Quantum Digital Signatures

Dominic Moylett*
Quantum Engineering Centre for Doctoral Training
University of Bristol

(Dated: May 27, 2016)

I. INTRODUCTION

Cryptography is the study of secure communication between parties, often called Alice and Bob. In classical cryptography, this security is guaranteed through assumed hardness. RSA [1], for example, assumes that factoring integers is hard. Unfortunately, several of these problems have been proven easy in both theory [2] and practice [3, 4] on quantum computers.

But quantum physics can also fix secrecy. Quantum Key Distribution (QKD) protocols such as BB84 [5] can establish a shared key with information theoretical security. Once Alice and Bob have a shared key, they can send messages such that an eavesdropper, Eve, cannot learn anything about their communications. This has also been demonstrated experimentally [6, 7] and now companies [8] offer commercial QKD.

But secrecy is only part of cryptography. Even if Alice and Bob have perfect secrecy, Eve could send a message of random gibberish to Bob pretending to be Alice's ciphertext. Alternatively, Eve might pretend to be Bob throughout the QKD protocol, fooling Alice into sending her message to Eve. This is one of the arguments in a CESG white paper concluding 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" [9].

The extra precautions required to prevent these attacks are signatures. Like how someone signs a letter, a digital signature is additional data to indicate authorship of a message. And like classical encryption, classical signatures rely on assumed hardness.

Based on the improvements in secrecy, one might ask if quantum physics can also benefit digital signatures. That is the subject of this essay. In SEC. II, we offer a definition of digital signatures. SEC. III describes a well-known classical digital signature, followed by quantum digital signatures (QDSs) in SEC. IV. Experimental results are highlighted in SEC. V. Finally, we conclude with some points of discussion.

II. DEFINITION OF DIGITAL SIGNATURES

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 Authentication: 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 possible issues:

Honest Abort: All participants are honest yet the protocol aborts anyway.

Repudiation: Alice creates a message that Bob accepts yet Charlie rejects.

Forgery: Bob creates a message that Charlie is convinced was signed by Alice.

The probability for any of the above events happening should be negligible:

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

III. LAMPORT'S ONE-TIME DIGITAL SIGNATURE

The original quantum digital signature was inspired from a classical family of digital signatures by Lamport[10], which use 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 signature is defined for an m-bit message below:

Key Generation: Alice's signing key is a pair of uniformly selected integers (k_0^i, k_1^i), and her verification key is the pairs $(f(k_0^i), f(k_1^i))$, for $i \in \{1, ..., m-1\}$.

Message Signing: For the i-th bit b_i, Alice sends k_{b_i} as her signature for that bit.

* dominic.moylett@bristol.ac.uk

Message Authentication: Given Alice's verification key and (m_{b_i}, k_{b_i}), Bob accepts if $v_{b_i} = f(k_{b_i})$ for all $i \in \{0, ..., m-1\}$.

Because this signature scheme is classical and deterministic, recipients can compare copies of the signed message and keys, so Alice cannot repudiate.

If an attacker has two different signed messages M, M' then they can construct a signature for the message $m_0 m_1 ... m'_i ... m_{m-1}$, where $m_i \neq m'_i$. So this scheme is only secure for 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 threshold for Bob authenticating a message from Alice directly, and $1/2 > s_v > s_a$ is the threshold for Charlie verifying a message from Alice forwarded by Bob. The step for verifying a forwarded message is the same as that for authenticating a message, the only difference being use of s_v instead of s_a.

A. Gottesman and Chuang

The first QDS was by Gottesman and Chuang [11]. The protocol is similar to Lamport's signature scheme, but used quantum one-way functions mapping L-bit strings k to n-qubit states $|f_k\rangle$. The protocol is described below for a single bit, where f is the quantum one-way function and $T < L/n$ is the number of copies of each key:

Key Generation: Alice generates pairs of L-bit strings $\{k_0^i, k_1^i\}, i \in \{0, ..., M-1\}$ uniformly at random for her signing key. Her verification key is $(|f_{k_0^i}\rangle, |f_{k_1^i}\rangle), i \in \{0, ..., M-1\}$.

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

Message Authentication: Given $(b, k_b^0, k_b^1, ..., k_b^{M-1})$, a recipient uses f and SWAP tests [12] 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, and if $s > s_v M$ then the recipient rejects the message. In the case where $s_a < s \leq s_v$, the recipient concludes the message is valid but not transferable.

Security against forgery is possible due to Holevo's theorem [13], 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 making a recipient accept a guessed signature is at most δ^2. By choosing s_v smaller than the probability of an adversary being accepted $(1-\delta^2)(1-2^{1-(L-Tn)})$, we ensure that each recipient most likely rejects the forgery.

It is harder to protect against repudiation, because if Alice sends Bob and Charlie nonorthogonal states, then 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, 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 enough tests fail then the protocol is aborted, otherwise the test keys are discarded and the protocol continues.

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 is negligible in terms of $s_v - s_a$ and L.

While Lamport's signature assumes the existence of 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. [12] which leads to a negligible probability of forgery. However, there are a number of disadvantages:

1. Verification keys cannot be copied due to the no-cloning theorem [14], 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 in long-time quantum memory until Alice signs a message.

3. Generating and sharing a quantum one-way function 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 [15], who removed the quantum memory,

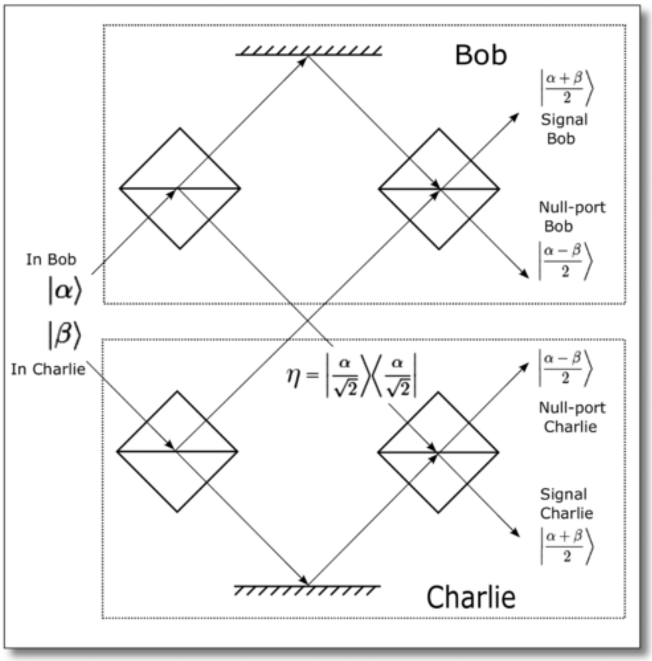
Bob
$\left|\frac{\alpha+\beta}{2}\right\rangle$
Signal
Bob
Null-port
Bob
$\left|\frac{\alpha-\beta}{2}\right\rangle$
In Bob
$|\alpha\rangle$
$|\beta\rangle$
In Charlie
$\eta = \left|\frac{\alpha}{\sqrt{2}}\right\rangle\left\langle\frac{\alpha}{\sqrt{2}}\right|$
$\left|\frac{\alpha-\beta}{2}\right\rangle$
Null-port
Charlie
Signal
Charlie
$\left|\frac{\alpha+\beta}{2}\right\rangle$
Charlie

FIG. 1. Design of a multiport. If $|\alpha\rangle = |\beta\rangle$ then $|(\alpha-\beta)/2\rangle = |0\rangle$, thus we would expect the vaccum state from the null-port. Figure from [15].

the quantum SWAP test and quantum one-way functions. Their protocol for three parties is below, using coherent states of light:

Key Generation: Alice generates two L-bit keys k^0, k^1, which are Alice's signing keys. Alice then generates states of the form $|(-1)^{k_l^b}\alpha\rangle, l \in \{0, ..., L-1\}, b \in \{0,1\}$, where α is a public positive real number and k_l^b is the l-th bit of k^b. These quantum states are 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 (see FIG. 1). For states which come out the signal port, they then use Unambiguous State Discrimination (USD) [16] to distinguish the states $\{|-\alpha\rangle, |\alpha\rangle\}$, and for each unambiguous result $|(-1)^{k_l^b}\alpha\rangle$ note the value of k_l^b, the index l and b.

Message Signing: To sign a bit b, Alice sends (b, k^b).

Message Authentication: Given 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, accepting if the number of mismatches is at most $s_a p_{USD} L$, where p_{USD} is the USD success probability.

The multiport prevents repudiation; 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 $|(\alpha+\beta)/2\rangle$. 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 repudiation being negligible in terms of $s_v - s_a$, p_{USD} and L.

To commit forgery, Bob must guess the bits that he was not able to unambiguously determine 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 detect by aborting if too many photons are detected through his null-port.

C. Quantum Digital Signatures using QKD

Wallden et al. [17] improved the QDS by removing the multiport. This scheme uses quantum state elimination [18] 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's signing keys are pairs $(k_l^0, k_l^1), 0 \leq l < L$ where $k \in \{0, 1, +, -\}$ is uniformly chosen. The states $\bigotimes_{l=0}^{L-1} |k_l^0\rangle$ and $\bigotimes_{l=0}^{L-1} |k_l^1\rangle$ are 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 $l \in \{0, ..., L-1\}$ and bits $b \in \{0,1\}$ for some r and send $(l, b, |k_l^b\rangle)$ to each other, aborting if they receive a number outside that limit. Bob and Charlie measure all their qubits in either the $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle\, |-\rangle\}$ bases, using the outcome of these measurements to note what states the key *cannot* be.

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

Message Authentication: Given $(b, k_0^b k_1^b ... k_{L-1}^b)$, Bob checks how many of the symbols in the signature are in the set of symbols he eliminated, accepting if this is fewer 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; 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. Insecure Quantum Channels

QDSs without authenticated quantum channels were proposed in two papers: one by Yin, Fu and Chen [19] and one by Amiri et al. [20]. Our focus is the latter paper.

This signature scheme uses a key generation protocol (KGP) based upon BB84 [5]. The KGP is described below:

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

2. Alice measures each state in either the X or Z basis, noting her 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 bits are produced.

4. Bob divides his key up into four parts of equal size:
   - The first part are results from X basis measurements, and will be compared with the corresponding bits from Alice.
   - The second part are results from Z basis measurements, and will be compared with the corresponding bits from Alice.
   - The third part are bits that are forwarded on to Charlie.
   - The fourth part are bits that Bob keeps.

5. If there is not enough correlation or the difference in correlation between the X and Z measurements is too high, then the protocol is aborted.

6. Alice & Bob discard their correlation measurement bits and Bob & Charlie exchange their parts of the keys through a secure classical channel.

We use this KGP 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 forwarded to the other party. Alice's copies of the keys are denoted $A_0^B, A_1^B, A_0^C, A_1^C$, 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 Authentication: Given (b, A_b^B, A_b^C), Bob checks the number of mismatches between A_b^B & B_b and the number of mismatches between A_b^C & B_b^C. If the total number of mismatches is below $s_a L/2$ then the message is accepted.

This QDS is a more general version of protocol P2 from [17]. While the protocol described above uses a key generation protocol that creates correlated bit strings between parties, protocol P2 uses already shared keys.

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

For Bob to forge a message, he needs to guess the bits that Charlie kept. Bob has the highest chance of success if he eavesdrops on the key generation protocol between Alice and Charlie, which he can as the quantum channel is insecure. If Bob regularly guesses the wrong qubit to forward to Alice, this will give low correlations between Alice and Charlie's measurements. When Alice and Charlie look at their correlations, they will either find low correlations in X measurements or a large difference between the number of correlations in X and Z. 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 results are discussed below.

One of the earliest experimental results was in 2012 by Clarke et al. [21]. This experiment encoded qubits in the phase of coherent light, created using an attenuated pulsed laser at an 850 nm wavelength. The states were of the form $\{|\alpha e^{2i\pi p/N}\rangle | p = 0, 1, ..., N\}$, generated by a Mach-Zender interferometer with a controllable phase modulator.

Rather than implement a distributed SWAP test, Alice's pulsed laser is passed through a multiport to Bob and Charlie. A phase modulator was placed between Alice's output and Bob's multiport input to test repudiation. To avoid needing quantum memory, Bob and Charlie measured their received photons immediately using a Mach-Zender interferometer, a controllable 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 measurements.

Clarke et al. saw that the gap between the probability of a successful signature for honest players and the probability of a successful forgery by Bob for their system was $8.03 \times 10^{-4} \pm 0.3 \times 10^{-4}$. 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 ranged from $36 - 42\%$.

A later paper by Collins et al. [22] implemented the signature from SEC. IV B. This experiment largely used the same setup as [21], but Bob and Charlie's measurements now used two Mach-Zender interferometers separated by a beamsplitter: one to measure $\{|\alpha\rangle, |\alpha e^{i\pi}\rangle\}$ and one to measure $\{|\alpha e^{i\pi/2}\rangle, |\alpha e^{3i\pi/2}\rangle\}$, which were the qubit encodings used by Alice. Another difference is that Collins et al. used unambiguous state elimination instead of USD.

Sadly, the gap was even smaller, at most 1.2^{-6}. For this protocol to fail with probability at most 0.01% when signing a one-bit message, this would require a verification 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. [23], 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 prevented by Bob & Charlie taking measurements and forwarding the results to each other.

When the sender and receiver were separated by 500 m 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 100 MHz pulse rate this experiment was operating at, one signature would take approximately 20 s. This signature length increased as the distance increased, but at 2000 m was still four orders of magnitude smaller than what was required in [22]. But this is still not on par with QKD or classical 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 [24] or even superconducting [25] detectors.

VI. CONCLUSION AND DISCUSSION

To quote the CESG white paper again [9], "modern services [...] rely more on authentication and integrity mechanisms, such as digital signatures, than on encryption." While quantum key distribution has the potential to be significantly beneficial over classical encryption alone, secrecy alone is not enough.

Despite only being proposed in 2001, QDSs have come a long way. Gottesman and Chuang's original scheme [11] had many practical limitations, but many of these have now been fixed, particularly following the work of Yin, Fu and Chen [19] and Amiri et al. [20]. But there are still limitations: While both protocols do not require quantum channel authentication, Amiri et al.'s is still dependent on authenticated classical channels, and it is unknown how to make Yin, Fu and Chen's scale with participants, particularly in order to prevent collusion attacks.

Experimentally, proof of principle QDSs have been demonstrated using phase-encoded coherent states of light over growing distances. However, the length of keys required in order to currently provide safe levels of security is impractical, taking 20 s to generate 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 further towards being on par with QKD.

Finally, it is worth noting one more weakness of QDSs: They are only secure for signing a single message. This means that all of the (quantum and classical) communication to establish keys must be repeated for every single bit. Classically, such overhead is avoided by using signatures which reuse keys, such as the Digital Signature Algorithm [26]. Such a property is sadly not trivial, if possible, in quantum digital signatures.

[1] R. L. Rivest, A. Shamir, and L. Adleman, Communications of the 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, Nature Photonics **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] P. Sibson, M. Godfrey, C. Erven, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. O'Brien, and M. G. Thompson, in *CLEO: 2015* (Optical Society of America, 2015) p. FF1A.6.

[8] `http://www.idquantique.com/`.

[9] CESG, *Quantum Key Distribution*, White Paper (2016).

[10] L. Lamport, Technical Report SRI-CSL-98 (1979).

[11] D. Gottesman and I. Chuang, "Quantum digital signatures," (2001), arXiv:quant-ph/0105032.

[12] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Physical Review Letters **87**, 167902 (2001).

[13] A. S. Holevo, Problems of Information Transmission **9**, 3 (1973).

[14] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[15] V. Dunjko, P. Wallden, and E. Andersson, Physical Review Letters **112**, 040502 (2014).

[16] I. Ivanovic, Physics Letters A **123**, 257 (1987).

[17] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, Physical Review A **91**, 042304 (2015).

[18] S. Bandyopadhyay, R. Jain, J. Oppenheim, and C. Perry, Physical Review A **89**, 022336 (2014).

[19] H.-L. Yin, Y. Fu, and Z.-B. Chen, Physical Review A **93**, 032316 (2016).

[20] R. Amiri, P. Wallden, A. Kent, and E. Andersson, Phys-

ical Review A **93**, 032325 (2016).

[21] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nature Communications (2012).

[22] 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).

[23] 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).

[24] G. S. Buller and R. J. Collins, Measurement Science and Technology **21**, 012002 (2010).

[25] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, Superconductor Science and Technology **25**, 063001 (2012).

[26] D. Kravitz, *Digital signature algorithm*, US Patent 5,231,668 (1993).