Quantum Digital Signatures

Dominic Moylett*
Quantum Engineering Centre for Doctoral Training
University of Bristol
(Dated: May 25, 2016)

I. INTRODUCTION

Cryptography is the study of secure communications between multiple parties, often called Alice and Bob. In classical cryptography, this security is guaranteed through the assumed hardness of certain problems. RSA [1], for example, is secure assuming that factoring integers is hard. Unfortunately, these have no strict guarantees. And even worse, some have been shown to be easy in both theory [2] and experimental work [3, 4] using quantum computers.

Thankfully, while quantum computers break secrecy, they can also fix it. Quantum Key Distribution (QKD) protocols such as BB84 [5] can information theoretically securely establish a shared key. Once Alice and Bob have a shared key, they can use a one-time pad to send messages with perfect secrecy. This means that it is impossible for an eavesdropper, Eve, to learn anything about what was said. This has also been demonstrated experimentally [6] and there are now companies such as ID Quantique [7] offering commercial products for QKD.

But alas, secrecy is only one aspect of cryptography. Even if Alice and Bob have guaranteed secrecy, that still doesn't stop Eve from sending a message of random gibberish to Bob while pretending to be Alice. Even worse, Eve might simply pretend to be Bob throughout the whole QKD protocol, and thus fool Alice into sending her the message intended for Bob. This is one of the arguments laid out in a white paper by CESG, which concludes that "CESG does not endorse QKD for government or military applications, and advises against replacing any existing public key solutions with QKD for commercial applications" [8].

The extra precautions required to prevent the above attacks are digital signatures. Like how someone signs a letter, a digital signature is an extra piece of data in a message to indicate who wrote it. And like classical encryption schemes, classical digital signatures rely on the hardness of certain problems.

Based on the improvements in secrecy, one might ask if quantum physics can also benefit digital signatures. This is the subject that this essay will explore. In SEC. II, we offer a definition of digital signatures. SEC. III describes the best known classical digital signature, followed by quantum digital signatures (QDSs) in SEC. IV and experimentally in SEC. V. Finally, we conclude with some points of discussion in SEC. VI.

* dominic.moylett@bristol.ac.uk

II. DEFINITION OF DIGITAL SIGNATURES

Definition II.1. *A function* $f : \mathbb{N} \to \mathbb{R}$ *is negligible iff* $\forall\ c > 0\ \exists\ n_0 \in \mathbb{N}$ *such that* $\forall\ n \geq n_0, |f(n)| < \frac{1}{n^c}$.

The most common example of negligible functions are functions of the form $2^{-p(n)}$ for some positive polynomial p.

A digital signature scheme consists of the following stages:

Key Generation: Alice generates a signing key and a verification key. The signing key is kept to herself, while the verification key is public.

Message Signing: Alice takes a message and her signing key and produces a message-signature pair.

Message Verification: Bob, takes a message-signature pair & Alice's verification key and accepts if he thinks the message was signed by Alice.

For security, we care about three properties with digital signatures:

Honest Abort: The probability of aborting if all parties are honest is negligible in terms of the security parameter (often the length of the signature).

Repudiation: The probability that Alice is able to convince Bob that a message-signature pair is valid and convince another party Charlie that the same pair is invalid is negligible.

Forgery: The probability that Bob can convince someone else that a message he wrote was written by Alice is negligible.

III. LAMPORT'S ONE-TIME DIGITAL SIGNATURE

The original quantum digital signature was inspired from a classical family of digital signatures first published by Lamport[9], and are reliant on the existence of one-way functions, defined below.

Definition III.1. *Let* $\mathcal{X}, \mathcal{Y}$ *be arbitrary sets. A function* $f : \mathcal{X} \to \mathcal{Y}$ *is one-way iff* f *can be computed in polynomial time, but for any polynomial-time randomised adversary* $f^{-1} : \mathcal{Y} \to \mathcal{X}$ *and uniformly selected* $x \in \mathcal{X}, \Pr[f(f^{-1}(x)) = f(x)]$ *is negligible.*

For a one-way function f, Lamport's one-time digital signature scheme is defined as follows for an m-bit message:

Key Generation: Alice generates m pairs of uniformly selected integers (k_0^i, k_1^i). These will act as Alice's signing key, while the verification key will be the pairs $(f(k_0^i), f(k_1^i))$ for $i \in \{0, ..., m-1\}$.

Message Signing: For each bit m_i of Alice's message, she sends $k_{m_i}^i$ as her signature for that bit.

Message Verification: Given Alice's verification key $\{v_0^i, v_1^i\}$ and her signature $k_{m_i}^i$, her message m_i can be verified by accepting if $v_{m_i}^i = f(k_{m_i}^i)$.

Because this signature scheme is classical and deterministic, verifying parties can share their copies of the message and verification keys, so Alice cannot repudiate.

Note that if an attacker has signatures for two different messages M, M' then they can construct the valid signature for the new message $m_0 m_1 ... m_i' ... m_{m-1}$, where $m_i \neq m_i'$. So this scheme only works for signing one message. But if an adversary can forge a message given only one message from Alice then it is possible to invert f, so f is not one-way.

IV. QUANTUM DIGITAL SIGNATURES

Note that for all of these protocols, L is the security parameter, $s_a \geq 0$ is the authentication threshold for authenticating a message from the original author, and $1 > s_v > s_a$ is the threshold for verifying a forwarded message.

A. Gottesman and Chuang

The first QDS was by Gottesman and Chuang [10]. The protocol used the same principles as Lamport's one-time signature scheme, but utilised quantum one-way functions, which map L-bit strings k to n-qubit states $|f_k\rangle$. The full protocol is described below, where f is the quantum one-way function and $T < L/n$ is the number of copies of each key:

Key Generation: To sign a single bit, Alice generates pairs of L-bit strings $\{k_0^i, k_1^i\}, i \in \{0, ..., M-1\}$ uniformly at random to act as her private key. Her public key is the pairs of quantum states $\{|f_{k_0^i}\rangle, |f_{k_1^i}\rangle\}, i \in \{0, ..., M-1\}$.

Message Signing: To sign a bit b, Alice sends the tuple $(b, k_b^0, k_b^1, ..., k_b^{M-1})$.

Message Verification: To verify a signed message $(b, k_b^0, k_b^1, ..., k_b^{M-1})$, a recipient can use f and SWAP tests [11] to determine if $|f_{k_b^i}\rangle$ matches the corresponding public key. The number of times a recipient finds that the SWAP test fails is noted as s. If $s \leq s_a M$ then the recipient accepts the message (**1-ACC**), and if $s \geq s_v M$ then the recipient rejects the message (**REJ**). In the case where $s_a < s \leq s_v$, the recipient notes that the message is valid but might not be transferable (**0-ACC**).

Security against forgery is possible due to Holevo's theorem [12], which states that even if an eavesdropper managed to acquire all T copies of the public key, they could only extract at most Tn bits of data, and thus their probability of correctly guessing a single L-bit string of the signing key is $2^{-(L-Tn)}$. If the distance between two public keys $|\langle f_k | f_{k'} \rangle| \leq \delta$ for $k \neq k'$, then the probability of an attacker managing to make a recipient accept a signature they weren't able to correctly guess is at most δ^2. Thus by choosing s_v smaller than the probability of a guessing adversary being accepted $(1-\delta^2)(1-2^{1-(L-Tn)})$, we can ensure that each recipient rejects the forgery with high probability.

It is harder to protect against repudiation, because Alice can send Bob and Charlie different states. Due to the no-cloning theorem [13], there is no perfect way for Bob and Charlie to check that their keys are identical. Gottesman and Chuang's solution is to introduce another step to the protocol, called Key Distribution, which uses a distributed SWAP test to check that the keys sent to Bob and Charlie match:

Key Distribution: Alice sends two copies of each key to Bob and Charlie. Bob and Charlie pick random indices $i \in \{0, ..., M-1\}$ to perform a distributed SWAP on. Some of these indices they will perform SWAP tests on their own copies of the key to ensure that those match, and others Charlie will send one of his copies to Bob for a SWAP test between recipients. If any tests fail then the protocol is aborted, otherwise they discard the test keys and continue the protocol with the remaining keys.

With this step in place, the probability of Alice being able to successfully repudiate is the probability that all distributed SWAP tests pass yet $|s_B - s_C| > (s_v - s_a)M$, where s_B and s_C are Bob and Charlie's incorrect counts, respectively. This probability can be exponentially small, depending on how large the gap between c_1 and c_2 is.

While Lamport's signature scheme assumes the existence of classical one-way functions, no such assumption is required here. This is because quantum one-way functions can be devised, such as the one by Buhrman et al. [11]. Thus using fingerprint states creates a negligible probability of forgery.

However, this protocol has a number of disadvantages:

1. Verification keys cannot be copied due to the no-cloning theorem [13], so all keys must come from Alice. This requires authenticated quantum channels from Alice to each recipient, to ensure a forger doesn't simply send their own keys.

2. The recipients need to store keys until Alice uses them to sign a message in long-time quantum memory.

3. Generating and sharing a quantum one-way function, while possible, is a complex task.

4. The distributed SWAP tests are not efficient.

Over the rest of this section, we will summarise how these problems have been overcome.

B. Initial Improvements

Improvements were initially made by Dunjko, Wallden and Andersson [14], who removed the need for quantum memory, the quantum SWAP test and quantum one-way functions. Their protocol for three parties is as follows:

Key Generation: Alice generates two L-bit keys k^0, k^1 at random for some security parameter L, which act as Alice's signing keys. Alice then generates states of the form $|(-1)^{k_l^b}\alpha\rangle$ for $l \in \{0, ..., L-1\}$ and $b \in \{0, 1\}$, where α is a positive real number known between all parties and k_l^b is the l-th bit of k^b. These quantum states will act as the verification key.

Key Distribution: For two recipients, Bob and Charlie, Alice generates a copy of the above state for each participant. Bob and Charlie run their states together through a multiport. For states which come out of the signal port, they then use Unambiguous State Discrimination (USD) [15] to distinguish the states $\{|-\alpha\rangle, |\alpha\rangle\}$, and for each unambiguous state $|(-1)^{k_l^b}\alpha\rangle$ note the value of k_l^b, the index l and whether $b = 0$ or 1.

Message Signing: To sign a message b, Alice sends the message (b, k^b) to Bob.

Message Verification: To verify a message-signature pair (b, k^b), Bob checks the bits of k^b sent to him with the bits he was able to unambiguously determine. If the number of mismatches is at most $s_a p_{USD} L$, where p_{USD} is the USD success probability, then Bob accepts.

The multiport prevents repudiation; even if Alice sends $|\alpha\rangle$ to Bob and $|\beta\rangle$ to Charlie, postselecting on photons that come out the signal outputs of the multiport ensures that both recipients have the state $|(\alpha+\beta)/2\rangle$. Alice's best strategy is to send a signature where the number of mismatches is halfway between the authentication and verification thresholds, which leads to her probability of successful repudiation being negligible in terms of $s_v - s_a$, p_{USD} and L.

In order for Bob to forge a message, Bob must guess the bits that he was not able to unambiguously get from Alice, yet Charlie was able to. The probability of this is negligible in terms of s_c, p_{USD} and L. Bob's other option is to send wrong states through the multiport, which Charlie can also defend against by aborting if too many photons are seen through his null output.

C. Quantum Digital Signatures using QKD

Wallden et al. [16] developed an improved QDS that didn't require a multiport. This scheme uses quantum state elimination [17] to build trust in Alice's signature. The protocol is explained below, using $|0\rangle, |1\rangle, |+\rangle = (|0\rangle+|1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle-|1\rangle)/\sqrt{2}$ as the BB84 [5] states:

Key Generation: Alice generates pairs $(k_l^0, k_l^1), 0 \leq l < L$ where $k \in \{0, 1, +, -\}$ is chosen at random. She then generates two copies of the states $\bigotimes_{l=0}^{L-1} |k_l^0\rangle$ and $\bigotimes_{l=0}^{L-1} |k_l^1\rangle$ to act as her verification keys.

Key Distribution: Alice sends copies of the verification keys to Bob and Charlie, who pick between $L/2 - r$ and $L/2 + r$ indices $0 \leq l < L$ and bits $b \in \{0, 1\}$ for some r and sends $(l, b, |k_l^b\rangle)$ to the other party, aborting if they receive a number of tuples outside that limit. Bob and Charlie then measure all their qubits in either the $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle |-\rangle\}$ bases. Bob and Charlie use the outcome of these measurements to note what states the key *cannot* be.

Message Signing: For a message b, Alice sends the signed message $(b, k_0^b k_1^b ... k_{L-1}^b)$.

Message Verification: To verify the signed message $(b, k_0^b k_1^b ... k_{L-1}^b)$, Bob checks how many of the symbols in the signing key are in the set of values they eliminated from measurement and accepts if this number is smaller than $s_a L$.

Because Alice does not know which qubits Bob measured and which he forwarded to Charlie (and vice versa), she gains no repudiation advantage from sending different states to them. There is also a negligible chance of forgery, as even if Bob faked the qubits he forwarded to Charlie, he would still need to guess the qubits that Charlie *didn't* forward to him.

D. Removing the need for Authenticated Quantum Channels

QDSs were finally proposed without authenticated quantum channels in two papers: one by Yin, Fu and Chen [18] and one by Amiri et al. [19]. The latter paper will be the focus of this section.

This signature scheme relies on a key generation protocol (KGP). Based upon BB84 [5], the KGP between Alice and Bob is described below:

1. Bob generates qubits in either $|0\rangle, |1\rangle, |+\rangle$ or $|-\rangle$ states and forwards these states to Alice.

2. Alice measures each state in either the X or Z basis, noting her chosen basis and results.

3. Alice and Bob publicly announce their choice of bases and keep results that were measured in the same basis. Steps 1-3 are repeated until enough shared bits are produced.

4. Bob divides his key up into four parts of equal size:

   - The first part, V, are results from X basis measurements, and will be compared with the corresponding bits from Alice to see how much correlation they have.
   - The second part, Z, are results from Z basis measurements, and will be compared with Alice's corresponding bits to determine eavesdropper activity.
   - The third part, C^B are bits that are forwarded on to Charlie.
   - The fourth part, B are the bits that Bob keeps for his own private key. Alice and Bob discard the bits in the first two parts.

5. If there is not enough correlation or the difference in the amount of correlation between the V and Z bits is too high, then the protocol is aborted.

6. Otherwise, Bob and Charlie exchange their parts of the keys through a secure classical channel.

This protocol allows Alice to generate highly correlated keys with the recipients. We use this to construct a QDS below:

Key Generation/Distribution: Bob and Charlie use the key generation protocol to generate two L-bit keys with Alice, half of each key being exchanged with the other party. Alice's copies of the keys are denoted A_0^B, A_1^B, A_0^C and A_1^C, where B (resp. C) denotes Bob (resp. Charlie). Bob and Charlie have their own keys with Alice B_0, B_1 & C_0, C_1 and their keys from each other B_0^C, B_1^C & C_0^B, C_1^B, respectively.

Message Signing: To sign a bit b, Alice sends (b, A_b^B, A_b^C).

Message Verification: Given (b, A_b^B, A_b^C), Bob checks the number of mismatches between A_b^B and B_b and the number of mismatches between A_b^C and B_b^C. If the total number of mismatches is above $s_a L/2$ then the message is rejected. Otherwise the message is accepted.

This signature is a more general version of protocol P2 from [16]. While the protocol described above uses a key generation protocol that creates correlated bit strings between parties, protocol P2 uses already shared keys which perfectly match.

Like the protocol in SEC. IV C, security against repudiation is offered as Alice does not know which bits of their respective keys Bob and Charlie passed on to each other.

For Bob to forge a message to send to Charlie, he needs to guess the values of the bits that Charlie did not forward on to him, which is negligible for the same reason as in SEC. IV C. Bob has the highest chance of success if he eavesdrops on the key generation protocol between Alice and Charlie, which he now can given that the channel is not authenticated. If Bob regularly guesses the wrong qubit to forward to Alice, this will result in low correlations between Alice and Charlie's measurements in the X or Z basis. Thus when Alice and Charlie look at the correlations between their V and X parts of their keys, they will either find low correlations in V or a large difference between the number of correlations in V and the number of correlations in X. Either way, the protocol will be aborted.

V. EXPERIMENTAL ACHIEVEMENTS

Although there are a number of difficulties in these QDSs, experimental results have been developed with compromises. Some of these results are discussed below.

One of the earliest experimental results was in 2012 by Clarke et al. [20]. This experiment encoded qubits in the phase of coherent light, created using an attenuated pulsed laser at an 850 nm wavelength. The states created were of the form $\{|\alpha e^{2i\pi p/N}\rangle | p = 0, 1, ..., N\}$ by use of a Mach-Zender interferometer with a controllable phase modulator.

Rather than implement a distributed SWAP test, Alice's pulsed laser is sent through a beamsplitter, the outputs of which are passed through a multiport to Bob and Charlie. A phase modulator was placed between Alice's beamsplitter output and Bob's multiport input to test repudiation. To avoid the use of quantum memory, Bob and Charlie measured their received photons immediately using a Mach-Zender interferometer, phase modulator and Silicon Single Avalanche Photo-Diode (Si-SAPD), noting basis and result. When Alice sends her message and a classical description of the signature state, Bob and Charlie check if it is consistent with their measurement results.

Clarke et al. saw that the gap between the probability of a successful signature – assuming honest players – and the probability of a successful forgery by Bob for their system was $g = 8.03 \times 10^{-4} \pm 0.3 \times 10^{-4}$. The primary reasons for a gap this small were the low count rates at the detectors, which had losses of 7.5 dB at the multiport null-ports and 7.1 dB during measurement. The overall detection efficiency of the experiment ranged from $36 - 42\%$.

A later paper, by Collins et al. [21], implemented the signature from SEC. IV B. This experiment largely used the same setup as [20], but Bob and Charlie's measurements were now two Mach-Zender interferometers separated by a beamsplitter: one to measure $\{|\alpha\rangle, |\alpha e^{i\pi}\rangle\}$ and one to measure $\{|\alpha e^{i\pi/2}\rangle, |\alpha e^{3i\pi/2}\rangle\}$. These were the qubit encodings used by Alice in this experiment. Another difference is that Collins et al. used unambiguous state elimination for checking the signatures.

Sadly, the gap was even smaller, at most 1.2^{-6}. For this protocol to fail with probability at most 0.01% for a one-bit message, this would require a signature key of 5.1×10^{13} qubits. To reduce this number, suggestions made by the authors include finding optimal photon numbers for state elimination, switching to protocols that do not require a multiport, and increasing clock speeds.

The final paper was by Donaldson et al. [22], where they demonstrated a QDS across $500 - 2000$ m of fibre. The distance limitations with the previous experiments were caused by the multiport, which restricted the transmission distance to 5 m. In this paper, the multiport is removed and repudiation is stopped by Bob & Charlie taking measurements and forwarding results to each other.

When the sender and receiver were separated by 500m of fibre, the gap was at most 2.86×10^{-4}. For a failure probability of at most 0.01%, this requires a signature of 1.93×10^{9} qubits. At the 100MHz pulse rate this experiment was operating at, one signature would take approximately 20s. This signature length increased as the distance increased, but at 2000m was still four orders of magnitude smaller than what was required in [21]. But this is still not practical in comparison to QKD or classical digital signatures. Suggested improvements include changing to 1550 nm wavelength lasers, which have lower losses in telecommunications fibres – 0.2 dB km^{-1} instead of 2.2 dB km^{-1} – as well as better detectors, such as semiconductor [23] or even superconducting [24] detectors.

VI. CONCLUSION AND DISCUSSION

While quantum key distribution has the potential to be significantly beneficial over classical encryption alone, secrecy is only a mere facet of cryptography. To quote the CESG white paper [8], "modern services [...] rely more on authentication and integrity mechanisms, such as digital signatures, than on encryption." Secrecy is not enough.

Despite only being proposed in 2001, QDSs have come a long way. While Gottesman and Chuang's original scheme [10] had many practical limitations, many of these have now been fixed, particularly following the work of Yin, Fu and Chen [18] and Amiri et al. [19]. But these protocols can still be improved. While both protocols do not require quantum channel authentication, Amiri et al.'s is still dependent on authenticated classical channels, but it is much less certain how Yin, Fu and Chen's will scale with participants, particularly to prevent collusion attacks.

Experimentally, proof of principle QDSs have been demonstrated using phase-encoded coherent states of light. However, the length of keys required in order to currently provide safe levels of security is impractical, taking 20 s to establish and share the keys for signing and verifying a single bit. By incorporating advances in optical devices such as improved single photon detectors, QDSs will hopefully advance to being on par with QKD.

[1] R. L. Rivest, A. Shamir, and L. Adleman, Commun. ACM **21**, 120 (1978).
[2] P. W. Shor, SIAM Review **41**, 303 (1999).
[3] E. Martin-Lopez, A. Laing, T. Lawson, R. Alvarez, X.-Q. Zhou, and J. L. O'Brien, Nat. Photon. **6**, 773 (1999).
[4] R. Dridi and H. Alghassi, "Prime factorization using quantum annealing and computational algebraic geometry," (2016), arXiv:1604.05796.
[5] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984) pp. 175–179.
[6] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Journal of Cryptology **5**, 3 (1992).
[7] `http://www.idquantique.com/`.
[8] CESG, *Quantum Key Distribution*, White Paper (GCHQ, Cheltenham, UK, 2016).
[9] L. Lamport, Technical Report SRI-CSL-98 (1979).
[10] D. Gottesman and I. Chuang, "Quantum digital signatures," (2001), arXiv:quant-ph/0105032.
[11] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).
[12] A. S. Holevo, Problems of Information Transmission **9**, 3 (1973).
[13] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).
[14] V. Dunjko, P. Wallden, and E. Andersson, Phys. Rev. Lett. **112**, 040502 (2014).
[15] I. Ivanovic, Physics Letters A **123**, 257 (1987).
[16] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Phys. Rev. A **91**, 042304 (2015).
[17] S. Bandyopadhyay, R. Jain, J. Oppenheim, and C. Perry, Phys. Rev. A **89**, 022336 (2014).
[18] H.-L. Yin, Y. Fu, and Z.-B. Chen, Phys. Rev. A **93**, 032316 (2016).
[19] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Phys. Rev. A **93**, 032325 (2016).
[20] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. (2012).
[21] 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).
[22] 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).
[23] G. S. Buller and R. J. Collins, Measurement Science and Technology **21**, 012002 (2010).
[24] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, Superconductor Science and Technology **25**, 063001 (2012).