Experimental measurement-device-independent quantum digital signatures over a metropolitan network

Hua-Lei Yin,[1,2] Wei-Long Wang,[3] Yan-Lin Tang,[1,2] Qi Zhao,[4] Hui Liu,[1,2] Xiang-Xiang Sun,[1,2] Wei-Jun Zhang,[5] Hao Li,[5] Ittoop Vergheese Puthoor,[6] Li-Xing You,[5] Erika Andersson,[6] Zhen Wang,[5] Yang Liu,[1,2] Xiao Jiang,[1,2] Xiongfeng Ma,[2,4] Qiang Zhang,[1,2] Marcos Curty,[3] Teng-Yun Chen,[1,2] and Jian-Wei Pan[1,2]

[1]*Hefei National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[2]*CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China*

[3]*Department of Signal Theory and Communications, Escola de Enxeñaría de Telecomunicación, University of Vigo, Vigo 36310, Spain*

[4]*Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, China*

[5]*State Key Laboratory of Functional Materials for Informatics, Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Shanghai 200050, China*

[6]*Institute of Photonics and Quantum Sciences, Heriot-Watt University, SUPA, Edinburgh EH14 4AS, United Kingdom*

(Received 3 March 2017; published 25 April 2017)

Quantum digital signatures (QDSs) provide a means for signing electronic communications with information-theoretic security. However, all previous demonstrations of quantum digital signatures assume trusted measurement devices. This renders them vulnerable against detector side-channel attacks, just like quantum key distribution. Here we exploit a measurement-device-independent (MDI) quantum network, over a metropolitan area, to perform a field test of a three-party MDI QDS scheme that is secure against any detector side-channel attack. In so doing, we are able to successfully sign a binary message with a security level of about 10^{-7}. Remarkably, our work demonstrates the feasibility of MDI QDSs for practical applications.

DOI: 10.1103/PhysRevA.95.042338

Digital signatures are cryptographic schemes that are widely used to guarantee both the authenticity and the transferability of digital messages and documents. They play an essential role in many applications such as software distribution, financial transactions, and emails. However, the security of currently used public-key digital signature schemes relies on computational assumptions, such as the difficulty of factorizing large numbers [1] or finding discrete logarithms [2]. Thus, advances in the development of efficient algorithms or a quantum computer can threaten their security.

Quantum digital signatures (QDSs) [3], on the other hand, can offer information-theoretic security based on quantum mechanics, given that the participants preshare some secret keys for authentication purposes. That is, they guarantee no forging (i.e., the message is signed by a legitimate sender and it has not been modified) and nonrepudiation (i.e., the sender cannot successfully deny the signature of the message) despite any future computational advance. This justifies the great attention that this topic has received recently. Indeed, QDS schemes based on coherent states [4,5] and schemes that do not need the use of quantum memories [6,7] have been proposed and experimentally demonstrated. Also, QDS protocols implementable with only quantum key distribution (QKD) components have been designed [8] and experimentally tested [9]. Remarkably, the need for trust on the quantum channels has also been removed [10,11]. All these efforts have paved the way for the development of more practical QDS schemes [12–14].

Despite this tremendous progress, however, in practice it is still very challenging to guarantee the security of the implementations. This is so because, just as for QKD, also here there is a big gap between practical realizations and the theoretical models that are assumed in the security proofs. As a result, we face security loopholes, or so-called side channels, that could seriously threaten the security of QDS schemes. Indeed, detector side-channel attacks [15–17] are arguably the most important threat. Very recently, motivated by the concept of measurement-device-independent (MDI) QKD [18], Puthoor *et al.* [19] introduced a MDI QDS scheme that is secure against all detector side-channel attacks.

Here we report an experimental demonstration of a three-party MDI QDS protocol that is immune to detector side-channel attacks and allows the signature of binary messages with a security level of 10^{-7}. This implementation makes use of a MDI quantum network with a star topology that is deployed over a metropolitan field. Our work demonstrates the feasibility of MDI QDS schemes for practical applications.

In the MDI QDS protocol of [19] there are at least three parties. One party (say, for instance, Alice) acts as a signer, while the other two parties (say Bob and Charlie) act as recipients. All parties are pairwise connected via authenticated classical channels. Also, they are connected to a relay (Eve) via quantum channels. The quantum channels between Bob and Eve, and Charlie and Eve, can be used to generate a secret key between Bob and Charlie by means of MDI QKD. This secret key allows them to interchange messages in full secrecy by means of one-time pad encryption.

The MDI QDS protocol consists of two stages: the distribution stage and the messaging stage. Quantum communication is needed only in the former, where Alice uses a so-called MDI key generation protocol (KGP) to generate correlated L-bit strings A_0^B, A_1^B and A_0^C, A_1^C with Bob and Charlie, respectively. The corresponding strings held by Bob (Charlie) are denoted by K_m^B (K_m^B), with $m = 0,1$. Note that the strings A_m^B (A_m^C) and K_m^B (K_m^C) do not need to be identical, but they just need to be sufficiently correlated. The quantum stage of the MDI KGP is

equal to that of MDI QKD, but its classical data postprocessing stage is different because in the MDI KGP there is no need to apply error correction and privacy amplification. After the MDI KGP, Bob and Charlie symmetrize their strings. For this, say Bob randomly chooses half of the bits of each of K_m^B and sends them (as well as the information of the positions of the bits chosen) to Charlie using a secure channel. Similarly, Charlie does the same with K_m^C. We denote Bob's (Charlie's) bit strings after the symmetrization step by S_m^B (S_m^C).

Finally, in the messaging stage, which typically occurs much later and where only classical communication takes place, Alice can sign a binary message m by simply sending $(m,\mathcal{S}_m)$ to the desired recipient (say Bob), where the signature $\mathcal{S}_m = (A_m^B, A_m^C)$. To verify that m indeed comes from Alice, Bob checks whether $\mathcal{S}_m$ matches his bit string S_m^B. For this, he checks separately the part of S_m^B received directly from Alice and that received from Charlie and he records the number of mismatches in each part. If the number of mismatches in both parts is below $s_a(L/2)$, where s_a is a pre-fixed threshold value satisfying $0 < s_a < 1/2$, then Bob accepts the message as authentic. Otherwise, he rejects it. If Bob wants to demonstrate to Charlie that Alice signed m, he sends him $(m,\mathcal{S}_m)$. Then Charlie performs a similar check to that done by Bob and only accepts m if the number of mismatches in both halves of S_m^C is below $s_v(L/2)$, with $0 < s_a < s_v < 1/2$. In so doing, the MDI QDS protocol is secure against general forging and repudiation attacks [19].

In order to experimentally demonstrate this MDI QDS scheme we use the MDI quantum network that has been deployed in the city of Hefei, China. This metropolitan network has been recently used to successfully demonstrate MDI QKD [20]. As shown in Fig. 1(a), Alice, Bob, and Charlie are connected to Eve, with a 25.3-, 17.2-, and 30.3-km deployed single-mode optical fiber, which has a propagation loss of 9.2, 5.1, and 8.1 dB, respectively. In collaboration with Eve, Alice and Bob (Charlie) exploit the *A-E-B* (*A-E-C*) insecure quantum link to implement the MDI KGP. Also, Bob and Charlie use the *B-E-C* insecure quantum link to implement the MDI QKD protocol. For this, Eve's Bell state measurement (BSM) device is shared between Alice, Bob, and Charlie. This is done by using an 8×4 mechanical optical switch (MOS) as a router, allowing us to perform three quantum protocols successively.

Since the quantum stage of the MDI KGP is identical to that of MDI QKD, identical state preparation setups are installed for the three participants, Alice, Bob, and Charlie, who communicate with each other through classical channels and exchange quantum signals with Eve by means of quantum channels. This is illustrated in Figs. 1(b) and 1(c). At each site, phase-randomized signal pulses at a repetition rate of 75 MHz are generated with an internally modulated distributed feedback laser. The wavelength of each signal pulse is 1550.12 nm and its pulse width is 2.5 ns. The intensities of the signal state, the decoy state, and the vacuum state are $\mu = 0.33$, $\nu = 0.1$, and $w = 0$, respectively. The corresponding probability distributions are set as 25.6%, 58.4%, and 16%, respectively. A time-bin phase-encoding scheme [24] is used to prepare Bennett-Brassard states [25], where the delay between two time bins is 6.37 ns. The signal (decoy) states are all prepared using the Z basis (the Z or the X basis with probability distribution 36.9% and 63.1%, respectively). In the case of the vacuum states w, it is not necessary to distinguish between the two bases. After applying a filter and a single-photon level modulation, each optical pulse is sent to Eve through the deployed fiber. A successful BSM result corresponds to coincidence counts in opposite time bins, which indicates a projection onto the singlet Bell state $|\Psi^-\rangle$. This means that the data shared between the participants are anticorrelated and one of them has to flip the bits to match those of the other participant. In the BSM, the efficiency of the time window for a single time bin is about 90%. The two superconducting nanowire single-photon detectors (SNSPDs) of the BSM work at 2.05 K and have detection efficiencies of 66% and 64%, respectively, as well as a dark count rate of 30 Hz. Also, the spurious noise of the deployed fiber brings dozens of extra dark counts per second. The inner insertion loss of Eve's system is 6.2 dB for the *A-E-B* link, 6.2 dB for the *A-E-C* link, and 7 dB for the *B-E-C* link, respectively. This insertion loss includes the loss contribution from the MOS, the dense wavelength division multiplexor, the electric polarization controller (EPC), the polarization beam splitter (PBS), the beam splitter (BS), and the optical fiber connection.

To achieve high-visibility two-photon interference in the BSM, the incoming photons have to be indistinguishable. For this, Eve uses three independent lasers at a wavelength of 1570 nm that generate 500-KHz signals to synchronize the entire system. Also, a programmable delay chip with 10-ps timing resolution is used to guarantee a precise overlap of the two interfering pulses [26]. The optical signal of the shared phase feedback laser with a wavelength of 1550.12 nm is divided into three beams by a BS. Each beam is sent to Alice, Bob, and Charlie, respectively. The phase reference frame is stabilized by using a phase shifter and two power meters [20]. The synchronization signal and the phase feedback signal are multiplexed in an additional deployed fiber. The polarization reference frame is stabilized by using an EPC, a PBS, a SNSPD, and a fast axis blocked polarization maintaining the BS. Also, we use the Hong-Ou-Mandel dip to calibrate the wavelength difference between the two interfering pulses [20].

We have run the MDI KGP between the participants for 73 423 (149 987) s to accumulate data for the pair of Alice and Bob (Alice and Charlie). Also, we accumulated data for 81 630 s during the MDI QKD session between Bob and Charlie. The experimental results are in Appendix D. In the case of the MDI QKD link between Bob and Charlie, we distill the key from the Z basis data, while the X basis data are all used for parameter estimation. The length ℓ of the resulting secret key that guarantees that the MDI QKD protocol is ϵ_{QKD} secure, i.e., it is both ϵ_{cor} correct and ϵ_{sec} secret with $\epsilon_{\mathrm{sec}} + \epsilon_{\mathrm{cor}} \leqslant \epsilon_{\mathrm{QKD}}$, is given by [27]

$$\ell = \sum_{b,c\in\{0,\nu,\mu\}} n_0^{b,c} + n_1^{b,c}\left[1 - h\left(e_1^{b,c}\right)\right] - \mathcal{L}_{\mathrm{EC}}^{b,c} - \log_2\frac{8}{\epsilon_{\mathrm{cor}}^{b,c}} - 2\log_2\frac{2}{\varepsilon'^{b,c}\hat{\varepsilon}^{b,c}} - 2\log_2\frac{1}{2\varepsilon_{\mathrm{PA}}^{b,c}}, \quad (1)$$

where $\epsilon_{\mathrm{cor}} = \sum_{b,c}\epsilon_{\mathrm{cor}}^{b,c}$ and $\epsilon_{\mathrm{sec}} = \sum_{b,c}\epsilon_{\mathrm{sec}}^{b,c}$, with $\epsilon_{\mathrm{sec}}^{b,c} = 2(\varepsilon'^{b,c} + 2\varepsilon_e^{b,c} + \hat{\varepsilon}^{b,c}) + \varepsilon_\beta^{b,c} + \varepsilon_0^{b,c} + \varepsilon_1^{b,c} + \varepsilon_{\mathrm{PA}}^{b,c}$. The parameters $\varepsilon_0^{b,c}$, $\varepsilon_1^{b,c}$, and $\varepsilon_e^{b,c}$ denote the failure probability associated

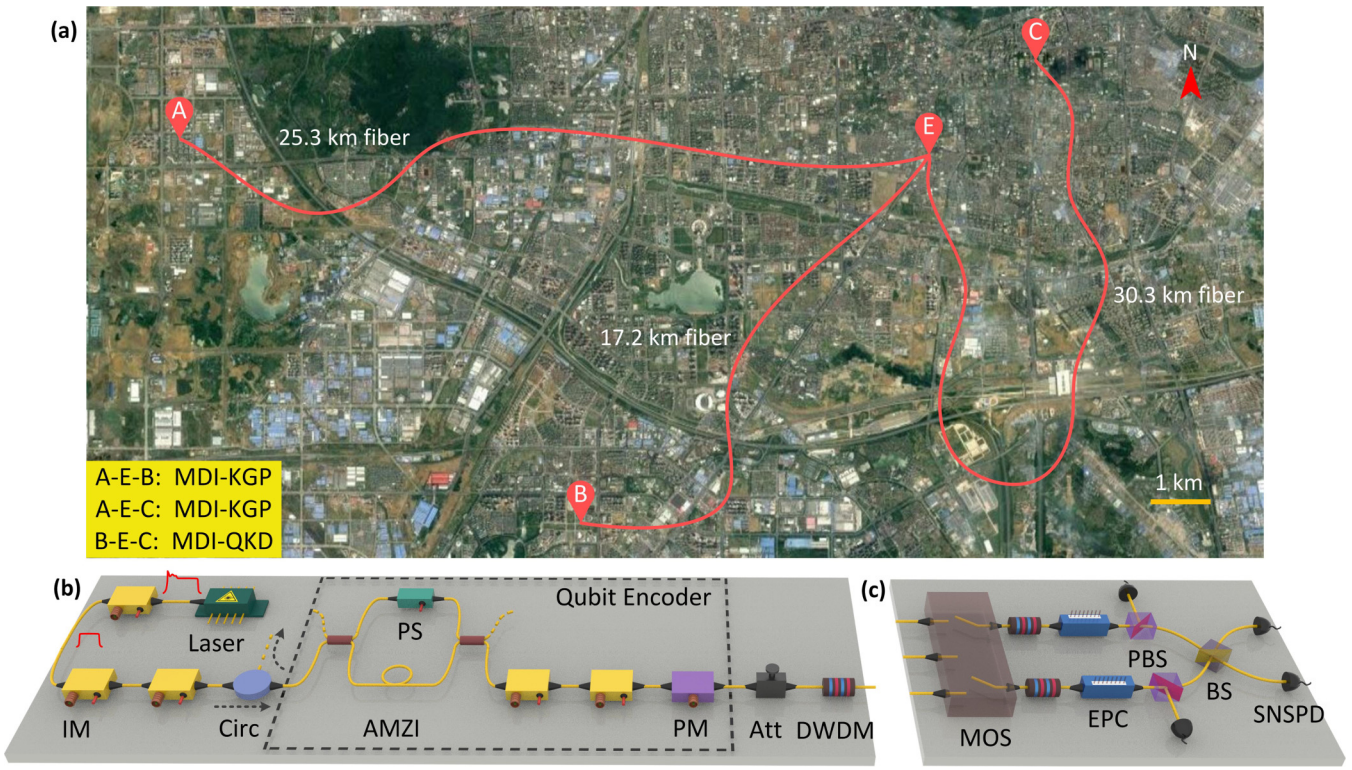

FIG. 1. Measurement-device-independent QDS experiment in a Hefei optical fiber network. (a) Birds-eye view of the MDI QDS experiment. Alice A is located in the Animation Industry Park (N31°50′6.24″, E117°7′52.08″), Bob B at the administrative committee of Hefei (N31°47′4.56″, E117°12′58.04″), Charlie C in an office building (N31°50′56.84″, E117°16′50.14″), and Eve E at the University of Science and Technology of China (N31°50′7.56″, E117°12′58.04″). The A-E-B (A-E-C) quantum link is used to perform the MDI KGP, which generates correlated L-bit strings A_m^B and K_m^B (A_m^C and K_m^C) between Alice and Bob (Charlie). The B-E-C quantum link is used to carry out the MDI QKD scheme, which generates a secure key between Bob and Charlie. This key is used to one-time pad encrypt the information exchanged by these two users during the symmetrization step of the MDI QDS scheme. (b) Alice's setup. The setups of Bob and Charlie are identical to the one of Alice. The internally modulated laser generates phase-randomized coherent-state signal pulses. The first intensity modulator (IM) removes the overshoot rising edge of the signal pulses. The following two IMs implement the decoy state method [21–23]. An asymmetrical Mach-Zehnder interferometer (AMZI) with a phase shifter (PS), in combination with two IMs and one phase modulator (PM), form a qubit encoder, which realizes a time-bin phase encoding. The attenuator (Att) is electrically controlled; it can quickly and automatically change the intensity of the outgoing signals to realize either the Hong-Ou-Mandel interference or single-photon level preparation. Spurious emission is removed by means of a dense wavelength division multiplexor (DWDM). (c) Eve's setup. An 8×4 mechanical optical switch (MOS) implements the routing function. An electric polarization controller (EPC), a polarization beam splitter (PBS), and a superconducting nanowire single-photon detector (SNSPD) form the polarization feedback system. The beam splitter (BS) and two SNSPDs are used to implement the Bell state measurement.

with the estimation of $n_0^{b,c}$, $n_1^{b,c}$, and $e_1^{b,c}$, respectively. Here $\epsilon_{\rm cor}^{b,c}$ and $\varepsilon_{\rm PA}^{b,c}$ represent the failure probability of the error verification and the privacy amplification steps, respectively. See Appendix B for further details. Here we use Bob's data as the reference raw key. Therefore, in Eq. (1), $n_0^{b,c}$ ($n_1^{b,c}$) is a lower bound for the number of events where Bob (Bob and Charlie) emitted a vacuum (single-photon) state that produced a successful BSM result, given that Bob and Charlie selected the intensity settings b and c, with $b,c \in \{0,\nu,\mu\}$, respectively. Further, $e_1^{b,c}$ is an upper bound for the single-photon phase-error rate and $\mathcal{L}_{\rm EC}^{b,c}$ is the information revealed during the error correction step with $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ being the Shannon entropy function.

According to Eq. (1), in principle one can distill the secret key from all the possible combinations of the intensity settings. In our experiment, however, we find that only the data corresponding to the intensity settings $b,c \in \{\nu,\mu\}$ provide a positive key rate. The values of the parameters $n_0^{b,c}$, $n_1^{b,c}$, $e_1^{b,c}$, and $\mathcal{L}_{\rm EC}^{b,c}$, with $b,c \in \{\nu,\mu\}$, are shown in Table I. Also, we use the cascade algorithm to implement error correction [28] and a Toeplitz matrix to perform privacy amplification. The random

TABLE I. Parameters $n_0^{b,c}$, $n_1^{b,c}$, $e_1^{b,c}$, and $\mathcal{L}_{\rm EC}^{b,c}$, with $b,c \in \{\nu,\mu\}$, for the MDI QKD link between Bob and Charlie.

Parameter	$\mu\mu$	$\mu\nu$	$\nu\mu$	$\nu\nu$
$n_0^{b,c}$	0	0	0	0
$n_1^{b,c}$	13144467	4208999	4208978	1346138
$e_1^{b,c}$	20.57%	20.61%	20.61%	20.72%
$\mathcal{L}_{\rm EC}^{ab}$	764378	446414	290251	133085

TABLE II. Value of the different parameters in the MDI QDS experiment.

$\bar{E}$	s_a	$s_a L/2$	s_v	$s_v L/2$	p_E	ε_{rob}	ε_{rep}	ε_{for}
0.25%	0.27%	1073	1.21%	4748	1.23%	2×10^{-8}	1.51×10^{-7}	9.76×10^{-8}

bit string that is needed to generate the Toeplitz matrix was obtained in a previous QKD experiment. The security level of the MDI QKD protocol is set as $\epsilon_{\text{QKD}} = 8\times10^{-8}$ and we obtain an ϵ_{QKD}-secure key of length $\ell = 4\,724\,819$ bits.

In the symmetrization step of the MDI QDS scheme, the position information about the exchanged bits is encoded as follows. For each L-bit string K_m^B (K_m^C) we prepare an L-bit string whose elements are set to 0 or 1 depending on whether or not the equivalent element of K_m^B is sent to Charlie (Bob). That is, for each K_m^B (or K_m^C) we need $3L/2$ secret bits for one-time pad encryption ($L/2$ bits are used to encrypt the actual bits exchanged between the participants and L bits are used to encrypt the string with the position information). In total we need $4\times3L/2 = 6L$ secret bits and thus we select $6L \leqslant \ell$. For our experiment, we choose $L = 787\,468$.

In the MDI KGP between Alice and Bob (Charlie), the signature bit strings A_m^B (A_m^C) are generated only from the data associated with those events where both Alice and Bob (Charlie) use the Z basis and the signal intensity μ. Moreover, Alice and Bob (Charlie) split the correlated bit strings generated in one run of the MDI KGP into two equally long bit strings. Then each of Alice and Bob (Charlie) selects L bits at random to form the bit strings A_0^B and A_1^B (A_0^C and A_1^C), respectively. The remaining bits are all announced to estimate the bit error rate of that string. The results associated with the randomly selected signatures are in Appendix D. With this bit error rate information, we use the Serfling inequality [29] to estimate an upper bound for the error rate between the part of the string K_m^B (K_m^C) that Bob (Charlie) keeps for himself and A_m^B (A_m^C), which is true except for a minuscule probability ε_{PE}. We denote these upper bounds by E_m^B and E_m^C, respectively, and we set $\bar{E} = \max\{E_m^B, E_m^C\}$.

Finally, to evaluate the security of the MDI QDS experiment, we follow the procedure introduced in [19]. This involves the calculation of the minimum rate p_E at which Eve is likely to make errors when guessing the part of K_m^B that Bob keeps for himself. Also, one has to select certain parameters s_a and s_v such that $\bar{E} < s_a < s_v < p_E$ to guarantee security against repudiation and forging. As a result, we have that the probability ε_{rep} of successful repudiation, i.e., that Alice can make Bob accept a message m and Charlie rejects it when it is transferred to him, is [19]

$$\varepsilon_{\text{rep}} \leqslant 2\exp\left[-\tfrac{1}{4}(s_v - s_a)^2 L\right] + \epsilon_{\text{QKD}}. \tag{2}$$

The first term on the right-hand side of this equation corresponds to the probability of successful repudiation given that Bob and Charlie share a perfectly secure secret key before they perform the MDI KGP [19], while the second term takes into account the probability that the secret key delivered by the MDI QKD protocol is not secure. Similarly, the probability ε_{for} of successful forging, i.e., that Bob can generate a fraudulent declaration $(m,\mathcal{S}_m)$ that Charlie accepts, satisfies [19]

$$\varepsilon_{\text{for}} \leqslant \frac{1}{f}(2^{-(L/2)[h(p_E)-h(s_v)]} + \varepsilon) + f + \varepsilon_{\text{PE}} + \varepsilon_{\text{est}}, \tag{3}$$

where the parameters ε, ε_{est}, and f are related to the failure probability when estimating p_E and ε_{PE} is related to the robustness ε_{rob} of the protocol. See Appendix C for more details. The value of each of these parameters in the MDI QDS experiment is shown in Table II.

After performing the two MDI KGPs and the MDI QKD scheme to generate the correlated bit strings A_m^B, K_m^B, A_m^C, and K_m^C as well as a secret key of length ℓ, we also implemented experimentally the classical network that is needed to actually sign a binary message. This includes the implementation of the symmetrization step to generate the bit strings S_m^B and S_m^C and the realization of the messaging stage. All the random bit strings needed for random sampling as well as the secret key that is used to authenticate the classical communications in the MDI QDS experiment are taken from previous QKD experiments. The secret key generated in the MDI QKD link is employed to one-time pad encrypt the information exchanged in the symmetrization step. In this work, Alice decides to sign the message $m = 1$ and sends $(1,\mathcal{S}_1)$ to Bob in the messaging stage. Bob calculates the number of mismatches, 897, between A_1^B and the part of K_1^B that he keeps for himself, and the number, 508, between A_1^C and the part of K_1^C received from Charlie. He accepts the message and forwards $(1,\mathcal{S}_1)$ to Charlie since both mismatches are below their corresponding threshold. Charlie performs a similar check like Bob and accepts m because the number of mismatches, 502, between A_1^C and the part of K_1^C that he keeps for himself and the number, 914, between A_1^B and the part of K_1^B received from Bob are below their corresponding thresholds.

In conclusion, we have experimentally demonstrated a complete MDI QDS protocol in a field test with a failure probability about 10^{-7}. This scheme is information-theoretically secure and is free of any detector side channel. In so doing, we have successfully signed a binary message between three parties. We remark that the signature efficiency of this work is relatively low because we did not perform the full parameter optimization. As in the case of MDI QKD, we believe that the use of the four-intensity decoy-state method [26] and increasing the system clock rate [30] would permit us to significantly decrease the time of data collection.

This work was supported by the National Fundamental Research Program (under Grant No. 2013CB336800), the National Natural Science Foundation of China, the Chinese Academy of Science, and the Science Fund of Anhui Province for Outstanding Youth. M.C. gratefully acknowledges support from the Galician Regional Government (through Grant No. EM2014/033, and consolidation of Research Units

AtlantTIC), MINECO, the Fondo Europeo de Desarrollo Regional through Grant No. TEC2014-54898-R, and the European Commission under project "QCALL" (H2020-MSCA-ITN-2015, project 675662). E.A. and I.V.P. acknowledge support from EPSRC Grant No. EP/M013472/1. W.-L.W. gratefully acknowledges support from the National Natural Science Foundation of China under Grant No. 61472446.

APPENDIX A: PROTOCOL

Here we describe the complete MDI QDS protocol in detail. The basic setup is illustrated in Fig. 2. The MDI QDS scheme consists of two stages: the distribution stage and the messaging stage. Also, it requires that Bob and Charlie previously share a secret key. In our experiment this is achieved by means of MDI QKD.

1. The MDI QKD protocol

Below we present the different steps of the MDI QKD protocol, which is implemented between Bob and Charlie to distribute a secret key [27].

State preparation. The first two steps of the protocol are repeated N times. In every round, each of Bob and Charlie generates a phase-randomized weak coherent pulse with a randomly selected intensity $\gamma \in \{\mu,\nu,0\}$, which encodes a random bit $r \in \{0,1\}$ in a basis $\alpha \in \{Z,X\}$ also selected at random. Then they send these pulses to Eve via the quantum channels.

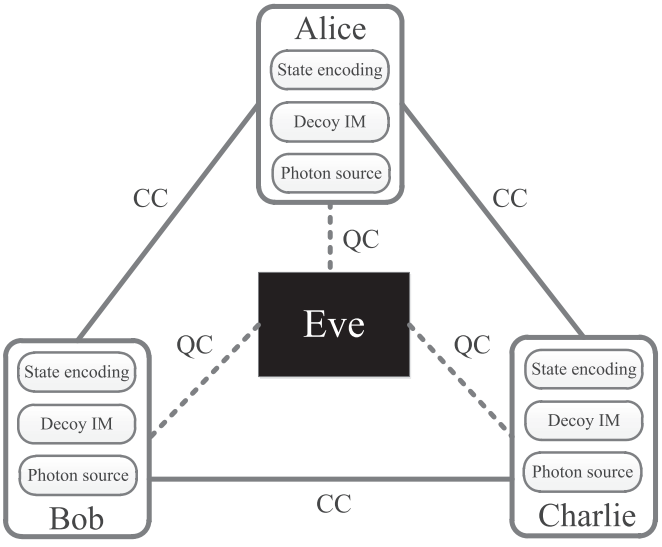

FIG. 2. Schematic diagram of the MDI QDS setup. The channels between the Alice-Eve, Bob-Eve, and Charlie-Eve links are quantum channels (QC); they are denoted by dashed lines. The Alice-Bob, Alice-Charlie, and Bob-Charlie links are also connected through authenticated classical channels (CC); these channels are represented with solid lines. The MDI QDS protocol requires that Bob and Charlie previously share a secret key. For this, they implement a MDI QKD protocol in which Eve acts as a relay. Each of Alice, Bob, and Charlie has one laser source that generates phase-randomized weak coherent pulses that encode different Bennett-Brassard states by means of a state encoding setup. Also, they generate decoy states with an intensity modulator. This modulator is denoted by Decoy IM in the figure. Eve is supposed to perform a Bell state measurement on the incoming signals.

Measurement. If Eve is honest, she performs a BSM on the signals received from Bob and Charlie. In any case, she announces through a public channel whether or not her measurement is successful, together with the Bell state obtained in case of success.

Sifting. Once the N rounds of quantum transmission and measurement have finished, Bob and Charlie communicate with each other through an authenticated channel their intensity and basis settings for the successful BSM results. Let $Z_k^{b,c}$ ($X_k^{b,c}$) be the sets that identify those signals where Eve declares the Bell state k and Bob and Charlie select the intensities b and c and the basis Z (X), respectively. If the sifting conditions $|Z_k^{b,c}| \geqslant N_k^{b,c}$ and $|X_k^{b,c}| \geqslant M_k^{b,c}$ are satisfied for all b,c,k, where $N_k^{b,c}$ and $M_k^{b,c}$ denote some preestablished threshold values, then Bob and Charlie randomly postselect $N_k^{b,c}$ ($M_k^{b,c}$) events from $Z_k^{b,c}$ ($X_k^{b,c}$) to be used in the following steps of the protocol. We will denote such postselected sets by $\hat{Z}_k^{b,c}$ and $\hat{X}_k^{b,c}$, respectively. That is, $|\hat{Z}_k^{b,c}| = N_k^{b,c}$ and $|\hat{X}_k^{b,c}| = M_k^{b,c}$ for all b,c,k. Also, depending on the Bell states announced by Eve, Charlie flips part of his bits to match with those of Bob [18]. If the sifting conditions are not satisfied, the protocol aborts.

Parameter estimation. Bob and Charlie form the code bit strings $z_k^{b,c}$ and $z_k'^{b,c}$, respectively, by randomly choosing $n_k^{b,c}$ bits from $\hat{Z}_k^{b,c}$. The remaining bits of $\hat{Z}_k^{b,c}$, which we denote by $R_k^{b,c}$, are used to compute the error rate $E_k^{b,c}$ and then they are discarded. Only if $E_k^{b,c} \leqslant E_{\rm tol}$, where $E_{\rm tol}$ is a pre-fixed threshold value, Bob and Charlie use the sets $\hat{Z}_k^{b,c}$ and $\hat{X}_k^{b,c}$ to estimate the following three parameters: $n_{k,0}^{b,c}$ ($n_{k,1}^{b,c}$), which is a lower bound for the number of bits in $z_k^{b,c}$ where Bob (Bob and Charlie) sent a vacuum (single-photon) state, and $e_{k,1}^{b,c}$, which is an upper bound for the single-photon phase error rate in $z_k^{b,c}$. If $E_k^{b,c} > E_{\rm tol}$ for all k, the protocol aborts.

Error correction and privacy amplification. For each intensity setting combination $\{b,c\}$, if the data corresponding to the Bell state k pass the parameter estimation step, then Charlie obtains an estimate of $z_k^{b,c}$, which we will denote by $\hat{z}_k^{b,c}$, by using an error correction scheme. This scheme requires that Bob sends Charlie $\mathcal{L}_{\rm EC,k}^{b,c}$ bits of error correction information. Afterward, Bob and Charlie implement an error verification protocol to confirm that $z_k^{b,c}$ and $\hat{z}_k^{b,c}$ are indeed equal except for a minuscule probability $\epsilon_{\rm cor}^{b,c}$. For this, Bob randomly selects a universal$_2$ hash function $\mathcal{H}$ and sends it to Charlie together with the hash value $\mathcal{H}(z_k^{b,c})$. The protocol aborts if $\mathcal{H}(\hat{z}_k^{b,c}) \neq \mathcal{H}(z_k^{b,c})\,\forall k$. Otherwise, Bob and Charlie perform privacy amplification to extract two shorter bit strings $S_k^{b,c}$ and $\hat{S}_k^{b,c}$ of length $\ell_k^{b,c}$ from $z_k^{b,c}$ and $\hat{z}_k^{b,c}$, respectively. They form the final secret key S_B and S_C by concatenating the bit strings $S_k^{b,c}$ and $\hat{S}_k^{b,c}$, respectively. That is, the length of the secret key is $|S_B| = |S_C| = \sum_{b,c\in\{0,\nu,\mu\}} \sum_k \ell_k^{b,c}$.

2. The MDI QDS scheme

We now describe the procedure for signing a binary message. As already mentioned above, the MDI QDS scheme consists of the distribution and the messaging stages. See [19] for more details. Below we assume that Bob and Charlie have

already performed the MDI QKD scheme and they share a secret key.

a. Distribution stage

For each possible bit message $m \in \{0,1\}$, Alice performs a MDI KGP with Bob and Charlie. As discussed in the main text, this protocol provides Alice with different L-bit strings A_m^B (A_m^C), which are correlated with the ones that are obtained by Bob (Charlie). We denote Bob's (Charlie's) L-bit strings by K_m^B (K_m^C).

For this, the MDI KGP builds on the MDI QKD protocol described in the preceding section but with a few modifications. In particular, let us take the MDI KGP between Alice and Bob as an example; the MDI KGP between Alice and Charlie is analogous. To generate the correlated bit strings A_m^B and K_m^B with $m \in \{0,1\}$, Alice and Bob only perform the first four steps of the MDI QKD protocol. That is, they do not implement the classical postprocessing steps of error correction and privacy amplification. Also, for simplicity, we will consider that they use only the data associated with a projection onto one particular Bell state k and discard the rest. In addition, Alice and Bob modify the parameter estimation step of the MDI QKD scheme as follows. They randomly distribute the bits from $\hat{Z}_k^{\mu,\mu}$ into two sets of equal size, which we will denote by $\hat{Z}_{k,m}^{\mu,\mu}$, with $m \in \{0,1\}$. Then they both respectively obtain A_m^B and K_m^B by simply selecting at random L bits from each of these sets. The remaining bits ($R_{k,m}^{\mu,\mu}$) from $\hat{Z}_{k,m}^{\mu,\mu}$ are used to calculate the bit error rate $E_{k,m}^{\mu,\mu}$. This bit error rate must be below a certain threshold value for all m. Otherwise the protocol aborts.

Next Bob and Charlie symmetrize the resulting bit strings K_m^B and K_m^C. This is achieved by each of them initially selecting half of the bits of their respective bit strings at random and then sending these bits (as well as the corresponding bit positions) through their secure channel. That is, say Bob randomly chooses $L/2$ bits from K_m^B and sends them to Charlie (together with the information of their positions in K_m^B) encrypted with the one-time pad. Likewise, Charlie does the same with K_m^C. We will denote the symmetrized L-bit strings of Bob and Charlie by S_m^B and S_m^C, respectively. That is, S_m^B (S_m^C) is composed of the part of K_m^B (K_m^C) that Bob (Charlie) decides to keep, which we will denote by $K_{\text{keep},m}^B$ ($K_{\text{keep},m}^C$), and the part of K_m^C (K_m^B) received from Charlie (Bob), which we will denote by $K_{\text{forward},m}^C$ ($K_{\text{forward},m}^B$).

Finally, Bob estimates the quantities $n_{m,0}$, $n_{m,1}$, and $e_{m,1}$ for the bit strings $K_{\text{keep},m}^B$, where $n_{m,0}$ ($n_{m,1}$) represents a lower bound for the number of bits in $K_{\text{keep},m}^B$ where Bob (Alice and Bob) sent a vacuum (single-photon) state and $e_{m,1}$ is an upper bound for the single-photon phase error rate. Likewise, Charlie does the same with $K_{\text{keep},m}^C$.

b. Messaging stage

To sign a binary message m, Alice sends $(m,\mathcal{S}_m)$ to the desired recipient (say, for instance, Bob), where $\mathcal{S}_m = (A_m^B, A_m^C)$ is the signature of m. Then Bob records the number of mismatches between $\mathcal{S}_m$ and S_m^B by separately comparing A_m^B with the part $K_{\text{keep},m}^B$ of S_m^B received from Alice and A_m^C with the part $K_{\text{forward},m}^C$ of S_m^B received from Charlie. If there are fewer than $s_a(L/2)$ mismatches in both cases, where $s_a < 1/2$ is a small threshold value that is determined by certain experimental parameters that depend on the desired security level of the protocol, Bob then accepts the message as coming from Alice.

If Bob wants to prove to Charlie that he received the message m from Alice, he forwards him $(m,\mathcal{S}_m)$. Then Charlie checks the mismatches between $\mathcal{S}_m$ and S_m^C in a similar way like Bob and accepts m if the number of mismatches is less than $s_v(L/2)$, where s_v is another threshold value that satisfies $0 < s_a < s_v < 1/2$.

APPENDIX B: SECRET KEY DISTILLATION

The symmetrization step of the MDI QDS protocol requires that Bob and Charlie interchange half of their bits (together with the information of the positions of the bits interchanged) in full secrecy. This means in particular that they need a secret key of length at least $6L$ to be used with the one-time pad. This is so because, as we saw in the main text, we need $3L/2$ secret bits for each K_m^B (or K_m^C) with $m \in \{0,1\}$.

To determine the secret key length of the MDI QKD link between Bob and Charlie we follow the finite-key analysis provided in [27]. In our experiment, Eve's BSM performs projections only onto one single Bell state k, so for simplicity below we remove the label k from all the parameters. Also, as already mentioned in the preceding section, note that Bob and Charlie distill a secret key from all the events where both of them select the Z basis and Eve declares a successful result, i.e., independently of the particular intensity setting selected. Thus, according to [27], we have that the length ℓ of the secret bit strings S_B and S_C is given by

$$\ell \geqslant \sum_{b,c\in\{0,\nu,\mu\}} \ell^{b,c}, \tag{B1}$$

with

$$\ell^{b,c} = \max\left(n_0^{b,c} + n_1^{b,c}\left[1 - h\left(e_1^{b,c}\right)\right] - \text{leak}_{\text{EC}}^{b,c} - \log_2\frac{8}{\epsilon_{\text{cor}}^{b,c}} - 2\log_2\frac{2}{\varepsilon'^{b,c}\hat{\varepsilon}^{b,c}} - 2\log_2\frac{1}{2\varepsilon_{\text{PA}}^{b,c}}, 0\right). \tag{B2}$$

The definition of the different parameters is given in the main text. We include it again here for completeness. In particular, we have that $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function, $\epsilon_{\text{cor}} = \sum_{b,c}\epsilon_{\text{cor}}^{b,c}$ is the correctness parameter with $\epsilon_{\text{cor}}^{b,c}$ being the failure probability of the error verification step that is applied to the bit strings $z^{b,c}$ and $\hat{z}^{b,c}$, and $\epsilon_{\text{sec}} = \sum_{b,c}\epsilon_{\text{sec}}^{b,c}$ is the secrecy parameter, with $\epsilon_{\text{sec}}^{b,c} = 2(\varepsilon'^{b,c} + 2\varepsilon_e^{b,c} + \hat{\varepsilon}^{b,c}) + \varepsilon_\beta^{b,c} + \varepsilon_0^{b,c} + \varepsilon_1^{b,c} + \varepsilon_{\text{PA}}^{b,c}$. The parameters $\varepsilon_0^{b,c}$, $\varepsilon_1^{b,c}$, and $\varepsilon_e^{b,c}$ denote the failure probability associated with the estimation of $n_0^{b,c}$, $n_1^{b,c}$, and $e_1^{b,c}$, respectively, and $\varepsilon_{\text{PA}}^{bc}$ represents the failure probability of the privacy amplification step.

To estimate the parameters $n_0^{b,c}$, $n_1^{b,c}$, and $e_1^{b,c}$ we follow the method used in [20]. In particular, let us define the data that we observe in the experiment as follows: $N_{bc}^{\alpha\beta}$ is the total number of pulses prepared by Bob and Charlie by using the bases α and β and the intensities b and c, respectively, with $\alpha,\beta \in \{Z,X\}$ and $b,c \in \{0,\nu,\mu\}$; $D_{bc}^{\alpha\beta}$ is the total number of

successful BSM events reported by Eve given that Bob and Charlie used the bases α and β and the intensities b and c, respectively; and $E_{bc}^{\alpha\beta}$ is the number of errors in $D_{bc}^{\alpha\beta}$.

Then, after applying the sifting step of the protocol, we have that only the data where Bob and Charlie use the same basis remain. Importantly, however, the data associated with those events where Bob or Charlie (or both of them together) send a vacuum state do not need to be distinguished by the encoding basis but can be assigned to any basis. This means in particular that Bob and Charlie can use data from mismatched basis events where they send vacuum states to obtain a tighter estimation of the parameters $n_0^{b,c}$, $n_1^{b,c}$, and $e_1^{b,c}$ in the finite-key regime. For instance, they can redefine the observed data in the Z and X bases as follows (see [20] for further details):

$$\begin{aligned}
&M_{\mu\mu}^{Z} = M_{\mu\mu}^{ZZ}, \quad M_{\mu 0}^{Z} = M_{\mu 0}^{ZZ}, \quad M_{00}^{Z} = M_{00}^{ZZ},\\
&M_{\nu\nu}^{X} = M_{\nu\nu}^{XX}, \quad M_{0\nu}^{X} = M_{0\nu}^{XX} + M_{0\nu}^{ZX}, \quad M_{\mu\nu}^{Z} = M_{\mu\nu}^{ZZ},\\
&M_{0\mu}^{Z} = M_{0\mu}^{ZZ}, \quad M_{\mu\mu}^{X} = M_{\mu\mu}^{XX}, \quad M_{\mu 0}^{X} = M_{\mu 0}^{XX} + M_{\mu 0}^{XZ},\\
&M_{\nu\mu}^{Z} = M_{\nu\mu}^{ZZ}, \quad M_{00}^{X} = M_{00}^{XX} + M_{00}^{ZX} + M_{00}^{XZ},\\
&M_{\nu 0}^{Z} = M_{\nu 0}^{ZZ};
\end{aligned} \tag{B3}$$

$$\begin{aligned}
&M_{\mu\nu}^{X} = M_{\mu\nu}^{XX}, \quad M_{0\mu}^{X} = M_{0\mu}^{XX} + M_{0\mu}^{ZX}, \quad M_{\nu\nu}^{Z} = M_{\nu\nu}^{ZZ},\\
&M_{0\nu}^{Z} = M_{0\nu}^{ZZ}, \quad M_{\nu\mu}^{X} = M_{\nu\mu}^{XX}, \quad M_{\nu 0}^{X} = M_{\nu 0}^{XX} + M_{\nu 0}^{XZ},
\end{aligned} \tag{B4}$$

where $M \in \{N, D, E\}$, i.e., the equations above are applied to $N_{bc}^{\alpha\beta}$, $D_{bc}^{\alpha\beta}$, and $E_{bc}^{\alpha\beta}$. Afterward, Bob and Charlie use a standard estimation procedure [27] on the redefined parameters to determine $n_0^{b,c}$, $n_1^{b,c}$, and $e_1^{b,c}$.

APPENDIX C: SECURITY PARAMETERS OF MDI QUANTUM DIGITAL SIGNATURES

Since the secret key obtained from the MDI QKD protocol is used to encrypt the information interchanged between Bob and Charlie in the key symmetrization step of the MDI QDS scheme, the security parameters of both protocols should be of the same order of magnitude in order to optimize the security level of the experiment.

Next we describe how to calculate the security parameters of the MDI QDS protocol. The analysis is based on the results introduced in [19]. In particular, we have that the robustness of the protocol, i.e., the probability of an honest run aborting, depends mainly on the parameter s_a, which determines if Bob accepts a message received from Alice. For MDI QDSs, we choose $s_a > \bar{E}$, where $\bar{E} = \max\{E_m^B, E_m^C\}$ and

$$E_m^B \geqslant E_{AB,m}^{\mu\mu} + g\left(\frac{L}{2}, R_{AB,m}^{\mu\mu}, \varepsilon_{p_E}\right), \tag{C1}$$

with

$$g\left(\frac{L}{2}, R_{AB,m}^{\mu\mu}, \varepsilon_{p_E}\right) = \sqrt{\frac{\left(R_{AB,m}^{\mu\mu} + L/2\right)\ln\left(\varepsilon_{p_E}{}^{-1}\right)}{\left(R_{AB,m}^{\mu\mu}\right)^2 L/2}} \times \sqrt{R_{AB,m}^{\mu\mu} + 1}. \tag{C2}$$

The parameters $E_{AB,m}^{\mu\mu}$ and $R_{AB,m}^{\mu\mu}$ refer to the quantities $E_{k,m}^{\mu\mu}$ and $R_{k,m}^{\mu\mu}$ introduced in Appendix A 2 for the MDI KGP between Alice and Bob. Here we have removed the subscript k because, as already mentioned, in our experiment Eve performs projections onto only one single Bell state and we have added the subscript AB to emphasize that we refer to the Alice-Bob link. Equation (C1) represents an upper bound on the error rate between Bob's bit string $K_{\text{keep},m}^B$ and the corresponding bits from Alice's bit string A_m^B, which is correct except for a failure probability ε_{p_E}. The parameter E_m^C is defined in a similar way but now for the Alice-Charlie link.

Then it can be shown that the robustness of the MDI QDS protocol is given by

$$\varepsilon_{\text{rob}} \leqslant 2\varepsilon_{p_E}, \tag{C3}$$

which is the probability that either $\bar{E}_{AB,m}^{\mu\mu}$ or $\bar{E}_{AC,m}^{\mu\mu}$ is not an upper bound for $E_{AB,m}^{\mu\mu}$ or $E_{AC,m}^{\mu\mu}$, respectively. On the other hand, it turns out that the probability that Alice can successfully repudiate the signature of a message satisfies

$$\varepsilon_{\text{rep}} \leqslant 2\exp\left[-\tfrac{1}{4}(s_v - s_a)^2 L\right] + \epsilon_{\text{QKD}}, \tag{C4}$$

where $\epsilon_{\text{QKD}} = \epsilon_{\text{cor}} + \epsilon_{\text{sec}}$ is the probability that the secret key shared between Bob and Charlie by means of MDI QKD is insecure.

In our simulations, we set the threshold parameters s_a and s_v as $s_a = \bar{E} + \frac{p_E - \bar{E}}{50}$ and $s_v = \bar{E} + \frac{49(p_E - \bar{E})}{50}$, respectively. In general, the parameter p_E represents the minimum rate at which a potential eavesdropper can make errors when guessing $K_{\text{keep},m}^B$ or $K_{\text{keep},m}^C$. That is, we set $p_E := \min\{p_E^{AB}, p_E^{AC}\}$, where p_E^{AB} and p_E^{AC} are the rates at which the eavesdropper can make errors in guessing the respective strings $K_{\text{keep},m}^B$ and $K_{\text{keep},m}^C$. This is given by

$$h\left(p_E^J\right) = c_{m,0}^J + c_{m,1}^J\left[1 - h\left(e_{m,1}^J\right)\right], \tag{C5}$$

where $J \in \{AB, AC\}$. Here $c_{m,i}^J := 2n_{m,i}^J/L$ and $e_{m,1}^J$ refer to the parameters estimated from $K_{\text{keep},m}^B$ and $K_{\text{keep},m}^C$. In our experiment, since we implement the case where Alice sends a signed message to Bob, we can take p_E as p_E^{AB}.

The threshold parameters s_a and s_v have to satisfy the condition $\bar{E} < s_a < s_v < p_E$ [19]. Also, Eq. (C4) indicates that the bigger the gap between s_a and s_v is, the smaller ε_{rep} would be. This means that s_a should be chosen close to $\bar{E}$. In the case of s_v, however, there is one additional constraint that must be satisfied. It arises from the need that the probability p_r that Bob makes fewer than $s_v L/2$ errors when guessing $K_{\text{keep},m}^C$ has to be smaller than a security parameter f, which protects the protocol against forging. More precisely, according to [19], we have that the probability p_r is upper bounded by

$$\langle p_r \rangle \leqslant \sum_{i=0}^{s_v L/2} \binom{L/2}{i} 2^{-H_{\min}^{\epsilon}(K_{\text{keep},m}^C|B)} + \varepsilon_H, \tag{C6}$$

where

$$H_{\min}^{\epsilon}\left(K_{\text{keep},m}^C|B\right) \approx n_{m,0} + n_{m,1}[1 - h(e_{m,1})] \tag{C7}$$

is Bob's smooth minimum entropy about Charlie's bit string $K_{\text{keep},m}^C$ and ε_H is the failure probability related to the

estimation of this smooth minimum entropy. Equation (C6) can be further upper bounded as

$$\begin{aligned}\langle p_r\rangle &\leqslant \sum_{i=0}^{s_v L/2}\binom{L/2}{i}2^{-\{n_{m,0}+n_{m,1}[1-h(e_{m,1})]\}}+\varepsilon_H\\ &=\sum_{i=0}^{s_v L/2}\binom{L/2}{i}2^{-(L/2)h(p_E)}+\varepsilon_H\\ &\leqslant \sum_{i=0}^{s_v L/2}\binom{L/2}{s_v L/2}2^{-(L/2)h(p_E)}+\varepsilon_H\\ &\leqslant \sum_{i=0}^{s_v L/2}2^{(L/2)h(s_v)}2^{-(L/2)h(p_E)}+\varepsilon_H\\ &=\left(\frac{s_v L}{2}+1\right)2^{-(L/2)[h(p_E)-h(s_v)]}+\varepsilon_H. \end{aligned}\tag{C8}$$

The first inequality is due to Eq. (C7), in the second one we use Eq. (C5), in the third one we use a property of the binomial coefficient together with the fact that $s_v < 1/2$, and in the fourth inequality we use $\binom{N}{k}\leqslant 2^{Nh(k/N)}$.

This means in particular that if s_v is chosen smaller than (but very close to) p_E such that $(\frac{s_v L}{2}+1)2^{-(L/2)[h(p_E)-h(s_v)]}$ is relatively small in comparison to ε_H and f is chosen larger than Eq. (C8), the resulting value of ε_{rep} decreases. This can be achieved, for instance, by setting $s_a=\bar{E}+\frac{p_E-\bar{E}}{50}$ and $s_v=\bar{E}+\frac{49(p_E-\bar{E})}{50}$, which provide better results than those reported in [19]. Finally, we have that the probability that Bob can successfully forge a message m is given by

$$\varepsilon_{\text{for}}\leqslant p_F+f+\varepsilon_{p_E}+\varepsilon_{m,0}+\varepsilon_{m,1}+\varepsilon_{m,e},\tag{C9}$$

where

$$p_F:=\frac{1}{f}(2^{-(L/2)\{c_{m,0}+c_{m,1}[1-h(e_{m,1})]-h(s_v)\}}+\varepsilon_H)\tag{C10}$$

and $\varepsilon_{m,0}$, $\varepsilon_{m,1}$, and $\varepsilon_{m,e}$ are the failure probabilities related to the estimation of $n_{m,0}$, $n_{m,1}$, and $e_{m,1}$.

For simulation purposes, we set the security level of the MDI QKD protocol as $\epsilon_{\text{QKD}}=8\times10^{-8}$ and we obtain a final secret key length of $\ell=4\,724\,819$. The threshold parameters of the MDI QDS scheme take the values $s_a=0.27\%$ and $s_v=1.21\%$ and we obtain $\varepsilon_{\text{rob}}=2\times10^{-8}$, $\varepsilon_{\text{rep}}=1.51\times10^{-7}$, and $\varepsilon_{\text{for}}=9.76\times10^{-8}$. That is, we observe an experimental demonstration of the complete MDI QDS protocol with a total security level of the order of 10^{-7}.

APPENDIX D: EXPERIMENTAL RESULTS

The detailed experimental results for the MDI KGP and the MDI QKD protocol are shown in Tables III–V. These tables present the total number of signals sent, the number of detection events, and the number of errors for all possible combinations of intensity and basis settings.

Finally, in Table VI we show the experimental results related to the creation of the signatures A_m^B, A_m^C, K_m^B, and K_m^C. As already mentioned above, the sets $\hat{Z}_{k,m}^{\mu,\mu}$ with $m\in\{0,1\}$ are obtained by randomly distributing the bits from $\hat{Z}_k^{\mu,\mu}$ into two sets. Then, from each set $\hat{Z}_{k,m}^{\mu,\mu}$ we select L bits at random to form the signatures, while the remaining bits $R_{k,m}^{\mu,\mu}$ from $\hat{Z}_{k,m}^{\mu,\mu}$ are used to estimate the error rate. In Table VI the column that contains the number of errors refers to the number of error found in $R_{k,m}^{\mu,\mu}$.

TABLE III. List of the experimental results in the MDI KGP between Bob and Alice.

B-E-A	Number of detection events			Number of errors			Total number of pulses		
	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$
$0-Z$	5	2281	9410	0	1151	4678	3.48×10^{10}	9.46×10^{10}	1.13×10^{11}
$\nu-Z$	6102	1749934	6900463	3097	11321	23079	9.46×10^{10}	2.56×10^{11}	3.04×10^{11}
$\mu-Z$	25327	6637000	25920132	12597	37586	57933	1.13×10^{11}	3.04×10^{11}	3.61×10^{11}
	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$
$0-X$	3	221587	0	0	109383	0	3.48×10^{10}	1.62×10^{11}	0
$\nu-X$	1567663	13559453	0	792879	4495014	0	1.62×10^{11}	7.50×10^{11}	0
$\mu-X$	0	0	0	0	0	0	0	0	0
	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$
$0-X$	8	2109	9926	0	1023	5094	3.58×10^{10}	8.91×10^{10}	1.17×10^{11}
$\nu-X$	1559324	7353412	16949068	752481	3699305	8601812	1.61×10^{11}	4.43×10^{11}	5.16×10^{11}
$\mu-X$	0	0	0	0	0	0	0	0	0
	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$
$0-Z$	10	224153	0	1	108354	0	3.32×10^{10}	1.63×10^{11}	0
$\nu-Z$	6342	3600069	0	3150	1794446	0	9.91×10^{10}	4.33×10^{11}	0
$\mu-Z$	24754	12375438	0	12589	6171201	0	1.10×10^{10}	5.23×10^{11}	0

TABLE IV. List of the experimental results in the MDI KGP between Alice and Charlie.

A-E-C	Number of detection events			Number of errors			Total number of pulses		
	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$
$0-Z$	56	2732	11538	33	1358	5889	7.12×10^{10}	1.93×10^{11}	2.30×10^{11}
$\nu-Z$	2676	1901132	7467976	1396	7043	19402	1.93×10^{11}	5.22×10^{11}	6.21×10^{11}
$\mu-Z$	11164	7547507	29400832	15521	18995	37340	2.30×10^{11}	6.21×10^{11}	7.37×10^{11}
	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$
$0-X$	53	934208	0	29	468323	0	7.12×10^{10}	3.30×10^{11}	0
$\nu-X$	468796	12232268	0	233884	3784406	0	3.30×10^{11}	1.53×10^{12}	0
$\mu-X$	0	0	0	0	0	0	0	0	0
	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$
$0-X$	71	2644	11841	32	1303	6184	7.32×10^{10}	1.82×10^{11}	2.40×10^{11}
$\nu-X$	459779	4574929	14265714	226537	2306807	7214626	3.28×10^{11}	9.05×10^{11}	1.05×10^{12}
$\mu-X$	0	0	0	0	0	0	0	0	0
	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$
$0-Z$	55	894712	0	38	435637	0	6.79×10^{10}	3.34×10^{11}	0
$\nu-Z$	2634	5801820	0	1306	2909919	0	2.02×10^{11}	8.85×10^{11}	0
$\mu-Z$	10616	16239773	0	5316	7809247	0	2.25×10^{11}	1.07×10^{12}	0

TABLE V. List of the experimental results in the MDI QKD protocol between Bob and Charlie.

B-E-C	Number of detection events			Number of errors			Total number of pulses		
	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$
$0-Z$	26	3030	12044	9	1577	6040	3.87×10^{10}	1.05×10^{11}	1.25×10^{11}
$\nu-Z$	7767	2270167	8869003	3864	13852	27681	1.05×10^{11}	2.84×10^{11}	3.38×10^{11}
$\mu-Z$	30578	8584134	33191574	15469	46320	68734	1.25×10^{11}	3.38×10^{11}	4.01×10^{11}
	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$
$0-X$	16	374541	0	10	189842	0	3.87×10^{10}	1.80×10^{11}	0
$\nu-X$	1692163	16386192	0	843731	5228055	0	1.80×10^{11}	8.34×10^{11}	0
$\mu-X$	0	0	0	0	0	0	0	0	0
	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$	$0-Z$	$\nu-Z$	$\mu-Z$
$0-X$	17	3055	12550	10	1487	6412	3.98×10^{10}	9.90×10^{10}	1.30×10^{11}
$\nu-X$	1699809	8511993	20790027	829897	4220816	10849002	1.79×10^{11}	4.93×10^{11}	5.74×10^{11}
$\mu-X$	0	0	0	0	0	0	0	0	0
	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$	$0-X$	$\nu-X$	$\mu-X$
$0-Z$	26	359290	0	14	173852	0	3.69×10^{10}	1.82×10^{11}	0
$\nu-Z$	7270	5072023	0	3632	2560729	0	1.10×10^{11}	4.82×10^{11}	0
$\mu-Z$	30047	16514489	0	14986	8200455	0	1.22×10^{11}	5.82×10^{11}	0

TABLE VI. List of experimental parameters related to the creation of the signatures A_m^B, A_m^C, K_m^B, and K_m^C.

Signature	$\lvert\hat{Z}_{k,m}^{\mu,\mu}\rvert$	L	$\lvert R_{k,m}^{\mu,\mu}\rvert$	Number of errors	$E_{k,m}^{\mu,\mu}$
$A_0^B-K_0^B$	12960066	787468	12172598	26880	0.219%
$A_1^B-K_1^B$	12960066	787468	12172598	27479	0.225%
$A_0^C-K_0^C$	14700416	787468	13912947	17786	0.127%
$A_1^C-K_1^C$	14700416	787468	13912947	17573	0.126%

[1] R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).
[2] T. ElGamal, in *Workshop on the Theory and Application of Cryptographic Techniques*, edited by G. R. Blakley and D. Chaum, Lecture Notes in Computer Science Vol. 196 (Springer, Berlin, 1984), pp. 10–18.
[3] D. Gottesman and I. Chuang, arXiv:quant-ph/0105032.
[4] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
[5] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. **3**, 1174 (2012).
[6] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).
[7] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Phys. Rev. Lett. **113**, 040502 (2014).
[8] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Phys. Rev. A **91**, 042304 (2015).
[9] R. J. Donaldson, R. J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, and G. S. Buller, Phys. Rev. A **93**, 012329 (2016).
[10] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Phys. Rev. A **93**, 032325 (2016).
[11] H.-L. Yin, Y. Fu, and Z.-B. Chen, Phys. Rev. A **93**, 032316 (2016).
[12] C. Croal, C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson, and N. Korolkova, Phys. Rev. Lett. **117**, 100503 (2016).
[13] H.-L. Yin, Y. Fu, H. Liu, Q.-J. Tang, J. Wang, L.-X. You, W.-J. Zhang, S.-J. Chen, Z. Wang, Q. Zhang, T.-Y. Chen, Z.-B. Chen, and J.-W. Pan, Phys. Rev. A **95**, 032334 (2017).
[14] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, Opt. Lett. **41**, 4883 (2016).
[15] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).
[16] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[17] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth, and H. Weinfurter, New J. Phys. **13**, 073024 (2011).
[18] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[19] I. V. Puthoor, R. Amiri, P. Wallden, M. Curty, and E. Andersson, Phys. Rev. A **94**, 022328 (2016).
[20] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You *et al.*, Phys. Rev. X **6**, 011024 (2016).
[21] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[22] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[23] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[24] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[25] C. H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems, and Signal Processing* (IEEE, Piscataway, NJ, 1984), pp. 175–179.
[26] 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, and J.-W. Pan, Phys. Rev. Lett. **117**, 190501 (2016).
[27] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[28] G. Brassard and L. Salvail, in *Workshop on the Theory and Application of Cryptographic Techniques*, edited by T. Helleseth, Lecture Notes in Computer Science Vol. 765 (Springer, Berlin, 1993), pp. 410–423.
[29] R. J. Serfling, Ann. Stat. **2**, 39 (1974).
[30] 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, Nat. Photon. **10**, 312 (2016).