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,[4,2] 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 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]*EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-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]*SUPA, Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*

(Dated: March 8, 2017)

Quantum digital signatures (QDS) 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 200-square-kilometer metropolitan area, to perform a field test of a three-party measurement-device-independent quantum digital signature (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-QDS for practical applications.

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 e-mails. However, the security of currently used public-key digital signature schemes rely 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 (QDS) [3], on the other hand, can offer information-theoretic security based on quantum mechanics, given that the participants pre-share 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 non-repudiation (*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 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.

In this Letter, we report the first experimental demonstration of a three-party MDI-QDS protocol which 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 200-square-kilometer 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 (MDI-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

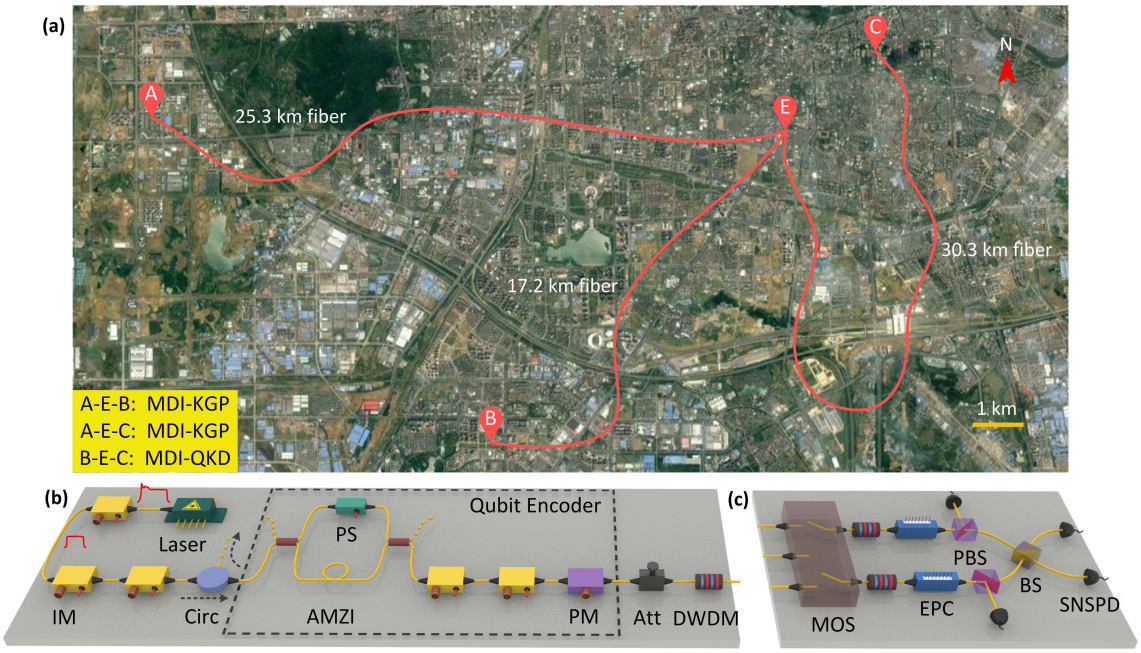

FIG. 1: MDI-QDS experiment in a Hefei optical fiber network. (a) Birds-eye view of the MDI-QDS experiment. Alice 'A' is located in the Animation Industry Park (N31°50′6.24″, E117°7′52.08″), Bob 'B' at the administrative committee of Hefei (N31°47′4.56″, E117°12′58.04″), Charlie 'C' in an office building (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 quantum link A-E-B (A-E-C) is used to perform the MDI-KGP, which generates correlated L-bit strings $A_m^{\rm B}$ and $K_m^{\rm B}$ ($A_m^{\rm C}$ and $K_m^{\rm C}$) between Alice and Bob (Charlie). The quantum link B-E-C 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 set-up. The set-ups 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 [20–22]. 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 outcoming signals to realize either the Hong-Ou-Mandel (HOM) interference or single-photon level preparation. Spurious emission is removed by means of a dense wavelength division multiplexor (DWDM). (c) Eve's set-up. An 8-by-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 (BSM).

by $K_m^{\rm B}$ ($K_m^{\rm B}$), with $m = 0, 1$. Note that the strings $A_m^{\rm B}$ ($A_m^{\rm C}$) and $K_m^{\rm B}$ ($K_m^{\rm C}$) 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 post-processing 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 $K_m^{\rm B}$ 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 $K_m^{\rm C}$. We denote Bob's (Charlie's) bit strings after the symmetrization step by $S_m^{\rm B}$ ($S_m^{\rm C}$).

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 $(m, {\rm Sig}_m)$ to the desired recipient (say Bob), where the signature ${\rm Sig}_m = \left(A_m^{\rm B},\ A_m^{\rm C}\right)$. To verify that m indeed comes from Alice, Bob checks whether ${\rm Sig}_m$ matches his bit string $S_m^{\rm B}$. For this, he checks separately the part of $S_m^{\rm B}$ 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 Charlie that Alice signed m, he sends him $(m,\ Sig_m)$. Then Charlie performs a similar check to that done by Bob and only accepts m if the number of mismatches in both halves of $S_m^{\rm C}$ 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 [23]. As shown in Fig. 1(a), Alice, Bob and Charlie are connected to Eve, with a 25.3 km, 17.2 km and 30.3 km deployed single-mode optical fiber which has a propagation loss of 9.2 dB, 5.1 dB and 8.1 dB, respectively. In collaboration with Eve, Alice and Bob

TABLE 1: Parameters $n_0^{b,c}$, $n_1^{b,c}$, $e_1^{b,c}$, and $\text{leak}_{\text{EC}}^{b,c}$, with $b, c \in \{\nu, \mu\}$, for the MDI-QKD link between Bob and Charlie.

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

(Charlie) exploit the insecure quantum link A-E-B (A-E-C) to implement the MDI-KGP. Also, Bob and Charlie use the insecure quantum link B-E-C 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-by-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 1984 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 bases 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 is anti-correlated 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 (DWDM), 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 (PS) and two power meters [23]. 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 BS. Also, we use the HOM dip to calibrate the wavelength difference between the two interfering pulses [23].

We have run the MDI-KGP between the participants for 73423 (149987) seconds to accumulate data for the pair Alice and Bob (Alice and Charlie). Also, we accumulated data for 81630 seconds during the MDI-QKD session between Bob and Charlie. The experimental results are in the Supplemental Material. In the case of the MDI-QKD link between Bob and Charlie, we distill key from the Z basis data, while the X basis data is all used for parameter estimation. The length ℓ of the resulting secret key which guarantees that the MDI-QKD protocol is ϵ_{QKD}-secure, *i.e.*, it is both ϵ_{cor}-correct and ϵ_{sec}-secret with $\epsilon_{\text{sec}} + \epsilon_{\text{cor}} \leq \epsilon_{\text{QKD}}$, is given by [27]

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

where $\epsilon_{\text{cor}} = \sum_{b,c}\epsilon_{\text{cor}}^{b,c}$ and $\epsilon_{\text{sec}} = \sum_{b,c}\epsilon_{\text{sec}}^{b,c}$, with $\epsilon_{\text{sec}}^{b,c} = 2\left(\varepsilon'^{b,c} + 2\varepsilon_e^{b,c} + \hat{\varepsilon}^{b,c}\right) + \varepsilon_\beta^{b,c} + \varepsilon_0^{b,c} + \varepsilon_1^{b,c} + \varepsilon_{\text{PA}}^{b,c}$. 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. $\epsilon_{\text{cor}}^{b,c}$ and $\varepsilon_{\text{PA}}^{b,c}$ represent the failure probability of the error verification and the privacy amplification steps, respectively. See [27] 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. $e_1^{b,c}$ is an upper bound for the single-photon phase-error

TABLE 2: The 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}

rate, and $\text{leak}_{\text{EC}}^{b,c}$ 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 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 $\text{leak}_{\text{EC}}^{b,c}$, 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 bit string that is needed to generate the Toeplitz matrix is obtained in a previous QKD experiment. The security level of the MDI-QKD protocol is set as $\epsilon_{\text{QKD}} = 8 \times 10^{-8}$ and we obtain a ϵ_{QKD}-secure key of length $\ell = 4724819$ 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 $4 \times 3L/2 = 6L$ secret bits, and thus we select $6L \leq \ell$. For our experiment, we choose $L = 787468$.

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 the Supplemental Material. With this bit error rate information, we use 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 $\bar{E} = \max\{E_m^{\text{B}}, E_m^{\text{C}}\}$.

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]

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

The first term on the RHS of this equation corresponds to the probability of success 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, Sig_m) that Charlie accepts, satisfies [19]

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

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 Supplemental Material 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 $(1, \text{Sig}_1)$ 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, 508, between A_1^{C} and the part of K_1^{C} received from Charlie. He accepts the message and forwards $(1, \text{Sig}_1)$ 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, 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 for the first time 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 increase the signature efficiency.

This work has been 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 (Grant No. EM2014/033, and consolidation of Research Units:AtlantTIC), MINECO, the Fondo Europeo de Desarrollo Regional (FEDER) through Grant No. TEC2014-54898-R, and the European Commission (Project QCALL). EA and IVP acknowledge support from EPSRC grant EP/M013472/1. W.W. gratefully acknowledges support from the National Natural Science Foundation of China under Grant No. 61472446.

[1] R. L. Rivest, A. Shamir, and L. Adleman, Communications of the ACM **21**, 120 (1978).
[2] T. ElGamal, in *Workshop on the Theory and Application of Cryptographic Techniques* (Springer, 1984) pp. 10–18.
[3] D. Gottesman and I. Chuang, arXiv preprint quant-ph/0105032 (2001).
[4] E. Andersson, M. Curty, and I. Jex, Physical Review A **74**, 022304 (2006).
[5] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nature communications **3**, 1174 (2012).
[6] V. Dunjko, P. Wallden, and E. Andersson, Physical review letters **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, Physical review letters **113**, 040502 (2014).
[8] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Physical Review 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, Physical Review A **93**, 012329 (2016).
[10] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Physical Review A **93**, 032325 (2016).
[11] H.-L. Yin, Y. Fu, and Z.-B. Chen, Physical Review 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, arXiv:1608.01086 (2016).
[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, Nature photonics **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 Journal of Physics **13**, 073024 (2011).
[18] H.-K. Lo, M. Curty, and B. Qi, Physical Review Letters **108**, 130503 (2012).
[19] I. V. Puthoor, R. Amiri, P. Wallden, M. Curty, and E. Andersson, Physical Review A **94**, 022328 (2016).
[20] W.-Y. Hwang, Physical Review Letters **91**, 057901 (2003).
[21] H.-K. Lo, X. Ma, and K. Chen, Physical Review Letters **94**, 230504 (2005).
[22] X.-B. Wang, Physical Review Letters **94**, 230503 (2005).
[23] 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.*, Physical Review X **6**, 011024 (2016).
[24] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).
[25] C. H. Bennett and G. Brassard, in *International Conference on Computer System and Signal Processing, IEEE* (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, Nature communications **5** (2014).
[28] G. Brassard and L. Salvail, in *Workshop on the Theory and Application of of Cryptographic Techniques* (Springer, 1993) pp. 410–423.
[29] R. J. Serfling, The Annals of Statistics , 39 (1974).
[30] L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, S.-B. Tam, Z. Yuan, R. Penty, and A. Shields, Nature Photonics (2016).