

Measurement-device-independent quantum key distribution with classical Bob and no joint measurement

Guang Ping He*

School of Physics, Sun Yat-sen University, Guangzhou 510275, China

Measurement-device-independent quantum key distribution (MDI-QKD) provides a method for secret communication whose security does not rely on trusted measurement devices. In all existing MDI-QKD protocols, the participant Charlie has to perform the Bell state measurement or other joint measurements. Here we propose an MDI-QKD protocol which requires individual measurements only. Meanwhile, all operations of the receiver Bob are classical, without the need for preparing and measuring quantum systems. Thus the implementation of the protocol has a lower technical requirement on Bob and Charlie.

I. INTRODUCTION

Quantum key distribution (QKD) is known to be a method for two parties Alice and Bob to exchange classical secret information by transmitting quantum states, usually encoded using photons [1]. In principle, the security of QKD against eavesdropping can be based solely on the validity of the axioms of quantum mechanics. But in practice, such an unconditional security is much harder to achieve, due to the imperfection of the actual devices used in the implementation schemes [2]. Especially, the theory-practice deviation of photon detectors could leave room for side-channel attacks and blinding attacks [3–5].

Then came the measurement-device-independent (MDI)-QKD [6] as a solution. It allows the detectors to be handled by a third party Charlie, who cannot learn the secret information of Alice and Bob even if he himself is the eavesdropper. That is, the security of MDI-QKD does not need to rely on the assumption that the detectors are controlled by honest parties. Note that it does not necessarily mean that MDI-QKD has to be a three-party cryptography. Instead, when there are only Alice and Bob, and the latter owns the detectors, then “Charlie” can be understood as the backdoor or spyware built into the detectors, which can communicate with or be controlled remotely by the eavesdropper. The existence of unconditionally secure MDI-QKD protocols mean that Bob can use the detectors from any manufacturer, even those from his enemy, while his secret information will remain secure. On the other hand, comparing with full device-independent QKD (see Refs. [7–12] and the references therein) which is secure even when the eavesdropper can access to not only the detectors but also other devices, MDI-QKD is much more feasible and the key rate can be very high. Therefore, it immediately caught great interests [13–19].

But the measurements in MDI-QKD are more complicated than those in previous conventional ones. In some of the conventional QKD such as the Bennett-Brassard84 (BB84) protocol [1], Bob can simply perform individual

measurements on every single photon from Alice one by one. In MDI-QKD such as the protocol in Ref. [6], however, both Alice and Bob send photons to Charlie, and Charlie needs to perform the Bell state measurement on both photons simultaneously. In a recent variation of MDI-QKD called the twin-field (TF) MDI-QKD [20–22], both Alice and Bob send weak coherent pulses and Charlie measures the interference when they combine on a beam splitter. Either way, Charlie’s operations are joint measurements. There was an MDI-QKD protocol claimed to be free from joint measurements [23], but its measurement for Charlie is actually a joint measurement on two pulses sent to him at different times. While all the above joint measurements are experimentally available with state-of-the-art technology, they are undoubtedly less efficient and convenient than individual measurements. Also, as pointed out in Ref. [23], most MDI-QKD protocols have to deal with the difficulty of the synchronization of the arrival times and phases of the photons or pulses from Alice and Bob.

In this paper, we will propose an MDI-QKD basing on a completely different route, so that strictly no joint measurement is needed. This makes it possible to enjoy the advantage of MDI (i.e., the protocol remains secure even when the measurement devices are controlled by the eavesdropper) using conventional optical detectors for individual measurements, which are generally more efficient than those for joint measurements. Moreover, our protocol also has an intriguing feature that the operations of Bob can all be considered classical.

The structure of the rest of this paper is as follows. In the next section, the general theoretical description of our protocol will be given, with its security discussed in section III. Then in section IV, we study a possible practical implementation of the protocol. The reason why Bob can be classical is elaborated in section V. Finally we summarize the result and compare its pros and cons with existing MDI-QKD protocols.

II. THE THEORETICAL SCHEME

Unlike previous MDI-QKD protocols where Alice and Bob both send photons or coherent pulses for Charlie

*Electronic address: hegp@mail.sysu.edu.cn

to measure, in our proposal only Alice sends photons to Charlie, while Bob performs some secret operations on these photons in the middle. To make the theoretical security analysis more explicit, here we first give a general description of our MDI-QKD protocol without going into the details on the implementation of the carriers of the quantum states and how they are transmitted, and consider the ideal case where the transmissions and detections are free from any loss and error.

Our protocol:

(1) For $i = 1$ to n :

(1.1) Alice sends Bob a batch of m quantum registers $\psi_1^{(i)}, \psi_2^{(i)}, \dots, \psi_m^{(i)}$ where m is an even number and $m \geq 8$ is recommended. Each register is a two-level system, whose state $|\psi_j^{(i)}\rangle$ ($j = 1, \dots, m$) is randomly chosen from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Here $|0\rangle$ and $|1\rangle$ are two orthogonal states of the two-level system, and $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$.

(1.2) Bob rearranges the order of the quantum registers. That is, he chooses randomly a permutation operation P_i and applies it on $\psi_1^{(i)}, \psi_2^{(i)}, \dots, \psi_m^{(i)}$ to obtain $|\phi_1^{(i)} \phi_2^{(i)} \dots \phi_m^{(i)}\rangle = P_i |\psi_1^{(i)} \psi_2^{(i)} \dots \psi_m^{(i)}\rangle$. Bob keeps his choice of P_i secret, which will never be announced throughout the entire protocol. Then he sends $\phi_1^{(i)}, \phi_2^{(i)}, \dots, \phi_m^{(i)}$ to Charlie, who is in charge of the measurement devices.

(1.3) Charlie is supposed to measure each of $\phi_1^{(i)}, \dots, \phi_{m/2}^{(i)}$ in the rectilinear basis $\{|0\rangle, |1\rangle\}$, and measure each of $\phi_{m/2+1}^{(i)}, \dots, \phi_m^{(i)}$ in the diagonal basis $\{|+\rangle, |-\rangle\}$. Then he announces the measurement results to Bob.

(1.4) Since Bob himself knows the permutation P_i , he deduces the measurement result of each of $\psi_1^{(i)}, \psi_2^{(i)}, \dots, \psi_m^{(i)}$ from Charlie's announced information. Then they repeat steps (1.1)-(1.4) for the next i , where Bob should choose a different P_i in step (1.2).

(2) Alice announces the bases (but not the exact state information) of all the $n \times m$ registers $\psi_j^{(i)}$ ($i = 1, \dots, n$, $j = 1, \dots, m$).

(3) The security check: Bob picks a portion of the registers and asks Alice to announce their exact states. Then he checks whether Charlie's measurement results matches Alice's announced states whenever Charlie has measured the corresponding registers in the correct basis (i.e., he has measured $|0\rangle, |1\rangle$ ($|+\rangle, |-\rangle$) in the rectilinear basis (the diagonal basis)), or the two states in the same basis occur with approximately equal probabilities whenever Charlie has measured the registers in the wrong basis.

(4) If no suspicious result is found, among the rest registers which were not picked for the security check, Bob keeps those which Charlie has measured in the correct basis, and announces their indices i, j to Alice. Since both Alice and Bob know the exact state of this portion of registers, they take $|0\rangle, |+\rangle$ as the bit 0 and $|1\rangle, |-\rangle$ as the bit 1, and thus obtain the raw secret key.

III. SECURITY ANALYSIS

We have to admit that at the present moment, we are unable to give a rigorous mathematical security proof of the protocol which could be sufficiently general to cover any cheating strategy that may potentially exist, like the proofs in Refs. [24, 25] for the BB84 protocol. And we wish that, like the case of the original MDI-QKD protocol [6], related rigorous proofs can be eventually completed by successive studies from various contributors [26–32]. But for now, at least we can obtain the following conclusions in a heuristic way.

Theorem 1. Without knowing Bob's permutation operations, Charlie's announcing the measurement result dishonestly will be discovered with a non-trivial probability.

Proof: In our protocol, Charlie is required to announce the measurement result in step (1.3), before Alice announces the bases of the quantum states in step (2). Therefore, he cannot delay his announcement until he learns the basis information. For each i , there are totally $m!$ possible choices for the m -body permutation operation P_i . When Charlie does not know P_i , for each specific $\phi_j^{(i)}$, from his point of view it could be any of $\psi_1^{(i)}, \psi_2^{(i)}, \dots, \psi_m^{(i)}$. Even if he intercepted so that he owns or has owned all $\psi_1^{(i)}, \psi_2^{(i)}, \dots, \psi_m^{(i)}$, there is no measurement on $\psi_1^{(i)}, \psi_2^{(i)}, \dots, \psi_m^{(i)}$ that can help him know the correct basis for $\phi_j^{(i)}$. Consequently, no matter he measures $\phi_j^{(i)}$ as required by the protocol or delays his measurement while announcing a random measurement result, his announced basis stands probability $1/2$ to be correct. In this case, if he announces a result opposite to what is obtained in his measurement (or announces a random result without actually performing the measurement) as the state of $\phi_j^{(i)}$, there is probability $\varepsilon_{ij} = 1$ ($\varepsilon_{ij} = 1/2$) that it will conflict with the actual state prepared by Alice. Once this $\phi_j^{(i)}$ is picked for the security check in step (3), Bob will discover such a cheating. If Charlie totally did this for k registers, then the probability for him to pass the security check will be at the order of magnitude of $(1 - \varepsilon/2)^{\lambda k}$, which drops exponentially as k increases. Here $\varepsilon \in [1/2, 1]$ and λ marks the portion of the registers that are picked for the security check and Charlie's announced measurement bases happen to be correct.

The above theorem guarantees that the performance of the measurement devices in the protocol is checkable, so that Alice and Bob can arrive at the same raw key correctly.

Meanwhile, the result below also holds.

Theorem 2. Without knowing Bob's permutation operations, the eavesdropper (including Charlie) cannot obtain a non-trivial amount of information on the secret key of Alice and Bob.

Proof: According to step (4), to learn a single bit of the raw key, the eavesdropper must know whether the state

of Alice's corresponding quantum register $\psi_j^{(i)}$ belongs to $\{|0\rangle, |+\rangle\}$ or $\{|1\rangle, |-\rangle\}$. Theorem 1 ensures that Bob can deduce the correct measurement result of $\psi_j^{(i)}$. So if we treat Bob and all measurement results as a whole party, then the situation between Alice and Bob is actually the same as that of the BB84 protocol. As a result, it is not hard to see that any intercept-resend attack on the quantum transmission channel between Alice and Bob cannot pass the security check with a non-trivial probability. That is, the eavesdropper (no matter he is Charlie himself or someone else) cannot intercept and measure Alice's state before it enters Bob's site. On the other hand, it is indeed possible to eavesdrop the measurement result of $\phi_j^{(i)}$ (by either intercept the state at Bob's output or get the information directly from Charlie). But as long as Bob's permutation P_i is kept secret, the relationship between $\psi_j^{(i)}$ and $\phi_j^{(i)}$ cannot be deduced. That is, eavesdropping at Bob's output and/or Charlie's site is insufficient for deducing the secret bits either.

Putting theorems 1 and 2 together, we can see that the hinge to the security of the protocol is to keep Bob's permutations P_i unknown to the eavesdropper. According to the protocol, Bob chooses every P_i by himself, and applies it locally in his own site without announcing anything about it throughout the protocol. Therefore, it seems easy to meet this requirement in principle.

Nevertheless, in practice it is more complicated. The implementation details of how the quantum states are transmitted may leave rooms for the eavesdropping. To be precise, when the eavesdropper takes control on both the input and output of Bob's site and is able to replace Alice's states with something else he prepared himself, it is possible for him to learn what operation is applied within Bob's site. Note that each P_i is an m -qubit permutation operation. When describing Alice's m -qubit state as a 2^m -dimensional vector, P_i is corresponding to a $2^m \times 2^m$ matrix. As there are $m!$ possible choices for P_i , its matrix has $m!$ independent elements. Denote $|\eta^{(i)}\rangle$ as the state that the eavesdropper inputs to Bob's site. Then the output state is $P_i |\eta^{(i)}\rangle$. The eavesdropper's task is to deduce P_i by measuring $P_i |\eta^{(i)}\rangle$. To determine P_i unambiguously, $P_i |\eta^{(i)}\rangle$ should be orthogonal to $P_{i'} |\eta^{(i')}\rangle$ for any $i' \neq i$, i.e.,

$$\langle \eta^{(i')} | P_{i'}^\dagger P_i | \eta^{(i)} \rangle = 0. \quad (1)$$

But as long as $m \geq 4$, there is

$$m! > 2^m. \quad (2)$$

Thus it is clear that using a 2^m -dimensional system as $|\eta^{(i)}\rangle$ (which has 2^m orthogonal states only) is insufficient for determining P_i unambiguously from all the $m!$ possible choices. Instead, the eavesdropper has to use a higher-dimensional quantum system. Consequently,

there is a difference in the dimension of the physical systems between the eavesdropper's $|\eta^{(i)}\rangle$ and Alice's actual $|\psi_1^{(i)} \psi_2^{(i)} \dots \psi_m^{(i)}\rangle$ to Bob's input. The question is whether Bob can tell the difference in practice.

A safe bet is to use the "teleportation trick": Bob does not allow the physical carriers of Alice's states to enter his site directly. Instead, he uses quantum teleportation [33] to transfer the quantum information of Alice's states to his own physical systems, whose dimension is completely under his control. With this method, he can be sure that the eavesdropper cannot fake Alice's physical systems with other systems and use them as a Trojan horse device to learn the information on his operation P_i (see Ref. [6] of Ref. [6] for details). So we can indeed achieve an unconditionally secure implementation of our protocol in practice. However, the quantum teleportation procedure requires Bob to perform additional measurements, making the implementation more inconvenient. Moreover, handing these measurement tasks to Charlie may cause extra security problems, while letting Bob himself to perform the measurements will make the protocol no longer an MDI one. Thus, to achieve both unconditional security and the MDI property simultaneously, we must take extra care on how the protocol is actually implemented in practice.

IV. A POSSIBLE PRACTICAL IMPLEMENTATION

In Fig.1, we illustrate a possible implementation scheme of our protocol, where Alice's single-photon sources, Bob's optical delays and Charlie's detectors are

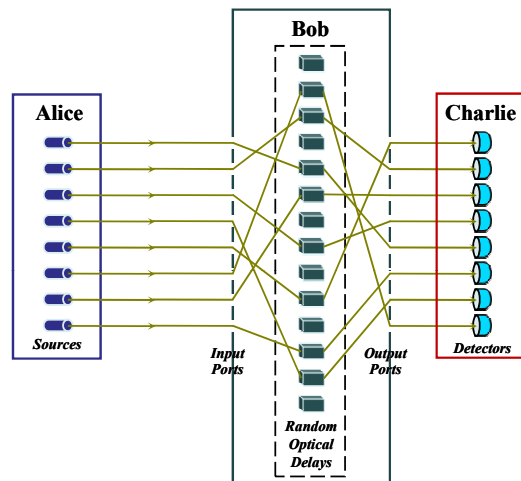


FIG. 1: Diagram of a practical implementation scheme of our MDI-QKD protocol with $m = 8$. All green lines stand for optical fibers. The combination of the optical fibers inside Bob's site should be arranged differently in each i th ($i = 1, \dots, n$) round of the protocol.

all connected via optical fibers. The whole duration of the quantum communication in the protocol is divided into n time slots. In each i th slot ($i = 1, \dots, n$), Alice sends a photon from each of the m sources, with the polarization direction prepared randomly as 0° , 90° , 45° or 135° , which stand for the states $|0\rangle$, $|1\rangle$, $|+\rangle$ or $|-\rangle$, respectively. She does not need to send these m photons at exactly the same moment. As long as their sending times belong to the same time slot then it will be fine. All photons then pass through Bob's site and finally reach Charlie's detectors. Bob should choose a different combination of the optical fibers between his input and output ports for each time slot, which serves as choosing a different permutation operation P_i on the m photons. For easy analysis and understanding on the security, we drew $m = 8$ pairs of optical sources and detectors in Fig.1. But in practice, by using the time division multiplexing technique [34, 35], only one source and one detector will be sufficient.

Like many other practical QKD systems, Bob should also use single-mode optical fibers, wavelength filters and single-photon filters [36] right after his input ports, to ensure that photons with extra dimensions or other characterizing information cannot enter his site [5], and the eavesdropper cannot input many photons to a single port simultaneously. Otherwise, in every time slot the eavesdropper can simply prepare and send different numbers of photons into different input ports of Bob. For example, he sends 1 photon to the first input port, and 2 photons to the second input port Then by measuring the photon number at each of Bob's output port, he can deduce Bob's permutation P_i . Meanwhile, he intercepts all Alice's photons, applies P_i on them and resends them to Charlie. As long as all these operations can be completed fast enough, he can hack the protocol without being revealed.

Nevertheless, though the use of the above filters can prevent the eavesdropper from inputting many photons to one input port simultaneously, he can still send these photons one by one. To avoid such a cheating, Bob should shut down all input ports before and after each time slot. Meanwhile, it is recommended to use low speed optical fibers in Bob's site (or at least use a short length of them after each input port) instead of better ones, to serve as a time-based photon number filter. Suppose that his optical fibers can transmit x bits per second, while the duration of each time slot is τ seconds. Then Bob should better choose optical fibers with speed

$$x \ll m/\tau. \quad (3)$$

In the most ideal case, when there is $x < 2/\tau$, we can be sure that no eavesdropper can input more than one photon to an input port during a time slot. This may seem technically challenging, because it means that the duration of each time slot should be as short as

$$\tau < 2/x, \quad (4)$$

which implies that Bob needs very high speed switches to

toggle the input ports on and off. But if the time division multiplexing technique is used for the implementation of our protocol, a single time slot will be shared by all the m ports. Then Eq. (4) will be replaced by

$$\tau < 2m/x. \quad (5)$$

We can see that it becomes possible to find suitable switches for the implementation when m is high.

For simplicity, the aforementioned filters and shutters are not shown in Fig.1. Other than that, when comparing with the above theoretical description of our protocol, the most distinct feature of Fig.1 is the presence of the optical delays in Bob's site. They are adopted against eavesdropping too. This is because, when these optical delays are not present and Bob connects the input ports to the output ports in random order using optical fibers directly, the eavesdropper (regardless he is Charlie or not) can still learn Bob's P_i using the following strategy. In each time slot, though Bob's filters and shutters limit the eavesdropper to input a single photon to each port only, each photon can be input at a slightly different time. That is, the eavesdropper can send a photon into Bob's first input port at time t_1 , another photon into Bob's second input port at time t_2 , a third photon into Bob's third input port at time t_3 , ... , and a photon into Bob's m th input port at time t_m . Here $t_1 < t_2 < \dots < t_m$ and they are all within the same time slot, while their difference is much smaller than the duration time τ . The eavesdropper then performs measurements at Bob's output ports to see when will a photon be detected at each port. Through the time order of the photon detection, he can deduce Bob's permutation P_i even though he sends only one photon to each port.

To defeat this attack strategy, we need the optical delays shown in the dashed box of Fig.1. The number of these delays should be larger than m , and each of them is set to a different delay time. Then Bob's randomizing the connection between these optical delays and the input ports is equivalent to introducing a random delay time to the photon from each port. In this case, if the eavesdropper applies the above attack by sending m photons in sequence, these photons will leave Bob's output ports in a randomized time order, so that the eavesdropper can no longer deduce which is the input port that each photon was sent from, making the attack futile.

V. CLASSICALITY OF BOB

The concept "QKD with classical Bob" was previously proposed by Boyer, Kenigsberg and Mor [37]. In their protocol, Bob's technical capability is limited to the following three operations: (1) measuring the qubit from Alice in the computational basis $\{|0\rangle, |1\rangle\}$, (2) preparing a (fresh) qubit in the computational basis and sending it, and (3) reflecting the qubit from Alice back undisturbed. The authors elaborated that such operations can be considered classical, because unlike conventional QKD

(e.g., the BB84 protocol) that uses both the measurement bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, the receiver Bob in their protocol does not involve any nonorthogonal states nor noncommuting operations, even though his operations are actually performed on quantum systems. Such a usage of the term “classical Bob” is also adopted later in Ref. [38].

Similarly, in our protocol Bob’s permutations P_i are a group of commutable operations which also exist in classical world. When using the practical implementation scheme in the previous section, we can see that P_i can be realized simply by arranging the connection of the optical fibers between the input ports, output ports and optical delays. Choosing different P_i is basically the same as resetting the jumpers in a classical telephone switchboard, and Bob’s role is very similar to a classical telephone operator. In a more practical setting, instead of plugging and unplugging the optical fibers manually, rearranging the connection between the input ports, output ports and optical delays can be implemented efficiently using microelectromechanical systems (MEMS) [39, 40] or other optical cross-connect (OXC) devices [41, 42]. Still, OXC devices are also widely used in classical information optics, so that they should be considered as classical despite that they can handle photons carrying quantum information as well. Therefore, our protocol also takes a “classical Bob” only. Furthermore, our Bob does not need the sources and detectors for preparing and measuring quantum systems. In this sense, it is somehow more classical than the “classical Bob” in Refs. [37, 38].

VI. DISCUSSIONS

In summary, we proposed an MDI-QKD protocol and considered its possible implementation in practice. Com-

paring with previous proposals, we should note that the original MDI-QKD protocol [6] has two distinctive advantages: (i) all detector side channels are removed so that its security does not need to rely on trusted measurement devices, and (ii) the secure distance with conventional lasers can be twice as that of conventional QKD while the key rate remains high in practice.

Ours does not have the advantage (ii) because in practical QKD nowadays, the secure distance is limited by the distance between the optical sources and the detectors. In our protocol (or conventional QKD such as the BB84 protocol), it means the distance between Alice and Charlie (or Bob), while in the original MDI-QKD, both Alice and Bob send photons or coherent pulses to Charlie so that the secure distance is the distance from Alice to Charlie plus the distance from Charlie to Bob.

But the advantage (i) remains in our protocol, and it also has two more advantages. First, it no longer needs joint measurements, and second, Bob can be classical. It is worth studying whether there can be other practical implementation schemes of our theoretical protocol so that Bob’s filters and shutters can be further simplified, enabling more users with low technical capacity to enjoy the advantages of quantum cryptography in practice.

Acknowledgements

The work was supported in part by Guangdong Basic and Applied Basic Research Foundation under Grant No. 2019A1515011048.

-
- [1] C. H. Bennett and G. Brassard, in *Proc. IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175. Quantum cryptography: public key distribution and coin tossing
 - [2] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, *Contemp. Phys.* **57**, 3 (2016). Attacks on practical quantum key distribution systems (and how to prevent them)
 - [3] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Nat. Photon.* **4**, 686 (2010). Hacking commercial quantum cryptography systems by tailored bright illumination
 - [4] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtz, and V. Makarov, *Nat. Commun.* **2**, 349 (2011). Full-field implementation of a perfect eavesdropper on a quantum cryptography system
 - [5] C. Navas-Merlo and J. C. Garcia-Escartin, *Quantum Inf. Process.* **20**, 196 (2021). Detector blinding attacks on counterfactual quantum key distribution
 - [6] H. -K. Lo, M. Curty, and B. Qi, *Phys. Rev. Lett.* **108**, 130503 (2012). Measurement-device-independent quantum key distribution
 - [7] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007). Device-independent security of quantum cryptography against collective attacks
 - [8] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, *New J. Phys.* **11**, 045021 (2009). Device-independent quantum key distribution secure against collective attacks
 - [9] M. McKague, *New J. Phys.* **11**, 103037 (2009). Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices
 - [10] L. Masanes, S. Pironio, and A. Acín, *Nat. Commun.* **2**, 238 (2011). Secure device-independent quantum key distribution with causally independent measurement devices
 - [11] M. Lucamarini, G. Vallone, I. Gianani, P. Mataloni, and G. Di Giuseppe, *Phys. Rev. A* **86**, 032325 (2012). Device-independent entanglement-based Bennett 1992 protocol

- [12] V. Scarani, *Acta Physica Slovaca* **62**, 347 (2012). The device-independent outlook on quantum physics (lecture notes on Bell inequalities)
- [13] P. Chan, J. A. Slater, I. Lucio-Martinez, A. Rubenok, and W. Tittel, *Opt. Express* **22**, 12716 (2014). Modeling a measurement-device-independent quantum key distribution system
- [14] Z. Y. Tang, Z. F. Liao, F. H. Xu, B. Qi, L. Qian, and H. -K. Lo, *Phys. Rev. Lett.* **112**, 190503 (2014). Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution
- [15] Y. -L. Tang, et. al., *Phys. Rev. Lett.* **113**, 190501 (2014). Measurement-device-independent quantum key distribution over 200 km
- [16] H. -L. Yin, W. -F. Cao, Y. Fu, Y. -L. Tang, Y. Liu, T. -Y. Chen, Z. -B. Chen, *Opt. Lett.* **39**, 5451 (2014). Long distance measurement-device-independent quantum key distribution with coherent-state superpositions
- [17] S. Pirandola, et. al., *Nat. Photon.* **9**, 397 (2015). High-rate measurement-device-independent quantum cryptography
- [18] Y. -L. Tang, et al., *Phys. Rev. X* **6**, 011024 (2016). Measurement-device-independent quantum key distribution over untrustful metropolitan network
- [19] H. -L. Yin, et al., *Phys. Rev. Lett.* **117**, 190501 (2016). Measurement-device-independent quantum key distribution over a 404 km optical fibre
- [20] M. Lucamarini, Z. L. Yuan, J. F. Dynes and A. J. Shields, *Nature* **557**, 400 (2018). Overcoming the rate-distance limit of quantum key distribution without quantum repeaters
- [21] X. Zhong, J. Hu, M. Curty, L. Qian, and H. -K. Lo, *Phys. Rev. Lett.* **123**, 100506 (2019). Proof-of-principle experimental demonstration of twin-field type quantum key distribution
- [22] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, *Nat. Photon.* **13**, 334 (2019). Experimental quantum key distribution beyond the repeaterless secret key capacity
- [23] M. Alhussein and K. Inoue, in *Proc. 78th JSAP Autumn Meeting* (Fukuoka, Japan, 2017). Available at: <https://confit.atlas.jp/guide/event-img/jsap2017a/5p-A414-4/public/pdf>. MDI-DPS-QKD with no joint measurement
- [24] H. -K. Lo and H. F. Chau, *Science* **283**, 2050 (1999). Unconditional security of quantum key distribution over arbitrarily long distances
- [25] P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85**, 441 (2000). Simple proof of security of the BB84 quantum key distribution protocol
- [26] M. Curty, F. H. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H. -K. Lo, *Nat. Commun.* **5**, 3732 (2014). Finite-key analysis for measurement-device-independent quantum key distribution
- [27] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, *Phys. Rev. A* **97**, 052327 (2018). Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks
- [28] Z. Chen, Y. -C. Zhang, G. Wang, Z. Li, and H. Guo, *Phys. Rev. A* **98**, 012314 (2018). Composable security analysis of continuous-variable measurement-device-independent quantum key distribution with squeezed states for coherent attacks
- [29] J. Lin and N. Lütkenhaus, *Phys. Rev. A* **98**, 042332 (2018). Simple security analysis of phase-matching measurement-device-independent quantum key distribution
- [30] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, *Phys. Rev. A* **99**, 062332 (2019). Versatile security analysis of measurement-device-independent quantum key distribution
- [31] H. -X. Ma, P. Huang, T. Wang, D. -Y. Bai, S. -Y. Wang, W. -S. Bao, and G. -H. Zeng, *Phys. Rev. A* **100**, 052330 (2019). Security bound of continuous-variable measurement-device-independent quantum key distribution with imperfect phase reference calibration
- [32] X. Wu, Y. Wang, S. Li, W. Zhang, D. Huang, and Y. Guo, *Quantum Inf. Process.* **18**, 372 (2019). Security analysis of passive measurement-device-independent continuous-variable quantum key distribution with almost no public communication
- [33] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993). Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels
- [34] P. D. Townsend, *Nature* **385**, 47 (1997). Quantum cryptography on multiuser optical fibre networks
- [35] J. Martínez-Mateo, A. Ciurana, and V. Martin, *IEEE Photonics Tech. Lett.* **26**, 881 (2014). Quantum key distribution based on selective post-processing in passive optical networks
- [36] L. De Santis, et. al., *Nature Nanotech.* **12**, 663 (2017). A solid-state single-photon filter
- [37] M. Boyer, D. Kenigsberg, T. Mor, *Phys. Rev. Lett.* **99**, 140501 (2007). Quantum key distribution with classical bob
- [38] Z. -W. Sun, R. -G. Du, and D. -Y. Long, *Int. J. Quantum Inf.* **11**, 1350005 (2013). Quantum key distribution with limited classical Bob
- [39] V. A. Aksyuk, et al., *IEEE Photonics Tech. Lett.* **15**, 587 (2003). 238×238 micromechanical optical cross connect
- [40] J. Kim, et al., *IEEE Photonics Tech. Lett.* **15**, 1537 (2003). 1100 x 1100 Port MEMS-based optical crossconnect with 4-dB maximum loss
- [41] H. Tsushima, S. Hanatani, T. Kanetake, J. A. Fee, and S. -K. Liu, *Hitachi Review* **47**, 85 (1998). Optical cross-connect system for survivable optical layer networks
- [42] S. V. Kartalopoulos, *IEEE Comm. Mag.* **39**, 22 (2001). Emerging technologies at the dawn of the millennium