Measurement-device-independent quantum digital signatures

Measurement-device-independent quantum digital signatures

Ittoop Vergheese Puthoor,[1,*] Ryan Amiri,[1] Petros Wallden,[2] Marcos Curty,[3] and Erika Andersson[1]
[1]*SUPA, Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*
[2]*LFCS, School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*
[3]*EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain*
(Received 14 May 2016; published 23 August 2016)

Digital signatures play an important role in software distribution, modern communication, and financial transactions, where it is important to detect forgery and tampering. Signatures are a cryptographic technique for validating the authenticity and integrity of messages, software, or digital documents. The security of currently used classical schemes relies on computational assumptions. Quantum digital signatures (QDS), on the other hand, provide information-theoretic security based on the laws of quantum physics. Recent work on QDS Amiri *et al.*, Phys. Rev. A **93**, 032325 (2016); Yin, Fu, and Zeng-Bing, Phys. Rev. A **93**, 032316 (2016) shows that such schemes do not require trusted quantum channels and are unconditionally secure against general coherent attacks. However, in practical QDS, just as in quantum key distribution (QKD), the detectors can be subjected to side-channel attacks, which can make the actual implementations insecure. Motivated by the idea of measurement-device-independent quantum key distribution (MDI-QKD), we present a measurement-device-independent QDS (MDI-QDS) scheme, which is secure against all detector side-channel attacks. Based on the rapid development of practical MDI-QKD, our MDI-QDS protocol could also be experimentally implemented, since it requires a similar experimental setup.

DOI: 10.1103/PhysRevA.94.022328

I. INTRODUCTION

Digital signatures are techniques for guaranteeing the authenticity and integrity of a message. They play a significant role for example in financial transactions, software distribution, and e-mail. Signature schemes allow a sender to exchange messages with many recipients, with the assurance that the messages cannot be forged or tampered with. In addition, signed messages are also transferable, and cannot be repudiated. Transferability means that a message, which is accepted by an honest recipient, will also be accepted by another recipient if the message is forwarded. Nonrepudiation is related to transferability and means that a sender cannot successfully deny having sent a signed message.

Classical digital signature schemes rely on public-key encryption. The security of such protocols is based on the assumed computational difficulty of inverting certain cryptographic functions. For example, an algorithm that is widely used for generating digital signatures is the Rivest-Shamir-Adleman (RSA) [1] cryptosystem, which relies on the difficulty of factoring the product of two large prime numbers. However, if a quantum computer is built, this may threaten the security of such protocols. This is a main motivation for developing unconditionally secure signature schemes [2,3], including quantum digital signature (QDS) schemes [4–8]. The latter are essentially quantum versions of Lamport's one-time signature scheme [9], and can offer information-theoretic security relying on the fundamental laws of quantum physics.

Previous QDS schemes [5–8] improved on the seminal work in [4] by removing the need for quantum memory. Wallden *et al.* [10] proposed more practical QDS schemes which could be realized using QKD [11] components. In these QDS schemes, Alice encodes her signatures in quantum states, and sends a copy of each state to both Bob and Charlie. Bob and Charlie are only able to gain partial information on the overall signature state, due to its quantum nature. Until recently, the security analysis of all QDS schemes assumed authenticated quantum channels. In [12,13], all trust assumptions on the quantum channels are removed, which is a significant improvement compared to the previous schemes.

It is however more challenging to guarantee the security of practical implementations of QDS schemes. This is so because practical realizations do not typically conform to the requirements imposed by the theory, as real devices can behave differently from the models considered in the security proofs. As a result, we have that any imperfection which is not accounted for might constitute a "side channel" which could be used by an adversary to render the QDS scheme insecure. Here, the most critical devices are arguably the single-photon detectors [14–21]. For example, an adversary can use detector loopholes to learn about a participant's (say Bob's) measurement results, and could then forge a message with Bob. In the context of QKD, detector side channels can be successfully removed by means of measurement-device-independent QKD (MDI-QKD) [22]. In this approach, Alice and Bob do not perform any measurement but only send quantum signals to be measured. Thus the advantage of MDI-QKD is that the legitimate parties need not hold a measurement device and may treat the measurement apparatus as a "black box," which may be fully controlled by Eve. This is important as it eliminates the requirement to certify the detectors in a QKD standarization process. Therefore, the bit strings generated by Alice and Bob are free from detector

*Ittoop.Puthoor@hw.ac.uk

side-channel attacks as they do not employ any detector. Hence this only requires Alice and Bob to characterize the quantum states which they send through the channel. This characterization should take place in a protected environment outside the influence of the adversary, which in principle is feasible. Since the invention of MDI-QKD, such schemes have been very actively studied both theoretically [23–26] and experimentally [27–32].

In this paper, we present a QDS protocol which eliminates all detector side-channel attacks by employing the concept of measurement device independence. This is desirable for actual practical use of QDS schemes. The main contribution of this work is to adapt the rigorous security proof of MDI-QKD given in [26], taking into account finite-size effects, to the QDS protocol proposed in [12]. The resulting security proof is valid against general forging and repudiation attacks. Long-distance implementation of MDI-QKD [27–32] has been recently achieved, and the experimental parameters allowing for MDI-QKD could equally well allow for implementation of our QDS protocol. Hence we envisage not just a long-distance implementation of a QDS protocol, but an implementation that is secure against detector side-channel attacks.

II. PROTOCOL

We outline our protocol for three parties, with a sender, Alice, and two recipients Bob and Charlie. The setup for MDI-QDS is illustrated in Fig. 1. We assume that between Alice and Bob, and between Alice and Charlie, there exist authenticated classical channels. There is no need for "direct" quantum channels between Alice and Bob, between Alice and Charlie, nor between Bob and Charlie. Each party has an untrusted and imperfect quantum channel with the relay (Eve). Bob and Charlie share a MDI-QKD link, which can be used to transmit classical messages in full secrecy. This is separately indicated in the figure, but could also be realized with Eve as relay. Any classical secret communication channel between Bob and Charlie would in fact suffice in place of this MDI-QKD link. We will describe the procedure for signing a one-bit message. For signing longer messages, the procedure can be suitably iterated, meaning that the signature length scales linearly with message length.

Alice, Bob, and Charlie each use a laser source to generate quantum signals that are diagonal in the Fock basis. Sources producing such signals include attenuated laser diodes emitting phase-randomized weak coherent pulses (WCPs), triggered spontaneous parametric down-conversion sources, and practical single-photon sources. The scheme makes use of a measurement-device-independent key generating protocol (MDI-KGP), performed in pairs separately by Alice-Bob and Alice-Charlie; see Sec. III for more details. The purpose of such an MDI-KGP scheme is to use the noisy untrusted quantum channels to generate two correlated bit strings, one for each participant in an MDI-KGP. The noise level is defined in terms of the relative Hamming distance between these strings. When the noise level is below a tolerated value, the relative Hamming distance between the respective strings of the participants is smaller than the relative Hamming distance between any string that an eavesdropper could produce, and the participant's string.

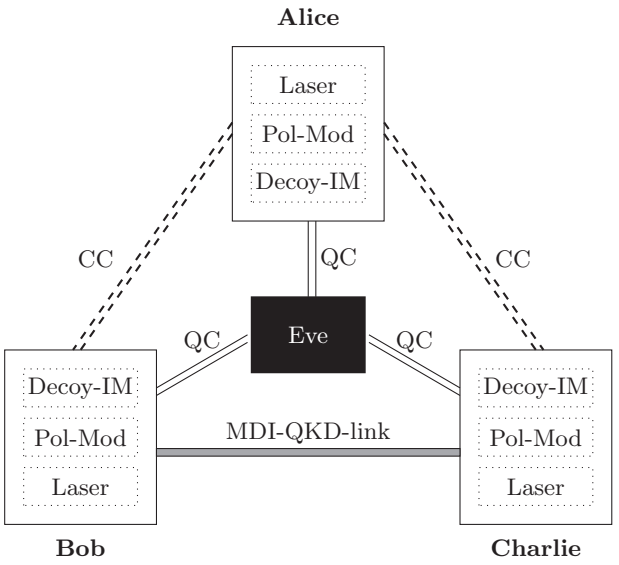

FIG. 1. Schematic diagram of a setup for MDI-QDS. Alice, Bob, and Charlie prepare quantum signals in different BB84 polarization states, using a polarization modulator (Pol-Mod). In addition, they generate decoy states with an intensity modulator (Decoy-IM). The signals are then sent to an untrusted party Eve, who acts like a relay and is supposed to perform a Bell state measurement, which projects the incoming signals into a Bell state. The channels between Alice-Eve, Bob-Eve, and Charlie-Eve are quantum channels (QC). Eve performs the measurement separately for the pairs Alice-Bob and Alice-Charlie. Bob and Charlie share a MDI-QKD link (gray channel), which can be used to transmit classical messages in full secrecy. The pairs Alice-Bob and Alice-Charlie have pairwise authenticated classical channels (CC) indicated as dashed lines, through which they can communicate their basis settings for the different key positions.

The QDS scheme above is related to the one proposed in [12], with a difference in the KGP. It comprises of two stages, a distribution stage, where all quantum communication takes place, and a messaging stage, which can occur much later, and where only classical communication is used.

A. Distribution stage

(1) For each possible future message $m = 0$ or 1, Alice uses the MDI-KGP to generate four different correlated bit strings, $A_0^B, A_1^B, A_0^C, A_1^C$, each one of length L. The superscript denotes the participant with whom Alice performed the MDI-KGP, and the subscript represents the future message, which is to be decided later by her. Bob holds the strings K_0^B, K_1^B and Charlie holds the strings K_0^C, K_1^C. Because of the KGP, it will be guaranteed that A_0^B contains fewer mismatches with K_0^B than does any string produced by an eavesdropper, and similarly for the other pairs of strings. Alice's signature for the future message m will be $\mathrm{Sig}_m = (A_m^B, A_m^C)$. The fact that only Alice knows all signatures for a message m protects the protocol against forging.

(2) For each future message, Bob and Charlie symmetrize their keys. This is done by each of them choosing at random

half of the bit values in their keys (K_m^B, K_m^C) and sending these bit values (as well as the corresponding positions) to the other participant using their secret classical channel. This will ensure that Alice cannot make Bob and Charlie disagree on the validity of a signature, if a message is forwarded from Bob to Charlie or vice versa in the messaging stage. If Bob (or Charlie) chooses to forward an element of K_m^B (or K_m^C) in the distribution stage to Charlie (or Bob), he will not, if he is honest, further use it to check the validity of a signature. Bob and Charlie will only use the bits they did not forward, and those received from the other participant. This is not strictly necessary, but simplifies the analysis of repudiation by a dishonest Alice in that from Alice's point of view, the probabilities are equal for Bob and Charlie to check a particular key bit. We denote their symmetrized keys by S_m^B and S_m^C, with the superscript indicating whether the key is held by Bob or Charlie. Bob (and Charlie) keep a record of whether an element in S_m^B (S_m^C) came directly from Alice or whether it was forwarded to him by Charlie (or Bob).

Each of the symmetrized strings held by Bob and Charlie now contains half of K_m^B and half of K_m^C. For each future possible message m, Bob and Charlie each have a bit string of length L. Alice has no information on whether it is Bob's S_m^B or Charlie's S_m^C that contains a particular element of the string (K_m^B, K_m^C), which is of length $2L$. This protects against repudiation. Bob has access to all of K_m^B and half of K_m^C. He does not know the other half of K_m^C which Charlie chose to keep. This protects the protocol against forging by Bob (and similarly against forging by Charlie).

B. Messaging stage

(1) To send a signed one-bit message m, Alice sends (m, Sig_m) to the desired recipient (say Bob).

(2) Bob checks whether (m, Sig_m) matches his S_m^B, and records the number of mismatches he finds. He separately checks the part of his key received directly from Alice and the part of the key received from Charlie. If there are fewer than $s_a(L/2)$ mismatches in both halves of the key, where $s_a < 1/2$ is a small threshold determined by the observed experimental parameters (see Appendix D for more details) and the desired security level of the protocol, then Bob accepts the message.

(3) To forward the message to Charlie, Bob forwards the pair (m, Sig_m) that he received from Alice.

(4) Charlie tests for mismatches in a similar way, but using a different threshold in order to protect against repudiation by Alice. He accepts the forwarded message if the number of mismatches in both halves of his key is below $s_v(L/2)$, where s_v is another threshold, with $0 < s_a < s_v < 1/2$. An important and necessary feature of unconditionally secure signature schemes [2,33] is that the recipients have to use different thresholds or acceptance criteria for messages received directly from the sender and for forwarded messages.

III. MEASUREMENT-DEVICE-INDEPENDENT KEY GENERATION PROTOCOL

MDI-QKD protocols [22,26,34] are schemes that remove all detector side-channel attacks. This is very important when we consider detector loopholes in conventional QKD implementations [14,21]. Similarly, the key generation protocol, which is part of the QDS scheme we are describing, can be made measurement device independent. Essentially, Alice and Bob (or Alice and Charlie) only perform the quantum part of the MDI-QKD scheme to generate raw different keys (the A_m^B and K_m^B described above) with imperfectly correlated and not completely secret bit strings. That is, Alice and Bob do not perform error correction and privacy amplification. This is sufficient for quantum signatures, since it is the number of mismatches with the recipient's key that matters for the signature protocol; perfectly correlated, perfectly secret strings are not necessary. The aim is to show that $\Lambda(A_m^B, K_m^B) < \Lambda(E_{\mathrm{guess}}, K_m^B)$ except with negligible probability, where $\Lambda(x,y)$ is the Hamming distance between x and y, and E_{guess} is Eve's attempt at guessing K_m^B. It can also be possible that the adversary Eve is Charlie (for the KGP performed between Alice and Bob, and for the KGP performed by Alice and Charlie, Eve could be Bob). The security of the signature protocol is proved in Sec. IV.

The underlying MDI-QKD protocol, upon which the KGP is built, is the decoy-state BB84 protocol using phase-randomized WCPs considered in [22]. We follow the steps of the protocol in [26], using the Z basis for key generation, but do not proceed with error correction and privacy amplification.

The different steps of the MDI-KGP are as follows.

(1) State preparation. Alice and Bob repeat the first two steps of the protocol for $i = 1, \ldots, N$ until the conditions in the sifting stage are met. For each i, Alice chooses an intensity $a \in \{a_s, a_{d_1}, a_{d_2}\}$, a basis $\alpha \in \{Z, X\}$, and a random bit $r \in \{0,1\}$ with probability $p_{a,\alpha}/2$. Here a_s (a_{d_j} where $j \in \{1,2\}$) is the intensity of the signal (decoy) states. Next, she generates a quantum signal (e.g., a phase-randomized WCP) of intensity a prepared in the basis state of α given by r. Similarly, Bob does the same. Alice and Bob then send their states to Eve via the quantum channel.

(2) Measurement. If Eve is honest, she makes a Bell state measurement of the signals she has received. Whether Eve is honest or not, she informs Alice and Bob through a public channel of whether or not her measurement was successful. If successful, she declares the Bell state that is obtained.

(3) Sifting. If Eve reports a successful result, Alice and Bob communicate through an authenticated channel their intensity and basis settings. For each Bell state k, we define two groups of sets: $Z_k^{a,b}$ and $X_k^{a,b}$. $Z_k^{a,b}$ is a set that identifies signals where Eve declares a Bell state k and Alice and Bob have selected the intensities a and b and the basis Z. Similarly, $X_k^{a,b}$ is a set that identifies signals where Eve declares a Bell state k and Alice and Bob have selected the intensities a and b and the basis X. The protocol is repeated until $|Z_k^{a,b}| \geqslant N_k^{a,b}$ and $|X_k^{a,b}| \geqslant M_k^{a,b}\ \forall a,b,k$ [35]. After this, Bob flips part of his bits to correctly correlate them with those of Alice. This is shown in Table I.

(4) Parameter estimation. Alice and Bob use n_k random bits from $Z_k^{a_s,b_s}$ to form the code bit strings $\mathcal{Z}_k$ and $\mathcal{Z}'_k$, respectively. The remaining R_k bits from $Z_k^{a_s,b_s}$ are used to compute the error rate $E_k^{a_s,b_s} = \frac{1}{R_k}\sum_l r_l \oplus r_{l'}$, where r_l and $r_{l'}$ are Alice's and Bob's bits, respectively. The bit string of length R_k is used to estimate the correlation between Alice and Bob's strings generated from the Z basis, after which they

TABLE I. Processing of data in the sifting stage. The Bell states are defined as $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$, $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle)$, and $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|HH\rangle - |VV\rangle)$.

	Bell state reported by Eve			
Alice's and Bob's basis	$\|\psi^-\rangle$	$\|\psi^+\rangle$	$\|\phi^-\rangle$	$\|\phi^+\rangle$
Z basis	Bit flip	Bit flip		
X basis	Bit flip		Bit flip	

are discarded. If $E_k^{a_s,b_s} > E_{\text{tol}} \forall k$, then Alice and Bob abort the protocol. If $E_k^{a_s,b_s} \leqslant E_{\text{tol}}$, Alice and Bob use $Z_k^{a,b}$ and $X_k^{a,b}$ to estimate $n_{k,0}$,$n_{k,1}$ and $e_{k,1}$. The parameter $n_{k,0}$ is a lower bound for the number of bits in $\mathcal{Z}'_{k,\text{keep}}$ where Bob sent a vacuum state. $\mathcal{Z}'_{k,\text{keep}}$ is the part of $\mathcal{Z}'_k$ which he chooses to keep with himself while he forwards the other remaining part, $\mathcal{Z}'_{k,\text{forward}}$, to Charlie during the key symmetrization process. That is, $|\mathcal{Z}'_{k,\text{keep}}| = |\mathcal{Z}'_{k,\text{forward}}| = n_k/2$. In a similar way, $n_{k,1}$ is a lower bound for the number of bits in $\mathcal{Z}'_{k,\text{keep}}$ where Alice and Bob sent a single-photon state. $e_{k,1}$ is an upper bound for the single-photon phase error rate. If $e_{k,1} \geqslant e_{\text{tol}}$, the code bit strings $\mathcal{Z}_k$ and $\mathcal{Z}'_k$ are discarded, and the protocol is aborted only if $e_{k,1} \geqslant e_{\text{tol}}\ \forall k$.

We will assume that Eve implements her Bell state measurement using linear optics. The measurement setup is illustrated in Fig. 2; it is able to identify two of the four Bell states. Alice and Bob choose $\mathcal{Z}_k$ and $\mathcal{Z}'_k$ as their respective secret keys A_m^B and K_m^B of length L (where $L = n_k$), for which they obtained the smallest phase error rate $e_{k,1}$. Here, we will consider a finite number of states that are sent and measured, where Eve is allowed to perform general coherent attacks.

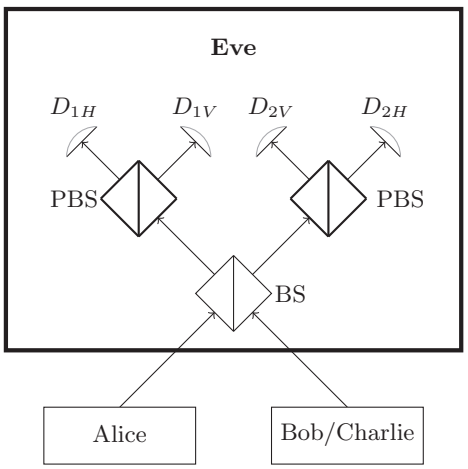

FIG. 2. Schematic diagram of Eve's measurement device. The combination of polarizing beam splitters (PBSs) and a 50:50 beam splitter (BS) projects the incoming signals from Alice and Bob or Charlie into horizontal (H) and vertical (V) polarization states. A joint click on the single-photon detectors D_{1H} and D_{2V}, or D_{1V} and D_{2H}, represents a projection into the Bell state $|\psi^-\rangle$, while a joint click in D_{1H} and D_{1V}, or D_{2V} and D_{2H}, indicates a projection into the Bell state $|\psi^+\rangle$.

Our strategy is to find Eve's information in terms of the smooth min-entropy [36], and then use it to bound the probability that she can make a signature declaration making fewer errors than a certain value. We begin by finding Eve's smooth min-entropy on Bob's bit string $\mathcal{Z}'_{k,\text{keep}}$, by following the same strategy as in [12]. In spite of the fact that the KGP is built on MDI-QKD, the security analysis for the MDI-KGP does not follow directly from the security of the MDI-QKD protocol. One reason is that the goal of an adversary in the signature protocol is different from that of an eavesdropper in MDI-QKD. For the signature protocol, what matters is the number of mismatches with a recipient's key; for QKD, what matters is the information an eavesdropper can hold about a key. These are related but not identical.

Previous work [12] followed [37] to find Eve's smooth min-entropy in a similar way as for decoy-state QKD. Another important difference from QKD is that in the signature protocol, Bob effectively gives the extra information $\mathcal{Z}'_{k,\text{forward}}$ to Eve (with respect to forging with Bob, Charlie can be "Eve"). In a similar way, let us denote the classical random variables R_k and Θ as the information gained by Eve from parameter estimation and basis declarations for all the pulses sent by Alice and Bob, respectively. Since Bob, if he is honest, does not use $\mathcal{Z}'_{k,\text{forward}}$, this could be treated as the part of the string R_k that is sacrificed for parameter estimation, as explained in [38]. We combine all of Eve's information into one quantum system living in the Hilbert space $\mathcal{H}_E$. This comprises the space containing Eve's ancilla quantum system following her general attack, $\mathcal{H}_{E'}$, as well as the spaces containing the states encoding the strings R_k,Θ and $\mathcal{Z}'_{k,\text{forward}}$. Then, according to [26], Eve's smooth min-entropy, which quantifies the average probability that she guesses $\mathcal{Z}'_{k,\text{keep}}$ within a certain threshold using the optimal strategy with access to E_k, is given by

$$H_{\min}^{\varepsilon_k}(\mathcal{Z}'_{k,\text{keep}}|E_k)_\rho \geqslant n_{k,0} + n_{k,1}[1 - h(e_{k,1})] - 2\log_2 \frac{2}{\varepsilon'_k \hat{\varepsilon}_k}, \tag{1}$$

where $\varepsilon_k \geqslant \varepsilon'_k + \hat{\varepsilon}_k$ and ρ is the state shared by Eve and the part of the key that Bob kept and did not forward. We are interested in a regime where the first two terms on the right-hand side (RHS) of Eq. (1) are much larger than the $\log_2$ term as ε'_k and $\hat{\varepsilon}_k$ are typically of the order say 10^{-5}–10^{-10}. Therefore, we arrive at the following approximation of Eq. (1):

$$H_{\min}^{\varepsilon_k}(\mathcal{Z}'_{k,\text{keep}}|E_k)_\rho \gtrapprox n_{k,0} + n_{k,1}[1 - h(e_{k,1})]. \tag{2}$$

Appendix A provides a brief analysis of the estimation of the parameters $n_{k,0}$, $n_{k,1}$, and $e_{k,1}$, and Appendix B briefly describes the steps involved to obtain Eq. (1).

Note that Eq. (2) is similar to Eq. (1) obtained in [12]. The next task is to bound the number of errors that Eve is likely to make when guessing Bob's key, given the bound on her smooth min-entropy. For this, we use Proposition 1 in [12] and follow the same argumentation.

Proposition 1. [12]. If Bob and Eve share the state ρ then, for any eavesdropping strategy, Eve's average probability of making at most r mistakes when guessing $\mathcal{Z}'_{k,\text{keep}}$ can be upper

bounded as

$$\langle p_r \rangle \leqslant \sum_{m=0}^{r} \binom{\frac{n_k}{2}}{m} 2^{-H_{\min}^{\varepsilon_k}(\mathcal{Z}'_{k,\mathrm{keep}}|E_k)_\rho} + \varepsilon_k. \tag{3}$$

The proof of this proposition follows the lines introduced in Appendix B of [12]. For large n_k, it can be shown from Markov's inequality that Eq. (3) implies

$$P(\text{Eve makes fewer than } r \text{ errors}) := p_r \leqslant g, \tag{4}$$

except with probability at most

$$p_F := \frac{1}{g}\left(2^{-\frac{n_k}{2}\{c_{k,0}+c_{k,1}[1-h(e_{k,1})]-h(2r/n_k)\}} + \varepsilon_k\right), \tag{5}$$

where $c_{k,i} := 2n_{k,i}/n_k$ is the lower bound on the count rate for the Z basis pulses containing i photons. Therefore, we arrive at the condition that determines whether or not Eve is able to make fewer than r errors with non-negligible probability, given as

$$c_{k,0} + c_{k,1}[1 - h(e_{k,1})] - h(2r/n_k) > 0. \tag{6}$$

If the condition holds, then n_k can be increased to make Eve's probability of making fewer than r errors arbitrarily small. We define p_E by the equation

$$c_{k,0} + c_{k,1}[1 - h(e_{k,1})] - h(p_E) = 0. \tag{7}$$

The meaning of this is that p_E is the minimum rate at which Eve can make errors for the code string associated with the Bell state k (except with negligible probability p_F). Suppose the error rate on the Z basis measurements between Alice and Bob is upper bounded as $\overline{E}_k$. As long as $p_E > \overline{E}_k$, there exists a choice of parameters and a sufficiently large signature length which makes the protocol secure. This means that MDI-QDS is possible as long as

$$c_{k,0} + c_{k,1}[1 - h(e_{k,1})] - h(\overline{E}_k) > 0. \tag{8}$$

IV. SECURITY ANALYSIS

We will now prove the security of the signature protocol, i.e., the robustness (probability of an honest run aborting), security against forging (probability that a recipient generates a signature, not originating from Alice, that is accepted as authentic), and repudiation (or transferability) (probability that Alice generates a signature that is accepted by Bob but then, when forwarded, is rejected by Charlie). In what follows we assume that Alice-Bob and Alice-Charlie have each used the MDI-KGP to generate bit strings of length $L = n_k$, to use in the QDS protocol described above.

(a) Robustness. Bob rejects a signed message if the $\frac{n_k}{2}$ bits received from either Alice or Charlie have a mismatch rate higher than s_a with Alice's signature. We note that Alice and Bob use a random sample, R_k bits from $Z_k^{a_s,b_s}$, to obtain the error rate $E_k^{a_s,b_s}$. This implies that the error rate $\overline{E}_k^{a_s,b_s}$ between the strings ($\mathcal{Z}_{k,\mathrm{keep}}$ and $\mathcal{Z}'_{k,\mathrm{keep}}$) generated using the Z basis satisfies the inequality [39]

$$\overline{E}_k^{a_s,b_s} \geqslant E_k^{a_s,b_s} + \mu\left(\frac{n_k}{2}, R_k, \varepsilon_{PE}\right), \tag{9}$$

where

$$\mu\left(\frac{n_k}{2}, R_k, \varepsilon_{PE}\right) = \sqrt{\frac{\left(\frac{n_k}{2} - R_k + 1\right)\ln\left(\frac{1}{\varepsilon_{PE}}\right)}{R_k n_k}}. \tag{10}$$

This means that the upper bound which we obtain from Eq. (9) on the error rate between Alice's and Bob's strings is true except with a very small probability ε_{PE}, and this probability can be fixed as small as desired. For any fixed value of the function μ, the failure probability decays exponentially fast in the parameter R_k. Then we set $\overline{E}_k := \max\{\overline{E}_{k,B}, \overline{E}_{k,C}\}$, where $\overline{E}_{k,B}$ and $\overline{E}_{k,C}$ refer to the upper bound obtained in Eq. (9) for the cases Alice-Bob and Alice-Charlie, and we choose s_a such that $s_a > \overline{E}_k$. We have that the probability that Bob will find an error rate higher than s_a is bounded by

$$P(\text{honest abort}) \leqslant 2\varepsilon_{PE}, \tag{11}$$

where the factor of 2 accounts for the fact that the abort can be due to either the states received from Alice or the states received from Charlie.

(b) Security against repudiation. Successful repudiation by Alice means, in the three-party scenario, that she makes Bob accept a declaration (m, Sig_m) that was sent to him by her, while Charlie rejects the same declaration when Bob forwards it to him (or similarly for a message forwarded from Charlie to Bob). Intuitively, security against repudiation follows because of the symmetrization performed by Bob and Charlie using the secret classical channel. Even if Alice knows and can control the error rates between A_m^B, A_m^C and K_m^B, K_m^C, she cannot control whether the errors end up with Bob or Charlie. After symmetrization the keys S_m^B and S_m^C will each have the same expected number of errors. To repudiate, one key must contain significantly more errors than the other. Using results from [12], we obtain

$$P(\text{repudiation}) \leqslant 2\,\exp\left[-\tfrac{1}{4}(s_v - s_a)^2 n_k\right]. \tag{12}$$

For a formal proof, please see Appendix C. Note that the probability of repudiation decays exponentially as the length n_k of the signature increases.

(c) Security against forging. It is easier for either Bob or Charlie to forge than it is for any other external party. Therefore, we will consider forging by an internal party. In order to forge a message, Bob must give a declaration (m, Sig_m) to Charlie that has fewer than $s_v n_k/2$ mismatches with the (to Bob) unknown half of S_m^C sent directly from Alice to Charlie, and also fewer than $s_v n_k/2$ mismatches with the half he himself forwarded to Charlie. An adversarial Bob will obviously be able to meet the threshold on the part he forwarded to Charlie. We therefore consider only the unknown half that Charlie received directly from Alice. We have that the maximum rate at which Alice will make errors with Charlie's key is given by $\overline{E}_k$. From Eq. (7), we also know the minimum rate at which Bob will make errors with the code string associated with the Bell state k of Charlie's key; we have denoted this by p_E. Assuming (8) holds, we choose s_v such that $\overline{E}_k < s_v < p_E$. In this case, Charlie will likely accept a legitimate signature sent by Alice, since the upper bound on their error rate, $\overline{E}_k$, is less than the threshold s_v. On the other hand, Charlie will likely reject any dishonest signature declaration by Bob, since the probability of Bob finding a signature with an error rate

smaller than s_v is restricted by (4) as

$$P(\text{Bob makes fewer than } s_v n_k/2 \text{ errors}) := p_r \leqslant g \quad (13)$$

except with probability at most p_F given by (5). If the estimation of the parameter $\overline{E}_k$ fails, which can happen with probability ε_{PE}, we will assume for simplicity that Bob is able to successfully forge with certainty. In a similar way as in [12], we are then able to bound Bob's probability of successfully forging as

$$P(\text{forge}) \leqslant p_F + g + \varepsilon_{PE} + \varepsilon_{k,0} + \varepsilon_{k,1} + \varepsilon_{k,e}. \quad (14)$$

This equation is valid for any choice of parameters $(g,\varepsilon_{PE},\varepsilon_{k,0},\varepsilon_{k,1},\varepsilon_{k,e})$ greater than zero. Thereby, Bob's probability to forge can be made arbitrarily small by increasing n_k. The addition of ε_{PE} accounts for the probability that the upper bound on $\overline{E}_k$ is incorrect and $\varepsilon_{k,0},\varepsilon_{k,1}$ and $\varepsilon_{k,e}$ are the error probabilities associated with the estimation of $n_{k,0}$, $n_{k,1}$, and $e_{k,1}$, respectively (see Appendix A).

V. COMPARISON TO MDI-QKD

According to [26], in MDI-QKD the length l_k of the secret bit string associated to the Bell state k is given by

$$l_k \leqslant n_{k,0} + n_{k,1}[1 - h(e_{k,1})] - \text{leak}_{EC,k} - \log_2 \frac{8}{\epsilon_{\text{cor}}} - 2\log_2 \frac{2}{\varepsilon'_k \hat{\varepsilon}_k} - 2\log_2 \frac{1}{2\varepsilon_{k,PA}}, \quad (15)$$

if the protocol is ϵ_{sec} secret, with $\epsilon_{\text{sec}} = \sum_k \epsilon_{k,\text{sec}}$ and $\epsilon_{k,\text{sec}} = 2(\varepsilon'_k + 2\varepsilon_{k,e} + \hat{\varepsilon}_k) + \varepsilon_{k,b} + \varepsilon_{k,0} + \varepsilon_{k,1} + \varepsilon_{k,PA}$. Here $\varepsilon_{k,PA}$ is the failure probability of privacy amplification, and the term $\text{leak}_{EC,k}$ is the information that is revealed by Alice in the error correction step. The meaning of the remaining epsilons can be found in [26]. The correctness of the protocol is guaranteed by the error correction step, and we say that the protocol is ϵ_{cor} correct if the probability that Alice's and Bob's bit strings are not identical is not greater than ϵ_{cor}. In the asymptotic limit of very large data blocks, one can neglect certain terms that reduce the secret key length and thereby Eq. (15) can be rewritten as

$$l_k \approx n_k\{c_{k,0} + c_{k,1}[1 - h(e_{k,1})]\} - \text{leak}_{EC,k}. \quad (16)$$

Here, $c_{k,i} := n_{k,i}/n_k$ increase the secret key rate, while $n_k c_{k,1} h(e_{k,1})$ and $\text{leak}_{EC,k}$ reduce it. These parameters depend on the sifted key length n_k [26]. $\text{leak}_{EC,k} = n_k \zeta h(\overline{E}_k^{a_s,b_s})$, where ζ is referred to as the leakage parameter, which depends on the value of n_k, and $h(.)$ denotes the binary Shannon entropy. ζ is assumed to be 1.16 in [26] but can generally be in the range 1.1–1.2, and when $n_k < 10^5$ the parameter ζ may be greater than 1.16. Therefore, for a sifted key length $\frac{n_k}{2}$, Eq. (16) can be written as

$$l_k \approx \frac{n_k}{2}\{c_{k,0} + c_{k,1}[1 - h(e_{k,1})] - \zeta h(\overline{E}_k)\}. \quad (17)$$

In a similar way as in [12], when we compare Eqs. (8) and (17), we find that there are Alice-Bob and Alice-Charlie quantum channels for which quantum signatures are possible and yet practical MDI-QKD is not, since the error threshold is less strict for the quantum channels used to perform the KGP in the signature protocol.

VI. DISCUSSION

In this section, we analyze the number of quantum transmissions necessary to sign a message with a security level of the order of 10^{-5} and 10^{-10}, respectively. If the security level of the protocol is of the order of, say, 10^{-5}, then this means that the probabilities of honest abort, forging, and repudiation are all less than 10^{-5}.

Using realistic experimental quantities, we estimate that a signature length of $n_k = 8.9 \times 10^6$ (for each of the possible single bit messages zero and 1) can be used to securely sign a single bit message, sent over a distance of 50 km. Essentially, it would require Bob or Charlie to transmit approximately $N_{\text{sig}} = 5.58 \times 10^{12}$ quantum states (per bit to be signed) to Alice during their KGPs (for full details, see Appendix D). With a source with a pulse rate of 1 GHz, we can calculate that it would take approximately 93 min to generate a raw key when the experiment uses standard single-photon detectors with detection efficiency (η_D) of 14.5%. This is for a security level of the order of 10^{-5}. By using detectors with higher detection efficiency we can improve the time of generating a raw key (t_r) since sending a smaller number of signals (N_{sig}) is then required to sign a single-bit message.

Table II shows the raw key generation times for various detectors that could be used in the protocol. We find that the most advanced superconducting nanowire single-photon detectors (SNSPDs) having 93% efficiency [42] would only require Bob or Charlie to send 6.4×10^{10} signals to perform the protocol with a secure threshold of the order of 10^{-5}. This would require just above a minute to generate the raw key. In order to improve the security threshold of the protocol (say 10^{-10}), Bob or Charlie would need to send a higher number of signals compared to the previous case. Table III shows the raw key generation times and the number of signals that are

TABLE II. Raw key generation times for various detectors that could be used in a MDI-QDS protocol for a distance of 50 km and a security threshold of 10^{-5}. The parameters $\eta_D(\%)$, Y_0, and N_{sig} denote respectively the detection efficiency, dark count rate of Eve's detectors, and the number of signals that Bob or Charlie sends to Alice during their KGPs. t_r is the time taken to generate the raw key and to estimate t_r we assume a source with a pulse rate of 1 GHz.

Detectors	η_D (%)	Y_0 ($\times 10^{-6}$)	N_{sig} ($\times 10^{12}$)	t_r (min)
Standard single-photon detectors [40]	14.5	6.02	5.58	93
InGaAs avalanche photodiodes detectors (APD) [32]	30	130	1.8	30
InGaAs/InP APD [41]	55	500	0.87	14.5
Superconducting nanowire single-photon detectors (SNSPDs) [42]	93	1	0.098	1.6

TABLE III. Raw key generation times for a distance of 50 km with a security threshold of 10^{-10}. For the definition of the different parameters, see the caption of Table II.

Detectors	$N_{\rm sig}$ ($\times 10^{12}$)	t_r (min)
Standard single-photon detectors [40]	10.5	175
InGaAs APD [32]	3.35	55.83
InGaAs/InP APD [41]	1.63	27.1
SNSPDs [42]	0.18	3

required to send for the protocol to be secure for a threshold of the order of 10^{-10}.

The protocol is secure to the order of 10^{-10} for a distance of 50 km, which in comparison is an improvement over the previous scheme [12] having a security threshold of 10^{-4}. The simulation results demonstrate that even with practical signals (for example, phase-randomized WCPs) and a finite size of data (say 10^{11} to 10^{14} signals) it is possible to perform secure MDI-QDS (with security threshold 10^{-10}) over long distances (up to about 150 km). Since the experimental platform for the implementation of MDI-QKD can also be used for MDI-QDS with slight modifications, in particular in the postprocessing of measurement results, we expect MDI-QDS could be widely used in practical QDS systems in the near future.

VII. CONCLUSION

In summary, we have presented a MDI-QDS protocol and proven it unconditionally secure against general attacks. It improves on previous quantum signature protocols by removing all detector side-channel attacks. This is essentially achieved by adapting the rigorous security proof of MDI-QKD given in [26], taking into account finite-size effects, to the QDS protocol proposed in [12] and we have presented that the resulting security proof is valid against general forging and repudiation attacks.

ACKNOWLEDGMENTS

The authors would like to thank Marco Lucamarini for discussions. This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) under Grant No. EP/M013472/1. R.A. acknowledges the support of the EPSRC CM-CDT under Grant No. EP/L015110/1. M.C. gratefully acknowledges support from the Galician Regional Government (program "Ayudas para proyectos de investigacion desarrollados por investigadores emergentes," Grant No. EM2014/033, and consolidation of Research Units: AtlantTIC), the Spanish Ministry of Economy and Competitiveness (MINECO), and the Fondo Europeo de Desarrollo Regional (FEDER) through Grant No. TEC2014-54898-R.

APPENDIX A: ESTIMATION OF RELEVANT PARAMETERS

In this Appendix we briefly discuss the estimation of the parameter $n_{k,0}$. This is a two-step process. First, we calculate a lower bound for the number of indices in $Z_k^{a_s,b_s}$ where Bob sent a vacuum state. This lower bound is denoted $m_{k,0}$. Second, we compute $n_{k,0}$ from $m_{k,0}$ using the Serfling inequality for random sampling without replacement [39]. The other parameters, $n_{k,1}$ and $e_{k,1}$, are also estimated using a similar approach. A detailed explanation is provided in the supplementary notes of [26].

We assume that Alice and Bob use two decoy states each and the photon-number distribution of their signals is Poissonian. That is, $a \in A = \{a_s, a_{d_1}, a_{d_2}\}$, with $a_s > a_{d_1} > a_{d_2}$, $b \in B = \{b_s, b_{d_1}, b_{d_2}\}$, with $b_s > b_{d_1} > b_{d_2}$, and the probability that Alice (Bob) sends an n-photon (m-photon) signal when she (he) selects the intensity a (b) is given by $p_{n|a} = e^{-a}a^n/n!$ ($p_{m|b} = e^{-b}b^m/m!$).

Let $S_{k,nm}$ denote the number of signals sent by Alice and Bob with n and m photons, respectively, when they select the basis Z and Eve declares the Bell state k. Now, for each combination of values n and m, the signal and decoy states provide a random sample of the population of all signals containing n and m photons, respectively. Therefore, one can apply the standard large deviation theory technique, in particular a multiplicative form of the Chernoff bound [26]. Then, if

$$\left(2\varepsilon_{a,b}^{-1}\right)^{1/\mu_{k,L}^{a,b}} \leqslant \exp[3/(4\sqrt{2})]^2],$$

and

$$\left(\hat{\varepsilon}_{a,b}^{-1}\right)^{1/\mu_{k,L}^{a,b}} \leqslant \exp(1/3),$$

with the parameter $\mu_{k,L}^{a,b}$ given by

$$\mu_{k,L}^{a,b} = \left|Z_k^{a,b}\right| - \sqrt{\sum_{a,b} |Z_k^{a,b}|/2\ln(1/\epsilon_{a,b})}, \tag{A1}$$

this implies that

$$\left|Z_k^{a,b}\right| = \sum_{n,m} p_{a,b|nm,Z} S_{k,nm} + \delta_{a,b}, \tag{A2}$$

except with error probability $\gamma_{a,b} = \epsilon_{a,b} + \varepsilon_{a,b} + \hat{\varepsilon}_{a,b}$. Here, $p_{a,b|nm,Z}$ refers to the conditional probability that Alice and Bob have selected the intensity settings a and b, respectively, given that their signals contain n and m photons, respectively, prepared in the Z basis. The parameter $\delta_{a,b} \in [-\Delta_{a,b}, \hat{\Delta}_{a,b}]$ with $\Delta_{a,b} = g(|Z_k^{a,b}|, \varepsilon_{a,b}^4/16)$ and $\hat{\Delta}_{a,b} = g(|Z_k^{a,b}|, \hat{\varepsilon}_{a,b}^{3/2})$, and the function $g(x,y) = \sqrt{2x\ \ln(y^{-1})}$.

By using similar arguments, the quantity $m_{k,0}$ can be written as

$$m_{k,0} = \sum_n p_{a_s,b_s|n0,Z} S_{k,n0} - \Delta_0, \tag{A3}$$

except with error probability ε_0, where $\Delta_0 = g(\sum_n p_{a_s,b_s|n0,Z} S_{k,n0}, \varepsilon_0)$. To obtain a lower bound for $m_{k,0}$, one can minimize Eq. (A3) given the linear constraints imposed by Eq. (A2) $\forall a,b$. This is solved both analytically and numerically in the supplementary notes of [26]. Then using Serfling inequality [39], we find

$$n_{k,0} = \max\left\{\left\lfloor \frac{n_k}{2}\frac{m_{k,0}}{\left|Z_k^{a_s,b_s}\right|} - \frac{n_k}{2}\Lambda\left(\left|Z_k^{a_s,b_s}\right|, \frac{n_k}{2}, \varepsilon''_{k,0}\right)\right\rfloor, 0\right\}, \tag{A4}$$

except with error probability

$$\varepsilon_{k,0} \leqslant \varepsilon'_{k,0} + \varepsilon''_{k,0}, \tag{A5}$$

where $\varepsilon'_{k,0} \leqslant \varepsilon_0 + \sum_{a,b} \gamma_{a,b}$ corresponds to the total error probability in the estimation of $m_{k,0}$ and the function $\Lambda(x,y,z)$ is defined as $\Lambda(x,y,z) = \sqrt{(x-y+1)\ln(z^{-1})/(2xy)}$.

A similar approach is followed to estimate $n_{k,1}$ and $e_{k,1}$ with associated error probabilities $\varepsilon_{k,1}$ and $\varepsilon_{k,e}$, respectively. We obtain

$$n_{k,1} = \max\left\{\left\lfloor \frac{n_k}{2}\frac{m_{k,1}}{\left|Z_k^{a_s,b_s}\right|} - \frac{n_k}{2}\Lambda\left(\left|Z_k^{a_s,b_s}\right|, \frac{n_k}{2}, \varepsilon''_{k,1}\right)\right\rfloor, 0\right\}, \tag{A6}$$

except with error probability

$$\varepsilon_{k,1} \leqslant \varepsilon'_{k,1} + \varepsilon''_{k,1}, \tag{A7}$$

where $\varepsilon'_{k,1} \leqslant \varepsilon_1 + \sum_{a,b} \gamma_{a,b}$. Here, $m_{k,1} = p_{a_s,b_s|11,Z} S_{k,11} - \Delta_1$, except with error probability ε_1 where the parameter $\Delta_1 = g(p_{a_s,b_s|11,Z} S_{k,11}, \varepsilon_1)$. Finally, the parameter $e_{k,1}$ is given as

$$e_{k,1} = \min\left\{\left\lceil n_{k,1}\left(\frac{\overline{e}_{k,1}}{\overline{n}_{k,1}}\right) + (n_{k,1}+\overline{n}_{k,1}) \times \Upsilon(n_{k,1}, \overline{n}_{k,1}, \varepsilon'''_{k,e})\right\rceil, n_{k,1}\right\}, \tag{A8}$$

except with error probability

$$\varepsilon_{k,e} \leqslant \varepsilon'_{k,e} + \varepsilon''_{k,e} + \varepsilon'''_{k,e}, \tag{A9}$$

where the function $\Upsilon(x,y,z)$ is defined as $\Upsilon(x,y,z) = \sqrt{(x+1)\ln(z^{-1})/[2y(x+y)]}$. The quantity $\overline{n}_{k,1}$ is a lower bound for the number of signals where Alice and Bob send a single-photon state prepared in the X basis and where Eve declares the Bell state k, $\overline{e}_{k,1}$ is an upper bound for the total number of errors in these signals, and $\varepsilon'_{k,e}$ and $\varepsilon''_{k,e}$ represent, respectively, their associated error probabilities. For more details about how to calculate these parameters, please see [26].

We have, therefore, that the error probability associated with the estimation of the different parameters is given by $\varepsilon_{PE} + \varepsilon_{k,0} + \varepsilon_{k,1} + \varepsilon_{k,e}$, with ε_{PE} given by Eq. (9).

APPENDIX B: EVE'S SMOOTH-MIN ENTROPY

The goal of this Appendix is to derive Eq. (B2). The analysis follows the procedure introduced in [26]. For this, let $H_{\min}^{\varepsilon_k}(\mathcal{Z}'_{k,\text{keep}}|E_k)$ denote the smooth min-entropy which quantifies the average probability that the adversary guesses $\mathcal{Z}'_{k,\text{keep}}$ correctly using the optimal strategy with access to E_k. Now the bits of $\mathcal{Z}'_{k,\text{keep}}$ can be distributed among three different strings, $\mathcal{Z}'^0_{k,\text{keep}}$, $\mathcal{Z}'^1_{k,\text{keep}}$, and $\mathcal{Z}'^{\text{rest}}_{k,\text{keep}}$. The first string contains bits where Bob sent a vacuum state, the second where Alice and Bob sent a single-photon state, and $\mathcal{Z}'^{\text{rest}}_{k,\text{keep}}$ contains the rest of the bits. Using the result of chain rule of entropies [43], we obtain

$$\begin{aligned} &H_{\min}^{\varepsilon_k}(\mathcal{Z}'_{k,\text{keep}}|E_k) \\ &\geqslant H_{\min}^{\epsilon'_k+2\epsilon''_k+(\hat{\epsilon}_k+2\hat{\epsilon}'_k+\hat{\epsilon}''_k)}\left(\mathcal{Z}'^0_{k,\text{keep}}\mathcal{Z}'^1_{k,\text{keep}}\mathcal{Z}'^{\text{rest}}_{k,\text{keep}}\middle|E_k\right) \\ &\geqslant n_{k,0} + H_{\min}^{\epsilon''_k}\left(\mathcal{Z}'^1_{k,\text{keep}}\middle|\mathcal{Z}'^0_{k,\text{keep}}\mathcal{Z}'^{\text{rest}}_{k,\text{keep}}E_k\right) - 2\log_2\frac{2}{\epsilon'_k\hat{\epsilon}_k}, \end{aligned} \tag{B1}$$

where $\varepsilon_k = \epsilon'_k + 2\epsilon''_k + (\hat{\epsilon}_k + 2\hat{\epsilon}'_k + \hat{\epsilon}''_k)$. Here, it is taken into consideration that $H_{\min}^{\hat{\epsilon}'_k}(\mathcal{Z}'^{\text{rest}}_{k,\text{keep}}|\mathcal{Z}'^0_{k,\text{keep}}E_k) \geqslant 0$, and $H_{\min}^{\hat{\epsilon}''_k}(\mathcal{Z}'^0_{k,\text{keep}}|E_k) \geqslant H_{\min}^0(\mathcal{Z}'^0_{k,\text{keep}}|E_k) = H_{\min}(\mathcal{Z}'^0_{k,\text{keep}}) = n_{k,0}$. The final part arises as the vacuum states contain no information about their bit values, which are uniformly distributed. In order to get the lower bound for the term $H_{\min}^{\epsilon''_k}(\mathcal{Z}'^1_{k,\text{keep}}|\mathcal{Z}'^0_{k,\text{keep}}\mathcal{Z}'^{\text{rest}}_{k,\text{keep}}E_k)$, it is considered that Alice and Bob prepare perfect BB84 states. Then, this quantity can be written in terms of the smooth max-entropy between them, which is directly bounded by the strength of the correlations [44]. From the entropy uncertainty relation [36], we obtain

$$\begin{aligned} H_{\min}^{\epsilon''_k}\left(\mathcal{Z}'^1_{k,\text{keep}}\middle|\mathcal{Z}'^0_{k,\text{keep}}\mathcal{Z}'^{\text{rest}}_{k,\text{keep}}E_k\right) &\geqslant n_{k,1} - H_{\max}^{\epsilon''_k}\left(\mathcal{X}'^1_k\middle|\mathcal{X}'^1_k\right) \\ &\geqslant n_{k,1} - n_{k,1}h(e_{k,1}). \end{aligned}$$

Using the above equation in Eq. (B1), we get

$$H_{\min}^{\varepsilon_k}(\mathcal{Z}'_{k,\text{keep}}|E_k) \geqslant n_{k,0} + n_{k,1}[1-h(e_{k,1})] - 2\log_2\frac{2}{\epsilon'_k\hat{\epsilon}_k}. \tag{B2}$$

We are interested in a regime where the first two terms on the RHS of Eq. (B2) are much larger than the $\log_2$ term, as ε'_k and $\hat{\varepsilon}_k$ are typically of the order say 10^{-5}–10^{-10}. Therefore, if we neglect this $\log_2$ term, we obtain Eq. (2) of the main paper,

$$H_{\min}^{\varepsilon_k}(\mathcal{Z}'_{k,\text{keep}}|E_k) \gtrapprox n_{k,0} + n_{k,1}[1-h(e_{k,1})]. \tag{B3}$$

APPENDIX C: SECURITY AGAINST REPUDIATION

We follow the approach in [10]. If Alice tries to repudiate a message, she sends a declaration (m, Sig_m) which Bob will accept and Charlie will reject. For this to happen, Bob must accept both the elements that Alice sent directly to him, and the elements that Charlie forwarded to him. In order for Charlie to reject he needs only to reject either the elements he received from Alice, or the elements Bob forwarded to him (or both). Intuitively, security against repudiation follows because of the symmetrization performed by Bob and Charlie using the secret classical channel. In the distribution stage, to send the future message m, Alice uses the MDI-KGP with Bob and Charlie to generate strings of length $n_k = L$. Suppose that Bob holds the string $(b_1,\ldots,b_L)$ and Charlie holds the string $(c_1,\ldots,c_L)$. Now, for simplicity, we consider that Alice has full power and we assume that later on, in the messaging stage, she is able to fully control the number of mismatches her signature declaration contains with $(b_1,\ldots,b_L)$ and $(c_1,\ldots,c_L)$. Let us denote the mismatch rates by e_B and e_C, respectively. Then, the symmetrization process means that Bob and Charlie will randomly (and unknown to Alice) receive $L/2$ elements of the other's string. We aim to show that any choice of e_C and e_B leads to an exponentially decaying probability of repudiation. Then we have the two following cases as in [10].

Case 1. First, let us assume that $e_C > s_a$. In this case, Bob receives $L/2$ elements from the set $\{c_1,\ldots,c_L\}$, which contains exactly $e_C L$ mismatches with Alice's future declaration. In order to accept the message, Bob must get fewer than $s_a L/2$ errors. Using [45] we can bound the probability that Bob gets

fewer than $s_a L/2$ mismatches as

$$P(\text{Bob gets less than } s_a L/2 \text{ mismatches from Charlie}) \leqslant \exp[-(e_C - s_a)^2 L]. \quad \text{(C1)}$$

To repudiate, Alice must make Bob accept the message, which means that Bob must accept both the part received from Alice and the part received from Charlie. Since $P(A \cap B) \leqslant \min\{P(A), P(B)\}$ the probability of repudiation must be less than or equal to the above expression, and so must also decrease exponentially.

Case 2. Suppose $e_C \leqslant s_a$. In this case, if $e_B > s_a$, the above argument shows that it is highly likely that Bob will reject the message, so we examine only the case where $e_B \leqslant s_a$. Consider first the set $\{b_1, \ldots, b_L\}$. We can use the same arguments as above to bound the probability of selecting more than $s_v L/2$ mismatches as

$$P(\text{Charlie gets more than } s_v L/2 \text{ mismatches from Bob}) \leqslant \exp[-(s_v - e_B)^2 L]. \quad \text{(C2)}$$

Then, Alice succeeds if Charlie finds more than $s_v L/2$ mismatches either from the set $\{b_1, \ldots, b_L\}$ or the set $\{c_1, \ldots, c_L\}$. Using $P(A \cup B) \leqslant P(A) + P(B)$, we can see that, for the choice of $e_B, e_C \leqslant s_a$, we have

$$P(\text{Charlie gets more than } s_v L/2 \text{ mismatches}) \leqslant 2 \exp[-(s_v - s_a)^2 L]. \quad \text{(C3)}$$

So again, the probability of Alice successfully repudiating decreases exponentially in the size of the signature, and Alice's best strategy would be to pick $e_B = e_C = \frac{1}{2}(s_v + s_a)$, in which case

$$P(\text{repudiation}) \leqslant 2 \exp\left[-\tfrac{1}{4}(s_v - s_a)^2 L\right]. \quad \text{(C4)}$$

APPENDIX D: CALCULATION OF THE NUMBER OF QUANTUM TRANSMISSIONS REQUIRED PER SIGNED BIT

1. Parameters and constraints

Similar to [12], the correctness and security of the protocol depends on the three equations (11), (12), and (14), which in turn depend on the choice of parameters s_a and s_v. The parameters are considered such that $\overline{E}_k < s_a < s_v < p_E$. We say that $\overline{E}_k$ is the maximum of the worst-case error rates that Alice makes with Bob's key (found from the Alice-Bob MDI-KGP), and the worst-case error rates Alice makes with Charlie's key (found from the Alice-Charlie MDI-KGP). Similarly, p_E is the minimum of the adversary's error rates found from the Alice-Bob and Alice-Charlie MDI-KGP. We follow [12] to choose the parameters that minimize the number of quantum transmissions required per signed bit. This will be larger than the signature length, L, due to factors such as channel loss, detection efficiency, and parameter estimation procedures. Because of this, Bob will have to transmit more than L quantum states to generate a signature of length L.

In the next section, we will calculate the length of the signature and the number of quantum transmissions necessary to sign a message with a security level of 10^{-5}. This means that the probabilities of honest abort, forging, and repudiation, given respectively by (11), (14), and (12), are all less than 10^{-5}. To find the length per possible one-bit message, of the signature necessary to securely sign a one-bit message, we must first choose the parameters s_a and s_v. That is, a signature sequence of length L needs to be transmitted for the possible message "0," and for the possible message "1," so that the total signature sequence has length $2L$. Ideally, our choice would minimize L. We choose to set $\varepsilon_{PE} = 10^{-5}$ and

$$s_a = \overline{E}_k + \frac{p_E - \overline{E}_k}{3}, \quad s_v = \overline{E}_k + \frac{2(p_E - \overline{E}_k)}{3}. \quad \text{(D1)}$$

These may not be the optimal choices of these parameters. However, a natural choice would be to choose the parameters in order to equally partition the gap between $\overline{E}_k$ and p_E.

2. Number of quantum transmissions required per signed bit

In this section, we use experimental data provided by [40] to give an optimal estimate of the number of states Bob needs to transmit over a 50 km quantum channel to securely sign a one bit message. We set $\epsilon_{PE} = 10^{-5}$ in all equations that follow. The experiment in [40] considers a free-space channel; we assume a fiber-based channel with a loss coefficient of 0.2 dB/km. Here, we consider standard single-photon detectors where the detection efficiency of the relay is 14.5% and the background rate is 6.02×10^{-6}. The overall misalignment in the channel is assumed to be 1% and the bound is fixed to be $\varepsilon_k = 10^{-10}$. The other parameters involved are as follows.

(i) Source: 1 GHz pulse rate.
(ii) Basis probabilities: $p_Z = 62.5\%$; $p_X = 37.5\%$.
(iii) Intensity levels: $(s, d_1, d_2) = (0.18, 0.09, 5 \times 10^{-4})$.
(iv) Intensity probabilities: $p_s = 50\%$; $p_{d1} = p_{d2} = 25\%$.

We consider the total number of signals sent by Bob to be 5.58×10^{12}, and find the raw key to contain 9.42×10^6 bit values from Z basis measurement outcomes. Assuming that 5.5% of the detected signals are used for error rate estimation ($R_k = 5.18 \times 10^5$), we obtain a signature length of $n_k = 8.9 \times 10^6$. Of these, Bob will randomly choose $n_k/2 = 4.45 \times 10^6$ to be $\mathcal{Z}'_{k,\text{keep}}$; another $n_k/2$ will be used as $\mathcal{Z}'_{k,\text{forward}}$.

For the given intensity levels and intensity choice probabilities, we observe an error rate in the Z basis given by $E_k^{a_s,b_s} = 2.07\%$. This error rate arises from the channel misalignment together with the dark-count rate of the detectors. We can then use Eq. (9) to upper bound the true error rate as $\overline{E}_k^{a_s,b_s} = 2.39\%$.

We use Appendix A to estimate the relevant parameters by setting all ε as 10^{-10}, and thereby we can calculate the min-entropy. Finally, setting $\varepsilon_k = 10^{-10}$, we get

$$H_{\min}^{\varepsilon_k}(\mathcal{Z}'_{k,\text{keep}}|E_k) = 8.69 \times 10^5. \quad \text{(D2)}$$

Then using (7) we find p_E as 3.02%, and so we obtain $s_a = 2.60\%$ and $s_v = 2.81\%$. Setting g as 10^{-5} and substituting these values into Eqs. (11), (14), and (12), we find $P(\text{honest abort}) = 2.00 \times 10^{-5}$, $P(\text{forge}) = 3 \times 10^{-5}$, and $P(\text{repudiation}) = 9.857 \times 10^{-5}$. Thus we observe that when 5.58×10^{12} states are transmitted, the protocol is secure to a level of the order of 10^{-5} for a distance of 50 km. The analysis for the other cases shown in Tables II and III is done in a similar way.

[1] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM **21**, 120 (1978).

[2] C. M. Swanson and D. R. Stinson, Unconditionally secure signature schemes revisited, *Information Theoretic Security, Proceedings of ICITS 2011, LNCS, Amsterdam* (Springer, Berlin Heidelberg, 2011), Vol. 6673, pp. 100–116.

[3] R. Amiri and E. Andersson, Unconditionally secure quantum signatures, Entropy **17**, 5635 (2015).

[4] D. Gottesman and I. Chuang, Quantum Digital Signatures, arXiv:quant-ph/0105032.

[5] E. Andersson, M. Curty, and I. Jex, Experimentally realizable quantum comparison of coherent states and its applications, Phys. Rev. A **74**, 022304 (2006).

[6] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light, Nat. Commun. **3**, 1174 (2012).

[7] V. Dunjko, P. Wallden, and E. Andersson, Quantum Digital Signatures Without Quantum Memory, Phys. Rev. Lett. **112**, 040502 (2014).

[8] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Realization of Quantum Digital Signatures Without the Requirement of Quantum Memory, Phys. Rev. Lett. **113**, 040502 (2014).

[9] L. Lamport, *Constructing Digital Signatures From a One-way Function* (SRI International Computer Science Laboratory, California, USA, 1979).

[10] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Quantum digital signatures with quantum-key-distribution components, Phys. Rev. A **91**, 042304 (2015).

[11] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[12] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Secure quantum signatures using insecure quantum channels, Phys. Rev. A **93**, 032325 (2016).

[13] H.-L. Yin, Y. Fu, and C. Zeng-Bing, Practical quantum digital signature, Phys. Rev. A **93**, 032316 (2016).

[14] B. Qi, H.-K. Lo, and X. Ma, Time-shift attack in practical quantum cryptosystems, Quantum Inf. Comput. **7**, 73 (2007).

[15] A. Lamas-Linares and C. Kurtsiefer, Breaking a quantum key distribution system through a timing side channel, Opt. Express **15**, 9388 (2007).

[16] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Phys. Rev. A **78**, 042333 (2008).

[17] F. Xu, B. Qi, and H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, New J. Phys. **12**, 113026 (2010).

[18] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. **4**, 686 (2010).

[19] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors, New J. Phys. **13**, 073024 (2011).

[20] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Full-field implementation of a perfect eavesdropper on a quantum cryptography system, Nat. Commun. **2**, 349 (2011).

[21] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution, Phys. Rev. A **87**, 062313 (2013).

[22] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[23] 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, Phys. Rev. A **85**, 042307 (2012).

[24] X. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).

[25] F. Xu, M. Curty, B. Qi, and H.-K. Lo, Practical aspects of measurement-device-independent quantum key distribution, New J. Phys. **15**, 113007 (2013).

[26] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[27] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, Phys. Rev. Lett. **111**, 130501 (2013).

[28] T. Ferreira da Silva, D. Vitoreti, 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 **88**, 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, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang and J.-W. Pan, Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **111**, 130502 (2013).

[30] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **112**, 190503 (2014).

[31] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, D.-X. Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T.-Y. Chen, Q. Zhang, and J.-W. Pan, Measurement-Device-Independent Quantum Key Distribution Over 200 km, Phys. Rev. Lett. **113**, 190501 (2014).

[32] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W.-B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields, Quantum cryptography without detector vulnerabilities using optically-seeded lasers, Nat. Photon. **10**, 312 (2016).

[33] J. M. Arrazola, P. Wallden, and E. Andersson, Multiparty quantum signature schemes, Quantum Inf. Comput. **6**, 0435 (2016).

[34] F. Xu, M. Curty, B. Qi, and H.-K. Lo, Measurement-device-independent quantum cryptography, IEEE J. Sel. Top. Quantum Electron. **21**, 6601111 (2015).

[35] If we exceed the limits of $M_k^{a,b}$ and $N_k^{a,b}$, we then select at random $M_k^{a,b}$ and $N_k^{a,b}$ elements for the analysis.

[36] M. Tomamichel and R. Renner, Uncertainty Relation for Smooth Entropies, Phys. Rev. Lett. **106**, 110506 (2011).

[37] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[38] M. Tomamichel and A. Leverrier, A rigorous and complete proof of finite key security of quantum key distribution, arXiv:1506.08458.

[39] R. J. Serfling, Probability inequalities for the sum in sampling without replacement, Ann. Statist. **2**, 39 (1974).

[40] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, Entanglement-based quantum communication over 144 km, Nat. Phys. **3**, 481 (2007).

[41] L. C. Comandar, B. Fröhlich, J. F. Dynes, A. W. Sharpe, M. Lucamarini, Z. L. Yuan, R. V. Penty, and A. J. Shields, Gigahertz-gated InGaAs/InP single-photon detector with detection efficiency exceeding 55% at 1550 mm, J. Appl. Phys. **117**, 083109 (2015).

[42] F. Marsili, B. V. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam, Detecting single infrared photons with 93% system efficiency, Nat. Photon. **7**, 210 (2013).

[43] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, Chain rules for smooth min- and max-entropies, IEEE Trans. Inf. Theory **59**, 2603 (2013).

[44] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[45] W. Hoeffding, Probability inequalities for sums of bounded random variables, J. Am. Stat. Assoc. **58**, 13 (1963).