Quantum Cryptography: Key Distribution and Beyond

Akshata Shenoy-Hejamadi [1] **, Anirban Pathak** [2] **& Srikanth Radhakrishna** [3]

[1] Group of Applied Physics, University of Geneva, Switzerland. E-mail: akshata.shenoy@etu.unige.ch
[2] Jaypee Institute of Information Technology, Noida, India. E-mail: anirban.pathak@jiit.ac.in
[3] Poornaprajna Institute of Scientific Research, Bangalore, India. E-mail: srik@poornaprajna.org

Uniquely among the sciences, quantum cryptography has driven both foundational research as well as practical real-life applications. We review the progress of quantum cryptography in the last decade, covering quantum key distribution and other applications.
Quanta 2017; 6: 1–47.

1 Introduction

Cryptography is the technique of concealing confidential information using physical or mathematical means. While cryptologists find newer methods to conceal a secret, cryptanalysts devise powerful methods to compromise the same. This recursive cat-and-mouse game has pushed the field and driven progress in it tremendously, motivating the participation of a large group of physicists, mathematicians and engineers.

The seminal work of Peter W. Shor [1] uncovered the security threat that quantum computation posed on all classical cryptographic schemes that are based on computational assumptions, such as the hardness of the discrete logarithm problem and the factorization problem. One such cryptographic scheme is the Rivest–Shamir–Adleman (RSA) scheme, which is widely used in e-commerce today. RSA in today's world is safe so long as a scalable quantum computer remains unfeasible. However, ideally, we wish to guarantee cryptographic security that follows only from basic physics. This is the promise of quantum cryptography.

In particular, note the recent report on a loophole-free test of Bell's inequality [2], thereby conclusively verifying the existence of quantum nonlocality in Nature, and also attesting to the advancement of experimental techniques to prepare, transmit, manipulate and measure quantum information. Another direction in cryptography is to provide practicable tools embracing experimental limitations, e.g. quantum key distribution with pulses having mean photon number much larger than one [3].

Several quantum cryptographic tools have now been commercialized. ID-Quantique, a major player in the quantum cryptography industry, sells complete cryptographic solutions. Their products include network encryption systems, quantum cryptographic systems especially designed for industry and government, a quantum random number generator, a state-of-art photon counting device, single photon source, etc. QUANTIS, a quantum random number generator from ID-Quantique deserves special mention, as it is used in quantum key distribution and various quantum-classical hybrid machines (e.g., in casinos); the CLAVIS series of products, which provide a platform for cryptography research, are worth noting. Further, ID-Quantique's cryptographic solution provides an open platform where buyers can incorporate their own encryption algorithms.

Further, there are several other companies trying to commercialize quantum key distribution (see a long list of such companies at Wikipedia, which depicts the importance of the field). Among this set of large number of other companies and the interesting products developed by them, we would like to point out a few. Toshiba markets an excellent room temperature single-photon detector, a photon number resolving detector and a quantum key distribution system using the T12 protocol [4], in which the probability that bit values are encoded in X and Z basis are different (otherwise, T12 is similar to Bennett–Brassard 1984 protocol (BB84)) and decoy qubits are used. A very attractive example of quantum-classical hybrid cryptographic product is the world's first quantum-key-distribution-based one-time-pad mobile phone software designed by Mitsubishi Electric.

The interaction between academia and industry, and the development of commercially viable products as a result, has been relatively thriving in this area. In 2015, H. Zbinden and his colleagues at GAP-Optique, University of Geneva, performed a record breaking long distance quantum key distribution experiment using a coherent one-way scheme that uses decoy qubits and a variant of BB84. They successfully distributed the key in a secure manner over 307 km. It took only a few months for the development of the corresponding commercial product, as in October 2015, ID-Quantique introduced a commercial product using the same protocol (cf. Cerberis QKD Blade at ID-Quantique).

While quantum key distribution remains the most popular application of quantum cryptography, potential usefulness has been recognized for other areas, in particular for *distrustful cryptography*. This involves players with conflicting interests who do not necessarily trust one another, unlike in quantum key distribution. The present review will try to cover many such areas, including relativistic quantum cryptography, developed in the last decade since two comprehensive reviews on quantum key distribution done in the previous decade [5, 6].

The present review is arranged as follows. In Section 2, we revisit quantum key distribution, briefly explaining intuitive and rigorous proofs of security, presenting some variants of quantum key distribution going beyond BB84, among them semi-quantum protocols, and touching on the issue of composability, which is relevant for a large-scale implementation of a quantum cryptography. A modification of the quantum key distribution, allowing for secure deterministic communication, and other allied protocols, is discussed in Section 3. In Section 4, we cover the paradigm of counterfactual key distribution, which is based on interaction-free measurements. Subsequently, in Section 5, we discuss the practically important area of device independence, in particular devoting subsections to the issues of side channels, and then five classifications of device independence, namely full, one-sided-, semi-, measurement- and detector-device independence. The formalism of device independence can in principle also be useful in a world where quantum mechanics fails to be valid, being replaced by a non-signaling theory. We also briefly touch upon this, along with the issue of self-testing, in the final subsection. Next, we cover various other issues in cryptography besides quantum key distribution, covering quantum versions for cryptotasks such as random number generation, strong and weak coin tossing, private querying, secret sharing and privacy preserving tasks. Some crypto-tasks not possible in non-relativistic classical cryptography become feasible with the inclusion of relativity or the conjunction of relativity and quantum mechanics. These issues are discussed in Section 7. Technological issues encountered in practical realization of quantum cryptography are discussed in Section 8. After covering continuous variable quantum cryptography in Section 9, we conclude in Section 11.

2 Quantum key distribution

Quantum cryptography was born when S. Wiesner came up with the idea of quantum money in the 1970s, though his paper eventually appeared only in 1983. In 1984, Bennett and Brassard introduced their famous, eponymous four-state protocol BB84 [7], using encoding based on photon polarization. This was seminal in showing how quantum features like uncertainty, impossibility of perfectly discriminating non-orthogonal states and measurement disturbance were 'just what the doctor ordered' as far as secret communication goes. For the first time, it became clear how quantum physical laws can provide unconditional security, impossible classically. Since then, quantum key distribution has progressed tremendously both in theory and practice. For a recent comprehensive review, see [8]. In 1991, Ekert proposed his celebrated E91 cryptographic protocol [9], using Einstein–Podolsky–Rosen pairs (maximally entangled states), where security was linked to the monogamous property of quantum nonlocality [10]. As a result, E91 has sometimes been dubbed 'experimental metaphysics'! Interestingly, it contained the seeds for the concept of device-independent protocols [11], that would be introduced about one-and-half decades later. Bennett's 1992 protocol, which introduced a two-state scheme, showed that two non-orthogonal states are sufficient for quantum cryptography [12]. Shor's efficient quantum algorithms for finding the prime factors of an integer and for the discrete logarithm problem [1] created a huge excitement, optimism and interest among physicists and computer

scientists because of their potential impact on computational complexity, indicating strongly that the quantum computers may prove to be more powerful than their classical counterparts. The factorization algorithm, which is now known as Shor's algorithm, got more attention because it threatened classical cryptography, on account of its potential ability to efficiently crack the RSA cryptographic protocol, which depends on the supposed inability of the classical computers to factorize a large integer in polynomial time.

The Goldenberg–Vaidman protocol [13] shows, intriguingly, that orthogonal states suffice for quantum key distribution. Based on a Mach–Zehnder interferometer architecture, Goldenberg and Vaidman introduced a new paradigm in the foundations of cryptography, where the spatial distribution of a pulse is exploited to obviate the need for non-orthogonality of the signal states to provide security. An experimental realization of Goldenberg–Vaidman protocol was reported by Avella *et al* [14]. Later on, Goldenberg–Vaidman protocol was generalized by various authors [15–21], in which they established that almost all cryptographic tasks that can be performed using a BB84 type conjugate coding based schemes can also be performed using orthogonal state based protocols. Specifically, they showed that it is possible to design orthogonal state based schemes for quantum private comparison, quantum key agreement, quantum key distribution, deterministic secure quantum communication, etc., and that thus conjugate coding is not essential for obtaining unconditional security.

The first ever experimental demonstration of the quantum teleportation phenomenon was reported in 1997 by Zeilinger's group at the University of Vienna, Austria [22], who used the polarization of a photon as a qubit. Quantum teleportation in its original form is cryptographically insecure, but it may be used as a primitive to build schemes for secure quantum communication.

Another new paradigm was introduced in cryptography in 1999 by Guo and Shi who proposed a protocol based on interaction-free measurement [23]. In 2009, this was followed by the Noh protocol [24], which replaces its use of the Mach–Zehnder interferometer with that of a Michelson interferometer. An experimental realization of the Noh protocol was reported by Brida et al. [25].

2.1 Intuitive security

Quantum key distribution is intuitively secure. In BB84, Alice sends Bob a stream of states prepared in the Pauli X or Z basis over an insecure channel. Bob measures them in the X or Z basis randomly. Later over a classical channel, he announces his measurement bases, and Alice informs him which results he can keep. This step, called

basis reconciliation, creates a shared sifted key, wherein Alice and Bob decide to assign bit value '0' to the +1 outcome of X and Z, and bit value '1' to the −1 of the bases. A fraction of this sifted key is publicly announced. If Alice's and Bob's records diverge on too many bits, they abandon the protocol run. Suppose an eavesdropper Eve intervenes by measuring the qubits in the X or Z basis. At the time of key reconciliation, she knows which qubits she measured in the right basis. Suppose Alice and Bob consume m check bits during their final test. The probability that Eve is not detected on a given bit is $\frac{3}{4}$, or $\left(\frac{3}{4}\right)^m$ on all m bits.

A more detailed treatment of the above attack must compare Bob's and Eve's information gain during her attack. Suppose an eavesdropper Eve intervenes by measuring a fraction f of qubits in the X or Z basis. She notes the result, and forwards the measured qubit. The probability that she measures in the right basis, and thus has the right sifted bit, is $\frac{f}{2}$. The error rate she introduces is $e = \frac{f}{4}$, so that the mutual information between Alice and Bob per sifted bit is $I(A : B) = 1 - h(e)$, where $I(A : B) \equiv H(A) + H(B) - H(AB)$, and $h(e) = -(e \log(e) + (1 - e) \log(1 - e))$ is Shannon binary entropy. Eve has more information than Alice, thereby potentially making the channel insecure [26], if Eve's mutual information

$$I(A : E) \equiv \frac{f}{2} = 2e \geq 1 - h(e) \equiv I(A : B), \qquad (1)$$

which happens around 17.05%. Here, it is assumed that Eve retrospectively knows when she measured in the right basis. This is the case if Alice and Bob use pseudo-random number generators for state preparation and measurement, respectively, and Eve is able to crack their pattern based on their public discussion for sifting the raw key. Otherwise, Eve's information would be $f(1 - h(1/4)) = 4e(1 - h(1/4)) \leq I(A:B)$ throughout the range $0 \leq f \leq 1$.

2.2 Unconditional security

More generally, Eve may use sophisticated attacks going beyond the above intercept-resend method. A rigorous proof for security must be able to cover not only general attacks on individual qubits, but also coherent attacks on all qubits, with Eve's final manipulations deferred until after basis reconciliation [27–30].

Here we very briefly review the proof of security of BB84 in the spirit of [29]. At its core are two ideas:

Entanglement distillation [31] via Calderbank–Shor–Steane (CSS) quantum error correcting codes or, more generally, stabilizer codes [32, 33]. This corresponds to privacy amplification at the quantum level.

Monogamy of entanglement [34], the property that if Alice and Bob share singlets with high fidelity, then there is no third party with which Alice's or Bob's particles could be entangled (cf. [30]). More generally, nonlocal no-signaling correlations are known to be monogamous [10].

It is interesting that these proofs, which assume trusted devices, make use of entanglement, which is the appropriate resource for device-independent cryptography (discussed below), but not necessary for security in the scenario of trusted devices. In this case, measurement disturbance and an information vs. disturbance trade-off suffice for guaranteeing unconditional security of key distribution, which is proven in [35].

Regarding the first point above, viz., distillation via stabilizer codes, an important observation is that quantum errors can be digitized into tensor products of Pauli operators—namely bit flips, phase flips and their products—if carefully encoded and the errors are small enough [36, 37], and thereby corrected using a classical-like (if subtler) technique.

Suppose we are given two classical linear error correcting codes $C_1 \equiv [n, k_1]$ and $C_2 \equiv [n, k_2]$ such that $C_2 \subset C_1$ and C_1 and $C_2^\perp$ correct up to t errors on n bits, with code rates k_1/n and k_2/n respectively. Then, there are associated *parity check matrices* H_1 and H_2 pertaining to C_1 and $C_2^\perp$, such that given a code word w in a code that picks up a bit flip error ϵ of weight of at most t, to become $w + \epsilon$, it can be corrected by computing the error syndrome $H_j(w + \epsilon) = H_j(\epsilon)$.

The codes C_j above define a $[n, k_1 - k_2]$ CSS quantum error correcting code, a subspace of $\mathbb{C}^{2^n}$. Given $u \in C_1$, a quantum code word, which is a basis state for the quantum error correcting code, is

$$|u + C_2\rangle = \frac{1}{\sqrt{|C_2|}} \sum_{v \in C_2} |u + v\rangle. \qquad (2)$$

Note that $|u + C_2\rangle = |u' + C_2\rangle$ if $u - u' \in C_2$, so that $|u + C_2\rangle$ only depends on the coset of C_1/C_2 which u is located in, whence the notation of (2) [37]. Under ϵ_b bit flip errors and ϵ_f phase errors, the above transforms to

$$\frac{1}{\sqrt{|C_2|}} \sum_{v \in C_2} (-1)^{(u+v) \cdot \epsilon_f} |u + v + \epsilon_b\rangle, \qquad (3)$$

The error correcting properties of C_1 can be used to correct the ϵ_b Pauli bit flip errors by *incompletely* measuring the quantum operators corresponding to the syndromes. After correcting these bit flip errors, it can be shown that applying a Hadamard transformation $H \equiv \frac{1}{\sqrt{2}}(X + Z)$ to each of the qubits, transforms these qubits to the form

$$\sqrt{\frac{|C_2|}{2^n}} \sum_{w \in C_2^\perp} (-1)^{u.w} |w + \epsilon_f\rangle, \qquad (4)$$

so that the phase flip errors now appear as bit flip errors, which can be corrected using the error correcting properties of the code $C_2^\perp$. We recover the state (2) after application of H to each qubit.

An application of CSS codes is to derive the Gilbert–Varshamov bound for quantum communication, which guarantees the existence of good quantum error correcting codes [29]. For a $[n, k]$ CSS code correcting all errors on at most $t \equiv \delta n$ qubits, the quantum Gilbert–Varshamov bound says that there exist codes in the asymptotic limit such that the code rate k/n is at least $1 - 2h(2t/n)$, while giving protection against t bit errors and t phase errors. Thus, in a protocol, after correction of total errors ($\lesssim 11\%$), Alice and Bob share almost pure singlets hardly correlated with Eve.

The use of CSS codes for distillation can be roughly described as follows. Suppose the channel introduces δn errors, and Alice and Bob encode k Bell states using a $[n, k]$ quantum error correcting code correcting up to this many errors. Alice sends Bob the qubits corresponding to the second particle in the Bell states. Both perform identical syndrome measurements and recovery operations on their own n-qubit halves of the noisy encoded Bell pairs, recovering k pairs of qubits that has a high degree of fidelity with k Bell pairs.

It is important to stress that the man in the middle can affect quantum key distribution as much as it does classical cryptography. This involves Eve impersonating Alice to Bob and Bob to Alice. Perhaps the only protection for quantum key distribution against man in the middle is for Alice and Bob to share a short inital secret (like a pass phrase) for the purpose of person authentication. At the end of the quantum key distribution session, Alice and Bob must store a small portion of the shared key to serve as the pass phrase for the subsequent session. This pass phrase thus serves as a seed that can be grown into the full key, making quantum key distribution as a kind of secret growing protocol [5]. But note that the initial seed must have been exhanged in person or such equivalent direct means.

2.3 Some variants

In 2002, Boström and Felbinger introduced the Pingpong protocol [38] which is a two-state deterministic scheme based on quantum dense coding. To illustrate the conceptual point that entanglement is not required, [39] proposed the non-entangled version of the Pingpong protocol.

In differential phase shift quantum key distribution [40], a single photon, split into three pulses, is transmitted to Bob by Alice. Bob extracts bit information by measuring the phase difference between two sequential pulses by passive differential phase detection. Suitable for fiber-

based transmission, this method offers a superior key generation rate in comparison with fiber-based BB84. The scheme has been extended to the use of weak coherent pulses [41, 42]. Its security against the photon number splitting attack [43] and detailed security, have been studied [44]. A variant of differential phase shift quantum key distribution, called the round-robin differential phase shift protocol [45] has been proposed, in which a guarantee of security is obtained even without any channel noise statistics being monitored. The robustness of round-robin differential phase shift with regard to source flaws has been studied [46]. Recently, round-robin differential phase shift has also been experimentally realized [47, 48].

The introduction of decoy states [49–51] allows implementation of quantum key distribution even with weak coherent pulses instead of single-photon pulses, even in the presence of high loss. Kak [52] introduced a fully quantum scheme in which Alice and Bob share secret bits by exchanging quantum information to and fro in three stages, in contrast to a protocol like BB84, where classical communication is necessary.

A research group from Toshiba Research Europe, UK, demonstrated in 2003 quantum key distribution over optical fibers about 122 km long. The commercial use of quantum technology was initiated by this key effort [53].

Building on ideas first introduced in [54], in [55] quantum key distribution was analyzed under collective attacks in the device independence scenario (discussed below), where devices are not assumed to be trusted or well characterized.

Another direction of research in the security of quantum key distribution is to ask whether it remains secure if only one of the two players is quantum, while the other is classical. Boyer *et al* [56, 57] showed that one obtains a robust security even in this weaker situation. This is of practical relevance, since it places a significantly lesser burden on implementation. An open issue may be to consider how to combine semi-quantum with device-independence (in particular, one-way device-independence, see below).

The South Africa held 2010 Soccer World Cup marks a milestone event for the use of quantum cryptography in a significant public event. Quantum-based encryption was facilitated by the research team led by F. Petruccione, Centre for Quantum Technology, University of KwaZulu-Natal.

The use of free-space quantum communication, rather than fiber-based optics, entered a significant phase when J.-W. Pan's group [58] implemented quantum teleportation over an optical free-space link. Given the low atmospheric absorption under certain wavelength ranges, this can help extend the communication distance in comparison with a fiber link. The same research group further reported [59] the demonstration of entanglement distribution over a free-space link of 100 km, and verifying violation of the Clauser–Horne–Shimony–Holt inequality [60]. The high-fidelity and high-frequency techniques for data acquisition, pointing and tracking in this process pave the way for futuristic satellite-based quantum cryptography.

A scheme for quantum key distribution based on measurement-device independence was proposed in [61]. Its practical advantage over full device independence is that it can tolerate the side-channel attacks and reduced efficiency of the detectors, while doubling the secure distance using just conventional lasers. Other works followed this: phase-encoding for measurement-device independence [62], study of the practical aspects of measurement-device independence such as asymmetric channel transmission and the use of decoys [63], extending secure distance to ultra-long distances using an entangled source in the middle [64], measurement-device-independent quantum key distribution with polarization encoding using commercial devices acquirable off-the-shelf [65].

An experimental satellite-based quantum key distribution system, with satellite transmitters and Earth-based (at Matera Laser Ranging Laboratory, Italy) quantum receivers was implemented with reasonably low noise, namely quantum bit error rate of about 4.6% [66]. Sending quantum messages via a satellite based global network took a further step when in 2016 China launched the $100 million satellite mission named *Quantum Experiments at Space Scale* (QUESS) aka *Micius* (after the ancient philosopher) from the Jiuquan Satellite Launch Center. The mission aims to study the feasibility of quantum cryptography through free-space.

2.4 Semi-quantum protocols

The protocols mentioned so far are completely quantum in the sense that all the users (senders and receivers) need to be able to perform quantum operations (like applying unitaries or measuring in non-commuting bases) in these schemes. By a *quantum user*, we mean a user who can prepare and measure quantum states in the computational basis as well as in one or more superposition bases (say in diagonal basis), whose states are non-orthogonal to the computation basis states. In contrast, a classical user is one who can perform measurement in the computational basis only, has no quantum memory, and who, upon receiving a qubit, can only either measure it in computational basis or reflect it without doing anything.

An interesting question is whether all the users need to be quantum? This important foundational question was first addressed by Boyer et al., [67], where they showed that some of the users can be classical in a scheme called

semi-quantum key distribution. Quite generally, such protocols, where some of the users are allowed to be classical, are called semi-quantum. After the seminal work of Boyer *et al*, several semi-quantum schemes have been proposed [21, 68–72], and their security proofs have been reported [73, 74]. For example, a semi-quantum scheme has recently been proposed for secure direct communication [68], private comparison [21], information splitting [69], and secret sharing [70]. Thus, in brief, most of the cryptographic tasks can be done in semi-quantum fashion, too. This is extremely important as in practical applications end users are often expected to be classical.

2.5 Composability

Universal composability [75] is a general cryptographic framework for protocols that demands security even when protocols are composed with other protocols or other instances of the same protocol. For large-scale applications, clearly composability plays an important role also in quantum cryptography [76]. In the context of quantum key distribution, universal composability specifies additional security criteria that must be fulfilled in order for quantum key distribution to be composed with other tasks to form a larger application. The ultimate goal of security analysis would be to prove composable security against coherent attacks. See [77] for proofs of composable security in the case of discrete-variable quantum key distribution and [78] for continuous-variable quantum key distribution.

The universal composability model entails that a key produced via quantum key distribution is safe to be used in other applications, such as a key to encrypt a message. Unconditional security of quantum key distribution, as conventionally defined, does not automatically preclude a joint attack on quantum key distribution and the message transmission based on the resulting key. Universal composability closes this possible security loophole. As it turns out, the conventional definition of security in quantum key distribution does entail composable security, meaning that a key that is produced in an unconditionally secure way is indeed safe to encode a message with [79].

A relevant example concerns quantum key distribution being sequentially composed in order to generate a continuous stream of secret bits. More generally, the criteria for composability would be more stringent when mutually mistrustful parties are involved. In this context, [80] defines a universally composable security of quantum multi-party computation. [81] invokes the composability of quantum key distribution to obtain hierarchical quantum secret sharing. A composable security has also been defined for quantum crypto-protocols that realizes certain classical two-party tasks [82].

3 Secure deterministic communication

There are several facets of secure quantum communication, which can in principle be derived by composing quantum key distribution and having access to a secure random number generator. In this subsection we aim to provide an interconnection between them [83, 84] via specific examples.

To begin with we describe a scheme for controlled quantum dialogue. There are three users Alice, Bob and Charlie, such that the communication channel between Alice and Bob is supervised by Charlie, who is referred to as controller. Alice and Bob both can send classical information to each other in a secure manner using this quantum channel, which constitutes a quantum dialogue. However, Charlie fully determines whether the channel is available to them both. Further, a requirement of quantum dialogue is that classical communication between Alice and Bob should be transmitted through the same quantum channel and that it should be transmitted simultaneously (namely, there must be a time interval, during which the information of both parties would be in an encoded state in the same channel).

Here, it is important to note that Alice and Bob need to be semi-honest (a semi-honest user strictly follows the protocol, but tries to cheat and/or obtain additional information remaining within the protocol), as otherwise they may create an independent quantum channel of their own and circumvent the control of Charlie. Now, we may briefly describe a simple scheme of controlled quantum dialogue as follows [85]:

Step 1: Charlie prepares n copies of a Bell state, diving them into two n-qubit sequences S_A and S_B, with the first and second halves of the Bell pair, respectively. Then, he transmits both S_A and S_B to Bob, after suitably permuting S_B. It is assumed that all qubit transmissions are secure, with the possible inclusion of decoy qubits, which are inserted to test for an eavesdropper and dropped afterwards [86].

Step 2: Using Pauli operations in the manner of quantum dense coding [37] (whereby I, X, iY, and Z correspond to encoded bit values 00, 01, 10, and 11, respectively), Bob encodes his message in the qubit string S_A, which he then transmits to Alice.

Step 3: After using the same method to encode her secret message, Alice transmits back the sequence S_A to Bob.

Step 4: Charlie reveals the permutation used. On this basis, Bob pairs up the partner particles and measures them in the Bell basis.

Step 5: Bob publicly announces the outcomes of his measurements, which allows each party to extract the other's message using knowledge of her/his own encoding and that of initial Bell state Charlie prepared.

Without Charlie revealing the particular permutation used, semi-honest Alice and Bob cannot decode the other's message, thereby ensuring Charlie's control. Moreover, just before step 4, both Alice and Bob's messages are encoded at the same time in the channel, which ensures satisfaction of the quantum dialogue requirement.

Charlie's choice of Bell state, if publicly known, would lead to information leakage, which is often considered to be an inherent feature of quantum dialogue and variants thereof. This problem can be eliminated if Charlie chooses his Bell state randomly, informing Alice and Bob of his choice via quantum secure direct communication or deterministic secure quantum communication [87].

The above scheme can be turned into other cryptotasks. If Bob, instead of Charlie, prepares the Bell states initially (with the difference of Charlie's announcement being absent in step 4), then the above scheme reduces to quantum dialogue, of the type introduced at first by Ba An [88]. This is called the Ba An protocol for quantum dialogue.

Likewise, a quantum dialogue scheme can always be obtained from a controlled quantum dialogue scheme. Further, in a quantum dialogue scheme, restricting one of the players, e.g., Alice, to trivial encoding (namely, simply applying Pauli I operation), we obtain a protocol for quantum secure direct communication, whereby Bob can communicate a message to Alice without the prior distribution of a key. In this way, any quantum dialogue can be turned into that for quantum secure direct communication. In quantum secure direct communication, a meaningful message is typically sent by the sender. Instead, transmission of a random key turns quantum secure direct communication into a quantum key distribution. Therefore, any quantum secure direct communication protocol can be turned into a quantum key distribution protocol [83].

Likewise, suppose that in a quantum dialogue scheme, Alice (resp., Bob) transmits key k_A (resp., k_B) to Bob (resp., Alice), after which they adopt $K = k_A \oplus k_B$ as the secret key for future communication, this constitutes a protocol for quantum key agreement, in which each player contributes equally to K, such that each bit of K cannot be unilaterally determined by either player. In this way, a quantum key agreement scheme can always be obtained from that for quantum dialogue. Also, in asymmetric quantum dialogue [87], a special case of the quantum dialogue scheme, involves Alice and Bob encoding an unequal amount of information (say, Alice sending m bits, and Bob sending $2m$ bits).

Other types of reduction are possible. In the above scheme for controlled quantum dialogue, suppose Charlie retains sequence S_B and only transmits S_A securely to Alice, who encodes her secret message using the dense coding method and then transmits the resultant qubit string to Bob. Upon reception, Bob encodes his secret using the same rule and sends the resultant sequence to Charlie, who finally measures each received particle with its partner particle retained by him, in the Bell basis. If in each case, he obtains the original Bell state, the Alice's and Bob's secrets are identical. This follows simply from the fact that $I = XX = (iY)(iY) = ZZ = I_2 I_2$, ensuring that two encoded messages are identical, then the travel qubits return as they left.

Therefore, a quantum dialogue or controlled quantum dialogue scheme can always be turned into one for quantum private comparison, which allows a third party to compare the secrets of two parties without being able to know their secrets [21]. This quantum private comparison is suitable for the socialist millionaire problem or Tierce problem [89], which is a secure two-party computation requiring two millionaires to find out if they are equally rich, without revealing how rich each is (unless of course they are equally rich). In brief, a modification of quantum dialogue or controlled quantum dialogue provides a solution for quantum private comparison, the socialist millionaire problem and a few other related problems.

Just as a quantum dialogue protocol can be turned into a quantum secure direct communication one, a controlled quantum dialogue protocol can be turned into one for controlled quantum secure direct communication (technically, actually one for controlled deterministic secure quantum communication). Now, controlled deterministic secure quantum communication can be used in a quantum e-commerce situation, where Charlie represents a bank, Alice a buyer and Bob an online shop. To make a purchase, Alice intimates Charlie, who executes step 1 above. Next, Alice encodes her purchase information in S_A, which she sends to Bob, who in turn informs Charlie of having received an order worth a specific amount from a certain buyer, whose identity is verified by Charlie, who then reveals the relevant permutation operation. Bob then performs Bell measurement and knows about Alice's order. Therefore, a quantum e-commerce protocol of this type is really a straightforward modification of a controlled quantum secure direct communication scheme.

In fact, in the recent past several schemes of quantum e-commerce and other similar applications of quantum cryptography have been proposed by various groups [90, 91], that have established that quantum cryptography can be used for various practical tasks beyond key

distribution and secure direct communication. Specifically, sealed-bid auctions [92–94] and other variants of auctioning (e.g., English and Dutch auctions) can be performed using quantum resources [95,96]. Binary voting can also be performed using quantum resources (cf. [97] and references therein).

4 Counterfactual quantum cryptography

Counterfactual quantum communication transmits information using the non-travel of a photon between Alice and Bob [98–101]. It is based on interaction-free measurement [23, 102, 103], where the presence of an object is detected without directly interrogating it. Famously known as the Elitzur–Vaidman scheme for bomb detection, it involves photon interferometery used to ascertain the presence of a quantum object in one of the arms without the photon actually passing through it. The single-photon injected into the beamspliiter of this set-up always exits one particular output port labelled as the bright port. The presence of an object in one of the arms of the interferometer permits the single photon to exit not from the bright port, but through the port that is otherwise dark.

Experimental realizations proved that indeed such interaction-free measurements are possible [103]. Further, a proposal to enhance its efficiency towards 100% using chained unbalanced beamsplitters, wherein repeated measurements of the initial state in order to arrest evolution, simulating the quantum Zeno effect, was put forth. The scheme works as follows: A single-photon incident on a beamspliiter after M cycles exits from the bright port but the presence of a detector in these ports restricts the photon to be always in the lower arm and exit from the dark port. The chained action leads to the evolution:

$$|\texttt{block}\rangle|0\rangle \rightarrow \cos^M \eta|\texttt{block}\rangle|0\rangle$$
$$|\texttt{pass}\rangle|1\rangle \rightarrow (\cos(M\eta)|0\rangle + \sin(M\eta)|1\rangle) \quad (5)$$

where M is the number of interferometric cycles, and the first equation indicates absorption at the obstacle. In 2009, Noh proposed the well-known counterfactual quantum protocol for cryptography [24].

Though counterfactual quantum cryptography may not be so useful for long-distance communication, it is interesting conceptually [104, 105]. Schemes to improve the efficiency of counterfactual quantum key distribution protocols [106, 107], security analysis of such schemes under various attacks such as intercept-resend and counterfactual attacks [108–110], experimental realisation using different set-ups [25, 111, 112], direct communication protocols [113] and counterfactual generation and distribution

of entanglement [114] have contributed towards better understanding of applying counterfactuality. The basic idea of the direct communication protocol is to ensure counterfactual transfer of information using the chained beamsplitter approach mentioned earlier. M-chained unbalanced beamsplitters are nested within N-chained outer unbalanced beamsplitters. By suitably choosing M and N, one can achieve direct communication between Alice and Bob. It has been further argued that this is fully counterfactual [115], an interpretation that has been debated. For an alternative perspective, see [116, 117], but also [118, 119]. Recently, the proposal in [115] for direct counterfactual communication has been implemented experimentally [120].

By letting the obstacle to be in a superposition state, as follows:

$$(\alpha|\texttt{block}\rangle + \beta|\texttt{pass}\rangle)|0\rangle \rightarrow \alpha \cos^M \eta|\texttt{block}\rangle|0\rangle$$
$$+ \beta|\texttt{pass}\rangle(\cos(M\eta)|0\rangle + \sin(M\eta)|1\rangle)$$
$$\rightarrow \alpha|\texttt{block}\rangle|0\rangle + \beta|\texttt{pass}\rangle|1\rangle \quad (6)$$

An idea along this line can be used to counterfactually transmit a qubit, as against a bit [121–123].

The well-known counterfactual protocol Noh09 [24] is briefly explained here. Alice and Bob are connected to each other through one of the arms of a Michelson interferometer (arm B). The other arm A is internal to Alice's station and is inaccessible to the outside world. A photon traveling along arm A is always reflected using a Faraday mirror (M_1). In addition, Alice is also equipped with a single-photon source which prepares polarization states in the vertical (V) or horizontal (H) direction, based on the output of a quantum random number generator (a). Bob's station also consists a quantum random number generator (b) whose output decides whether a reflection using Faraday mirror (M_2) or a detection using a detector D_B is to be applied. R_B controls a switch Q whose polarization state P (pass V and block H) or B (block V and pass H) determines which of the above operations is to be applied. The protocol is as follows (cf. Figure 1):

1. Alice prepares polarization states randomly in V or H states based on a and transmits it to Bob.

2. Bob applies P or B randomly based on b. The following table gives the conditional probabilities based on Alice and Bob's joint action:

(Alice,Bob)	D_1	D_2	D_B
(V, P) or (H, B)	0	1	0
(V, B) or (H, P)	RT	R^2	T

D_1 and D_2 are detectors in Alice's station. R and T are the coefficient of reflectance and transmittance of the beamsplitter respectively such that $R + T = 1$.

3. At the end, D_1 detections lead to the generation of secret key and D_2 detections are used for detecting eavesdropping. D_1 detection is counterfactual in the sense that the photon did not travel to Bob and his blocking action leads to a remote detection by Alice. In some sense, the photon takes into account Bob's choices before detection.

Future directions here could explore applying the counterfactual paradigm to other crypto-tasks besides quantum key distribution.

5 Device independent scenarios

We already noted that a classical cryptographic protocol is secure only under some assumptions about the hardness of performing some computational tasks. In contrast, BB84, B92 and other protocols for quantum key distribution, mentioned above, are unconditionally secure in the sense that their security proof is not based on such computational assumptions, but instead is guaranteed by quantum physical laws.

However, the security proofs assume that the practical realization is faithful to the theoretical specifications, and that the devices used by Alice and Bob are trusted and that the duo have perfect control over the devices used for the preparation of the quantum states, manipulation and their measurement. Devices are also assumed to be free from any side channels that would leak secret information from the laboratories of Alice and Bob.

5.1 Side-channel attacks

Quantum key-distribution promises unconditional security under the assumption of perfect implementation of the protocols in the real-world. But, imperfections in the experimental set-up creates side-channels that can be employed by a malicious eavesdropper to compromise the security without the knowledge of the legitimate participants Alice and Bob. Side-channel attack allows Eve to gain information based on certain behavioural patterns of the devices used for key-distribution and does not depend upon the theoretical security [124].

Some examples of side-channels are detector clicks, dark counts and recovery time of the detectors, electromagnetic leaks. Sometimes the side-channel attacks are so powerful that the basis information may be leaked and render the protocol completely insecure. Such side-channel attacks identified [125, 126] the danger posed by not being able to completely characterise sources and detectors, leading to the device-independent paradigm [127].

Here, we list some powerful quantum hacking attacks and countermeasures on commercial quantum key distribution systems:

- Time-shift attacks, which make use of the detection efficiency loophole, which plays a key role in the Bell inequality tests [128]. Here we may count bright illumination pulses to control single-photon avalanche photodetectors [129], passive detector side channel attacks [130] and detector blinding attacks. In particular, information leakage due to the secondary photo-emission of a single photon avalanche detector can be countered by backflash light characterization [131].

- Time side channel attack where the timing information revealed during the public communication during Alice and Bob is used to extract some parts of the secret key [132].

- Optical side-channel attacks in order to gain information about the internal states being propagated in the channel [133].

- Source attacks based on tampering of the photon sources in the measurement device-independent paradigm [134].

- Preventing side-channel attacks in continuous-variable quantum key distribution by modulating the source signal appropriately to compensate for a lossy channel [135].

5.2 Device-independence

The practical realization of an otherwise unconditionally secure quantum key distribution protocol will involve the use of untrusted devices [136], whose imperfections may be exploited by a malicious eavesdropper to undermine its security. In 1998, Mayers and Yao [137] introduced the concept of quantum cryptography with the guarantee of security based only on the passing by the measurement data of certain statistical tests, under the assumptions of validity of quantum mechanics and the physical isolation (no information leakage) of Alice's and Bob's devices; in other words, a quantum key distribution set-up that can self-test.

In [54], it was shown how a single random bit can be securely distributed in the presence of a non-signalling—not just quantum—eavesdropper. This qualitative argument was made quantitative by several following works, providing efficient protocols against individual attacks [138, 139], and subsequently collective attacks [140–142] against a non-signaling eavesdropper. Better key rates, but assuming an eavesdropper constrained by quantum
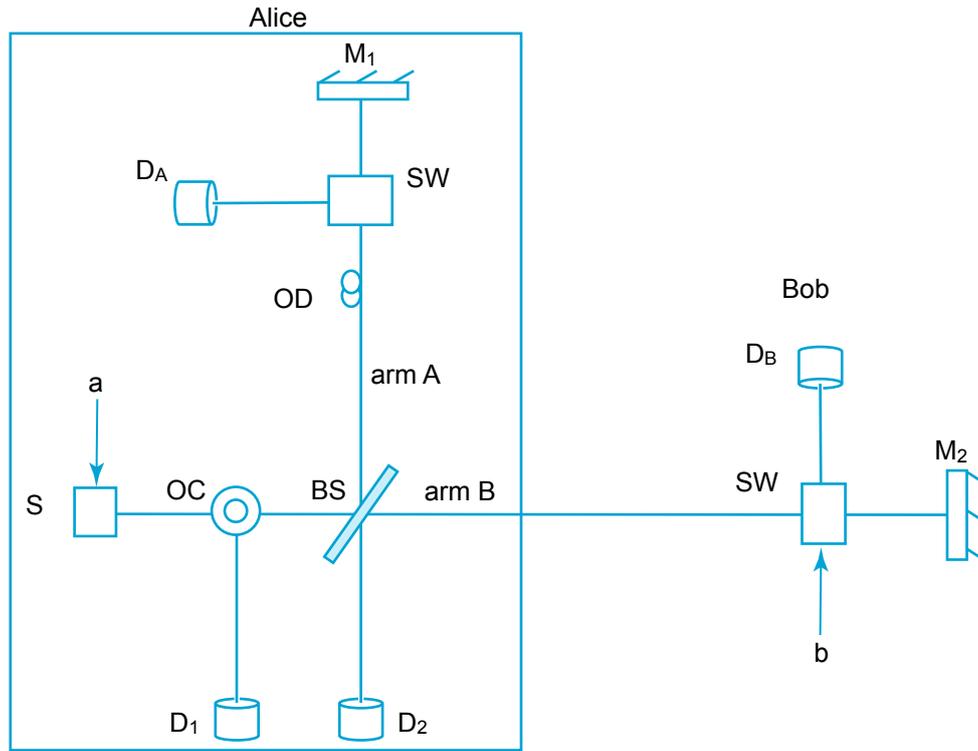
Figure 1: *Basic set-up for counterfactual [24] or semi-counterfactual [104] quantum key distribution based on a Mach–Zehnder interferometer. Alice's station consisting of the source (S) initiates the protocol by sending light pulses through the optical circulator (OC) to the beamsplitter (BS), which splits them into beams along arms A and B. The optical delay (OD) maintains the phase between the arm by compensating for the path difference in the two arms. Light along arm A is subjected to absorption by detector D_A or reflection from mirror M_1 by Alice based on her switch (SW) state. Likewise by Bob along arm B who also possesses a switch (SW), a detector D_B and a mirror M_2.*

laws, are reported in [55, 143, 144]. All these proofs of security require an independence assumption, namely that successive measurements performed on the devices commute with each other [144]. While [145] fixes this issue, by allowing Alice and Bob to use just one device each, it is inefficient and lacks noise tolerance. The device-independent protocol of [146] reports an improvement guaranteeing the generation of a linear key rate even with devices subject to a constant noise rate, but relaxing other assumptions such as the availability of several independent pairs of devices.

We briefly mention the connection of device independence and nonlocality. A necessary condition in order to guarantee security in the scenario where devices are not assumed to be trustworthy—characteristic of the device-independent scenario—is that Alice's and Bob's joint correlation $P(x, y|a, b)$, where a, b are the respective inputs and x, y their respective outputs, must be such that

$$P(x, y|a, b) \neq \sum_{\lambda} P(x|a, \lambda)P(y|b, \lambda)P_{\lambda}, \qquad (7)$$

where $P(x|a, \lambda)$ and $P(y|b, \lambda)$ are arbitrary probability distributions for Alice and Bob; and P_{λ} is the probability distribution of some underlying variable λ. For if this were not so, then in principle, knowing λ, Eve would be able to determine the outcomes of Alice and Bob, when they announce a and b publicly during the key reconciliation step. This entails that $P(x, y|a, b)$ must be nonlocal, namely it should violate a Bell-type inequality, making the sharing of quantum entanglement necessary.

Other than this, the quantum apparatuses used by Alice and Bob are viewed as black boxes, with no assumption made about the internal workings. Interestingly, the root concept for device-independent quantum key distribution was implicit as early as 1991 in the E91 protocol [9], but its true significance was not recognized before the advent of the study into device-independent cryptography. Because the security of any device-independent scheme requires nonlocal correlations, which is in practice an expensive and delicate resource, it would be difficult to achieve full device independence. For example, the detector efficiencies are usually too low to support full device-independent security. Although the hope for practical realization of device-independent quantum key distribution has been raised by recent loophole-free Bell experiments [2, 147, 148], the secure key rates are expected to be quite low even for short distances.

Although we have generally talked of quantum key distribution in the context of device independence, other tasks can also be considered in this framework, among them self-testing of the *W* state [149]

$$W \equiv \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$$

and that of any two projective observables of a qubit [150], have been reported.

Of interest here is the device-independent quantum key distribution protocol based on a local Bell test [151]. Several relaxed variants of device-independent quantum key distribution idea (including semi-device-independent and one-way device-independent) have been proposed [61, 152–155] and are briefly discussed below.

5.3 Measurement-device independence

A more feasible solution than device-independent quantum key distribution is the measurement-device-independent quantum key distribution [61] scheme, which builds on [156, 157]. Using weak coherent light pulses along with decoy states, the measurement-device-independent quantum key distribution protocol is made immune to all side-channel attacks on the measurement device, often the most vulnerable part. However, it is assumed in measurement-device-independent quantum key distribution that Eve cannot access state preparation by Alice and Bob. The security of measurement-device-independent quantum key distribution against general coherent attacks, exploiting the effect of finite data size, has been proven in [158]. In this context, see [124], which proposes using quantum memory and entanglement to replace all real channels in a quantum key distribution protocol with side-channel-free virtual counterparts.

Measurement-device-independent quantum key distribution, in contrast to a full device-independent scheme, requires neither almost perfect detectors nor a qubit amplifier nor a measurement of photon number using quantum non-demolition measurement techniques [61, 159]; also cf. related references cited in Section 2. The most recent developments of the measurement-device-independent quantum key distribution scenario, including its strengths, assumptions and weaknesses are reviewed in [159].

The basic idea behind measurement-device independence is that Alice and Bob transmit weak coherent pulses representing randomized BB84 polarization states to a central untrusted Bell state measurement station, manned by Charlie or even Eve. The probabilistic production of Bell states can be shown to lead to a secure bits, even if the untrusted station uses only linear optics.

Measurement-device-independent schemes have been experimentally realized by various groups [65, 160, 161].

It has even been demonstrated through a distance over 200 km, whereas a full device-independent scheme is yet to be realized experimentally. For discrete-variable measurement-device-independent quantum key distribution, the key rate for practical distances turns out to be just 2 orders of magnitude below the Takeoka–Guha–Wilde bound [162], enabling this method to meet the high speed demand in metropolitan networks.

5.4 Detector-device-independence

Whereas the key rate of measurement-device-independent quantum key distribution scales linearly with transmittance of the channel (just as with conventional quantum key distribution), it has the drawback that its key rate scales quadratically (rather than linearly, as in conventional quantum key distribution) with detector efficiency [8], which can be a practical problem if detectors of sufficiently high efficiency are not available. Detector-device-independent quantum key distribution aims to combine the efficiency of the conventional quantum key distribution protocols with the security of measurement-device-independent quantum key distribution [163, 164]. In detector-device-independent quantum key distribution, receiver Bob decodes photon information from an insecure channel using a trusted linear optics, followed by a Bell state measurement with untrusted detectors.

The advantage of detector-device-independent quantum key distribution over measurement-device-independent quantum key distribution is that key rate scales linearly (rather than quadratically) with detector efficiency, essentially because it replaces the two-photon Bell state measurement scheme of measurement-device-independent quantum key distribution with a single-photon Bell state measurement scheme [165]. (In a single-photon Bell state, spatial and polarization modes—each representing a bit—are entangled.) However, the security of detector-device-independent quantum key distribution against all detector side-challels remains yet to be shown. It is known [166] that either countermeasures to certain Trojan horse attacks [167] or some trustworthiness to the Bell state measurement device is required to guarantee the security of detector-device-independent quantum key distribution (as against the strong security of measurement-device-independent quantum key distribution, where such assumptions are not needed.) Indeed, a simple implementation of a detector-device-independent quantum key distribution protocol can be built directly on the standard phase-encoding-based BB84 quantum key distribution [168].

5.5 One-sided device-independence

Further, violation of Bell's inequality or equivalently the use of a Bell nonlocal state can ensure the security of a device-independent quantum key distribution mentioned above, but if one of the users (Alice or Bob) trusts her/his devices then we obtain a weakening of device-independent quantum key distribution, known as one-sided device-independent quantum key distribution [152], whose security does not require the violation of Bell's inequality, but rather a weaker type of nonlocality, namely quantum steerability.

The condition (7) is symmetric between Alice and Bob. Now suppose $P(x, y|a, b)$ satisfies the asymmetric but weaker condition [169]:

$$P(x, y|a, b) \neq \sum_\lambda P(x|a, \lambda) P^Q(y|b, \lambda) P_\lambda, \qquad (8)$$

where $P^Q(y|b, \lambda)$ is any quantumly realizable probability distribution for Bob. Such a state is said to be steerable, and can be pointed out by the violation of a steering inequality. Steering is a stronger condition than nonseparability, but weaker than nonlocality.

C. Branciard et al [152] first studied the security and practicability of one-sided device-independent quantum key distribution, which belongs to a scenario intermediate between device-independent quantum key distribution and standard quantum key distribution. This makes it more applicable to practical situations than the latter. Just as a sufficient violation of a Bell-type inequality is necessary to establish device-independent quantum key distribution, so a demonstration of steering is necessary for security in the one-sided device-independent quantum key distribution scenario.

It may be noted that the prepare-and-measure schemes of quantum key distribution that do not use entangled states (e.g., BB84 and B92 protocols) can also be turned into entanglement-based equivalents, from which we can obtain their device-independent counterparts by employing suitable Bell-type inequalities. For example, M. Lucamarini et al [170] presented a device-independent version of a modified B92 protocol. T. Gehring et al [171] reported an experimental realization of continuous-variable quantum key distribution with composable and one-sided device-independent security against coherent attacks. A one-sided device-independent implementation of continuous-variable quantum key distribution has been experimentally implemented, wherein the key rate is directly linked to the violation of the Einstein–Podolsky–Rosen steering inequality relevant to the context [172].

Here it would be apt to note that for pure states, entanglement, steering and nonlocality are equivalent. However, for mixed states they are different and all Bell nonlocal states are steerable, and all steerable states are entangled, but not the other way in each case, namely entanglement is the weakest and nonlocality the strongest nonclassicality condition among these.

5.6 Semi-device independence

In quantum mechanics, an entangled measurement is represented by an operator, at least one of whose eigenstates corresponds to an entangled state. In the *semi-device-independent* approach [173], one can certify that the measurement is indeed entangled on basis of the measurement statistics alone, provided it can be assumed that the states prepared for testing the measurement apparatus are of fixed Hilbert space dimension, even if uncharacterized otherwise. This approach has been applied to other quantum information processing tasks, among them cryptography [154].

Now, it is possible to test the dimension of a physical system in a device-independent manner, namely on basis of measurement outcomes alone, without requiring the devices to be characterized, by means of Bell inequalities [174, 175] or bounds pertaining to quantum random access codes [176]. More recently, the semi-device-independent approach has been applied to estimate classical and quantum dimensions for systems in a prepare-and-measure setup [177, 178]. Experimental realization of these ideas have been reported [179, 180], as well as their application to cryptography [154] and random number generation [181, 182].

For prepare-and-measure protocols in quantum information processing, since quantum nonlocality is out of question, a more natural notion of device independence applicable is the semi-device-independent scenario. This uses the notion of bounding the classical or quantum dimension required to reproduce the observed quantum correlations by measurements on transmitted particles prepared in specific states [177, 183]. Let

$$P(y|\alpha, b) = \text{Tr}(\rho_\alpha \Pi_b^y) \qquad (9)$$

denote Bob's probability for getting outcome y given measurement b acting on state ρ_α transmitted by Alice, with Π_b^y being the corresponding quantum mechanical measurement operator.

A dimension witness for the prepare-and-measure scenario has the form

$$\sum_{\alpha, b, y} f_{\alpha, b, y} P(y|\alpha, b) \leq C_d, \qquad (10)$$

where $f_{\alpha, b, y}$ are a set of real numbers and C_d is a positive real number. Violation of (10) would mean that no classical particle of dimension d could have generated the observed experimental correlation $P(y|\alpha, b)$. More generally,

one can bound the quantum dimension, also [177]. This violation serves as the basis for semi-device-independent security, just as violation of a Bell inequality serves as the basis for device-independent security.

In [155] a semi-device-independent version of BB84 protocol has been presented using the notion of semi-device-independence introduced in [154]. Similar device-independent and semi-device-independent generalizations of other protocols are also possible, and a general prescription for the same is a problem worth exploring.

5.7 Security in a post-quantum world

There is an intrinsic and quite reasonable assumption in the security proof of all the above protocols on the validity of quantum mechanics. What would happen to the keys if the nature is found to obey a theory other than quantum mechanics? It turns out that so long as a theory admits a no-cloning theorem, then (possibly assuming trusted devices) security is possible [184], whereas device-independent security would be possible if it is a nonlocal non-signaling theory. In fact, the concept of device independence can be adapted to provide security against even a post-quantum Eve constrained, assuming only the no-signaling principle [54, 185].

6 Further applications of quantum cryptography

We shall now survey various crypto-tasks other than quantum key distribution for which quantum cryptographic schemes have been proposed.

6.1 Quantum random number generation

Apart from key distribution, current levels of quantum technology suffice for providing a good source of genuine randomness, which is important for cryptography and in algorithms for simulation. As noted above, quantum random number generators are available commercially now. By *genuinely random* we refer to a source whose output is unpredictable and irreproducible according to known physical laws. This stands in contrast to pseudo-random number generator, which generates strings which are predetermined according to a deterministic algorithm. One may then hope that the numbers produced by a pseudo-random number generator are distributed indistinguishably from a uniform probability distribution. The robustness of pseudo-random number generators is an issue that would merit careful consideration [186].

From the perspective of algorithmic information theory, genuinely random strings are incompressible, namely their Kolmogorov complexity is not smaller than the string's length [187], whereas pseudo-randomness is algorithmically compressible. Kolmogorov complexity of string S refers to the length in bits of the shortest computer program (in a given programming language) that generates S as its output. However, in general, randomness cannot be proven because Kolmogorov complexity is uncomputable. For practical purposes, the randomness of given data may be evaluated by running the data through standard statistical tests for random number generators, such as the suite provided by the National Institute for Standards and Testing [188].

The most straightforward quantum random number generator exploits the randomness of outcomes in quantum measurements, for example, by reading off the output of a 50/50 beam splitter [189–191]. Other sources of randomness include single photon arrival times [192–195], a laser's phase noise [196–198] and vacuum fluctuations [199, 200]. Mobile phone cameras provide a good, if classical, source of randomness [201].

An important issue here is to estimate the entropy of the randomness source, namely the raw random bits generated, from which truly random bits can be extracted [202]. Sophisticated techniques have been developed to estimate entropy in specific cases [203, 204]. However, these methods are somewhat difficult to implement and do not easily lend themselves to generalization nor to easy real-time monitoring. Device-independent quantum random number generator provides a possible solution [205, 206], which makes use of suitable tests of violation of a Bell-type inequality [206, 207], making them however not so simple to implement in practice as a basis for a quantum random number generator.

Semi-device-independent certification of randomness [182] is simpler, but not entirely free from loopholes in practice [208]. A method based on the uncertainty principle, but requiring a fully characterized measurement device, has recently been proposed [209]. As an improvement, Lunghi *et al* [210] have proposed a self-testing prepare-and-measure quantum random number generator protocol based on measuring a pair of incompatible quantum observables.

The incompatibility, and consequently the amount of genuine randomness, can be quantified directly from the experimental data. These authors have also reported a practical implementation using a single-photon source and fiber optical communication channel, through which they report a 23-bit throughput of genuine randomness at 99% confidence level [210] .

6.2 Quantum secret sharing

Secret sharing is a crypto-task where a dealer splits a secret into two or more shares and distributes them among multiple agents such that only designated groups of agents (who define an access structure) can reconstruct the full secret.

Secret sharing is a cryptographic primitive used widely to design schemes for digital signature, key management, secure multiparty computation, etc. Classical secret sharing, first proposed independently by Shamir and Blakely, makes certain computational assumptions about complexity, making its security computational rather than unconditional. Quantum mechanics has given grounds for hope here [211, 212]. The original proposal for quantum secret sharing [211] distributes a 3-qubit state among three participants:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$
$$= \frac{1}{2}(|+++\rangle + |--+\rangle + |-+-\rangle + |+--\rangle) \quad (11)$$

The three parties measure in X or Z basis. On a quarter of the time (that may be established by classical communication), all three would have been measured in the same basis, and it is clear from Eq. (11) that Bob and Charlie can reconstruct Alice's bit (designated the secret) by combining their results. Any attempt by a third party to find out the secret disrupts the correlation, which can be detected by the legitimate parties by announcing full outcomes in some trial runs. Another important aspect to be considered is that one or more of the participants themselves could be colluding to cheat. A full proof of security must also consider such player collusion scenarios.

An extension of the above is a quantum (N, k) threshold scheme, where a quantum secret, split among N parties, can be reconstructed only if at least k parties combine their shares. The no-cloning theorem implies that $2k > N$. Threshold schemes have similarities with quantum error correcting codes [213]. Generalizations of quantum secret sharing to more general access structures [214, 215] and the use of various relatively easily prepared quantum states beyond the Greenberger–Horne–Zeilinger states [216] have been studied, as well as their use in the related task of quantum information splitting [217, 218].

The concept of quantum secret sharing has been further generalized in various ways, among them: hierarchical quantum secret sharing [219], hierachical dynamic quantum secret sharing [81]. Further, in a recent direction [220], quantum secret sharing based on a d-level particle (with d being an odd-prime in order to exploit the cyclic property of the $d + 1$ mutually unbiased bases in these dimensions), rather than entanglement, has been studied. Suppose the vector in this system is denoted $\Psi_{j;k}$, where j is the basis and k the index of the vector in that basis. The generalizations of the qubit Pauli operators, denoted X_d and Y_d, are defined by the actions

$$X_d : \Psi_{j;k} \to \Psi_{j;k+1}$$
$$Y_d : \Psi_{j;k} \to \Psi_{j+1;k}, \quad (12)$$

where additions are in modulo d arithmetic. Each of the N participants, denoted $n \in \{0, 1, 2, \cdots, N\}$, with the 0th player being the secret dealer, applies the operation $X_d^{x_n} Y_d^{y_n}$ to the sequentially transmitted qudit, where $x_n, y_n \in \{0, 1, \cdots, d - 1\}$ are private data held by the nth player. The dealer measures in a random basis Ξ to obtain outcome ξ. Through public announcement, the players verify whether $\sum_{j=0}^{n} y_n = \Xi$ (which happens with probability $1/d$) and reject the round if not. If not rejected, then the protocol guarantees the perfect correlations

$$\sum_{n=0}^{N} x_n = \xi, \quad (13)$$

which provides a basis for sharing a secret via a (N, N) threshold scheme [220]. Over multiple rounds of the protocol, the players can test for departure from (13), which can be used to upper-bound eavesdropping. For details on security against eavesdropping and or a collusional attack on the scheme, see [220].

6.3 Strong and weak quantum coin tossing

Suppose Alice and Bob are getting divorced. Coin tossing is a crypto-task suitable to divide their assets randomly. Perfect coin tossing is a primitive for Mental Poker [221]. Classically, (non-relativistic) coin tossing is based on computational complexity [222], whereas relativistic classical coin tossing involves Alice and Bob sending each other messages with sufficient simultaneity as to ensure the independence of their messages (see Section 7).

A crypto-task closely related to coin tossing is bit commitment, serves as a primitive for other tasks such as zero-knowledge proofs [223]. Bit commitment requires Alice to commit to a bit a by submitting an evidence to Bob. Later, she unveils a. During the holding phase between commitment and unveiling, the evidence must bind Alice while hiding a from Bob. Quantum coin tossing can be built on top of quantum bit commitment: Alice commits to a bit a; Bob publicly announces bit b; Alice unveils a. The toss is $a + b \mod 2$. However, an unconditionally secure bit commitment protocol cannot be constructed via calls to a secure coin tossing black box, even given additional finite classical or quantum communication between Alice and Bob, making bit commitment strictly stronger than coin tossing in the standard cryptographic framework [224].

It is conventionally believed that (nonrelativistic) quantum bit commitment is not secure, owing to an entanglement-based attack uncovered by Mayers, Lo and Chau (MLC) [225–227], described briefly below. For a similar reason, the impossibility of quantum coin tossing is also accepted to hold generally [228]. Similar no-go arguments exist for the impossibility of ideal coin flipping, oblivious transfer and secure two-party computation.

The MLC argument can be cast as follows. In a quantum bit commitment protocol, suppose ρ_a, with $a \in \{0, 1\}$, denotes the density operator of the evidence of commitment to bit a that Alice submits to Bob. To be concealing to Bob, we require

$$\rho_0 \simeq \rho_1. \qquad (14)$$

Mixed states can always be purified by going to a larger Hilbert space. In this case, the purifications of ρ_a must correspond to Schmidt decompositions with the same Schmidt coefficients, say ξ_j. We associate two of these purifications with the states associated with Alice's commitment

$$|\Psi_0\rangle = \sum_j \sqrt{\xi_j} |\alpha_j^A\rangle |\beta_j\rangle,$$

$$|\Psi_1\rangle = \sum_j \sqrt{\xi_j} |\alpha_j^{A'}\rangle |\beta_j\rangle, \qquad (15)$$

where $|\beta_j\rangle$ are eigenstates of $\rho_0 = \rho_1$, while the states $|\alpha_j^A\rangle$ and $|\alpha_j^{A'}\rangle$ are orthogonal basis states. Alice can cheat because she only requires a local rotation, connecting these two bases. She can use this local unitary to switch her commitment between $|\Psi_0\rangle$ and $|\Psi_1\rangle$ at the time of unveiling. This no-go result is an application of the Hughston–Jozsa–Wootters theorem [229], which shows that any two ensembles with Bob having the same density operator, can be prepared remotely by Alice, who holds the second system that purifies Bob's state.

It may be noted that various authors have questioned the generality of the cryptographic framework used to derive the standard no-go theorem for quantum bit commitment [230–235].

For the most part, the MLC result has motivated research in certain directions deviating from ideal quantum bit commitment, among them bit string commitment [236], where Alice securely commits n bits such that recipient Bob can extract at most $m < n$ of these bits; a weaker form of bit commitment, namely cheat-sensitive bit commitment, where the condition (14) is relaxed to $\rho_0 \neq \rho_1$. Here, if either party cheats, then the other party has a non-vanishing probability for cheat detection [237] (but see [238]). Note that even cheat sensitive bit commitment is classically impossible.

Likewise, weaker versions of quantum coin tossing beyond ideal quantum coin tossing have been studied. Here,

one can distinguish between weak and strong flavors of coin tossing. In strong coin tossing, the coin toss must be perfectly random. This is the requirement of correctness. In weak coin tossing, it is known that the two parties want opposite outcomes, e.g., Alice wants 'heads' whereas Bob 'tails'. Then the coin tossing protocol need not protect against Alice biasing the outcome towards 'tails' and Bob towards 'heads'. Strong coin tossing is required when the bit preferred by the other party is not known or their preferences clash.

The requirements for a (strong) quantum coin tossing protocol:

Correctness. If both parties play honestly, then both outcomes of the coin are equal, namely $P(t = 0) = P(t = 1) = \frac{1}{2}$, where t is the toss outcome.

Bounded bias. If Bob is honest but Alice is not, then $P_A(t) \leq \frac{1}{2} + \epsilon_A$, where ϵ_A is her bias. Analogously for honest Alice and dishonest Bob, $P_B(t) \leq \frac{1}{2} + \epsilon_B$.

The protocol's bias is ϵ, defined as the maximum of ϵ_j for $j \in \{A, B\}$. In an ideal quantum coin tossing, $\epsilon_j = 0$. Quantum coin tossing can be based on quantum bit commitment [239] or entanglement-based [240].

Quantum coin tossing is known to offer an advantage over classical coin tossing in that quantum coin tossing can guarantee a cheating probability strictly lower than 1, which is impossible in a non-relativistic classical coin tossing scheme. Quantum coin tossing protocols with bias ϵ lower than half have been proposed [239, 241–243].

Kitaev [244] found that a bias lower than $\frac{1}{\sqrt{2}} - \frac{1}{2} \approx 0.207$ cannot be achieved by a fair (one where $\epsilon_A = \epsilon_B$) quantum coin tossing protocol, a bound that has been demonstrated to be reachable arbitrarily close [245] (also cf. [246, 247]).

Quantum coin tossing under noisy conditions can draw help from quantum string coin flipping [248]. In [249], it is allowed for honest players to abort with a certain probability determined by the level of noise. Quantum coin tossing with partial noise tolerance by means of a nested structure is proposed in [250]. These considerations are relevant to practical implementations of quantum coin tossing. Recent such works include a string of coin tosses generated using photonic qutrits with entanglement in orbital angular momentum [251] and an all optical-fiber single-coin quantum coin tossing [252]. An experimental realization of the loss resistant quantum coin tossing protocol proposed in [253] is reported in [254], where, however entanglement is employed rather than a practical weak coherent source, because of the protocol's vulnerability to multi-photon pulses. Quantum coin tossing, which is primarily considered for two mistrustful parties, can be generalized to multiple parties [255].

The coin tossing protocol [253] uses the encoding states

$$|\chi_{\beta,a}\rangle = \sqrt{\frac{1 + (-1)^a x}{2}}|0\rangle + (-1)^{\beta+a}\sqrt{\frac{1 - (-1)^a x}{2}}|1\rangle, \quad (16)$$

where $x \in \{0, 1\}$, β represents the basis and a the secret bit. Alice partially commits to bit a by submitting the states $\rho_a = \frac{1}{2}(|\chi_{0,a}\rangle\langle\chi_{0,a}| + |\chi_{1,a}\rangle\langle\chi_{1,a}|$. The supports of ρ_0 and ρ_1 are not disjoint, and thus Bob's ability to discriminate between ρ_0 and ρ_1 is constrained by a minimum error discrimination bound. This is just the reason that Alice is able to re-transmit a state if Bob's measurement fails and that the scheme has loss-resistance in conjunction with the use of a single-photon source.

The protocol proposed in [256] aims to correct this reliance on a single-photon source (as against using a source of weak coherent pulses), albeit by fixing the number of pulses emitted and thereby bounding the multiphoton probability. However, its practical realization [257] is not found to be entirely loss-tolerant, although admitting several imperfections that would be encountered in practice.

It is an interesting question whether device-independent methods can be extended to distrustful cryptography. It turns out that for quantum bit commitment with finite cheat probability and bias, one can construct a device-independent scheme, and then build coin tossing on top of that [258]. These authors present a device-independent scheme for cheat-sensitive quantum bit commitment, where Alice's and Bob's cheating probabilities are $\simeq 0.854$ and 0.75, which is used to propose a device-independent protocol for coin flipping with bias $\lesssim 0.336$.

Zhao *et al* [259] report using measurement-device independence [61, 159] to protect quantum coin tossing against detector-side channel attacks due to Alice, who may launch a detector-blinding attack based on a recent experiment. This scheme essentially modifies the protocol of [253] to incorporate the measurement-device-independent method, but the authors also consider the possibility of using weak coherent pulses. This scheme is found to be loss-tolerant when single-photon sources are employed. As expected from the use of measurement-device independence, the resulting measurement-device-independent quantum coin tossing is shown to potentially offer a doubling of the secure distance in some cases.

6.4 Quantum private query

Private information retrieval or private query [260] is a crypto-task involving two parties, a user Alice interacting with a server Bob, wherein Alice queries him to obtain an element held by Bob in his private database, such that Bob does not know which element she queried for (user

security), while he in turn, wishes to restrict information Alice may gain about other elements in the database (database security). A protocol for quantum private query was proposed in 2007 [261, 262], where it was shown to provide an exponential savings in communicational and computational complexity [263].

While an unconditionally secure private query is known to be impossible, practical, cheat-sensitive schemes can be proposed. The basic idea of quantum private query can be illustrated using the phase-encoded scheme proposed in [264]. Let server Bob possess D elements in the database, labelled $d(j) \in \{0, 1\}$, where $0 \le j \le D - 1$. To query item j, Alice transmits the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |j\rangle)$, whereas Bob performs the oracle operation given by

$$U = \sum_{j=0}^{D-1} (-1)^{d(j)}|j\rangle\langle j| \quad (17)$$

whereby the query state transforms to

$$|\phi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{d(j)}|j\rangle) \quad (18)$$

and Alice determines her required information by distinguishing between the two possibilities $\frac{1}{\sqrt{2}}(|0\rangle \pm |j\rangle)$. Such a quantum private query protocol is of practical importance, assuming Bob does not launch entanglement-based attacks.

In Eq. (17), the oracle unitary U can be difficult to implement for large D. As a result, various quantum private query protocols based on quantum key distribution have been proposed [265–273].

6.5 Quantum fingerprinting and digital signatures

Other related protocols include the quantum oblivious set-membership [274] and private set intersection [275]. In quantum oblivious set-membership, Bob's server decides if a user Alice's secret is a member of his private set in an oblivious fashion, namely without his knowing which element it is [274]. Requiring a communication cost of $O(1)$ bits, it yields an exponential reduction in communication cost with respect to classical solutions to the problem.

Signature schemes, which are prevalent in today's electronic communication, were first proposed by Diffie and Hellman in 1976 in the classical framework. They permit messages to be transmitted from a sender to multiple recipients, with the guarantee that the messages remain authentic and can be forwarded to other recipients without invalidation.

In contrast to classical signature schemes, that depend on computationally secure one-way protocols based on the RSA algorithm or the elliptic curve digital signature algorithm, a scheme for quantum digital signature leverages quantum physical laws for the purpose.

In the first proposal for quantum digital signature [276], in analogy with the classical signature scheme, a quantum public key is proposed, which is a set of quantum states, while the private key is the classical description of those states. A quantum one-way function thus replaces the classical one-way function to guarantee unconditional or information theoretic security. Note that quantum one-way or hash functions have the further property that the quantum hashes can be exponentially shorter than the original function input, thereby yielding *quantum fingerprints* [277] (see [278] which reports an experimental realization).

In contrast to the preceding scheme for quantum digital signature, which required quantum memory in order to hold the public key and were thus not practical, the authors of [279, 280] propose a quantum digital signature scheme where this requirement is absent, taking a giant stride towards practicality. A further improvement on this is quantum digital signature protocols that have the same practical requirements as quantum key distribution [281].

Quantum digital signature has been extended in analogy with its classical counterpart to three or more parties [282]. From an experimental perspective, both kilometer-range quantum digital signature [283] as well as free-space quantum digital signature [284] have been demonstrated.

6.6 Blind quantum computation

Universal blind quantum computation is a measurement quantum computation based protocol, wherein a quantum server carries out quantum computation for client Alice, such that her input, output and computation remain private and she does not require any memory or computational power [285]. The protocol is interactive and has a feed-forward mechanism whereby subsequent instructions by Alice to the server can be based on single-qubit measurements. The method submits naturally to fault tolerance.

Normally, the client must be able to prepare single-qubit states. But even a classical client can perform blind quantum computation by interacting with two entangled (but non-communicating) servers. It turns out that in this setting, with authentication, any problem in bounded-error quantum polynomial time class has a two-prover interactive proof with a classical verifier. Blind quantum computation has recently been experimentally realized [286].

7 Relativistic quantum cryptography

Unlike quantum key distribution, some mistrustful crypto-tasks are believed to be insecure even when quantum resources are leveraged, among them, as we saw, bit commitment and ideal coin tossing. Since bit commitment can act as a primitive for various other crypto-tasks, such as zero-knowledge proofs, these results are thought to weaken the case for the security of quantum mistrustful protocols for communication and multiparty computation.

However, these tasks may be secure under other frameworks, such as that based on relativistic constraints or the assumption of noisy storage with the adversary. Under the latter assumption, various otherwise insecure two-party protocols become secure, among them secure identification, oblivious transfer and quantum bit commitment [287].

A. Kent [288] studied how bit commitment could be implemented by exploiting special relativity constraints. Alice and Bob are each split in two agents, and security is obtained against classical attacks provided relativistic constraints can be invoked to prohibit commucation between agents of the same player. The protocol evades [289] the MLC attack [225, 226] essentially by departing from the concealment condition (14), but using synchronous exchange of classical or quantum information between the players in order to be concealing to Bob, which imposes strong complexity, space and time constraints on the protocol.

This was followed by another scheme employing both quantum and classical communication [290], which was shown to be secure under the assumption of perfect devices [291, 292], and has been experimentally realized as a robust method [293, 294]. However, these protocols were restricted to a one-round communication, which entails that for terrestrial agents, the commitment remains valid for at most just over 20 ms. To improve on this, [295] proposed a method involving several rounds of classical communication, which was proved secure against classical attacks, wherein the holding phase could be made arbitrarily long via periodic, coordinated communication between the agents of Alice and Bob. The bound on the probability ϵ to cheat in this method was improved by other authors independently [296–298]. In particular, K. Chakraborty *et al* [296] show ϵ to satisfy the linear bound: $\epsilon \lesssim (r + 1)2^{(-n+3)/2}$, where n is the length of the bit string to be communicated between the agents at each of r rounds. This allows the complexity of protocols to scale only linearly with the commitment time, during which Alice and Bob are required to perform efficient computation and communicate classically.

Based on this theoretical breakthrough, E. Verbanis *et al* [299] reported on a relativistic bit commitment implementation for a 24-hour bit commitment, with a potential for extension to over a year by modifying the positions of agents. Recently, the possibility of making relativistic quantum bit commitment device-independent has been studied [300]. In the case of quantum cryptographic tasks that are secure in the relativistic setting, one can ask (as in bit commitment) whether special relativity by itself can provide security, without invoking quantum mechanics (though quantum mechanics helps).

One crypto-task that requires a conjunction of both properties of relativity and quantum mechanics is *variable-bias coin toss* [301], in which a random bit is shared by flipping a coin whose bias, within a predetermined range, is covertly fixed by one of the players, while the other player only learns the random outcome bit of the toss. While one player is able to influence the outcome, the other can save face by attributing a negative outcome to bad luck. Security arises from the impossibility of superluminal signaling and quantum theory.

Two other protocols, whose security is known to be guaranteed under the conjunction of relativity and quantum mechanics are location-oblivious data transfer [302] and space-time-constrained oblivious transfer [303]. The location-oblivious data transfer involves two mistrustful parties, wherein Alice transfers data in Minkowski space to Bob at a space-time location determined by their joint actions and that neither can predict in advance. Alice is assured that Bob will learn the data, while Bob is assured that Alice cannot find out the transfer location. In the space-time-constrained oblivious transfer, Bob has to output a_b (see definition of oblivious transfer above) within B_b, where B_0 and B_1 are spacelike separated regions.

In contrast to bit commitment, some crypto-tasks, such as secure two-party quantum computation of various classical functions [240, 304, 305], in particular all-or-nothing oblivious transfer [205, 240, 306] and 1-out-of-2 oblivious transfer [304], which are believed to be insecure in nonrelativistic quantum settings, remain so even in the context of relativistic quantum settings. In 1-out-of-2 oblivious transfer, Alice inputs two numbers a_0 and a_1, while Bob inputs bit b and then outputs a_b. In all-or-nothing oblivious transfer, Bob retrieves a bit string sent by Alice with a probability half or gets nothing at all. Also, position-based cryptography, which uses only geographic position as the sole credential of a player, is known to be insecure even with a conjunction of special relativity and quantum mechanics, if adversaries can pre-share a quantum state of unbounded entanglement. A quantum relativistic that is forbidden is that Alice can make available a state received from Bob at an arbitrary event in the causal future, as per the no-summoning theorem [307, 308].

8 Technological issues

In this section, we cover the practical issues regarding experimental realization of a quantum key distribution. This works in tandem with advances in theory, for example, the quantum de Finetti theorem, which would be applicable when it is difficult to bound the dimension of the communication medium (possibly corrupted maliciously). This result has been applied to derive secure quantum key distribution when signals used are technologically limited to Gaussian states or weak coherent states [309], rather than single-photons.

Practical challenges that emerge because of technological issues include:

1. In discrete-variable protocols, key information is encoded in the polarization or the phase of weak coherent pulses simulating true single photon states. Hence, such implementations employ single photon detection techniques, e.g. BB84. However, the use of weak coherent pulses leads to some practical attacks such as the photon number splitting attack for which decoy states have to be used (cf. Section 8.5).

2. In the continuous variable protocols, information has to be encoded in the quadratures of the quantized electromagnetic fields such as those of the coherent states and homodyne or heterodyne detection techniques such as those used for optical classical communication (cf. Section 9).

3. The security level of a protocol is decided by the type of attack considered in its security proof, which in turn could be dictated by technological considerations (e.g., Eve's ability to fight decoherence by realizing massive entangled states). Proving the security against collective (coherent) attacks and universal composability (which, for quantum key distribution, would cover joint attacks over the distribution of the key as well as its eventual use [79]), at speeds and distance that are compatible with practical applications and technologically feasible, is quite a challenge. In practice, this would require the ability to realize efficient post-processing, including parameter estimation of quantum key distribution performance with stable setups across large data blocks. In a quantum network, the performance of any protocol is assessed point to point by considering the key distribution rate at a given security level under these attacks.

For prevalent usage of quantum cryptography, low cost and robustness are important. Among efforts being undertaken in this direction, it has been shown that quantum

key distribution systems can coexist with dense data traffic within the same fibre, thereby precluding the need for dark fibers, which are costly and moreover frequently unavailable [8, 310]. With access network architecture, multiple quantum key distribution users can have simultaneous access in a way that would be compatible with Gigabit Passive Optical Network traffic [311]. Yet another direction to reduce not only cost, but also system complexity and power consumption is through a chip-level photonic integration, which would lead to a high degree of mass-manufacturable, low cost miniaturization [312].

We first begin with a short introduction of classical fiber optical communication [313, 314] and then its adaptation for quantum communication.

8.1 Classical fiber-optics

There has been a tremendous demand for increasing the capacity of information transmitted and internet services. Scientists and communication engineers are in pursuit of achieving this technological challenge. The invention of LASER systems in the 1960s dramatically altered the position of lightwave technologies as compared to radio or microwaves. The availability of a coherent source allowed one to pack an enormous amount of information into light signals increasing the bandwidth. A lightwave communication system consists of a transmission unit with source and electronics to modulate the signals, an optical fiber channel connecting the sender and the receiver and optical amplifiers (also known as repeaters) placed at certain distances along the fiber link to boost the signal strength, a receiving unit with optical detectors and accompanying electronics to retrieve the original signal and extract the transmitted information. Each unit of the fiber-optic communication system is described briefly.

In standard telecom optical fibers of 1550 nm, attenuation of light is 0.2 dB/km (improved in the recently developed ultralow-loss fibers to 0.16 dB/km). This lossy property will restrict of point-to-point quantum key distribution nodes to a few hundreds of kms and strong bounds on the key rate [162, 315]. With practical quantum key distribution, the rates achieved are Mbit/s even though classical fiber optics can deliver speeds upto 100 Gbit/s per wavelength channel.

8.1.1 Transmission

The choice of a source depends on the type of application. For high-speed low loss communication with bit rates of the order of Gbps, the source should meet the following requirements:

1. Generation of wavelengths leading to low losses in the channel for a given power level such that the repeater spacing is large.

2. Spectral line width of the order of ≤ 1 nm to avoid dispersion (variation in phase velocity of a wave depending on its frequency).

3. High-speed modulation for achieving the desired transmission rate.

Typically, semiconductor-based (InGaAsP or GaAs) light sources, such as laser diodes and LEDs, are used in optical communication. They emit required wavelengths, are highly efficient, compact in size and can be modulated corresponding to the input electrical signals.

LED diodes are basically forward-biased p-n junctions emitting incoherent light due to spontaneous emission with 0.1 mW output power and are suitable for transmission distances of a few kms at 10–100 Mbps bit rates. On the contrary, semiconductor laser diodes emit coherent light via stimulated emission with an output power of 0.1 W suitable for longer distances at Gbps bit rates. Laser diodes have narrow spectral-widths, allowing 50% of the output power to be coupled into fibers and useful in reducing chromatic dispersion. In addition, laser diodes have a short recombination time, enabling them to be directly modulated at high rates necessary for high-speed long-distance communications.

High dimension quantum key distribution based on d-level systems allows transmission of greater than 1 bit per photon detection, which can enhance communication capacity at fixed particle rate [316–318]. The round-robin differential phase shift quantum key distribution protocol (Section 2.3) allows a positive key in principle for any quantum bit error rate [45]. Simply by choosing experimental parameters, Eve's information can be tightly bounded, thereby removing the need for monitoring the noise level of the channel. The strong security of measurement-device-independent quantum key distribution is counterbalanced by the quadratic scaling of key rate with detector efficiency, a drawback that can be overcome in practice by reverting to detector-device-independent quantum key distribution (Section 5.4).

8.1.2 Channel

Optical fibers acting as transmission channels have a central dielectric core (usually doped silica) with higher refractive index surrounded by a cladding (pure silica) of lower refractive index. Light signals are guided along the fiber axis using the phenomenon of total internal reflection. Fibers with sudden and gradual change in the refractive index at the core-clad boundary are known as

step-index (which include single-mode and multi-mode fibers) and graded-index fibers respectively. Single-mode (multi-mode) step-index fibers can sustain only one mode (many modes) of light. Different modes travel at different speeds in a graded-index fiber due to the gradual decrease in refractive index from the center of the core, allowing all of them to reach the output at the same instant of time, thereby reducing chromatic dispersion.

Faithful transmission of signals through these channels depend on the transmission characteristics of the fibers which include attenuation, distortion, absorption, dispersion and scattering losses.

8.1.3 Detection

Optical detectors convert light signals into electrical signals which is then amplified and processed by external circuity. Commonly used detectors for fiber-optics are semiconductor-based using materials such as Si, Ge, GaAs, InGaAs, owing to good response characteristics in the optical domain and compatibility with optical fibers. Incident light with energies greater than the bandgap of the semiconductor are absorbed to generate e-h pairs leading to an external photocurrent. The photocurrent is suitably amplified and processed for the extraction of transmitted data. PIN (p-doped, intrinsic, n-doped layers) diodes and Avalanche photodiodes (APDs) are mostly used for photodetection. Both the devices are operated in the reverse-biased condition and the e-h pairs are absorbed in the depletion region.

The key enabling factor of single-photon detectors is their low noise, which in turn would depend on the type of the detection technique. Room temperature single-photon detectors have been shown to be suitable for high bit rate discrete-variable quantum key distribution [319]. For continuous variable quantum key distribution (Section 9), cooling is not necessary.

8.2 Quantum communication

With this background of classical communication, we now discuss quantum communication using fiber-optics. Looking at the Table 1 it is clear that single-mode fibers are preferable for quantum communication. For secure quantum communication, the sender and receiver are connected by quantum channels. There is nothing special about these channels except for the fact that the information is carried using single quantum systems known as qubits, realized as photons, where information is encoded in one of the degrees of freedom, in fact polarization.

Protecting the polarization of a photon from environmental effects known as decoherence and decoupling the polarization degree of a photon from its other de-

grees of freedom (such as frequency) to ensure the faithful transmission of quantum information is very tricky. Single-photons are fragile in nature and cannot sustain themselves typically after traveling for 200 km.

Optical amplifiers known as quantum repeaters are placed at certain intervals along the quantum communication network to maintain the signal strength and increase the transmission distance. It is worth noting here that, quantum repeaters [320, 321] are not a straightforward extensions of their classical counterparts. Quantum signals *cannot* be detected or amplified directly without disturbing it, by virtue of the *no-cloning theorem*. Hence, amplification and restoration of the original signal must be achieved without direct interaction.

In addition, quantum cryptographic security requires the generation of genuine random number sequences where each random number is completely uncorrelated with other numbers in the sequence. It is also not desirable to have any correlations across the runs among different sequences. Quantum indeterminism forms the basis for generation of truly random numbers. Measurement of a single quantum system, an entangled state, coherent state, vacuum state are some methods of random number generation. Quantum randomness cannot be directly accessed at the macroscopic level. The quantum fluctuations are classically amplified to extract genuine randomness (though there is a theoretical proposal [322] for *quantum* amplification of quantum fluctuations). The random number sequences generated are helpful in the random selection of basis for encoding a qubit.

It is worth pointing out that measurement-device-independent quantum key distribution [158] is amenable for upscaling to a multi-user, high speed communication networks in metropolitan areas [323, 324], inasmuch as measurement devices can be positioned in an untrusted, dense relay, where is accessed by a number of quantum key distribution users [325], a scenario whose feasibility has been validated by a number of groups (cf. [326] and references therein), in particular discrete-variable measurement-device-independent quantum key distribution over a distance of 200 km in a telecom fiber [161] and 404 km in an ultralow-loss fiber [327]. Channel loss upto 60 dB can be tolerated given high efficiency single-photon detectors, which translates to a distance of 300 km over standard telecom fiber [328].

Quantum repeaters. Photons are very fragile and hence for long-distance communication one needs to maintain the signal to noise strength for faithful communication [329, 330]. With quantum repeaters, the idea is to divide the entire communication distance into smaller nodes with quantum repeater stations, such that sufficiently noiseless entanglement can be shared between two consecutive nodes. One then performs entanglement

Table 1: *Comparison between single-mode and multi-mode step-index optical fibers. Note that the above mentioned transmission distance and rates are for classical communication.*

Properties	Single-mode fibers	Multi-mode fibers
Core (μm)	8-10	50-100
source	LASERs	LEDs
Transmission distance and rate	> 1000 km at 10Gbps	550m at 10Gbps
Operating wavelengths (nm)	1310 or 1500	850 or 1300
Attenuation loss for above wavelenghts (dB/km)	0.4 or 0.2	3 or 1
Cost	high	low

swapping [331] to entangle nodes farther out, thereby establishing entanglement between far away nodes

$$|\Psi\rangle_{1234} = \frac{1}{2}(|00\rangle_{12} + |11\rangle_{12})(|00\rangle_{34} + |11\rangle_{34})$$
$$= (|\Phi^+\rangle_{14}|\Phi^+\rangle_{23} + |\Phi^-\rangle_{14}|\Phi^-\rangle_{23}$$
$$+ |\Psi^+\rangle_{14}|\Psi^+\rangle_{23} + |\Psi^-\rangle_{14}|\Psi^-\rangle_{23}), \qquad (19)$$

where $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ and $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ are the Bell states [37]. In Eq. (19) measuring particles 2-3 in a Bell basis projects particles 1-4, that may never have interacted, into an entangled state.

Based on the different approaches to rectify fiber attenuation and operation (gate, measurement) losses at each node and performance for specific operational parameters (local gate speed, coupling efficiency, etc.), one can classify the quantum repeaters into different generations [332–334]. Each generation aims to achieve better key rates and decrease in memory errors for long-distance communication [335]. For loss (operational) error suppression, the method employed is heralded generation (heralded purification) which is probabilistic and involves two-way classical communication. But, the quantum error correction approach for both is deterministic and involves one-way communication. Various realizations of quantum repeaters with or without memory are being explored [321, 336–342]

8.3 Single-photon sources

Quantum communication, especially quantum cryptography and quantum random number generation, demands that single-photons be employed [343, 344], in order for standard security proofs such as [29, 30] to work. Typically attenuated lasers are used as substitute single-photon sources. Usually, they should emit photons with mean photon-number $\mu = 1$, variance $\Delta^2 = 0$ and their second order correlation function $g^{(2)}(t) = 0$. Ideally, single-photon sources should generate single photons as and when required, namely on-demand, with 100% probability. Such deterministic systems are of two types:

Single emitters. Single atoms, single ion and single molecule emitters are either Λ or three-level systems in which controlling the pump laser and the atom-cavity coupling, a certain coherent state is transferred to the ground state via stimulated Raman adiabatic passage or radiative de-excitation respectively to generate a single photon in the cavity mode. These sources are scalable, emit indistinguishable photons, have low decoherence and multiphoton effects. Quantum dots [345] and diamond nitrogen-vacancy (N-V) centers are other popular sources where single photons are generated by radiative recombination of electron-hole pairs and optical transitions in the N-V center respectively. But, they suffer from small coupling efficiency, scaling and indistingishability of the generated photons.

Ensemble-based emitters. Single photons are generated by the collective excitations of atomic ensembles of Cs or Rb. The ensemble is also a Λ-type system with metastable ground states $|g_1\rangle$ and $|g_2\rangle$ and an excited state $|e\rangle$. A weak optical light is coupled to the population inverted atoms to induce the $|g_1\rangle \rightarrow |e\rangle$ transition. The de-excitation of a single photon from $|e\rangle \rightarrow |g_2\rangle$ is detected and its presence confirmed. This process is known as heralding. Next, a strong pulse induces a transition $|g_2\rangle \rightarrow |e\rangle$ generating a single heralded photon with $|e\rangle \rightarrow |g_1\rangle$ transition.

Single-photon sources based on probabilistic photon emission through parametric down-conversion and four-wave mixing are also available. The probability of multiphoton generation in such sources increases with the probability of single-photon generation. A single-photon detector cannot distinguish between single photons and multiple photons. This imperfection can be used by an eavesdropper to obtain secret key information after basis reconciliation by measuring the photons acquired from these multi-photon pulses.

8.4 Single-photon detectors

An ideal single-photon detector should detect an incident photon with 100% probability and have nil dead-time and dark-count rates. There are various types of single photon detectors (e.g., single-photon avalanche photodiodes (In-GaAs,Ge,Si), photo-multiplier tubes and superconducting based nanowire single-photon detectors). However, none of them can be considered as an ideal single photon detector as they do not satisfy the above mentioned set of criteria that is expected to be satisfied by an ideal single photon detector.

In particular, detection efficiency, wavelength dependence of efficiency and dead time of single photon detectors are still a big concern, and much effort has been made in the recent past to design better detectors. Often the choice of optical components and the frequency of transmission depend on the efficiency of the single photon detector and the loss characteristics of the transmission channel. Practically, it is an optimization.

The highest efficiency of single photon detectors is obtained for incident photons of frequency around 800 nm, but the lowest attenuation in an optical fiber happens around 1500 nm. Consequently, open air quantum communication systems, including those which involve satellites, are performed using photons with frequency near 800 nm, as the single photon detectors perform best at this frequency, but fiber-based implementations of quantum cryptography are realized in teleportation range (1350–1550 nm), where existing optical fibers show minimum attenuation.

It is of cryptographic advantage if the detectors can also resolve the number of photons in a pulse known as photon-number resolution. Superconducting-tunnel-junctions, quantum dot optically gated field effect transistors are some photon-number resolving detectors. Let us discuss some of the detectors briefly. For a detailed comparison of different detectors and their external circuitry refer [346].

Photo-multiplier tubes (PMTs): An incident photon knocks an electron from a photocathode made of low work function material, which knocks more electrons causing an amplification of electrons. PMTs have large and sensitive collection areas, fast response time, about 10–40 % efficiency. They are vacuum operated which limits their scaling and integration abilities.

Single-photon avalanche photodiode (SPAD): An incident photon creates e-h pairs in the Geiger-mode operated photodiode [347]. SPADs have a detection efficiency of 85% but higher dark count rates as compared to PMTs. Also, once a pulse is detected, the wait time for re-biasing the circuitry for next

detection, namely the dead time is longer. Schemes to reduce this afterpulsing have been realized.

Quantum dot field effect transistors: A thin layer of quantum dots between the gate and the conduction channel in a field-effect transistor traps incident photons modifying the channel conductance. This detector is useful for operation in the infrared region.

The above characteristics discussed are for non-photon resolving operations but the detector's operation for photon-number resolution is also being pursued. The active area of a detector is divided into many pixels. Each pixel detects a photon and collectively many photons are detected and resolved by the detector. Every time a pixel detects a photon, the amplification process takes place independently and the pixel undergoes dead- and recovery-time. Thus, the greater the number of pixels, the better the resolution is.

8.5 Photon-number splitting attacks

In quantum cryptography, the characteristics of the single-photon sources and detectors dominate the practical security issues. Multi-photon generation, blank pulses, detector unresponsiveness for certain wavelengths, high dark counts, dead times, recovery times and jitter are the crucial features which have been used to launch powerful device attacks which cannot be detected by usual methods. In this context, we may specifically mention a particular type of attack that arise due to our technological inability to build perfect on-demand single photon source and photon number resolving detectors that would not destroy the polarization states of the incident photons. The attack is referred to as the photon number splitting attack and illustrates a well known principle of cryptography—Alice and Bob are restricted by the available technology, but Eve is not, she is restricted by laws of physics only (in other words, to provide a security proof, we are not allowed to underestimate Eve by assuming any technological limitations of the devices used by her).

Let us clarify the point. As we do not have a perfect on-demand single photon source, we use approximate single photon sources, usually one obtained by a weak laser pulse attenuated by a neutral density filter. Such an approximate single photon source usually contains single photon (in non-empty pulses), but with finite probability it contains 2 photons, 3 photons, etc. Now, Eve may use a photon number resolving detector to count the number of photons present in each pulse (without changing the polarization state of the incident photon), and stop all the single-photon pulses, while she allows all the multi-photon pulses to reach Bob, keeping one photon from each multi-photon pulse.

Subsequently, she may perform measurements on the photons that she kept from the multi-photon pulses using right basis (based on Alice's and Bob's announcements during basis reconciliation) without introducing any disturbance. This is the photon number splitting attack, which requires a photon-number resolving detector that does not destroy polarization states of the incident photon. Although, quantum mechanics or any law of physics does not prohibit construction of such a detector, until now we do not have any technology to build such a detector.

Otherwise, Alice could use the similar strategy to the multi-photon pulses and allow only single photon pulses to be transmitted. This would have solve the need of single photon sources, too. Unfortunately, no such photon number resolving detector exists until now. However, we know a trick to circumvent photon number splitting attack, which is the decoy state method [49–51, 348]. Specifically, one may randomly mix intentionally prepared multi-photon pulses (decoy qubits) with the pulses generated at the output of an approximate single-photon source, which would generate single photon pulses most of the time. Eve cannot selectively attack pulses generated from the single photon source. In most incidents, pulses originating from the single photon source will not reach Bob, but those originating from the multi-photon source would reach Bob. Thus, loss profile statistics for the pulses generated from the two sources will be different and this difference (bias) would identify Eve, who is performing photon number splitting attack from the natural channel noise which would not be biased. Therefore, applying decoy states [49–51], Alice and Bob can estimate both the probability that a transmission results in a successful output as well as the error rate for different initial pulses.

8.6 Nonlinear effects

Finally, we discuss some nonlinear effects that occur in single-mode fibers that have an impact on its propagation properties. Single-mode fibers are subject to polarization effects such as birefringence (different phase velocities for orthogonal polarization modes), polarization dependent losses (differential attenuation between orthogonal modes) and polarization mode-dispersion (different group velocities for orthogonal states). Fiber irregularities and asymmetries are the cause for such effects which can be overcome by polarization maintaining fibers where birefringence is introduced on purpose to uncouple the polarization modes. Fibers are also subject to dispersion, which is the broadening of signal pulses in the time domain as they propagate along the fiber. Each signal pulse consists different components which travel at different speeds and hence their arrival time at the output varies.

In case of chromatic dispersion, different wavelengths travel at different velocities. The overall chromatic dispersion in a fiber is governed by the type of material used and its refractive index profile. Since the material dispersion is fixed, the refractive index profile has to be engineered in order to reduce such effects. Dispersion compensating fibers and techniques (Bragg grating) are employed to fix this issue.

9 Continuous variable quantum cryptography

Before we conclude this review, we need to mention that all the single-photon-based schemes for quantum key distribution that are discussed here and most of the other protocols for quantum key distribution, quantum secure direct communication and other cryptographic tasks mentioned are discrete-variable based protocols in the sense that in these schemes information is encoded in a discrete variable. However, it is possible to implement most of these schemes by encoding information in continuous variable and distributed phase reference, too [349].

Basically, continuous-variable quantum key distribution involves homodyne detection instead of photon counting encountered in discrete-variable quantum key distribution. Continuous-variable quantum key distribution was first introduced with discrete modulation [350–352] and later with Gaussian modulation using coherent states [353, 354].

Continuous-variable quantum key distribution and other continuous-variable based cryptographic schemes that are usually implemented by continuous modulation of the light field quadratures (usually with the coherent state [353] or squeezed state [355, 356] of light), are important for various reasons. For example, they are immune to some of the side-channel attacks that exploit imperfections of single-photon detectors used in discrete-variable quantum key distribution to cause leakage of information. This is so because coherent detectors (implementing homodyne or heterodyne detection) are used in continuous-variable quantum key distribution.

Further, continuous-variable quantum key distribution can be implemented using commercially available components [357] since the seminal work in continuous-variable quantum key distribution by Ralph in 1999 [351]. In this and the subsequent works by Ralph and his collaborators [358], small phase and amplitude modulations of continuous wave light beams were exploited to carry the key information. Subsequently, many schemes for continuous-variable quantum key distribution have been proposed [124, 353, 354, 359–363] and security proofs for a large set of those schemes have been pro-

vided [78, 353, 364, 365], and interestingly some of the security proofs are composable in nature (cf. [365] and references therein). Continuous-variable quantum key distribution has been experimentally realized by various groups [366, 367]. For example, in [366, 367] experimental realizations of long distance continuous-variable quantum key distribution has been reported. However, continuous-variable quantum key distribution is not immune to all possible side channel attacks, and various strategies to perform side channels attacks have been discussed in the recent past (cf. [349, 357, 368] and references therein).

Although continuous-variable quantum key distribution protocols are not more complicated than their discrete-variable quantum key distribution counterparts, the security analysis in continuous-variable quantum key distribution can be relatively involved, with different considerations of hardware imperfections and noise models. See the recent review [369] and references therein, where a less restricted notion of unconditional security in continuous-variable quantum key distribution is considered. An earlier good overview covering the conceptual issues but without detailed calculations is [370].

A composable security against general coherent attacks for continuous-variable quantum key distribution that encodes via two-mode squeezed vacuum states and measurement by homodyne detection, based on the uncertainty relation formulated in terms of smooth entropies [371], is given in [78]. Also, see [171] (Section 5.5).

Continuous-variable quantum key distribution has been adapted to one-sided device-independent framework [171, 172], which would be relevant when secure hubs (such as banks) are linked to less secure satellite stations. Continuous-variable quantum key distribution has also been implemented in the measurement-device-independent quantum key distribution framework [372–374]. Here, Charlie measures the correlation between two Gaussian-modulated coherent states sent by Alice and Bob. However, continuous-variable measurement-device-independent quantum key distribution requires homedyne detectors of efficiency over 85% to generate a positive key rate [159], which has indeed been recently attained [171, 374]. However, scaling up to an optical network can be challenging because of losses in the detector coupling and network interconnects (but see [375]). Therefore, in the measurement-device-independent quantum key distribution, for long distance communication, discrete-variable based quantum key distribution is preferable to continuous-variable based, though the promise of high key rates makes continuous-variable measurement-device-independent quantum key distribution an interesting option to consider. Techniques proposed recently may help realize a dependable phase reference for the

continuous-variable quantum key distribution systems [360, 361, 376]. In a variant of this theme, quantum key distribution can also be based on continuous variables such as spatial or temporal degrees of freedom, which are basically used for upscaling the dimension of the information carrier in quantum key distribution. The spatial degree of freedom of a photon can be used as the information carrier, but this faces the technological challenge of high-speed modulators being available [377, 378].

Continuous variable quantum key distribution can be used to encode in large alphabets, such as the arrival time of energy-time entangled photons [379], which was proven secure against collective attacks [380] and also realized experimentally, where it was found to achieve a rate of 6.9 bits per coincidence detection across a distance of 20 km at a key rate of 2.7 MBits/s [381]. While this advancement improves the key rate of entanglement based schemes vis-a-vis prepare-and-measure quantum key distribution methods, practical implementation would require to meet the challenge of attaining high level of interference visibility.

10 Post-quantum cryptography

Thus far, we have mentioned several schemes of quantum cryptopgraphy, and noted that one of the main reasons behind the enhanced interest in these schemes underlies in the pioneering work of Shor [1], which entailed that if a scalabale quantum computer could be built, then many classical schemes for key exchange, encryption, authentication, etc., would not remain secure, as the quantum algorithms are capable of performing certain computationally difficult tasks (which are used to provide security in classical system) much faster than their classical counterparts. Specifically, in a post-quantum world (namely, when a scalable quantum computer will be realized) RSA, DSA, elliptic curve DSA (ECDSA), ECDH, etc., would not remain secure [382].

Here, we draw the reader's attention toward the point that "quantum algorithm can only perform certain computationally difficult tasks (which are used to provide security in classical system) much faster than their classical counterparts". This is so because until now there exist only a few quantum algorithms that provide the required speedup (cf. [383] for an interesting discussion on "Why haven't more quantum algorithms been found?"). This leads to a few questions—What happens to those classical cryptographic schemes which use such computationally difficult problems that do not have a quantum algorithm with required speedup? Can they be quantum resistant in the sense that they can resist an adversary with a scalable quantum computer?

Efforts to answer these questions led to a new branch of cryptography, known as post-quantum cryptography that deals with families of classical crytographic schemes which are expected to remain secure in a world where practical, scalable quantum computers are available [384]. Such schemes are usually classified into six families [382] such as:

Lattice-based cryptography. This includes all cryptosystems that are based on lattice problems [385, 386]. These schemes are interesting as some of them are provably secure under a worst-case hardness assumption. However, it seems difficult to provide precise estimates on the security of these schemes against some well known techniques of cryptanalysis [382].

Code-based cryptography. This encryption system is primarily based on error correcting codes. In these type of schemes, there is trade-off between key sizes and structures introduced into the codes. Added structures reduces key size [387], but often allows attacks [388]. A classic example of this type is McEliece's hidden-Goppa-code public key encryption system, which was introduced in 1978 [389] and has not been broken until now [382].

Multivariate polynomial cryptography. This is based on the computational difficulty associated in solving a set of multivariate polynomials over finite fields. Although, several schemes of this type have been broken [390, 391], confidence of the community is high on some of the schemes like Patarin's scheme for public-key-signature system that uses Hidden Fields Equations (HFE) and Isomorphisms of Polynomials (IP) [392].

Hash-based signatures. This includes schemes for digital signatures constructed using hash functions [393–395]. Although, several hash-based systems have been broken in the past, confidence on the recent hash-based schemes is very high.

Secret-key cryptography. Examples of type *Advanced Encryption Standard* (AES), which is a symmetric private key encryption algorithm, created by Joan Daemen and Vincent Rijmen. A design goal behind AES is efficiency in software and hardware and software.

Other schemes not covered under the above mentioned families.

Shor's algorithm cannot be used to attack the cryptosystems that belong to above families as the associated computational tasks are different. However, Grover's algorithm may be used to attack some of the schemes, but since Grover's algorithm provides only a quadratic speedup, an attack based on Grover's algorithm may be circumvented using longer keys. Thus, it is believed that the schemes belonging to above families would remain secure in the post-quantum world.

We have briefly mentioned about post-quantum cryptography, an interesting facet of the modern cryptography as without a mention of post-quantum cryptography any discussion on quantum cryptography would remain incomplete. However, it is not our purpose to discus these schemes in detail. We conclude this short discussion on post-quantum cryptography by noting that the confidence of the cryptographic community in these schemes is a bit artificial as it is impossible to prove that faster quantum algorithms for all or some of the computationally difficult problems used in these schemes will not be designed in future. In brief, if a fast quantum algorithm for a task is not available today, it does not mean that the same will not be proposed tomorrow. Specifically, there is some practical reasons for limited number of quantum algorithms that can provide required speedup [383] and consequently, it is difficult to strongly establish the security of the above mentioned schemes in the post-quantum world.

11 Conclusions and perspectives

In this brief review, we covered a number of quantum cryptographic topics besides quantum key distribution, among them different crypto-tasks and cryptographic frameworks. In a review of a vast area such as quantum cryptography, it is, unfortunately, inevitable that some important topics may not be covered. A case in point here is the topic of quantum memory as applied to channel or device attacks.

Theoretically, the main work ahead in the area is in extending security proofs in various scenarios to the composable framework under the most general coherent attack. The main practical challenges are perhaps developing on-chip quantum cryptographic modules that are free from side channels and able to be scale to global networks, by integrating point-to-point quantum cryptographic links. This may drive the search for proper trade-offs between ease of implementation and resource usage, or between reasonable security and economic feasibility.

Regarding the foundational implications of quantum cryptography, an interesting question is whether the no-go theorems that give security to quantum cryptography can be used to derive quantum mechanics. R. Clifton *et al* [396] presented a derivation of quantum mechanics from three *quantum cryptographic axioms*, namely, no-signaling, no-cloning and no bit commitment. J. Smolin

[397] criticized this view by presenting a toy theory that simulated these features but was not quantum mechanics. In response, H. Halvorson and J. Bub [398] argued that Smolin's toy theory violated an independence reasonable condition for spacelike separated systems assumed in [396]. More recently, [184] have argued that general probability theories for single systems can be distinguished between *base* theories, which feature a no-cloning theorem, which similar to Spekkens' toy theory that defends an epistemic view of quantum states [399], and *contextual* theories. The former supports a type of unconditional security in the framework of trusted devices, whereas the latter allows a degree of device independence.

It is known that the usual definition of security in quantum key distribution implies security under universal composition. However, keys produced by repeated runs of quantum key distribution have been shown to degrade gradually. It would be interesting to study direct secure communication (Section 3) in the context of universal composability, and the advantage of schemes for direct secure communication, if any, over quantum key distribution under repeated usage.

Acknowledgments

References

[1] Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings of the *35th Annual Symposium on Foundations of Computer Science*, November, 20–22, 1994, pp. 124–134. `doi:10.1109/sfcs.1994.365700`

[2] Hensen B, Bernien H, Dreau AE, Reiserer A, Kalb N, Blok MS, Ruitenberg J, Vermeulen RFL, Schouten RN, Abellan C, Amaya W, Pruneri V, Mitchell MW, Markham M, Twitchen DJ, Elkouss D, Wehner S, Taminiau TH, Hanson R. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* 2015; **526**(7575): 682–686. `doi:10.1038/nature15759`

[3] Chan KWC, El Rifai M, Verma P, Kak S, Chen Y. Security analysis of the multi-photon three-stage quantum key distribution. *International Journal on Cryptography and Information Security* 2015; **5**(3–4): 1–13. `arXiv:1503.05793`, `doi:10.5121/ijcis.2015.5401`

[4] Lucamarini M, Patel KA, Dynes JF, Fröhlich B, Sharpe AW, Dixon AR, Yuan ZL, Penty RV, Shields AJ. Efficient decoy-state quantum key distribution with quantified security. *Optics Express* 2013; **21**(21): 24550–24565. `arXiv:1310.0240`, `doi:10.1364/OE.21.024550`

[5] Gisin N, Ribordy G, Tittel W, Zbinden H. Quantum cryptography. *Reviews of Modern Physics* 2002; **74**(1): 145–195. `arXiv:quant-ph/0101098`, `doi:10.1103/RevModPhys.74.145`

[6] Alléaume R, Branciard C, Bouda J, Debuisschert T, Dianati M, Gisin N, Godfrey M, Grangier P, Länger T, Lütkenhaus N, Monyk C, Painchault P, Peev M, Poppe A, Pornin T, Rarity J, Renner R, Ribordy G, Riguidel M, Salvail L, Shields A, Weinfurter H, Zeilinger A. Using quantum key distribution for cryptographic purposes: A survey. *Theoretical Computer Science* 2014; **560**(1): 62–81. `arXiv:quant-ph/0701168`, `doi:10.1016/j.tcs.2014.09.018`

[7] Bennett CH, Brassard G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science* 2014; **560**(1): 7–11. `doi:10.1016/j.tcs.2014.05.025`

[8] Diamanti E, Lo H-K, Qi B, Yuan Z. Practical challenges in quantum key distribution. *NPJ Quantum Information* 2016; **2**: 16025. `doi:10.1038/npjqi.2016.25`

[9] Ekert AK. Quantum cryptography based on Bell's theorem. *Physical Review Letters* 1991; **67**(6): 661–663. `doi:10.1103/PhysRevLett.67.661`

[10] Toner B. Monogamy of non-local quantum correlations. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science* 2009; **465**(2101): 59–69. `arXiv:quant-ph/0601172`, `doi:10.1098/rspa.2008.0149`

[11] Scarani V, Kurtsiefer C. The black paper of quantum cryptography: Real implementation problems. *Theoretical Computer Science* 2014; **560**(1): 27–32. `arXiv:0906.4547`, `doi:10.1016/j.tcs.2014.09.015`

[12] Bennett CH. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters* 1992; **68**(21): 3121–3124. doi:10.1103/PhysRevLett.68.3121

[13] Goldenberg L, Vaidman L. Quantum cryptography based on orthogonal states. *Physical Review Letters* 1995; **75**(7): 1239–1243. arXiv:quant-ph/9502021, doi:10.1103/PhysRevLett.75.1239

[14] Avella A, Brida G, Degiovanni IP, Genovese M, Gramegna M, Traina P. Experimental quantum-cryptography scheme based on orthogonal states. *Physical Review A* 2010; **82**(6): 062309. arXiv:1007.2588, doi:10.1103/PhysRevA.82.062309

[15] Shukla C, Pathak A, Srikanth R. Beyond the Goldenberg–Vaidman protocol: secure and efficient quantum communication using arbitrary, orthogonal, multi-particle quantum states. *International Journal of Quantum Information* 2012; **10**(8): 1241009. arXiv:1210.2583, doi:10.1142/S0219749912410092

[16] Yadav P, Srikanth R, Pathak A. Two-step orthogonal-state-based protocol of quantum secure direct communication with the help of order-rearrangement technique. *Quantum Information Processing* 2014; **13**(12): 2731–2743. arXiv:1209.4304, doi:10.1007/s11128-014-0825-8

[17] Aravinda S, Banerjee A, Pathak A, Srikanth R. Orthogonal-state-based cryptography in quantum mechanics and local post-quantum theories. *International Journal of Quantum Information* 2014; **12**(7–8): 1560020. arXiv:1409.8505, doi:10.1142/S0219749915600205

[18] Shukla C, Pathak A. Orthogonal-state-based deterministic secure quantum communication without actual transmission of the message qubits. *Quantum Information Processing* 2014; **13**(9): 2099–2113. arXiv:1307.5995, doi:10.1007/s11128-014-0792-0

[19] Shukla C, Alam N, Pathak A. Protocols of quantum key agreement solely using Bell states and Bell measurement. *Quantum Information Processing* 2014; **13**(11): 2391–2405. doi:10.1007/s11128-014-0784-0

[20] Pathak A. Efficient protocols for unidirectional and bidirectional controlled deterministic secure quantum communication: different alternative approaches. *Quantum Information Processing* 2015; **14**(6): 2195–2210. arXiv:1411.6430, doi:10.1007/s11128-015-0957-5

[21] Thapliyal K, Sharma RD, Pathak A. Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. arXiv:1608.00101

[22] Bouwmeester D, Pan J-W, Mattle K, Eibl M, Weinfurter H, Zeilinger A. Experimental quantum teleportation. *Nature* 1997; **390**(6660): 575–579. doi:10.1038/37539

[23] Guo G-C, Shi B-S. Quantum cryptography based on interaction-free measurement. *Physics Letters A* 1999; **256**(2–3): 109–112. doi:10.1016/S0375-9601(99)00235-2

[24] Noh T-G. Counterfactual quantum cryptography. *Physical Review Letters* 2009; **103**(23): 230501. arXiv:0809.3979, doi:10.1103/PhysRevLett.103.230501

[25] Brida G, Cavanna A, Degiovanni IP, Genovese M, Traina P. Experimental realization of counterfactual quantum cryptography. *Laser Physics Letters* 2012; **9**(3): 247–252. arXiv:1107.5467, doi:10.1002/lapl.201110120

[26] Csiszár I, Körner J. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory* 1978; **24**(3): 339–348. doi:10.1109/TIT.1978.1055892

[27] Mayers D. Quantum key distribution and string oblivious transfer in noisy channels. In: *Advances in Cryptology – CRYPTO '96: 16th Annual International Cryptology Conference Santa Barbara, California, August 18–22, 1996 Proceedings*. Koblitz N (editor), Berlin: Springer, 1996, pp. 343–357. arXiv:quant-ph/9606003, doi:10.1007/3-540-68697-5_26

[28] Mayers D. Unconditional security in quantum cryptography. *Journal of the ACM* 2001; **48**(3): 351–406. arXiv:quant-ph/9802025, doi:10.1145/382780.382781

[29] Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters* 2000; **85**(2): 441–444. arXiv:quant-ph/0003004, doi:10.1103/PhysRevLett.85.441

[30] Lo H-K, Chau HF. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* 1999; **283**(5410): 2050–2056. `arXiv:quant-ph/9803006`, `doi:10.1126/science.283.5410.2050`

[31] Bennett CH, DiVincenzo DP, Smolin JA, Wootters WK. Mixed-state entanglement and quantum error correction. *Physical Review A* 1996; **54**(5): 3824–3851. `arXiv:quant-ph/9604024`, `doi:10.1103/PhysRevA.54.3824`

[32] Steane AM. Simple quantum error-correcting codes. *Physical Review A* 1996; **54**(6): 4741–4751. `arXiv:quant-ph/9605021`, `doi:10.1103/PhysRevA.54.4741`

[33] Calderbank AR, Shor PW. Good quantum error-correcting codes exist. *Physical Review A* 1996; **54**(2): 1098–1105. `arXiv:quant-ph/9512032`, `doi:10.1103/PhysRevA.54.1098`

[34] Coffman V, Kundu J, Wootters WK. Distributed entanglement. *Physical Review A* 2000; **61**(5): 052306. `arXiv:quant-ph/9907047`, `doi:10.1103/PhysRevA.61.052306`

[35] Biham E, Boyer M, Boykin PO, Mor T, Roychowdhury V. A proof of the security of quantum key distribution. *Journal of Cryptology* 2006; **19**(4): 381–439. `arXiv:quant-ph/0511175`, `doi:10.1007/s00145-005-0011-3`

[36] Shor PW. Scheme for reducing decoherence in quantum computer memory. *Physical Review A* 1995; **52**(4): R2493–R2496. `doi:10.1103/PhysRevA.52.R2493`

[37] Nielsen MA, Chuang IL. *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2010.

[38] Boström K, Felbinger T. Deterministic secure direct communication using entanglement. *Physical Review Letters* 2002; **89**(18): 187902. `arXiv:quant-ph/0209040`, `doi:10.1103/PhysRevLett.89.187902`

[39] Lucamarini M, Mancini S. Secure deterministic communication without entanglement. *Physical Review Letters* 2005; **94**(14): 140501. `doi:10.1103/PhysRevLett.94.140501`

[40] Inoue K, Waks E, Yamamoto Y. Differential phase shift quantum key distribution. *Physical Review Letters* 2002; **89**(3): 037902. `doi:10.1103/PhysRevLett.89.037902`

[41] Inoue K, Waks E, Yamamoto Y. Differential-phase-shift quantum key distribution using coherent light. *Physical Review A* 2003; **68**(2): 022317. `doi:10.1103/PhysRevA.68.022317`

[42] Collins RJ, Amiri R, Fujiwara M, Honjo T, Shimizu K, Tamaki K, Takeoka M, Andersson E, Buller GS, Sasaki M. Experimental transmission of quantum digital signatures over 90 km of installed optical fiber using a differential phase shift quantum key distribution system. *Optics Letters* 2016; **41**(21): 4883–4886. `doi:10.1364/OL.41.004883`

[43] Inoue K, Honjo T. Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. *Physical Review A* 2005; **71**(4): 042305. `doi:10.1103/PhysRevA.71.042305`

[44] Waks E, Takesue H, Yamamoto Y. Security of differential-phase-shift quantum key distribution against individual attacks. *Physical Review A* 2006; **73**(1): 012344. `doi:10.1103/PhysRevA.73.012344`

[45] Sasaki T, Yamamoto Y, Koashi M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* 2014; **509**(7501): 475–478. `doi:10.1038/nature13303`

[46] Mizutani A, Imoto N, Tamaki K. Robustness of the round-robin differential-phase-shift quantum-key-distribution protocol against source flaws. *Physical Review A* 2015; **92**(6): 060303. `doi:10.1103/PhysRevA.92.060303`

[47] Guan J-Y, Cao Z, Liu Y, Shen-Tu G-L, Pelc JS, Fejer MM, Peng C-Z, Ma X, Zhang Q, Pan J-W. Experimental passive round-robin differential phase-shift quantum key distribution. *Physical Review Letters* 2015; **114**(18): 180502. `doi:10.1103/PhysRevLett.114.180502`

[48] Li Y-H, Cao Y, Dai H, Lin J, Zhang Z, Chen W, Xu Y, Guan J-Y, Liao S-K, Yin J, Zhang Q, Ma X, Peng C-Z, Pan J-W. Experimental round-robin differential phase-shift quantum key distribution. *Physical Review A* 2016; **93**(3): 030302. `doi:10.1103/PhysRevA.93.030302`

[49] Hwang W-Y. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters* 2003; **91**(5): 057901. `doi:10.1103/PhysRevLett.91.057901`

[50] Lo H-K, Ma X, Chen K. Decoy state quantum key distribution. *Physical Review Letters* 2005; **94**(23): 230504. `doi:10.1103/PhysRevLett.94.230504`

[51] Wang X-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters* 2005; **94**(23): 230503. `doi:10.1103/PhysRevLett.94.230503`

[52] Kak S. A three-stage quantum cryptography protocol. *Foundations of Physics Letters* 2006; **19**(3): 293–296. `arXiv:quant-ph/0503027`, `doi:10.1007/s10702-006-0520-9`

[53] Gobby C, Yuan ZL, Shields AJ. Quantum key distribution over 122 km of standard telecom fiber. *Applied Physics Letters* 2004; **84**(19): 3762–3764. `arXiv:quant-ph/0412171`, `doi:10.1063/1.1738173`

[54] Barrett J, Hardy L, Kent A. No signaling and quantum key distribution. *Physical Review Letters* 2005; **95**(1): 010503. `arXiv:quant-ph/0405101`, `doi:10.1103/PhysRevLett.95.010503`

[55] Acín A, Brunner N, Gisin N, Massar S, Pironio S, Scarani V. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters* 2007; **98**(23): 230501. `doi:10.1103/PhysRevLett.98.230501`

[56] Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. *Physical Review Letters* 2007; **99**(14): 140501. `doi:10.1103/PhysRevLett.99.140501`

[57] Boyer M, Gelles R, Kenigsberg D, Mor T. Semiquantum key distribution. *Physical Review A* 2009; **79**(3): 032341. `arXiv:0812.4835`, `doi:10.1103/PhysRevA.79.032341`

[58] Jin X-M, Ren J-G, Yang B, Yi Z-H, Zhou F, Xu X-F, Wang S-K, Yang D, Hu Y-F, Jiang S, Yang T, Yin H, Chen K, Peng C-Z, Pan J-W. Experimental free-space quantum teleportation. *Nat Photon* 2010; **4**(6): 376–381. `doi:10.1038/nphoton.2010.87`

[59] Yin J, Ren J-G, Lu H, Cao Y, Yong H-L, Wu Y-P, Liu C, Liao S-K, Zhou F, Jiang Y, Cai X-D, Xu P, Pan G-S, Jia J-J, Huang Y-M, Yin H, Wang J-Y, Chen Y-A, Peng C-Z, Pan J-W. Quantum teleportation and entanglement distribution over 100-kilometre free-space channels. *Nature* 2012; **488**(7410): 185–188. `doi:10.1038/nature11332`

[60] Clauser JF, Horne MA, Shimony A, Holt RA. Proposed experiment to test local hidden-variable theories. *Physical Review Letters* 1969; **23**(15): 880–884. `doi:10.1103/PhysRevLett.23.880`

[61] Lo H-K, Curty M, Qi B. Measurement-device-independent quantum key distribution. *Physical Review Letters* 2012; **108**(13): 130503. `arXiv:1109.1473`, `doi:10.1103/PhysRevLett.108.130503`

[62] Tamaki K, Lo H-K, Fung C-HF, Qi B. Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw. *Physical Review A* 2012; **85**(4): 042307. `arXiv:1111.3413`, `doi:10.1103/PhysRevA.85.042307`

[63] Xu F, Curty M, Qi B, Lo H-K. Practical aspects of measurement-device-independent quantum key distribution. *New Journal of Physics* 2013; **15**(11): 113007. `doi:10.1088/1367-2630/15/11/113007`

[64] Xu F, Qi B, Liao Z, Lo H-K. Long distance measurement-device-independent quantum key distribution with entangled photon sources. *Applied Physics Letters* 2013; **103**(6): 061101. `doi:10.1063/1.4817672`

[65] Tang Z, Liao Z, Xu F, Qi B, Qian L, Lo H-K. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Physical Review Letters* 2014; **112**(19): 190503. `arXiv:1306.6134`, `doi:10.1103/PhysRevLett.112.190503`

[66] Vallone G, Bacco D, Dequal D, Gaiarin S, Luceri V, Bianco G, Villoresi P. Experimental satellite quantum communications. *Physical Review Letters* 2015; **115**(4): 040502. `arXiv:1406.4051`, `doi:10.1103/PhysRevLett.115.040502`

[67] Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. Proceedings of the *First International Conference on Quantum, Nano, and Micro Technologies, 2007 (ICQNM '07)*, January 2–6, pp. 10. `doi:10.1109/ICQNM.2007.18`

[68] Luo Y-P, Hwang T. Authenticated semi-quantum direct communication protocols using Bell states. *Quantum Information Processing* 2016; **15**(2): 947–958. `doi:10.1007/s11128-015-1182-y`

[69] Nie Y-Y, Li Y-H, Wang Z-S. Semi-quantum information splitting using GHZ-type states. *Quan-*

tum Information Processing 2013; **12**(1): 437–448. doi:10.1007/s11128-012-0388-5

[70] Li L, Qiu D, Mateus P. Quantum secret sharing with classical Bobs. *Journal of Physics A: Mathematical and Theoretical* 2013; **46**(4): 045304. doi:10.1088/1751-8113/46/4/045304

[71] Krawec WO. Mediated semiquantum key distribution. *Physical Review A* 2015; **91**(3): 032323. arXiv:1411.6024, doi:10.1103/PhysRevA.91.032323

[72] Zou X, Qiu D, Zhang S, Mateus P. Semiquantum key distribution without invoking the classical party's measurement capability. *Quantum Information Processing* 2015; **14**(8): 2981–2996. doi:10.1007/s11128-015-1015-z

[73] Krawec WO. Security proof of a semi-quantum key distribution protocol. Proceedings of the *2015 IEEE International Symposium on Information Theory (ISIT)*, June 14–19, pp. 686–690. doi:10.1109/ISIT.2015.7282542

[74] Krawec WO. Security of a semi-quantum protocol where reflections contribute to the secret key. *Quantum Information Processing* 2016; **15**(5): 2067–2090. doi:10.1007/s11128-016-1266-3

[75] Canetti R. Universally composable security: a new paradigm for cryptographic protocols. *Cryptology ePrint Archive* 2013: 2000/2067. https://eprint.iacr.org/2000/067

[76] Müller-Quade J, Renner R. Composability in quantum cryptography. *New Journal of Physics* 2009; **11**(8): 085006. doi:10.1088/1367-2630/11/8/085006

[77] Scarani V, Renner R. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters* 2008; **100**(20): 200501. doi:10.1103/PhysRevLett.100.200501

[78] Furrer F, Franz T, Berta M, Leverrier A, Scholz VB, Tomamichel M, Werner RF. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. *Physical Review Letters* 2012; **109**(10): 100502. doi:10.1103/PhysRevLett.109.100502

[79] Ben-Or M, Horodecki M, Leung DW, Mayers D, Oppenheim J. The universal composable security of quantum key distribution. In: *Theory of Cryptography: Second Theory of Cryptography Conference, TCC 2005, Cambridge, Massachusetts, February 10–12, 2005. Proceedings*. Kilian J (editor), Lecture Notes in Computer Science, vol.3378, Berlin: Springer, 2005, pp. 386-406. doi:10.1007/978-3-540-30576-7_21

[80] Unruh D. Universally composable quantum multiparty computation. In: *Advances in Cryptology – EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 – June 3, 2010. Proceedings*. Gilbert H (editor), Lecture Notes in Computer Science, vol.6110, Berlin: Springer, 2010, pp. 486–505. doi:10.1007/978-3-642-13190-5_25

[81] Mishra S, Shukla C, Pathak A, Srikanth R, Venugopalan A. An integrated hierarchical dynamic quantum secret sharing protocol. *International Journal of Theoretical Physics* 2015; **54**(9): 3143–3154. arXiv:1409.2037, doi:10.1007/s10773-015-2552-z

[82] Fehr S, Schaffner C. Composing quantum protocols in a classical environment. In: *Theory of Cryptography: 6th Theory of Cryptography Conference, TCC 2009, San Francisco, California, March 15–17, 2009. Proceedings*. Reingold O (editor), Berlin: Springer, 2009, pp. 350–367. doi:10.1007/978-3-642-00457-5_21

[83] Thapliyal K, Pathak A, Banerjee S. Quantum cryptography over non-Markovian channels. *Quantum Information Processing* 2017; **16**(5): 115. arXiv:1608.06071, doi:10.1007/s11128-017-1567-1

[84] Pathak A. *Elements of Quantum Computation and Quantum Communication*. Boca Raton: CRC Press, 2013.

[85] Thapliyal K, Pathak A. Applications of quantum cryptographic switch: various tasks related to controlled quantum communication can be performed using Bell states and permutation of particles. *Quantum Information Processing* 2015; **14**(7): 2599–2616. arXiv:1501.04187, doi:10.1007/s11128-015-0987-z

[86] Sharma RD, Thapliyal K, Pathak A, Pan AK, De A. Which verification qubits perform best for secure communication in noisy channel? *Quantum Information Processing* 2016; **15**(4): 1703–1718. `arXiv:1508.05237, doi:10.1007/s11128-015-1207-6`

[87] Banerjee A, Shukla C, Thapliyal K, Pathak A, Panigrahi PK. Asymmetric quantum dialogue in noisy environment. *Quantum Information Processing* 2017; **16**(2): 49. `arXiv:1605.08363, doi:10.1007/s11128-016-1508-4`

[88] Nguyen BA. Quantum dialogue. *Physics Letters A* 2004; **328**(1): 6–10. `doi:10.1016/j.physleta.2004.06.009`

[89] Boudot F, Schoenmakers B, Traoré J. A fair and efficient solution to the socialist millionaires' problem. *Discrete Applied Mathematics* 2001; **111**(1–2): 23–36. `doi:10.1016/S0166-218X(00)00342-5`

[90] Wen X, Chen Y, Fang J. An inter-bank E-payment protocol based on quantum proxy blind signature. *Quantum Information Processing* 2013; **12**(1): 549–558. `doi:10.1007/s11128-012-0398-3`

[91] Huang W, Yang Y-H, Jia H-Y. Cryptanalysis and improvement of a quantum communication-based online shopping mechanism. *Quantum Information Processing* 2015; **14**(6): 2211–2225. `doi:10.1007/s11128-015-0958-4`

[92] Zhao Z, Naseri M, Zheng Y. Secure quantum sealed-bid auction with post-confirmation. *Optics Communications* 2010; **283**(16): 3194–3197. `doi:10.1016/j.optcom.2010.04.019`

[93] Naseri M. Secure quantum sealed-bid auction. *Optics Communications* 2009; **282**(9): 1939–1943. `doi:10.1016/j.optcom.2009.01.026`

[94] Yang Y-G, Naseri M, Wen Q-Y. Improved secure quantum sealed-bid auction. *Optics Communications* 2009; **282**(20): 4167–4170. `doi:10.1016/j.optcom.2009.07.010`

[95] Piotrowski EW, Sładkowski J. Quantum English auctions. *Physica A: Statistical Mechanics and its Applications* 2003; **318**(3–4): 505–515. `arXiv:quant-ph/0108017, doi:10.1016/S0378-4371(02)01533-9`

[96] Piotrowski EW, Sładkowski J. Quantum auctions: facts and myths. *Physica A: Statistical Mechanics and its Applications* 2008; **387**(15): 3949–3953. `arXiv:0709.4096, doi:10.1016/j.physa.2008.02.071`

[97] Thapliyal K, Sharma RD, Pathak A. Protocols for quantum binary voting. *International Journal of Quantum Information* 2016; **15**(1): 1750007. `doi:10.1142/S0219749917500071`

[98] Jozsa R. Quantum effects in algorithms. In: *Quantum Computing and Quantum Communications: First NASA International Conference, QCQC'98 Palm Springs, California, February 17–20, 1998 Selected Papers*. Williams CP (editor), Berlin: Springer, 1999, pp. 103–112. `doi:10.1007/3-540-49208-9_7`

[99] Mitchison G, Jozsa R. Counterfactual computation. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 2001; **457**(2009): 1175–1194. `arXiv:quant-ph/9907007, doi:10.1098/rspa.2000.0714`

[100] Hosten O, Rakher MT, Barreiro JT, Peters NA, Kwiat PG. Counterfactual quantum computation through quantum interrogation. *Nature* 2006; **439**(7079): 949–952. `doi:10.1038/nature04523`

[101] Vaidman L. Impossibility of the counterfactual computation for all possible outcomes. *Physical Review Letters* 2007; **98**(16): 160403. `arXiv:quant-ph/0610174, doi:10.1103/PhysRevLett.98.160403`

[102] Elitzur AC, Vaidman L. Quantum mechanical interaction-free measurements. *Foundations of Physics* 1993; **23**(7): 987–997. `arXiv:hep-th/9305002, doi:10.1007/bf00736012`

[103] Kwiat P, Weinfurter H, Herzog T, Zeilinger A, Kasevich MA. Interaction-free measurement. *Physical Review Letters* 1995; **74**(24): 4763–4766. `doi:10.1103/PhysRevLett.74.4763`

[104] Akshata Shenoy H, Srikanth R, Srinivas T. Semi-counterfactual cryptography. *EPL (Europhysics Letters)* 2013; **103**(6): 60008. `doi:10.1209/0295-5075/103/60008`

[105] Akshata Shenoy H, Srikanth R. The wave-function is real but nonphysical: A view from counterfactual quantum cryptography. 2013: `arXiv:1311.7127`

[106] Sun Y, Wen Q-Y. Counterfactual quantum key distribution with high efficiency. *Physical Review A*

2010; **82**(5): 052318. `doi:10.1103/PhysRevA.82.052318`

[107] Zhang S, Zhang B, Liu X-T. Improved direct counterfactual quantum communication. 2014: `arXiv:1410.2769`

[108] Yin Z-Q, Li H-W, Chen W, Han Z-F, Guo G-C. Security of counterfactual quantum cryptography. *Physical Review A* 2010; **82**(4): 042335. `doi:10.1103/PhysRevA.82.042335`

[109] Zhang S, Wang J, Tang CJ. Counterfactual attack on counterfactual quantum key distribution. *Europhysics Letters* 2012; **98**(3): 30012. `doi:10.1209/0295-5075/98/30012`

[110] Zhang S, Wang J, Tang C-J. Security proof of counterfactual quantum cryptography against general intercept-resend attacks and its vulnerability. *Chinese Physics B* 2012; **21**(6): 060303. `doi:10.1088/1674-1056/21/6/060303`

[111] Liu Y, Ju L, Liang X-L, Tang S-B, Tu G-LS, Zhou L, Peng C-Z, Chen K, Chen T-Y, Chen Z-B, Pan J-W. Experimental demonstration of counterfactual quantum communication. *Physical Review Letters* 2012; **109**(3): 030501. `doi:10.1103/PhysRevLett.109.030501`

[112] Yin Z-Q, Li H-W, Yao Y, Zhang C-M, Wang S, Chen W, Guo G-C, Han Z-F. Counterfactual quantum cryptography based on weak coherent states. *Physical Review A* 2012; **86**(2): 022313. `doi:10.1103/PhysRevA.86.022313`

[113] Akshata Shenoy H, Srikanth R, Srinivas T. Counterfactual quantum certificate authorization. *Physical Review A* 2014; **89**(5): 052307. `arXiv:1402.2250`, `doi:10.1103/PhysRevA.89.052307`

[114] Shenoy-Hejamadi A, Srikanth R. Counterfactual distribution of Schrödinger cat states. *Physical Review A* 2015; **92**(6): 062308. `arXiv:1506.03033`, `doi:10.1103/PhysRevA.92.062308`

[115] Salih H, Li Z-H, Al-Amri M, Zubairy MS. Protocol for direct counterfactual quantum communication. *Physical Review Letters* 2013; **110**(17): 170502. `arXiv:1206.2042`, `doi:10.1103/PhysRevLett.110.170502`

[116] Vaidman L. Comment on "Direct counterfactual transmission of a quantum state". *Physical Review A* 2016; **93**(6): 066301. `doi:10.1103/PhysRevA.93.066301`

[117] Vaidman L. Counterfactuality of 'counterfactual' communication. *Journal of Physics A: Mathematical and Theoretical* 2015; **48**(46): 465303. `arXiv:1410.2723`, `doi:10.1088/1751-8113/48/46/465303`

[118] Salih H, Li Z-H, Al-Amri M, Zubairy MS. Salih et al. Reply. *Physical Review Letters* 2014; **112**(20): 208902. `doi:10.1103/PhysRevLett.112.208902`

[119] Gisin N. Optical communication without photons. *Physical Review A* 2013; **88**(3): 030301. `arXiv:1304.8053`, `doi:10.1103/PhysRevA.88.030301`

[120] Cao Y, Li Y-H, Cao Z, Yin J, Chen Y-A, Yin H-L, Chen T-Y, Ma X, Peng C-Z, Pan J-W. Direct counterfactual communication via quantum Zeno effect. *Proceedings of the National Academy of Sciences* 2017; **114**(19): 4920–4924. `doi:10.1073/pnas.1614560114`

[121] Guo Q, Cheng L-Y, Chen L, Wang H-F, Zhang S. Counterfactual distributed controlled-phase gate for quantum-dot spin qubits in double-sided optical microcavities. *Physical Review A* 2014; **90**(4): 042327. `doi:10.1103/PhysRevA.90.042327`

[122] Guo Q, Cheng L-Y, Chen L, Wang H-F, Zhang S. Counterfactual quantum-information transfer without transmitting any physical particles. *Scientific Reports* 2015; **5**: 8416. `doi:10.1038/srep08416`

[123] Salih H. Protocol for counterfactually transporting an unknown qubit. *Frontiers in Physics* 2016; **3**: 94. `doi:10.3389/fphy.2015.00094`

[124] Braunstein SL, Pati AK. *Quantum Information with Continuous Variables*. Dordrecht: Kluwer Academic Publishers, 2003. `doi:10.1007/978-94-015-1258-9`

[125] Nauerth S, Fürst M, Schmitt-Manderbach T, Weier H, Weinfurter H. Information leakage via side channels in freespace BB84 quantum cryptography. *New Journal of Physics* 2009; **11**(6): 065001. `doi:10.1088/1367-2630/11/6/065001`

[126] Rau M, Vogl T, Corrielli G, Vest G, Fuchs L, Nauerth S, Weinfurter H. Spatial mode side channels in free-space QKD implementations. *IEEE Journal of Selected Topics in Quantum Electronics* 2015; **21**(3): 187–191. `doi:10.1109/JSTQE.2014.2372008`

[127] Boaron A, Korzh B, Houlmann R, Boso G, Lim CCW, Martin A, Zbinden H. Detector-device-independent quantum key distribution: security analysis and fast implementation. *Journal of Applied Physics* 2016; **120**(6): 063101. `doi:10.1063/1.4960093`

[128] Zhao Y, Fung C-HF, Qi B, Chen C, Lo H-K. Quantum hacking: experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A* 2008; **78**(4): 042333. `doi:10.1103/PhysRevA.78.042333`

[129] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J, Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* 2010; **4**(10): 686–689. `doi:10.1038/nphoton.2010.214`

[130] Lu H. Two-way deterministic quantum key distribution against passive detector side channel attacks in the forward line. *Quantum Information Processing* 2015; **14**(10): 3827–3834. `doi:10.1007/s11128-015-1083-0`

[131] Meda A, Degiovanni IP, Tosi A, Yuan Z, Brida G, Genovese M. Quantifying backflash radiation to prevent zero-error attacks in quantum key distribution. *Light: Science & Applications* 2017; **6**: e16261. `arXiv:1605.05562`

[132] Lamas-Linares A, Kurtsiefer C. Breaking a quantum key distribution system through a timing side channel. *Optics Express* 2007; **15**(15): 9388–9393. `doi:10.1364/oe.15.009388`

[133] Ferrigno J, Hlavac M. When AES blinks: introducing optical side channel. *IET Information Security* 2008; **2**(3): 94–98. `doi:10.1049/iet-ifs:20080038`

[134] Sun S-H, Xu F, Jiang M-S, Ma X-C, Lo H-K, Liang L-M. Effect of source tampering in the security of quantum cryptography. *Physical Review A* 2015; **92**(2): 022304. `doi:10.1103/PhysRevA.92.022304`

[135] Derkach I, Usenko VC, Filip R. Preventing side-channel effects in continuous-variable quantum key distribution. *Physical Review A* 2016; **93**(3): 032309. `doi:10.1103/PhysRevA.93.032309`

[136] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H, Gisin N. "Plug and play" systems for quantum cryptography. *Applied Physics Letters* 1997; **70**(7): 793–795. `arXiv:quant-ph/9611042`, `doi:10.1063/1.118224`

[137] Mayers D, Yao A. Quantum cryptography with imperfect apparatus. Proceedings of the *IEEE 54th Annual Symposium on Foundations of Computer Science*, Palo Alto, California, November 8–11, 1998, pp. 503. `arXiv:quant-ph/9809039`, `doi:10.1109/sfcs.1998.743501`

[138] Acín A, Massar S, Pironio S. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics* 2006; **8**(8): 126. `doi:10.1088/1367-2630/8/8/126`

[139] Scarani V, Gisin N, Brunner N, Masanes L, Pino S, Acín A. Secrecy extraction from no-signaling correlations. *Physical Review A* 2006; **74**(4): 042339. `arXiv:quant-ph/0606197`, `doi:10.1103/PhysRevA.74.042339`

[140] Masanes L, Renner R, Christandl M, Winter A, Barrett J. Full security of quantum key distribution from no-signaling constraints. *IEEE Transactions on Information Theory* 2014; **60**(8): 4973–4986. `arXiv:quant-ph/0606049`, `doi:10.1109/tit.2014.2329417`

[141] Masanes L. Universally composable privacy amplification from causality constraints. *Physical Review Letters* 2009; **102**(14): 140501. `arXiv:0807.2158`, `doi:10.1103/PhysRevLett.102.140501`

[142] Hänggi E, Renner R, Wolf S. Efficient device-independent quantum key distribution. In: *Advances in Cryptology – EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 – June 3, 2010. Proceedings.* Gilbert H (editor), Berlin: Springer, 2010, pp. 216–234. `doi:10.1007/978-3-642-13190-5_11`

[143] Pironio S, Acín A, Brunner N, Gisin N, Massar S, Scarani V. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics* 2009; **11**(4): 045021. `doi:10.1088/1367-2630/11/4/045021`

[144] Masanes L, Pironio S, Acín A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications* 2011; **2**: 238. `arXiv:1009.1567`, `doi:10.1038/ncomms1244`

[145] Barrett J, Colbeck R, Kent A. Unconditionally secure device-independent quantum key distribution with only two devices. *Physical Review A*

2012; **86**(6): 062326. `arXiv:1209.0435`, `doi: 10.1103/PhysRevA.86.062326`

[146] Vazirani U, Vidick T. Fully device-independent quantum key distribution. *Physical Review Letters* 2014; **113**(14): 140501. `arXiv:1210.1810`, `doi: 10.1103/PhysRevLett.113.140501`

[147] Shalm LK, Meyer-Scott E, Christensen BG, Bierhorst P, Wayne MA, Stevens MJ, Gerrits T, Glancy S, Hamel DR, Allman MS, Coakley KJ, Dyer SD, Hodge C, Lita AE, Verma VB, Lambrocco C, Tortorici E, Migdall AL, Zhang Y, Kumor DR, Farr WH, Marsili F, Shaw MD, Stern JA, Abellán C, Amaya W, Pruneri V, Jennewein T, Mitchell MW, Kwiat PG, Bienfang JC, Mirin RP, Knill E, Nam SW. Strong loophole-free test of local realism. *Physical Review Letters* 2015; **115**(25): 250402. `arXiv: 1511.03189`, `doi:10.1103/PhysRevLett.115. 250402`

[148] Giustina M, Versteegh MAM, Wengerowsky S, Handsteiner J, Hochrainer A, Phelan K, Steinlechner F, Kofler J, Larsson J-Å, Abellán C, Amaya W, Pruneri V, Mitchell MW, Beyer J, Gerrits T, Lita AE, Shalm LK, Nam SW, Scheidl T, Ursin R, Wittmann B, Zeilinger A. Significant-loophole-free test of Bell's theorem with entangled photons. *Physical Review Letters* 2015; **115**(25): 250401. `arXiv: 1511.03190`, `doi:10.1103/PhysRevLett.115. 250401`

[149] Wu X, Cai Y, Yang TH, Le HN, Bancal J-D, Scarani V. Robust self-testing of the three-qubit *W* state. *Physical Review A* 2014; **90**(4): 042339. `arXiv:1407.5769`, `doi:10. 1103/PhysRevA.90.042339`

[150] Kaniewski J. Self-testing of binary observables based on commutation. 2017: `arXiv:1702.06845`

[151] Lim CCW, Portmann C, Tomamichel M, Renner R, Gisin N. Device-independent quantum key distribution with local Bell test. *Physical Review X* 2013; **3**(3): 031006. `arXiv:1208.0023`, `doi: 10.1103/PhysRevX.3.031006`

[152] Branciard C, Cavalcanti EG, Walborn SP, Scarani V, Wiseman HM. One-sided device-independent quantum key distribution: security, feasibility, and the connection with steering. *Physical Review A* 2012; **85**(1): 010301. `arXiv:1109.1435`, `doi: 10.1103/PhysRevA.85.010301`

[153] Zhou C, Bao W-S, Zhang H-l, Li H-W, Wang Y, Li Y, Wang X. Biased decoy-state measurement-device-independent quantum key distribution with finite resources. *Physical Review A* 2015; **91**(2): 022313. `doi:10.1103/PhysRevA.91.022313`

[154] Pawłowski M, Brunner N. Semi-device-independent security of one-way quantum key distribution. *Physical Review A* 2011; **84**(1): 010302. `arXiv:1103.4105`, `doi:10.1103/PhysRevA.84.010302`

[155] Woodhead E. Semi device independence of the BB84 protocol. *New Journal of Physics* 2016; **18**(5): 055010. `doi:10.1088/1367-2630/18/5/ 055010`

[156] Biham E, Huttner B, Mor T. Quantum cryptographic network based on quantum memories. *Physical Review A* 1996; **54**(4): 2651–2658. `arXiv: quant-ph/9604021`, `doi:10.1103/PhysRevA. 54.2651`

[157] Inamori. Security of practical time-reversed EPR quantum key distribution. *Algorithmica* 2002; **34**(4): 340–365. `doi:10.1007/s00453-002-0983-4`

[158] Curty M, Xu F, Cui W, Lim CCW, Tamaki K, Lo H-K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nature Communications* 2014; **5**: 3732. `doi:10. 1038/ncomms4732`

[159] Xu F, Curty M, Qi B, Lo HK. Measurement-device-independent quantum cryptography. *IEEE Journal of Selected Topics in Quantum Electronics* 2015; **21**(3): 6601111. `arXiv:1409.5157`, `doi: 10.1109/jstqe.2014.2381460`

[160] Liu Y, Chen T-Y, Wang L-J, Liang H, Shentu G-L, Wang J, Cui K, Yin H-L, Liu N-L, Li L, Ma X, Pelc JS, Fejer MM, Peng C-Z, Zhang Q, Pan J-W. Experimental measurement-device-independent quantum key distribution. *Physical Review Letters* 2013; **111**(13): 130502. `arXiv:1209.6178`, `doi: 10.1103/PhysRevLett.111.130502`

[161] Tang Y-L, Yin H-L, Chen S-J, Liu Y, Zhang W-J, Jiang X, Zhang L, Wang J, You L-X, Guan J-Y, Yang D-X, Wang Z, Liang H, Zhang Z, Zhou N, Ma X, Chen T-Y, Zhang Q, Pan J-W. Measurement-device-independent quantum key distribution over 200 km. *Physical Review Letters* 2014; **113**(19): 190501. `arXiv:1407.8012`, `doi: 10.1103/PhysRevLett.113.190501`

[162] Takeoka M, Guha S, Wilde MM. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications* 2014; **5**: 5235. `doi:10.1038/ncomms6235`

[163] González P, Rebón L, Ferreira da Silva T, Figueroa M, Saavedra C, Curty M, Lima G, Xavier GB, Nogueira WAT. Quantum key distribution with untrusted detectors. *Physical Review A* 2015; **92**(2): 022337. `doi:10.1103/PhysRevA.92.022337`

[164] Lim CCW, Korzh B, Martin A, Bussières F, Thew R, Zbinden H. Detector-device-independent quantum key distribution. *Applied Physics Letters* 2014; **105**(22): 221112. `arXiv:1410.1850`, `doi:10.1063/1.4903350`

[165] Kim Y-H. Single-photon two-qubit entangled states: preparation and measurement. *Physical Review A* 2003; **67**(4): 040301. `arXiv:quant-ph/0303125`, `doi:10.1103/PhysRevA.67.040301`

[166] Qi B. Trustworthiness of detectors in quantum key distribution with untrusted detectors. *Physical Review A* 2015; **91**(2): 020303. `arXiv:1410.3685`, `doi:10.1103/PhysRevA.91.020303`

[167] Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A* 2006; **73**(2): 022320. `arXiv:quant-ph/0507063`, `doi:10.1103/PhysRevA.73.022320`

[168] Liang W-Y, Li M, Yin Z-Q, Chen W, Wang S, An X-B, Guo G-C, Han Z-F. Simple implementation of quantum key distribution based on single-photon Bell-state measurement. *Physical Review A* 2015; **92**(1): 012319. `arXiv:1505.00897`, `doi:10.1103/PhysRevA.92.012319`

[169] Wiseman HM, Jones SJ, Doherty AC. Steering, entanglement, nonlocality, and the Einstein-Podolsky-Rosen paradox. *Physical Review Letters* 2007; **98**(14): 140402. `arXiv:quant-ph/0612147`, `doi:10.1103/PhysRevLett.98.140402`

[170] Lucamarini M, Vallone G, Gianani I, Mataloni P, Di Giuseppe G. Device-independent entanglement-based Bennett 1992 protocol. *Physical Review A* 2012; **86**(3): 032325. `arXiv:1111.1997`, `doi:10.1103/PhysRevA.86.032325`

[171] Gehring T, Händchen V, Duhme J, Furrer F, Franz T, Pacher C, Werner RF, Schnabel R. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. *Nature Communications* 2015; **6**: 8795. `arXiv:1406.6174`, `doi:10.1038/ncomms9795`

[172] Walk N, Hosseini S, Geng J, Thearle O, Haw JY, Armstrong S, Assad SM, Janousek J, Ralph TC, Symul T, Wiseman HM, Lam PK. Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution. *Optica* 2016; **3**(6): 634–642. `arXiv:1405.6593`, `doi:10.1364/optica.3.000634`

[173] Vértesi T, Navascués M. Certifying entangled measurements in known Hilbert spaces. *Physical Review A* 2011; **83**(6): 062112. `arXiv:1101.5361`, `doi:10.1103/PhysRevA.83.062112`

[174] Brunner N, Pironio S, Acin A, Gisin N, Méthot AA, Scarani V. Testing the dimension of Hilbert spaces. *Physical Review Letters* 2008; **100**(21): 210503. `arXiv:0802.0760`, `doi:10.1103/PhysRevLett.100.210503`

[175] Navascués M, de la Torre G, Vértesi T. Characterization of quantum correlations with local dimension constraints and its device-independent applications. *Physical Review X* 2014; **4**(1): 011011. `arXiv:1308.3410`, `https://link.aps.org/doi/10.1103/PhysRevX.4.011011`

[176] Wehner S, Christandl M, Doherty AC. Lower bound on the dimension of a quantum system given measured data. *Physical Review A* 2008; **78**(6): 062112. `arXiv:0808.3960`, `doi:10.1103/PhysRevA.78.062112`

[177] Gallego R, Brunner N, Hadley C, Acín A. Device-independent tests of classical and quantum dimensions. *Physical Review Letters* 2010; **105**(23): 230501. `arXiv:1010.5064`, `doi:10.1103/PhysRevLett.105.230501`

[178] Brunner N, Navascués M, Vértesi T. Dimension witnesses and quantum state discrimination. *Physical Review Letters* 2013; **110**(15): 150501. `arXiv:1209.5643`, `doi:10.1103/PhysRevLett.110.150501`

[179] Hendrych M, Gallego R, Micuda M, Brunner N, Acin A, Torres JP. Experimental estimation of the dimension of classical and quantum systems. *Nature Physics* 2012; **8**(8): 588–591. `arXiv:1111.1208`, `doi:10.1038/nphys2334`

[180] Ahrens J, Badziag P, Cabello A, Bourennane M. Experimental device-independent tests of classical and quantum dimensions. *Nature Physics*

2012; **8**(8): 592–595. `arXiv:1111.1277, doi:` `10.1038/nphys2333`

[181] Li H-W, Pawłowski M, Yin Z-Q, Guo G-C, Han Z-F. Semi-device-independent randomness certification using $n \rightarrow 1$ quantum random access codes. *Physical Review A* 2012; **85**(5): 052308. `arXiv:1109.5259, doi:10.` `1103/PhysRevA.85.052308`

[182] Li H-W, Yin Z-Q, Wu Y-C, Zou X-B, Wang S, Chen W, Guo G-C, Han Z-F. Semi-device-independent random-number expansion without entanglement. *Physical Review A* 2011; **84**(3): 034301. `arXiv:1108.1480, doi:10.` `1103/PhysRevA.84.034301`

[183] Bowles J, Quintino MT, Brunner N. Certifying the dimension of classical and quantum systems in a prepare-and-measure scenario with independent devices. *Physical Review Letters* 2014; **112**(14): 140407. `arXiv:1311.1525, doi:10.` `1103/PhysRevLett.112.140407`

[184] Aravinda S, Srikanth R, Pathak A. On the origin of nonclassicality in single systems. 2016: `arXiv:` `1607.01768`

[185] Acín A, Gisin N, Masanes L. From Bell's theorem to secure quantum key distribution. *Physical Review Letters* 2006; **97**(12): 120405. `arXiv:quant-` `ph/0510094, doi:10.1103/PhysRevLett.97.` `120405`

[186] Dodis Y, Pointcheval D, Ruhault S, Vergniaud D, Wichs D. Security analysis of pseudo-random number generators with input: /dev/random is not robust. Proceedings of the *2013 ACM SIGSAC Conference on Computer & Communications Security*, Berlin, Germany, November 4–8, 2013, Association for Computing Machinery, pp. 647–658. `doi:10.1145/2508859.2516653`

[187] Chaitin GJ. *Algorithmic Information Theory*. Cambridge Tracts in Theoretical Computer Science, Cambridge: Cambridge University Press, 2004.

[188] Bassham LE, Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J, Vo S. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Special Publication (NIST SP) - 800-22 Rev 1a, Gaithersburg, Maryland: National Institute of Standards and Technology,

2010. `http://ws680.nist.gov/publication/` `get_pdf.cfm?pub_id=906762`

[189] Rarity JG, Owens PCM, Tapster PR. Quantum random-number generation and key sharing. *Journal of Modern Optics* 1994; **41**(12): 2435–2444. `doi:10.1080/09500349414552281`

[190] Stefanov A, Gisin N, Guinnard O, Guinnard L, Zbinden H. Optical quantum random number generator. *Journal of Modern Optics* 2000; **47**(4): 595–598. `arXiv:quant-ph/9907006, doi:10.1080/` `09500340008233380`

[191] Jennewein T, Achleitner U, Weihs G, Weinfurter H, Zeilinger A. A fast and compact quantum random number generator. *Review of Scientific Instruments* 2000; **71**(4): 1675–1680. `arXiv:quant-` `ph/9912118, doi:10.1063/1.1150518`

[192] Dynes JF, Yuan ZL, Sharpe AW, Shields AJ. A high speed, postprocessing free, quantum random number generator. *Applied Physics Letters* 2008; **93**(3): 031109. `arXiv:0807.4111, doi:` `10.1063/1.2961000`

[193] Wahl M, Leifgen M, Berlin M, Röhlicke T, Rahn H-J, Benson O. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements. *Applied Physics Letters* 2011; **98**(17): 171105. `doi:` `10.1063/1.3578456`

[194] Nie Y-Q, Zhang H-F, Zhang Z, Wang J, Ma X, Zhang J, Pan J-W. Practical and fast quantum random number generation based on photon arrival time relative to external reference. *Applied Physics Letters* 2014; **104**(5): 051110. `arXiv:1401.2594,` `doi:10.1063/1.4863224`

[195] Stipčević M, Rogina BM. Quantum random number generator based on photonic emission in semiconductors. *Review of Scientific Instruments* 2007; **78**(4): 045104. `doi:10.1063/1.2720728`

[196] Qi B, Chi Y-M, Lo H-K, Qian L. High-speed quantum random number generation by measuring phase noise of a single-mode laser. *Optics Letters* 2010; **35**(3): 312–314. `doi:10.1364/ol.35.000312`

[197] Uchida A, Amano K, Inoue M, Hirano K, Naito S, Someya H, Oowada I, Kurashige T, Shiki M, Yoshimori S, Yoshimura K, Davis P. Fast physical random bit generation with chaotic semiconductor lasers. *Nature Photonics* 2008; **2**(12): 728-732. `doi:` `10.1038/nphoton.2008.227`

[198] Abellán C, Amaya W, Jofre M, Curty M, Acín A, Capmany J, Pruneri V, Mitchell MW. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Optics Express* 2014; **22**(2): 1645–1654. `arXiv:1401.5658`, `doi:10.1364/oe.22.001645`

[199] Gabriel C, Wittmann C, Sych D, Dong R, Mauerer W, Andersen UL, Marquardt C, Leuchs G. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics* 2010; **4**(10): 711–715. `doi:10.1038/nphoton.2010.197`

[200] Symul T, Assad SM, Lam PK. Real time demonstration of high bitrate quantum random number generation with coherent laser light. *Applied Physics Letters* 2011; **98**(23): 231103. `arXiv:1107.4438`, `doi:10.1063/1.3597793`

[201] Sanguinetti B, Martin A, Zbinden H, Gisin N. Quantum random number generation on a mobile phone. *Physical Review X* 2014; **4**(3): 031056. `doi:10.1103/PhysRevX.4.031056`

[202] Nisan N, Ta-Shma A. Extracting randomness: a survey and new constructions. *Journal of Computer and System Sciences* 1999; **58**(1): 148–173. `doi:10.1006/jcss.1997.1546`

[203] Frauchiger D, Renner R, Troyer M. True randomness from realistic quantum devices. 2013: `arXiv:1311.4547`

[204] Ma X, Xu F, Xu H, Tan X, Qi B, Lo H-K. Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Physical Review A* 2013; **87**(6): 062327. `arXiv:1207.1473`, `doi:10.1103/PhysRevA.87.062327`

[205] Colbeck R. *Quantum and Relativistic Protocols for Secure Multi-Party Computation*. PhD Thesis, University of Cambridge, Cambridge, 2006. `arXiv:0911.3814`

[206] Pironio S, Acín A, Massar S, de la Giroday AB, Matsukevich DN, Maunz P, Olmschenk S, Hayes D, Luo L, Manning TA, Monroe C. Random numbers certified by Bell's theorem. *Nature* 2010; **464**(7291): 1021–1024. `doi:10.1038/nature09008`

[207] Christensen BG, McCusker KT, Altepeter JB, Calkins B, Gerrits T, Lita AE, Miller A, Shalm LK, Zhang Y, Nam SW, Brunner N, Lim CCW, Gisin N, Kwiat PG. Detection-loophole-free test of quantum nonlocality, and applications. *Physical Review Letters* 2013; **111**(13): 130406. `arXiv:1306.5772`, `doi:10.1103/PhysRevLett.111.130406`

[208] Dall'Arno M, Passaro E, Gallego R, Pawlowski M, Acin A. Detection loophole attacks on semi-device-independent quantum and classical protocols. *Quantum Information and Computation* 2015; **15**(1–2): 37–49. `arXiv:1210.1272`

[209] Vallone G, Marangon DG, Tomasin M, Villoresi P. Quantum randomness certified by the uncertainty principle. *Physical Review A* 2014; **90**(5): 052327. `arXiv:1401.7917`, `doi:10.1103/PhysRevA.90.052327`

[210] Lunghi T, Brask JB, Lim CCW, Lavigne Q, Bowles J, Martin A, Zbinden H, Brunner N. Self-testing quantum random number generator. *Physical Review Letters* 2015; **114**(15): 150501. `arXiv:1410.2790`, `doi:10.1103/PhysRevLett.114.150501`

[211] Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. *Physical Review A* 1999; **59**(3): 1829–1834. `arXiv:quant-ph/9806063`, `doi:10.1103/PhysRevA.59.1829`

[212] Karlsson A, Koashi M, Imoto N. Quantum entanglement for secret sharing and secret splitting. *Physical Review A* 1999; **59**(1): 162–168. `doi:10.1103/PhysRevA.59.162`

[213] Cleve R, Gottesman D, Lo H-K. How to share a quantum secret. *Physical Review Letters* 1999; **83**(3): 648–651. `arXiv:quant-ph/9901025`, `doi:10.1103/PhysRevLett.83.648`

[214] Gottesman D. Theory of quantum secret sharing. *Physical Review A* 2000; **61**(4): 042311. `arXiv:quant-ph/9910067`, `doi:10.1103/PhysRevA.61.042311`

[215] Singh SK, Srikanth R. Generalized quantum secret sharing. *Physical Review A* 2005; **71**(1): 012328. `doi:10.1103/PhysRevA.71.012328`

[216] Muralidharan S, Panigrahi PK. Perfect teleportation, quantum-state sharing, and superdense coding through a genuinely entangled five-qubit state. *Physical Review A* 2008; **77**(3): 032321. `arXiv:0708.3785`, `doi:10.1103/PhysRevA.77.032321`

[217] Muralidharan S, Panigrahi PK. Quantum-information splitting using multipartite cluster states. *Physical Review A*

2008; **78**(6): 062333. `arXiv:0802.0781`, `doi:10.1103/PhysRevA.78.062333`

[218] Keet A, Fortescue B, Markham D, Sanders BC. Quantum secret sharing with qudit graph states. *Physical Review A* 2010; **82**(6): 062315. `arXiv:1004.4619`, `doi:10.1103/PhysRevA.82.062315`

[219] Shukla C, Pathak A. Hierarchical quantum communication. *Physics Letters A* 2013; **377**(19–20): 1337–1344. `arXiv:1301.0498`, `doi:10.1016/j.physleta.2013.04.010`

[220] Tavakoli A, Herbauts I, Żukowski M, Bourennane M. Secret sharing with a single *d*-level quantum system. *Physical Review A* 2015; **92**(3): 030302. `arXiv:1501.05582`, `doi:10.1103/PhysRevA.92.030302`

[221] Goldwasser S, Micali S. Probabilistic encryption & how to play mental poker keeping secret all partial information. Proceedings of the *14th Annual ACM Symposium on Theory of Computing*, San Francisco, California, May 5–7, 1982, Association for Computing Machinery, pp. 365–377. `doi:10.1145/800070.802212`

[222] Blum M. Coin flipping by telephone. In: *High Technology in the Information Industry: Digest of Papers, COMPCON Spring 82, 24th IEEE Computer Society International Conference, Jack Tar Hotel, San Francisco, California, February 22–25.* Institute of Electrical and Electronics Engineers, 1982, pp. 133–137.

[223] Goldreich O, Micali S, Wigderson A. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *Journal of the ACM* 1991; **38**(3): 690–728. `doi:10.1145/116825.116852`

[224] Kent A. Coin tossing is strictly weaker than bit commitment. *Physical Review Letters* 1999; **83**(25): 5382–5384. `arXiv:quant-ph/9810067`, `doi:10.1103/PhysRevLett.83.5382`

[225] Mayers D. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters* 1997; **78**(17): 3414–3417. `arXiv:quant-ph/9605044`, `doi:10.1103/PhysRevLett.78.3414`

[226] Lo H-K, Chau HF. Is quantum bit commitment really possible? *Physical Review Letters* 1997; **78**(17): 3410–3413. `arXiv:quant-ph/9603004`, `doi:10.1103/PhysRevLett.78.3410`

[227] Chiribella G, D'Ariano GM, Perinotti P, Schlingemann D, Werner R. A short impossibility proof of quantum bit commitment. *Physics Letters A* 2013; **377**(15): 1076–1087. `arXiv:0905.3801`, `doi:10.1016/j.physleta.2013.02.045`

[228] Doescher C, Keyl M. An introduction to quantum coin-tossing. 2002: `arXiv:quant-ph/0206088`

[229] Hughston LP, Jozsa R, Wootters WK. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A* 1993; **183**(1): 14–18. `doi:10.1016/0375-9601(93)90880-9`

[230] Srikanth R. Quantum bit commitment with a composite evidence. *Physica Scripta* 2004; **70**(6): 343–346. `doi:10.1088/0031-8949/70/6/002`

[231] He GP. Quantum key distribution based on orthogonal states allows secure quantum bit commitment. *Journal of Physics A: Mathematical and Theoretical* 2011; **44**(44): 445305. `arXiv:1101.4587`, `doi:10.1088/1751-8113/44/44/445305`

[232] He GP. Can relativistic bit commitment lead to secure quantum oblivious transfer? *European Physical Journal D* 2015; **69**(4): 93. `arXiv:1210.5681`, `doi:10.1140/epjd/e2015-50882-4`

[233] He GP. Simplified quantum bit commitment using single photon nonlocality. *Quantum Information Processing* 2014; **13**(10): 2195–2211. `arXiv:1212.4962`, `doi:10.1007/s11128-014-0728-8`

[234] Yuen HP. An unconditionally secure quantum bit commitment protocol. 2012: `arXiv:1212.0938`

[235] Cheung C-Y. Quantum bit commitment using Wheeler's delayed choice experiment. 2015: `arXiv:1504.05551`

[236] Kent A. Quantum bit string commitment. *Physical Review Letters* 2003; **90**(23): 237901. `arXiv:quant-ph/0111099`, `doi:10.1103/PhysRevLett.90.237901`

[237] Hardy L, Kent A. Cheat sensitive quantum bit commitment. *Physical Review Letters* 2004; **92**(15): 157901. `arXiv:quant-ph/9911043`, `doi:10.1103/PhysRevLett.92.157901`

[238] He GP. Security bound of cheat sensitive quantum bit commitment. *Scientific Reports* 2015; **5**: 9398. `doi:10.1038/srep09398`

[239] Spekkens RW, Rudolph T. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A* 2001; **65**(1): 012310. arXiv:quant-ph/0106019, doi:10.1103/PhysRevA.65.012310

[240] Colbeck R. Impossibility of secure two-party classical computation. *Physical Review A* 2007; **76**(6): 062308. arXiv:0708.2843, doi:10.1103/PhysRevA.65.012310

[241] Aharonov D, Ta-Shma A, Vazirani UV, Yao AC. Quantum bit escrow. Proceedings of the *32nd annual ACM symposium on Theory of computing*, Portland, Oregon, Association for Computing Machinery, pp. 705–714. doi:10.1145/335305.335404

[242] Ambainis A. A new protocol and lower bounds for quantum coin flipping. *Journal of Computer and System Sciences* 2004; **68**(2): 398–416. doi:10.1016/j.jcss.2003.07.010

[243] Nayak A, Shor P. Bit-commitment-based quantum coin flipping. *Physical Review A* 2003; **67**(1): 012304. arXiv:quant-ph/0206123, doi:10.1103/PhysRevA.67.012304

[244] Kitaev AY. Quantum coin flipping. Presented at *QIP 2003: 6th Annual Workshop on Quantum Information Processing*, Berkeley, California, December 13–18, 2002. http://www.msri.org/publications/ln/msri/2002/qip/kitaev/1/index.html

[245] Chailloux A, Kerenidis I. Optimal quantum strong coin flipping. 2009: arXiv:0904.1511

[246] Mochon C. Large family of quantum weak coin-flipping protocols. *Physical Review A* 2005; **72**(2): 022341. arXiv:quant-ph/0502068, doi:10.1103/PhysRevA.72.022341

[247] Mochon C. Quantum weak coin flipping with arbitrarily small bias. 2007: arXiv:0711.4114

[248] Lamoureux LP, Brainis E, Amans D, Barrett J, Massar S. Provably secure experimental quantum bit-string generation. *Physical Review Letters* 2005; **94**(5): 050503. arXiv:quant-ph/0408121, doi:10.1103/PhysRevLett.94.050503 https://link.aps.org/doi/10.1103/PhysRevLett.94.050503

[249] Hänggi E, Wullschleger J. Tight bounds for classical and quantum coin flipping. In: *Theory of Cryptography: 8th Theory of Cryptography Conference, TCC 2011, Providence, Rhode Island, March 28–30, 2011. Proceedings*. Ishai Y (editor), Berlin: Springer, 2011, pp. 468–485. arXiv:1009.4741, doi:10.1007/978-3-642-19571-6_28

[250] Zhang S, Zhang Y. Quantum coin flipping secure against channel noises. *Physical Review A* 2015; **92**(2): 022313. doi:10.1103/PhysRevA.92.022313

[251] Molina-Terriza G, Vaziri A, Ursin R, Zeilinger A. Experimental quantum coin tossing. *Physical Review Letters* 2005; **94**(4): 040501. doi:10.1103/PhysRevLett.94.040501

[252] Nguyen AT, Frison J, Huy KP, Massar S. Experimental quantum tossing of a single coin. *New Journal of Physics* 2008; **10**(8): 083037. doi:10.1088/1367-2630/10/8/083037

[253] Berlín G, Brassard G, Bussières F, Godbout N. Fair loss-tolerant quantum coin flipping. *Physical Review A* 2009; **80**(6): 062321. doi:10.1103/PhysRevA.80.062321

[254] Berlín G, Brassard G, Bussières F, Godbout N, Slater JA, Tittel W. Experimental loss-tolerant quantum coin flipping. *Nature Communications* 2011; **2**: 561. doi:10.1038/ncomms1572

[255] Ambainis A, Buhrman H, Dodis Y, Rohrig H. Multiparty quantum coin flipping. Proceedings of the *19th IEEE Annual Conference on Computational Complexity, 2004*, Amherst, Massachusetts, June 21–24, 2004, Institute of Electrical and Electronics Engineers, pp. 250–259. arXiv:quant-ph/0304112, doi:10.1109/ccc.2004.1313848

[256] Pappa A, Chailloux A, Diamanti E, Kerenidis I. Practical quantum coin flipping. *Physical Review A* 2011; **84**(5): 052305. arXiv:1106.1099, doi:10.1103/PhysRevA.84.052305

[257] Pappa A, Jouguet P, Lawson T, Chailloux A, Legré M, Trinkler P, Kerenidis I, Diamanti E. Experimental plug and play quantum coin flipping. *Nature Communications* 2014; **5**: 3717. doi:10.1038/ncomms4717

[258] Silman J, Chailloux A, Aharon N, Kerenidis I, Pironio S, Massar S. Fully distrustful quantum bit commitment and coin flipping. *Physical Review Letters* 2011; **106**(22): 220501. doi:10.1103/PhysRevLett.106.220501

[259] Zhao L, Yin Z, Wang S, Chen W, Chen H, Guo G, Han Z. Measurement-device-independent quantum coin tossing. *Physical Review A* 2015; **92**(6): 062327. `doi:10.1103/PhysRevA.92.062327`

[260] Chor B, Kushilevitz E, Goldreich O, Sudan M. Private information retrieval. *Journal of the ACM* 1998; **45**(6): 965–981. `doi:10.1145/293347.293350`

[261] Giovannetti V, Lloyd S, Maccone L. Quantum private queries. *Physical Review Letters* 2008; **100**(23): 230502. `arXiv:0708.2992`, `doi:10.1103/PhysRevLett.100.230502`

[262] Giovannetti V, Lloyd S, Maccone L. Quantum private queries: security analysis. *IEEE Transactions on Information Theory* 2010; **56**(7): 3465–3477. `arXiv:0809.1934`, `doi:10.1109/tit.2010.2048446`

[263] Baumeler Ä, Broadbent A. Quantum private information retrieval has linear communication complexity. *Journal of Cryptology* 2015; **28**(1): 161–175. `arXiv:1304.5490`, `doi:10.1007/s00145-014-9180-2`

[264] Olejnik L. Secure quantum private information retrieval using phase-encoded queries. *Physical Review A* 2011; **84**(2): 022313. `doi:10.1103/PhysRevA.84.022313`

[265] Jakobi M, Simon C, Gisin N, Bancal J-D, Branciard C, Walenta N, Zbinden H. Practical private database queries based on a quantum-key-distribution protocol. *Physical Review A* 2011; **83**(2): 022301. `arXiv:1002.4360`, `doi:10.1103/PhysRevA.83.022301`

[266] Gao F, Liu B, Wen Q-Y, Chen H. Flexible quantum private queries based on quantum key distribution. *Optics Express* 2012; **20**(16): 17411–17420. `arXiv:1111.1511`, `doi:10.1364/oe.20.017411`

[267] Zhang J-L, Guo F-Z, Gao F, Liu B, Wen Q-Y. Private database queries based on counterfactual quantum key distribution. *Physical Review A* 2013; **88**(2): 022334. `doi:10.1103/PhysRevA.88.022334`

[268] Yang Y-G, Sun S-J, Xu P, Tian J. Flexible protocol for quantum private query based on B92 protocol. *Quantum Information Processing* 2014; **13**(3): 805–813. `doi:10.1007/s11128-013-0692-8`

[269] Wang C, Hao L, Zhao L-J. Implementation of quantum private queries using nuclear magnetic resonance. *Chinese Physics Letters* 2011; **28**(8): 080302. `doi:10.1088/0256-307X/28/8/080302`

[270] Chan P, Lucio-Martinez I, Mo X, Simon C, Tittel W. Performing private database queries in a real-world environment using a quantum protocol. *Scientific Reports* 2014; **4**: 5233. `doi:10.1038/srep05233`

[271] Yang Y-G, Zhang M-O, Yang R. Private database queries using one quantum state. *Quantum Information Processing* 2015; **14**(3): 1017–1024. `doi:10.1007/s11128-014-0902-z`

[272] Shi W-X, Liu X-T, Wang J, Tang C-J. Multi-bit quantum private query. *Communications in Theoretical Physics* 2015; **64**(3): 299–304. `doi:10.1088/0253-6102/64/3/299`

[273] Liu B, Gao F, Huang W, Wen Q. QKD-based quantum private query without a failure probability. *Science China Physics, Mechanics & Astronomy* 2015; **58**(10): 100301. `arXiv:1511.05267`, `doi:10.1007/s11433-015-5714-3`

[274] Shi R-H, Mu Y, Zhong H, Zhang S. Quantum oblivious set-member decision protocol. *Physical Review A* 2015; **92**(2): 022309. `doi:10.1103/PhysRevA.92.022309`

[275] Shi R-H, Mu Y, Zhong H, Cui J, Zhang S. An efficient quantum scheme for private set intersection. *Quantum Information Processing* 2016; **15**(1): 363–371. `doi:10.1007/s11128-015-1165-z`

[276] Gottesman D, Chuang I. Quantum digital signatures. 2001: `arXiv:quant-ph/0105032`

[277] Buhrman H, Cleve R, Watrous J, de Wolf R. Quantum fingerprinting. *Physical Review Letters* 2001; **87**(16): 167902. `doi:10.1103/PhysRevLett.87.167902`

[278] Xu F, Arrazola JM, Wei K, Wang W, Palacios-Avila P, Feng C, Sajeed S, Lütkenhaus N, Lo H-K. Experimental quantum fingerprinting with weak coherent pulses. *Nature Communications* 2015; **6**: 8735. `arXiv:1503.05499`, `doi:10.1038/ncomms9735`

[279] Dunjko V, Wallden P, Andersson E. Quantum digital signatures without quantum memory. *Physical Review Letters* 2014; **112**(4): 040502. `arXiv:1309.1375`, `doi:10.1103/PhysRevLett.112.040502`

[280] Collins RJ, Donaldson RJ, Dunjko V, Wallden P, Clarke PJ, Andersson E, Jeffers J, Buller GS. Realization of quantum digital signatures without

the requirement of quantum memory. *Physical Review Letters* 2014; **113**(4): 040502. `doi:10.1103/PhysRevLett.113.040502`

[281] Wallden P, Dunjko V, Kent A, Andersson E. Quantum digital signatures with quantum-key-distribution components. *Physical Review A* 2015; **91**(4): 042304. `arXiv:1403.5551`, `doi:10.1103/PhysRevA.91.042304`

[282] Arrazola JM, Wallden P, Andersson E. Multiparty quantum signature schemes. *Quantum Information and Computation* 2016; **16**(5–6): 435–464. `arXiv:1505.07509`

[283] Donaldson RJ, Collins RJ, Kleczkowska K, Amiri R, Wallden P, Dunjko V, Jeffers J, Andersson E, Buller GS. Experimental demonstration of kilometer-range quantum digital signatures. *Physical Review A* 2016; **93**(1): 012329. `arXiv:1509.07827`, `doi:10.1103/PhysRevA.93.012329`

[284] Croal C, Peuntinger C, Heim B, Khan I, Marquardt C, Leuchs G, Wallden P, Andersson E, Korolkova N. Free-space quantum signatures using heterodyne measurements. *Physical Review Letters* 2016; **117**(10): 100503. `arXiv:1604.03708`, `doi:10.1103/PhysRevLett.117.100503`

[285] Broadbent A, Fitzsimons J, Kashefi E. Universal blind quantum computation. Proceedings of the *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, October 25–27, 2009, pp. 517–526. `arXiv:0807.4154`, `doi:10.1109/focs.2009.36`

[286] Barz S, Kashefi E, Broadbent A, Fitzsimons JF, Zeilinger A, Walther P. Demonstration of blind quantum computing. *Science* 2012; **335**(6066): 303–308. `arXiv:1110.1381`, `doi:10.1126/science.1214707`

[287] Wehner S, Curty M, Schaffner C, Lo H-K. Implementation of two-party protocols in the noisy-storage model. *Physical Review A* 2010; **81**(5): 052336. `arXiv:0911.2302`, `doi:10.1103/PhysRevA.81.052336`

[288] Kent A. Unconditionally secure bit commitment. *Physical Review Letters* 1999; **83**(7): 1447–1450. `arXiv:quant-ph/9810068`, `doi:10.1103/PhysRevLett.83.1447`

[289] Halvorson H. Remote preparation of arbitrary ensembles and quantum bit commitment. *Journal of Mathematical Physics* 2004; **45**(12): 4920–4931. `arXiv:quant-ph/0310001`, `doi:10.1063/1.1812827`

[290] Kent A. Unconditionally secure bit commitment by transmitting measurement outcomes. *Physical Review Letters* 2012; **109**(13): 130501. `arXiv:1108.2879`, `doi:10.1103/PhysRevLett.109.130501`

[291] Croke S, Kent A. Security details for bit commitment by transmitting measurement outcomes. *Physical Review A* 2012; **86**(5): 052309. `doi:10.1103/PhysRevA.86.052309`

[292] Kaniewski J, Tomamichel M, Hänggi E, Wehner S. Secure bit commitment from relativistic constraints. *IEEE Transactions on Information Theory* 2013; **59**(7): 4687–4699. `arXiv:1206.1740`, `doi:10.1109/tit.2013.2247463`

[293] Lunghi T, Kaniewski J, Bussières F, Houlmann R, Tomamichel M, Kent A, Gisin N, Wehner S, Zbinden H. Experimental bit commitment based on quantum communication and special relativity. *Physical Review Letters* 2013; **111**(18): 180504. `arXiv:1306.4801`, `doi:10.1103/PhysRevLett.111.180504`

[294] Liu Y, Cao Y, Curty M, Liao S-K, Wang J, Cui K, Li Y-H, Lin Z-H, Sun Q-C, Li D-D, Zhang H-F, Zhao Y, Chen T-Y, Peng C-Z, Zhang Q, Cabello A, Pan J-W. Experimental unconditionally secure bit commitment. *Physical Review Letters* 2014; **112**(1): 010504. `arXiv:1306.4413`, `doi:10.1103/PhysRevLett.112.010504`

[295] Lunghi T, Kaniewski J, Bussières F, Houlmann R, Tomamichel M, Wehner S, Zbinden H. Practical relativistic bit commitment. *Physical Review Letters* 2015; **115**(3): 030502. `arXiv:1411.4917`, `doi:10.1103/PhysRevLett.115.030502`

[296] Chakraborty K, Chailloux A, Leverrier A. Arbitrarily long relativistic bit commitment. *Physical Review Letters* 2015; **115**(25): 250501. `arXiv:1507.00239`, `doi:10.1103/PhysRevLett.115.250501`

[297] Fehr S, Fillinger M. On the composition of two-prover commitments, and applications to multi-round relativistic commitments. In: *Advances in Cryptology – EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8–12, 2016, Proceedings, Part II*. Fischlin M,

Coron J-S (editors), Berlin: Springer, 2016, pp. 477–496. `arXiv:1507.00240`, `doi:10.1007/978-3-662-49896-5_17`

[298] Pivoluska M, Pawłowski M, Plesch M. Tight bound on the classical value of generalized Clauser–Horne–Shimony–Holt games. *Physical Review A* 2016; **94**(2): 022338. `arXiv:1601.08095`, `doi:10.1103/PhysRevA.94.022338`

[299] Verbanis E, Martin A, Houlmann R, Boso G, Bussières F, Zbinden H. 24-hour relativistic bit commitment. *Physical Review Letters* 2016; **117**(14): 140506. `arXiv:1605.07442`, `doi:10.1103/PhysRevLett.117.140506`

[300] Adlam E, Kent A. Device-independent relativistic quantum bit commitment. *Physical Review A* 2015; **92**(2): 022315. `arXiv:1504.00944`, `doi:10.1103/PhysRevA.92.022315`

[301] Colbeck R, Kent A. Variable-bias coin tossing. *Physical Review A* 2006; **73**(3): 032320. `arXiv:quant-ph/0508149`, `doi:10.1103/PhysRevA.73.032320`

[302] Kent A. Location-oblivious data transfer with flying entangled qudits. *Physical Review A* 2011; **84**(1): 012328. `arXiv:1102.2816`, `doi:10.1103/PhysRevA.84.012328`

[303] Pitalúa-García D. Spacetime-constrained oblivious transfer. *Physical Review A* 2016; **93**(6): 062346. `doi:10.1103/PhysRevA.93.062346`

[304] Lo H-K. Insecurity of quantum secure computations. *Physical Review A* 1997; **56**(2): 1154–1162. `arXiv:quant-ph/9611031`, `doi:10.1103/PhysRevA.56.1154`

[305] Buhrman H, Christandl M, Schaffner C. Complete insecurity of quantum protocols for classical two-party computation. *Physical Review Letters* 2012; **109**(16): 160501. `arXiv:1201.0849`, `doi:10.1103/PhysRevLett.109.160501`

[306] Rudolph T. The laws of physics and cryptographic security. 2002: `arXiv:quant-ph/0202143`

[307] Kent A. A no-summoning theorem in relativistic quantum theory. *Quantum Information Processing* 2013; **12**(2): 1023–1032. `arXiv:1101.4612`, `doi:10.1007/s11128-012-0431-6`

[308] Hayden P, May A. Summoning information in spacetime, or where and when can a qubit be?

Journal of Physics A: Mathematical and Theoretical 2016; **49**(17): 175304. `arXiv:1210.0913`, `doi:10.1088/1751-8113/49/17/175304`

[309] Renner R, Cirac JI. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Physical Review Letters* 2009; **102**(11): 110504. `arXiv:0809.2243`, `doi:10.1103/PhysRevLett.102.110504`

[310] Patel KA, Dynes JF, Lucamarini M, Choi I, Sharpe AW, Yuan ZL, Penty RV, Shields AJ. Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks. *Applied Physics Letters* 2014; **104**(5): 051123. `arXiv:1402.1508`, `doi:10.1063/1.4864398`

[311] Fröhlich B, Dynes JF, Lucamarini M, Sharpe AW, Tam SWB, Yuan Z, Shields AJ. Quantum secured gigabit optical access networks. *Scientific Reports* 2015; **5**: 18121. `doi:10.1038/srep18121`

[312] Hughes RJ, Nordholt JE, McCabe KP, Newell RT, Peterson CG, Somma RD. Network-centric quantum communications with application to critical infrastructure protection. 2013: `arXiv:1305.0305`

[313] Ghatak A, Thyagarajan K. *Introduction to Fiber Optics*. Cambridge: Cambridge University Press, 1998.

[314] Agrawal GP. *Fiber-Optic Communication Systems*, 4th edition. New York: Wiley, 2010.

[315] Pirandola S, Laurenza R, Ottaviani C, Banchi L. Fundamental limits of repeaterless quantum communications. *Nature Communications* 2017; **8**: 15043. `arXiv:1510.08863`, `doi:10.1038/ncomms15043`

[316] Bechmann-Pasquinucci H, Tittel W. Quantum cryptography using larger alphabets. *Physical Review A* 2000; **61**(6): 062308. `arXiv:quant-ph/9910095`, `doi:10.1103/PhysRevA.61.062308`

[317] Bourennane M, Karlsson A, Björk G. Quantum key distribution using multilevel encoding. *Physical Review A* 2001; **64**(1): 012306. `doi:10.1103/PhysRevA.64.012306`

[318] Cerf NJ, Bourennane M, Karlsson A, Gisin N. Security of quantum key distribution using *d*-level systems. *Physical Review Letters* 2002; **88**(12): 127902. `arXiv:quant-ph/0107130`, `doi:10.1103/PhysRevLett.88.127902`

[319] Comandar LC, Fröhlich B, Lucamarini M, Patel KA, Sharpe AW, Dynes JF, Yuan ZL, Penty RV, Shields AJ. Room temperature single-photon detectors for high bit rate quantum key distribution. *Applied Physics Letters* 2014; **104**(2): 021101. `arXiv:1402.2210`, `doi:10.1063/1.4855515`

[320] Sangouard N, Simon C, Minář J, Zbinden H, de Riedmatten H, Gisin N. Long-distance entanglement distribution with single-photon sources. *Physical Review A* 2007; **76**(5): 050301. `arXiv:0706.1924`, `doi:10.1103/PhysRevA.76.050301`

[321] Sangouard N, Simon C, de Riedmatten H, Gisin N. Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics* 2011; **83**(1): 33–80. `arXiv:0906.2699`, `doi:10.1103/RevModPhys.83.33`

[322] Shenoy HA, Srikanth R, Srinivas T. Efficient quantum random number generation using quantum indistinguishability. *Fluctuation and Noise Letters* 2013; **12**(4): 1350020. `doi:10.1142/S021947751350020X`

[323] Tang Y-L, Yin H-L, Zhao Q, Liu H, Sun X-X, Huang M-Q, Zhang W-J, Chen S-J, Zhang L, You L-X, Wang Z, Liu Y, Lu C-Y, Jiang X, Ma X, Zhang Q, Chen T-Y, Pan J-W. Measurement-device-independent quantum key distribution over untrustful metropolitan network. *Physical Review X* 2016; **6**(1): 011024. `arXiv:1509.08389`, `doi:10.1103/PhysRevX.6.011024`

[324] Comandar LC, LucamariniM, FröhlichB, Dynes JF, Sharpe AW, Tam SWB, Yuan ZL, Penty RV, Shields AJ. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nature Photonics* 2016; **10**(5): 312–315. `arXiv:1509.08137`, `doi:10.1038/nphoton.2016.50`

[325] Fröhlich B, Dynes JF, Lucamarini M, Sharpe AW, Yuan Z, Shields AJ. A quantum access network. *Nature* 2013; **501**(7465): 69–72. `arXiv:1309.6431`, `doi:10.1038/nature12493`

[326] Tang YL, Yin HL, Chen SJ, Liu Y, Zhang WJ, Jiang X, Zhang L, Wang J, You LX, Guan JY, Yang DX, Wang Z, Liang H, Zhang Z, Zhou N, Ma X, Chen TY, Zhang Q, Pan JW. Field test of measurement-device-independent quantum key distribution. *IEEE Journal of Selected Topics in Quantum Electronics* 2015; **21**(3): 116–122. `doi:10.1109/jstqe.2014.2361796`

[327] Yin H-L, Chen T-Y, Yu Z-W, Liu H, You L-X, Zhou Y-H, Chen S-J, Mao Y, Huang M-Q, Zhang W-J, Chen H, Li MJ, Nolan D, Zhou F, Jiang X, Wang Z, Zhang Q, Wang X-B, Pan J-W. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical Review Letters* 2016; **117**(19): 190501. `arXiv:1606.06821`, `doi:10.1103/PhysRevLett.117.190501`

[328] Valivarthi R, Lucio-Martinez I, Chan P, Rubenok A, John C, Korchinski D, Duffin C, Marsili F, Verma V, Shaw MD, Stern JA, Nam SW, Oblak D, Zhou Q, Slater JA, Tittel W. Measurement-device-independent quantum key distribution: from idea towards application. *Journal of Modern Optics* 2015; **62**(14): 1141–1150. `arXiv:1501.07307`, `doi:10.1080/09500340.2015.1021725`

[329] Briegel HJ, Dür W, Cirac JI, Zoller P. Quantum repeaters: the role of imperfect local operations in quantum communication. *Physical Review Letters* 1998; **81**(26): 5932–5935. `doi:10.1103/PhysRevLett.81.5932`

[330] Dür W, Briegel HJ, Cirac JI, Zoller P. Quantum repeaters based on entanglement purification. *Physical Review A* 1999; **59**(1): 169–181. `arXiv:quant-ph/9808065`, `doi:10.1103/PhysRevA.59.169`

[331] Halder M, Beveratos A, Gisin N, Scarani V, Simon C, Zbinden H. Entangling independent photons by time measurement. *Nature Physics* 2007; **3**(10): 692–695. `arXiv:0704.0758`, `doi:10.1038/nphys700`

[332] Peters NA, Lim CC. Practical multiplexing for third generation quantum repeaters. Proceedings of the *Conference on Lasers and Electro-Optics*, San Jose, California, June 5–10, 2016, Optical Society of America, pp. FM1N.8. `doi:10.1364/CLEO_QELS.2016.FM1N.8`

[333] Muralidharan S, Kim J, Lütkenhaus N, Lukin MD, Jiang L. Ultrafast and fault-tolerant quantum communication across long distances. *Physical Review Letters* 2014; **112**(25): 250501. `arXiv:1310.5291`, `doi:10.1103/PhysRevLett.112.250501`

[334] Muralidharan S, Jiang L. Potential for ultrafast quantum communication. *SPIE Newsroom* 2016: `doi:10.1117/2.1201512.006150`

[335] Li L, Muralidharan S, Kim J, Lutkenhaus N, Lukin M, Jiang L. Highly efficient long-distance quantum communication: a blueprint for implementa-

tion. Presented at *APS March Meeting*, San Antonio, Texas, March 2–6, 2015.

[336] Azuma K, Tamaki K, Lo H-K. All-photonic quantum repeaters. *Nature Communications* 2015; **6**: 6787. `doi:10.1038/ncomms7787`

[337] Simon C, de Riedmatten H, Afzelius M, Sangouard N, Zbinden H, Gisin N. Quantum repeaters with photon pair sources and multimode memories. *Physical Review Letters* 2007; **98**(19): 190503. `arXiv:quant-ph/0701239`, `doi:10.1103/PhysRevLett.98.190503`

[338] Childress L, Taylor JM, Sørensen AS, Lukin MD. Fault-tolerant quantum communication based on solid-state photon emitters. *Physical Review Letters* 2006; **96**(7): 070504. `doi:10.1103/PhysRevLett.96.070504`

[339] Sangouard N, Dubessy R, Simon C. Quantum repeaters based on single trapped ions. *Physical Review A* 2009; **79**(4): 042340. `arXiv:0902.3127`, `doi:10.1103/PhysRevA.79.042340`

[340] Zwerger M, Dür W, Briegel HJ. Measurement-based quantum repeaters. *Physical Review A* 2012; **85**(6): 062326. `arXiv:1204.2178`, `doi:10.1103/PhysRevA.85.062326`

[341] Mazurek P, Grudka A, Horodecki M, Horodecki P, Łodyga J, Pankowski Ł, Przysiezna A. Long-distance quantum communication over noisy networks without long-time quantum memory. *Physical Review A* 2014; **90**(6): 062311. `arXiv:1202.1016`, `doi:10.1103/PhysRevA.90.062311`

[342] Razavi M, Piani M, Lütkenhaus N. Quantum repeaters with imperfect memories: cost and scalability. *Physical Review A* 2009; **80**(3): 032301. `doi:10.1103/PhysRevA.80.032301`

[343] Eisaman MD, Fan J, Migdall A, Polyakov SV. Single-photon sources and detectors. *Review of Scientific Instruments* 2011; **82**(7): 071101. `doi:10.1063/1.3610677`

[344] Lounis B, Orrit M. Single-photon sources. *Reports on Progress in Physics* 2005; **68**(5): 1129. `doi:10.1088/0034-4885/68/5/R04`

[345] Buckley S, Rivoire K, Vučković J. Engineered quantum dot single-photon sources. *Reports on Progress in Physics* 2012; **75**(12): 126503. `arXiv:1210.1234`, `doi:10.1088/0034-4885/75/12/126503`

[346] Komiyama S, Astafiev O, Antonov V, Kutsuwa T, Hirai H. A single-photon detector in the far-infrared range. *Nature* 2000; **403**(6768): 405–407. `doi:10.1038/35000166`

[347] Cova S, Ghioni M, Lotito A, Rech I, Zappa F. Evolution and prospects for single-photon avalanche diodes and quenching circuits. *Journal of Modern Optics* 2004; **51**(9–10): 1267–1288. `doi:10.1080/09500340408235272`

[348] Bao H, Bao W, Wang Y, Zhou C, Chen R. Finite-key analysis of a practical decoy-state high-dimensional quantum key distribution. *Journal of Physics A: Mathematical and Theoretical* 2016; **49**(20): 205301. `arXiv:1605.04536`, `doi:10.1088/1751-8113/49/20/205301`

[349] Stiller B, Khan I, Jain N, Jouguet P, Kunz-Jacques S, Diamanti E, Marquardt C, Leuchs G. Quantum hacking of continuous-variable quantum key distribution systems: Realtime Trojan-horse attacks. Proceedings of the *2015 Conference on Lasers and Electro-Optics (CLEO)*, May 10–15, 2015, pp. FF1A.7. `doi:10.1364/cleo_qels.2015.ff1a.7`

[350] Hillery M. Quantum cryptography with squeezed states. *Physical Review A* 2000; **61**(2): 022309. `arXiv:quant-ph/9909006`, `doi:10.1103/PhysRevA.61.022309`

[351] Ralph TC. Continuous variable quantum cryptography. *Physical Review A* 1999; **61**(1): 010303. `doi:10.1103/PhysRevA.61.010303`

[352] Reid MD. Quantum cryptography with a predetermined key, using continuous-variable Einstein–Podolsky–Rosen correlations. *Physical Review A* 2000; **62**(6): 062308. `arXiv:quant-ph/9909030`, `doi:10.1103/PhysRevA.62.062308`

[353] Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. *Physical Review Letters* 2002; **88**(5): 057902. `arXiv:quant-ph/0109084`, `doi:10.1103/PhysRevLett.88.057902`

[354] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using gaussian-modulated coherent states. *Nature* 2003; **421**(6920): 238–241. `arXiv:quant-ph/0312016`, `doi:10.1038/nature01289`

[355] Gottesman D, Preskill J. Secure quantum key distribution using squeezed states. In: *Quantum Information with Continuous Variables*. Braunstein SL, Pati

AK (editors), Dordrecht: Springer, 2003, pp. 317–356. doi:10.1007/978-94-015-1258-9_22

[356] Cerf NJ, Lévy M, Van Assche G. Quantum distribution of Gaussian keys using squeezed states. *Physical Review A* 2001; **63**(5): 052311. arXiv:quant-ph/0008058, doi:10.1103/PhysRevA.63.052311

[357] Qin H, Kumar R, Alleaume R. Quantum hacking on a practical continuous-variable quantum cryptosystem by inserting an external light. *Proceedings of SPIE* 2015; **9648**(96480V. doi:10.1117/12.2195433

[358] Ralph TC. Security of continuous-variable quantum cryptography. *Physical Review A* 2000; **62**(6): 062306. arXiv:quant-ph/0007024, doi:10.1103/PhysRevA.62.062306

[359] Lorenz S, Korolkova N, Leuchs G. Continuous-variable quantum key distribution using polarization encoding and post selection. *Applied Physics B* 2004; **79**(3): 273–277. arXiv:quant-ph/0403064, doi:10.1007/s00340-004-1574-7

[360] Qi B, Lougovski P, Pooser R, Grice W, Bobrek M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Physical Review X* 2015; **5**(4): 041009. arXiv:1503.00662, doi:10.1103/PhysRevX.5.041009

[361] Soh DBS, Brif C, Coles PJ, Lütkenhaus N, Camacho RM, Urayama J, Sarovar M. Self-referenced continuous-variable quantum key distribution protocol. *Physical Review X* 2015; **5**(4): 041010. arXiv:1503.04763, doi:10.1103/PhysRevX.5.041010

[362] Pirandola S, Mancini S, Lloyd S, Braunstein SL. Continuous-variable quantum cryptography using two-way quantum communication. *Nature Physics* 2008; **4**(9): 726–730. arXiv:quant-ph/0611167, doi:10.1038/nphys1018

[363] Huang D, Huang P, Lin D, Zeng G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports* 2016; **6**: 19201. doi:10.1038/srep19201

[364] Leverrier A, Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Physical Review Letters* 2009; **102**(18): 180504. arXiv:0812.4246, doi:10.1103/PhysRevLett.102.180504

[365] Leverrier A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Physical Review Letters* 2015; **114**(7): 070501. arXiv:1408.5689, doi:10.1103/PhysRevLett.114.070501

[366] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf NJ, Tualle-Brouri R, McLaughlin SW, Grangier P. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A* 2007; **76**(4): 042305. arXiv:0706.4255, doi:10.1103/PhysRevA.76.042305

[367] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P, Diamanti E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics* 2013; **7**(5): 378–381. arXiv:1210.6216, doi:10.1038/nphoton.2013.63

[368] Huang J-Z, Weedbrook C, Yin Z-Q, Wang S, Li H-W, Chen W, Guo G-C, Han Z-F. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Physical Review A* 2013; **87**(6): 062329. arXiv:1302.0090, doi:10.1103/PhysRevA.87.062329

[369] Laudenbach F, Pacher C, Fung C-HF, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P, Hübel H. Continuous-variable quantum key distribution with Gaussian modulation – the theory of practical implementations. 2017: arXiv:1703.09278

[370] Diamanti E, Leverrier A. Distributing secret keys with quantum continuous variables: principle, security and implementations. *Entropy* 2015; **17**(9): 6072–6092. arXiv:1506.02888, doi:10.3390/e17096072

[371] Tomamichel M, Renner R. Uncertainty relation for smooth entropies. *Physical Review Letters* 2011; **106**(11): 110506. arXiv:1009.2015, doi:10.1103/PhysRevLett.106.110506

[372] Li Z, Zhang Y-C, Xu F, Peng X, Guo H. Continuous-variable measurement-device-independent quantum key distribution. *Physical Review A* 2014; **89**(5): 052301. arXiv:1312.4655, doi:10.1103/PhysRevA.89.052301

[373] Ma X-C, Sun S-H, Jiang M-S, Gui M, Liang L-M. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. *Physical Review A* 2014; **89**(4): 042335. arXiv:1312.5025, doi:10.1103/PhysRevA.89.042335

[374] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein SL, Lloyd S, Gehring T, Jacobsen CS, Andersen UL. High-rate measurement-device-independent quantum cryptography. *Nature Photonics* 2015; **9**(6): 397–402. `doi:10.1038/nphoton.2015.83`

[375] Pirandola S, Ottaviani C, Spedalieri G, Weedbrook C, Braunstein SL, Lloyd S, Gehring T, Jacobsen CS, Andersen UL. Reply to 'Discrete and continuous variables for measurement-device-independent quantum cryptography'. *Nature Photonics* 2015; **9**(12): 773–775. `doi:10.1038/nphoton.2015.207`

[376] Huang D, Huang P, Lin D, Wang C, Zeng G. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Optics Letters* 2015; **40**(16): 3695–3698. `doi:10.1364/ol.40.003695`

[377] Etcheverry S, Cañas G, Gómez ES, Nogueira WAT, Saavedra C, Xavier GB, Lima G. Quantum key distribution session with 16-dimensional photonic states. *Scientific Reports* 2013; **3**: 2316. `arXiv:1308.0019`, `doi:10.1038/srep02316`

[378] Mirhosseini M, Magaña-Loaiza OS, O'Sullivan MN, Rodenburg B, Malik M, Lavery MPJ, Padgett MJ, Gauthier DJ, Boyd RW. High-dimensional quantum cryptography with twisted light. *New Journal of Physics* 2015; **17**(3): 033033. `arXiv:1402.7113`, `doi:10.1088/1367-2630/17/3/033033`

[379] Zhang L, Silberhorn C, Walmsley IA. Secure quantum key distribution using continuous variables of single photons. *Physical Review Letters* 2008; **100**(11): 110504. `doi:10.1103/PhysRevLett.100.110504`

[380] Zhang Z, Mower J, Englund D, Wong FNC, Shapiro JH. Unconditional security of time-energy entanglement quantum key distribution using dual-basis interferometry. *Physical Review Letters* 2014; **112**(12): 120506. `arXiv:1311.0825`, `doi:10.1103/PhysRevLett.112.120506`

[381] Tian Z, Hongchao Z, Robert DH, Catherine L, Varun BV, Adriana EL, Alessandro R, Joshua CB, Richard PM, Thomas G, Sae Woo N, Francesco M, Matthew DS, Zheshen Z, Ligong W, Dirk E, Gregory WW, Jeffrey HS, Franco NCW. Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding. *New Journal of Physics* 2015; **17**(2): 022002. `doi:10.1088/1367-2630/17/2/022002`

[382] Chen L, Jordan S, Liu Y-K, Moody D, Peralta R, Perlner R, Smith-Tone D. *Report on Post-Quantum Cryptography*. NISTIR 8105, Gaithersburg, Maryland: National Institute of Standards and Technology, 2016. `doi:10.6028/NIST.IR.8105`

[383] Shor PW. Why haven't more quantum algorithms been found? *Journal of the ACM* 2003; **50**(1): 87–90. `doi:10.1145/602382.602408`

[384] Bernstein DJ, Buchmann J, Dahmen E. *Post-Quantum Cryptography*. Berlin: Springer, 2009. `doi:10.1007/978-3-540-88702-7`

[385] Peikert C. A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science* 2016; **10**(4): 283–424. `doi:10.1561/0400000074` `https://eprint.iacr.org/2015/939`

[386] Micciancio D, Regev O. Lattice-based cryptography. In: *Post-Quantum Cryptography*. Bernstein DJ, Buchmann J, Dahmen E (editors), Berlin: Springer, 2009, pp. 147–191. `doi:10.1007/978-3-540-88702-7_5`

[387] Berger TP, Cayrel P-L, Gaborit P, Otmani A. Reducing key length of the McEliece cryptosystem. In: *Progress in Cryptology – AFRICACRYPT 2009: Second International Conference on Cryptology in Africa, Gammarth, Tunisia, June 21–25, 2009. Proceedings*. Preneel B (editor), Berlin: Springer, 2009, pp. 77–97. `doi:10.1007/978-3-642-02384-2_6`

[388] Bernstein DJ, Lange T, Peters C. Attacking and defending the McEliece cryptosystem. In: *Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008, Cincinnati, Ohio, October 17–19, 2008 Proceedings*. Buchmann J, Ding J (editors), Berlin: Springer, 2008, pp. 31–46. `doi:10.1007/978-3-540-88403-3_3`

[389] McEliece RJ. A public-key cryptosystem based on algebraic coding theory. In: *The Deep Space Network Progress Report, DSN PR 42–44*. Pasadena, California: Jet Propulsion Laboratory, 1978, pp. 114–116.

[390] Dubois V, Fouque P-A, Shamir A, Stern J. Practical cryptanalysis of SFLASH. In: *Advances in Cryptology – CRYPTO 2007: 27th Annual International Cryptology Conference, Santa Barbara, California, August 19–23, 2007. Proceedings*. Menezes A (editor), Berlin: Springer, 2007, pp. 1–12. `doi:10.1007/978-3-540-74143-5_1`

[391] Patarin J. Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88. In: *Advances in Cryptology – CRYPT0'95: 15th Annual International Cryptology Conference Santa Barbara, California, August 27–31, 1995 Proceedings*. Coppersmith D (editor), Berlin: Springer, 1995, pp. 248–261. `doi:10.1007/3-540-44750-4_20`

[392] Patarin J. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In: *Advances in Cryptology – EUROCRYPT'96: International Conference on the Theory and Application of Cryptographic Techniques Saragossa, Spain, May 12–16, 1996 Proceedings*. Maurer U (editor), Berlin: Springer, 1996, pp. 33–48. `doi:10.1007/3-540-68339-9_4`

[393] Bernstein DJ. Introduction to post-quantum cryptography. In: *Post-Quantum Cryptography*. Bernstein DJ, Buchmann J, Dahmen E (editors), Berlin: Springer, 2009, pp. 1–14. `doi:10.1007/978-3-540-88702-7_1`

[394] Mozaffari-Kermani M, Azarderakhsh R. Reliable hash trees for post-quantum stateless cryptographic hash-based signatures. Proceedings of the *2015 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFTS)*, October 12–14, 2015, pp. 103–108. `doi:10.1109/dft.2015.7315144`

[395] Song F. A note on quantum security for post-quantum cryptography. In: *Post-Quantum Cryptography: 6th International Workshop, PQCrypto 2014, Waterloo, Ontario, Canada, October 1–3, 2014. Proceedings*. Mosca M (editor), Cham, Switzerland: Springer, 2014, pp. 246–265. `arXiv:1409.2187`, `doi:10.1007/978-3-319-11659-4_15`

[396] Clifton R, Bub J, Halvorson H. Characterizing quantum theory in terms of information-theoretic constraints. *Foundations of Physics* 2003; **33**(11): 1561–1591. `arXiv:quant-ph/0211089`, `doi:10.1023/a:1026056716397`

[397] Smolin JA. Can quantum cryptography imply quantum mechanics? 2003: `arXiv:quant-ph/0310067`

[398] Halvorson H, Bub J. Can quantum cryptography imply quantum mechanics? Reply to Smolin. 2003: `arXiv:quant-ph/0311065`

[399] Spekkens RW. Evidence for the epistemic view of quantum states: A toy theory. *Physical Review A* 2007; **75**(3): 032110. `arXiv:quant-ph/0401052`, `doi:10.1103/PhysRevA.75.032110`