Measurement-device-independent quantum cryptography

Feihu Xu, Marcos Curty, Bing Qi, and Hoi-Kwong Lo

(Invited Paper)

Abstract—In theory, quantum key distribution (QKD) provides information-theoretic security based on the laws of physics. Owing to the imperfections of real-life implementations, however, there is a big gap between the theory and practice of QKD, which has been recently exploited by several quantum hacking activities. To fill this gap, a novel approach, called measurement-device-independent QKD (mdiQKD), has been proposed. It can remove all side-channels from the measurement unit, arguably the most vulnerable part in QKD systems, thus offering a clear avenue towards secure QKD realisations. Here, we review the latest developments in the framework of mdiQKD, together with its assumptions, strengths and weaknesses.

Index Terms—Quantum key distribution (QKD), quantum cryptography, quantum hacking, measurement-device-independent QKD, quantum communication.

I. INTRODUCTION

Secure communication is essential in today’s digital society, with billions of users accessing the Internet via different terminals and mobile devices. The goal is to transmit a secret message from a sender (Alice) to a receiver (Bob) such that an eavesdropper (Eve) cannot access the message. It is well known that this problem can be solved using the one-time-pad protocol [1]. This protocol requires, however, that Alice and Bob share a secret key. With this key, Alice can encrypt the message (so-called plaintext) into a ciphertext that is unintelligible to Eve. On receiving the ciphertext, Bob can recover the plaintext by using his key. Importantly, the security of the one-time-pad protocol relies only on the secrecy of the shared key. This renders the problem of secure communication essentially equivalent to that of distributing a key securely. This is the task of quantum key distribution (QKD) [2].

Unlike the widely-used public-key cryptography [3], which bases its security on unproven computational assumptions, QKD can provide information-theoretically secure key distribution based solely on the laws of physics. Indeed, if a quantum computer is ever built, many classical public-key schemes will become insecure [4]. In sharp contrast, QKD will always remain secure despite the computational and technological power of Eve. That is, when combined with the one-time-pad protocol, QKD can be used to achieve perfectly secure communication.

A. Quantum key distribution (QKD)

The best-known QKD protocol is the so-called BB84 scheme introduced by Bennett and Brassard in 1984 [2]. Its security is based on the quantum no-cloning theorem, which states that it is impossible (for Eve) to make perfect copies of an unknown quantum state. Therefore, the higher the amount of information that Eve learns about a quantum signal, the higher the amount of disturbance that she causes on it. By sacrificing a randomly chosen portion of their data, Alice and Bob can estimate this disturbance (by calculating, for instance, the quantum bit error rate (QBER)) and thus bound Eve’s information about the distributed key. This compromised information can then be removed from the final key by using privacy amplification methods. The unconditional security of QKD has been rigorously proven in several papers [5], [6], [7], [8], [9].

B. Quantum hacking

While in theory QKD is unconditionally secure, in practice, however, there is an important gap between the assumptions made in the security proofs of QKD and the actual implementations. This is so because real devices suffer from inevitable imperfections that can cause them to operate quite differently from the mathematical models used to prove security. As a result, Eve could exploit such imperfections to learn the distributed key without being detected.

The first successful quantum hacking attack against a commercial QKD system was the time-shift attack [10]. It is based on an earlier theoretical proposal introduced in [11] (see Fig. 1a). Standard single-photon detectors (SPDs) such as, for example, InGaAs avalanche photodiodes, are often operated in a gated mode [12]. This means that their detection efficiency is time-dependent [13]. Importantly, since every QKD system contains at least two detectors to measure two different bit values, it is usually quite difficult to guarantee that both detectors have precisely the same detection efficiency all the time. In this scenario, Eve can simply shift the arrival time of each signal such that one detector has a much higher detection efficiency than the other [11]. As a result, she could obtain partial information about the final key without introducing almost any error.

Recently, a more powerful attack—the so-called detector blinding attack—was introduced in [14]. It allows Eve to learn the whole key without being detected. The procedure
is as follows (see Fig. 1b). Eve sends bright light to Bob’s detectors to force them enter into the so-called linear mode operation [14]. In so doing, the SPDs are no longer sensitive to single-photon pulses but they behave like classical intensity photo-detectors. As a consequence, Eve can now fully control which detector “clicks” just by sending Bob a tailored light pulse. This attack has been successfully implemented against both commercial [14], [15], [16] and research [17] QKD setups.

Quantum hacking has attracted a lot of research interest in recent years, and several attacks have been demonstrated experimentally [18], [19], [20], [21], [22], [23], [24], [25], [26]. Most of them exploit loopholes in Bob’s measurement system [18], [20], [21], [22], [24], [25], [26], which can be considered as the Achilles heel of QKD implementations. This is so because Eve can send Bob any signal she wishes, which makes the protection of Bob’s device quite difficult. In contrast, Alice can in principle protect her source by using, for instance, optical isolators. It is therefore reasonable to expect that she can determine the quantum states that she prepares and then include this information in the security analysis [27].

C. Countermeasures against quantum hacking

Currently there are at least four main possible approaches to avoid the problem of quantum hacking and recover the security of QKD implementations.

The first solution consists in obtaining “precise mathematical models” for all the devices and then include this information into the security proof [28], [29]. However, as QKD components are complex apparatuses, this approach is unfortunately very challenging to realise in practice.

The second one is what we call “patches”. Fortunately, once a particular attack is known, it is typically relatively easy to find an appropriate countermeasure against it [30], [31]. The main drawbacks of this solution are, however, unanticipated attacks. This is so because this approach only protects against known hacking strategies. Therefore, its security resembles that of classical cryptography.

The third solution is called device-independent QKD (diQKD) [32], [33], [34], [35]. Here, Alice and Bob do not need to know how their devices operate, but they can treat them as two “black boxes”. It requires, however, that certain assumptions are satisfied (see Table I). For instance, Alice and Bob need to guarantee that there is no leakage of unwanted information from their measurement apparatuses. In this scenario, it is possible to prove the security of diQKD based solely on the violation of a Bell inequality, which certifies the existence of quantum correlations. Remarkably, this approach can remove all side-channels from QKD implementations. Its main drawback, however, is that it needs a loophole-free Bell test which so far has never been performed. Also, the expected secret key rate at practical distances is unfortunately very limited with current technology (of the order of $10^{-10}$ bits per signal) [36], [37]. Still, diQKD could be a viable solution for short distance transmission in the future with improved technology.

In summary, the first solution is very difficult to realise in practice, the second one is ad hoc and cannot provide information-theoretic security, and diQKD is unfeasible with present-day technology. The rest of the paper is dedicated to analyse the fourth solution, which is called measurement-device-independent QKD (mdiQKD) [38]. As will be discussed below, this approach can remove all side-channels from the measurement unit, which is (as discussed previously) the weakest part of a QKD realisation. Most importantly, mdiQKD is fully practical with current technology and it allows QKD with a high key rate and at a long distance. Therefore, mdiQKD offers a clear avenue to bridge the gap between theory and practice in QKD.

II. MEASUREMENT-DEVICE-INDEPENDENT QKD

To understand the working principle of mdiQKD, let us first introduce an Einstein-Podolsky-Rosen (EPR) based QKD protocol (see Fig. 2a). Each of Alice and Bob prepares an EPR pair and sends half of it to an untrusted third party, Charles. Charles is supposed to perform an entanglement swapping operation on the incoming signals via a Bell state measurement (BSM), and then broadcast his measurement results. Once this
step is completed, Alice and Bob measure their halves of the EPR pairs by using two conjugate bases (the rectilinear basis $Z$, or the diagonal basis $X$) that they select at random. Importantly, by doing so they can determine whether or not Charles is honest. For this, they can compare a randomly chosen subset of their data to test if it satisfies the expected correlations associated with the Bell state declared by Charles.

Interestingly, this protocol can also be implemented in a “time-reversal” fashion (see Fig. 2b). This is so because Charles’ operations commute with those of Alice and Bob. Therefore, one can reverse the order of the measurements. That is, it is not necessary that Alice and Bob wait for Charles’ results in order to measure their halves of the EPR pairs, but they can measure them beforehand. Note that Charles’ BSM is only used to check the parity of Alice’s and Bob’s bits and, therefore, it does not reveal any information about the individual bit values. This rephrases the original EPR based QKD protocol into an equivalent prepare-and-measure scheme where Alice and Bob directly send Charles BB84 states and Charles performs the measurements. Most importantly, like in the original EPR based QKD protocol, Alice and Bob can test the honesty of Charles by just comparing a random portion of their signals.

This time-reversal scenario has been studied in\textsuperscript{1} \cite{39}, \cite{40}. Unfortunately, however, these important works offered very limited performance and, therefore, they had been largely forgotten by the QKD community. For instance, the scheme in \cite{39} requires perfect single-photon sources and long-term quantum memories, which renders it impractical with current technology. Inamori’s scheme \cite{40} uses practical weak coherent pulses (WCPs) but it does not include decoy states, as it was proposed long before the advent of the decoy-state method\textsuperscript{2} \cite{41}, \cite{42}, \cite{43}. The main merits of the mdiQKD proposal introduced in \cite{38} are twofold: first, it realised the importance of the results in \cite{39}, \cite{40} to remove all detector side-channels from QKD implementations and, second, it significantly improves the system performance with practical signals by including decoy states.

An example of a possible mdiQKD implementation is illustrated in Fig. 3a \cite{38}. The protocol can be summarised in the following three steps (see the caption of Fig. 3 for further details):

Step 1: Alice and Bob prepare phase-randomised WCPs (together with decoy signals) in the BB84 states and send them to an untrusted relay Charles.

Step 2: If Charles is honest, he performs a BSM that projects Alice’s and Bob’s signals into a Bell state. In any case, he announces whether or not his measurements are successful, including the Bell states obtained.

Step 3: Post-processing: Alice and Bob keep the data corresponding to Charles’ successful measurement results and discard the rest. Also, they post-select the events where they employ the same basis and, based on the outcomes announced by Charles, say Alice flips part of her bits to correctly correlate them with those of Bob. Finally, they use the decoy-state method to estimate the gain and QBER of the single-photon contributions.

Note that opposed to diQKD, now there is no need to protect Charles’ measurement unit from unwanted leakage of information to the outside (see Table I). Indeed, this device can be fully controlled or even manufactured by Eve. This is significant because it means that there is no need to certify

\textsuperscript{1} Note that this approach also resembles that proposed in \cite{6}, where Bob teleports any incoming signal from outside to himself by setting up a teleportation gateway inside his own secured laboratory. In so doing, it is possible to remove all side-channels from his measurement unit. However, note that the authors of \cite{6} considered that the BSM that is required for teleportation could be trusted.

\textsuperscript{2} The key idea of the decoy-state method is to send a sequence of signals each of which is chosen randomly from a set of different intensity settings (\textit{i.e.}, average photon numbers) and compute the gain (\textit{i.e.}, the transmission probability) and QBER for each intensity setting separately. This provides Alice and Bob with a better estimation of the behaviour of the quantum channel, and it boosts a significant improvement of both the achievable secret key rate and distance.
the detectors in a QKD standardisation process. A small drawback of mdiQKD is that Alice and Bob need to know which states they send to Charles\textsuperscript{5}. However, as we have seen in Sec. I-B, it is reasonable to expect that they can indeed characterise their sources and protect their state preparation processes from Eve’s influence. Also, as will be discussed below in Sec. IV-C, recent results show that a full source characterisation is not absolutely necessary for mdiQKD to work [27], [45], [46].

In the asymptotic scenario where Alice and Bob send Charles an infinite number of signals, the secret key rate has the form [38]

\[
R \geq Q_{11}^{Z}[1 - H_{2}(e_{11}^{X})] - Q_{11}^{Z}f_{e}(E_{11}^{Z})H_{2}(E_{11}^{Z}),
\]

(1)

where \(Q_{11}^{Z}\) is the gain \(i.e.,\) the probability that Charles declares a successful result) when Alice and Bob send him one single-photon each in the Z basis; \(e_{11}^{X}\) is the phase error rate of these single-photon signals; \(Q_{11}^{Z}\) and \(E_{11}^{Z}\) represent, respectively, the gain and the quantum bit error rate (QBER) in the Z basis when Alice and Bob send Charles WCPs of intensity \(\mu; f_{e} \geq 1\) is the error correction inefficiency function, and \(H_{2}(x) = -x \log_{2}(x) - (1 - x) \log_{2}(1 - x)\) is the binary entropy function.

Eq. (1) assumes that Alice and Bob use the Z basis for key generation and the X basis for testing only [47]. The term \(Q_{11}^{Z}H_{2}(e_{11}^{X})\) corresponds to the information removed from the final key in the privacy amplification step of the protocol, while \(Q_{11}^{Z}f_{e}(E_{11}^{Z})H_{2}(E_{11}^{Z})\) is the information revealed by Alice in the error correction step. The quantities \(Q_{11}^{Z}\) and \(E_{11}^{Z}\) are directly measured in the experiment, while \(Q_{11}^{Z}\) and \(e_{11}^{X}\) can be estimated using the decoy-state method [38].

### III. Experimental Demonstrations

Up to date, four successful independent mdiQKD experimental realisations have already been reported [48], [49], [50], [51]. Table II includes a brief summary of their main features. In the POP (proof-of-principle) demonstrations [48], [49], both Alice and Bob send the same quantum state repeatedly without random selection of the encoding states or bases. Therefore, no secret key is actually distributed between Alice and Bob. In [50], [51], however, two real demonstrations with key exchange have been performed. Below, we review in more detail these results.

The main experimental challenge of mdiQKD is to perform a high-fidelity BSM between photons from different light sources, which is not required in conventional QKD schemes. Indeed, to obtain high-visibility two-photon interference (and, therefore, to have a low QBER), Alice’s photons should be indistinguishable from those of Bob\textsuperscript{6}. Furthermore, if one implements mdiQKD over telecom fibres, it is necessary to include feedback controls to compensate the time-dependent polarisation rotations and propagation delays caused by the fibres. Note that in standard QKD systems, this requirement can

\textsuperscript{5}In principle, one may suggest that first Charles sends strong light pulses (from the same laser) to both Alice and Bob, who then encode their bit values, attenuate the pulses, and send them back to Charles. However, note that this design could compromise the security of the whole system, as now Charles could try to interfere with Alice’s and Bob’s state preparation processes.
be relaxed by using phase encoding [52], [53], because the two optical pulses, which interfere with each other at the receiver’s end, pass through the same optical fibre and thus experience the same polarisation rotation and phase change. Therefore, one can achieve high interference visibility without performing any polarisation control. Nevertheless, this advantage of phase encoding (in comparison to other encoding schemes) cannot be directly translated to mdiQKD. The reason is that now Alice’s and Bob’s signals are generated from two independent lasers and they propagate through two independent quantum channels. Consequently, in mdiQKD, polarisation management is required in all encoding schemes.

The feasibility of generating indistinguishable photons from two independent lasers was already investigated in the original mdiQKD proposal [38], where the authors conducted a Hong-Ou-Mandel (HOM) experiment using two independent commercial off-the-shelf lasers. By carefully matching the central frequencies, the pulse shapes, the arrival times, and the polarisation states of the photons, an HOM interference visibility close to the theoretical value of 50% was observed at different average photon numbers (from 0.2 to 4). The near perfect HOM visibility implied that the photons generated by the two lasers were almost identical. The same method was also adopted in more recent studies to verify the indistinguishability of photons from different sources [48], [49], [50], [51].

So far, both time-bin [48], [50] and polarisation encoding [49], [51] mdiQKD have been demonstrated. In the first POP mdiQKD demonstration [48], an HOM interference experiment was conducted with photons generated by independent sources that travel through separate field-deployed fibres of lengths 6.2 km and 12.4 km, respectively. By performing automatic polarisation stabilisation, manual adjustment of the photons arrival time, and manual adjustment of the lasers frequency, a high interference visibility was obtained even under a real-world environment. The two light pulses constructing a time-bin signal were generated by modulating the output of a CW laser twice. When compared to other recent experimental implementations of mdiQKD [49], [50], [51], the scheme in [48] required higher laser frequency stability. This is so because the phase difference between Alice’s and Bob’s lasers must be constant within a time window corresponding to two time-bin pulses rather than to only a single laser pulse.

A similar time-bin encoding mdiQKD scheme was investigated in [50] (see Fig. 4). The authors performed a real mdiQKD demonstration with random selection of encoding states and bases. They made use of custom-made and specialised devices including high-efficiency up-conversion single-photon detectors. Here, the time-bin signals were generated by sending a laser pulse through an unbalanced fibre interferometer. Compared to [48], this approach relaxes the requirement on the frequency stability of two lasers but it needs phase stabilisation of the fibre interferometers.

Polarisation encoding mdiQKD was also performed by two independent research groups. In particular, [49] demonstrated that the polarisation rotation due to a long fibre could be compensated using conventional polarisation feedback control. [49] is a POP experiment and no key was actually exchanged. In [51], the authors performed a real mdiQKD demonstration over 10 km of single-mode fibre using solely commercial off-the-shelf devices. This implementation setup is shown in Fig. 5. The two lasers used in this experiment are two commercial frequency-stabilized lasers where the frequency of each laser is individually locked to a local gas cell that is integrated by the manufacturer. Thus, there is no optical or electronic link between the two lasers. Here, a finite-key security analysis [54] was applied to optimise the experimental parameters and to evaluate the final secure key rate. This rate is slightly lower than that in [50] due to the limited detection efficiency and repetition rate of the system.

All these experiments, when taken together, complete the cycle needed to demonstrate the feasibility of using off-the-shelf optoelectronic devices to build a QKD system that is immune to all detector side-channel attacks.

IV. THEORETICAL ASPECTS FOR MDI QKD

As we have seen in Sec. II, since practical and efficient single-photon sources are still unavailable, the original theoretical proposal of mdiQKD [38], together with the experimental realisations presented in the previous section, considers WCPs and decoy states instead. However, in order to apply the results of [38] to real-life systems, there are still some loose ends that need to be addressed. In particular, [38] assumes that Alice and Bob use an infinite number of decoy-state settings. Also, for simplicity, this study neglects statistical fluctuations due to the finite data size. In this section, we review the latest developments in mdiQKD to overcome these limitations.

A. Decoy-state protocol with a finite number of settings

The analysis of this scenario is basically the same as that of conventional decoy-state QKD systems [41], [42], [43]. The sole difference is that now both Alice and Bob send decoy signals to a common receiver (instead of only Alice sending decoy states to Bob), which makes the mathematics slightly more cumbersome. Fortunately, it has been shown that also in this situation it is enough if Alice and Bob employ just two decoy settings each. That is, this configuration can already provide them with a quite tight estimation of the relevant parameters that are needed to prove security (i.e., $Q_{11}$ and $e^{N}$ in Eq. (1)).

For instance, the authors of [55] proposed a numerical method (based on linear programming) for the case where Alice and Bob employ two (or three) decoy states each. Similarly, Refs. [56], [57] presented different analytical estimation approaches, based on Gaussian elimination, under the assumption that Alice and Bob can prepare a vacuum state. Also, following similar analytical lines, the authors of [58], [54] studied the situation where none of the two decoy signals are vacuum, because a vacuum state is relatively hard to realise in practice due to the finite extinction ratio of a practical intensity modulator [53]. More recently, [59] compared different decoy-state methods for mdiQKD and confirmed that two decoy settings are enough to obtain a near optimal estimation of the relevant parameters. That is, the use of three or more decoy intensities does not result in any significant improvement of the final secret key rate in neither the asymptotic nor the finite
Fig. 4. (Color online) Demonstration of mdiQKD using time-bin encoding realised in China [50]. (a) Alice (Bob) passes her (his) laser pulses through an unbalanced Mach-Zehnder (MZ) interferometer to generate two time-bin pulses. Three amplitude modulators (AMs) and a phase modulator (PM) are used to generate decoy states and encode the time-bin qubit. The pulses are then attenuated by an attenuator (ATT) and pass through 25 km fibre spools of each arm to the measurement unit. The pulses finally interfere at a 50:50 fibre beam-splitter (BS) to perform a BSM. The two outputs are detected by up-conversion detectors. (Part b) Schematic diagram of the up-conversion single-photon detector. In the figure: (PC) polarisation controller, (DM) dichroic mirror, (BP) band pass filter, and (SP) short pass filter. (Part c) Schematic diagram of the phase stabilisation setup. (Cir) circulator, (PS) phase shifter, and (PBS) polarising beam-splitter. (Reprinted Figure with permission from [50]).

Fig. 5. (Color online) Demonstration of mdiQKD using polarisation encoding realised in Toronto, Canada [51]. Each of the two CW frequency-locked lasers is attenuated by an optical attenuator (Attn) and modulated by an intensity modulator (IM), which is driven by an electrical pulse generator (PG), to prepare weak coherent pulses (WCPs). The phases of these pulses are uniformly modulated by a phase modulator (PM) for active phase randomisation. Next, an acousto-optic modulator (AOM) randomly modulates their intensities to implement the decoy-state protocol. Key bits are encoded into polarisation states of the WCPs using a polarisation modulator (Pol-M). Alice and Bob send their signals to Charles through a 5 km fibre spool. On receiving the transmission, Charles performs a BSM on the incoming pulses using a beam-splitter (BS) and a polarising beam-splitter (PBS) together with two commercial SPDs. Synchronisation is done with the help of an electrical delay generator (DG). In the figure: (PC) polarisation controller, (RNG) random number generator and (TIA) time interval analyser. (Figure reproduced from [51]).

data size regimes. All these results provide experimentalists a clear path to implement mdiQKD with WCPs and decoy states.

B. Finite-key security analysis

The second question that needs to be solved is related with the fact that any QKD realisation only produces a finite amount of data. Of course, a real-life QKD experiment is always completed in finite time, which means that the length of the output secret key is obviously finite. Thus, the parameter estimation procedure in QKD needs to take the statistical fluctuations of the different parameters into account. This problem has attracted a lot of research attention in recent years, and several security proofs in the finite-key regime for conventional QKD systems have been obtained [60], [61] (see also [62] for a review on this topic). Very recently, it was possible to obtain tight finite-key security bounds for both the BB84 protocol with single-photons [63] and the decoy-state BB84 scheme [64], [65]. These security bounds are valid against the most general attacks.

Similar techniques can also be applied to mdiQKD. For example, the authors of [55] made a first step in this direction and provided a finite-key security analysis that assumes a Gaussian distribution for the statistical fluctuations. Also, [66] includes an analogous study that is valid against particular types of attacks. More recently, [54] presented a finite-key security proof that is valid against general attacks and it does not assume any particular distribution for the statistical fluctuations. In addition, this result satisfies the “composable”
definition of the security of QKD [67], [68]. That is, the generated secret keys remain secure when they are employed as a resource for other cryptographic systems (e.g., the one-time-pad protocol). All these results confirm the feasibility of long-distance implementations of mdiQKD (for instance, say 100 km of optical fibre with 0.2 dB/km loss) with current technology and within a reasonable time-frame of signal transmission. As an illustration, Fig. 6 shows the simulation result presented in [54].

C. Further theoretical developments

1) Encoding schemes: The original theoretical proposal of mdiQKD [38] uses polarisation encoding. However, mdiQKD can be realised as well, as we have seen in Section III, using other encoding schemes like phase encoding [69], [70] or time-bin encoding [71]. Polarisation encoding is typically more suitable for free-space implementations due to the negligible birefringence of air, while phase encoding and time-bin encoding are usually more convenient for fibre-based realisations. In order to select the optimal experimental parameters for these implementations, detailed theoretical system models have been developed in [58] (for polarisation encoding), in [70] (for phase encoding), and in [71] (for time-bin encoding). Also, a parameter optimisation method has been presented in [59].

Of course, the channels that connect Alice and Bob with Charles are typically of different length and have different transmittances. Indeed, such asymmetric case is expected in most mdiQKD realisations [48]; it has been studied in [58].

2) Extending the covered distance and achievable secret key rate: One possible solution to achieve these goals is, of course, to use ultra-low loss fibres [72] in combination with high detection efficiency SPDs [73]. For instance, Fig. 7 shows the asymptotic secret key rate versus distance for both the decoy-state BB84 and mdiQKD, when the detection efficiency of the SPDs is 93% [73]. Other experimental parameters coincide with those of Fig. 6.

Alternatively, one could also include quantum memories in Charles’s measurement device. This last situation has been analysed in [74], [75] (see Fig. 8). The main idea is quite simple. Instead of performing a Bell state measurement (BSM) between each pair of signals received from Alice and Bob, Charles firstly stores the incoming photons in two heralded quantum memories, one for Alice’s signals and one for Bob’s signals. After that, he performs a BSM only between those photons that have been successfully stored in the memories. By doing so, he can increase the success probability of his measurement unit and, therefore, also the covered distance and achievable secret key rate are increased. In the figure: (QM) quantum memory, and (BSM) Bell state measurement.
been studied in [76]. Its main drawback, however, is its limited key rate. This is so because of the low detection efficiency of today’s SPDs [12] together with the fact that now one requires that two different BSMs are successful at the same time.

3) State preparation flaws: Recently, there have been also efforts to prove the security of mdiQKD when Alice’s and Bob’s devices are flawed [27], [69], or when their apparatuses are not fully characterised [45], [46]. Remarkably, the authors of [27] showed that state preparation flaws do not significantly affect the performance of mdiQKD. That is, it is not necessary that Alice’s and Bob’s state preparation process is very precise to obtain a good performance. Indeed, a modified version of mdiQKD where Alice and Bob send Charles only three different states can deliver the same key rate as the original scenario where they send him four BB84 states [27].

4) Alternative system implementations: The idea of mdiQKD is compatible as well with other QKD protocols like continuous-variable schemes [77], [78], [79] or the Scarani-Acin-Ribordy-Gisin scheme [80]. Also, it can be implemented with different types of sources [81], [82].

V. OUTLOOK

On the experimental side, it would be necessary to improve the performance of the mdiQKD implementations realised so far. For instance, current experimental demonstrations consider short-distance transmission (i.e., below 50 km) and their system clock rate is relatively low (below 2 MHz). For practical applications, it would be desirable to achieve longer distances (say around 100-200 km) and to use higher system clock rates (say 100MHz-1GHz). Using state-of-the-art SPDs [73], for example, could also help to substantially increase the final key generation rate.

It would be interesting as well to prove the feasibility of mdiQKD for free-space communications. Such implementation would constitute a first step towards future satellite-based mdiQKD networks, in which an untrusted satellite can be shared by many users. Moreover, continuous-variable mdiQKD demonstrations using standard telecom devices are still missing. Furthermore, in the long term, mdiQKD could be used to build a fibre-based QKD network with untrusted nodes, in which the users possess low cost, compact devices to transmit quantum states, while all the expensive calibration and measurement apparatuses are located within the network servers. This scenario is illustrated in Fig. 9.

Much work needs to be done as well on the theoretical side. For instance, as already discussed, a key assumption in mdiQKD is that Alice’s and Bob’s sources can be trusted. It would be therefore necessary to further investigate how this essential requirement could be guaranteed in practice. Also, it would be important to take both source flaws and detector flaws into account by combining mdiQKD with the Scarani-Acin-Ribordy-Gisin scheme [80]. Also, it can be implemented with different types of sources [81], [82].

In summary, mdiQKD enables new scientific developments in the field of quantum optics, as well as advanced novel applications for quantum information and quantum communication. In a popular book “The Code Book” [88] by Simon Singh, the author suggested that QKD will be the end point of evolution of cryptography. In this paper, we have shown that while quantum hacking has threatened the security of QKD, mdiQKD has now appeared to be an important counter measure against it, thus constituting a major step towards the Holy Grail of cryptography—unconditional security in communication.

ACKNOWLEDGMENTS

The authors thank L. Qian, K. Tamaki for helpful discussions. We thank Z. Tang and L. Yang for allowing us to use the figures of polarisation-encoding and time-bin mdiQKD setup. Support from NSERC, the CRC program, Connaught Innovation fund and Industry Canada, the European Regional Development Fund (ERDF), the Spanish National Research and Development Program under project Terasense CSD2008-00068 (Consolider-Ingenio 2010), and the Galician Regional Government (projects CN2012/279, CN 2012/260, consolida tion of Research Units: AtlantTIC, and the program "ayudas para proyectos de investigacin desarrollados por investigadores emergentes") is gratefully acknowledged. F. Xu thanks the Shahid U.H. Qureshi Memorial Scholarship and the OGS VISA award for financial support.

REFERENCES

[1] G. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications,” Transactions of the American Institute of Electrical Engineers, vol. 45, pp. 295–301, 1926.
[2] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179.
[3] R. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key communications,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[4] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM J. Sci. Statist. Comput.*, vol. 26, p. 1484, 1997.

[5] D. Mayers, “Unconditional security in quantum cryptography,” *Journal of ACM*, vol. 48, no. 3, pp. 351–406, 2001.

[6] H.-K. Lo and H. F. Chau, “Unconditional security of quantum key distribution over arbitrarily long distances,” *Science*, vol. 283, no. 5410, pp. 2050–2056, 1999.

[7] P. W. Shor and J. Preskill, “Simple proof of security of the bb84 quantum key distribution protocol,” *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, 2000.

[8] A. Curty, L. Lydersen, and J. Skaar, “Security of quantum key distribution with arbitrary individual imperfections,” *Phys. Rev. A*, vol. 82, p. 032337, 2010.

[9] T. Ferreira da Silva, G. B. Xavier, G. P. Temporão, and J. P. von der Weid, “Real-time monitoring of single-photon detectors against eavesdropping in quantum key distribution systems,” *Optics express*, vol. 20, no. 17, pp. 19311–19324, 2012.

[10] Z. Yuan, J. Dynes, and A. Shields, “Resilience of gated avalanche photodiodes against bright illumination attacks in quantum cryptography,” *Applied physics letters*, vol. 98, no. 23, pp. 23104–23104, 2011.

[11] D. Mayers and A. C.-C. Yao, “Quantum cryptography with imperfect apparatus,” in *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*. IEEE Computer Society Press, 1998, pp. 503–509.

[12] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, “Device-independent security of quantum cryptography against collective attacks,” *Physical Review Letters*, vol. 98, no. 23, p. 230501, 2007.

[13] S. L. Braunstein and S. Pirandola, “Side-channel-free quantum key distribution,” *Physical Review Letters*, vol. 108, no. 13, p. 130502, 2012.

[14] B. W. Reichardt, F. Unger, and U. Vazirani, “Classical command of quantum systems,” *Nature*, vol. 496, pp. 456–460, 2013.

[15] N. Gisin, S. Pironio, and N. Sangouard, “Proposal for implementing device-independent quantum key distribution based on a heralded qubit amplifier,” *Phys. Rev. Lett.*, vol. 105, p. 070501, 2010.

[16] M. Curty and T. Moroder, “Heralded-qubit amplifiers for practical device-independent quantum key distribution,” *Phys. Rev. A*, vol. 84, p. 010304(R), 2011.

[17] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” *Physical Review Letters*, vol. 108, no. 13, p. 130503, 2012.

[18] E. Bihm, B. Huttner, and T. Mor, “Quantum cryptographic network based on quantum memories,” *Physical Review A*, vol. 54, no. 4, p. 2651, 1996.

[19] H. Inamori, “Security of practical time-reversed epr quantum key distribution1,” *Algorithmica*, vol. 34, pp. 340–365, 2002.

[20] W. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” *Physical Review Letters*, vol. 91, p. 57901, 2003.

[21] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” *Physical Review Letters*, vol. 94, p. 230504, 2005.

[22] H. Inamori, “Security of practical time-reversed epr quantum key distribution2,” *Physical Review Letters*, vol. 94, p. 230504, 2005.

[23] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, “One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering,” *Physical Review A*, vol. 85, no. 1, p. 010301, 2012.

[24] Z.-Q. Yin, C.-H. F. Fung, X. Ma, C.-M. Zhang, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, “Measurement-device-independent quantum key distribution with uncharacterized qubit sources,” *Physical Review A*, vol. 88, no. 6, p. 062322, 2013.

[25] Z.-Q. Yin, C.-H. F. Fung, X. Ma, C.-M. Zhang et al., “Mismatched-basis statistics enable quantum key distribution with uncharacterized qubit sources,” arXiv preprint arXiv:1407.1924, 2014.

[26] H. Inamori, H.-F. Chau, S. P. Walborn, V. Scarani, and C. Kurtsiefer, “Efficient quantum key distribution scheme and a proof of its unconditional security,” *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[27] A. Acín, J. A. Slater, P. Chan, I. Lucio-Martínez, and W. Tittel, “Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks,” *Phys. Rev. Lett.*, vol. 111, p. 130501, 2013.

[28] T. Fereira da Silva, D. Vittoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, “Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits,” *Phys. Rev. A*, vol. 85, p. 052303, 2013.

[29] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li et al., “Experimental measurement-device-independent quantum key distribution,” *Phys. Rev. Lett.*, vol. 111, p. 130502, 2013.

[30] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, “Experimental demonstration of polarization encoding measurement-device-
X. Ma, C.-H. F. Fung, and M. Razavi, “Statistical fluctuation analysis for measurement-device-independent quantum key distribution,” Nature communications, vol. 5, p. 3732, 2014.

X. Ma, C.-H. F. Fung, and M. Razavi, “Statistical fluctuation analysis for measurement-device-independent quantum key distribution,” Physical Review A, vol. 86, no. 5, p. 052305, 2012.

X.-B. Wang, “Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors,” Physical Review A, vol. 87, no. 1, p. 012320, 2013.

S.-H. Sun, M. Gao, C.-Y. Li, and L.-M. Liang, “Practical decoy-state measurement-device-independent quantum key distribution,” Physical Review A, vol. 87, no. 5, p. 052329, 2013.

F. Xu, M. Curty, B. Qi, and H.-K. Lo, “Practical aspects of measurement-device-independent quantum key distribution,” New Journal of Physics, vol. 15, no. 11, p. 113007, 2013.

F. Xu, H. Xu, and H.-K. Lo, “Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution,” Physical Review Letters, vol. 100, no. 20, p. 200501, 2008.

V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Reviews of Modern Physics, vol. 81, no. 3, p. 1301, 2009.

M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, “Tight finite-key analysis for quantum cryptography,” Nature communications, vol. 3, p. 634, 2012.

M. Hayashi and R. Nakayama, “Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths,” New Journal of Physics, vol. 16, no. 6, p. 063009, 2014.

C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, “Concise security bounds for practical decoy-state quantum key distribution,” Physical Review A, vol. 89, no. 2, p. 022307, 2014.

T.-T. Song, Q.-Y. Wen, F.-Z. Guo, and X.-Q. Tan, “Finite-key analysis for measurement-device-independent quantum key distribution,” Physical Review A, vol. 86, p. 022332, 2012.

M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, “The universal composite security of quantum key distribution,” in Theory of Cryptography. Springer, 2005, pp. 386–406.

R. Renner and R. König, “Universally composable privacy amplification against quantum adversaries,” in Theory of Cryptography. Springer, 2005, pp. 407–425.

K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, “Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw,” Physical Review A, vol. 85, no. 4, p. 042307, 2012.

X. Ma and M. Razavi, “Alternative schemes for measurement-device-independent quantum key distribution,” Physical Review A, vol. 86, no. 6, p. 062319, 2012.

P. Chan, J. Slater, I. Lucio-Martinez, A. Rubenok, and W. Tittel, “Modeling a measurement-device-independent quantum key distribution system,” Optics Express, vol. 22, no. 11, pp. 12716–12736, 2014.

D. Stucki, N. Walenta, F. Vannel, R. Thew, N. Gisin, H. Zbinden, S. F. M. C. Towery, and S. Ten, “High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres,” New Journal of Physics, vol. 11, p. 075003, 2009.

F. Marsili, V. Verma, J. Stern, S. Harrington, A. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. Shaw, R. Mirin et al., “Detecting single infrared photons with 95% system efficiency,” Nature Photonics, vol. 7, no. 2, pp. 120–123, 2013.

S. Abruzzo, H. Kampermann, and D. Brüll, “Measurement-device-independent quantum key distribution with quantum memories,” Physical Review A, vol. 89, no. 1, p. 012301, 2014.
Marcos Curty received his M.Sc. and Ph.D in Telecommunication Engineering from Vigo University in 1999 and 2004 respectively. In 2001 he joined the Quantum Information Theory Group at the University of Erlangen-Nürnberg and he obtained a Ph.D in Physics (2006) under the supervision of Prof. Norbert Lütkenhaus. After postdoc positions at Toronto University and at the Institute for Quantum Computing, Waterloo University, he joined the Department of Electronic and Communications Engineering at Zaragoza University as Assistant Professor. Currently he is an Associate Professor in the Theory of Signal and Communications Department at Vigo University. His research interest lies in quantum information processing, particularly quantum cryptography.

Bing Qi is a Research Scientist at Oak Ridge National Laboratory (ORNL). He received a Ph.D. in Optics in 1996 from Dalian University of Technology and joined the ORNL staff in 2013. Before joining ORNL, he was a Senior Research Associate in the Quantum Communication group and in the Emerging Fiber-Optic Technologies group, Dept. of Electrical and Computer Engineering, University of Toronto. Dr. Qi’s research interests include quantum communication and optical sensing.

Hoi-Kwong Lo is a Full Professor at the Center for Quantum Information and Quantum Control (CQIQC), the Department of Physics and the Department of Electrical and Computer Engineering, at the University of Toronto. His research interest lies in quantum information processing, particularly quantum cryptography. He received his B.A. in Mathematics from Trinity College, Cambridge University in 1989 and his M.Sc. and Ph.D. in Physics from Caltech in 1991 and 1994 respectively. Prof. Lo had six years of industrial research experience at Hewlett-Packard Lab., Bristol UK and also as the Chief Scientist and Senior Vice President, R&D, of MagiQ Technologies, Inc., New York. He was a co-founder of a leading journal Quantum Information and Computation (QIC).