, 2017). Moreover, high-rate MDI-QKD over asymmetric fiber channels was demonstrated recently by H. Liu *et al.* (2019), based on the theoretical proposal by Wang, Xu, and Lo (2019). The asymmetric MDI-QKD is valuable to practical metropolitan network settings, where the channel losses are naturally asymmetric and the user nodes could be dynamically added or deleted. Furthermore, Wei *et al.* (2019) implemented the first chip-based MDI-QKD at a 1.25-GHz clock rate. This is important for developing a low-cost and secure quantum network, where expensive devices such as single-photon detectors can be placed in the central untrusted relay and each user requires only a simple Si chip.

C. Twin-field QKD

A fundamental bound (Takeoka, Guha, and Wilde, 2014) and secret key capacity (SKC) (Pirandola *et al.*, 2017) have been obtained for the secure key rate versus the distance of the QKD. It was proven that, in the absence of relays, the key rate basically scales linearly with transmittance $O(\eta)$, where η is the transmittance of the channel between Alice and Bob. This is called the linear bound (of the secret key rate of a lossy quantum channel). There is tremendous research interest in developing a feasible scheme, known as a quantum repeater (Sangouard *et al.*, 2011), to overcome the fundamental rate-distance limit. However, the deployment of a quantum repeater is still beyond the capabilities of current technology.

Lucamarini *et al.* (2018) proposed a novel phase-encoding MDI-QKD protocol called twin-field QKD (TF-QKD) which shows the possibility of overcoming the SKC. In TF-QKD (see Fig. 17), weak optical pulses are generated by two phase-locked laser sources, which are phase randomized and then phase encoded with secret bits and bases. The pulses are sent to Charlie for interference on a beam splitter. Depending on which detector clicks, Charlie can infer whether the secret bits of the users Alice and Bob are equal or different but cannot learn their absolute values. TF-QKD essentially uses single-photon interference (Duan *et al.*, 2001), and the implementation requires only standard optical elements without the requirement of quantum memory (Sangouard *et al.*, 2011). The key goal of the TF-QKD protocol is to achieve a quadratic improvement [i.e., scaling to $O(\sqrt{\eta})$] to the key rate as a function of channel transmittance. Unfortunately, in the original paper (Lucamarini *et al.*, 2018), such a quadratic improvement was proven for only a restricted class of attacks by Eve.

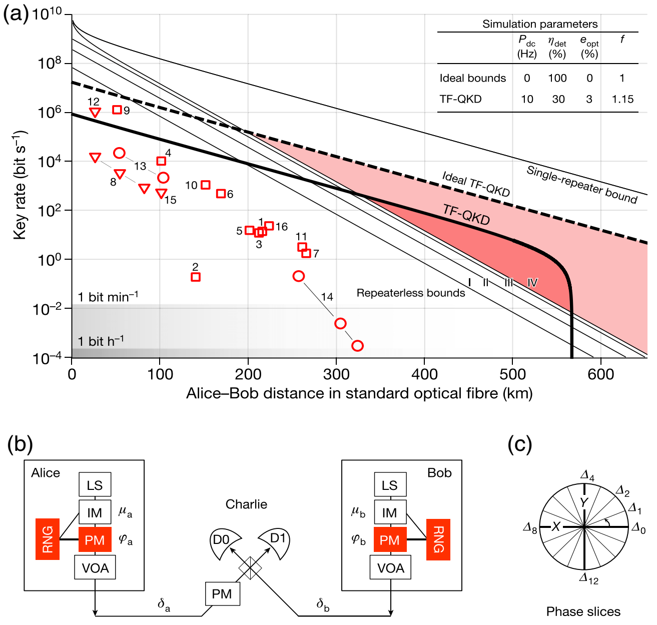

FIG. 17. Schematic diagram of TF-QKD. (a) Theoretical bounds (lines) and experimental results (symbols) for fiber-based quantum schemes. Theoretical bounds: I, decoy-state MDI-QKD; II, decoy-state QKD; III, single-photon QKD; IV, SKC (Pirandola *et al.*, 2017). Experimental results: squares, triangles, and circles are for QKD, continuous-variable QKD, and MDI-QKD [see Lucamarini *et al.* (2018) for details]. The solid (dashed) line represents the realistic (ideal) TF-QKD key rate and the dark-pink (light-pink) shaded area is the region in which it overcomes the SKC. (Inset) Parameters used for numerical simulations. $P_{\rm dc}$, dark count probability; $\eta_{\rm det}$, total detection efficiency; $e_{\rm opt}$, channel optical error rate; f, error correction coefficient. (b) Setup to implement TF-QKD. The light sources (LSs) generate pulses whose intensities $\mu_{a,b}$ are randomly varied by the intensity modulators (IMs) to implement the decoy-state technique. Phase modulators (PMs) are combined with random number generators (RNG) to encode each light pulse with phases $\varphi_{a,b}$. The variable optical attenuators (VOAs) set the average output intensity of the pulses to bright (classical regime) or dim (quantum regime). The pulses travel along independent channels, acquiring phase noise $\delta_{a,b}$, to then interfere on Charlie's beam splitter and be detected by the single-photon detectors D0 and D1. Charlie uses the bright pulses in the classical regime and the phase modulator in his station to phase align the dim pulses emitted in the quantum regime that provide the bits of the key. (c) Discretization of the phase space for identifying the twin fields during the public discussion. From Lucamarini *et al.*, 2018.

Following the TF-QKD scheme (Lucamarini *et al.*, 2018), Ma, Zeng, and Zhou (2018) proposed a protocol named phase-matching QKD (PM-QKD) and proved its unconditional security, inspired by the previous phase-encoding MDI-QKD protocol (Tamaki *et al.*, 2012) and the MDI version of the Bennett 1992 protocol (Ferenczi, 2013). PM-QKD employs coherent states as information carriers directly and uses the decoy-state method in an indirect way. In a sense, PM-QKD adopts a discrete-modulation continuous-variable encoding and discrete-variable single-photon detection. The performance of PM-QKD is shown in Fig. 18. One can see that its key rate can go beyond the linear SKC with certain realistic parameter settings.

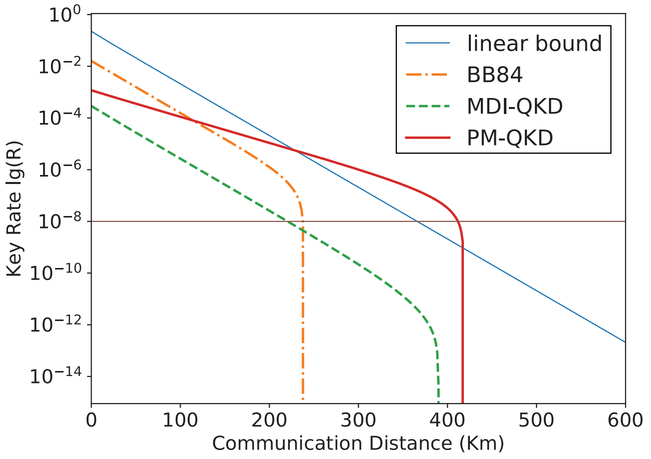

FIG. 18. Key rate of PM-QKD compared to the theoretical SKC (Pirandola *et al.*, 2017) and other protocols (Ma, Zeng, and Zhou, 2018). The key rate is shown to surpass the linear key-rate bound when the communication distance $l > 230$ km. The simulation uses realistic parameters: detector efficiency 14.5%, dark count rate 7.2×10^{-8}, error correction efficiency 1.15, channel misalignment error 1.5%, and number of phase slices 16. From Ma, Zeng, and Zhou, 2018.

On the other hand, with the BB84-type two-basis analysis, Tamaki *et al.* (2018) proposed a modified X/Y–basis protocol, and Wang, Yu, and Hu (2018) proposed an X/Z–basis protocol where the single-photon states used were regarded as the information carrier. Afterward, simplified coherent-state-based protocols without phase randomization on the key-generation mode were proposed (Lin and Lütkenhaus, 2018; Cui *et al.*, 2019; Curty, Azuma, and Lo, 2019) and analyzed in the infinite data size case. Later, Maeda, Sasaki, and Koashi (2019) introduced an efficient parameter estimation method for the PM-QKD protocol and complete the finite-size analysis. All of these recent theoretical works make the new TF-type MDI-QKD protocols important for the deployment of QKD over long distances.

The security of PM-QKD, unlike the usual BB84-type two-basis protocol, is closely related to the symmetry of source state with respect to the encoding operation. To establish the correlation between encoding symmetry and privacy, Zeng, Wu, and Ma (2019) introduced a symmetry-based security proof method for a general type of MDI-QKD protocols. For these MDI-QKD protocols, there exist symmetric source states that promise perfect privacy, i.e., that cause no information leakage. Therefore, for a generic source state input, the privacy of the protocol depends only on the ratio of the symmetric component contained in it, regardless of the channel noise. As a result, this symmetry-based security proof allows higher error tolerance than the original complementarity-based proof. For example, PM-QKD has proved to be able to yield a positive key even with a high bit error rate of up to 50% and surpassing the linear key-rate bound even with bit error rate of 13% (Zeng, Wu, and Ma, 2019).

From a technical point of view, the replacement of two-photon detection with single-photon detection is the key reason for the quadratic improvement, but single-photon interference with two remote independent lasers requires subwavelength-order phase stability for optical channels (Duan *et al.*, 2001), which is more demanding in long-distance communication than achieving two-photon interference, which does not require phase stability between the two photons. Nonetheless, TF-QKD protocols are expected to be feasible with the current techniques of active phase randomization, optical phase locking, etc. Indeed, in 2019 four research groups reported experimental demonstrations on the feasibility of TF-QKD (Y. Liu *et al.*, 2019; Minder *et al.*, 2019; Wang, He *et al.*, 2019; Zhong *et al.*, 2019). Recently, the PM-QKD experiment was realized with random modulations and a consideration of the finite-key effect by Fang *et al.* (2019), whose key rate surpassed the linear key-rate bound via 302- and 402-km commercial fiber. Through a 502-km ultra-low-loss fiber with an 87.1-dB total loss, PM-QKD can yield a key rate of 0.118 bits/s with unconditional security. By using the ultrastable cavity and optical phase locking, a sending-or-not-sending version of the TF-QKD protocol was demonstrated over 509-km ultra-low-loss fiber (J.-P. Chen *et al.*, 2020), where the achieved secure key rate is even higher than that of a traditional QKD protocol running with a perfect repeaterless QKD device. A proof-of-principle experiment demonstrated TF-QKD over optical channels with asymmetric losses (Zhong *et al.*, 2020). Table IV summarizes the recent TF-QKD experiments.

VII. CONTINUOUS-VARIABLE QKD

Broadly speaking, QKD can be divided into two classes, namely, DV and CV. Unlike DV or qubit-based QKD, the secret keys in CV-QKD are encoded in quadratures of the quantized electromagnetic field and decoded by coherent detections (Weedbrook *et al.*, 2012). Coherent detection is a promising candidate for practical quantum-cryptographic implementations due to its compatibility with existing telecommunications equipment and high detection efficiencies without the requirement of cooling. CV-QKD protocols can be divided into several categories depending upon whether the prepared state is coherent (Grosshans and Grangier, 2002) or squeezed state (Hillery, 2000), the modulation schemes are Gaussian (Cerf, Lévy, and Assche, 2001) or discrete modulations (Ralph, 1999; Hillery, 2000; Reid, 2000), the detection schemes are homodyne (Grosshans and Grangier, 2002) or heterodyne detections (Weedbrook *et al.*, 2004), the error correction schemes are direct or reverse reconciliations (Grosshans *et al.*, 2003), etc.

In this section, we primarily review the simplest and the most widely developed CV-QKD protocol: the Gaussian-modulated coherent-state (GMCS) protocol (Grosshans and Grangier, 2002; Grosshans *et al.*, 2003), which is believed to be the core of today’s implementations. We briefly discuss the security analysis and experimental developments of CV-QKD, together with a focus on the practical security aspects in its implementations, including the side channels and the advanced countermeasures. We do not cover much in the way of other CV-QKD protocols (Silberhorn *et al.*, 2002; Pirandola *et al.*, 2008; Weedbrook *et al.*, 2010; Usenko and Grosshans, 2015), which can be found in an earlier review (Weedbrook *et al.*, 2012). We also refer interested readers to two recent CV-QKD reviews on security analysis and practical issues (Diamanti and Leverrier, 2015), the issues of trusted noise (Usenko and Filip, 2016), and the models of implementation and noise (Laudenbach *et al.*, 2018).

A. Protocol and security

1. Gaussian-modulated protocol

The first Gaussian continuous modulated protocol was a Gaussian-modulated squeezed-state protocol (Cerf, Lévy, and Assche, 2001), where the key is encrypted in the displacement of a squeezed state. The random choice of the direction in which to squeeze is similar to the basis choice in the BB84 protocol. The squeezed-state protocol was later extended to GMCS protocols (Grosshans and Grangier, 2002; Grosshans *et al.*, 2003) since coherent states are easier to prepare in practice. We summarize the prepare-and-measure version of a general GMCS protocol in Box VII.A.1. A difference from a DV-QKD protocol is that, in a coherent-state protocol, the key information of both bases is encrypted in the prepared state simultaneously per channel use. Therefore, Bob’s measurement can be correlated with Alice’s key in either basis or both bases.

Box VII.A.1: GMCS QKD protocol.

(1) Alice produces two random numbers x_A and p_A from random numbers following a Gaussian distribution with a variance of $V_A N_0$, where N_0 is the vacuum noise unit.
(2) Alice prepares a coherent state $|x_A + ip_A\rangle$ and sends it to Bob through an untrusted quantum channel.
(3) Bob chooses homodyne (heterodyne) detection to measure X and P randomly (simultaneously) and obtains the outcomes x_B and p_B.
(4) After repeating this process N times, Alice and Bob sift the measurement results using a classical channel and obtain N pairs of raw keys, i.e., the correlated Gaussian variables, in the homodyne detection protocol ($2N$ pairs in the heterodyne detection protocol).
(5) Alice and Bob perform postprocessing on the raw key including parameter estimation, error correction, and privacy amplification.

In the GMCS protocol (Grosshans and Grangier, 2002; Grosshans *et al.*, 2003), the source is a mixture of coherent state $|\alpha_j\rangle = |x_j + ip_j\rangle$ with quadrature components x_j and p_j as the realizations for two i.i.d. random variables X and P. These two random variables obey the same zero-centered Gaussian distribution $\mathcal{N}(0, V_m)$, where V_m is the modulated variance. The total variance of the Gaussian-modulated source is $V = V_s + V_m$, where V_s is the intrinsic quadrature uncertainty of the coherent state. Another type of GMCS scheme is a coherent-state source mixed with trusted thermal noise (Weedbrook *et al.*, 2010) whose total variance is $V = V_s + V_m + V_{th}$, with an additional thermal variance V_{th}. This type of protocol is also widely used due to its low cost in state preparation together with the feasibility for QKD in a wavelength longer than the optical band. The decoding process is based on coherent detection measuring quadratures of optical fields. For CV-QKD schemes, coherent detection can be classified into homodyne detection and heterodyne detection, measuring quadratures of optical fields (Weedbrook *et al.*, 2012).

Note that the coherent-state protocol with homodyne detection can be modified to a no-switching protocol using heterodyne detection, which enables the communication partners to extract secure keys from both quadrature measurements (Weedbrook *et al.*, 2004). Postselection (Silberhorn *et al.*, 2002) and two-way communication (Pirandola *et al.*, 2008) can also be applied to improve performance. The GMCS protocol is believed to be the best understood protocol to date in terms of security and implementation. Its implementation is also relatively simple, as it requires only standard technology in telecommunication.

2. Discrete-modulated protocol

Besides the Gaussian-modulated protocol, there exists another type of protocol using discrete modulation. Here the key is encoded in the random phases of coherent states, and the source is an N-discrete randomized coherent-state mixture. In fact, the discrete-modulated protocol was proposed before the Gaussian-modulated protocol (Ralph, 1999; Reid, 2000; Hiroshima, 2006). However, owing to its non-Gaussian nature, a complete security proof of the discrete-modulated protocol that gives a good key rate in practice is challenging. In a discrete-modulated protocol, Alice prepares an alphabet of N coherent states $|\alpha_k\rangle = ||\alpha|e^{i2k\pi/N}\rangle$, where k is the secret key. Bob uses either homodyne or heterodyne detection to estimate k. The discrete-modulated protocol is more practical because (i) a real Gaussian modulation can never be perfectly implemented, and (ii) it can simplify the crucial step of error correction. Early proofs of discrete-modulated protocol restrict attacks to a linear quantum channel between Alice and Bob (Leverrier and Grangier, 2009). Though there are proofs for specific protocols where $N = 2$ (Zhao *et al.*, 2009) or $N = 3$ (Brádler and Weedbrook, 2018), the key rate is quite pessimistic and cannot be generalized to multiple state cases.

Recently, a numerical method of security analysis was proposed (Coles, Metodiev, and Lütkenhaus, 2016) where the security analysis is transformed into a convex optimization problem with the constraints that the statistics of certain observable should be compatible with experimental data. Following this line, there are two independent works analyzing the asymptotic security of the quadrature-phase-shift-keying protocol (Ghorai *et al.*, 2019; Lin, Upadhyaya, and Lütkenhaus, 2019), i.e., $N = 4$. With a photon-number cutoff assumption on Bob's side, it is feasible to compute the target function and constraints as a function of Alice and Bob's two-mode state. Such a photon-number cutoff assumption is valid since composable security proofs of CV-QKD usually require a projection onto a low-dimensional subspace of the Fock space via an energy test (Renner and Cirac, 2009). These proofs can be generalized to multiple state cases, showing that the key rate converges to Gaussian-modulated protocols when $N \to \infty$. Moreover, another security proof was reported recently that applies entropic continuity bounds and approximates a complex Gaussian probability distribution with a finite-size Gauss-Hermite constellation (Kaur, Guha, and Wilde, 2019). How to generalize the existing security proofs to the finite-size case remains an open question.

3. Security analysis

Intuitively, the security of coherent-state protocol comes from the fact that coherent states are nonorthogonal, which ensures the no-cloning theorem. To rigorously analyze the security, it is convenient to consider an entanglement-based protocol. Alice prepares a two-mode EPR state $|EPR_{AA'}\rangle$. Alice keeps one mode A in her lab and sends the other mode A' to Bob through a noisy channel $\mathcal{E}_{A'\to B}$. Alice performs heterodyne detection on her mode and gets a coherent-state output, which is identical to preparing a coherent state for Bob from Eve's point of view. We assume the worst-case scenario, where Eve holds a purification of ρ_{AB}. Then the tripartite state shared by Alice, Bob, and Eve is given by

$$\rho_{ABE} = [id_A \otimes \mathcal{U}_{A'\to BE}(|\mathrm{EPR}\rangle\langle\mathrm{EPR}|_{AA'})], \tag{53}$$

where id_A denotes the identity map on Alice's mode A and $\mathcal{U}_{A'\to BE}$ is an isometry. Alice and Bob's secure information under collective attack in the asymptotic limit for reverse reconciliation is given by the Devetak-Winter formula (Devetak and Winter, 2005)

$$K = I(A:B) - \sup \chi(B:E), \tag{54}$$

where $\chi(B:E)$ is the Holevo bound (Holevo, 1973). The supremum is computed over all possible quantum channels compatible with the statistics obtained in the parameter estimation step in implementation. The secure key can be distilled as long as Alice and Bob's mutual information is larger than the maximum of Bob's classical information accessible to Eve through the quantum channel between Bob and Eve.

Specifically, in the parameter estimation step, Alice and Bob exchange the statistics calculated from a subset of the sifted raw key and estimate the covariance matrix of the two-mode state shared by them

$$\gamma_{AB} = \begin{pmatrix} V_A I_2 & Z\sigma_z \\ Z\sigma_z & V_B I_2 \end{pmatrix}, \tag{55}$$

where V_A and V_B are the variance of the quadratures, I_2 is the two-dimensional identity matrix, and Z is the covariance calculated with the experimental data.

Thanks to the Gaussian optimality proved by García-Patrón and Cerf (2006), Navascués, Grosshans, and Acín (2006), and Wolf, Giedke, and Cirac (2006), the optimal collective attack Eve can implement is the one based on Gaussian operations, which results in a two-mode Gaussian state. Owing to the one-to-one correspondence between the Gaussian states and the covariance matrix, we can directly calculate the secure key rate under collective attack by the covariance matrix. Suppose that the optimal attack is characterized by a Gaussian channel of transmittance T and excess noise ξ. Then there will be the following relations:

$$\begin{aligned} V_B &= T(V_A + \xi)\,, \\ Z &= \sqrt{T(V_A^2 - 1)}. \end{aligned} \tag{56}$$

The mutual information between Alice and Bob is given by

$$I(A:B) = \frac{\omega}{2}\log\frac{V+\xi}{\xi+1}, \tag{57}$$

where $\omega = 1$, 2 corresponds to Bob's homodyne detection and heterodyne detection, respectively. The Holevo bound is calculated using

$$\chi(B:E) = S(E) - S(E|b) = S(AB) - S(E|b), \tag{58}$$

where the second equation is given because Eve holds a purification of ρ_{AB} and b is Bob's measurement result. Both $S(AB)$ and $S(E|b)$ can be calculated from the corresponding covariance matrix γ_{AB} and $\gamma_{E|b}$ (Grosshans, 2005; Navascués and Acín, 2005). The form of $V(E|b)$ depends on the homodyne detection or heterodyne detection that Bob performs. Notice that to obtain a secret key the two important parameters are the transmittance T and the excess noise ξ, which should be carefully estimated in the parameter estimation step.

The previous security analysis is restricted to collective attacks in the asymptotic limit of infinitely long keys. On the one hand, one needs to generalize the collective attacks to coherent or general attacks, which is a challenging problem in CV-QKD. Fortunately, it turns out that collective attacks are as efficient as coherent attacks, assuming the permutation symmetry of the classical postprocessing (Renner and Cirac, 2009). The phase-space symmetries and the postselection technique (Christandl, König, and Renner, 2009) can also be exploited to perform a reduction from general to collective attacks (Leverrier *et al.*, 2013). Recently, a new type of Gaussian de Finetti reduction was proposed that confirms the belief that proving security against Gaussian collective attacks in CV-QKD is sufficient to obtain security against coherent attacks (Leverrier, 2017).

On the other hand, the security analysis should be extended to the *finite-key case*. The finite-key rate will deviate from the asymptotic limit, which is due to statistical fluctuations in the parameter estimation. Moreover, other deviations arise when we assume Gaussian attacks and consider collective attacks instead of coherent attacks. These issues have been well addressed in the literature (Furrer *et al.*, 2012; Leverrier *et al.*, 2013; Leverrier, 2015). Based on the postselection technique (Christandl, König, and Renner, 2009), the security of GMCS CV-QKD was proven against general attacks in the finite-size regime (Leverrier *et al.*, 2013), but the security proof is not composable. For composable security proof, Furrer *et al.* (2012) provided the first proof for CV-QKD with squeezed states using the entropic uncertainty principle, whereas the analysis is only moderately tolerant to loss. For coherent-state protocols, Leverrier (2015) gave the first composable security proof against only collective attacks and proposed a new type of Gaussian de Finetti reduction that shows potential for finite-key security with small data sizes (Leverrier, 2017). Nevertheless, the current proof techniques for composable security against coherent attacks still require rather large block sizes, e.g., $> 10^{13}$ (Leverrier, 2017). The composable security of CV-QKD against coherent or general attacks in a realistic finite-size regime remains an outstanding open issue for the future study of improved proof techniques.

In addition to the coherent state, the squeezed-state protocol has also been widely studied for CV-QKD. In a squeezed-state protocol (Hillery, 2000; Cerf, Lévy, and Assche, 2001), Alice squeezes the X quadrature of a vacuum state and displaces it by an amount a, which follows a Gaussian distribution of variance V_A. Then Alice adds a random phase of 0 or $\pi/2$ to it, which is equivalent to randomly choosing a direction to squeeze. Finally, Alice randomly displaces the output state along the other direction (not the squeezing direction) following another Gaussian variable of variance V. The two variances V_A and V should satisfy $V_A + V^{-1} = V$ such that Eve cannot distinguish which quadrature is squeezed. Bob randomly measures the X or P quadrature. Alice and Bob perform the postprocessing after a certain round of measurements. The squeezed-state protocol is more similar to the DV-QKD protocols than to the coherent-state protocol. Its security is based on an entropic uncertainty principle (Cerf, Lévy, and Assche, 2001). The composable security of finite-size analyses was also given by Furrer *et al.* (2012) and Furrer (2014), together with experimental verifications (Gehring *et al.*, 2015).

B. Experimental developments

The widely implemented CV-QKD protocol is the GMCS protocol (Grosshans and Grangier, 2002; Grosshans *et al.*, 2003) (see Box VII.A.1) due to the simplicity in preparation, modulation, and detection of its coherent states. An illustration of the implementation is shown in Fig. 19 (Lodewyck *et al.*, 2007). Alice employs a laser diode to generate optical pulses, each of which is split into a signal and a local oscillator (LO) by a fiber-optic coupler. The signal pulses are modulated in amplitude and phase according to a Gaussian distribution and attenuated to the desired modulation variance with a variable attenuator. The LO is time delayed and then combined with the signal at Alice's output. Bob passively demultiplexes the signal and LO using a coupler and then performs the measurement using a shot-noise-limited homodyne detector. Bob can select the quadrature to be measured by adjusting the measurement phase with a phase modulator placed in the LO path. An advanced feature of this

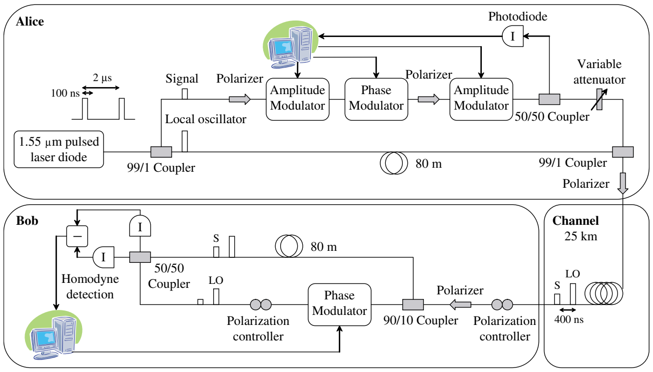

FIG. 19. An illustration of the implementation of GMCS CV-QKD. From Lodewyck *et al.*, 2007.

implementation is that it consists entirely of standard fiber optics and telecommunication components.

Reverse reconciliation was introduced to the GMCS protocol in 2003 (Grosshans *et al.*, 2003), and it allows GMCS to beat the 3-dB loss limit. Moreover, a free-space experiment in the visible light wavelength was also performed there. With telecommunication wavelength, GMCS was performed over a practical distance of optical fibers of 25 and 5 km, respectively, by Lodewyck *et al.* (2007) and Qi, Huang *et al.* (2007). Meanwhile, the heterodyne detection (Lance *et al.*, 2005) and Gaussian postselection (Symul *et al.*, 2007) were also demonstrated. Later, the feasibility of GMCS CV-QKD was extensively tested in field environments (Fossier *et al.*, 2009). The secure distance was substantially extended to 80 km based on the improved efficiency of postprocessing techniques (Jouguet *et al.*, 2013). By controlling the excess noise, the distance was further extended to 100-km standard fiber (Huang, Huang, Lin, and Zeng, 2016). Recently, state-of-the-art CV-QKD implementations were sequentially reported, among them high-rate demonstrations with a secret key rate up to 3.14 Mbits/s in the asymptotic limit over 25-km fiber (T. Wang *et al.*, 2018), a four-node field network (Huang, Huang, Li *et al.*, 2016), a field test over 50-km commercial fiber (Y. Zhang *et al.*, 2019), a long-distance CV-QKD over about 200-km ultra-low-loss fiber (Zhang *et al.*, 2020), a Si photonic chip-based CV-QKD implementation (G. Zhang *et al.*, 2019), etc. Although we focus on the GMCS implementations, we note several other important experiments, such as the squeezed-state protocols (Gehring *et al.*, 2015) and a CV-QKD experiment with entangled states over 50-km fiber (N. Wang *et al.*, 2018). Some recent developments of CV-QKD are shown in Table V.

From a practical point of view, CV-QKD presents a key advantage in that it requires only standard telecommunications technology that is compatible with classical optical communications; i.e., it uses coherent detection techniques instead of the single-photon detection technology required in DV-QKD. Moreover, the LO in CV-QKD can serve as a built-in single-mode filter, which makes it naturally resistant against background noise (Qi *et al.*, 2010). This is particularly useful in practical situations, as in the coexistence of QKD with classical channels via dense wavelength-division multiplexing (DWDM) (Qi *et al.*, 2010; Kumar, Qin, and Alléaume, 2015), the daylight free-space CV quantum communication (Heim *et al.*, 2014; Peuntinger *et al.*, 2014; Vasylyev *et al.*, 2017; Wang, Huang *et al.*, 2019). Nonetheless, CV-QKD systems are in general sensitive to losses, which restricts the secure distance, normally below 100-km fiber (Jouguet *et al.*, 2013). However, in theory CV-QKD may provide higher key rates than DV-QKD at relatively short distances because of its high dimensionality (Jouguet, Elkouss, and Kunz-Jacques, 2014), while the exact rate in terms of bits/s depends on the technology of real implementation. High-rate CV-QKD requires high-speed and real-time implementations of several challenging techniques (T. Wang *et al.*, 2018), such as the use of a low-noise homodyne detector, efficient error correction codes, precise parameter estimation, etc. In addition, the composable security proofs against general attacks still require large block sizes to allow a positive key in the finite-key regime (Leverrier, 2015), which results in a cascade of challenges on the stability of the system. These issues are important subjects for future research.

C. Quantum hacking and countermeasures

Similar to DV-QKD, the implementations of CV-QKD also suffer from side channels. On the source part, the Trojan-horse attacks can probe Alice's modulators in CV-QKD systems (Jain *et al.*, 2014). Similar to DV-QKD, a countermeasure is to put an optical isolator and a monitoring detector at the output of Alice's setup. The imperfections in state preparation may also cause an increase of the excess noise and misestimate of the channel loss (Liu *et al.*, 2017). On the detection part, the wavelength dependence of the beam-splitter can be exploited by Eve to hack CV-QKD based on heterodyne detection (Huang *et al.*, 2013; Ma *et al.*, 2013b). Qin *et al.* demonstrated the detector saturation attack (Qin, Kumar, and Alléaume, 2016) and blinding attack (Qin *et al.*, 2018) against homodyne detectors in CV-QKD by exploiting the nonlinear behavior of coherent detectors. A wavelength filter is effective against the first attack, and a proper monitor at detection may counter the second attack. A more general solution is to perform the real-time shot-noise measurement analyzed by Kunz-Jacques and Jouguet (2015) and Y.-C. Zhang *et al.* (2019).

To completely remove the detection attacks, a CV version of MDI-QKD was proposed by Pirandola *et al.* (2015); see also Li *et al.* (2014) and Ma *et al.* (2014) for a security analysis against restricted attacks. The concept is similar to the MDI-QKD protocol discussed in Sec. VI.B, but here Alice and Bob prepare coherent states with a Gaussian modulation and send them to Charlie. Charlie then mixes them on a balanced beam splitter, measures a different quadrature for both output modes, and publicly announces his measurement results. The security of CV MDI-QKD can be analyzed by considering the entanglement-based version of the protocol (Lupo *et al.*, 2018). A proof-of-principle CV MDI-QKD experiment was demonstrated in free space with advanced detection techniques in 2015 (Pirandola *et al.*, 2015). Nonetheless, a full implementation with practical lengths of optical fibers is still a great challenge that has not been reported on in the literature yet, partly because of the requirement of high-efficiency detection (Xu, Curty, Qi, Quan, and Lo, 2015). Even so, CV MDI-QKD has the potential to provide slightly higher key rates, and it might be interesting for network communication over relatively short distances (Pirandola *et al.*, 2015).

Besides, an additional threat to CV-QKD is the transmission of LO, which can be manipulated by Eve. Attacks made by controlling the transmitted LO were proposed by Ma *et al.* (2013a). Eve can also exploit a subtle link between the local oscillator calibration procedure and the clock generation procedure employed in practical setups (Jouguet, Kunz-Jacques, and Diamanti, 2013). A countermeasure against the LO attacks consists of implementing a rigorous and robust real-time measurement of the shot noise (Kunz-Jacques and Jouguet, 2015; Y.-C. Zhang *et al.*, 2019). A better solution is the locally LO (LLO) CV-QKD scheme (Qi *et al.*, 2015; Soh *et al.*, 2015) (see Fig. 20), which can completely avoid the

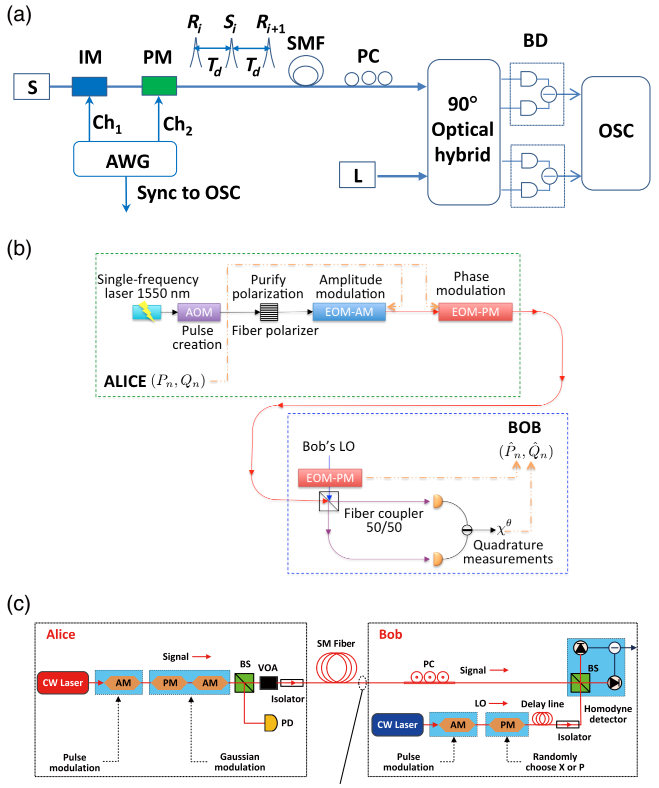

FIG. 20. Initial local LO (LLO) CV-QKD experiments. (a) LLO CV-QKD experiment with the pilot-aided feed-forward data recovery scheme using commercial off-the-shelf devices. From Qi *et al.*, 2015. (b) LLO CV-QKD experiment with self reference. From Soh *et al.*, 2015. (c) A high-speed LLO CV-QKD experiment. From Huang, Huang *et al.*, 2015.

transmission of the LO through the insecure channel. In this scheme, Bob uses a second, independent laser to produce LO pulses locally for the coherent detection. A challenge here is how to effectively establish a reliable phase reference between Alice's and Bob's independent lasers, which require a careful synchronization of the frequencies and phases. This can be achieved by sending the reference or pilot-aided pulse along with the signal pulse from Alice. Bob can use his LO pulse to perform coherent detection for the reference pulse to estimate the relative phase between Alice's and Bob's lasers. A phase correction can thus be established on Alice's and Bob's signal data to generate the secret key. Owing to the enhanced security of LLO CV-QKD, much attention has been given to this scheme. In 2015, three groups independently demonstrated LLO CV-QKD (Huang, Huang *et al.*, 2015; Qi *et al.*, 2015; Soh *et al.*, 2015). These experiments are shown in Fig. 20. Afterward, a LLO CV-QKD experiment with pilot and quantum signals multiplexed in the frequency domain was reported by Kleis, Rueckmann, and Schaeffer (2017), a comprehensive framework to model the performance of LLO CV-QKD was reported by Marie and Alléaume (2017), a pilot-assisted coherent intradyne reception methodology for LLO CV-QKD was proposed and demonstrated by Laudenbach *et al.* (2017) and a high-rate LLO CV-QKD was demonstrated by T. Wang *et al.* (2018).

VIII. OTHER QUANTUM-CRYPTOGRAPHIC PROTOCOLS

A. Device-independent QKD

A QKD protocol is device independent if its security does not rely on trusting the quantum devices used to be truthful. A schematic illustration of device-independent QKD (DI-QKD) is shown in Fig. 21. DI-QKD (Mayers and Yao, 1998; Barrett, Hardy, and Kent, 2005; Acín *et al.*, 2007) [hinted at earlier by Ekert (1991)] relaxes all modeling assumptions on the quantum devices and allows the users to do QKD with uncharacterized devices. DI-QKD performs self-testing of the underlying devices; i.e., the devices cannot pass the test unless they carry out the QKD protocol securely. As a result, as long as certain necessary assumptions are satisfied, one can prove the security of DI-QKD based solely on a Bell nonlocal behavior, typically violation of a Bell inequality, which certifies the presence of quantum correlations in a self-testing manner. Table XVI lists a summary of the necessary assumptions of DI-QKD (Pironio *et al.*, 2009). The security proofs have required the assumption that the devices have no memory between trials or that each party has many strictly isolated devices (Barrett, Hardy, and Kent, 2005; Acín *et al.*, 2007; Pironio *et al.*, 2009; Masanes, Pironio, and Acín, 2011). If the devices have memory or the devices are reused, DI-QKD will suffer from memory attacks (Barrett, Colbeck, and Kent, 2013) and covert channels (Curty and Lo, 2019).

The security proof for DI-QKD is a challenging task because in DI-QKD both the quantum state (generated by the source) and the measurement operators (generated by the detection devices) are untrusted or under Eve's control. Fortunately, recent theoretical efforts have significantly advanced the development of DI-QKD to make it possible in a large quantum system (Reichardt, Unger, and Vazirani, 2013), secure for a large class of protocols by independent measurements (Masanes, Pironio, and Acín, 2011), secure against general attacks (Vazirani and Vidick, 2014; Miller and Shi, 2016), and robust against noise (Arnon-Friedman *et al.*, 2018). In the asymptotic case against collective attacks, the key-rate formula can be expressed as a function of the Bell violation value. For a protocol where Alice and Bob carry out

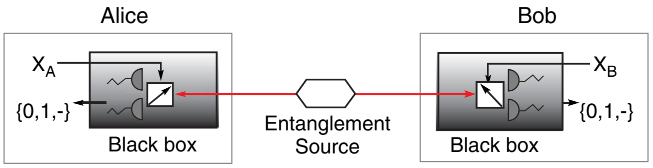

FIG. 21. Schematic diagram of DI-QKD (Mayers and Yao, 1998; Acín *et al.*, 2007). Entangled-photon pairs are distributed to Alice and Bob, who are supposed to perform some measurements. Alice and Bob see their quantum devices as black boxes producing classical outputs as a function of classical inputs X_A and X_B. From the observed statistics and without making any assumptions about the internal working of the devices, they should be able to conclude whether or not they establish a secret key. Alice and Bob assume giving the untrusted quantum devices tests that cannot be passed unless they carry out the QKD protocol securely, which can be checked via violation of a Bell inequality (Pironio *et al.*, 2009).

a Clauser-Horne-Shimony-Holt (CHSH-) type Bell test for self-testing privacy, the key rate can be given by (Pironio *et al.*, 2009)

$$r \geq 1 - h(E) - h\left(\frac{1+\sqrt{(S/2)^2-1}}{2}\right), \qquad (59)$$

where the quantum bit error rate E determines the amount of randomness consumed for error correction, and the violation value S of the CHSH inequality determines the amount of randomness for privacy amplification.

Though DI-QKD is remarkable in theory, unfortunately, it is hard to realize with current technology because it needs almost perfectly efficient single-photon detection (Masanes, Pironio, and Acín, 2011). In experiments, however, the emitted photons may not be detected due to losses in the transmission or the limited detection efficiency of imperfect detectors. In addition, a faithful realization of DI-QKD requires that the Bell inequality is violated under the following two conditions: (i) the measurement settings are not correlated with the devices, and (ii) the devices observe a no-signaling behavior in generating the outcomes. To meet these conditions, a so-called loophole-free Bell test normally needs to be carried out. A key problem in a loophole-free Bell test is the limited detection efficiency, which is referred to as an efficiency loophole (Pearle, 1970). It has been proven that, for the simplest bipartite Bell inequalities with binary inputs and outputs, a detector efficiency of at least $2/3$ is necessary for a faithful Bell inequality violation (Eberhard, 1993). For the purpose of DI-QKD, a much higher efficiency is needed due to the requirement of information reconciliation. To guarantee the no-signaling behavior between devices, i.e., the locality loophole, a spacelike separated measurement setup can be implemented (Aspect, 1975). The requirement of uncorrelated inputs is referred to as the freewill loophole, which cannot be closed completely. Nonetheless, practical quantum random number generators can be used to overcome the problem to some extent.

Recently, researchers demonstrated the Bell inequality that closed the locality loophole and the detection loophole simultaneously in the same experiment (Giustina *et al.*, 2015; Hensen *et al.*, 2015; Shalm *et al.*, 2015; Rosenfeld *et al.*, 2017; Y. Liu *et al.*, 2018). This is a milestone result toward the realization of DI-QKD. In the future, advanced technology might make DI-QKD more practical, and ideas such as qubit amplification (Gisin, Pironio, and Sangouard, 2010) might also prove to be useful to increase the key rate and distance of DI-QKD, though the key rate might be relatively low (Curty and Moroder, 2011; Seshadreesan, Takeoka, and Sasaki, 2016). Recent theoretical works proposed two-way classical communication to enhance noise tolerance (Tan, Lim, and Renner, 2020) and provided detailed analysis toward the realization of DI-QKD (Murta *et al.*, 2019). Overall, we do believe that DI-QKD is an important subject for future research.

B. Some new QKD implementations

In addition to effort directed toward the security of imperfect devices, quite a few new QKD protocols have been proposed and implemented during the past ten years; they are summarized in Table VII.

1. Round-robin DPS QKD

In general, a threshold of the error rate exists for each scheme, above which no secure key can be generated. This threshold puts a restriction on environmental noise. Specifically, in the key-rate formula the bit error can be directly computed from the experimental data, whereas the phase error needs to be estimated or bounded. In the BB84 protocol with strong symmetry, both error rates are approximately the same in the long key length limit. In other protocols, there is normally a relation between the two error rates. In the end, when the bit error rate goes beyond some threshold level, no secure key can be generated. For example, BB84 cannot tolerate error rates beyond 25%, considering a simple intercept-and-resend attack (Bennett and Brassard, 1984). This threshold puts a stringent requirement on the system environment, which makes some practical implementations challenging.

Round-robin differential-phase-shifted (RRDPS) QKD, proposed by Sasaki, Yamamoto, and Koashi (2014), essentially removes this restriction and can, in principle, tolerate more environmental disturbance. In this protocol, Eve's information can be bounded only by a user's certain experiment parameters, other than the error rates. In particular, the phase error rate e_p is determined by the user's own settings rather than the channel performance, which makes the protocol fundamentally interesting and allows it to tolerate more errors.

In the RRDPS QKD protocol, the sender Alice puts a random phase, chosen from $\{0, \pi\}$, on each L pulse, with an average photon number of μ in such an L-pulse signal. Upon receiving the block, the receiver Bob implements single-photon interference with a Mach-Zehnder interferometer (MZI), as shown in Fig. 22(a). Bob can randomly adjust the length difference of the two arms of the MZI. After

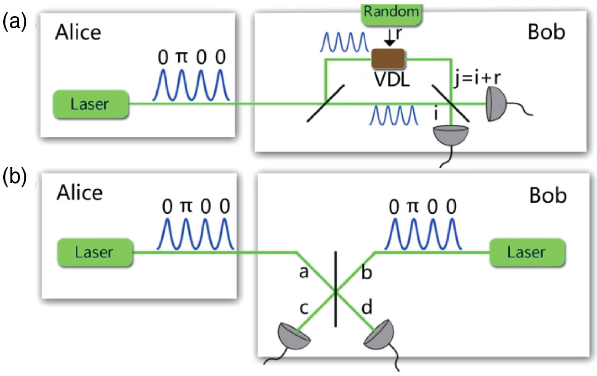

FIG. 22. (a) The original RRDPS scheme (Sasaki, Yamamoto, and Koashi, 2014). VDL stands for variable-delay line. Bob splits the received signals into two paths and applies a variable delay r to one of the paths. A click at ith place will indicate interference between the pulses i and $j = i + r$. (b) The passive RRDPS scheme. Bob uses a local laser to generate an L-pulse reference, which interferes with Alice's L-pulse signal. Bob then records the coincidence clicks. From Guan *et al.*, 2015.

obtaining a detection click, Bob first identifies which two pulses interfere and then announces the corresponding indices i and j to Alice. Alice can derive the relative phase between the two pulses as the raw key, and Bob can record the raw key from the measurement results. The phase error rate depends only on the number of photons in the L-pulse signal and L, not on the bit error rate. By setting a larger L, the phase error tends to 0, and the scheme can tolerate a higher bit error rate.

Triggered by the original protocol, an alternative passive type of RRDPS QKD was proposed by Guan *et al.* (2015). As shown in Fig. 22(b), when Bob receives a block from Alice, he prepares a local L-pulse reference in plain phases; i.e., all phases are encoded at phase 0. This L-pulse reference interferes with the L-pulse signal sent by Alice on a beam splitter. For each block, Bob records the status of his two detectors with time stamps i and j. If Bob's reference is in phase with Alice's signal, i.e., Bob has a phase reference, the whole setup is essentially a large Mach-Zehnder interferometer. Any detection signal at time slot i will tell the phase difference between i and the phase reference. Then the encoding bit value can be figured out by Bob. If the Bob's phase reference is random relative to Alice's signal, the interference is Hong-Ou-Mandel-type interference (Hong, Ou, and Mandel, 1987) instead of a MZI. Bob postselects the block where there are exactly two detections and announces their positions i and j (if $i = j$, the detection result is discarded). The raw key is the relative phase between these two pulses in the L-pulse signal. Alice can derive this phase difference from her record, while Bob can infer the bit value by knowing that the coincidence happens between two different detectors or one detector in two different time slots. The security proofs of the two protocols are beyond the scope of this review; we refer interested reader to Sasaki, Yamamoto, and Koashi (2014) and Guan *et al.* (2015).

The first published experimental result was based on the passive protocol (Guan *et al.*, 2015). Compared to the original protocol, the passive one avoids randomly adjusting the length difference of the MZI. Based on current technology, the main adjust-delay method is to utilize optical switches, which cannot provide both high speed and low insertion loss simultaneously. Meanwhile, it requires remote optical phase locking, which is challenging in real deployment.

The key point for an active RRDPS is to realize the random time delay. Takesue *et al.* (2015) exploited a one-input, four-output optical splitter followed by four silica waveguides based MZI with 0.5-, 1.0-, 1.5-, and 2.0-ns temporal delays. Any two delays constitute a new MZI and the whole system realizes a $L = 1$–5 variable delay. With this delay, Takesue *et al.* achieved a secure key rate through 30-km fiber with an error rate of 18%. Later, S. Wang *et al.* (2015) combined a three-port circulator, a beam splitter, and two 1×8 optical switches followed by two groups of fiber delays. The two optical switches actively chose different delays and achieved an $L = 1$ to 64 bit variable-delay Faraday-Michelson interferometer. Based on the delay, Wang *et al.* distributed a secret key over a distance of 90-km fiber. In addition, Li *et al.* (2016) exploited a different configuration. They put seven MZIs in a series to achieve a 127-value variable delay. Each MZI is constructed of a Pockels cell, a fiber, or a free-space link with specific length and two PBSs. The Pockels cell, controlled by a random number, may change the polarization of the photon and thus provide a delay. Recently, the secure distance was extended to 140 km by increasing the bound on information leakage (Yin *et al.*, 2018).

2. High-dimensional QKD

In addition to qubit-based QKD, the secret keys can also be encoded with a multilevel system, i.e., high-dimensional QKD (HD-QKD). HD-QKD can provide a higher key rate per particle than the qubit system (Bourennane, Karlsson, and Björk, 2001), and it has a higher tolerance of noise (Cerf *et al.*, 2002). A recent review on the subject was given by Xavier and Lima (2020). The first experimental attempts of HD-QKD used higher-order dimensional alphabets with spatial degrees of freedom of photons (Walborn *et al.*, 2006) or energy-time entangled-photon pairs (Ali-Khan, Broadbent, and Howell, 2007). The latter is shown in Fig. 23(a). With this setup, Ali-Khan, Broadbent, and Howell generated a large-alphabet key with over 10 bits of information per photon pair, albeit with large noise. A QKD with a 5% bit error rate is demonstrated with 4 bits of information per photon pair, where the security of the quantum channel is determined by the visibility of the Franson interference fringes.

Z. Zhang *et al.* (2014) reported a complete security proof of time-energy entanglement QKD using dual-basis interferometry. Mower *et al.* (2013) suggested utilizing dispersive optics to replace the Franson interferometer and demonstrated its security against a collective attack. In this scheme, as shown in Fig. 23(b) (Lee *et al.*, 2014), Alice or Bob utilize normal or abnormal group-velocity dispersive element to measure the frequency basis. The absolute group delays of their dispersive elements are matched such that the group-velocity dispersion is nonlocally canceled. Alice and Bob use time basis measurements for generating keys and frequency basis measurements for bounding Eve's maximum accessible information about the time basis measurements. This is based on the fact that the dispersion cancellation happens only with

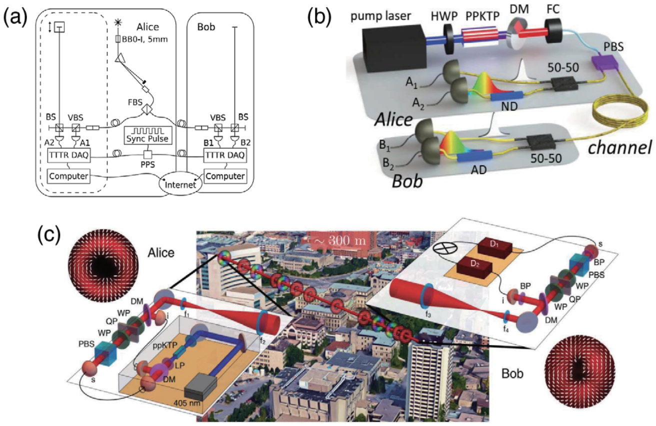

FIG. 23. The experimental setup for HD-QKD. (a) HD-QKD with time-energy entangled-photon pairs. From Ali-Khan, Broadbent, and Howell, 2007. (b) Dispersive-optics time-energy HD-QKD. From Lee *et al.*, 2014. (c) A field test of OAM HD-QKD in Ottawa, Ontario, Canada. From Sit *et al.*, 2017.

entanglement, and any reduced entanglement visibility due to eavesdropping broadens the time correlation measurement.

With the time-energy entangled-photon pairs, Zhong *et al.* (2015) observed a secure key rate of 2.7 Mbits/s after 20-km fiber transmission with a key capacity of 6.9 bits per photon coincidence. Recently, high-rate QKD using time-bin qudits was reported by Islam *et al.* (2017). Time-energy-type HD-QKD has an advantage with a constant clock rate because it can utilize more time slots with a high time resolution single-photon detector. However, the advantage is offset when the clock rate is increased to the bandwidth of the single-photon detector (Zhang *et al.*, 2008). One solution is to utilize a degree of freedom other than time, for example, the optical angular momentum (OAM). The first HD-QKD for OAM was published in 2006 (Gröblacher *et al.*, 2006). Qutrit entangled-photon pairs were utilized to generate quantum key. In an E91-type protocol (Ekert, 1991), the violation of a three-dimensional Bell inequality verifies the security of the generated keys. A key is obtained with a qutrit error rate of approximately 10%. Later, Etcheverry *et al.* (2013) reported an automated prepare-and-measure HD-QKD with 16-dimensional photonic states; Mafu *et al.* (2013) exploited high-dimension OAM up to five dimensions for HD-QKD; Mirhosseini *et al.* (2015) used the OAM of a weak coherent state and the corresponding mutually unbiased basis of the angular position; Sit *et al.* (2017) implemented a field test of OAM HD-QKD in Ottawa, Ontario, Canada, where four-dimensional OAM HD-QKD was implemented and a QBER of 11% was attained with a corresponding secret key rate of 0.65 bits per sifted photon; see Fig. 23(c). Recently, Cozzolino *et al.* (2019) demonstrated OAM HD-QKD over a 1.2-km-long multimode fiber. Different groups utilized spatial-division multiplexing optical fibers such as multicore fibers to perform HD-QKD (Cañas *et al.*, 2017; Ding *et al.*, 2017).

Naively, one might think that a HD-QKD system offers a higher key rate per signal than a qubit-based QKD system. It always seems better to use a HD-QKD system. One has to be extremely careful when making such a comparison because the key rate per signal may not be the best measure when the signal size itself is big. The key rate per second for a certain period of time can have more merit for applications. In fact, a HD-QKD protocol uses, e.g., many time bins or modes for each signal. Now if one were to use the many time bins or modes separately and in parallel with many sets of high-speed single-photon detectors, one would actually get a higher key rate in such a multiplexed QKD system. The private capacity per mode of a simple prepare-and-measure QKD system is limited by fundamental bounds (Takeoka, Guha, and Wilde, 2014; Pirandola *et al.*, 2017). The key rate of HD-QKD is still limited by those fundamental bounds. Nonetheless, HD-QKD may be useful in a practical situation, where the single-photon detector has a long dead time or resetting time and it cannot operate at high speed (Zhong *et al.*, 2015). Overall, the practical advantages of HD-QKD in real-life applications remain to be seen.

3. QKD with wavelength-division multiplexing

Except for the new protocols, reducing the cost of QKD system is another important topic in the field. Wavelength-division multiplexing (WDM) technology, which enables QKD and telecommunications to coexist in a single fiber, is exploited to reduce the cost of the channel.

To protect ultraweak QKD signals, most previous QKD experiments were implemented in dark fiber. This implies dedicated fiber installations for QKD networks, which bear cost penalties in fiber leasing and maintenance, as well as limitations on the network scale. In classical optical communications, WDM technology has been widely exploited to increase the data bandwidth and reduce the requirement of fiber resource. Therefore, it is natural for QKD to coexist with classical optical communication based on WDM technology. The scheme of simultaneously transmitting QKD with conventional data was first introduced by Townsend (1997). A series of QKD experiments integrated with various classical channels have been conducted (Chapuran *et al.*, 2009; Eraerds *et al.*, 2010; Patel *et al.*, 2012, 2014; L.-J. Wang *et al.*, 2015; Dynes *et al.*, 2016). Currently, by using spectral and temporal controls, state-of-the-art developments have been made to realize copropagation of QKD with one 100-Gbits/s DWDM data channel in a 150-km ultra-low-loss fiber at −5 dBm launch power (Fröhlich *et al.*, 2017). By setting the QKD wavelength to 1310 nm and inserting 100 GHz DWDM filters, Wang *et al.* implement QKD together with classical traffic with 11 dBm input power over 80 km fiber spools (L.-J. Wang *et al.*, 2017). A field trial of simultaneous QKD transmission and four 10 Gbits/s encrypted data channels was implemented over 26 km installed fiber at −10 dBm launch power (Choi *et al.*, 2014).

Recently, the coexistence of QKD and the commercial backbone network of 3.6 $\mathrm{Tb}its/s$ classical data over 66-km fiber at 21 dBm launch power was demonstrated by Mao *et al.* (2018). The system provides 3 kbits/s secure key rate with a 2.5% quantum bit error rate. Note that in current backbone networks, the data traffic is around a Tbit/s and the launch power is around 20 dBm. In that sense, Mao *et al.* (2018) demonstrated the possible coexistence of QKD with a backbone network.

4. Chip-based QKD

Integrating a QKD system has attracted more attention due to an advantage in compact size, low energy consumption, and the potential for low cost (Orieux and Diamanti, 2016). QKD, including optics and electronics, is a complicated system. Thus, an integrated QKD system research should include the integration of both optics and electronics. Fortunately, integrated circuits (ICs) are already commercialized and integrated optics are also well developed in industry. Table VI summarizes a list of chip-based QKD experiments.

In 2005, a commercial unbalanced Mach-Zahnder interferometer made of planar lightwave circuits (PLCs) based on silica-on-silicon technology was exploited for the first time in a QKD system (Takesue *et al.*, 2005) to replace the fiber-based interferometer. Compared to its fiber counterpart, the PLC interferometer is more stable and can maintain its phase for several hours without any feedback (Takesue *et al.*, 2007; Nambu, Yoshino, and Tomita, 2008). Meanwhile, ICs have been employed in research on a compact and low-cost QKD system (Duligall *et al.*, 2006). As is shown in Fig. 24(a), Alice

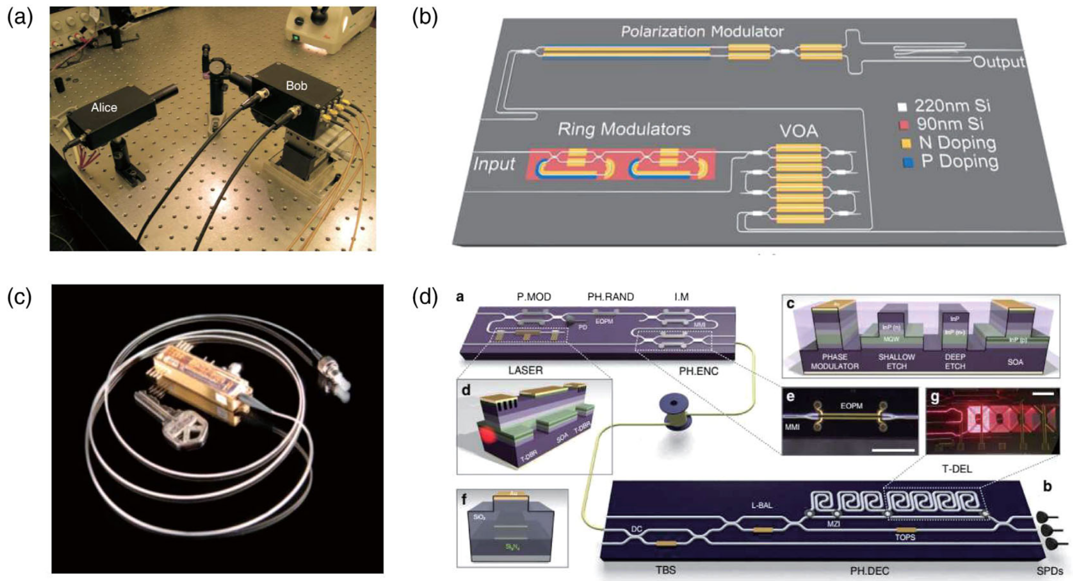

FIG. 24. Experimental layouts. (a) Low-cost and compact QKD setup. From Duligall *et al.*, 2006. (b) A silicon photonic QKD emitter. From C. Ma *et al.*, 2016. (c) Compact QKD transmitter QCard. From Hughes *et al.*, 2013. (d) InP-based QKD sender and SiO_xN_y receiver chip. From Sibson, Kennard *et al.*, 2017.

module uses off-the-shelf IC components in a driver circuit to control four AlInGaP light-emitting diodes to emit four polarized BB84 states. The channel is a several-meter free-space link, which could have an application in a future quantum-based automated teller machine or even a smart phone according to Pizzi, Rossetti, and D'Arenzo (2012). Along these lines of research, Vest *et al.* (2015) demonstrated an integrated QKD sender where an array of four vertical cavity surface-emitting lasers emit synchronized picosecond optical pulses, which are coupled to micropolarizers generating polarization qubits. The final size of the QKD device can be as small as $25 \times 2 \times 1\ \mathrm{mm}^3$, which makes the system a strong candidate for short-distance free-space QKD applications.

On the metropolitan fiber network side, many individual users in the network trust a central relay station. This is a so-called network-centric structure (Hughes *et al.*, 2013) or access network (Fröhlich *et al.*, 2013). In such a structure, many users are all senders and share only one central relay receiver. In that sense, the receiving station can have more space, and an expensive and bulky detection system can be used. Therefore, the community concentrates more integration efforts on the sending side. Hughes *et al.* (2013) provided a QCard in their pioneering paper, as is shown in Fig. 24(b). The QCard has a similar size as an electro-optic modulator or a normal key. It incorporates a distributed feedback laser and modulator. The laser is attenuated into single-photon level and modulated into a BB84 polarization state with a decoy state. The repetition frequency is 10 MHz at the wavelength of 1550 nm, the telecommunications band.

Recently, the size of the QKD sender was reduced dramatically. In 2014, P. Zhang *et al.* (2014) put forward an on-chip $\mathrm{LiNbO_3}$ polarization rotator and demonstrated the reference-frame-independent QKD protocol to overcome unstable fiber birefringence. In 2015, the same group from the University of Bristol implemented an integration of QKD based on an indium phosphide transmitter chip and a silicon oxynitride receiver chip (Sibson *et al.*, 2017). This chip is shown in Fig. 24(d). Sibson *et al.* exploited the chips in three different QKD protocols, namely, BB84, coherent-one-way, and differential-phase-shift QKD.

Later, researchers from the University of Toronto (C. Ma *et al.*, 2016) and the University of Bristol (Sibson, Kennard *et al.*, 2017) employed silicon photonics to build QKD sender systems. As shown in Fig. 24(c), C. Ma *et al.* (2016) fabricated the QKD sender chip with a standard Si photonic foundry process and integrated two ring modulators, a variable optical attenuator, and a polarization modulator in a $1.3 \times 3\ \mathrm{mm}^2$ die area. Meanwhile, Sibson, Kennard *et al.* (2017) demonstrated coherent one-way QKD, polarization-encoded BB84, and time-bin-encoded BB84 based on Si photonic devices. Sibson, Kennard *et al.* achieved estimated asymptotic secret key rates of up to 916 kbits/s and QBER as low as 1.01% over 20 km of fiber. The clock rate of the latter experiment is much higher than that of the former one. However, C. Ma *et al.* integrated more components on the chip, i.e., the whole QKD emitter.

Recently other research groups demonstrated high-speed Si photonic chips for high-dimensional QKD over multimode fiber (Ding *et al.*, 2017), transceiver circuit (Cai *et al.*, 2017), and metropolitan QKD (Bunandar *et al.*, 2018). Moreover, CV-QKD is naturally suitable for photonic chip integration, as its implementation is compatible with current telecommunication technologies; see Sec. VII. In particular, CV-QKD essentially uses the same devices as classical coherent communication, and only a homodyne detector is required rather than a dedicated single-photon detector. Indeed, a recent experiment demonstrates Si photonic chips for CV-QKD, which integrates all of the optical components except the laser source (G. Zhang *et al.*, 2019). Furthermore, based on the directly phase modulated light source (Yuan *et al.*, 2016;

Roberts *et al.*, 2018), a modulator-free QKD transmitter chip was demonstrated by (Paraïso *et al.* (2019). This approach has advantage in that it does not require conventional phase modulators and it is versatile enough to accommodate several QKD protocols, including BB84, COW, and DPS, using the same optics.

C. Other quantum-cryptographic protocols

At this time, QKD is the most developed and mature subfield of quantum cryptography. Meanwhile, quantum cryptography has many other protocols (Broadbent and Schaffner, 2016) that have also achieved quite remarkable progress. A list of recent developments of other quantum-cryptographic protocols is shown in Table VIII. We will review a few examples.

1. Quantum bit commitment

Bit commitment is another important and fundamental cryptographic task that guarantees a secure commitment between two mutually mistrusted parties. Alice first commits her to a particular bit value b. After a period of time, Alice reveals the bit value to Bob. A successful bit commitment requires that Bob not learn b before Alice reveals it, a circumstance called the concealing criterion. Meanwhile, Alice should not change b once she has made the commitment. This is called the binding criterion. Bit commitment is a building block for many cryptographic primitives, including coin tossing (Brassard and Crépeau, 1991), zero-knowledge proofs (Goldreich, Micali, and Wigderson, 1986; Goldwasser, Micali, and Rackoff, 1989), oblivious transfer (Bennett, Brassard *et al.*, 1992; Unruh, 2010), and secure two-party computation (Kilian, 1988).

In conventional cryptography, bit commitment is based on computational complexity assumptions similar to public-key exchange protocols and might be vulnerable to quantum attacks. Unfortunately, it has been proven that information-theoretically secure bit commitments are impossible even if Alice and Bob are allowed to use quantum resources in the standard quantum circuit model by Mayers (1996, 1997) and Lo and Chau (1997). Subsequently, such a no-go theorem was further extended to a case with superselection rules (Kitaev, Mayers, and Preskill, 2004); for a reexamination of this result, see, e.g., D'Ariano *et al.* (2007). Furthermore, information-theoretic security of oblivious transfer and two-party secure computations were also proven to be impossible by Lo (1997).

If we take into account the signaling constraints implied by the Minkowski causality in a relativistic context, it has been shown that there are bit commitment protocols offering unconditional security (Kent, 2012; Kaniewski *et al.*, 2013). On the experimental side, two groups implemented the secure relativistic quantum bit commitment simultaneously in 2013. One followed the original protocol and utilized the decoy-state method in the free-space channel (Liu *et al.*, 2014), and the other exploited a revised protocol with a plug-and-play system in a fiber link (Lunghi *et al.*, 2013). Both experiments were secure against any quantum or classical attack. The commitment time is defined as the maximal time during which the commitment can be held. The commitment time in these two experiments, however, is limited to 21 ms if all attendees are located on Earth, considering the relativistic constrains. Later, new protocols with weaker security but longer commitment time were proposed by Chakraborty, Chailloux, and Leverrier (2015) and Lunghi *et al.* (2015). A 24-h committed experiment (Verbanis *et al.*, 2016) was presented that is secure only against classical attacks. Alternatively, a secure quantum bit commitment can be achieved with additional physical assumptions such as the attacker's quantum memory being noisy (Ng *et al.*, 2012).

2. Quantum digital signature

As opposed to the previous two-party protocols, the digital signature has one sender and multiple recipients, requiring the messages not to be forged or tampered with. Classical digital signature mainly exploits the Rivest-Shamir-Adleman protocol (Rivest, Shamir, and Adleman, 1978), the security of which is based on the mathematical complexity of the integer factorization problem. Based on quantum physics, a quantum digital signature (QDS) protocol established by Gottesman and Chuang (2001) could provide information-theoretical security (Guest, 2001). Although novel, this protocol needs nondestructive state comparison, longtime quantum memory, and a secure quantum channel for real application. QDS has attracted a great deal of interest in both theory (Andersson, Curty, and Jex, 2006; Dunjko, Wallden, and Andersson, 2014; Wallden *et al.*, 2015) and experiment (Clarke *et al.*, 2012; Collins *et al.*, 2014; Donaldson *et al.*, 2016). All three requirements were fixed sequentially (Clarke *et al.*, 2012; Collins *et al.*, 2014; Donaldson *et al.*, 2016). Later, a more than 100-km QDS experiment was demonstrated based on a decoyed BB84 system (Yin *et al.*, 2017a) and DPS QKD (Collins *et al.*, 2016), both of which are also secure against a PNS attack. Recently MDI QDSs were implemented in both the lab (Roberts *et al.*, 2017) and field (Yin *et al.*, 2017b).

3. Other protocols

QKD has assumed that the eavesdropper has unlimited power as long as it does not violate quantum physics. A protocol is said to be information-theoretically secure if it allows an adversary (e.g., an eavesdropper) to have unlimited quantum computing power as long as it does not violate quantum mechanics. As noted in Sec. VIII.C.1, information-theoretic security is not possible for quantum bit commitment, quantum oblivious transfer, or two-party secure quantum computation. Naturally, restriction on an adversary's power can expand the territory of quantum cryptography. Wehner, Schaffner, and Terhal (2008) proposed one realistic assumption, that quantum storage of qubits is noisy, and demonstrated that an *oblivious transfer* protocol is unconditionally secure for any amount of quantum-storage noise (Damgård *et al.*, 2008; Konig, Wehner, and Wullschleger, 2012). Similar to bit commitment, the oblivious transfer protocol is another primitive cryptograph protocol between two entrusted parties. The demonstration of the protocol was performed based on a modified entangled QKD system (Erven *et al.*, 2014). The experiment exchanged a 1366-bit random oblivious transfer string in 3 min and include a full security analysis under the noisy-storage model, accounting for all experimental error rates and finite-size effects.

Similar to bit commitment and oblivious transfer, a quantum protocol for *coin flipping* (Blum, 1981) can be unconditionally secure when considering relativistic constraints. This also means that without relativistic designs no bias coin flipping could be unconditionally secure (Lo and Chau, 1998). Nevertheless, a quantum protocol can limit the cheating probability strictly lower than $1/\sqrt{2}$ (Kitaev, 1999; Aharonov *et al.*, 2000). The first experimental demonstration was provided with OAM qutrit entangled-photon pairs, and it shows the quantum advantage of coin flipping for the first time (Molina-Terriza *et al.*, 2005). As a proof-of-principle demonstration, this experiment does not consider channel loss. Theoretical and experimental efforts have been attempted in this direction (Nguyen *et al.*, 2008; Berlín *et al.*, 2011; Pappa *et al.*, 2014). For instance, an implementation of the loss-tolerant protocol using an entangled-photon source was provided by Berlín *et al.* (2011). The secure distance was extended to 15 km with a modified plug-and-play system (Pappa *et al.*, 2014).

Quantum *data locking* (DiVincenzo *et al.*, 2004) allows one to lock information in quantum states with an exponentially shorter key, presenting an efficient solution to many resource-limited secure applications. However, the original quantum data-locking scheme may suffer from significant qubit loss. Fawzi, Hayden, and Sen (2013) developed a loss-tolerant quantum data-locking scheme in which the possible information leakage could be made arbitrarily small in a lossy environment, while the unlocked information was significantly larger than the key size. This feature also makes the protocol attractive in secure communication (Lloyd, 2013; Lupo, Wilde, and Lloyd, 2014). Two groups have implemented loss-tolerant protocols (Liu *et al.*, 2016; Lum *et al.*, 2016).

Quantum *secret sharing* was proposed to share a secret quantum state among multiple parties (Cleve, Gottesman, and Lo, 1999) or to use quantum states to share classical secrets (Cleve, Gottesman, and Lo, 1999; Hillery, Bužek, and Berthiaume, 1999). Moreover, secure multiparty computing has been extended to quantum computation with quantum inputs and circuits (Crépeau, Gottesman, and Smith, 2002).

In *distributed quantum computing*, quantum-cryptographic protocols are still inevitable. Quantum computing is currently attracting tremendous interest from both academia and industry (Mohseni *et al.*, 2017). However, because of quantum computation's implementation complexity and cost, its future path strongly believed to include the delegation of computational tasks to powerful quantum servers in the cloud (Fitzsimons, 2017). Universal blind quantum computing (UBQC) (Broadbent, Fitzsimons, and Kashefi, 2009) is an effective method for the common user, who has limited or no quantum computational power, to delegate computation to an untrusted quantum server without leaking any information about the user's input and computational task. The security or blindness of the UBQC protocol is unconditional; i.e., the server cannot learn anything about the user's computation except its size. A proof of concept demonstration was reported by Barz *et al.* (2012) Recently, a UBQC protocol with completely classical clients was proposed (Reichardt, Unger, and Vazirani, 2013) and demonstrated in experiment (Huang *et al.*, 2017). UBQC with weak coherent states was proposed by Dunjko, Kashefi, and Leverrier (2012), and adding the ingredient of decoy states an efficient experimental demonstration with weak coherent states was made by Jiang *et al.* (2019). Because of the developments in the field of quantum computing, we expect that BQC will play an important role in the future infrastructure of delegated quantum computation (Fitzsimons, 2017).

IX. CONCLUDING REMARKS

In this review, we have discussed the security aspects of practical QKD. These range from the security proofs of practical QKD (Sec. II) to the implementation (Sec. III) to the practical vulnerabilities (Sec. IV) to the solutions of advanced QKD protocols (Secs. V, VI, and VII) to the advances of other quantum-cryptographic protocols (Sec. VIII.C).

Historically, QKD has been a concrete playground for concepts in quantum mechanics. The study of QKD often leads to unexpected insights in other areas of quantum information. For instance, the concept of quantum teleportation was apparently invented during a search for a security proof of QKD (Bennett *et al.*, 1993). We expect that in the future the study of QKD will continue to lead to many new insights in other subfields of quantum information.

Meanwhile, as a new technology stemming from the counterintuitive theory of quantum physics, QKD might not be easily understood or recognized by a general audience. To appeal to broad interests, in the Appendix we summarize a few frequently asked questions and other concerns about practical QKD, together with our views on how they can be overcome. Finally, we discuss the perspectives on the past, the present, and the future on the development of QKD.

Overall, during the past three decades, the theory and practice of QKD have developed extensively. These developments can be divided into several stages, which can be summarized as follows, with a focus on DV-QKD.

(1) *Stage 1*.—After its invention by Bennett and Brassard (1984) and Ekert (1991), QKD was first demonstrated in the early 1990s (Bennett, Bessette *et al.*, 1992), spawning a series of theories and experiments (Townsend, Rarity, and Tapster, 1993; Townsend, 1994; Franson and Jacobs, 1995; Muller, Zbinden, and Gisin, 1996) seeking to prove the possibility of QKD.

(2) *Stage 2*.—The implementation of QKD was extended from laboratory to outdoor environments, and various technical difficulties were studied (Townsend, 1997; Buttler *et al.*, 1998; Hughes, Morgan, and Peterson, 2000; Ribordy *et al.*, 2000; Gobby, Yuan, and Shields, 2004). See Gisin *et al.* (2002) for a review of developments in the early experiments. Meanwhile, on the theory side the security proof of QKD was a major challenge until a few papers appeared and solved the problem (Lo and Chau, 1999; Biham *et al.*, 2000; Shor and Preskill, 2000; Mayers, 2001). These results put the security of QKD on a solid foundation.

(3) *Stage 3*.—With the security proofs for QKD under imperfect devices (Hwang, 2003; Gottesman *et al.*, 2004; Lo, Ma, and Chen, 2005; Wang, 2005), the feasibility of QKD was demonstrated from short range to long range, up to the scale of 100-km standard fiber (Zhao *et al.*, 2006b; Peng *et al.*, 2007; Rosenberg *et al.*, 2007) and free space (Schmitt-Manderbach *et al.*, 2007).

(4) *Stage 4*.—QKD was extensively deployed from point-to-point to small-scale metropolitan networks in the field (Elliott *et al.*, 2005; Chen *et al.*, 2009; Peev *et al.*, 2009; Sasaki *et al.*, 2011). Meanwhile, the practical security loopholes, particularly those for detection devices, were identified (Lydersen *et al.*, 2010) and then removed by the advanced MDI-QKD protocol (Lo, Curty, and Qi, 2012); see also Braunstein and Pirandola (2012).

(5) *Stage 5*.—The feasibility of QKD was extended to long distances and high rates, as in a scale of 400 km (Yin *et al.*, 2016; Boaron *et al.*, 2018) over ultra-low-loss fiber and 1200 km over free space (Liao *et al.*, 2017a), and a secret key rate of over 10 Mbits/s with a gigahertz QKD system (Yuan *et al.*, 2018).

(6) *Stage 6*.—QKD was implemented from small scale to large scale and covers a wide area (Y.-A. Chen *et al.*, 2020). See Fig. 2 for an example of the QKD network that has more than 700 QKD links, and covers a more than 2000-km area. New TF-QKD protocols (Lucamarini *et al.*, 2018) were proposed to enable secure QKD to work over even longer distances (J.-P. Chen *et al.*, 2020; Fang *et al.*, 2019).

In the future, working toward the ultimate goal of a global QKD network, we expect that more QKD networks will be built in different countries. Alongside physicists, the communities of computer science, engineering, optics, mathematics, etc., may work together to realize this goal. We do believe that a revolutionized global QKD network for secure communication stemming from quantum physics will be deployed and find widespread application in the near future. This review concludes with a discussion of a few directions for future research.

(1) *Quantum repeaters*.—Quantum repeaters can achieve an effective restoration of quantum information without resorting to a direct measurement of the quantum state (Briegel *et al.*, 1998; Duan *et al.*, 2001), enabling the realization of a global quantum network in existing optical networks. The quantum repeater has attracted intense research effort in recent years (Kimble, 2008; Sangouard *et al.*, 2011; Pan *et al.*, 2012; Wehner, Elkouss, and Hanson, 2018). A recent experiment demonstrated entanglement of two atomic ensemble quantum memories via 50 km fiber spool and 20 km deployed fiber (Yu *et al.*, 2020). Nonetheless, the limited performance of quantum memory will still be a major obstacle in realizing practical quantum repeaters without a future experimental breakthrough (Sangouard *et al.*, 2011; Yang *et al.*, 2016). New recent approaches manage to reduce the need for quantum memory by using all-photonic quantum repeaters (Azuma, Tamaki, and Lo, 2015; Hasegawa *et al.*, 2019; Li *et al.*, 2019), but they require the resources of large-scale cluster states. Overall, we believe that the quantum repeater is an important subject for future research. The first goal is to develop a practical quantum repeater that can beat the fundamental limits of direct quantum communication (Takeoka, Guha, and Wilde, 2014; Pirandola *et al.*, 2017).

(2) *Standardization*.—To facilitate widespread applications, commercial standards for QKD should be established. Important progress has been made in this direction, including the efforts of ETSI, ISO, China Communications Standards Association, and ITU in several countries. One important direction is to include practical security in the standardization process by defining the best practices to operate QKD systems and standardizing those countermeasures to guarantee the security of a QKD setup. We encourage future research to establish commercial standards for QKD.

(3) *Battle-testing security*.—We provided a review on the practical vulnerabilities in Sec. IV, together with solutions for advanced countermeasures and QKD protocols. However, the practical security issue has not been perfectly solved. For instance, as discussed in Sec. VI.B, a security assumption in MDI-QKD is that the source should be trusted without loopholes. It is important to verify this assumption in practice. Hence, research analyzing the practical security of QKD setup should continue. This includes the developments of practically secure QKD systems building on the experience gained from the research on practical vulnerabilities and advanced countermeasures. It is highly important to battle test existing QKD implementations, quantify and validate the security claims of real-world QKD systems, and design real-life QKD systems with testable security assumptions.

(4) *Small-size, low-cost, long-distance system*.—Recent developments of the integrated QKD system were reviewed in Sec. VIII.B.4. These developments should continue to further reduce the costs and sizes of QKD, and to realize robust fully integrated chip-based QKD systems. One important direction is on developing a star-type quantum access network (Fröhlich *et al.*, 2013; Hughes *et al.*, 2013) in which expensive devices such as single-photon detectors can be placed in the central relay and many users can share this relay. Each user requires only a low-cost transmitter such as a compact QCard (Hughes *et al.*, 2013) or a simple Si chip (C. Ma *et al.*, 2016; Sibson *et al.*, 2017). Together with MDI-QKD, the central relay can be untrusted. Wei *et al.* (2019) already implemented the first chip-based MDI-QKD at high secret key rates. This is particularly valuable for star-type metropolitan QKD networks. Moreover, by using the new type of twin-field QKD (Lucamarini *et al.*, 2018), the distance can be further extended for intercity QKD. Therefore, we expect that MDI-type QKD networks will play an important role in future global quantum networks.

(5) *QKD network with untrusted relays*.—The previously deployed networks were based on trusted relays

(Elliott *et al.*, 2005; Chen *et al.*, 2009; Peev *et al.*, 2009; Sasaki *et al.*, 2011; Y.-A. Chen *et al.*, 2020), which may raise concerns about the security properties of the relays. To eliminate these concerns, it is important to develop QKD networks with untrusted relays. In fact, MDI-QKD is naturally suited to a star-type metropolitan network with an untrusted relay. Y.-L. Tang *et al.* (2016) already put forward the first implementation of a MDI-QKD network. We expect that metropolitan MDI-QKD networks will be built soon. Besides, the TF-QKD can also be adopted to extend transmission distance with an untrusted relay. Moreover, in entanglement-based QKD, the relay can be fully untrusted. A possible direction is to develop an entanglement-based QKD network, e.g., one based on a satellite (Yin *et al.*, 2019). For ultra-long-distance QKD in fiber, it needs quantum repeaters (Sangouard *et al.*, 2011) to realize QKD networks with untrusted relays. We expect that with technical improvements quantum-repeater-assisted QKD networks may be achieved in the near future.

(6) *Satellite-based QKD*.—The reported satellite-based QKD was based on a low-Earth-orbit satellite of Micius (Liao *et al.*, 2017a, 2018). To increase the coverage time and area for a more efficient satellite-based QKD network, one can launch higher-orbit quantum satellites and implement QKD in daytime. Progress has been made in this direction (Hughes *et al.*, 2002; Liao *et al.*, 2017b). The ultimate goal is to realize a satellite-constellation-based global quantum network.

ACKNOWLEDGMENTS

We are thankful for the enlightening discussions with and helpful comments from reviewers and numerous colleagues, including K. Azuma, D. Bacco, C. H. Bennett, Y.-A. Chen, A. Huang, D. Huang, Y. Liu, M. Lucamarini, S. Pirandola, B. Qi, K. Tamaki, K. Wei, G. B. Xavier, Z. Yuan, P. Zeng, and H. Zhou. F. X., X. M., Q. Z., and J.-W. P. were supported by the National Key Research and Development (R&D) Plan of China, the National Natural Science Foundation of China, the Anhui Initiative in Quantum Information Technologies, and the Chinese Academy of Sciences. H.-K. L. was supported by NSERC, the U.S. Office of Naval Research, the CFI, the ORF, Mitacs Accelerate, the Royal Bank of Canada (RBC), and Huawei Canada.

APPENDIX: GENERAL QUESTIONS ON QKD

We summarize a few frequently asked concerns on QKD and share our views on how they can be overcome.

(1) *Concern 1*.—Since RSA is secure under current computational power, we do not need QKD now.

Our view.—Some important data such as government secrets and health data need to be kept secret for decades, i.e., long-term security. RSA cannot guarantee long-term security because one can record the encrypted information and later decrypt it when the quantum computer comes up or a new advanced algorithm is discovered. In contrast, QKD can provide everlasting security that is independent of any future hardware advances. Hence, QKD is required today for the transmission of top-secret data.

(2) *Concern 2*.—QKD versus postquantum cryptography.

Our view.—QKD and postquantum cryptography are two parallel research directions. They go hand in hand. It is not an either-or situation. Postquantum cryptography has the advantage of being compatible with the existing cryptographic infrastructure, but it has the drawback that its security cannot be proven or it is secure only against known quantum attacks. In contrast, QKD has the advantage of proven security based on the laws of quantum physics, but it is a symmetric-key algorithm that cannot replicate all of the functionalities of public-key cryptography. In the future, we believe that QKD is likely to be combined with postquantum cryptography to jointly form the infrastructure of a quantum-safe encryption scheme.

(3) *Concern 3*.—QKD does not address large parts of the security problem.

Our view—The secure keys generated from QKD have widespread applications, such as encryption and authentication. Note that in QKD authentication is required for only a short period; once it is done, QKD can be employed for encryption over a rather long period.[21] Moreover, with the development of a high key-generation rate, QKD is also suitable for certain future challenges, such as securing the Internet of things, big data, or cloud applications. Furthermore, as mentioned in Sec. VIII.C.2, quantum digital signature schemes with information-theoretical security exist.

(4) *Concern 4*—Distance limitation.

Our view—In fiber, even without a quantum repeater, the feasibility of QKD was proved in experiments over long ranges of 400–500 km (Yin *et al.*, 2016; Boaron *et al.*, 2018; J.-P. Chen *et al.*, 2020; Fang *et al.*, 2019). Using trusted relays, the distance has been extended to 2000-km fiber (Y.-A. Chen *et al.*, 2020). Using quantum satellites, QKD has been demonstrated up to 7600 km (Liao *et al.*, 2018). Moreover, with the help of quantum repeaters (Briegel *et al.*, 1998; Duan *et al.*, 2001), QKD is feasible over arbitrarily long distances even with untrusted relay nodes. Important progress has been made in the development of quantum repeaters (Pan *et al.*, 2012; Munro *et al.*, 2015).

(5) *Concern 5*.—Cost limitation.

Our view.—Recent developments in integrated QKD, such as compact transmitter (Hughes *et al.*, 2013) and Si photonic chip-based QKD systems (C. Ma *et al.*, 2016; Sibson *et al.*, 2017; Wei *et al.*,

[21] As an example, one can even use a public-key-based authentication scheme in the initial authentication of a QKD session. Provided that the public-key-based authentication scheme is secure for a short time in the initial authentication, the generated QKD key will be secure forever. Therefore, postquantum cryptography and QKD may go hand in hand.

2019), have already demonstrated the possibility of low-cost hardware for QKD. Hence, QKD is likely to be cost effective. See Sec. VIII.B.4 for details.

(6) *Concern 6*.—Point-to-point limitation.

Our view.—Small-scale metropolitan QKD networks were intensively deployed in the field by several countries (Elliott *et al.*, 2005; Chen *et al.*, 2009; Peev *et al.*, 2009; Sasaki *et al.*, 2011). A large-scale network covering a wide area was established recently (Y.-A. Chen *et al.*, 2020). These networks already enable secure QKD when used with multiple users instead of point

to point. Furthermore, the recent discoveries of MDI-QKD protocols (Lo, Curty, and Qi, 2012) and TF-QKD protocols (Lucamarini *et al.*, 2018) work well in a star-type network setting (Xu, Curty, Qi, Quan, and Lo, 2015) by sharing a single detection system between multiple users. A prototype of the MDI-QKD network was already implemented in 2016 (Y.-L. Tang *et al.*, 2016). Therefore, these QKD networks and advanced QKD protocols enable QKD for network settings beyond point to point.

(7) *Concern 7*.—Trusted-relay limitation.

Our view.—The discovery of MDI-QKD protocols (Lo, Curty, and Qi, 2012) and TF-QKD protocols (Lucamarini *et al.*, 2018) enable QKD with untrusted relays. Moreover, entanglement-based QKD works well with untrusted relays, and it has been demonstrated between two ground stations separated by a distance of more than 1120 km (Yin *et al.*, 2019). Furthermore, quantum repeaters (Briegel *et al.*, 1998; Duan *et al.*, 2001) enable secure QKD over arbitrarily long distances even with untrusted relay nodes. Hence, a trusted node is not a true limitation in QKD.

(8) *Concern 8*.—Hardware patches are expensive.

Our view.—MDI-QKD already enables secure QKD with untrusted measurement devices, in which expensive measurement devices do not need to be recalled or replaced once they are installed. Moreover, chip-based QKD makes patches for the hardware at a low cost and in a simple manner. We believe that a star type of MDI-QKD network, together with a chip-based transmitter, is promising for realizing a low-cost and practical QKD for applications.

(9) *Concern 9*.—Security loopholes in practical QKD.

Our view.—Researchers in the field of QKD have extensively understood and managed security loopholes. All quantum attacks reported in the literature were reviewed in Sec. IV. Those crucial loopholes have been eliminated by designing advanced countermeasures (Secs. V, VI, and VII). In particular, MDI-QKD has removed the weakest security link, i.e., the detection, in a standard QKD system (Lo, Curty, and Qi, 2012). Secret sharing ideas have been proposed to foil covert channels and malicious classical post-processing units (Curty and Lo, 2019). Advanced technology in the future might make DI-QKD feasible (Hensen *et al.*, 2015). Therefore, the gap between theory and practice of QKD has been reduced significantly, and a number of loopholes have been completely removed. These achievements have made QKD a robust solution for secure communication.

(10) *Concern 10*.—Denial of service (DoS) attack.

Our view.—One solution for a DoS attack is to use alternative channel links by designing suitable network architectures. For instance, a circle type of QKD network was implemented in the Beijing metropolitan network; see Fig. 2. Moreover, the Tokyo (Sasaki *et al.*, 2011) and Secure Communication based on Quantum Cryptography (known as SECOQC) (Peev *et al.*, 2009) QKD networks have already demonstrated robustness against DoS attacks. Another solution is to conduct the secure communication off-line. One can load the secret keys generated from QKD to Universal Serial Bus or mobile phones. The secure communication via a mobile phone will be immune to DoS attack. This method has already been used commercially, e.g., for the QUKey.[22]

[22] See http://www.quantum-info.com/English/product/2017/1007/394.html.

REFERENCES

Abruzzo, S., H. Kampermann, and D. Bruß, 2014, Phys. Rev. A **89**, 012301.

Acín, A., N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, 2007, Phys. Rev. Lett. **98**, 230501.

Adachi, Y., T. Yamamoto, M. Koashi, and N. Imoto, 2007, Phys. Rev. Lett. **99**, 180503.

Aharonov, D., A. Ta-Shma, U. V. Vazirani, and A. C. Yao, 2000, in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing (STOC '00), Portland, OR* (ACM, New York), pp. 705–714.

Ali-Khan, I., C. J. Broadbent, and J. C. Howell, 2007, Phys. Rev. Lett. **98**, 060503.

Andersson, E., M. Curty, and I. Jex, 2006, Phys. Rev. A **74**, 022304.

Arnon-Friedman, R., F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, 2018, Nat. Commun. **9**, 459.

Arute, F., *et al.*, 2019, Nature (London) **574**, 505.

Aspect, A., 1975, Phys. Lett. **54A**, 117.

Azuma, K., K. Tamaki, and H.-K. Lo, 2015, Nat. Commun. **6**, 6787.

Azuma, K., K. Tamaki, and W. J. Munro, 2015, Nat. Commun. **6**, 10171.

Barrett, J., R. Colbeck, and A. Kent, 2013, Phys. Rev. Lett. **110**, 010503.

Barrett, J., L. Hardy, and A. Kent, 2005, Phys. Rev. Lett. **95**, 010503.

Barz, S., E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, 2012, Science **335**, 303.

Beaudry, N. J., T. Moroder, and N. Lütkenhaus, 2008, Phys. Rev. Lett. **101**, 093601.

Bennett, C. H., 1992, Phys. Rev. Lett. **68**, 3121.

Bennett, C. H., G. Brassard, C. Crépeau, and U. Maurer, 1995, IEEE Trans. Inf. Theory **41**, 1915.

Bennett, C. H., F. Bessette, G. Brassard, L. Salvail, and J. Smolin, 1992, J. Cryptol. **5**, 3.

Bennett, C. H., and G. Brassard, 1984, in *Proceedings of the IEEE International Conference on Computers, Systems and*

Signal Processing, Bangalore, India, 1984 (IEEE, New York), pp. 175–179.

Bennett, C. H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, 1993, Phys. Rev. Lett. **70**, 1895.

Bennett, C. H., G. Brassard, C. Crépeau, and M.-H. Skubiszewska, 1992, in *Advances in Cryptology—CRYPTO '91*, edited by J. Feigenbaum (Springer, Berlin), pp. 351–366.

Bennett, C. H., G. Brassard, and N. D. Mermin, 1992, Phys. Rev. Lett. **68**, 557.

Bennett, C. H., D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, 1996, Phys. Rev. A **54**, 3824.

Ben-Or, M., 2002, in *Proceedings of the Quantum Information Processing Workshop, Berkeley, CA, 2002*, http://www.msri.org/workshops/204/schedules/1258.

Ben-Or, M., M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, 2005, in *Proceedings of the Second International Conference on Theory of Cryptography (TCC '05), Cambridge, MA, 2005*, edited by J. Kilian (Springer-Verlag, Berlin), pp. 386–406.

Berlín, G., G. Brassard, F. Bussières, N. Godbout, J. A. Slater, and W. Tittel, 2011, Nat. Commun. **2**, 561.

Berta, M., M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, 2010, Nat. Phys. **6**, 659.

Biham, E., M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, 2000, in *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, Portland, OR, 2000* (ACM, New York), pp. 715–724.

Biham, E., B. Huttner, and T. Mor, 1996, Phys. Rev. A **54**, 2651.

Bloom, S., E. Korevaar, J. Schuster, and H. Willebrand, 2003, J. Opt. Networking **2**, 178.

Blum, M., 1981, in *Proceedings of the IEEE Workshop on Communications Security: Advances in Cryptology (CRYPTO '81), Santa Barbara, CA, 1981* (IEEE, New York), p. 11.

Boaron, A., *et al.*, 2018, Phys. Rev. Lett. **121**, 190502.

Bourennane, M., A. Karlsson, and G. Björk, 2001, Phys. Rev. A **64**, 012306.

Brádler, K., and C. Weedbrook, 2018, Phys. Rev. A **97**, 022310.

Branciard, C., E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, 2012, Phys. Rev. A **85**, 010301.

Brassard, G., and C. Crépeau, 1991, in *Advances in Cryptology—CRYPTO '90*, edited by A. J. Menezes and S. A. Vanstone (Springer, Berlin), pp. 49–61.

Brassard, G., N. Lütkenhaus, T. Mor, and B. C. Sanders, 2000, Phys. Rev. Lett. **85**, 1330.

Brassard, G., and L. Salvail, 1994, in *Advances in Cryptology—EUROCRYPT '93*, edited by T. Helleseth (Springer, Berlin), pp. 410–423.

Braunstein, S. L., and S. Pirandola, 2012, Phys. Rev. Lett. **108**, 130502.

Briegel, H.-J., W. Dür, J. I. Cirac, and P. Zoller, 1998, Phys. Rev. Lett. **81**, 5932.

Broadbent, A., J. Fitzsimons, and E. Kashefi, 2009, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS '09), Atlanta, 2009* (IEEE, New York), pp. 517–526.

Broadbent, A., and C. Schaffner, 2016, Des. Codes Cryptogr. **78**, 351.

Brumley, D., and D. Boneh, 2005, Comput. Networks **48**, 701.

Brunner, N., D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, 2014, Rev. Mod. Phys. **86**, 419.

Bruß, D., 1998, Phys. Rev. Lett. **81**, 3018.

Bugge, A. N., S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, and V. Makarov, 2014, Phys. Rev. Lett. **112**, 070503.

Bunandar, D., *et al.*, 2018, Phys. Rev. X **8**, 021009.

Buttler, W. T., R. Hughes, P. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, 1998, Phys. Rev. Lett. **81**, 3283.

Buttler, W. T., S. K. Lamoreaux, J. R. Torgerson, G. Nickel, C. Donahue, and C. G. Peterson, 2003, Phys. Rev. A **67**, 052303.

Cai, H., *et al.*, 2017, Opt. Express **25**, 12282.

Calderbank, A. R., and P. W. Shor, 1996, Phys. Rev. A **54**, 1098.

Cañas, G., *et al.*, 2017, Phys. Rev. A **96**, 022317.

Canetti, R., 2001, in *Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, Newport Beach, CA, 2001* (IEEE, New York), pp. 136–145.

Cao, Z., Z. Zhang, H.-K. Lo, and X. Ma, 2015, New J. Phys. **17**, 053014.

Cerf, N. J., M. Bourennane, A. Karlsson, and N. Gisin, 2002, Phys. Rev. Lett. **88**, 127902.

Cerf, N. J., M. Lévy, and G. V. Assche, 2001, Phys. Rev. A **63**, 052311.

Chaiwongkhot, P., K. B. Kuntz, Y. Zhang, A. Huang, J.-P. Bourgoin, S. Sajeed, N. Lütkenhaus, T. Jennewein, and V. Makarov, 2019, Phys. Rev. A **99**, 062315.

Chakraborty, K., A. Chailloux, and A. Leverrier, 2015, Phys. Rev. Lett. **115**, 250501.

Chapuran, T. E., *et al.*, 2009, New J. Phys. **11**, 105001.

Chau, H.-F., 2002, Phys. Rev. A **66**, 060302.

Chau, H.-F., 2005, IEEE Trans. Inf. Theory **51**, 1451.

Chen, J.-P., *et al.*, 2020, Phys. Rev. Lett. **124**, 070501.

Chen, T.-Y., *et al.*, 2009, Opt. Express **17**, 6540.

Chen, T.-Y., *et al.*, 2010, Opt. Express **18**, 27217.

Chen, Y.-A., *et al.*, 2020 (to be published).

Choi, I., *et al.*, 2014, Opt. Express **22**, 23121.

Choi, Y., O. Kwon, M. Woo, K. Oh, S.-W. Han, Y.-S. Kim, and S. Moon, 2016, Phys. Rev. A **93**, 032319.

Christandl, M., R. König, and R. Renner, 2009, Phys. Rev. Lett. **102**, 020504.

Clarke, P. J., R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, 2012, Nat. Commun. **3**, 1174.

Cleve, R., D. Gottesman, and H.-K. Lo, 1999, Phys. Rev. Lett. **83**, 648.

Coles, P. J., M. Berta, M. Tomamichel, and S. Wehner, 2017, Rev. Mod. Phys. **89**, 015002.

Coles, P. J., E. M. Metodiev, and N. Lütkenhaus, 2016, Nat. Commun. **7**, 11712.

Collins, R. J., R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, 2016, Opt. Lett. **41**, 4883.

Collins, R. J., R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, 2014, Phys. Rev. Lett. **113**, 040502.

Comandar, L. C., M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W. B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, 2016, Nat. Photonics **10**, 312.

Cozzolino, D., *et al.*, 2019, Phys. Rev. Applied **11**, 064058.

Crépeau, C., D. Gottesman, and A. Smith, 2002, in *Proceedings of the Thirty-Fourth Annual ACM Symposium on Theory of Computing, Montreal, 2002* (ACM, New York), pp. 643–652.

Cui, C., Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, 2019, Phys. Rev. Applied **11**, 034053.

Curty, M., K. Azuma, and H.-K. Lo, 2019, npj Quantum Inf. **5**, 64.

Curty, M., M. Lewenstein, and N. Lütkenhaus, 2004, Phys. Rev. Lett. **92**, 217903.

Curty, M., and H.-K. Lo, 2019, npj Quantum Inf. **5**, 14.

Curty, M., X. Ma, B. Qi, and T. Moroder, 2010, Phys. Rev. A **81**, 022310.

Curty, M., and T. Moroder, 2011, Phys. Rev. A **84**, 010304.

Curty, M., F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, 2014, Nat. Commun. **5**, 3732.

DamgÅrd, I., S. Fehr, L. Salvail, and C. Schaffner, 2008, SIAM J. Comput. **37**, 1865.

D'Ariano, G. M., D. Kretschmann, D. Schlingemann, and R. F. Werner, 2007, Phys. Rev. A **76**, 032328.

da Silva, T. F., G. B. Xavier, G. P. Temporão, and J. P. von der Weid, 2012, Opt. Express **20**, 18911.

De, A., C. Portmann, T. Vidick, and R. Renner, 2012, SIAM J. Comput. **41**, 915.

Deutsch, D., A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, 1996, Phys. Rev. Lett. **77**, 2818.

Devetak, I., and A. Winter, 2005, Proc. R. Soc. A **461**, 207.

Diamanti, E., and A. Leverrier, 2015, Entropy **17**, 6072.

Diamanti, E., H.-K. Lo, B. Qi, and Z. Yuan, 2016, npj Quantum Inf. **2**, 16025.

Dieks, D., 1982, Phys. Lett. **92A**, 271.

Ding, Y., D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, 2017, npj Quantum Inf. **3**, 25.

DiVincenzo, D. P., M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, 2004, Phys. Rev. Lett. **92**, 067902.

Dixon, A. R., and H. Sato, 2015, Sci. Rep. **4**, 7275.

Dixon, A. R., Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, 2008, Opt. Express **16**, 18790.

Donaldson, R. J., R. J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, and G. S. Buller, 2016, Phys. Rev. A **93**, 012329.

Duan, L.-M., M. Lukin, J. I. Cirac, and P. Zoller, 2001, Nature (London) **414**, 413.

Duligall, J. L., M. S. Godfrey, K. A. Harrison, W. J. Munro, and J. G. Rarity, 2006, New J. Phys. **8**, 249.

Dunjko, V., E. Kashefi, and A. Leverrier, 2012, Phys. Rev. Lett. **108**, 200502.

Dunjko, V., P. Wallden, and E. Andersson, 2014, Phys. Rev. Lett. **112**, 040502.

Dušek, M., M. Jahma, and N. Lütkenhaus, 2000, Phys. Rev. A **62**, 022306.

Dynes, J. F., *et al.*, 2016, Sci. Rep. **6**, 35149.

Dynes, J. F., *et al.*, 2019, npj Quantum Inf. **5**, 101.

Eberhard, P. H., 1993, Phys. Rev. A **47**, R747.

Ekert, A. K., 1991, Phys. Rev. Lett. **67**, 661.

Elkouss, D., A. Leverrier, R. Alléaume, and J. J. Boutros, 2009, in *Proceedings of the 2009 IEEE International Symposium on Information Theory (ISIT 2009), Seoul, 2009* (IEEE, New York), pp. 1879–1883.

Elliott, C., A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, 2005, in *Quantum Information and Computation III*, SPIE Proceedings Vol. 5815 (SPIE—International Society for Optics and Photonics, Bellingham, WA), pp. 138–149.

Eraerds, P., N. Walenta, M. Legré, N. Gisin, and H. Zbinden, 2010, New J. Phys. **12**, 063027.

Erven, C., N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, 2014, Nat. Commun. **5**, 3418.

Etcheverry, S., G. Cañas, E. Gómez, W. Nogueira, C. Saavedra, G. Xavier, and G. Lima, 2013, Sci. Rep. **3**, 2316.

Fang, X.-T., *et al.*, 2020, Nat. Photonics (in press).

Fawzi, O., P. Hayden, and P. Sen, 2013, J. Assoc. Comput. Mach. **60**, 44.

Ferenczi, A., 2013, Ph.D. thesis (University of Waterloo).

Ferreira da Silva, T., D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, 2013, Phys. Rev. A **88**, 052303.

Fitzsimons, J. F., 2017, npj Quantum Inf. **3**, 23.

Fossier, S., E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, 2009, New J. Phys. **11**, 045023.

Fossorier, M. P., M. Mihaljevic, and H. Imai, 1999, IEEE Trans. Commun. **47**, 673.

Franson, J. D., and B. Jacobs, 1995, Electron. Lett. **31**, 232.

Fröhlich, B., J. F. Dynes, M. Lucamarini, A. W. Sharpe, Z. Yuan, and A. J. Shields, 2013, Nature (London) **501**, 69.

Fröhlich, B., M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, 2017, Optica **4**, 163.

Fung, C.-H. F., H. F. Chau, and H.-K. Lo, 2011, Phys. Rev. A **84**, 020303.

Fung, C.-H. F., X. Ma, and H. F. Chau, 2010, Phys. Rev. A **81**, 012318.

Fung, C.-H. F., B. Qi, K. Tamaki, and H.-K. Lo, 2007, Phys. Rev. A **75**, 032314.

Fung, C.-H. F., *et al.*, 2009, Quantum Inf. Comput. **9**, 131.

Furrer, F., 2014, Phys. Rev. A **90**, 042325.

Furrer, F., T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, 2012, Phys. Rev. Lett. **109**, 100502.

García-Patrón, R., and N. J. Cerf, 2006, Phys. Rev. Lett. **97**, 190503.

Gehring, T., V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, 2015, Nat. Commun. **6**, 8795.

Gerhardt, I., Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, 2011a, Nat. Commun. **2**, 349.

Gerhardt, I., Q. Liu, A. Lamas-Linares, J. Skaar, V. Scarani, V. Makarov, and C. Kurtsiefer, 2011b, Phys. Rev. Lett. **107**, 170404.

Ghorai, S., P. Grangier, E. Diamanti, and A. Leverrier, 2019, Phys. Rev. X **9**, 021059.

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

Gisin, N., S. Pironio, and N. Sangouard, 2010, Phys. Rev. Lett. **105**, 070501.

Gisin, N., G. Ribordy, W. Tittel, and H. Zbinden, 2002, Rev. Mod. Phys. **74**, 145.

Giustina, M., *et al.*, 2015, Phys. Rev. Lett. **115**, 250401.

Gobby, C., Z. Yuan, and A. Shields, 2004, Appl. Phys. Lett. **84**, 3762.

Goldreich, O., S. Micali, and A. Wigderson, 1986, in *Proceedings of the 27th Annual Symposium on Foundations of Computer Science (SFCS 1986), Toronto, 1986* (IEEE, New York), pp. 174–187.

Goldwasser, S., S. Micali, and C. Rackoff, 1989, SIAM J. Comput. **18**, 186.

Gottesman, D., and I. Chuang, 2001, arXiv:quant-ph/0105032.

Gottesman, D., and H.-K. Lo, 2003, IEEE Trans. Inf. Theory **49**, 457.

Gottesman, D., H.-K. Lo, N. Lütkenhaus, and J. Preskill, 2004, Quantum Inf. Comput. **4**, 325.

Gröblacher, S., T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, 2006, New J. Phys. **8**, 75.

Grosshans, F., 2005, Phys. Rev. Lett. **94**, 020504.

Grosshans, F., and P. Grangier, 2002, Phys. Rev. Lett. **88**, 057902.

Grosshans, F., G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, 2003, Nature (London) **421**, 238.

Guan, J.-Y., Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X. Ma, Q. Zhang, and J.-W. Pan, 2015, Phys. Rev. Lett. **114**, 180502.

Guest, M. A., 2001, arXiv:math/0105032.

Ha, J., J. Kim, D. Klinc, and S. W. McLaughlin, 2006, IEEE Trans. Inf. Theory **52**, 728.

Hadfield, R., 2009, Nat. Photonics **3**, 696.

Hänggi, E., R. Renner, and S. Wolf, 2010, in *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (Springer, New York), pp. 216–234.

Hasegawa, Y., R. Ikuta, N. Matsuda, K. Tamaki, H.-K. Lo, T. Yamamoto, K. Azuma, and N. Imoto, 2019, Nat. Commun. **10**, 378.

Heim, B., C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, 2014, New J. Phys. **16**, 113018.

Henning, W., K. Harald, R. Markus, F. Martin, N. Sebastian, and W. Harald, 2011, New J. Phys. **13**, 073024.

Hensen, B., *et al.*, 2015, Nature (London) **526**, 682.

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

Hillery, M., 2000, Phys. Rev. A **61**, 022309.

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

Hiroshima, T., 2006, Phys. Rev. A **73**, 012330.

Holevo, A. S., 1973, Probl. Peredachi Inf. **9**, 3.

Hong, C. K., Z. Y. Ou, and L. Mandel, 1987, Phys. Rev. Lett. **59**, 2044.

Horodecki, K., M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, 2008a, IEEE Trans. Inf. Theory **54**, 2604.

Horodecki, K., M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, 2008b, Phys. Rev. Lett. **100**, 110502.

Hu, X.-Y., E. Eleftheriou, and D.-M. Arnold, 2005, IEEE Trans. Inf. Theory **51**, 386.

Huang, A., Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, 2019, Phys. Rev. Applied **12**, 064043.

Huang, A., S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, 2016, IEEE J. Quantum Electron. **52**, 8000211.

Huang, A., S.-H. Sun, Z. Liu, and V. Makarov, 2018, Phys. Rev. A **98**, 012330.

Huang, D., P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng, 2016, Opt. Lett. **41**, 3511.

Huang, D., P. Huang, D. Lin, C. Wang, and G. Zeng, 2015, Opt. Lett. **40**, 3695.

Huang, D., P. Huang, D. Lin, and G. Zeng, 2016, Sci. Rep. **6**, 19201.

Huang, D., D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, 2015, Opt. Express **23**, 17511.

Huang, H.-L., *et al.*, 2017, Phys. Rev. Lett. **119**, 050503.

Huang, J.-Z., C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, 2013, Phys. Rev. A **87**, 062329.

Hughes, R., G. Morgan, and C. Peterson, 2000, J. Mod. Opt. **47**, 533.

Hughes, R. J., J. E. Nordholt, D. Derkacs, and C. G. Peterson, 2002, New J. Phys. **4**, 43.

Hughes, R. J., J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma, 2013, arXiv:1305.0305.

Hwang, W.-Y., 2003, Phys. Rev. Lett. **91**, 057901.

Inamori, H., 2002, Algorithmica **34**, 340.

Inamori, H., N. Lütkenhaus, and D. Mayers, 2007, Eur. Phys. J. D **41**, 599.

Inoue, K., E. Waks, and Y. Yamamoto, 2002, Phys. Rev. Lett. **89**, 037902.

Islam, N. T., C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, 2017, Sci. Adv. **3**, e1701491.

Jain, N., E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, 2014, New J. Phys. **16**, 123030.

Jain, N., B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, 2016, Contemp. Phys. **57**, 366.

Jain, N., B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, 2015, IEEE J. Sel. Top. Quantum Electron. **21**, 168.

Jain, N., C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, 2011, Phys. Rev. Lett. **107**, 110501.

Jiang, M.-S., S.-H. Sun, C.-Y. Li, and L.-M. Liang, 2012, Phys. Rev. A **86**, 032310.

Jiang, Y.-F., *et al.*, 2019, Phys. Rev. Lett. **123**, 100503.

Joshi, S. K., *et al.*, 2018, New J. Phys. **20**, 063016.

Jouguet, P., D. Elkouss, and S. Kunz-Jacques, 2014, Phys. Rev. A **90**, 042329.

Jouguet, P., S. Kunz-Jacques, and E. Diamanti, 2013, Phys. Rev. A **87**, 062313.

Jouguet, P., S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, 2013, Nat. Photonics **7**, 378.

Kaneda, F., F. Xu, J. Chapman, and P. G. Kwiat, 2017, Optica **4**, 1034.

Kaniewski, J., M. Tomamichel, E. Hänggi, and S. Wehner, 2013, IEEE Trans. Inf. Theory **59**, 4687.

Kaur, E., S. Guha, and M. M. Wilde, 2019, arXiv:1901.10099.

Kent, A., 2012, Phys. Rev. Lett. **109**, 130501.

Kilian, J., 1988, in *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing (STOC '88), Chicago, 1988* (ACM, New York), pp. 20–31.

Kimble, H., 2008, Nature (London) **453**, 1023.

Kitaev, A., 1999, report, 2nd Workshop on Algorithms in Quantum Information Processing, DePaul University, 1999.

Kitaev, A., D. Mayers, and J. Preskill, 2004, Phys. Rev. A **69**, 052326.

Kleis, S., M. Rueckmann, and C. G. Schaeffer, 2017, Opt. Lett. **42**, 1588.

Koashi, M., 2006, J. Phys. Conf. Ser. **36**, 98.

Koashi, M., 2009, New J. Phys. **11**, 045018.

Koashi, M., and J. Preskill, 2003, Phys. Rev. Lett. **90**, 057902.

Kocher, P., J. Jaffe, and B. Jun, 1999, in *Advances in Cryptology—CRYPTO '99*, edited by M. Wiener (Springer, New York), pp. 388–397.

Koehler-Sidki, A., J. Dynes, M. Lucamarini, G. Roberts, A. Sharpe, Z. Yuan, and A. Shields, 2018, Phys. Rev. Applied **9**, 044027.

Kok, P., and S. L. Braunstein, 2000, Phys. Rev. A **61**, 042304.

Konig, R., S. Wehner, and J. Wullschleger, 2012, IEEE Trans. Inf. Theory **58**, 1962.

Korzh, B., C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, 2015, Nat. Photonics **9**, 163.

Kumar, R., H. Qin, and R. Alléaume, 2015, New J. Phys. **17**, 043027.

Kunz-Jacques, S., and P. Jouguet, 2015, Phys. Rev. A **91**, 022307.

Kurtsiefer, C., P. Zarda, S. Mayer, and H. Weinfurter, 2001, J. Mod. Opt. **48**, 2039.

Lamas-Linares, A., and C. Kurtsiefer, 2007, Opt. Express **15**, 9388.

Lance, A. M., T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, 2005, Phys. Rev. Lett. **95**, 180503.

Laudenbach, F., C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, 2018, Adv. Quantum Technol. **1**, 1800011.

Laudenbach, F., B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, F. Karinou, A. Poppe, M. Peev, and H. Hübel, 2017, arXiv:1712.10242.

Lee, C., *et al.*, 2014, Phys. Rev. A **90**, 062331.

Leverrier, A., 2015, Phys. Rev. Lett. **114**, 070501.

Leverrier, A., 2017, Phys. Rev. Lett. **118**, 200501.

Leverrier, A., R. García-Patrón, R. Renner, and N. J. Cerf, 2013, Phys. Rev. Lett. **110**, 030502.

Leverrier, A., and P. Grangier, 2009, Phys. Rev. Lett. **102**, 180504.

Li, H.-W., *et al.*, 2011, Phys. Rev. A **84**, 062308.

Li, Y.-H., *et al.*, 2016, Phys. Rev. A **93**, 030302(R).

Li, Z., Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, 2014, Phys. Rev. A **89**, 052301.

Li, Z.-D., *et al.*, 2019, Nat. Photonics **13**, 644.

Liao, S.-K., *et al.*, 2017a, Nature (London) **549**, 43.

Liao, S.-K., *et al.*, 2017b, Nat. Photonics **11**, 509.

Liao, S.-K., *et al.*, 2018, Phys. Rev. Lett. **120**, 030501.

Lim, C. C. W., M. Curty, N. Walenta, F. Xu, and H. Zbinden, 2014, Phys. Rev. A **89**, 022307.

Lim, C. C. W., N. Walenta, M. Legré, N. Gisin, and H. Zbinden, 2015, IEEE J. Sel. Top. Quantum Electron. **21**, 192.

Lin, J., and N. Lütkenhaus, 2018, Phys. Rev. A **98**, 042332.

Lin, J., T. Upadhyaya, and N. Lütkenhaus, 2019, arXiv:1905.10896.

Liu, H., J. Wang, H. Ma, and S. Sun, 2018, Optica **5**, 902.

Liu, H., *et al.*, 2019, Phys. Rev. Lett. **122**, 160501.

Liu, W., X. Wang, N. Wang, S. Du, and Y. Li, 2017, Phys. Rev. A **96**, 042312.

Liu, Y., *et al.*, 2010, Opt. Express **18**, 8587.

Liu, Y., *et al.*, 2013, Phys. Rev. Lett. **111**, 130502.

Liu, Y., *et al.*, 2014, Phys. Rev. Lett. **112**, 010504.

Liu, Y., *et al.*, 2016, Phys. Rev. A **94**, 020301.

Liu, Y., *et al.*, 2018, Nature (London) **562**, 548.

Liu, Y., *et al.*, 2019, Phys. Rev. Lett. **123**, 100505.

Lloyd, S., 2013, arXiv:1307.0380.

Lo, H.-K., 1997, Phys. Rev. A **56**, 1154.

Lo, H.-K., 2001, Quantum Inf. Comput. **1**, 81.

Lo, H.-K., 2003, New J. Phys. **5**, 36.

Lo, H.-K., 2004, in *Proceedings of the 2004 IEEE International Symposium on Information Theory (ISIT 2004), Chicago, 2004* (IEEE, New York), pp. 137.

Lo, H.-K., and H. F. Chau, 1997, Phys. Rev. Lett. **78**, 3410.

Lo, H.-K., and H. F. Chau, 1998, Physica (Amsterdam) **120D**, 177.

Lo, H.-K., and H. F. Chau, 1999, Science **283**, 2050.

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

Lo, H.-K., M. Curty, and K. Tamaki, 2014, Nat. Photonics **8**, 595.

Lo, H.-K., X. Ma, and K. Chen, 2005, Phys. Rev. Lett. **94**, 230504.

Lo, H.-K., and J. Preskill, 2007, Quantum Inf. Comput. **7**, 431.

Lodewyck, J., *et al.*, 2007, Phys. Rev. A **76**, 042305.

Lorenzo, G. C., A. Navarrete, K. Azuma, M. Curty, and M. Razavi, 2019, arXiv:1910.11407.

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

Lucamarini, M., K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, 2013, Opt. Express **21**, 24550.

Lucamarini, M., Z. Yuan, J. Dynes, and A. Shields, 2018, Nature (London) **557**, 400.

Lum, D. J., J. C. Howell, M. S. Allman, T. Gerrits, V. B. Verma, S. W. Nam, C. Lupo, and S. Lloyd, 2016, Phys. Rev. A **94**, 022315.

Lunghi, T., J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden, 2013, Phys. Rev. Lett. **111**, 180504.

Lunghi, T., J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden, 2015, Phys. Rev. Lett. **115**, 030502.

Lupo, C., C. Ottaviani, P. Papanastasiou, and S. Pirandola, 2018, Phys. Rev. A **97**, 052327.

Lupo, C., M. M. Wilde, and S. Lloyd, 2014, Phys. Rev. A **90**, 022326.

Lütkenhaus, N., 1999, Phys. Rev. A **59**, 3301.

Lütkenhaus, N., 2000, Phys. Rev. A **61**, 052304.

Lydersen, L., M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, 2011, New J. Phys. **13**, 113042.

Lydersen, L., N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, 2011, Phys. Rev. A **84**, 032320.

Lydersen, L., C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, 2010, Nat. Photonics **4**, 686.

Ma, C., W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, F. Xu, T. Thiessen, H.-K. Lo, and J. K. S. Poon, 2016, Optica **3**, 1274.

Ma, J., Y. Zhou, X. Yuan, and X. Ma, 2019, Phys. Rev. A **99**, 062325.

Ma, X., 2004, master's thesis (University of Toronto) [arXiv:quant-ph/0503057].

Ma, X., 2006, Phys. Rev. A **74**, 052325.

Ma, X., 2008, Ph.D. thesis (University of Toronto) [arXiv:0808.1385].

Ma, X., C.-H. F. Fung, J.-C. Boileau, and H. Chau, 2011, Comput. Secur. **30**, 172.

Ma, X., C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, 2006, Phys. Rev. A **74**, 032330.

Ma, X., C.-H. F. Fung, and H.-K. Lo, 2007, Phys. Rev. A **76**, 012307.

Ma, X., C.-H. F. Fung, and M. Razavi, 2012, Phys. Rev. A **86**, 052305.

Ma, X., and H.-K. Lo, 2008, New J. Phys. **10**, 073018.

Ma, X., B. Qi, Y. Zhao, and H.-K. Lo, 2005, Phys. Rev. A **72**, 012326.

Ma, X., and M. Razavi, 2012, Phys. Rev. A **86**, 062319.

Ma, X., F. Xu, H. Xu, X. Tan, B. Qi, and H.-K. Lo, 2013, Phys. Rev. A **87**, 062327.

Ma, X., X. Yuan, Z. Cao, B. Qi, and Z. Zhang, 2016, npj Quantum Inf. **2**, 16021.

Ma, X., P. Zeng, and H. Zhou, 2018, Phys. Rev. X **8**, 031043.

Ma, X.-C., S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, 2014, Phys. Rev. A **89**, 042335.

Ma, X.-C., S.-H. Sun, M.-S. Jiang, and L.-M. Liang, 2013a, Phys. Rev. A **88**, 022339.

Ma, X.-C., S.-H. Sun, M.-S. Jiang, and L.-M. Liang, 2013b, Phys. Rev. A **87**, 052309.

MacKay, D. J., and R. M. Neal, 1996, Electron. Lett. **32**, 1645.

MacKay, D. J., S. T. Wilson, and M. C. Davey, 1999, IEEE Trans. Commun. **47**, 1449.

Maeda, K., T. Sasaki, and M. Koashi, 2019, Nat. Commun. **10**, 3140.

Mafu, M., A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, 2013, Phys. Rev. A **88**, 032305.

Makarov, V., 2009, New J. Phys. **11**, 065003.

Makarov, V., A. Anisimov, and J. Skaar, 2006, Phys. Rev. A **74**, 022313.

Makarov, V., J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, 2016, Phys. Rev. A **94**, 030302.

Makarov, V., and D. R. Hjelme, 2005, J. Mod. Opt. **52**, 691.

Mao, Y., *et al.*, 2018, Opt. Express **26**, 6010.

Marie, A., and R. Alléaume, 2017, Phys. Rev. A **95**, 012316.

Marøy, Ø., L. Lydersen, and J. Skaar, 2010, Phys. Rev. A **82**, 032337.

Martinez-Mateo, J., D. Elkouss, and V. Martin, 2010, in *Proceedings of the 6th International Symposium on Turbo Codes and Iterative Information Processing, Brest, France, 2010* (IEEE, New York), pp. 270–274.

Masanes, L., S. Pironio, and A. Acín, 2011, Nat. Commun. **2**, 238.

Mauerer, W., and C. Silberhorn, 2007, Phys. Rev. A **75**, 050305.

Maurer, U. M., and S. Wolf, 1999, IEEE Trans. Inf. Theory **45**, 499.

Mayers, D., 1996, in *Proceedings of the Fourth Workshop on Physics and Computation (STOC '88)* (New England Complex System Institute, Boston), p. 226.

Mayers, D., 1997, Phys. Rev. Lett. **78**, 3414.

Mayers, D., 2001, J. Assoc. Comput. Mach. **48**, 351.

Mayers, D., and A. Yao, 1998, in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS '98), Palo Alto, CA, 1998* (IEEE Computer Society, Washington, DC), pp. 503.

Miller, C. A., and Y. Shi, 2016, J. Assoc. Comput. Mach. **63**, 33.

Minder, M., M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, 2019, Nat. Photonics **13**, 334.

Mirhosseini, M., O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, 2015, New J. Phys. **17**, 033033.

Mohseni, M., P. Read, H. Neven, S. Boixo, V. Denchev, R. Babbush, A. Fowler, V. Smelyanskiy, and J. Martinis, 2017, Nature (London) **543**, 171.

Molina-Terriza, G., A. Vaziri, R. Ursin, and A. Zeilinger, 2005, Phys. Rev. Lett. **94**, 040501.

Mower, J., Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, 2013, Phys. Rev. A **87**, 062322.

Muller, A., H. Zbinden, and N. Gisin, 1996, Europhys. Lett. **33**, 335.

Munro, W. J., K. Azuma, K. Tamaki, and K. Nemoto, 2015, IEEE J. Sel. Top. Quantum Electron. **21**, 78.

Murta, G., S. B. van Dam, J. Ribeiro, R. Hanson, and S. Wehner, 2019, Quantum Sci. Technol. **4**, 035011.

Nakassis, A., J. C. Bienfang, and C. J. Williams, 2004, in *Quantum Information and Computation II*, Vol. 5436 (SPIE—International Society for Optics and Photonics, Bellingham, WA), pp. 28–35.

Nambu, Y., K. Yoshino, and A. Tomita, 2008, J. Mod. Opt. **55**, 1953.

Nauerth, S., M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, 2009, New J. Phys. **11**, 065001.

Navascués, M., and A. Acín, 2005, Phys. Rev. Lett. **94**, 020505.

Navascués, M., F. Grosshans, and A. Acín, 2006, Phys. Rev. Lett. **97**, 190502.

Ng, N. H. Y., S. K. Joshi, C. C. Ming, C. Kurtsiefer, and S. Wehner, 2012, Nat. Commun. **3**, 1326.

Nguyen, A. T., J. Frison, K. P. Huy, and S. Massar, 2008, New J. Phys. **10**, 083037.

Orieux, A., and E. Diamanti, 2016, J. Opt. **18**, 083002.

Pan, J.-W., D. Bouwmeester, M. Daniell, H. Weinfurter, and A. Zeilinger, 2000, Nature (London) **403**, 515.

Pan, J.-W., Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski, 2012, Rev. Mod. Phys. **84**, 777.

Panayi, C., M. Razavi, X. Ma, and N. Lütkenhaus, 2014, New J. Phys. **16**, 043005.

Pang, X.-L., A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, and X.-M. Jin, 2019, arXiv:1902.10423.

Pappa, A., P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, 2014, Nat. Commun. **5**, 3717.

Paraïso, T. K., I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, M. Lucamarini, Z. Yuan, and A. J. Shields, 2019, npj Quantum Inf. **5**, 42.

Patel, K. A., J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, 2012, Phys. Rev. X **2**, 041010.

Patel, K. A., J. F. Dynes, M. Lucamarini, I. Choi, A. W. Sharpe, Z. L. Yuan, R. V. Penty, and A. J. Shields, 2014, Appl. Phys. Lett. **104**, 051123.

Pawłowski, M., and N. Brunner, 2011, Phys. Rev. A **84**, 010302.

Pearle, P. M., 1970, Phys. Rev. D **2**, 1418.

Pedersen, T. B., and M. Toyran, 2013, arXiv:1307.7829.

Peev, M., *et al.*, 2009, New J. Phys. **11**, 075001.

Peng, C.-Z., J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, 2007, Phys. Rev. Lett. **98**, 010505.

Peuntinger, C., B. Heim, C. R. Müller, C. Gabriel, C. Marquardt, and G. Leuchs, 2014, Phys. Rev. Lett. **113**, 060502.

Pinheiro, P. V. P., P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, 2018, Opt. Express **26**, 21020.

Pirandola, S., R. Laurenza, C. Ottaviani, and L. Banchi, 2017, Nat. Commun. **8**, 15043.

Pirandola, S., S. Mancini, S. Lloyd, and S. L. Braunstein, 2008, Nat. Phys. **4**, 726.

Pirandola, S., C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, 2015, Nat. Photonics **9**, 397.

Pironio, S., A. AcÃn, N. Brunner, N. Gisin, S. Massar, and V. Scarani, 2009, New J. Phys. **11**, 045021.

Pizzi, R., D. Rossetti, and D. D'Arenzo, 2012, Int. J. Comput. **2**, 1052.

Qi, B., C.-H. F. Fung, H. K. Lo, and X. Ma, 2007, Quantum Inf. Comput. **7**, 73.

Qi, B., L.-L. Huang, L. Qian, and H.-K. Lo, 2007, Phys. Rev. A **76**, 052323.

Qi, B., P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, 2015, Phys. Rev. X **5**, 041009.

Qi, B., W. Zhu, L. Qian, and H.-K. Lo, 2010, New J. Phys. **12**, 103042.

Qian, Y.-J., D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, 2018, Phys. Rev. Applied **10**, 064062.

Qian, Y.-J., D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, 2019, Optica **6**, 1178.

Qin, H., R. Kumar, and R. Alléaume, 2016, Phys. Rev. A **94**, 012325.

Qin, H., R. Kumar, V. Makarov, and R. Alléaume, 2018, Phys. Rev. A **98**, 012312.

Qiu, J., 2014, Nature (London) **508**, 441.

Ralph, T. C., 1999, Phys. Rev. A **61**, 010303.

Reichardt, B. W., F. Unger, and U. Vazirani, 2013, Nature (London) **496**, 456.

Reid, M. D., 2000, Phys. Rev. A **62**, 062308.

Renner, R., 2007, Nat. Phys. **3**, 645.

Renner, R., 2008, Int. J. Quantum. Inform. **06**, 1.

Renner, R., 2012, arXiv:1209.2423.

Renner, R., and J. I. Cirac, 2009, Phys. Rev. Lett. **102**, 110504.

Renner, R., N. Gisin, and B. Kraus, 2005, Phys. Rev. A **72**, 012332.

Renner, R., and R. König, 2005, in *Proceedings of the Second International Conference on Theory of Cryptography (TCC '05), Cambridge, MA* (Springer-Verlag, Berlin), pp. 407–425.

Ribordy, G., J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden, 2000, J. Mod. Opt. **47**, 517.

Richardson, T. J., and R. L. Urbanke, 2001, IEEE Trans. Inf. Theory **47**, 599.

Rivest, R. L., A. Shamir, and L. Adleman, 1978, Commun. ACM **21**, 120.

Roberts, G., M. Lucamarini, J. Dynes, S. Savory, Z. Yuan, and A. Shields, 2018, Quantum Sci. Technol. **3**, 045010.

Roberts, G., M. Lucamarini, Z. Yuan, J. Dynes, L. Comandar, A. Sharpe, A. Shields, M. Curty, I. Puthoor, and E. Andersson, 2017, Nat. Commun. **8**, 1098.

Rogers, D. J., J. C. Bienfang, A. Nakassis, H. Xu, and C. W. Clark, 2007, New J. Phys. **9**, 319.

Rosenberg, D., J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, 2007, Phys. Rev. Lett. **98**, 010503.

Rosenberg, D., *et al.*, 2009, New J. Phys. **11**, 045009.

Rosenfeld, W., D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, 2017, Phys. Rev. Lett. **119**, 010402.

Rubenok, A., J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, 2013, Phys. Rev. Lett. **111**, 130501.

Sajeed, S., P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, 2015, Phys. Rev. A **91**, 062301.

Sajeed, S., I. Radchenko, S. Kaiser, J.-P. Bourgoin, A. Pappa, L. Monat, M. Legré, and V. Makarov, 2015, Phys. Rev. A **91**, 032326.

Sangouard, N., C. Simon, H. de Riedmatten, and N. Gisin, 2011, Rev. Mod. Phys. **83**, 33.

Sasaki, M., *et al.*, 2011, Opt. Express **19**, 10387.

Sasaki, T., Y. Yamamoto, and M. Koashi, 2014, Nature (London) **509**, 475.

Sauge, S., L. Lydersen, A. Anisimov, J. Skaar, and V. Makarov, 2011, Opt. Express **19**, 23590.

Scarani, V., A. Acín, G. Ribordy, and N. Gisin, 2004, Phys. Rev. Lett. **92**, 057901.

Scarani, V., H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, 2009, Rev. Mod. Phys. **81**, 1301.

Scarani, V., and R. Renner, 2008, Phys. Rev. Lett. **100**, 200501.

Schmitt-Manderbach, T., *et al.*, 2007, Phys. Rev. Lett. **98**, 010504.

Sergienko, A. V., 2018, *Quantum Communications and Cryptography* (CRC Press, Boca Raton, FL).

Seshadreesan, K. P., M. Takeoka, and M. Sasaki, 2016, Phys. Rev. A **93**, 042328.

Shalm, L. K., *et al.*, 2015, Phys. Rev. Lett. **115**, 250402.

Shannon, C. E., 1949, Bell Syst. Tech. J. **28**, 656.

Shor, P. W., 1997, SIAM J. Comput. **26**, 1484.

Shor, P. W., and J. Preskill, 2000, Phys. Rev. Lett. **85**, 441.

Sibson, P., J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, and M. G. Thompson, 2017, Optica **4**, 172.

Sibson, P., *et al.*, 2017, Nat. Commun. **8**, 13984.

Silberhorn, C., T. C. Ralph, N. Lütkenhaus, and G. Leuchs, 2002, Phys. Rev. Lett. **89**, 167901.

Singh, S., 2000, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Anchor, Garden City, NY).

Sit, A., *et al.*, 2017, Optica **4**, 1006.

Smith, D. H., *et al.*, 2012, Nat. Commun. **3**, 625.

Soh, D. B. S., C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, 2015, Phys. Rev. X **5**, 041010.

Steane, A. M., 1996, Phys. Rev. A **54**, 4741.

Stucki, D., N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, 2005, Appl. Phys. Lett. **87**, 194108.

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

Stucki, D., *et al.*, 2011, New J. Phys. **13**, 123001.

Sun, Q.-C., *et al.*, 2014, Laser Phys. Lett. **11**, 085202.

Sun, S.-H., M. Gao, M.-S. Jiang, C.-Y. Li, and L.-M. Liang, 2012, Phys. Rev. A **85**, 032304.

Sun, S.-H., M.-S. Jiang, and L.-M. Liang, 2011, Phys. Rev. A **83**, 062331.

Sun, S.-H., F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, and L.-M. Liang, 2015, Phys. Rev. A **92**, 022304.

Symul, T., D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, 2007, Phys. Rev. A **76**, 030303.

Takeoka, M., S. Guha, and M. M. Wilde, 2014, Nat. Commun. **5**, 5235.

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

Takesue, H., S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, 2007, Nat. Photonics **1**, 343.

Takesue, H., T. Sasaki, K. Tamaki, and M. Koashi, 2015, Nat. Photonics **9**, 827.

Tamaki, K., M. Curty, G. Kato, H.-K. Lo, and K. Azuma, 2014, Phys. Rev. A **90**, 052314.

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

Tamaki, K., M. Koashi, and N. Imoto, 2003, Phys. Rev. Lett. **90**, 167904.

Tamaki, K., H.-K. Lo, C.-H. F. Fung, and B. Qi, 2012, Phys. Rev. A **85**, 042307.

Tamaki, K., H.-K. Lo, W. Wang, and M. Lucamarini, 2018, arXiv:1805.05511.

Tamaki, K., and N. Lütkenhaus, 2004, Phys. Rev. A **69**, 032316.

Tan, E. Y.-Z., C. C.-W. Lim, and R. Renner, 2020, Phys. Rev. Lett. **124**, 020502.

Tang, G.-Z., S.-H. Sun, F. Xu, H. Chen, C.-Y. Li, and L.-M. Liang, 2016, Phys. Rev. A **94**, 032326.

Tang, Y. L., *et al.*, 2015, IEEE J. Sel. Top. Quantum Electron. **21**, 116.

Tang, Y.-L., H.-L. Yin, X. Ma, C.-H. F. Fung, Y. Liu, H.-L. Yong, T.-Y. Chen, C.-Z. Peng, Z.-B. Chen, and J.-W. Pan, 2013, Phys. Rev. A **88**, 022308.

Tang, Y.-L., *et al.*, 2014, Phys. Rev. Lett. **113**, 190501.

Tang, Y.-L., *et al.*, 2016, Phys. Rev. X **6**, 011024.

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

Tomamichel, M., C. C. W. Lim, N. Gisin, and R. Renner, 2012, Nat. Commun. **3**, 634.

Tomamichel, M., and R. Renner, 2011, Phys. Rev. Lett. **106**, 110506.

Tomamichel, M., C. Schaffner, A. Smith, and R. Renner, 2011, IEEE Trans. Inf. Theory **57**, 5524.

Townsend, P. D., 1994, Electron. Lett. **30**, 809.

Townsend, P. D., 1997, Electron. Lett. **33**, 188.

Townsend, P. D., J. Rarity, and P. Tapster, 1993, Electron. Lett. **29**, 1291.

Tsurumaru, T., 2018, arXiv:1809.05479.

Tsurumaru, T., and K. Tamaki, 2008, Phys. Rev. A **78**, 032302.

Unruh, D., 2010, in *Advances in Cryptology—EUROCRYPT 2010* (Springer, Berlin), pp. 486–505.

Usenko, V. C., and R. Filip, 2016, Entropy **18**, 20.

Usenko, V. C., and F. Grosshans, 2015, Phys. Rev. A **92**, 062337.

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

Valivarthi, R., Q. Zhou, C. John, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, and W. Tittel, 2017, Quantum Sci. Technol. **2**, 04LT01.

Valivarthi, R., *et al.*, 2015, J. Mod. Opt. **62**, 1141.

Vasylyev, D., A. Semenov, W. Vogel, K. Günthner, A. Thurn, Ö. Bayraktar, and C. Marquardt, 2017, Phys. Rev. A **96**, 043856.

Vazirani, U., and T. Vidick, 2014, Phys. Rev. Lett. **113**, 140501.

Verbanis, E., A. Martin, R. Houlmann, G. Boso, F. Bussières, and H. Zbinden, 2016, Phys. Rev. Lett. **117**, 140506.

Vernam, G. S., 1926, Trans. Am. Inst. Electr. Eng. **XLV**, 295.

Vest, G., M. Rau, L. Fuchs, G. Corrielli, H. Weier, S. Nauerth, A. Crespi, R. Osellame, and H. Weinfurter, 2015, IEEE J. Sel. Top. Quantum Electron. **21**, 131.

Walborn, S., D. Lemelle, M. Almeida, and P. S. Ribeiro, 2006, Phys. Rev. Lett. **96**, 090501.

Wallden, P., V. Dunjko, A. Kent, and E. Andersson, 2015, Phys. Rev. A **91**, 042304.

Walls, D., and G. Milburn, 2008, *Quantum Optics* (Springer, Berlin).

Wang, C., X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, and Z.-F. Han, 2015, Phys. Rev. Lett. **115**, 160502.

Wang, C., Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, 2017, Optica **4**, 1016.

Wang, J.-Y., *et al.*, 2013, Nat. Photonics **7**, 387.

Wang, L.-J., L.-K. Chen, L. Ju, M.-L. Xu, Y. Zhao, K. Chen, Z.-B. Chen, T.-Y. Chen, and J.-W. Pan, 2015, Appl. Phys. Lett. **106**, 081108.

Wang, L.-J., *et al.*, 2017, Phys. Rev. A **95**, 012301.

Wang, N., S. Du, W. Liu, X. Wang, Y. Li, and K. Peng, 2018, Phys. Rev. Applied **10**, 064028.

Wang, Q., W. Chen, G. Xavier, M. Swillo, T. Zhang, S. Sauge, M. Tengner, Z.-F. Han, G.-C. Guo, and A. Karlsson, 2008, Phys. Rev. Lett. **100**, 090501.

Wang, S., D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, 2019, Phys. Rev. X **9**, 021046.

Wang, S., P. Huang, T. Wang, and G. Zeng, 2019, Phys. Rev. Applied **12**, 024041.

Wang, S., Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, H.-W. Li, L.-J. Zhang, Z. Zhou, G.-C. Guo, and Z.-F. Han, 2015, Nat. Photonics **9**, 832.

Wang, S., *et al.*, 2010, Opt. Lett. **35**, 2454.

Wang, T., P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, 2018, Opt. Express **26**, 2794.

Wang, W., K. Tamaki, and M. Curty, 2018, New J. Phys. **20**, 083027.

Wang, W., F. Xu, and H.-K. Lo, 2019, Phys. Rev. X **9**, 041012.

Wang, X.-B., 2005, Phys. Rev. Lett. **94**, 230503.

Wang, X.-B., 2013, Phys. Rev. A **87**, 012320.

Wang, X.-B., Z.-W. Yu, and X.-L. Hu, 2018, Phys. Rev. A **98**, 062323.

Wang, Y., I. W. Primaatmaja, E. Lavie, A. Varvitsiotis, and C. C. W. Lim, 2019, npj Quantum Inf. **5**, 17.

Weedbrook, C., A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, 2004, Phys. Rev. Lett. **93**, 170504.

Weedbrook, C., S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, 2012, Rev. Mod. Phys. **84**, 621.

Weedbrook, C., S. Pirandola, S. Lloyd, and T. C. Ralph, 2010, Phys. Rev. Lett. **105**, 110501.

Wehner, S., D. Elkouss, and R. Hanson, 2018, Science **362**, eaam9288.

Wehner, S., C. Schaffner, and B. M. Terhal, 2008, Phys. Rev. Lett. **100**, 220502.

Wei, K., W. Zhang, Y.-L. Tang, L. You, and F. Xu, 2019, Phys. Rev. A **100**, 022325.

Wei, K., *et al.*, 2019, arXiv:1911.00690.

Wiechers, C., L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, and G. Leuchs, 2011, New J. Phys. **13**, 013043.

Winick, A., N. Lütkenhaus, and P. J. Coles, 2018, Quantum **2**, 77.

Wolf, M. M., G. Giedke, and J. I. Cirac, 2006, Phys. Rev. Lett. **96**, 080502.

Wootters, W. K., and W. H. Zurek, 1982, Nature (London) **299**, 802.

Xavier, G. B., and G. Lima, 2020, Commun. Phys. **3**, 9.

Xu, F., 2015, Phys. Rev. A **92**, 012333.

Xu, F., M. Curty, B. Qi, and H. Lo, 2015, IEEE J. Sel. Top. Quantum Electron. **21**, 148.

Xu, F., M. Curty, B. Qi, and H.-K. Lo, 2013, New J. Phys. **15**, 113007.

Xu, F., M. Curty, B. Qi, L. Qian, and H.-K. Lo, 2015a, Nat. Photonics **9**, 772.

Xu, F., B. Qi, Z. Liao, and H.-K. Lo, 2013b, Appl. Phys. Lett. **103**, 061101.

Xu, F., B. Qi, and H.-K. Lo, 2010, New J. Phys. **12**, 113026.

Xu, F., K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, 2015b, Phys. Rev. A **92**, 032305.

Xu, F., H. Xu, and H.-K. Lo, 2014, Phys. Rev. A **89**, 052333.

Yang, S.-J., X.-J. Wang, X.-H. Bao, and J.-W. Pan, 2016, Nat. Photonics **10**, 381.

Yin, H.-L., *et al.*, 2016, Phys. Rev. Lett. **117**, 190501.

Yin, H.-L., *et al.*, 2017a, Phys. Rev. A **95**, 032334.

Yin, H.-L., *et al.*, 2017b, Phys. Rev. A **95**, 042338.

Yin, J., *et al.*, 2019 (to be published).

Yin, Z.-Q., C.-H. F. Fung, X. Ma, C.-M. Zhang, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, 2014, Phys. Rev. A **90**, 052319.

Yin, Z.-Q., Z.-F. Han, W. Chen, F.-X. Xu, Q.-L. Wu, and G.-C. Guo, 2008, Chin. Phys. Lett. **25**, 3547.

Yin, Z.-Q., S. Wang, W. Chen, Y.-G. Han, R. Wang, G.-C. Guo, and Z.-F. Han, 2018, Nat. Commun. **9**, 457.

Yoshino, K.-i., M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, and A. Tomita, 2018, npj Quantum Inf. **4**, 8.

Yu, Y., *et al.*, 2020, Nature (London) **578**, 240.

Yu, Z.-W., Y.-H. Zhou, and X.-B. Wang, 2015, Phys. Rev. A **91**, 032318.

Yuan, X., H. Zhou, Z. Cao, and X. Ma, 2015, Phys. Rev. A **92**, 022124.

Yuan, Z., *et al.*, 2018, J. Lightwave Technol. **36**, 3427.

Yuan, Z. L., A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, 2009, New J. Phys. **11**, 045019.

Yuan, Z. L., J. F. Dynes, and A. J. Shields, 2010, Nat. Photonics **4**, 800.

Yuan, Z. L., J. F. Dynes, and A. J. Shields, 2011, Appl. Phys. Lett. **98**, 231104.

Yuan, Z. L., B. Fröhlich, M. Lucamarini, G. Roberts, J. Dynes, and A. Shields, 2016, Phys. Rev. X **6**, 031044.

Yuan, Z. L., A. W. Sharpe, and A. J. Shields, 2007, Appl. Phys. Lett. **90**, 269901.

Yuen, H. P., 2016, IEEE Access **4**, 724.

Zeng, P., W. Wu, and X. Ma, 2019, arXiv:1910.05737.

Zhang, G. *et al.*, 2019, Nat. Photonics **13**, 839.

Zhang, J., M. A. Itzler, H. Zbinden, and J.-W. Pan, 2015, Light Sci. Appl. **4**, e286.

Zhang, P., *et al.*, 2014, Phys. Rev. Lett. **112**, 130501.

Zhang, Q., C. Langrock, H. Takesue, X. Xie, M. Fejer, and Y. Yamamoto, 2008, Opt. Express **16**, 3293.

Zhang, Q., F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, 2018, Opt. Express **26**, 24260.

Zhang, Y. *et al.*, 2019, Quantum Sci. Technol. **4**, 035006.

Zhang, Y.-C., Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, 2020, arXiv:2001.02555.

Zhang, Y.-C., Y. Huang, Z. Chen, Z. Li, S. Yu, and H. Guo, 2019, arXiv:1908.06230.

Zhang, Z., J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, 2014, Phys. Rev. Lett. **112**, 120506.

Zhang, Z., Q. Zhao, M. Razavi, and X. Ma, 2017, Phys. Rev. A **95**, 012333.

Zhao, Q., Y. Liu, X. Yuan, E. Chitambar, and X. Ma, 2018, Phys. Rev. Lett. **120**, 070403.

Zhao, Y., C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, 2008, Phys. Rev. A **78**, 042333.

Zhao, Y., B. Qi, X. Ma, H.-k. Lo, and L. Qian, 2006a, in *Proceedings of the 2006 IEEE International Symposium on Information Theory, Seattle, 2006* (IEEE, New York), pp. 2094–2098.

Zhao, Y., B. Qi, X. Ma, H.-K. Lo, and L. Qian, 2006b, Phys. Rev. Lett. **96**, 070502.

Zhao, Y.-B., M. Heid, J. Rigas, and N. Lütkenhaus, 2009, Phys. Rev. A **79**, 012307.

Zhong, T., *et al.*, 2015, New J. Phys. **17**, 022002.

Zhong, X., J. Hu, M. Curty, L. Qian, and H.-K. Lo, 2019, Phys. Rev. Lett. **123**, 100506.

Zhong, X., W. Wang, L. Qian, and H.-K. Lo, 2020, arXiv:2001.10599.

Zhou, Y.-H., Z.-W. Yu, and X.-B. Wang, 2016, Phys. Rev. A **93**, 042324.