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*

I. INTRODUCTION

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)[1, 2], on the other hand, provide information-theoretic security based on the laws of quantum physics.

Recent work on QDS [3] 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) [4], we present a measurement-device-independent QDS (MDI-QDS) scheme [5], which is secure against all detector side-channel attacks. This is because in MDI-QKD the legitimate parties do not perform any measurement but only send quantum signals to be measured. Thus, the 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 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 [6], taking into account finite-size effects, to the QDS protocol proposed in [3]. The resulting security proof is valid against general forging and repudiation attacks.

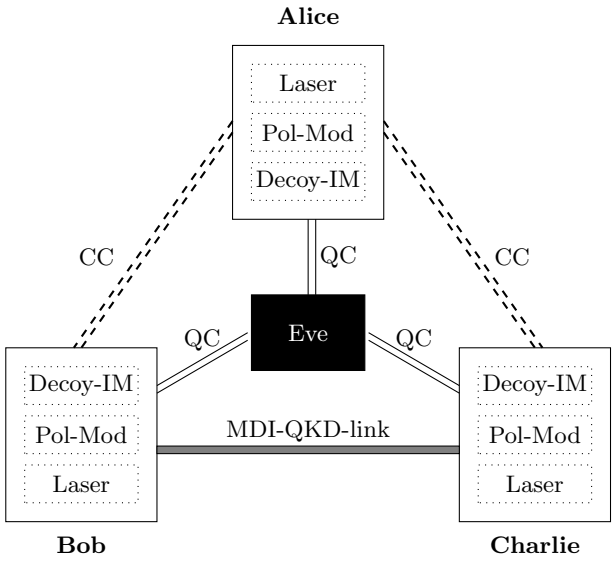

FIG. 1. A schematic diagram of a setup for MDI-QDS. Alice, Bob and Charlie prepare quantum signals in different BB84 polarisation states, using a polarisation modulator (Pol-Mod). In addition, they generate decoy-states with an intensity modulator (Decoy-IM). The signals are then sent to an untrusted party Eve, who 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 (grey 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.

II. THE PROTOCOL

We outline our protocol for three parties, with a sender, Alice, and two recipients Bob and Charlie. The set-up 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 realised with Eve as relay. Any classical secret communication channel between Bob and Charlie would in fact suffice in place of this MDI-QKD link.

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-randomised weak coherent pulses (WCPs), triggered spontaneous parametric down-conversion sources and practical single-photon sources. The scheme makes use of a measurement-

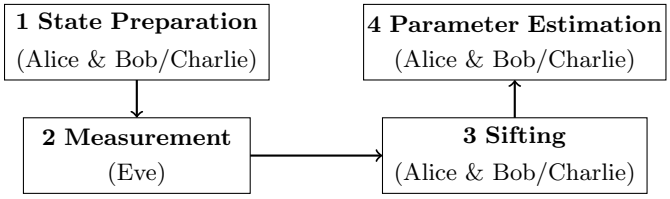

FIG. 2. A schematic diagram of the steps involved in MDI-KGP with the participants indicated in the brackets. First, Alice and Bob/Charlie generates a quantum signal of certain intensity prepared in the Z or X basis. They send their states to Eve through the quantum channel. Second, Eve (assuming she is honest) makes a Bell state measurement of the signlals she has received. She informs Alice and Bob/Charlie through a public channel of whether or not her measurement was successful. If successful, she declares the Bell state that is obtained. Third, if Eve reports a successful result, Alice and Bob/Charlie communicate through an authenticated channel their intensity and basis settings. After this, Bob/Charlie flips part of his bits to correctly correlate them with those of Alice. In the last step, Alice and Bob/Charlie uses a certain fraction of random bits from their bit strings to form the code bit strings and the remaining bits are used to compute the error rate.

device-independent key generating protocol (MDI-KGP), performed in pairs separately by Alice-Bob and Alice-Charlie. The main steps involved in the KGP are shown in Fig. 2 and see [5] 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.

The QDS scheme above is related to the one proposed in [3], 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. In the distribution stage, the pairs (Alice-Bob and Alice-Charlie) separately perform the MDI-KGP. Thereby the pairs generate different (but correlated) strings or raw keys that are not entirely secret. The fact that only Alice holds both the correlated strings protects the protocol against forging. Further, to protect against repudiation and to ensure transferability, Bob and Charlie use a MDI-QKD link to secretly exchange half of their respective strings. This symmetrisation process between Bob and Charlie ensures that Alice cannot make them disagree on the validity of a message, except with negligible probability.

In the subsequent messaging stage, Alice presents the message together with the full classical information. A recipient (say Bob) of a signed message records the number of mismatches he finds with the part of his string that he received directly from Alice and the part of the string received from other party (say Charlie). He accepts the message as genuine if there are sufficiently few mismatches. Similarly, if Bob forwards the message to Charlie then Charlie again tests for mismatches and verifies if these are few enough.

III. SECURITY ANALYSIS

In order to analyse the security of the protocol, we find Eve's information about the secret keys of the participants in the protocol in terms of the smooth min-entropy [7]. Then we use it to bound the probability that she can make a signature declaration making fewer errors than a certain value. 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. A detailed analysis regarding the security of the signature protocol is provided in [5], i.e. 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).

IV. SIMULATION RESULTS

We analysed 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 the order of 10^6 (for each of the possible single bit messages 0 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 around 10^{12} quantum states (per bit to be signed) to Alice during their KGPs. With a source with a pulse rate of 1GHz, we can calculate that it would take approximately 61 minutes to generate a raw key when the experiment uses standard single-photon detectors with detection efficiency 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 since sending a smaller number of signals is then required to sign a single-bit message. Full details regarding the experimental parameters and the raw key

generation times for various detectors that could be used in the protocol are provided in [5]. The simulation results demonstrate that even with practical signals (for example, phase-randomised weak coherent pulses) and a finite size of data (say 10^{11} to 10^{14} signals) it is possible to perform secure MDI-QDS over long distances (up to about 150 km).

V. CONCLUSION

In summary, we have presented a MDI-QDS protocol and it is proved to be 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 [6], taking into account finite size effects, to the QDS protocol proposed in [3]. The resulting security proof is valid against general forging and repudiation attacks. Since the experimental platform for the implementation of MDI-QKD can also be used for MDI-QDS with slight modifications, we expect MDI-QDS could be widely used in practical QDS systems in the near future.

Please refer to our full technical work included as a supplementary document for more details on our results.

[1] D. Gottesman and I. Chuang, arXiv preprint quant-ph/0105032 (2001).
[2] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
[3] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Phys. Rev. A **93**, 032325 (2016).
[4] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[5] I. V. Puthoor, R. Amiri, P. Wallden, M. Curty, and E. Andersson, in preparation (2016).
[6] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat Commun **5** (2014).
[7] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).