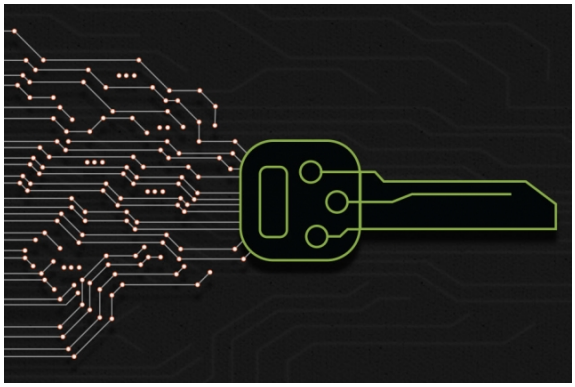
Quantum Digital Signatures

Sajeda Mokbel
20609975



PHYS 467 - Introduction to Quantum Computing
Taught by Dr. Michele Mosca
Department of Physics and Astronomy
University of Waterloo
Waterloo, ON
17th April 2020

Contents

Abstract

In this review, based on Gottesman and Chuangs *Quantum Digital Signatures*, a quantum digital signature scheme is proposed that is in compliance with the fundamental theories of quantum mechanics. A sender, Alice, is able to sign a message and have it validated by a number of recipients, who will collectively agree on whether the message came from Alice or if it has been invalidated by a third party. Each recipient receives a copy of Alice's public key - which is a set of unknown quantum states, with only Alice knowing their exact identity. The distribution of the keys is limited to avoid an insecurity. The report discusses how to avoid potential security issues that will arise with the quantum analogue of the scheme, by detailing specific key distribution methods and security protocols. The quantum digital signature scheme provides a realistic model that transfers the key ideas of conventional public key cryptography into the quantum domain.

1 Introduction

The main goals of classical cryptography are secrecy and authentication. Secrecy assures that encrypted information is not understood to eavesdroppers while authentication verifies that information from a genuine sender is valid. This is often done through a crypotographic protocol such as digital signatures, which use public and private keys to certify the origin of a message. A private key is a random hexidecimal number that must be kept private by the account holder, and a public key is another hexidecimal number that can be shared publicly. The keys are connected to each other through a mathematical relationship, in which given a private key, it is easy to determine the public key, but with a public key, it is computationally hard to determine the private key. These schemes can be created out of any one-way function. $f(x)$ is a one-way function if it is easy to compute given x, but very difficult to retrieve x given $f(x)$. The security of all public key digital signature schemes depends on the inability of a forger to solve these mathematical problems in a realistic time period, hence, such schemes are only computationally secure, not information-theoretically secure [1]. This means that technically, all the information about the private key can be computed from the public key, it just appears to take a lot of time to compute it. This, of course, is assuming that problems like factoring primes are classically hard, and that quantum computers have not yet been built.

The conventional computers used today obey the laws of classical physics. The smallest unit of information is stored in bits, which are binary numbers equal to 0 or 1. A quantum computer generally differs with one basic element - their smallest unit of information is a *quantum* bit, which holds the advantageous feature of being in a superposition of two states - $|0\rangle$, and $|1\rangle$ at the same time. This allows a computer to follow multiple computational paths simultaneously, giving it inherent parallelism not achievable through classical computation. Thus, when it comes to cryptography, quantum computers can break conventional security schemes. The hard mathematical problems are tractable for quantum computers, allowing digital signatures to be easily forged. New cryptographic protocols must be set in order to bring security into the quantum world. A digital quantum signature scheme is introduced, based on a quantum analogue of a one-way function. Unlike classical one-way functions, this scheme is proven to be secure from an information-theoretic standpoint, regardless of the computer used.

In the paper titled *Quantum Digital Signatures*, Daniel Gottesman and Isaac L. Chuang present an absolutely secure digital signature scheme based on fundamental principles of quantum mechanics. The input of the quantum one-way function is a classical bit-string k and the output is a quantum state $|f_k\rangle$. It is shown, however, that simply replacing the

classical one-way function, $f(x)$, with $|f_k\rangle$ is insufficient. Due to the no cloning theorem [2], which proves that it is impossible to create an identical copy of an unknown state, a perfect equality test does not exist. The nature of quantum states also allows the signer, Alice, to get away with cheating strategies. A limited number of public keys can be distributed before the scheme looses security. The protocol presented is demonstrated with a specific security and key distribution scheme, that will make the probability of these challenges occurring exponentially small. Thus, the quantum digital signatures protocol presented by Gottesman and Chuang is a reliable cryptographic solution for quantum computers.

1.1 Classical digital signature scheme

Classical digital signature schemes can be created out of any one-way function [1]. A digital signature can be described as follows: Alice, the sender, chooses k_0 and k_1 as her private keys, and publicly announces function f, and the pairs $(0, f(k_0))$, and $(1, f(k_1)$. Then, when Alice wants to *sign* a bit b, she presents (b, k_b) [1]. The reciever can easily compute $f(k_b)$ from this information, and they can confirm it was sent from Alice due to her previous public announcements, since only she knew k_0 and k_1 [1].

2 Quantum one-way functions

A quantum one-way function is introduced, which takes advantage of two properties [1] of quantum systems: (i) the ability to have a set of basis states exponentially larger than the number of qubits, and (ii) the inability to invert the mapping $k \rightarrow |f_k\rangle$ without knowing k. The general state of one qubit can be written as a two component vector: $\alpha_0 |1\rangle + \alpha_1 |1\rangle$, where $|1\rangle$ and $|0\rangle$ form an orthonormal basis for the state. Hence, in a general sense, n qubits exist in 2^n different states. For instance, 3 qubits $|a_1 a_2 a_3\rangle$ have the set of states $\{|000\rangle, |001\rangle, |011\rangle .. |111\rangle\}$, which add up to be a set of size 2^3. The key idea here is that qubits can exist in a number of states, exponentially larger than the size of qubit system.

2.1 Size of basis states

The distance between two states is defined as $d = \sqrt{1 - |\langle\phi| |\phi'\rangle|^2}$, and is a non-integer value less than the maximum 1. The set of states $\{|\phi^n\rangle\}$ exist satisfying $|\langle\phi_k^n| |\phi_{k'}^n\rangle|, k \neq k' \leqslant \delta$, and can have many more than 2^n states if $\delta < 1$, i.e., when the states are not maximally distant from eachother. Results from a quantum fingerprinting [3] experiment actually proved that for $\delta \approx 0.9$, the set will be of size $2^{O(2^n)}$. This is a key result made use of in this paper. Classical bit strings k of length L will each be assigned a state $|f_k\rangle$ of n

qubits. As proven by Buhrman et. al [3], L = $O(2^n)$ with $\delta \approx 0.9$. This set of states is easily created using universal quantum gates [1].

2.2 Holevo's theorem

A fundamental theorem of quantum information theory, Holevo's theorem, makes it impossible to retain a classical bit string k from a quantum state $|f_k\rangle$ [4]. Although the mapping from $k \rightarrow |f_k\rangle$ is easy to compute, it is not possible to compute $|f_k\rangle$ from k. Holevo's theorem puts an upper limit on how much classical information can be contained in a quantum system [4]. One qubit can contain at most one classical bit of information. As mentioned above, the proposed system will have classical bit strings k of length L, each one being assigned a state $|f_k\rangle$ of n qubits [1]. Thus, given x copies of of the state $|f_k\rangle$, the largest amount of bits of information we can learn from string k is xn. Since $L >> xn$, the chance of successfully guessing the string k is exponentially small. This proves that the $k \rightarrow |f_k\rangle$ system acts as a quantum one-way function, with a classical input and quantum output [1].

2.3 Workarounds

Certain properties of classical one way functions that are straightforward are no longer so with the quantum analogue. Firstly, to ensure two outputs $|f_k\rangle$ and $|f_{k'}\rangle$ are the same, a quantum circuit must be established to do so (figure 1). This circuit acts as a SWAP test [1], with the ancilla as the control state and $|f_k\rangle$ and $|f_{k'}\rangle$ as targets. Then, a Hadamard is applied on the ancilla and its state is measured.

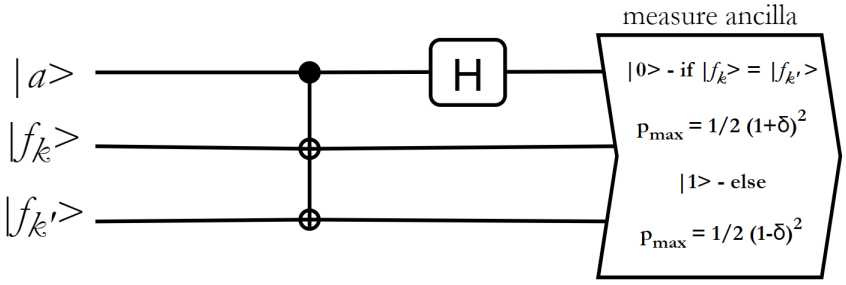


Figure 1: SWAP test for verification procedure. The ancilla, $|a\rangle = \frac{1}{2}(|0\rangle + |1\rangle)$, acts as the control state for a Fredkin gate (controlled-SWAP) with $|f_k\rangle$ and $|f_{k'}\rangle$ as the targets.

If the measured result is $|0\rangle$, then the swap test is passed - this happens indefinitely when $|f_k\rangle = |f_{k'}\rangle$. If $\langle f_{k'}|f_k\rangle| \leqslant \delta$, the result $|0\rangle$ will occur with a maximum probability of $\frac{1+\delta^2}{2}$. If the result is $|1\rangle$, the test fails and this only occurs if $k \neq k'$ with a probability of $\frac{1-\delta^2}{2}$ [1]. The main takeaway is that the classical equality test can be recreated for the quantum scheme, but it fails with a non-zero probability [1].

Another key property required for the quantum one-way function, is the ability to verify its output. Given string k, one must be able to ensure that the output state $|\phi\rangle = |f_k\rangle$. This is pretty straightforward, since $|k\rangle|0\rangle \rightarrow |k\rangle|f_k\rangle$, where $|0\rangle$ is the n qubit state, the inverse operation can be applied, and the second register measured. If $|\phi\rangle \neq |f_k\rangle$, the measurement will be non-zero with a $1 - |\langle\phi||f_k\rangle|^2$ [1]. Verification is once again probabilistic.

3 Quantum digital signature

3.1 Challenges

Many challenges arise if one naively tries to replace a classical one way function output, $f(x)$, with $|f_k\rangle$. Imitating the classical quantum scheme with the $|f_k\rangle$ state is not effective considering the probabilistic results of verification tests. Descriptively, Alice would generate k_0 and k_1 as her private keys and publicly announce the keys $(0, |f_{k_0}\rangle), (1, |f_{k_1}\rangle)$. She signs a bit b and presents $(b, |k_b\rangle)$ to the recipient, Bob. Bob now has to validate the key, by checking that $|k_b\rangle|f_{f_b}\rangle \rightarrow |k_b\rangle|0\rangle$. After he validates it, he must pass it on to another friend, Charlie, to confirm its validity. The issue is that, as mentioned above, Bob's test is possible, but it is probabilistic so it will sometimes fail. Additionally, it irreversibly consumes one of Alice's keys [1]. Alice also now has the ability to pursue quantum cheating strategies. Since the keys cannot be validated with 100% certainty, Alice can hand out public keys that are not necessarily identical. Alice can also prepare entangled states, where she can delay choosing k until after she has given $|f_k\rangle$ away. This means measurements can always be postponed in an undetectable way, making bit commitment impossible [5]. Another major potential problem that arises is that $|f_k\rangle$ always leaks some information about the classical input, k, as explained by Holevo's theorem. Luckily, Alice is the *only* person who has the ability to play cheating games, which is not necessarily beneficial to her as it would be to a third party eavesdropper. Thus, quantum one-way functions can still be used for digital signatures. Most of these issues can be resolved by using multiple public keys per message bit rather than just one [1].

3.2 Quantum Digital Signature Protocol

The quantum digital signature protocol is described in detail, beginning with the main goal of the protocol and how to evaluate its security. The usual idea of a one-use digital signature is adapted, meaning Alice will have a set of private keys and the recipients will hold the corresponding public keys. Alice will produce a single signed message, $(b, s(b))$, and the recipients will process the message and signature pair to reach any one of the conclusions in Figure 2.

A message is only transferable if a recipient can be sure that all other recipients will also

1-ACC	Message is valid and can be transferred
0-ACC	Message is valid but it might not be transferable
REJ	Message is not valid

Figure 2: Recipient validation conclusions

agree that the message is valid. The result **REJ** occurs when the recipient cannot reach a conclusion about the authenticity of the message. The goal is for any recipient receiving the correct message to always reach the **1-ACC** conclusion.

3.2.1 Security criteria

The protocol should follow two main security criteria [1]:

1. It should be secure against forging
2. It should be secure against the senders attempts to cheat the message

The protocol presented should be secure against forging, meaning that given access to a signed message, $(b, s(b))$, no eavesdropper has a meaningful chance in creating a message/signature pair (b', s') such that an honest recipient will accept it with a **1-ACC** or **0-ACC** outcome. The protocol must also be secure against Alice's (the senders) cheating strategies. This means the first recipient, Bob, must reach a **1-ACC** conclusion and Charlie must conclude either **1-ACC** or **0-ACC**.

This scheme differs from the classical scheme in three main aspects: (i) The **0-ACC** result usually does not exist in classical digital signatures, (ii) the security criteria only hold with high probability instead of full certainty, and (iii) the public keys are quantum states rather than classical strings.

3.2.2 Quantum signature protocol specification

The private keys of this protocol are a number of pairs of L-bit strings $(k_0^i, k_1^i), 1 \leqslant i \leqslant M$, chosen independently for each i. The ks are used to sign messages $b = 0$ and $b = 1$, respectively. M keys are used to sign each bit rather than just single keys, and acts as a security parameter - if all other parameters are fixed, the states will be exponentially secure in M [1]. The i-dependent states $\{\left|f_{k_0^i}\right\rangle, \left|f_{k_1^i}\right\rangle\}$ will act as Alice's public keys for the quantum one-way function f. The no cloning theorem makes it impossible to perfectly copy unknown quantum states [1]. Thus, Alice must create these keys herself or allow someone she trusts to make them. First, the assumption is made that all recipients have received the correct, identical public key copies.

The protocol participants can easily map $k \rightarrow |f_k\rangle$, and will also know two constants - c_1, c_2 which are the thresholds for acceptance and rejection, respectively. To send a single-bit message, Alice uses the following procedure [1]:

1. She sends a signed message $\{b, |k_b^1\rangle .. |k_b^M\rangle\}$ over the public channel, revealing the identity of half of her keys
2. The recipients of the signed message check all of the public keys to verify that $k_b^i \rightarrow \left|f_{k_b^i}\right\rangle$. The last recipient j will count the number of incorrect keys
3. Recipient j will either accept the message as **1-ACC** or **REJ**. If the number of incorrect keys, s, is $\leqslant c_1 M$, the message is accepted and transferred. If $s \geqslant c_2 M$, the message is invalid, resulting in **REJ**. If $c_1 M < s < c_2 M$, the message is valid but not transferrable, **0-ACC**.

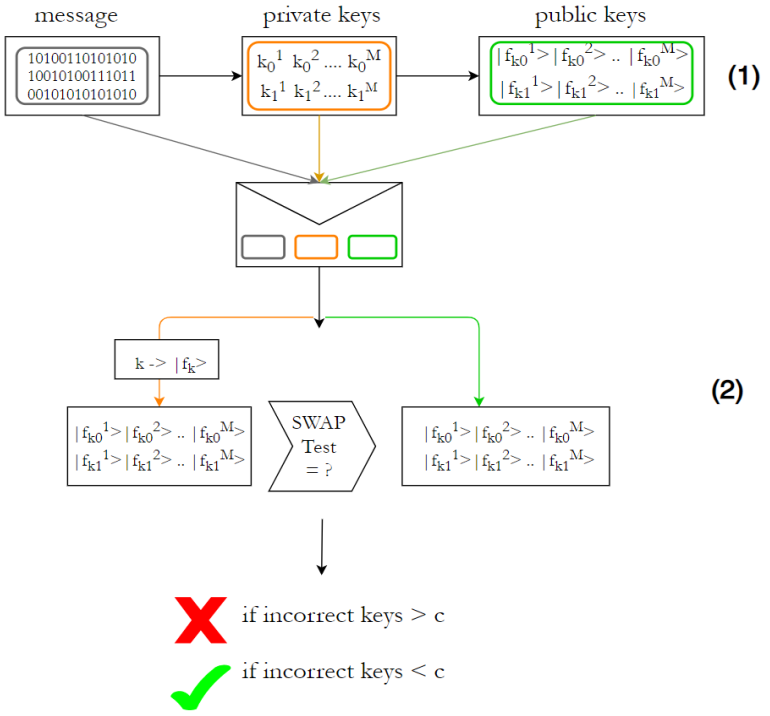


Figure 3: (1) sending process, (2) validation process, the number of incorrect keys cannot be greater than the threshold rejection constant. If it is, the message is rejected

The number of incorrect keys compared with the acceptance and rejection thresholds c_1, c_2 demonstrates how *much* a message has been tampered with. When it is relatively small, it is concluded that the message has not really changed much, and can be accepted with confidence. Section 5 details how these two threshold constants can prevent forgery and cheating by Alice. To better understand this, a key distribution scenario will first be demonstrated.

4 Key Distribution

Key distribution can be described following a particular scenario - Alice is dishonest, and wants her recipients to disagree about whether her message is valid or not. If Alice can give

different public keys to her two recipients, Bob and Charlie, she would easily achieve her goal. Thus, the signature scheme must be accompanied with a key distribution scheme that will remove Alice's ability to cheat the keys.

Broadcast channels, where public keys are broadcast to all recipients, cannot be created in a quantum scheme as a result of the no-broadcast theorem [6]. Since quantum states cannot be generally copied [2], they cannot be broadcast. Instead, the existence of a trusted key distribution center, that has links to all the recipients, is assumed. Alice sends her public keys to this distribution center, where SWAP tests are performed (see figure 1) to the pairs of public keys. If any pair fails the SWAP test, it is concluded that Alice is cheating [1]. If all tests pass, identical copies of the public key are forwarded to the recipients.

Alice is able to prepare any state she desires for the public keys - whether it is entangled states, or states outside of $|f_k\rangle$. Alice can still use her clever trickery, except now it won't be as effective. If Alice creates two keys, one valid and the other invalid, she will not be able to control *who* receives the valid key, because the distribution center will release them randomly. Thus, for a large M, the difference between the number of incorrect keys that Bob receives, s_B, and Charlie receives, s_C, is in $O(\sqrt{M})$ with high probability [1]. This means that it is very unlikely that both Charlie and Bob will get valid, differing results. If Bob accepts a message with **1-ACC**, it means $s_B < c_1 M$, Charlie would only reject the message if $s_C > c_2 M$, which is almost never. Thanks to the natural gap between $c_1 M$ and $c_2 M$, recipients are protected against cheating strategies made by Alice.

Of course, more sophisticated schemes can be set up, where the recipients, Charlie and Bob, can compare each others public keys. Each recipient can receive two copies of each of the public keys, so that a total of $T = 4$ keys are distributed. Then, for each value of i and b, the recipients can verify that they have all received the same corresponding public key, $f_{k_b^i}$. This can be achieved with each recipient first doing a SWAP test between their two keys, then passing one copy to one recipient. The single recipient, Bob, will then check that the two keys also pass the SWAP test. If any keys fail the test, the protocol is terminated, and if not, the test keys are just discarded. The keys that remain are called the **kept** keys, and are used to verify the messages in the main protocol [1].

5 Proof of security: Repudiation and Transferability

This section will explain how the proposed digital signature scheme can prevent Alice from cheating by repudiating a message she as already signed. This is done by analyzing the probability, p_{cr}, that Alice is able to pass all the SWAP tests with $|s_B - s_C| > (c_2 - c_1)M$, i.e., with Charlie and Bob obtaining opposite conclusions about the validity of the message. This

is accomplished by analyzing a global pure state $|\psi\rangle$, which describes all public keys and all of Alice's states that are entangled with the keys. Each set will have two test keys and two kept keys [1]. Any state which passes the initial SWAP tests will be symmetric between the test keys and the kept keys. A type-1 term is one that passes the SWAP test, and leaves Bob and Charlie in agreement, on average, about the validity of the keys. A type-2 term fails the swap test frequently. Thus, the most general state $|\psi\rangle$ can be written as a superposition of these two *types* of terms, $|\psi_1\rangle + |\psi_2\rangle$ [1]. Every summand in $|\psi_1\rangle$ contains at most r type-2 terms, and where $r = cM$ for $c > 0$. $|\psi_2\rangle$ contains terms with $> r$ type-2 terms [1].

Using the lemma in Appendix A of the paper [1], it is shown that, for a large M and small constant c, the probability that $|s_B - s_C| < (c_2 - c_1)M$ is still exponentially small in M for $|\psi_1\rangle$. Similarly, for $|\psi_2\rangle$, the probability of passing the SWAP test is at most $2^{-r} = 2^{-cM}$, and since c is small, this result is exponentially small in M. Although the $|\psi_1\rangle$ term has a decent chance in passing the SWAP tests, it yields and exponentially small chance of giving a meaningful separation between s_C and s_B and can be disregarded. The $|\psi_2\rangle$ term has $O(1)$ probability of $|s_B - s_C| > (c_2 - c_1)M$, but an exponentially small chance of passing the SWAP tests ($O(2^{-r})$) [1]. Putting these results together, the upper bound on p_{cr} is $\approx O(d^{-M})$ [1], for $d > 1$. Hence, Alice has a very small chance of successfully cheating by repudiation.

6 Generalizations

One generalization that can be made, is to use the distributed SWAP test with several recipients [1]. The SWAP test can be replaced with a complete symmetry test for s states. In the SWAP test described above, a controlled-ancilla is created in the state $|0\rangle + |1\rangle/\sqrt{2}$. This can instead be replaced by a superposition over states indexed by all permutations of the s elements. Then, a permutation ω can be performed, conditioned on the ancilla being in $|\omega\rangle$. The ancilla is finally measured to determine if it remains in its initial superposition [1]. This test always passes if the state of the keys that are tested are completely symmetric [1]. If not, it will sometimes fail. The distributed symmetry provides the ability to distribute the public key for $t > 2$ recipients. The validation procedure for this generalization ends up reducing to the distributed SWAP test again [1], proving that the protocol remains secure even after expanding the system to many recipients. The protocol can also be extended to multi-bit messages. This is done by repeating the process using M pairs of public keys for each message bit [1]. M will scale linearly with N, the length of the message, and the security procedures will still hold true.

7 Conclusions and future direction

In conclusion, Gottesman and Chuang successfully demonstrated the existence of an unconditionally secure public key quantum digital signature scheme. However, many opportunities for improvement remain. The biggest challenge would be with scaling the system - unlike the classical scheme, when many public keys are distributed, if this happens in the quantum scheme, recipients can take careful measurements to determine the corresponding state, destroying secrecy. Thus, a quantum digital signature scheme requires limited distribution of the public key. Another requirement is that the size of the signed message must only scale linearly with L, as mentioned above. Perhaps in future work, an improved scheme can be created such that the size of the message, N, can scale logarithmically with T. As mentioned early in this report, the scheme requires a new set of keys with each message. Thus, the total amount of keys used scales linearly with the amount of messages sent. In future discoveries, it would be an improvement to create a protocol in which the keys also scale logarithmically with the messages being sent. Designing a protocol would be challenging, however, since reusing keys cannot be accomplished in the quantum scheme like it can be classically [1]. Thus, further research and innovation is required in this area to make the quantum digital signature protocol as efficient as possible.

References

[1] Gottesman, D., Chuang, I. L. (2001). Quantum Digital Signatures. Retrieved from arXiv:quant-ph/0105032v2.

[2] Wootters, W. K., Zurek, H. W. (2009). The no-cloning theorem. Physics Today **62**, 2, 76. Retrieved from https://physicstoday.scitation.org/doi/10.1063/1.3086114

[3] Buhrman, H., Cleve, R., Watrous. J., De Wolf, R. (2001). Quantum fingerprinting. Retrieved from https://arxiv.org/abs/quant-ph/0102001v1.

[4] Watrous, J. (2011). Lecture 12: Holevo's theorem and Nayak's bound. Retrieved from https://cs.uwaterloo.ca/ watrous/LectureNotes/CS766.Fall2011/12.pdf.

[5] Mayers, D. (1997). Unconditionally secure quantum bit commitment is impossible. Retrieved from https://arxiv.org/abs/quant-ph/9605044.

[6] Barnum, H., Barrett, J., Leifer, M., Wilce, A. (2007). A generalized no-broadcasting theorem. Phys. Rev. Lett. 99:240501. Retrieved from https://arxiv.org/abs/0707.0620