Realization of Quantum Digital Signatures without the Requirement of Quantum Memory

Robert J. Collins,[1] Ross J. Donaldson,[1] Vedran Dunjko,[1,2,3,*] Petros Wallden,[1] Patrick J. Clarke,[1,†] Erika Andersson,[1] John Jeffers,[4] and Gerald S. Buller[1]

[1]SUPA, Institute of Photonics and Quantum Sciences, School of Engineering and Physical Sciences, Heriot-Watt University, David Brewster Building, Edinburgh EH14 4AS, United Kingdom

[2]School of Informatics, Informatics Forum, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom

[3]Laboratory of Evolutionary Genetics, Division of Molecular Biology, Ruđer Bošković Institute, Bijenička Cesta 54, 10000 Zagreb, Croatia

[4]SUPA, Department of Physics, University of Strathclyde, John Anderson Building, 107 Rottenrow, Glasgow G4 0NG, United Kingdom

(Received 24 January 2014; published 21 July 2014)

Digital signatures are widely used to provide security for electronic communications, for example, in financial transactions and electronic mail. Currently used classical digital signature schemes, however, only offer security relying on unproven computational assumptions. In contrast, quantum digital signatures offer information-theoretic security based on laws of quantum mechanics. Here, security against forging relies on the impossibility of perfectly distinguishing between nonorthogonal quantum states. A serious drawback of previous quantum digital signature schemes is that they require long-term quantum memory, making them impractical at present. We present the first realization of a scheme that does not need quantum memory and which also uses only standard linear optical components and photodetectors. In our realization, the recipients measure the distributed quantum signature states using a new type of quantum measurement, quantum state elimination. This significantly advances quantum digital signatures as a quantum technology with potential for real applications.

DOI: 10.1103/PhysRevLett.113.040502 PACS numbers: 03.67.Dd, 03.67.Ac, 03.67.Hk, 42.50.Ex

Digital signatures are used to ensure that messages cannot be forged or tampered with. Signed messages are also transferable, meaning that it is unlikely that one recipient accepts a message as genuine, while another recipient, to whom the message is forwarded, rejects it. This important property is also called nonrepudiation: a sender cannot deny having sent a message. Digital signature schemes are different from encryption, which guarantees the privacy of a message. Both are important cryptographic tasks. Quantum key distribution (QKD) [1,2] can be used to distribute a secret key for information-theoretically secure encryption, and commercial systems are already available [3,4]. Analogously, digital signature schemes relying on quantum mechanics [5–8] can also be made information-theoretically secure, in contrast to currently used classical digital signature schemes. In this Letter we show that quantum digital signature (QDS) and QKD require similar experimental components and a comparable level of experimental complexity.

Protocols for quantum digital signatures have a distribution stage and a messaging stage. We will describe the case with one sender and two recipients, but this can be extended to more recipients. In the distribution stage, the sender, Alice, transmits quantum signature states to the recipients, Bob and Charlie. She chooses a sequence of L states for each possible message that she might later want to send, for a suitable chosen integer L, and distributes one copy of each state sequence to each recipient. The quantum states are randomly chosen from a set of nonorthogonal states; in our realization, we choose four coherent states $|\alpha\rangle$, $|\alpha e^{i\pi/2}\rangle$, $|\alpha e^{i\pi}\rangle$, and $|\alpha e^{3\,i\pi/2}\rangle$, with known magnitude α. The chosen phase sequences are analogous to a private key, known only to Alice. In the simplest case, to send a one-bit message later on, Alice distributes two sequences of states to both Bob and Charlie, one corresponding to the possible message 0, and one corresponding to the message 1.

In the subsequent messaging stage, Alice accompanies the message she sends with the classical information about the corresponding sequence of quantum states; in our realization, this is the sequence of phases. A recipient of a signed message tests that this agrees with the previously distributed quantum signature states, and accepts the message as genuine if there are sufficiently few mismatches for the whole sequence. Similarly, to forward a message, a recipient forwards the message together with the information about the corresponding quantum signature states. The new recipient again tests for mismatches and verifies that these are below a desired threshold.

Previous QDS schemes [5–7] required that recipients store the signature states in long-term quantum memory until the messaging stage. Once a recipient is given the private information about a signature state—say, that it

should be equal to some state $|\phi\rangle$—the best way to test for a mismatch is to make a quantum measurement with measurement operators $|\phi\rangle\langle\phi|$, $\mathbf{1} - |\phi\rangle\langle\phi|$(that is, to test if the state has any component orthogonal to the state it is declared to be).

The requirement for quantum memory is clearly infeasible at present. There may be days, weeks, or longer between the distribution and the messaging stages, whereas state-of-the-art quantum memories cannot achieve coherence times longer than tens of minutes at room temperature [9,10]. A protocol that circumvents quantum memory was suggested in [8], and our current experiment realizes a variant of this scheme. Here, the recipients measure the signature states directly at the end of the distribution stage. Only classical information needs to be stored. In [8], unambiguous state discrimination measurements were envisaged. In our realization, we improve on this idea so that Bob and Charlie instead use "unambiguous quantum state elimination" (USE) [11,12] to probabilistically exclude one or more phase for each signature state.

Our experimental setup is shown in Fig. 1. The state elimination measurement can for coherent states be realized using linear optics and photodetectors. Each recipient uses two detection systems, shown within dashed light blue lines in the bottom right of Fig. 1, where the signature states are interfered with reference pulses of phase 0 in the top and phase $\pi/2$ in the bottom interferometer. Polarization routing [13] is employed for the orthogonally polarized signal and reference pulses, using the polarizing beam combiner and splitters. The reference pulses enter through the left-hand input ports of beam splitters 2 and 3 while the delayed signal pulses enter through the top. Detecting photons in any of the output ports excludes one possible phase, similar to a recent realization of unambiguous state discrimination (USD) [14]. Whereas USD requires excluding all but one of the quantum states, we only require elimination of at least one state (phase). This significantly increases the number of usable signature elements, by requiring fewer detection coincidences. The process of USE is summarized here and is described in more detail in the Supplemental Material [15]. To estimate the resulting advantage, assume that the amplitude entering Bob's and Charlie's measurement setups is β and neglect, e.g., phase imperfections. The probability of excluding the coherent state of opposite phase to the one that is sent is then $1 - \exp(-|\beta|^2) = p$, and the probabilities of excluding the other two are $1 - \exp(-|\beta|^2/2) = q$. The probability of excluding all three states that were not sent is pq^2, while the probability of excluding at least one of them is $1 - (1-p)(1-q)^2$, which is always greater. If, as in our experiment, $|\beta|$ is small, then this quantity is much greater than pq^2.

A forger must avoid declaring a phase that has been eliminated; more precisely, he must avoid this for sufficiently many signature sequence positions. If Bob (or Charlie) succeeds in eliminating three of the four possible phases for one signature position, then a forger must select

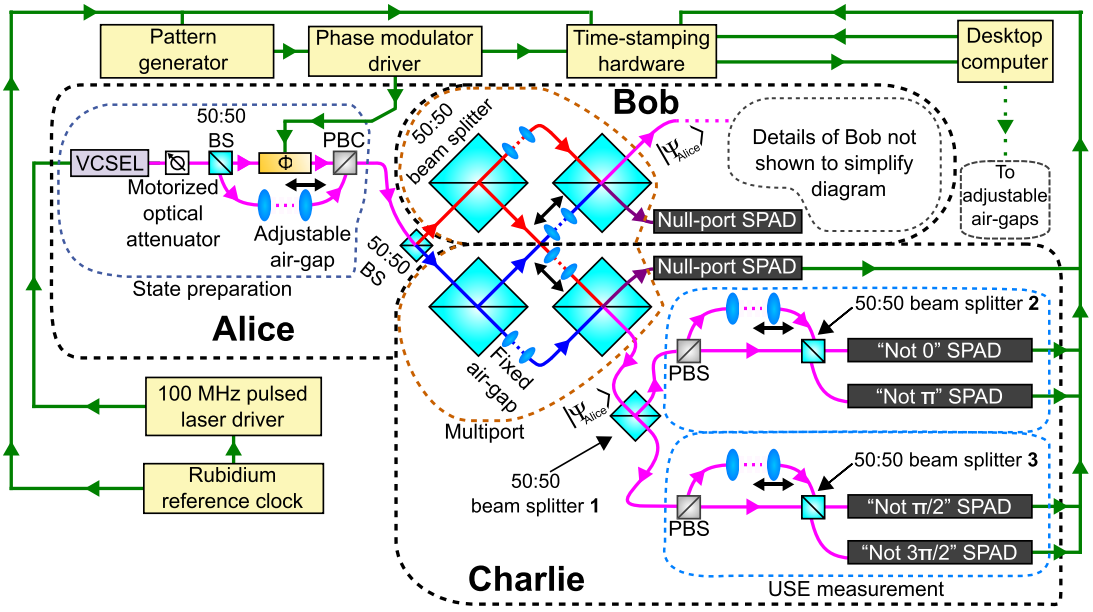

FIG. 1 (color online). Experimental setup for distributing quantum digital signatures. VCSEL denotes a vertical cavity surface emitting laser. Alice uses a $LiNbO_3$ phase modulator to apply a phase shift Φ, randomly chosen as 0, $\pi/2$, π, or $3\pi/2$, to each coherent state. The recipients Bob and Charlie use an all-optical fiber multiport to ensure nonrepudiation and guard against forging, consisting of the four beam splitters within the brown dashes in the center of the figure. For detection, the USE measurement setups within the light blue dashes in the bottom right are used to eliminate one or more. For detection, the setups within the light blue dashes are used to eliminate one or more possible phases. The detectors are silicon single-photon avalanche diodes (SPADs). PBC denotes a polarization beam combiner and PBS denotes a polarization beam splitter.

the single remaining phase to avoid a mismatch. But even if just one phase is ruled out, a forger must avoid selecting this phase. With USE, therefore, many events which would count as nondetected if using USD will now contribute to the detection of forging. Consequently, using state elimination leads to an improvement in the signature generation rate. For both USE and USD, the forger's probability of avoiding too many mismatches decays exponentially with the signature length L.

A more detailed security analysis is found in [8] and in the Supplemental Material [15]. We have examined security for a single use of the protocol, for general repudiation attacks and all forging attacks except those involving entangling operations on successive signature sequence states. So-called "composable security" remains an important issue. In short, security against forging follows since Alice's signature states are chosen from a set of nonorthogonal quantum states, which cannot be distinguished perfectly. Only Alice has the full description of these states. Note that the number of recipients depends on protocol parameters, because if too many copies of Alice's signature states are available, or if $|\alpha|^2$ is too large, then the private phases could be determined reliably enough to forge a message unless protocol parameters such as L are adjusted.

To prevent repudiation, recipients must ensure that they are sufficiently unlikely to disagree on the validity of a message. Here, as in [7], this is achieved using an all-optical fiber multiport, shown in the center of Fig. 1 within the dashed brown line. Bob and Charlie split the pulses received from Alice using a 50:50 beam splitter. Bob sends to Charlie half of the pulse he received from Alice, and Charlie does correspondingly. Bob then combines the component he received directly from Alice with the component he received from Charlie on another 50:50 beam splitter, and Charlie again does correspondingly. This symmetrizes Bob's and Charlie's quantum states for each position in the signature sequences, so that their measurement statistics at the output of the multiport are identical. By choosing a lower allowed fraction of mismatches s_a for accepting a message received directly from Alice, and a higher allowed fraction s_v for verifying that a forwarded message is genuine, it can be made unlikely that two recipients will disagree on the validity of a message, see [5,8] and [15].

Moreover, the multiport guarantees that even if Alice uses general, possibly entangled, quantum states, she still cannot make Bob and Charlie significantly disagree on the validity of a signature. In addition, by considering counts at the multiport null ports, the recipients can guard against certain types of forging.

In [8] and in the Supplemental Material [15] we show that the probabilities for repudiation and forging decay exponentially in L, by suitable choice of protocol parameters depending on the properties of an actual implementation. The scheme can also be made robust; that is, if all parties are honest, then the protocol runs as intended with high probability. In any implementation, errors will occur even if all parties are honest. Therefore, to ensure robustness, one should for example select $s_a > 0$.

Defining the level of security in QDS is not straightforward, since different parties may be honest and dishonest. Here we assume that one chooses values of s_a and s_v such that the probabilities for repudiation, forging, and rejection if all participants are honest are all equal (see [15]). The probability of any of these undesirable events occurring is then

$$P\ (\text{failure}) \leq \exp[-(g^2/8)L], \tag{1}$$

where g is the gap giving a lower bound on the advantage that someone (e.g., Alice) has if she knows the signature, compared to someone else (e.g., a forger) who makes a guess by performing a measurement on the signature copies (see [15]). In this Letter, we will call the failure probability the "security level of the QDS scheme." Equation (1) shows that a greater gap g gives better protocol performance.

The figure of merit that we will use to quantify the performance of our experiment is the length of the signature L required to sign a "half-bit" message for a given security level. One can also define the rate of the signature as the number of bits per second that can be signed securely, given the clock rate of the source used. Our experiment uses a clock rate of 100 MHz, due to the temporal response profile of the Geiger-mode silicon single-photon avalanche diodes (Si-SPADs) [16].

We explored mean photon numbers per pulse from $|\alpha|^2 = 1$ to 11. Coherent states are generated by a temperature-stabilized pulsed VCSEL with wavelength 850.17 nm, attenuated to the desired mean photon number per pulse $|\alpha|^2$, defined at the launch from Alice into the multiport. For a given run of the experiment with some $|\alpha|^2$, we registered the phases that Bob and Charlie ruled out.

These experimental data give the probabilities of excluding particular states, given that Alice sent a certain state. All losses are included, because these probabilities are determined from the experimentally measured ratio of detection events to the total number of pulses sent by Alice. For the QDS scheme to be secure, an honest participant must be able to detect a difference between forged and genuine signatures (see [15]). How large this difference is determines g (see [15,17]), and therefore, through Eq. (1), determines the length L required for a desired security level. The gap g is proportional to the transmittance (one minus the losses) [15]; therefore, the length L for a fixed security level decreases quadratically as the transmittance increases. In short, the difference between the success and failure probabilities for USE determines how well a participant can identify a false declaration.

Experimental results are shown in Fig. 2. Each data point represents the mean of several measurements. Vertical error bars are the standard deviation, and horizontal error bars the

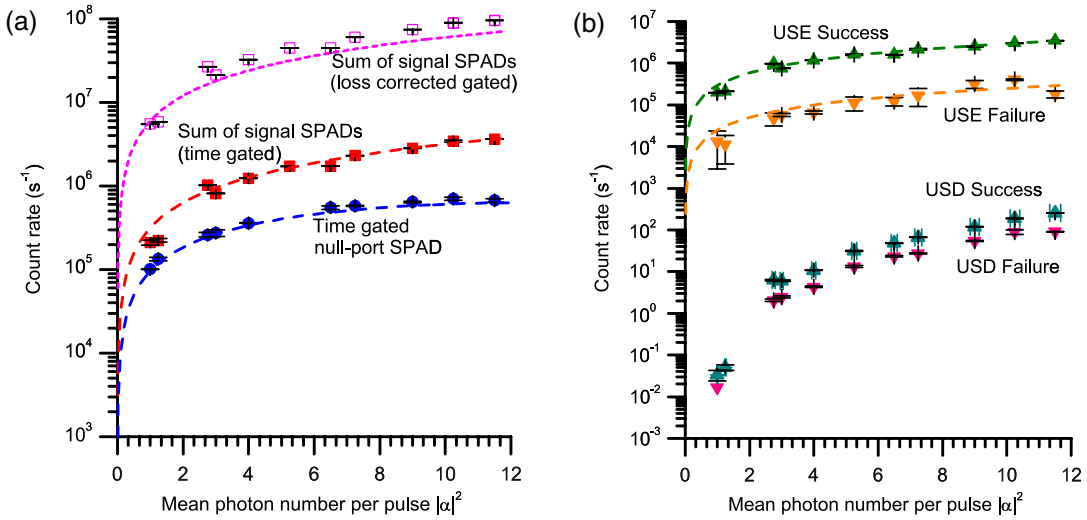

FIG. 2 (color online). (a) Experimentally measured time-gated detector events for Charlie. The time-gated signal count rate is the detector click rate summed over all four of Charlie's signal SPADs, filtered by a window of ± 1 ns around the expected pulse arrival time. The "loss corrected gated rate" is the calculated time-gated count rate at the signal output of the multiport. (b) Rates of successful and failed measurements for one recipient. "USE success" means that at least one state was correctly excluded using quantum state elimination. That is, the state Alice actually sent was not excluded, and at least one other state was excluded. "USE failure" means that the state Alice actually sent was excluded. "USD success" is the rate of successful unambiguous state discrimination (the correct state was obtained) while "USD failure" is the rate of unsuccessful unambiguous state discrimination (the obtained state differs from that sent by Alice). Data points represent experimental results and dashed lines are theoretical predictions [18]. Experimental data are averaged over several measurements and error bars in the count rate are the standard deviation. Horizontal error bars for the mean photon number are dominated by a worst-case assumption that the pulse-to-pulse variation in the output power of our laser is the experimentally measured maximum of $\pm 1.5\%$.

uncertainty in the mean photon number due to a pulse-to-pulse variation of $< \pm 1.5\%$ in VCSEL intensity. In Fig. 2(b) USE success means that at least one state was eliminated, as long as the state that Alice actually sent was not eliminated. USE failure means that the state that Alice actually sent was eliminated. The success probability for USD is also shown, and is considerably lower than for USE. With USE, one sometimes excludes more than one state. All USD success events are included in the USE success data. As already noted, with USE many events which would count as undetected in USD will now contribute to the detection of forging, in addition to all USD success events. The difference between the success and failure probabilities is greater for USE than it is for USD, similarly indicating that USE leads to a greater chance of detecting forging.

For all investigated values of $|\alpha|^2$, the success probability for USE is much higher than the failure rate. For higher failure rates, one has to set acceptance and verification thresholds s_a and s_v higher to ensure robustness. This in turn increases the signature length required to ensure the same security level. The primary cause of a failure, for both USE and USD, was the fringe visibility of the detection setups, which was 80.9%. The multiport has a fringe visibility of 99.7%.

When determining the optimal $|\alpha|^2$, one has to consider that the gap also depends on $p_{\min}$, which is the minimum error probability that a forger obtains if he tries to guess Alice's signature by measuring a copy of the quantum signature [15]. For very small α, $p_{\min}$ is large, but detecting a false declaration is difficult, while for very large α, $p_{\min}$ is small but detecting a false declaration is relatively easy. Since the ability to detect a false declaration is estimated from experimental data, and does not have an analytical expression, it is not straightforward to determine the optimum α. In our experiment, the best gap $g = 1.20 \times 10^{-6}$ occurs for $|\alpha|^2 = 1$. For a security level of 0.01% this gives $L = 5.10 \times 10^{13}$ to sign a half bit. This is an impractical signature length, and below we will comment on planned improvements in order to make this rate more practical.

The signature length L increases with increased distance between parties, since g in Eq. (1) is proportional to the transmittance η. For example, if η is squared, then the L required for the same level of security will increase by a factor of η^{-2}. In any event, if honest recipients see a difference between a forged and a genuine signature, however small, then it is always possible to find values of s_a, s_v, and L to give a desired level of security.

To conclude, we have experimentally demonstrated a first realization of a QDS scheme which does not require long-term quantum memory, and where the recipients use quantum state elimination. This is an important step in developing practical QDS systems. Our experiment uses phase-encoded coherent states. Recently, Arrazola and

Lütkenhaus suggested using phase-encoded coherent states for quantum fingerprinting [19]. In our demonstration, due to the difficulty of stabilizing a multiport with long optical paths, the sender and receivers were only separated from each other by approximately five meters of optical fiber. Separate reference signals are needed for calibration before signature transmission, and as phase reference for the USE measurements. Tampering with reference pulses by a malevolent party should not lead to higher probability of forging or repudiation than tampering with signal states themselves [15]. Also, reference signals can be bright, and thus can in principle be fully monitored through quantum tomography.

We are currently exploring three changes to significantly improve performance. First, by extrapolating data from a recent experiment on USE, we expect the optimal $|\alpha|^2$ to be around 0.5. Because of the high losses of this early prototype we were unable to successfully resolve measurements at this $|\alpha|^2$. The second improvement is to use a protocol that does not require a multiport, in order to decrease loss. Nonrepudiation then needs to be guaranteed in an alternative way, similar to our recently proposed alternative QDS schemes [20], which could be modified to use phase-encoded coherent states, similar to the current realization. We estimate that implementing these changes will result in a gap of $g = 1.96 \times 10^{-4}$, and length $L = 1.19 \times 10^9$ for a security level of 0.01%. This protocol also potentially offers increased distances between sender and receivers.

Finally, increasing the clock rate, and therefore the transmission rate, is possible. The phase modulators, VCSEL, and driving electronics are capable of clock rates up to 3.3 GHz. In the system described in this Letter we did not employ such clock rates due to the limitations of the time-stamping electronics [21].

This work was supported by the U.K. Engineering and Physical Sciences Research Council (EPSRC) through Grants No. EP/G009821/1, No. EP/K022717/1, and No. EP/K015338/1. P. W. gratefully acknowledges partial support from COST Action MP1006. V. D. gratefully acknowledges support from the U.K. EPSRC.

[*]Present address: Institute for Quantum Optics and Quantum Information, Austrian Academy of Sciences, Technikerstrasse 21 A, A-6020 Innsbruck, Austria.

[†]Present address: School of Instrumentation Science and Opto-electronics Engineering, Beihang University, 37 Xueyuan Road, Haidian District, Beijing 100191, China.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] L. Widmer, in *Internet—Technical Development and Applications*, edited by E. Tkacz and A. Kapczynski, Advances in Intelligent and Soft Computing Vol. 64 (Springer, Berlin, 2009), p. 217.
[4] For example, http://www.magiqtech.com, http://www.idquantique.com, http://www.quintessencelabs.com, and http://www.sequrenet.com, all visited May 12, 2014.
[5] D. Gottesman and I. Chuang, arXiv:quant-ph/0105032v2.
[6] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).
[7] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. **3**, 1174 (2012).
[8] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).
[9] P. C. Maurer *et al.*, Science **336**, 1283 (2012).
[10] K. Saeedi, S. Simmons, J. Z. Salvail, P. Dluhy, H. Riemann, N. V. Abrosimov, P. Becker, H.-J. Pohl, J. J. L. Morton, and M. L. W. Thewalt, Science **342**, 830 (2013).
[11] S. Barnett, *Quantum Information* (Oxford University Press, New York, 2009), pp. 103–104.
[12] S. Bandyopadhyay, R. Jain, J. Oppenheim, and C. Perry, Phys. Rev. A **89**, 022336 (2014).
[13] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).
[14] F. E. Becerra, J. Fan, and A. Migdall, Nat. Commun. **4**, 2028 (2013).
[15] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.113.040502 for full details of the experimental methods, and the security statements and proofs.
[16] P. J. Clarke *et al.*, New J. Phys. **13**, 075008 (2011).
[17] P. Wallden, V. Dunjko, and E. Andersson, J. Phys. A. **47**, 125303 (2014).
[18] P. J. Clarke, R. J. Collins, P. A. Hiskett, P. D. Townsend, and G. S. Buller, Appl. Phys. Lett. **98**, 131103 (2011).
[19] J. M. Arrazola and N. Lütkehnaus, arXiv:1309.5005.
[20] V. Dunjko, P. Wallden, and E. Andersson, arXiv:1403.5551.
[21] M. Wahl, H.-J. Rahn, T. Röhlicke, G. Kell, D. Nettels, F. Hillger, B. Schuler, and R. Erdmann, Rev. Sci. Instrum. **79**, 123113 (2008).