ADVANCED QUANTUM TECHNOLOGIES
www.advquantumtech.com

Implementation Security in Quantum Key Distribution

Víctor Zapatero, Álvaro Navarrete,* and Marcos Curty*

The problem of implementation security in quantum key distribution (QKD) refers to the difficulty of meeting the requirements of mathematical security proofs in real-life QKD systems. Here, a succint review is provided on this topic, focusing on discrete-variable QKD setups. Particularly, we discuss some of their main vulnerabilities and comment on possible approaches to overcome them.

1. Introduction

Almost forty years after its conception,[1] quantum key distribution (QKD) has become a mature technology excelling among quantum information applications, with dedicated companies providing QKD services,[2–6] metropolitan QKD networks being deployed around the globe,[7–12] record secret key rates and transmission distances being achieved over optical fibers,[13–18] and a space-ground integrated QKD backbone being extended over thousands of kilometers[19] in China.

The crucial cryptographic advantage of QKD is that it allows for information-theoretically secure key exchange through an insecure channel,[20] which provides a unique solution for long-term communication security. More specifically, while the security of standard public-key cryptosystems presumes computational limitations on a potential adversary, mathematical QKD security proofs rely on fundamental properties of quantum mechanics—such as the unclonability[21] of quantum states or quantum entanglement[22]—together with models of the behavior of the physical devices involved in a QKD protocol.[23,24] To put it another way, QKD security stems from unique physical-layer properties, which is a double-edged sword: on the one-hand, it eliminates the need for computational assumptions that become increasingly weaker over time, but on the other hand, it is significantly dependent on the proper characterization of the quantum communication hardware. The latter observation gives rise to a variety of concerns regarding the security of QKD implementations, and in this review we unravel some of the intricacies of this topic. To be more specific, we recall that two different variants exist for the deployment QKD: discrete-variable QKD—which encodes the key information discretely in, say, the polarization or the phase of individual photons, and typically uses single-photon detection—and continuous-variable QKD—which encodes the key information in the quadratures of the electromagnetic field and typically uses coherent detection—. In this context, the present work is dedicated to the former approach.

As is customary in the literature on QKD, in what follows we often refer to the honest parties trying to establish a secret key as Alice and Bob, and to the eavesdropper in the quantum channel as Eve.

2. Implementation Security

To state it shortly, if the assumptions invoked by the security proof of a QKD protocol are not met exactly in a real implementation, the security of the implementation does not follow. In particular, QKD security proofs typically rely on mathematical models of the QKD equipment, which opens the door for mischaracterization loopholes. This is problematic given the complexity of QKD hardware and our engineering limitations, which prevent us from fully controlling the operation of the devices. On top of it, faithfully describing the functioning of a QKD transmitter or receiver with which an adversary can arbitrarily interact is a major challenge, as illustrated by the rich literature on quantum hacking.[24–26]. This includes a variety of quantum hacking attacks successfully implemented,[27–31] a rapidly growing list given the non-stop emergence of new adversarial strategies.[32–39] For these reasons, rigorously quantifying the level of security of QKD implementations is a difficult task, an issue we refer to as the implementation security of QKD. In fact, the problem of implementation security is also a threat for conventional cryptosystems, but it is probably more severe for QKD, being this an eminently hardware solution.

Fortunately, outstanding theoretical and experimental efforts are being made to address this problem. For at least two decades, theorists have been devising new QKD protocols and security proofs are more and more robust to experimental imperfections, and experimentalists have developed special-purpose hardware for optical quantum communications, getting closer and closer to the specifications of the theoretical security proofs.

In a deeper level, the security proofs follow the so-called real-world versus ideal-world paradigm,[20] in which the security of a protocol is quantified by measuring its distinguishability from

V. Zapatero, Á. Navarrete, M. Curty
AtlanTTic, Departamento de Teoría do Sinal e Comunicacións
University of Vigo
Vigo E-36310, Spain
E-mail: vzapatero@vqcc.uvigo.es; anavarrete@vqcc.uvigo.es

The ORCID identification number(s) for the author(s) of this article can be found under https://doi.org/10.1002/qute.202300380

DOI: 10.1002/qute.202300380

an ideal execution of the cryptographic task under consideration. Particularly, the ideal functionality of QKD is defined by the following two requirements on the output key: it must be uniformly distributed and uncorrelated from the knowledge of Eve (secrecy requirement), and Alice and Bob must hold identical copies of it (correctness requirement). In order to evaluate the distinguishability of a QKD protocol from this ideal functionality, very diverse assumptions are typically presumed. From the implementation point of view, an inevitable premise seems to be the proper isolation of the parties' QKD labs. Indeed, since the exchange of quantum signals requires that the labs be connected to the outside world through a quantum channel, this assumption already gives rise to implementation issues, with information being potentially leaked in different ways, both active and passive. Furthermore, information leakage (IL) can also occur through classical channels, via e.g., electromagnetic radiation, power consumption, or covert channels in sabotaged QKD hardware inter alia.

Generally speaking, passive information leakage in the quantum channel arises due to the mis-modeling of either the quantum states prepared in the QKD transmitter or of the quantum measurements performed in the QKD receiver. A paradigmatic example is given by the so-called photon-number splitting attack against the ideal BB84 protocol, originally suggested in ref. [40] and extensively discussed in e.g. ref. [41]. Essentially, the attack is based on photon counting and may reveal Eve the bit values redundantly encoded in multi-photon pulses without introducing errors. This is so because multi-photon pulses provide Eve with perfect copies of the state of the single-photon pulses, thus bypassing the limitations imposed by the no-cloning theorem.[21] Security-wise, the problem is not the presence of multi-photons in the states emitted by the laser, but rather the assumption that individual photons are being prepared. Indeed, a more realistic approach accounting for the presence of multi-photons consists of modeling the laser pulses as phase-randomized weak coherent states[42] when the laser is driven under gain-switching conditions. Within this model, the threat of photon-number splitting attacks can be overcome by using the decoy-state method,[43–45] which consists on randomly alternating among various intensities in the QKD transmission. Irrespectively of Eve's attack, the detection statistics of the different intensities allow to tightly estimate the detection statistics of the single-photon pulses, from which the provably secure key length can be calculated.

In the following, we address several other implementation security breaches, separately discussing receiver vulnerabilities and transmitter vulnerabilities in different sections. Coming next, we shortly present the device-independent (DI) approach to QKD and the threat of malicious/sabotaged devices, to finally end up the review with some prospects and concluding remarks.

3. Receiver Vulnerabilities

The receiver is widely regarded as the most vulnerable element of a QKD scheme. This is mainly attributable to its need to be open to interactions for signal measurement purposes, thereby providing Eve opportunity to readily interact with it and manipulate its operation. Moreover, inevitable imperfections offer an exploitable scenario for Eve to enhance her malicious interventions.

For instance, most security analyses assume that all detectors at the receiver have the same detection efficiency. This facilitates the merging of detection inefficiency and channel transmission loss under adversary control, allowing the use of conventional security-proof techniques in a simpler model with higher effective channel loss and ideal single-photon detectors (SPDs). In general, however, the detector's response to a photon often depends on various degrees of freedom—e.g., frequency, space,[46–48] arrival time, or polarization[49]—which may not intentionally play a role in the encoding. This allows Eve to perform, e.g., a fake-state attack,[50,51] a particular type of intercept-and-resend attack in which Eve randomly measures Alice's signals in one of the BB84 bases—if we consider this particular protocol—and then resends the state corresponding to the inverse of her bit guess in the opposite basis at a time when Bob's detector associated with that inverse bit has a significantly lower efficiency than the other detector. If Eve's and Bob's measurement bases are not in agreement, the signal resent by Eve will only collide with the low-efficiency detector and rarely trigger it. If their bases match, the signal will be distributed between the two detectors, but the one associated with the opposite of Eve's bit guess will be activated with lower probability. Eve could also perform a time-shift attack[27,52] by simply shifting the arrival time at Bob's side of each signal sent by Alice to a time instance where the sensitivity of one detector far exceeds that of the other. In the most extreme scenarios—where one detector is completely insensitive while the other remains receptive—either of these attacks would allow Eve to learn the entire secret key without being detected.

SPDs might also suffer from backflash radiation, whereby photons are emitted upon a detection event due to the recombination of electrons with holes within the avalanche breakdown region.[53–56] While the backflash photons carry no information about the detected states, they have the potential to reveal information about the internal state of the receiver's components that they encounter while traveling to the channel, which may lead to IL about the final key. Indeed, IL about the receiver's internal configuration can even be actively induced by Eve via a Trojan-horse attack[57–59] (THA). In a THA, Eve injects bright light into the receiver—usually opting for a wavelength that avoids detector triggering at Bob—which then undergoes reflections within the internal components of Bob's receiver, thereby conveying sensitive information to the channel.

The THA is an example of an attack in which Eve not only exploits existing imperfections to enhance her eavesdropping capabilities, but she interacts with Bob's devices to create new vulnerabilities. The best known instance of this kind is the so-called blinding attack,[28,29,36,37,60–64] in which Eve injects strong light into the receiver's single-photon avalanche diodes (SPADs) to make them operate in linear mode rather than Geiger mode. As a result, the detectors no longer function as SPDs but as conventional photodiodes. This can be later used to manipulate the detectors' clicking behavior by sending them classical light of properly chosen intensity.

Indeed, the blinding attack can be regarded as an instance of a broader class of intercept-and-resend attacks called detector-control attacks, where Eve does not try to replicate Alice's original states, but instead resends light pulses—classical or quantum—that manipulate Bob's detections such that they can only produce a click when the signals resent by Eve match those of Alice. Another example is the after-gate attack,[65] which targets gated SPADs. Here, Eve forces Bob's detectors to operate in

linear mode by sending him strong signals just after the gating process, when the detectors are no longer in Geiger mode. In general, a detector-control attack is feasible if the detector exhibits a higher detection probability for multiple, nearly simultaneous photons—compared to separate, temporally distinct photons—a phenomenon termed superlinear behavior.[66,67]

The dead time of the SPDs may also open up potential vulnerabilities. Typically, the receiver only acknowledges detections that occur within a certain time window to minimize dark counts. This allows Eve to send light pulses to Bob before Alice's transmitted pulses reach the receiver, with the aim of triggering certain detectors at Bob's side[30] before the window is open. Since these detectors need time to reset, they cannot be triggered again in the same transmission round by Alice's original signals. Therefore, Eve can be confident that any subsequent detection announcement in that round must be attributed to the remaining operative detector(s).

Lastly, it has been demonstrated[68,69] that Eve could even use laser illumination to irreversibly modify some characteristics of the detectors—such as their detection efficiency and dark count rate—thereby creating permanent exploitable vulnerabilities in the receiver.

The previous examples represent common vulnerabilities in QKD receivers that require comprehensive risk mitigation strategies. Hardware-wise, a rigorous device calibration of the receiver's components is essential. For this, routine calibration intervals—monitoring parameters such as current, voltage, temperature, and detection efficiency—of Bob's detectors might help to ensure their correct functioning throughout the QKD session. To defend against invasive attacks from Eve—such as blinding attacks or THAs—optical isolators, circulators, and narrow spectral filters are often used to restrict any incoming light to the appropriate wavelength in Bob's receiver. In addition, optical fuses and power limiters can be used to limit the intensity of the incoming light from the channel. Moreover, the use of watchdog detectors with different response times also enables continuous monitoring of potential light-injection attempts by Eve.

An additional countermeasure against active IL is the implementation of passive receivers.[16,70] This type of receiver passively distributes the incoming signals across the measurement bases, preventing the leakage of basis information to Eve via a THA.

With respect to the detector efficiency mismatch, a practical hardware solution is to use a four-state QKD receiver[71,72] equipped with a single detector. In such a scheme, Bob randomly chooses not only the measurement basis, but also the bit to be measured. Indeed, this four-state idea can also be extended to two-detector receivers,[52] being in this case similar to randomly switching between the two detectors in every round. This guarantees that the detection efficiency associated to each bit value is the same.

From a theoretical point of view, considerable effort has been devoted to characterize the vulnerabilities of the devices and to incorporate these imperfections into the security proofs, a prime example being the GLLP framework.[73] Specifically, a preliminary security analysis against backflash radiation has been discussed e.g. in Ref. [54]. Also, as demonstrated in Ref. [74–78], a well-characterized, stable detection-efficiency mismatch can be incorporated into the security proof, albeit under the premise that

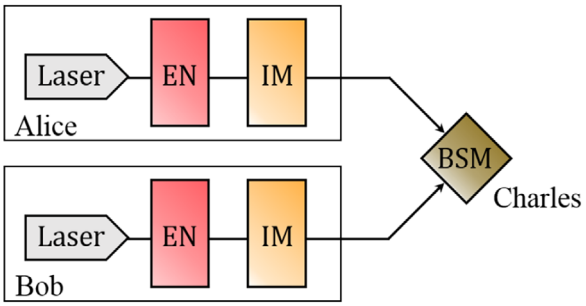

Figure 1. Illustration of an MDI-QKD setup. Alice and Bob send decoy-state BB84 pulses to an untrusted intermediate party, who performs a Bell-state measurement (BSM). EN: bit/basis encoder; IM: intensity modulator; BSM: Bell-state measurement.

Eve cannot add photons to the transmitted signals. Remarkably, recent numerical[79] and analytical[80] security analyses have effectively removed this assumption.

Withal, there exists an ultimate solution that rules out all security loopholes concerning the receiver units, namely, interference-based QKD, such as measurement-device-independent[81] (MDI) or twin-field[82] (TF) QKD.

3.1. Interference-Based QKD

In MDI-QKD both Alice and Bob play the role of transmitters, sending BB84 states to an intermediate party—say, Charles—who jointly measures the incoming signals and publicly announces the measurement results (see **Figure 1**). The key feature of MDI-QKD is that its security does not rely on the integrity of Charles, who may even be Eve. Essentially, this is because MDI-QKD can be seen as a time-reversed Einstein-Podolsky-Rosen (EPR)-based QKD protocol.[83,84]

In an EPR-based protocol, Alice and Bob each prepares an EPR pair and send one half to Charles, who performs a Bell-state measurement. Subsequently, Charles publicly announces the measurement results, and Alice and Bob randomly perform Z and X measurements—defined by the qubit states $\{|0\rangle, |1\rangle\}$ and $\{(|0\rangle + |1\rangle)/\sqrt{2}, (|0\rangle - |1\rangle)/\sqrt{2}\}$, respectively—on their respective halves. Note that Charles' measurement and announcement serve as a mechanism for entanglement swapping, resulting in Alice's and Bob's local systems being left in an entangled state. By analyzing the measurement statistics, Alice and Bob can detect any dishonest behavior from Charles. Notably, this feature remains unchanged if Alice and Bob proceed with their local measurements before sending their respective EPR halves to Charles—effectively preparing these qubits in BB84 states—which is the basis of MDI-QKD.

In practice, Charles' measurement setup can be implemented with basic linear optical elements—such as beamsplitters and polarizing beamsplitters—and threshold detectors, while the transmitters' are identical to those used in standard decoy-state QKD implementations. Due to its immunity to detector side channels, together with its practicality and good performance, MDI-QKD has given rise to numerous theoretical studies. These include refined parameter estimation methods,[85] finite-key security analyses[86,87] and alternative schemes using different

encoding approaches.[88,89] In fact, several experimental implementations have been reported in the last decade.[14,90–96]

A noteworthy variant of interference-based QKD is twin-field (TF) QKD.[82] It is well known that point-to-point QKD configurations have inherent limitations, causing the secret key rate to scale at best linearly with the transmittance of the quantum channel between the two parties. Unfortunately, despite its intermediate-node configuration, MDI-QKD is unable to overcome this limit due to the requirement of two-photon interference at the central node. In order to surpass this limitation, various theoretical solutions have been proposed, including for instance quantum repeaters[97–99] or MDI-QKD protocols incorporating quantum memories[100] or quantum nondemolition measurements.[101] However, these solutions are impractical with existing technology.

In this light, TF-QKD emerges as a practical solution that overcomes linear scaling through a setup that is implementable with current technology. Sharing its mid-node structure and immunity to detector side channels with MDI-QKD, the key rate of TF-QKD scales with the square root of the channel transmittance, thus essentially doubling the maximum achievable distance when compared to MDI-QKD. This feature can be attributed to the entanglement swapping operation at the central node, which is based on single-photon interference. In other words, the arrival of a single photon at the central node (be it from Alice or from Bob) is enough to distill a key. This advantage, nonetheless, comes at the cost of requiring strict phase stability.

In the last years, numerous TF-QKD variants have refined the original idea to enhance its practicality and performance,[102–105] many of them having already witnessed experimental implementations.[14,17,18,106–116] Interestingly, recent solutions have mitigated the need for phase stability,[117–120] thus greatly simplifying their practical deployment. Overall, this class of QKD protocols is becoming the standard for long-distance fiber communication. Indeed, this assertion is supported by the current record transmission distance over fiber,[14] which potentially delivers a positive asymptotic key rate for a link of 1002 km.

4. Transmitter Vulnerabilities

Real-world transmitters also suffer from inevitable imperfections that are frequently ignored in security proofs. Among them, the most obvious may be encoding errors or state preparation flaws (SPFs). These refer to subtle deviations between the actually transmitted states and the idealized states considered in the theoretical models, and may arise due to the faulty construction of the encoding devices or finite precision limitations. In certain protocols, such as the BB84 scheme, SPFs often enable Eve to partially discern between the two bases. While the GLLP analysis[73] addresses SPFs, its performance deteriorates significantly at relatively short distances even for minor imperfections. Alternatively, the so-called loss-tolerant (LT) protocol[95,121–124] resolves this problem by rendering the protocol almost insensitive to SPFs. For this, SPFs must be well characterized, and they must not take the transmitted single-photons out of their original qubit space.

Another instance of faulty state preparation can be found in decoy-state QKD protocols. The effective implementation of the decoy-state method requires precise knowledge and temporal stability of the intensities of Alice's transmitted pulses. However, practical transmitters often encounter minor intensity fluctuations that must be incorporated into the security analysis.[122] In addition, it is crucial for the method's integrity that the optical phase of each coherent pulse appears uniformly random to any potential eavesdropper. A conventional approach for achieving this involves gain-switching the laser source.[16,125–130] In doing so, each pulse is triggered by a spontaneous emission event, leading to an optical phase that is essentially random. Unfortunately, inherent imperfections in the devices can hinder the achievement of a perfectly uniform phase distribution.[131,132] To solve this, recent techniques[133,134] permit to accommodate this kind of phase imperfections into the security proofs. Another frequently adopted solution involves utilizing an external phase modulator.[135–138] However, this requires a fresh supply of random numbers to feed the modulator. Worse still, only a discrete set of optical phases can be selected, thereby violating the fundamental assumption of the decoy-state method. To address this challenge, more sophisticated decoy-state analyses[139,140] have been proposed to restore the security even when utilizing a finite number of phases. Furthermore, these ideas have been extended to encompass the general scenario where the phase of each pulse follows an arbitrary—continuous or discrete—probability density function.[141]

As with receivers, imperfections in the transmitters can also be actively induced by eavesdropping attacks. For example, in a laser seeding attack, Eve deliberately manipulates the intensity[142] and/or the phase[143] of Alice's transmitted signals by introducing light into her laser source, thereby triggering stimulated emission. Recent studies also demonstrated the effectiveness of laser-injection attacks in manipulating lithium niobate-based optical modulators.[34,35] Moreover, Eve could inject light to irreversibly damage the transmitter,[144] permanently increasing the intensity of Alice's emitted signals.

Also crucial for the transmitter's integrity is to prevent any kind of IL. Passive generation of IL may be produced e.g., via mode dependencies in Alice's transmitter.[39,145–149] This occurs when Alice's settings become encoded in other degrees of freedom associated with the emitted light—such as frequency, space and time—or through unintended emissions of a different nature—such as unwanted electromagnetic radiation, power consumption, or even apparatus-generated noise—resulting in the transmission of higher-dimensional quantum states. From this perspective, IL can be regarded as a specific manifestation of imperfect state preparation, in which the dimensionality of the transmitted states increases, thereby creating a side channel that enhances the distinguishability of the signals and thus the effectiveness of Eve's attacks. For example, Alice's signals might become linearly independent, in so allowing Eve to perform an unambiguous state discrimination attack. Needless to say, this would severely restrict the performance of the protocol. Moreover, Eve could actively provoke a similar effect e.g., by launching a THA[150,151] against the transmitter (see **Figure 2**), or by establishing a dependency between the encoding of Alice's signals and their frequency.[32,38] In fact, this could be executed in tandem with any of the aforementioned laser injection attacks.

IL may also manifest through pulse correlations. To enhance the secret key rate, modern QKD systems aim to increase the

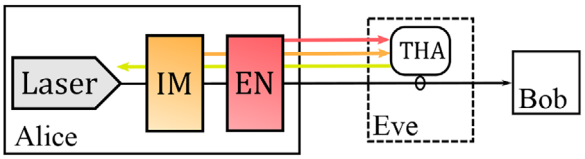

Figure 2. Schematic diagram of a THA. Eve injects a photonic state into Alice's transmitter and analyses the back-reflected light, which can provide information about the internal configuration of Alice's bit/basis encoder (EN) and intensity modulator (IM).

repetition rate of the sources, achieving up to gigahertz repetition rates in current experimental implementations.[16,130,152,153] However, operating at high speed typically introduces memory effects in the modulators and electronics that control them,[154–158] resulting in correlations between optical pulses. This means that the state of a quantum signal emitted by the source at a given instant may depend not only on the settings chosen by Alice at that round, but also on previous setting choices. As a result, the settings used to encode each quantum signal can be partially inferred from the quantum states of subsequent signals, acting as a side channel.

Securing the source against IL is challenging. Nonetheless, significant effort has been devoted by theorists in developing security analyses that encompass their various manifestations. For example, recent security analyses[159–161] have successfully accommodated multiple source imperfections—as mode dependencies (which may arise passively or be actively induced via a THA), SPFs, and pulse correlations—using the novel reference technique (RT) framework.[162] Essentially, the method considers some reference states that closely resemble the actual states transmitted in the protocol, but whose simpler structure facilitates the estimation of Eve's side information. Then, by exploiting the similarity between these two sets of states—e.g., via a Cauchy-Schwarz type inequality[162]—one can estimate Eve's side information from the detection statistics of the actual transmitted states.

The high flexibility and tolerance to source imperfections of the RT comes with certain trade-offs. Specifically, it imposes a sequential execution of the protocol where Alice emits a pulse only after Bob has measured the preceding one. It is worth mentioning though that simple relativistic arguments can be invoked to slightly relax this constraint,[161,163] and parallel executions of the protocol can mitigate its effects. Fortunately, a recent solution proposed in Ref. [163] has effectively overcome this constraint by reintroducing the quantum coin idea[73,164] and integrating it with the rejected data analysis of the LT protocol[121] alongside random sampling techniques.[124] By doing so, the method in Ref. [163] effectively considers the inherent distinction between qubit SPFs and side channels—unlike the original GLLP analysis—resulting in enhanced robustness to channel loss (see **Figure 3**). Withal, a major assumption underlying all of the techniques discussed in this section is that a fidelity-type bound between the real leaky systems and their idealized counterparts is satisfied, its precise experimental verification still being an open problem.

As mentioned above, pulse correlations can be regarded as a particular manifestation of IL and, therefore, some of the aforementioned techniques already allow to accommodate them into the security analysis. Setting-choice-independent correlations—

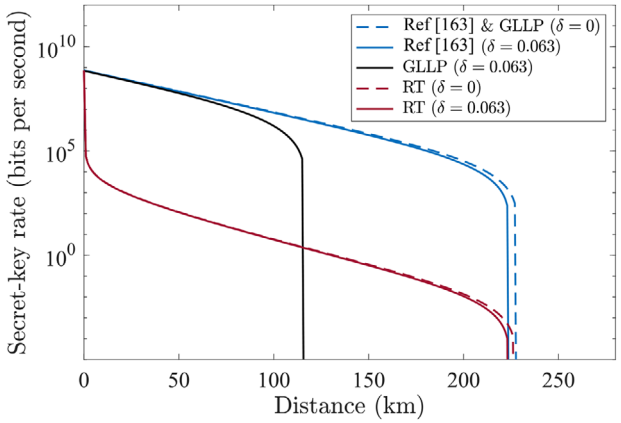

Figure 3. Rate-distance performance of the BB84 protocol with the recent security proof in Ref. [163], compared with that of the original quantum coin (GLLP)[73] and reference technique (RT)[162] analyses. The figure considers a lower bound on the fidelity between the actual leaky states and the reference states (without side channel) of $\epsilon = 10^{-6}$. The parameter δ represents the magnitude of the qubit flaws, and an attenuation coefficient $\alpha = 0.2$ dBkm^{-1} is assumed. The figure has been adapted with permission from Ref. [163].

that is, pulse correlations unaffected by the setting choices made during state preparation—have been extensively explored in the literature.[165,166] Likewise, recent works have addressed correlations in the bit/basis encoding for the more comprehensive setting-choice-dependent scenario,[161,162] as well as intensity correlations in decoy-state QKD protocols.[157,167,168] Moreover, correlations between the optical phases of coherent pulses emitted by a gain-switched laser have been addressed[134] recently.

Security proofs that contemplate THAs against the transmitter include.[159–161,169–174] Naturally, the transmitter may be experimentally safeguarded from THAs by installing optical isolators, narrow spectral filters, optical fuses, and power limiters at its output.[172,175–177] Moreover, monitor detectors could be employed to measure the intensity of the incident light. However, these hardware solutions are limited—achieving a perfect level of isolation is impossible—and might be also subject to Eve's intervention.[33,144,177] Hence, it is necessary to combine the above techniques (capable of upper-bounding the maximum intensity of Eve's back-reflected light) with appropriate security proofs that accommodate IL.

Importantly as well, since, as stated above, memory effects in the modulators pose an IL threat, a modulator-free approach to QKD has also been extensively explored, known as passive QKD (see **Figure 4**). In this regard, the works in Ref. [178, 179] proposed a QKD transmitter passively implementing both the encoding of BB84 states and the preparation of decoy intensities using linear optical elements and coherent light, combining earlier ideas presented in Ref. [180, 181]. In fact, these papers were soon followed by proof-of-principle experimental demonstrations[182,183] and novel proposals for fully passive TF-QKD[184] and MDI-QKD.[185] It is nevertheless worth mentioning that, although the passive approach may remove all modulation side-channels, passive QKD transmission relies on the post-selection of the desired protocol states through one or more (typically classical) measurements, possibly opening other

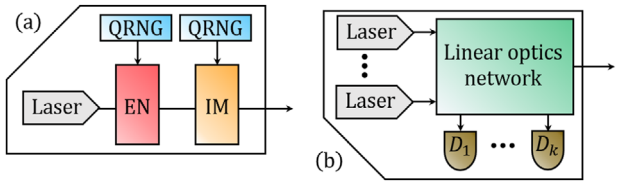

Figure 4. Comparison of (a) active and (b) passive decoy-state QKD transmission. In the active setup, an encoding device (EN) and an intensity modulator (IM) are externally driven by quantum random number generators (QRNGs) to implement the protocol settings. In the passive setup, one or more laser sources generate pulses that interfere in a linear optics network. Based on the detection outcomes observed in the photodetectors ($\{D_j\}$), different signal states can be post-selected.

security loopholes that have not been studied in detail yet.[179,186] As an example, a passive source might be vulnerable to intrusions similar to laser-seeding[142] or laser-damage[144] attacks, but with light injections potentially targeted at both the laser source and the measurement unit required for post-selection.

5. DI-QKD

As already discussed, interference-based QKD allows to establish the security of QKD as long as the functioning of the QKD transmitter is characterized, eliminating all security loopholes from the measurement unit. Note, however, that exhaustively characterizing a QKD transmitter is a difficult task (see e.g., Ref. [159, 162] for recent analyses). What is more, the source models are often dependent on the details of the implementation.

Some of these problems can be avoided in the fully DI approach to QKD[187–191], a variant of entanglement-based QKD where the honest parties hold QKD receivers and an external untrusted source distributes entangled states between them (see **Figure 5**). Crucially, the DI approach completely removes the need for modeling the quantum states prepared and the measurements performed. It requires however that the QKD receivers do not reveal any information about the measurement outcomes to the outside world, which could in fact be hard to guarantee in practice given the difficulty of characterizing IL. Nevertheless, an attempt to do so has been presented in Ref. [192].

Fundamentally, DI security requires that Alice's and Bob's measurement outcomes largely violate a Bell inequality[193], which certifies the presence of monogamous correlations between these outcomes on the sole basis of the input-and-output measurement statistics (see e.g., Ref. [190] for an updated review on the security of DI-QKD protocols). Importantly, the conclusiveness of a Bell test is subject to the closure of a detection loophole and a locality loophole among others (see for instance[194]),

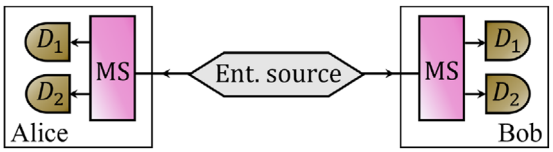

Figure 5. Schematic illustration of a DI-QKD setup. MS: measurement setting; $\{D_j\}$: photo-detectors. With this architecture, one can establish QKD security without internally characterizing either the entanglement source or the measurement units.

setting stringent constraints on the tolerable loss and the timing/synchronization of Alice's and Bob's systems. Notwithstanding, various loophole-free Bell tests have been conducted in the last decade—both photonic[195–197] and non-photonic[198,199]—and the first proof-of-concept DI-QKD experiments have recently been reported using different platforms.[200–202]

Remarkably though, in spite of the security upgrade, the key generation rate and the transmission distances achievable by DI-QKD in the foreseeable future are significantly limited if compared with non-DI QKD solutions.[191,203]

6. Malicious Equipment

While different QKD variants require different levels of physical characterization, a transversal assumption common to all of them is the honesty of the QKD devices and the classical post-processing units, as failure to fulfill this assumption may obviously jeopardize the implementation security of QKD as well. After all, once the quantum communication of a QKD protocol ends, the resulting key data is a purely classical object subject to being copied, and a malicious manufacturer could have plenty of time and opportunities to sabotage the QKD equipment and benefit from this vulnerability. Indeed, private information might be revealed in very convoluted ways by a malicious device (be it a quantum module or a classical processor with access to the key data), and practical solutions to tackle this problem have in fact been studied.[204–206] As an example, the techniques presented in Ref. [205, 206] are based on using redundant devices and secret sharing techniques, and a related experiment has proven their feasibility.[207]

7. Outlook

The information-theoretic security of QKD is entirely rooted in the physical layer: it stems from the quantumness of the information carriers and the measurements performed on them. As a consequence, the long-term security guarantee offered by QKD comes at the price of accurately modeling the QKD equipment, and failure to do so may open practical security loopholes.

Focusing on discrete-variable QKD, in this work we have discussed many of the implementation vulnerabilities that threaten these systems, together with the suggested solutions and countermeasures. In this regard, the progress in bridging the gap between security proofs and experiments has been led by the refinement of both the theory and the practice of QKD, the former being the main focus of this review. Decoy-state QKD, loss-tolerant QKD, interference-based QKD or device-independent QKD are prominent examples pushing the implementation security boundaries, each of them with its own merits and limitations.

At the present time, the implementation security of QKD is one of the main concerns of governments and institutions regarding the standardization of this technology.[208–210] Apparently, the proliferation of quantum hacking attacks has undermined the idealized picture of QKD originally drawn in its early years. Notwithstanding, quantum hacking is actually helping us improve the implementation security of QKD. In fact, the combination of interference-based QKD with sufficiently isolated transmitters seems to provide an already practical solution today. On

top of it, for most hardware vulnerabilities of a QKD system, either they are exploited during the key distribution session or they can never compromise the security of the delivered keys.

One way or the other, the progress in securing QKD implementations is undeniable. The gap between theory and practice has been reduced significantly and multiple applications are popping up for this disruptive technology.

Acknowledgements

This work was supported by the Cisco Systems Inc., the Galician Regional Government (consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through the grant no. PID2020-118178RB-C21, MICIN with funding from the European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the "Planes Complementarios de I+D+I con las Comunidades Autónomas" in Quantum Communication, the European Union's Horizon Europe Framework Programme under the Marie Sklodowska-Curie Grant no. 101072637 (Project QSI) and the project "Quantum Security Networks Partnership" (QSNP, grant agreement no. 101114043). Funding for open access charge: Universidade de Vigo/CISUG.

Conflict of Interest

The authors declare no conflict of interest.

Keywords

implementation security, quantum hacking, quantum key distribution

Received: October 27, 2023
Revised: December 18, 2023
Published online: January 7, 2024

[1] C. H. Bennett, G. Brassard, in,*Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing*, IEEE NY, Bangalore, India**1984**.
[2] https://www.idquantique.com.
[3] https://www.global.toshiba/ww/products-solutions/security-ict/qkd.html.
[4] https://qubridge.io/.
[5] https://www.thinkquantum.com/.
[6] http://www.quantum-info.com/.
[7] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger1, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, et al., *New J. Phys.* **2009**, *11*, 075001.
[8] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, Z.-F. Han, G.-C. Guo, *Chin. Sci. Bull.* **2009**, *54*, 2991.
[9] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, et al., *Opt. Express* **2011**, *19*, 10387.
[10] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voiro, N. Walenta, H. Zbinden, *New J. Phys.* **2011**, *13*, 123001.
[11] J. Dynes, A. Wonfor, W.-S. Tam, A. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. Yuan, A. Dixon, J. Cho, Y. Tanizawa, J. -P. Elbers, H. Greißer, I. H. White, R. V. Penty, A. J. Shields, *npj Quantum Inf.* **2019**, *5*, 101.
[12] Y.-H. Yang, P.-Y. Li, S.-Z. Ma, X.-C. Qian, K.-Y. Zhang, L.-J. Wang, W.-L. Zhang, F. Zhou, S.-B. Tang, J.-Y. Wang, Y. Yu, Q. Zhang, J.-W. Pan, *Opt. Express* **2021**, *29*, 25859.
[13] F. Grünenfelder, A. Boaron, G. V. Resta, M. Perrenoud, D. Rusca, C. Barreiro, R. Houlmann, R. Sax, L. Stasi, S. El-Khoury, E. Hänggi, N. Bosshard, F. Bussiéres, H. Zbinden, *Nat. Photonics* **2023**, *17*, 422.
[14] Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, W.-X. Pan, D. Ma, H. Dong, J.-M. Xiong, C.-J. Zhang, H. Li, R.-C. Wang, J. Wu, T.-Y. Chen, L. You, X.-B. Wang, Q. Zhang, J.-W. Pan, *Phys. Rev. Lett.* **2023**, *130*, 210801.
[15] W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, J. Huang, H. Li, Z. Wang, H.-K. Mao, B. Yan, Q. Li, Y. Liu, Q. Zhang, C.-Z. Peng, L. You, F. Xu, J.-W. Pan, *Nat. Photonics* **2023**, *17*, 416.
[16] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, H. Zbinden, *Phys. Rev. Lett.* **2018**, *121*, 190502.
[17] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, J.-W. Pan, *Nat. Photonics* **2021**, *15*, 570.
[18] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, Z.-F. Han, *Nat. Photonics* **2022**, *16*, 154.
[19] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, et al., *Nature* **2021**, *589*, 214.
[20] C. Portmann, R. Renner, *Rev. Mod. Phys.* **2022**, *94*, 025008.
[21] W. K. Wootters, W. H. Zurek, *Nature* **1982**, *299*, 802.
[22] M. A. Nielsen, I. L. Chuang, Quantum computation and quantum information, Cambridge University Press, **2010**.
[23] M. Curty, K. Azuma, H.-K. Lo, *Phys. Today* **2021**, *74*, 36.
[24] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, J.-W. Pan, *Rev. Mod. Phys.* **2020**, *92*, 025002.
[25] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, G. Leuchs, *Contemp. Phys.* **2016**, *57*, 366.
[26] S. Sun, A. Huang, *Entropy* **2022**, *24*, 260.
[27] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, H.-K. Lo, *Phys. Rev. A* **2008**, *78*, 042333.
[28] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov, *Nat. Photonics* **2010**, *4*, 686.
[29] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, V. Makarov, *Nat. Commun.* **2011**, *2*, 349.
[30] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, H. Weinfurter, *New J. Phys.* **2011**, *13*, 073024.
[31] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, G. Leuchs, *Phys. Rev. Lett.* **2011**, *107*, 110501.
[32] X.-L. Pang, A.-L. Yang, C.-N. Zhang, J.-P. Dou, H. Li, J. Gao, X.-M. Jin, *Phys. Rev. Appl.* **2020**, *13*, 034008.
[33] H. Tan, W.-Y. Zhang, L. Zhang, W. Li, S.-K. Liao, F. Xu, *Quantum Sci. Tech.* **2022**, *7*, 045008.
[34] P. Ye, W. Chen, G.-W. Zhang, F.-Y. Lu, F.-X. Wang, G.-Z. Huang, S. Wang, D.-Y. He, Z.-Q. Yin, G.-C. Guo, Z.-F. Han, *Phys. Rev. Appl.* **2023**, *19*, 054052.

[35] L. Han, Y. Li, H. Tan, W. Zhang, W. Cai, J. Yin, J. Ren, F. Xu, S. Liao, C. Peng, Effect of light injection on the security of practical quantum key distribution, *preprint arXiv:2303.14683* **2023**.
[36] Z. Wu, A. Huang, H. Chen, S.-H. Sun, J. Ding, X. Qiang, X. Fu, P. Xu, J. Wu, *Opt. Express* **2020**, *28*, 25574.
[37] B. Gao, Z. Wu, W. Shi, Y. Liu, D. Wang, C. Yu, A. Huang, J. Wu, Strong pulse illumination hacks self-differencing avalanche photodiode detectors in a high-speed quantum key distribution system, *preprint arXiv:2205.04177* **2022**.
[38] X.-X. Zhang, M.-S. Jiang, Y. Wang, Y.-F. Lu, H.-W. Li, C. Zhou, Y. Zhou, W.-S. Bao, *Phys. Rev. A* **2022**, *106*, 062412.
[39] A. Baliuka, M. Stöcker, M. Auer, P. Freiwang, H. Weinfurter, L. Knips, *Phys. Rev. Appl.* **2023**, *20*, 054040.
[40] B. Huttner, N. Imoto, N. Gisin, T. Mor, *Phys. Rev. A* **1995**, *51*, 1863.
[41] G. Brassard, N. Lütkenhaus, T. Mor, B. C. Sanders, *Phys. Rev. Lett.* **2000**, *85*, 1330.
[42] H. Inamori, N. Lütkenhaus, D. Mayers, *Eur. Phys. J. D* **2007**, *41*, 599.
[43] W.-Y. Hwang, *Phys. Rev. Lett.* **2003**, *91*, 057901.
[44] H.-K. Lo, X. Ma, K. Chen, *Phys. Rev. Lett.* **2005**, *94*, 230504.
[45] X.-B. Wang, *Phys. Rev. Lett.* **2005**, *94*, 230503.
[46] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, V. Makarov, *Phys. Rev. A* **2015**, *91*, 062301.
[47] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, H. Weinfurter, *IEEE J. Sel. Top. Quantum Electron.* **2014**, *21*, 187.
[48] P. Chaiwongkhot, K. B. Kuntz, Y. Zhang, A. Huang, J.-P. Bourgoin, S. Sajeed, N. Lütkenhaus, T. Jennewein, V. Makarov, *Phys. Rev. A* **2019**, *99*, 062315.
[49] K. Wei, W. Zhang, Y.-L. Tang, L. You, F. Xu, *Phys. Rev. A* **2019**, *100*, 022325.
[50] V. Makarov, D. R. Hjelme, *J. Mod. Opt.* **2005**, *52*, 691.
[51] V. Makarov, A. Anisimov, J. Skaar, *Phys. Rev. A* **2006**, *74*, 022313.
[52] B. Qi, C.-H. F. Fung, H.-K. Lo, X. Ma, *Quantum Inf. Process.* **2007**, *7*, 73.
[53] C. Kurtsiefer, P. Zarda, S. Mayer, H. Weinfurter, *J. Mod. Opt.* **2001**, *48*, 2039.
[54] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, V. Makarov, *Opt. Express* **2018**, *26*, 21020.
[55] A. Meda, I. P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, M. Genovese, *Light: Sci. Appl.* **2017**, *6*, e16261.
[56] A. Meda, I. P. Degiovanni, A. Tosi, Z. Yuan, G. Brida, M. Genovese, in *Quantum Technologies 2018*, vol. *10674*, SPIE, Bellingham, WA **2018**, pp. 138–144.
[57] S. Sajeed, C. Minshull, N. Jain, V. Makarov, *Sci. Rep.* **2017**, *7*, 8403.
[58] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, G. Leuchs, *IEEE J. Sel. Top. Quantum Electron.* **2014**, *21*, 168.
[59] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, G. Leuchs, *New J. Phys.* **2014**, *16*, 123030.
[60] V. Makarov, *New J. Phys.* **2009**, *11*, 065003.
[61] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, V. Makarov, *New J. Phys.* **2011**, *13*, 113042.
[62] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, V. Makarov, *IEEE J. Quantum Electron.* **2016**, *52*, 1.
[63] V. Chistiakov, A. Huang, V. Egorov, V. Makarov, *Opt. Express* **2019**, *27*, 32253.
[64] G. Gras, N. Sultana, A. Huang, T. Jennewein, F. Bussières, V. Makarov, H. Zbinden, *J. Appl. Phys.* **2020**, *127*, 9.
[65] C. Wiechers, L. Lydersen, C. Wittmann, D. Elser, J. Skaar, C. Marquardt, V. Makarov, G. Leuchs, *New J. Phys.* **2011**, *13*, 013043.
[66] L. Lydersen, N. Jain, C. Wittmann, Ø. Marøy, J. Skaar, C. Marquardt, V. Makarov, G. Leuchs, *Phys. Rev. A* **2011**, *84*, 032320.
[67] M. Ye, J.-H. Li, Y. Wang, P. Gao, X.-X. Lu, Y.-J. Qian, *Commun. Theor. Phys.* **2020**, *72*, 115102.
[68] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen, V. Makarov, *Phys. Rev. Lett.* **2014**, *112*, 070503.
[69] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, S. Sajeed, *Phys. Rev. A* **2016**, *94*, 030302.
[70] D. Rusca, A. Boaron, M. Curty, A. Martin, H. Zbinden, *Phys. Rev. A* **2018**, *98*, 052336.
[71] P. M. Nielsen, C. Schori, J. L. Sørensen, L. Salvail, I. Damgard, E. Polzik, *J. Mod. Opt.* **2001**, *48*, 1921.
[72] M. LaGasse, Secure use of a single single-photon detector in a qkd system, US Patent App. 11/030,241 **2005**.
[73] D. Gottesman, H.-K. Lo, N. Lütkenhaus, J. Preskill, *Quantum Inf. Process.* **2004**, *4*, 325.
[74] F. Fung, K. Tamaki, B. Qi, H.-K. Lo, X. Ma, *Quantum Inf. Process.* **2009**, *9*, 131.
[75] L. Lydersen, J. Skaar, *Quantum Inf. Process.* **2010**, *10*, 60.
[76] A. Winick, N. Lütkenhaus, P. J. Coles, *Quantum* **2018**, *2*, 77.
[77] M. Bochkov, A. Trushechkin, *Phys. Rev. A* **2019**, *99*, 032308.
[78] J. Ma, Y. Zhou, X. Yuan, X. Ma, *Phys. Rev. A* **2019**, *99*, 062325.
[79] Y. Zhang, P. J. Coles, A. Winick, J. Lin, N. Lütkenhaus, *Phys. Rev. Res.* **2021**, *3*, 013076.
[80] A. Trushechkin, *Quantum* **2022**, *6*, 771.
[81] H.-K. Lo, M. Curty, B. Qi, *Phys. Rev. Lett.* **2012**, *108*, 130503.
[82] M. Lucamarini, Z. L. Yuan, J. F. Dynes, A. J. Shields, *Nature* **2018**, *557*, 400.
[83] C. H. Bennett, G. Brassard, N. D. Mermin, *Phys. Rev. Lett.* **1992**, *68*, 557.
[84] E. Biham, B. Huttner, T. Mor, *Phys. Rev. A* **1996**, *54*, 2651.
[85] Y.-H. Zhou, Z.-W. Yu, X.-B. Wang, *Phys. Rev. A* **2016**, *93*, 042324.
[86] X. Ma, C.-H. F. Fung, M. Razavi, *Phys. Rev. A* **2012**, *86*, 052305.
[87] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, H.-K. Lo, *Nat. Commun.* **2014**, *5*, 3732.
[88] K. Tamaki, H.-K. Lo, C.-H. F. Fung, B. Qi, *Phys. Rev. A* **2012**, *85*, 042307.
[89] X. Ma, M. Razavi, *Phys. Rev. A* **2012**, *86*, 062319.
[90] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, W. Tittel, *Phys. Rev. Lett.* **2013**, *111*, 130501.
[91] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, H.-K. Lo, *Phys. Rev. Lett.* **2014**, *112*, 190503.
[92] C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, C.-M. Zhang, G.-C. Guo, Z.-F. Han, *Phys. Rev. Lett.* **2015**, *115*, 160502.
[93] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, J.-W. Pan, *Phys. Rev. Lett.* **2016**, *117*, 190501.
[94] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, A. Shields, *Nat. Photonics* **2016**, *10*, 312.
[95] Z. Tang, K. Wei, O. Bedroya, L. Qian, H.-K. Lo, *Phys. Rev. A* **2016**, *93*, 042308.
[96] K. Wei, W. Li, H. Tan, Y. Li, H. Min, W.-J. Zhang, H. Li, L. You, Z. Wang, X. Jiang, T.-Y. Chen, S.-K. Liao, C.-Z. Peng, F. Xu, J.-W. Pan, *Phys. Rev. X* **2020**, *10*, 031030.
[97] H.-J. Briegel, W. Dür, J. I. Cirac, P. Zoller, *Phys. Rev. Lett.* **1998**, *81*, 5932.
[98] L.-M. Duan, M. D. Lukin, J. I. Cirac, P. Zoller, *Nature* **2001**, *414*, 413.
[99] N. Sangouard, C. Simon, H. De Riedmatten, N. Gisin, *Rev. Mod. Phys.* **2011**, *83*, 33.
[100] S. Abruzzo, H. Kampermann, D. Bruß, *Phys. Rev. A* **2014**, *89*, 012301.
[101] K. Azuma, K. Tamaki, W. J. Munro, *Nat. Commun.* **2015**, *6*, 10171.
[102] M. Curty, K. Azuma, H.-K. Lo, *npj Quantum Inf.* **2019**, *5*, 64.
[103] X. Ma, P. Zeng, H. Zhou, *Phys. Rev. X* **2018**, *8*, 031043.
[104] J. Lin, N. Lütkenhaus, *Phys. Rev. A* **2018**, *98*, 042332.
[105] X.-B. Wang, Z.-W. Yu, X.-L. Hu, *Phys. Rev. A* **2018**, *98*, 062323.

[106] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. Yuan, A. J. Shields, *Nat. Photonics* **2019**, *13*, 334.
[107] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, Z.-F. Han, *Phys. Rev. X* **2019**, *9*, 021046.
[108] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, J.-W. Pan, *Phys. Rev. Lett.* **2019**, *123*, 100505.
[109] X. Zhong, J. Hu, M. Curty, L. Qian, H.-K. Lo, *Phys. Rev. Lett.* **2019**, *123*, 100506.
[110] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, J.-W. Pan, *Nat. Photonics* **2020**, *14*, 422.
[111] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, J.-W. Pan, *Phys. Rev. Lett.* **2020**, *124*, 070501.
[112] H. Liu, C. Jiang, H.-T. Zhu, M. Zou, Z.-W. Yu, X.-L. Hu, H. Xu, S. Ma, Z. Han, J.-P. Chen, Y. Dai, S.-B. Tang, W. Zhang, H. Li, L. You, Z. Wang, F. Zhou, Q. Zhang, X.-B. Wang, T.-Y. Chen, J.-W. Pan, *Phys. Rev. Lett.* **2021**, *126*, 250502.
[113] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, Y. Chen, X.-B. Wang, Q. Zhang, J.-W. Pan, *Phys. Rev. Lett.* **2022**, *128*, 180502.
[114] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, A. J. Shields, *Nat. Photonics* **2021**, *15*, 530.
[115] W. Li, L. Zhang, Y. Lu, Z.-P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X.-B. Wang, Q. Zhang, L. You, F. Xu, J.-W. Pan, *Phys. Rev. Lett.* **2023**, *130*, 250802.
[116] L. Zhou, J. Lin, Y. Jing, Z. Yuan, *Nat. Commun.* **2023**, *14*, 928.
[117] P. Zeng, H. Zhou, W. Wu, X. Ma, *Nat. Commun.* **2022**, *13*, 3903.
[118] H.-T. Zhu, Y. Huang, H. Liu, P. Zeng, M. Zou, Y. Dai, S. Tang, H. Li, L. You, Z. Wang, Y.-A. Chen, X. Ma, T.-Y. Chen, J.-W. Pan, *Phys. Rev. Lett.* **2023**, *130*, 030801.
[119] L. Zhou, J. Lin, Y.-M. Xie, Y.-S. Lu, Y. Jing, H.-L. Yin, Z. Yuan, *Phys. Rev. Lett.* **2023**, *130*, 250801.
[120] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, Z.-B. Chen, *PRX Quantum* **2022**, *3*, 020315.
[121] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, K. Azuma, *Phys. Rev. A* **2014**, *90*, 052314.
[122] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, K. Tamaki, *New J. Phys.* **2015**, *17*, 093011.
[123] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, H.-K. Lo, *Phys. Rev. A* **2015**, *92*, 032305.
[124] G. Currás-Lorenzo, Á. Navarrete, M. Pereira, K. Tamaki, *Phys. Rev. A* **2021**, *104*, 012406.
[125] Z. Yuan, A. Sharpe, A. Shields, *Appl. Phys. Lett.* **2007**, *90*, 011118.
[126] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, A. Shields, *Opt. Express* **2008**, *16*, 18790.
[127] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, J.-W. Pan, *Opt. Express* **2010**, *18*, 8587.
[128] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, A. Shields, *Opt. Express* **2013**, *21*, 24550.
[129] R. Valivarthi, Q. Zhou, C. John, F. Marsili, V. B. Verma, M. D. Shaw, S. W. Nam, D. Oblak, W. Tittel, *Quantum Sci. Tech.* **2017**, *2*, 04LT01.
[130] Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, A. J. Shields, *J. Lightwave Technol.* **2018**, *36*, 3427.
[131] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, H.-K. Lo, *Opt. Express* **2012**, *20*, 12366.
[132] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, M. W. Mitchell, *Opt. Express* **2014**, *22*, 1645.
[133] S. Nahar, T. Upadhyaya, N. Lütkenhaus, Imperfect phase-randomisation and generalised decoy-state quantum key distribution, *preprint arXiv:2304.09401* **2023**.
[134] G. Currás-Lorenzo, K. Tamaki, M. Curty, *Quantum Sci. Tech.* **2024**, *9*, 015025.
[135] Y. Zhao, B. Qi, H.-K. Lo, *Appl. Phys. Lett.* **2007**, *90*, 044106.
[136] S.-H. Sun, L.-M. Liang, *Appl. Phys. Lett.* **2012**, *101*, 071107.
[137] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O'Brien, M. G. Thompson, *Nat. Commun.* **2017**, *8*, 13984.
[138] D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, N. Boynton, N. Martinez, C. DeRose, C. Chen, M. Grein, D. Trotter, A. Starbuck, A. Pomerene, S. Hamilton, F. N. C. Wong, R. Camacho, P. Davids, J. Urayama, D. Englund, *Phys. Rev. X* **2018**, *8*, 021009.
[139] Z. Cao, Z. Zhang, H.-K. Lo, X. Ma, *New J. Phys.* **2015**, *17*, 053014.
[140] G. Currás-Lorenzo, L. Wooltorton, M. Razavi, *Phys. Rev. Appl.* **2021**, *15*, 014016.
[141] X. Sixto, G. Currás-Lorenzo, K. Tamaki, M. Curty, *EPJ Quantum Tech.* **2023**, *10*, 53.
[142] A. Huang, Á. Navarrete, S.-H. Sun, P. Chaiwongkhot, M. Curty, V. Makarov, *Phys. Rev. Appl.* **2019**, *12*, 064043.
[143] S.-H. Sun, F. Xu, M.-S. Jiang, X.-C. Ma, H.-K. Lo, L.-M. Liang, *Phys. Rev. A* **2015**, *92*, 022304.
[144] A. Huang, R. Li, V. Egorov, S. Tchouragoulov, K. Kumar, V. Makarov, *Phys. Rev. Appl.* **2020**, *13*, 034017.
[145] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, H. Weinfurter, *New J. Phys.* **2009**, *11*, 065001.
[146] A. Duplinskiy, D. Sych, *Phys. Rev. A* **2021**, *104*, 012601.
[147] J. E. Bourassa, A. Gnanapandithan, L. Qian, H.-K. Lo, *Phys. Rev. A* **2022**, *106*, 062618.
[148] W.-S. Huang, W. Zhang, Y.-D. Huang, *J. Electron. Sci. Technol.* **2019**, *17*, 195.
[149] P. Arteaga Díaz, D. Cano, V. Fernandez, *IEEE Access* **2022**, *10*, 82697.
[150] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, G. Ribordy, *Phys. Rev. A* **2006**, *73*, 022320.
[151] A. Vakhitov, V. Makarov, D. R. Hjelme, *J. Mod. Opt.* **2001**, *48*, 2023.
[152] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, H. Weinfurter, *Phys. Rev. Lett.* **2007**, *98*, 010504.
[153] B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, A. J. Shields, *Optica* **2017**, *4*, 163.
[154] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, H. Zbinden, *Appl. Phys. Lett.* **2020**, *117*, 144003.
[155] T. Kobayashi, A. Tomita, A. Okamoto, *Phys. Rev. A* **2014**, *90*, 032320.
[156] G. Roberts, M. Pittaluga, M. Minder, M. Lucamarini, J. Dynes, Z. Yuan, A. Shields, *Opt. Lett.* **2018**, *43*, 5110.
[157] K.-i. Yoshino, M. Fujiwara, K. Nakata, T. Sumiya, T. Sasaki, M. Takeoka, M. Sasaki, A. Tajima, M. Koashi, A. Tomita, *npj Quantum Inf.* **2018**, *4*, 8.
[158] Y. Gao, Z. Yuan, *Opt. Lett.* **2023**, *48*, 1068.
[159] M. Pereira, M. Curty, K. Tamaki, *npj Quantum Inf.* **2019**, *5*, 62.
[160] Á. Navarrete, M. Pereira, M. Curty, K. Tamaki, *Phys. Rev. Appl.* **2021**, *15*, 034072.
[161] M. Pereira, G. Currás-Lorenzo, Á. Navarrete, A. Mizutani, G. Kato, M. Curty, K. Tamaki, *Phys. Rev. Res.* **2023**, *5*, 023065.
[162] M. Pereira, G. Kato, A. Mizutani, M. Curty, K. Tamaki, *Sci. Adv.* **2020**, *6*, 37 eaaz4487.
[163] G. Currás-Lorenzo, M. Pereira, G. Kato, M. Curty, K. Tamaki, A security framework for quantum key distribution implementations, *preprint arXiv:2305.05930* **2023**.
[164] H.-K. Lo, J. Preskill, *Quantum Inf. Comput.* **2007**, *7*, 431.

[165] Y. Nagamatsu, A. Mizutani, R. Ikuta, T. Yamamoto, N. Imoto, K. Tamaki, *Phys. Rev. A* **2016**, *93*, 042325.
[166] A. Mizutani, G. Kato, K. Azuma, M. Curty, R. Ikuta, T. Yamamoto, N. Imoto, H.-K. Lo, K. Tamaki, *npj Quantum Inf.* **2019**, *5*, 8.
[167] V. Zapatero, Á. Navarrete, K. Tamaki, M. Curty, *Quantum* **2021**, *5*, 602.
[168] X. Sixto, V. Zapatero, M. Curty, *Phys. Rev. Appl.* **2022**, *18*, 044069.
[169] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. Yuan, A. J. Shields, *Phys. Rev. X* **2015**, *5*, 031030.
[170] K. Tamaki, M. Curty, M. Lucamarini, *New J. Phys.* **2016**, *18*, 065008.
[171] W. Wang, K. Tamaki, M. Curty, *New J. Phys.* **2018**, *20*, 083027.
[172] H. Tan, W. Li, L. Zhang, K. Wei, F. Xu, *Phys. Rev. Appl.* **2021**, *15*, 064038.
[173] Á. Navarrete, M. Curty, *Quantum Sci. Tech.* **2022**, *7*, 035021.
[174] H.-J. Ding, J.-Y. Liu, X.-Y. Zhou, C.-H. Zhang, J. Li, Q. Wang, *Phys. Rev. Appl.* **2023**, *19*, 044022.
[175] S. Todoroki, S. Inoue, in, Proceedings of the XXth International Congress on Glass, Report No. O-14-010, Kyoto, Japan, **2004**.
[176] G. Zhang, I. W. Primaatmaja, J. Y. Haw, X. Gong, C. Wang, C. C. W. Lim, *PRX Quantum* **2021**, *2*, 030304.
[177] A. Ponosova, D. Ruzhitskaya, P. Chaiwongkhot, V. Egorov, V. Makarov, A. Huang, *PRX Quantum* **2022**, *3*, 040307.
[178] W. Wang, R. Wang, C. Hu, V. Zapatero, L. Qian, B. Qi, M. Curty, H.-K. Lo, *Phys. Rev. Lett.* **2023**, *130*, 220801.
[179] V. Zapatero, W. Wang, M. Curty, *Quantum Sci. Tech.* **2023**, *8*, 025014.
[180] M. Curty, X. Ma, B. Qi, T. Moroder, *Phys. Rev. A* **2010**, *81*, 022310.
[181] M. Curty, X. Ma, H.-K. Lo, N. Lütkenhaus, *Phys. Rev. A* **2010**, *82*, 052325.
[182] F.-Y. Lu, Z.-H. Wang, V. Zapatero, J.-L. Chen, S. Wang, Z.-Q. Yin, M. Curty, D.-Y. He, R. Wang, W. Chen, G.-J. Fan-Yuan, G.-C. Guo, Z.-F. Han, *Phys. Rev. Lett.* **2023**, *131*, 110802.
[183] C. Hu, W. Wang, K.-S. Chan, Z. Yuan, H.-K. Lo, *Phys. Rev. Lett.* **2023**, *131*, 110801.
[184] W. Wang, R. Wang, H.-K. Lo, Fully-passive twin-field quantum key distribution, *preprint arXiv:2304.12062* **2023**.
[185] J. Li, W. Wang, H.-K. Lo, , Fully passive measurement-device-independent quantum key distribution, *preprint arXiv:2309.07673* **2023**.
[186] V. Zapatero, M. Curty, Finite-key security of passive quantum key distribution, *preprint arXiv:2308.02376* **2023**.
[187] D. Mayers, A. Yao, in *Proceedings 39th Annual Symposium on Foundations of Computer Science*, IEEE, Piscataway, NJ **1998**, pp. 503–509.
[188] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, V. Scarani, *Phys. Rev. Lett.* **2007**, *98*, 230501.
[189] J. Barrett, L. Hardy, A. Kent, *Phys. Rev. Lett.* **2005**, *95*, 010503.
[190] I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J. T.-F. Khoo, S. Ghorai, C. C.-W. Lim, *Quantum* **2023**, *7*, 932.
[191] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, M. Curty, *npj Quantum Inf.* **2023**, *9*, 10.
[192] E. Y. Z. Tan, Robustness of implemented device-independent protocols against constrained leakage, *preprint arXiv:2302.13928* **2023**.
[193] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, S. Wehner, *Rev. Mod. Phys.* **2014**, *86*, 419.
[194] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, V. Scarani, *New J. Phys.* **2009**, *11*, 045021.
[195] M. Giustina, M. A. Versteegh, S. Wengerowsky, J. Handsteiner, A. Hochrainer, K. Phelan, F. Steinlechner, J. Kofler, J.-Å. Larsson, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, J. Beyer, T. Gerrits, A. E. Lita, L. K. Shalm, S. W. Nam, T. Scheidl, R. Ursin, B. Wittmann, A. Zeilinger, *Phys. Rev. Lett.* **2015**, *115*, 250401.
[196] L. K. Shalm, E. Meyer-Scott, B. G. Christensen, P. Bierhorst, M. A. Wayne, M. J. Stevens, T. Gerrits, S. Glancy, D. R. Hamel, M. S. Allman, K. J. Coakley, S. D. Dyer, C. Hodge, A. E. Lita, V. B. Verma, C. Lambrocco, E. Tortorici, A. L. Migdall, Y. Zhang, D. R. Kumor, W. H. Farr, F. Marsili, M. D. Shaw, J. A. Stern, C. Abellán, W. Amaya, V. Pruneri, T. Jennewein, M. W. Mitchell, P. G. Kwiat, et al., *Phys. Rev. Lett.* **2015**, *115*, 250402.
[197] M.-H. Li, C. Wu, Y. Zhang, W.-Z. Liu, B. Bai, Y. Liu, W. Zhang, Q. Zhao, H. Li, Z. Wang, L. You, W. J. Munro, J. Yin, J. Zhang, C.-Z. Peng, X. Ma, Q. Zhang, J. Fan, J.-W. Pan, *Phys. Rev. Lett.* **2018**, *121*, 080404.
[198] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, R. Hanson, *Nature* **2015**, *526*, 682.
[199] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, H. Weinfurter, *Phys. Rev. Lett.* **2017**, *119*, 010402.
[200] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, J.-D. Bancal, *Nature* **2022**, *607*, 682.
[201] W. Zhang, T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, H. Weinfurter, *Nature* **2022**, *607*, 687.
[202] W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, M.-H. Li, Y. Liu, J. Fan, F. Xu, Q. Zhang, J.-W. Pan, *Phys. Rev. Lett.* **2022**, *129*, 050502.
[203] V. Zapatero, M. Curty, *Sci. Rep.* **2019**, *9*, 17749.
[204] J. Barrett, R. Colbeck, A. Kent, *Phys. Rev. Lett.* **2013**, *110*, 010503.
[205] M. Curty, H.-K. Lo, *npj Quantum Inf.* **2019**, *5*, 14.
[206] V. Zapatero, M. Curty, *npj Quantum Inf.* **2021**, *7*, 26.
[207] W. Li, V. Zapatero, H. Tan, K. Wei, H. Min, W.-Y. Liu, X. Jiang, S.-K. Liao, C.-Z. Peng, M. Curty, F. Xu, J.-W. Pan, *Phys. Rev. Appl.* **2021**, *15*, 034081.
[208] https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.
[209] https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies.
[210] https://www.ssi.gouv.fr/en/publication/should-quantum-key-distribution-be-used-for-secure-communications/.

Víctor Zapatero obtained a bachelor's degree and a master's degree in Theoretical Physics at the Universidad Complutense de Madrid. Then, he was granted a national scholarship to do a Ph.D. in quantum cryptography at the University of Vigo, under the supervision of Prof. Marcos Curty. Upon completion of his Ph.D. in 2021, Víctor started a postdoc position in the same group, to later on become a senior postdoc researcher in the Vigo Quantum Communication Center. The main focus of his research is the security of quantum key distribution, and he is also interested in the foundations of quantum mechanics.

Álvaro Navarrete received his B.Sc. in Telecommunication Technologies Engineering in 2015 and his M.Sc. in Laser and Photonics in 2016. He then received a national grant to start his doctoral studies at the University of Vigo, where his research focused on the security and performance of quantum key distribution systems. He successfully defended his Ph.D. in 2021 and is currently working as a postdoctoral researcher at the Vigo Quantum Communication Center.

Marcos 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 obtained a Ph.D in theoretical Physics (2006). After postdoc positions at Toronto University and at the Institute for Quantum Computing, Waterloo University (Canada), he was Assistant Professor at the department of Electronic and Communications Engineering at Zaragoza University (Spain). Currently, he is full Professor at the department of Theory of Signal and Communications at Vigo University. His research interest lies in quantum communication, particularly quantum cryptography. He is co-author of about hundred scientific publications in this field and a few patents.