Quantum digital signatures without quantum memory

Quantum Digital Signatures without Quantum Memory

Vedran Dunjko,[1,2,3,*] Petros Wallden,[3,4,†] and Erika Andersson[3,‡]
[1]School of Informatics, University of Edinburgh, Edinburgh EH8 9AB, United Kingdom
[2]Division of Molecular Biology, Rud Bošković Institute, Bijenička cesta 54, P.P. 180, 10002 Zagreb, Croatia
[3]SUPA, Institute for Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, Edinburgh EH14 1AS, United Kingdom
[4]Physics Department, University of Athens, Panepistimiopolis 157-71, Ilisia Athens, Greece
(Received 9 September 2013; published 31 January 2014)

Quantum digital signatures (QDSs) allow the sending of messages from one sender to multiple recipients, with the guarantee that messages cannot be forged or tampered with. Additionally, messages cannot be repudiated—if one recipient accepts a message, she is guaranteed that others will accept the same message as well. While messaging with these types of security guarantees are routinely performed in the modern digital world, current technologies only offer security under computational assumptions. QDSs, on the other hand, offer security guaranteed by quantum mechanics. All thus far proposed variants of QDSs require long-term, high quality quantum memory, making them unfeasible in the foreseeable future. Here, we present a QDS scheme where no quantum memory is required, which also needs just linear optics. This makes QDSs feasible with current technology.

DOI: 10.1103/PhysRevLett.112.040502 PACS numbers: 03.67.Hk, 03.67.Ac, 03.67.Dd, 42.50.Ex

Introduction.—Quantum digital signatures (QDSs) [1] offer unconditionally secure exchange of classical messages between one sender and many recipients, with security against forging and security against repudiation. No forging means that no recipient or other party can forge or alter a message. Security against repudiation (sometimes called transferability) implies that a sender cannot make recipients disagree on the validity of a message. Digital signatures are constantly required in modern communication. However, currently used classical public-key based digital signature protocols only offer security based on unproven computational assumptions. The key advantage of QDSs is in the information-theoretic security (security against computationally unbounded adversaries), similar to quantum key distribution (QKD).

In a generic QDS protocol, the sender sends pairs of quantum states, quantum signatures, to the multiple recipients. The recipients store the signatures in quantum memory until the sender decides to send a particular message. Authenticity is effectively guaranteed since the information about the quantum signatures, accessible to forgers, is limited. Nonrepudiability is enforced by the recipients performing some type of nondestructive quantum state comparison on the quantum signatures (for instance, a SWAP test [1]). Although general nondestructive state comparison is currently experimentally difficult, in [2], a QDS scheme based on coherent states was proposed, where comparison can be performed using linear optics. This scheme has been recently implemented [3]. However, the remaining and more challenging requirement for QDSs to become a viable substitute for currently used classical digital signature schemes is the quantum memory. Digital signatures are typically used to sign messages months or even years after the (public) keys are distributed. Therefore, for QDSs to compete with classical protocols we may have to store millions of qubits (or qumodes) coherently, for similarly long times. This is a serious shortcoming given that state-of-the-art quantum memories cannot achieve coherence times longer than minutes [4]. This makes all previous QDS proposals unfeasible in practice [5]. In this Letter, we circumvent the requirement for quantum memory. We propose a QDS scheme with the same security guarantees as those in [1–3], without needing quantum memory. The scheme can be implemented using just linear optics and photodetectors that distinguish only between zero and nonzero photons.

QDSs without quantum memory.—QDS protocols have a distribution stage, where quantum signatures are sent to all future recipients, and a messaging stage, where classical messages are sent and verified. The distribution stage enables a sender, Alice, to send a message to, in the simplest case, either or both of two recipients, Bob and Charlie, at some point in the future (during the messaging stage). The distribution stage is independent of the future message sent in the messaging stage. Our protocol differs from all previous proposals in both stages. In the distribution stage, the quantum signatures are converted to classical information through quantum measurements, thus, eliminating the

need for quantum memory. Following this, authentication and verification procedures in the messaging stage only process classical data. Our QDS protocol, similar to the scheme presented in [2], uses trains of coherent states, and a multiport (described below) for the initial part of the distribution stage.

For simplicity, we will consider the case with two receivers, and explain how this can be generalized later. The quantum signatures comprise trains of coherent states randomly chosen by Alice as $|\alpha\rangle$ or $|-\alpha\rangle$ [6]. In this scheme, just as in [2,3], nonrepudiability is ensured by using a multiport, see Fig. 1. The multiport is a passive linear optical device comprising four 50:50 beam splitters. The top two belong to Bob and the bottom two to Charlie. The input states to both Bob's and Charlie's first beam splitters are a vacuum state and the inbound state from Alice. The outputs of these beam splitters are fed into the second two beams splitters, as shown in Fig. 1. We will refer to the output ports of the second two beam splitters as Bob's and Charlie's signal port and null port, respectively.

Intuitively, the multiport nondestructively [7] compares the coherent states entering at Bob's and Charlie's in ports.

The true multiport function is twofold. It symmetrizes the inbound states, which prevents repudiation. Also, the null-port counts safeguard against active forging. This we explain further below.

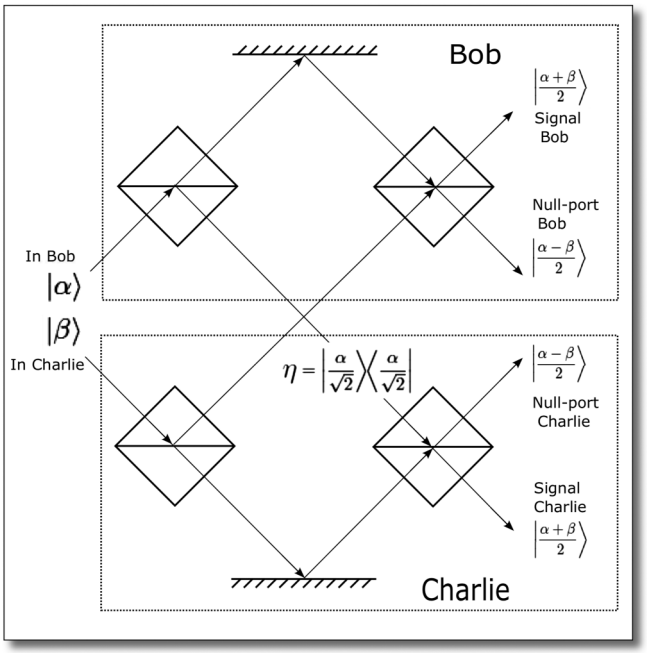

FIG. 1. The multiport: The out-signal arms contain a state symmetric under swap. The null ports contain vacuum if the in-signal arms contained identical states. In active cheating, Bob chooses what state η he sends back to Charlie, so as to optimize his cheating strategies. However, Charlie's null port counts measure the fidelity between honest and dishonest states η. In the figure, η is set to the honest response state.

Similar to all other QDS proposals, we assume that all classical communication is performed over an authenticated channel (which is an inexpensive resource), and that the quantum channel from Alice to the recipients also is authenticated. The standard QDS assumption, that these quantum channels are authenticated, greatly simplifies our security analysis, but, as we elaborate at the end, for our purposes, we actually require less than the resource-expensive fully authenticated quantum channels.

At the end of the distribution stage, the received quantum signatures are measured using unambiguous state discrimination (USD) [8–10], which, for two coherent states, can be optimally realized using linear optics alone [11]. An (ideal) unambiguous quantum measurement gives a result that is guaranteed to be correct, at the expense of sometimes failing to give a result at all. In the subsequent messaging stage, Alice accompanies a message with the sequence of phases ($|\alpha\rangle$ or $|-\alpha\rangle$) she chose for the corresponding sequence of coherent states. The recipients verify that a low enough number of phases disagrees with those measured during the distribution stage.

Since the security of quantum protocols such as quantum key distribution relies on the quantum nature of states representing data, it is not evident that security can be maintained when quantum information is replaced by classical information through a measurement. Previous protocols for QDSs required the recipients to use knowledge available to them only in the messaging stage for choosing the best possible measurement to test the validity of a signed message. In the messaging phase, recipients should test if the signature states are orthogonal to the states they are declared to be. If the recipients measure the signature states directly at the end of the distribution stage, without the knowledge of what the states are supposed to be, then a forger could use an equally effective measurement in an attempt to forge a signature. By delaying their measurements until the messaging stage, as in previous QDS protocols, it is clear that recipients have an advantage over potential forgers. It is not immediately clear that the recipients retain an advantage if signature states are measured already in the distribution stage. We have, however, been able to show that the classical measurement outcomes obtained at the end of the distribution stage can still be used for the secure distribution of messages.

The basic protocol, outlined below, describes how single-bit messages can be securely distributed. For longer messages, both stages are iterated. We will introduce certain internal parameters which should be appropriately chosen. We also introduce an external parameter L, which directly influences the security level. Finally, $p_{\mathrm{USD}} = 1 - e^{-2\alpha^2}$ is the optimal success probability of unambiguous discrimination of $\{|\alpha\rangle, |-\alpha\rangle\}$ [8–11].

Distribution stage.—(1) For each possible future message $k = 0, 1$, Alice generates two copies of a sequence of coherent states (called quantum signatures)

$\text{QuantSig}_k = \otimes_{l=1}^{L} \rho_l^k$, where $\rho_l^k = |b_l^k \alpha\rangle\langle b_l^k \alpha|$, α is a real positive amplitude, $b_l^k \in \{-1, 1\}$ are randomly chosen signs, and L is a suitably chosen integer. The state QuantSig_k and the sequence of signs $\text{PrivKey}_k = (b_1^k, \ldots b_L^k)$ are called the quantum signature and the private key, respectively, for message k. The individual state ρ_l^k we call the lth quantum signature element state for message k. (2) Alice sends one copy of QuantSig_k to Bob and one to Charlie, for each possible message $k = 0$ and $k = 1$. (3) Bob and Charlie send their sequences QuantSig_k for $k = 0$ and $k = 1$, one signature element at a time, through the QDS multiport, shown in Fig. 1. For each signature element they (a) note whether photons are registered at their multiport null port. They also (b) measure the multiport signal states using the USD measurement for $\{|\alpha\rangle, |-\alpha\rangle\}$. They store the unambiguous outcomes, and the index of the state for which it occurred, for $k = 0, 1$. Thus, they store triplets of the form $\{(k, l', b_{l'}^k)\}$ where $1 \leq l' \leq L$.

Messaging stage.—(1) For the bit message m, Alice sends (m, PrivKey_m) to the desired recipient (say Bob). (2) Bob checks whether (m, PrivKey_m) matches with his stored sequence, for positions where he obtained an unambiguous outcome. In particular, he confirms that the number of mismatches is below $s_a p_{\text{USD}} L$, where s_a is an authentication threshold. (3) Provided the authentication threshold was not breached, before accepting the message, Bob checks that he has no reason to abort the protocol. (a) If the number of signature elements for which nonzero null-port counts are registered breaches a threshold rL for $0 \leq r < 1$, he aborts. (b) If the number of unambiguous outcomes is not inside the expected interval $[(p_{\text{USD}} - \delta)L, (p_{\text{USD}} + \delta)L]$, where $0 < \delta < 1$ is the unambiguous count tolerance, he aborts. If the authentication threshold was not breached, and the protocol has not been aborted, Bob accepts the message coming from Alice. (4) To forward the message to Charlie, Bob forwards to Charlie the pair (m, PrivKey_m) he received from Alice. Charlie tests for mismatches similarly to Bob, and checks whether or not the number of mismatches is below $s_v p_{\text{USD}} L$ where s_v is the verification threshold, with $0 \leq s_a < s_v < 1$. (5) For Charlie to accept the forwarded message, provided the verification threshold was not breached, he confirms that he has no reason to abort the protocol, in the same way as Bob.

The roles Bob and Charlie play are, of course, arbitrary. One player authenticates a message received directly from Alice, and the other one verifies a forwarded message.

Protocol performance.—We will consider correctness, security against repudiation, and security against forging of our protocol, for a single bit message. Another important property, robustness, which guarantees that the protocol works even if physical imperfections are present, we address briefly later in this Letter. Below, we will show that the probabilities of incorrect behavior, forging, and repudiation decay exponentially in L, if internal parameters are chosen appropriately. Note that in the three-player setting it only makes sense to consider, at most, one player being malevolent, since two or more malevolent players can always trivially cheat on the third.

Correctness: Correctness implies that if everybody behaves honestly (and no imperfections are present), then the protocol is aborted only with negligible probability, and the message is accepted by both recipients. If everybody is honest, abort can only occur if the number of unambiguous outcomes either recipient obtains is outside the tolerance window $[(p_{\text{USD}} - \delta)L, (p_{\text{USD}} + \delta)L]$. This occurs with probability

$$P(\text{honest abort}) \leq (1 - 2\exp(-2\delta^2 L))^2. \quad (1)$$

To see this, note that the expected value for the number of unambiguous outcomes, for each recipient and if everybody is honest, is exactly $p_{\text{USD}} L$. The expression $2\exp(-2\delta^2 L)$, by Hoeffding's inequalities [12], bounds the probability that the deviation from this mean is larger than δL, and expression (1) takes into account that neither player should abort.

Security against repudiation: Repudiation occurs when the protocol is not aborted, the message is authenticated by one of the recipients, but gets rejected when forwarded to another recipient. Thus, Alice is, here, the malevolent player, and her strategies effectively comprise the possible choices of quantum states she sends in the distribution stage. Security against repudiation relies on the symmetrization property of the multiport—the joint states of Bob's and Charlie's signal ports are invariant under swaps of matching quantum signature elements—and the fact that the acceptance thresholds s_a and s_v differ, so that $s_v > s_a$.

The symmetrization property of the multiport implies that even when post-selected on some sequence of outcomes for Bob and Charlie, for part of the quantum signature, the matching reduced density matrices for each remaining key element are always equal for Bob and Charlie. This guarantees security against all types of repudiation attacks. Intuitively, any strategy of Alice, besides the honest one, will yield a certain average fraction of mismatches (a fraction Alice can control) between the declared private key and the signs measured using USD. Since Bob's and Charlie's reduced states are equal, and they compare their measurement outcomes with the same declaration, the fraction of mismatches will, on average, be equal for both players. It is very unlikely for Alice to make both Bob observe less than $s_a p_{\text{USD}} L$ mismatches and Charlie observe more than $s_v p_{\text{USD}} L$ mismatches. Alice can choose the average number of mismatches, but each mismatch independently occurs for either Bob or Charlie with equal probability. One can show that her optimal choice is to cause a mismatch with probability $(s_v + s_a) p_{\text{USD}}/2$ for each element. Then, Alice's repudiation probability is bounded by

$$P(\text{repudiation}) \leq \exp\left(-\frac{1}{2}p_{\text{USD}}^2(s_v - s_a)^2 L\right). \quad (2)$$

Equation (2) again stems from Hoeffding's inequalities, which give the probability that the number of mismatches deviates from the expected value by more than a fraction. The full technical derivation of (2), based on ideas above, which also shows that classical correlations or entanglement does not help Alice, is given in [14].

Security against forging: By forging, we denote the scenario where a dishonest recipient convinces an honest recipient that Alice has sent a message when Alice has sent no message at all (message forging), or a message m' differing from the message m Alice has in fact sent (message tampering). For our setting, the probability of successful message tampering equals the probability of message forging, as the private keys for two differing messages are independently distributed. Without loss of generality, assume that the forging party is Bob.

We identify different types of forging attacks. First, we distinguish between passive and active attacks. In passive attacks, Bob behaves honestly in the distribution stage until step (a) of the protocol. Here, he stores all the quantum systems outbound from the multiport in quantum memory, and performs measurements which will optimize his cheating probability. In active attacks, Bob acts maliciously throughout the distribution stage. Specifically, Bob can tamper with his part of the multiport.

Second, we distinguish between individual, collective, and coherent attacks. This classification is reminiscent of the traditionally studied attacks in QKD [13]. In individual attacks, Bob's action (whether it is measuring the quantum signature or tampering with his section of the multiport) is independent for each signature element. In collective attacks, he may use only strategies which are classically correlated for different signature elements. For coherent attacks, we remove this last constraint, allowing quantum correlations. Such attacks constitute the most general type of forging activity. Here, we will address the security of our protocol both for passive and active attacks, and for individual and collective attacks, and leave the analysis of coherent attacks for future work.

In passive attacks, Bob wants to make Charlie accept $\text{PrivKey}_{m'}$ for the single bit message m' Bob has chosen. Note that knowing $\text{PrivKey}_{m'\oplus 1}$ for message $m'\oplus 1$ does not help, since the signs of the two messages are independently distributed. Similarly, since all the signs within one private key are independently distributed, the optimal collective forging strategy can be shown to be [14] performing minimum-error measurements [15] on each of the signature elements in $\text{QuantSig}_{m'}$. The results of the measurements are reported to Charlie, who then checks them against his unambiguous outcomes. Let $p_{\min}$ be the minimum-error probability, i.e., the probability that Bob incorrectly identifies a quantum signature element. For two states [8–10],

$$p_{\min} = 1 - \frac{1}{2}(\sqrt{1 - e^{-4\alpha^2}} + 1). \quad (3)$$

For Bob to successfully forge with Charlie (that is, have a faked message verified, which is easier than to forge a transferrable message as $s_a < s_v$), Bob must correctly guess a sufficient fraction of Charlie's unambiguous measurement outcomes. Since forging, by definition, can occur only if Charlie does not abort, Charlie has received at least $p'_{\text{USD}}L$ unambiguous outcomes, with $p'_{\text{USD}} = p_{\text{USD}} - \delta$. This lower bound is also the best scenario for forger Bob, and one can show that

$$P(\text{forge}) \leq \exp\left(-2\left(p_{\min} - s_v\frac{p_{\text{USD}}}{p'_{\text{USD}}}\right)^2 p'_{\text{USD}}L\right). \quad (4)$$

By setting $\delta = 0$, Eq. (4) would bound the probability of Bob making an error in his estimate of the encoded phases fewer than $s_v p_{\text{USD}}L$ times, out of $p_{\text{USD}}L$ guesses.

In active individual attacks, Bob can prepare response states η, see Fig. 1, which modifies Charlie's quantum signature states. To counteract such attacks, Charlie must check the multiport null-port counts during distribution, as they measure the fidelity between the passive-strategy response state and an active one [14]. Requiring that there are no null-port counts (i.e., setting $r = 0$) implies, in the limit $L \to \infty$, that Bob must have been honest throughout the distribution stage. This reduces active individual attacks to passive attacks. For collective attacks, it is easy to see that the space of collective strategies forms a convex structure, and the optimal cheating probability is achieved at an extremal point—corresponding to an individual attack. Thus, collective strategies are no better than individual. We provide more details, and quantitative security statements in [14].

Robustness and parameter constraints: Equations (1), (2), and (3) constrain the internal parameters to ensure exponential decay in the probabilities of unwanted events, as a function of L. Concretely, as long as $\delta > 0$ and $s_v < p_{\min}(p_{\text{USD}} - \delta)/p_{\text{USD}}$ (say $\delta = p_{\text{USD}}/10$ and $s_v = p_{\min}/4$), we obtain an exponential decay. The parameters r and s_a can, in the ideal case, be set to 0. We have, however, left them in expressions and protocol definition, as they can be used to counteract imperfections occurring in any realization. For instance, imperfections can cause mismatches or null-port counts even when everybody is honest. One can, therefore, choose $s_a > 0$ or $r > 0$, respectively. However, detailed analysis of imperfect settings are beyond the scope of this Letter.

We have assumed that all the players share a trusted reference frame, necessary to define the phase of the coherent states. This could be realized by having a fourth party send sequences of strong reference pulses. Alternatively, Alice could send time-multiplexed pairs of signal-idler coherent states, with the idler as reference

beam, as in [3]. The security analysis would then be slightly different (as the reference beam could be tampered with), but, with minor modifications, our results would still hold.

Discussion.—A remaining issue, aside from security against coherent forging, is the requirement for authenticated quantum channels. While general quantum message authentication [16] is resource-expensive, we need verification of only two possible states. Potentially, techniques similar to those in standard QKD could be employed, by sacrificing a fraction of the states. This should suffice, as all that is required is that the classical measurement outcomes of the quantum states remain unperturbed by the adversary, rather than arbitrary quantum states. Such an approach would, in the worst case, yield an additional overhead for the distribution stage comparable to the cost of running a QKD protocol. However, it may be possible to further lower this overhead, and we will further address this in upcoming work. Finally, our protocol is easily generalized in many ways. First, using a generalized multiport [2], it can be extended to any number of recipients. Moreover, the quantum signatures could be chosen from more than two states, or among linearly dependent states as in BB84 [17] QKD. In the latter case, USD is impossible, but minimum-error measurements, nonoptimal schemes [18–20], or quantum state elimination could be sufficient. Our protocol also highlights that certain classical multiparty correlations are sufficient for secure digital signatures. One may ask whether such correlations can be achieved by other means, for instance, by many point-to-point QKD systems.

Support by EPSRC Grants No. EP/G009821/1, No, EP/K022717/1, the EPSRC Doctoral Prize Fellowship, and partial support from COST Action No. MP1006 is gratefully acknowledged.

*vdunjko@inf.ed.ac.uk
†petros.wallden@hw.ac.uk
‡e.andersson@hw.ac.uk

[1] D. Gottesman and I. Chuang, arXiv:quant-ph/0105032v2.
[2] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
[3] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. **3**, 1174 (2012).
[4] P. C. Maurer *et al.*, Science **336**, 1283 (2012).
[5] In the demonstration presented in [3], Alice sent the message she wanted to sign simultaneously with the quan- tum signatures, to avoid the need for long-term quantum memory. This was therefore a proof-of-principle demonstration of the authentication stage of the protocol only, since in a real situation, there is always a delay between the distribution and messaging stages.
[6] This particular choice of coherent states is not crucial, but it simplifies the security analysis. One may also envisage protocols using other nonorthogonal states, such as qubit states, or more than two states.
[7] The action of the multiport is nondestructive if the inbound states are the same, which happens when Alice is honest.
[8] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[9] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[10] A. Peres, Phys. Lett. A **128**, 19 (1988).
[11] K. Banaszek, Phys. Lett. A **253**, 12 (1999).
[12] W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).
[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[14] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.112.040502 for full details of the security statements and proofs.
[15] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).
[16] H. Barnum et al., in 43rd Annual IEEE Symposium on Foundations of Computer Science: Proceedings: Vancouver, BC, Canada, 2002 (IEEE Computer Society Press, Los Alamitos, CA, 2002), p. 449.
[17] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE, New York, 1984), p. 175.
[18] S. J. van Enk, Phys. Rev. A **66**, 042313 (2002).
[19] V. Dunjko and E. Andersson, Phys. Rev. A **86**, 042322 (2012).
[20] F. E. Becerra, J. Fan, and A. Migdall, Nat. Commun. **4**, 2028 (2013).