Quantum Blind Signature with an Offline Repository

J. RIBEIRO
Departamento de Matemática, IST – Universidade de Lisboa
Avenida Rovisco Pais 1049-001, Lisboa, Portugal
email: j.l.ribeiro@ist.utl.pt

A. SOUTO
Departamento de Matemática, IST – Universidade de Lisboa
SQIG, Instituto de Telecomunicações
Avenida Rovisco Pais 1049-001, Lisboa, Portugal
email: a.souto@math.ist.utl.pt

P. MATEUS
Departamento de Matemática, IST – Universidade de Lisboa
SQIG, Instituto de Telecomunicações
Avenida Rovisco Pais 1049-001, Lisboa, Portugal
email: pmat@math.ist.utl.pt

March 17, 2015

Abstract

We propose a quantum blind signature scheme that achieves perfect security under the assumption of an honest offline repository. The security of the protocol also relies on perfect private quantum channels, which are achievable using quantum one-time pads with keys shared via a QKD protocol. The proposed approach ensures that signatures cannot be copied and that the sender must compromise to a single message, which are important advantages over classical protocols for certain applications.

Keywords: Quantum blind signatures; Trusted party; Bell states.

1 Introduction

Digital signatures are mechanisms for authenticating the validity or authorship of a certain digital message and they aim to be digital counterparts to real (or analog) signatures. The concept was introduced by Diffie and Hellman [1] in 1976 and properly formalized by Goldwasser, Micali, and Rivest [2]. The earliest classical digital signature schemes are based on public key cryptographic schemes and were proposed and studied by Rivest, Shamir, and Adleman, [3] Lamport, [4] Rabin [5] and Goldwasser, Micali, and Rivest [2]. Notice that, when certified, digital signatures have the same legal power as traditional signatures. One such scheme was proposed by Merkle [6]. It is possible to find several variants of the concept of digital signature in the literature. For example, ring signatures [7] aim to ensure the authorship among a group of possible signers without revealing the real signer

(useful for anonymously revealing secrets inside an organization, for example), undeniable signatures [8] are schemes in which the verification procedure requires the cooperation of the signer and in which the signer cannot, in court, deny the authorship of the signature. Another important variation is the blind signature, [9] which can be used to provide authenticity to a message without linking it to its creator.

With the advent of quantum computation and quantum information, new adversarial paradigms appear. Shor's algorithm [10] allows a polynomial-time factorization of semi-prime numbers in a quantum computer. Consequently, all the digital signatures schemes mentioned above (as almost all cryptographic standards used nowadays) became vulnerable, compromising fundamental properties of signature schemes: authenticity and authorship uniqueness.

In order to overcome the potential threat of quantum computation, even before the publication of Shor's algorithm, the community started to envisage the possibility of using quantum mechanics laws to develop new protocols that are resilient against quantum adversaries. One of the first protocols presented addressed the problem of securely distributing a key [11]. The evolution of this field was made in several fronts. There was a prominent focus on designing public key protocols which are resistant against quantum adversaries and are information-theoretically secure. These protocols are based on encoding information which only the private key holder is able to decipher using the quantum registers (one such example can be found in Reference [12]).

Gottesman and Chuang [13] were the first to propose a quantum counterpart to digital signatures. Their scheme is based on the existence of quantum one-way functions. Other proposed schemes were presented in Reference [14] following a similar idea, and more recently in Reference [15] in which the scheme uses quantum key distribution protocols. There are also proposals regarding quantum blind signatures (see for example Reference [16]). Our approach is substantially different since we rely on Bell states and a trusted repository which stores quantum states relevant to the verification procedure. Since our repository is only used to store information and provide it when requested playing no other active role in the protocol we called it offline. A similar situation occurs with commonly used and widely implemented public key infrastructures (PKI). With a PKI one agent can retrieve an authenticated public key of another agent to whom he can then communicate, otherwise the agent has no way to confirm the identity of the agent he intends to communicate with. During the communication the PKI has no role, so it can be offline. The offline repository in the proposed protocol plays a similar role. It does not need to be online for Bob to verify the signature.

The trusted repository is an acceptable assumption since public key infrastructures functioning as mediators in a protocol are a common occurrence in the real world and nowadays all schemes in use rely on the existence of such trustful entities. For example, in order to obtain the public key of an enterprise, one has to rely on PKI's (Public key infrastructures) that provide important information relative to public keys, such as the key itself, revoked keys, date of validity, etc. In our case, the repository is used to ensure that the data used for the verification procedure (quantum states and classical information) is randomly distributed between the parties involved in the protocol. Notice that the information can be spread through many repositories using some kind of secret sharing protocol, thus severely limiting the impact of a repository being dishonest. In this paper we assume that the repository is honest and works properly.

Our proposal is suitable for elections as we explain next. Consider the following situation: Bob is hosting an election and Alice wants to vote. In order to participate, a person must be registered in a voter's club controlled by Eve, who signs the ballots. There is a set time limit for participants to vote, after which the votes are received and counted (non-anonymously) by Bob. Before the votes are collected, it is in

the best interest of the voters and Bob to keep the votes private, otherwise the election could be rigged. Nevertheless, the ballot still needs to be authenticated by Eve, who must not gain any knowledge whatsoever about the votes. Furthermore, no adversary should be able to forge a signed ballot or alter someone else's vote. Additionally, participants should not be able to disavow their votes after they have been cast and Eve should not be able to deny a valid signature. Finally, participants cannot vote more than once and should compromise to a single voting option before the votes are collected. Our scheme allows Alice and Bob to interact in a safe way, solving all these issues.

The rest of the paper is organized as follows: the subsequent section is devoted to the presentation of basic definitions, necessary results and notation. In Section 3 we present the states used in the blind signature scheme. We also explain the signing phase by presenting the algorithms used to create the signature, to verify Eve's honesty, to blind the signature, and the process used by Bob to check the validity of the signature. Furthermore, we provide detailed proofs of the correctness and security of the protocol. In Section 4 we summarize the results obtained and point some future research.

2 Preliminaries

We assume the reader is familiar with Dirac's bra and ket notation. In particular we use Greek letters such as $|\psi\rangle$, $|\phi\rangle$ to denote pure states and ρ to denote mixed states. We refer the reader to the book of Nielsen and Chuang [17] for a complete study of this topic.

We fix a binary alphabet $\Sigma = \{0, 1\}$ and consider binary strings as elements of Σ^*. Usually classical binary strings are denoted by m, k, v, s, etc. Given a string m, m_i represents the ith bit in m and $|m|$ is the notation for size of the string. We adopt the notation $\oplus$ to denote the exclusive or binary operator and $\odot$ to denote concatenation.

2.1 Universal hash functions

During the protocol, hash functions are required to ensure the message is not tampered by someone else other than Alice. For that purpose we use *universal hash functions*. A hash function provides a compress *digest* of a message in such a way that it identifies it (for details and construction see Reference [18]). For that reason, collisions, *i.e.* values that are mapped to the same hash value, are unavoidable. The properties enjoyed by these functions that we will be using are:

- hashes are almost equally distributed;
- their computation is feasible in polynomial time;

Definition 2.1. Let A and B be two sets of size respectively a and b such that $a > b$. Let also H be a collection of hash functions $h : A \to B$. H is said to be a *universal family of hash functions* if for all $x \neq y$

$$\Pr_{h \in H}[h(x) = h(y)] \leq \frac{1}{b}.$$

The next result provides well known bounds on the number of collisions.

Proposition 1. *Let A and B be two sets of size respectively a and b such that $a > b$. Let also H be a collection of hash functions $h : A \to B$. If H is a universal family of hash functions then for any set $A' \subset A$ of size N, for any $x \in A$, the expected number of collisions between x and other elements in A' is at most N/b.*

In particular, considering A and B to be the sets of all strings of length n and $n/2$, respectively, then, for each h there are $2^{n/2}$ strings with the same fixed hash value. In due course, we will use universal hash functions in order to prevent a third party from altering Alice's message by providing a randomly chosen digest of the message through a random choice of a hash function $h \in H$ that can be checked after measurement of certain quantum states.

2.2 Bell states as the bases for the system

A Bell state is an entangled pair of qubits. It can take one of the four possible forms:

$$\begin{aligned} |\Phi^+\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) & |\Phi^-\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle|0\rangle - |1\rangle|1\rangle) \\ |\Psi^+\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle|1\rangle + |1\rangle|0\rangle) & |\Psi^-\rangle &= \tfrac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle). \end{aligned}$$

The following facts are easy to prove:

Proposition 2. *The state $|\Phi^+\rangle$ is computationally easy to obtain from $|0\rangle|0\rangle$ in quantum polynomial time.*

Indeed, from $|0\rangle|0\rangle$, one can just apply the Hadamard gate to the first qubit and then the Cnot gate to obtain $|\Phi^+\rangle$.

Proposition 3. *It is possible to transform $|\Phi^+\rangle$ into $|\Psi^+\rangle$ using Pauli's operator $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0|$. Furthermore, any Bell state is transformable into another bell state by unitary transformations.*

Notice that it suffices to be in possession of a single qubit of a Bell state for someone to transform a Bell state into the other.

Proposition 4. *Let $\mathbb{B}$ be a Bell state of the form $|\Phi^+\rangle$ or $|\Psi^+\rangle$ and assume that Alice is in possession of one of the qubits of that state. If Alice measures her qubit then the result is completely random. Furthermore Alice is not able to infer the state of the whole system.*

In fact, assuming without loss of generality that $\mathbb{B} = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$ and Alice is given access to the first qubit then its density matrix representation is

$$\mathbb{B} = |\Phi^+\rangle\langle\Phi^+| = \frac{1}{2}(|0\rangle|0\rangle + |1\rangle|1\rangle)(\langle 0|\langle 0| + \langle 1|\langle 1|)$$

Hence from Alice's point of view her qubit is:

$$\begin{aligned} \rho_A &= \frac{1}{2}\sum_{k=0}^{1}\langle k|(|0\rangle|0\rangle + |1\rangle|1\rangle)(\langle 0|\langle 0| + \langle 1|\langle 1|)|k\rangle \\ &= \frac{1}{2}[(\langle 0|(|0\rangle|0\rangle + |1\rangle|1\rangle)(\langle 0|\langle 0| + \langle 1|\langle 1|)|0\rangle \\ &\quad + \langle 1|(|0\rangle|0\rangle + |1\rangle|1\rangle)(\langle 0|\langle 0| + \langle 1|\langle 1|)|1\rangle) \\ &= \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \\ &= \frac{\mathsf{Id}}{2} \end{aligned}$$

where Id is the identity operator in one qubit.

Hence, with access to a single qubit of $\mathbb{B}$, Alice cannot infer what was the original state of the system.

It is easy to see that all Bell states are orthogonal to each other and hence they are pairwise perfectly distinguishable. Hence if one has full access to a Bell state $\mathbb{B}$, which is either $|\Phi^+\rangle$ or $|\Psi^+\rangle$, then one is able to determine which pair of qubits was considered for that Bell state. A possible measurement operator to distinguish them is:

$$M = 0 \cdot P_{\Phi^+} + 1 \cdot P_{\Phi^-} + 2 \cdot P_{\Psi^+} + 3 \cdot P_{\Psi^-}$$

where $P_{\Phi^+} = |\Phi^+\rangle \langle\Phi^+|$, $P_{\Psi^+} = |\Psi^+\rangle \langle\Psi^+|$, $P_{\Phi^-} = |\Phi^-\rangle \langle\Phi^-|$ and $P_{\Psi^-} = |\Psi^-\rangle \langle\Psi^-|$. Notice also that if one measures each qubit separately using the computational basis then, in the case where $\mathbb{B} = |\Phi^+\rangle$ both measurements yield the same result and when $\mathbb{B} = |\Psi^+\rangle$ the measurements yield distinct results.

2.3 Quantum one-time pad protocol based on BB84

In 1984 Bennett and Brassard published the first quantum key distribution protocol [11]. This scheme is unconditionally secure and allows Alice and Bob to agree on a key that can then be used to transmit classical or quantum information. Similar protocols are B92 proposed by Bennett[19] and E91 proposed by Ekert[20].

Later, Ambainis *et. al* [21] generalized the idea of classical one time pad for the quantum domain. In particular, the protocol bellow, using Pauli matrices, allows the transmission of any n-qubit state from Alice to Bob using $2n$-bit keys.

Protocol 5 (Quantum one time pad as in Reference [21])**.**

Input: *$s \in \Sigma^{2n}$ a string of classical bits shared by Alice and Bob (obtained by following the BB84 protocol) and a state $|\psi\rangle = |\psi_1\rangle \otimes \ldots \otimes |\psi_n\rangle$ of n qubits known to Alice.*

Output: *Bob ends with state $|\psi\rangle$.*

Step 1. *For each qubit i, Alice applies one of the following operations:*

$$\begin{cases} \mathsf{Id} & \text{if } s_i s_{i+1} = 00 \\ \sigma_x & \text{if } s_i s_{i+1} = 01 \\ \sigma_y & \text{if } s_i s_{i+1} = 10 \\ \sigma_z & \text{if } s_i s_{i+1} = 11 \end{cases}$$

where σ_x, σ_y and σ_z are Pauli unitary operators. Let $|\psi'\rangle$ be the resulting state.

Step 2. *Alice sends $|\psi'\rangle$ to Bob.*

Step 3. *Bob applies the same operations to each qubit according to the string s to recover the state $|\psi\rangle$.*

It follows from the security of BB84 that, if the two parties share a private *a priori* seed, then the protocol is unconditionally secure. In particular, if a third party intercepts the state traveling from Alice to Bob, then the state is in a complete mixture state. We refer the reader to Reference [21] for a detailed proof of this statement.

2.4 Quantum fingerprinting

Quantum fingerprinting is a quantum procedure that can be used to test whether two given quantum states $|\phi\rangle$ and $|\psi\rangle$ are identical or distinct with inner product δ. This procedure, described in Reference [22], allows us to test such hypotheses with nearly optimal error probability.

The procedure takes the two states and an ancilla state $|0\rangle$ and applies the operator

$$(\mathsf{H}\otimes\mathsf{Id})(\mathsf{C\text{-}Swap})(\mathsf{H}\otimes\mathsf{Id}),$$

where H is the Hadamard transform, $\mathsf{C\text{-}Swap}$ is the controlled-Swap that depending on the value of the control qubit (usually the first one) switches the second and the third registers and, as previously mentioned, Id is the identity operator. By applying this operator to the system $|0\rangle|\phi\rangle|\psi\rangle$ we obtain the state

$$\frac{1}{2}|0\rangle(|\phi\rangle|\psi\rangle+|\psi\rangle|\phi\rangle)+\frac{1}{2}|1\rangle(|\phi\rangle|\psi\rangle-|\psi\rangle|\phi\rangle).$$

Notice that if $|\phi\rangle=|\psi\rangle$ then the above state can be simplified to $|0\rangle|\phi\rangle|\psi\rangle$ and hence measuring the first qubit of the system in the computational basis will always yield 0. On the other hand, if the states are distinct, the measurement in the computational basis will yield 1 with probability $1/2-\delta^2/2$, where $\delta=\langle\phi|\psi\rangle$. Hence, the one-sided error probability p of the quantum fingerprinting procedure, i.e. the probability of concluding that the states are identical even though they are distinct, is at most $p=1/2+\delta^2/2$.

3 The scheme for signing

In the sequel we present our scheme for a blind signature that is suitable for elections and other situations that benefit from the impossibility of copying signatures and the insurance of unique message compromisal. We divide this section into three subsections. The first subsection presents the structure of the states used in the signature scheme and provides the reasoning for the efficiency of their use. The second subsection presents the protocol for signing, verifying Eve's honesty, blinding the signature, and Bob's verification procedure. The third subsection contains detailed proofs of the correctness of the protocol.

3.1 Main idea

Our protocol is based on Bell states $\mathbb{B}$, presented in the previous section, and the creation of entanglement between relevant qubits of the state that will correspond to a signature. It exploits the fact that entanglement must be created locally.

For simplicity, assume that m, the message to be signed, is of length ℓ. For the signature we will be dealing with states of the form

$$\begin{aligned}|\psi\rangle = &\quad \frac{1}{\sqrt{2^{6\ell}}}\sum_{k\in\{0,1\}^{2\ell}}\mathcal{K}\otimes\mathcal{V}(k,v)\otimes\mathcal{S}(k,m)\\ = &\quad \frac{1}{\sqrt{2^{6\ell}}}\sum_{k\in\{0,1\}^{2\ell}}|k\rangle\left[\bigotimes_{j=1}^{2\ell}(\sigma_x)^{k_j\oplus v_j}|\Phi^+\rangle\right]\left[\bigotimes_{i=1}^{2\ell}(\sigma_x)^{(m\odot r\odot h_r(m))_i\oplus k_i}|\Phi^+\rangle\right]\end{aligned}$$

where $v=v_1\ldots v_{2\ell}$ is a verification string, $r\in\{0,1\}^{\ell/2}$ is a bit string chosen at random that identifies, in the universal hash family of functions, to be used and $h_r(m)$ is the hash value of message m through the hash function h_r. In fact, if we are given access to a entire system of qubits, by measuring the first 2ℓ in computational basis and the remaining ones with M we recover first k, confirm it with verification key v and finally recover m (using r and h_r). Notice that the systems composing the superposition of the state $|\psi\rangle$ are highly entangled.

Theorem 3.1. *Let $v \in \{0,1\}^{2\ell}$ be a fixed binary string. The above states are easy to create with probability 1 from $|v\rangle \otimes |0\rangle^{\otimes 10\ell}$ using a quantum polynomial time algorithm.*

Notice that in the above theorem there is an abuse of notation. In fact $|v\rangle$ is the abbreviation for a quantum system with 2ℓ qubits.

Proof. We present an algorithm that outputs the required states with probability 1 from the designated input.

Algorithm 6 (Preparing the signing states)**.**

Input: $|v\rangle \otimes |0\rangle^{\otimes 10\ell}$.

Output: $|\psi\rangle = \frac{1}{\sqrt{2^{6\ell}}} \sum_{k\in\{0,1\}^{2\ell}} |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{k_i} |\Phi^+\rangle\right]$.

Step 1. *Apply* H*, the Hadamard transformation, to the qubits with indices* $4\ell + 2i - 1$ *for* $i = 1, \ldots, 4\ell$.

Step 2. *Using the qubits of the previous Step as controls and the qubit immediately to its right as a target, apply the* Cnot *transformation; Notice that, after these steps, the last* 8ℓ *qubits are pairwise Bell states of the form* $|\Psi^+\rangle$, i.e., *the system becomes:*

$$\frac{1}{\sqrt{2^{4\ell}}} |v\rangle \otimes |0\rangle^{2\ell} \left[\bigotimes_{j=1}^{2\ell} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} |\Phi^+\rangle\right].$$

Step 3. *Apply* $\mathsf{Id}^{\otimes 2\ell} \otimes \mathsf{H}^{\otimes 2\ell} \otimes \mathsf{Id}^{\otimes 8\ell}$*. The resulting state is:*

$$\frac{1}{\sqrt{2^{6\ell}}} |v\rangle \sum_{k\in\{0,1\}^{2\ell}} |k\rangle \left[\bigotimes_{j=1}^{2\ell} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} |\Phi^+\rangle\right].$$

Step 4. *Apply* $\oplus$ *to the systems containing* $|v\rangle$ *and* $|k\rangle$ *and store the result in the first register. The resulting state is:*

$$\frac{1}{\sqrt{2^{6\ell}}} \sum_{k\in\{0,1\}^{2\ell}} |v \oplus k\rangle |k\rangle \left[\bigotimes_{j=1}^{2\ell} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} |\Phi^+\rangle\right].$$

Step 5. *Apply the transformation* σ_x *to each qubit with index* $4\ell + 2i$ *with* $i = 1 \ldots 2\ell$ *controlled by the qubit with index* i*. The resulting state is*

$$\frac{1}{\sqrt{2^{6\ell}}} \sum_{k\in\{0,1\}^{2\ell}} |v \oplus k\rangle |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} |\Phi^+\rangle\right].$$

Step 6. *Apply the transformation* σ_x *to each qubit with index* $8\ell + 2i$ *controlled by the qubit with index* $2\ell + i$ *with* $i = 1 \ldots 2\ell$*. The resulting state is*

$$\frac{1}{\sqrt{2^{6\ell}}} \sum_{k\in\{0,1\}^{2\ell}} |v \oplus k\rangle |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{k_i} |\Phi^+\rangle\right].$$

Step 7. *Measure the first 2ℓ registers in the computational basis. The resulting state is*

$$\frac{1}{\sqrt{2^{6\ell}}} \sum_{k\in\{0,1\}^{2\ell}} |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{k_i} |\Phi^+\rangle\right].$$

Notice that all the operations used in this algorithm including H, Cnot and σ_x are computed in quantum polynomial time. The correctness of the algorithm and the probability of success are straightforward. □

As it will be discussed in the next section when considering the creation of the states composing the signature, if Eve is given a string s of length 2ℓ she can easily prepare the state

$$\frac{1}{\sqrt{2^{6\ell}}} \sum_{k\in\{0,1\}^{2\ell}} |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{s_i \oplus k_i} |\Phi^+\rangle\right]$$

by performing similar steps to Step 4 and Step 5 as in the Algorithm 6 .

Reasoning Notice that the first part of the system can be used as a key to unleash the rest of the system. Without it, the system is untreatable by any other party, in the sense that without the key no one can verify the validity of the produced states as a valid signature of any message. Keeping the first qubit of each system composing $\mathcal{V}(k, v)$ in the repository will allow someone who accesses the first register to verify, with a great level of certainty, the signature. The random value r and the corresponding hash function h_r are used to prevent another party from altering Alice's message without being detected, i.e. forging Alice's commitment to another message. In particular, if for each state, r was not random them a third party accessing to states prepared by Alice, could measure one of the states and compute m, r and $h_r(m)$ and then could impersonate Alice and alter the message applying Pauli gates by computing the parity of $m \odot r \odot h_r(m)$ in each qubit of the other states. With r and h_r chosen at random for each system composing the signature, the final receiver would be able to detect any dishonest change by checking those parameters.

Furthermore, Alice's message is unknown for Eve since, at the end, Eve without accessing the system is not able to recover Alice's message. Notice that Eve blindly signs m by signing a random value s that afterwards will be replaced by a unique identifier of Alice's message using local operations.

Lemma 7. *Assume that the systems corresponding to the first qubits of $\mathcal{V}(k, v)$ and $\mathcal{S}(m, k)$ are given to Alice. If she is given access to the system containing $\mathcal{K}$ and the second qubit of $\mathcal{V}(k, v)$, then it is possible to infer with probability 1 the states of the systems composing $\mathcal{V}(k, v)$ and $\mathcal{S}(k, m)$ efficiently.*

Proof. Assume that Alice's states are of the correct form and let k be the result of measuring the first system in the computational basis. By tracing out $|k\rangle$, the resulting state $|\psi\rangle$ in Alice's possession collapses to:

$$|k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{[m\odot r\odot h_r(m)]_i \oplus k_i} |\Phi^+\rangle\right].$$

By definition of σ_x, the result of measuring the entire system with $M^{\otimes 4\ell}$ is:

$$(k \oplus v) \odot (m \odot r \odot h_r(m)) \oplus k).$$

Using the value k obtained in the first part, Alice can recover and check v and confirm the validity of the final concatenation. □

3.2 The Protocol for a blind signature

We now combine the previous results to setup the blind signature scheme suitable for the situations described in Subsection 1. We consider three entities:

Alice The sender of the message;

Bob The receiver of the message;

Eve The blind signer for Alice;

We also assume that Eve will only sign messages from registered and authenticated users. Furthermore, Eve only participates during the signing phase and the transmission of the signature to the repository. After these stages she can be called off and will only play a role again in case of disavowal. So, the signer is called to prepare the states in initial stage and has no further role in the protocol if she is honest.

In order for the protocol to work correctly, we need to assume that the three parties have access to a trusted repository which is not controlled by anyone involved in the protocol. Notice that this is a conventional assumption. It is also assumed that this repository has the property of broadcasting information about the quantum states available for checking for each user. This requirement ensures that Bob, upon receiving a message from Alice, can immediately verify that the states received were not yet used. Furthermore, we assume that all the communications are secure through the use of private quantum channels. This is achievable through secure protocols for quantum key distribution and quantum one-time pad. The repository is defined by three simple rules:

- Only Eve is allowed to send information (classical and quantum) regarding signatures to the repository.
- Someone can then extract relevant information by identifying himself and presenting a password.
- A given party can only access the repository once.

The repository is used as follows: upon signing a message for Alice, Eve sends packets of classical and quantum information pertaining the signature to the repository, linking each packet with a certain verification string v that acts as a password. Alice and Bob can then randomly extract a packet of information by properly identifying themselves and providing the respective password v.

Protocol 8 (Creation, Blinding and verification of a signature)**.**

Public Knowledge:

- *Parameter $\tau \in \mathbb{N}$ of the number of copies that Eve will produce of the signature. δ the number of copies that Alice will test. β the number of copies that Alice will send to Bob.*
- *A family of universal hash functions H of the form $h_r : \{0,1\}^{\ell} \to \{0,1\}^{\ell/2}$ where the indexes of the functions are identified by strings of length $\ell/2$, r.*
- *A quantum one-time pad protocol presented in Protocol 5.*

Blinding Phase

Step 1. *Alice sends a $2\tau\ell$-bit string*

$$s = s_1 \dots s_\tau = (s_{11} \dots s_{12\ell}) \dots (s_{\tau 1} \dots s_{\tau 2\ell})$$

to Eve using Protocol 5.

Signing Phase

Step 2. *Eve receives the bit string s from Alice and checks whether Alice is a verified sender. If so, Eve prepares, using Algorithm 6, τ copies of the following form:*

$$|\psi_\alpha\rangle = \frac{1}{\sqrt{2^{6\ell}}} \sum_{k \in \{0,1\}^{2\ell}} |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j^\alpha} |\Phi^+\rangle \right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{(s_\alpha)_i \oplus k_i} |\Phi^+\rangle \right]$$

where v^α is randomly chosen and $s_\alpha = s_{\alpha 1} \dots s_{\alpha 2\tau}$, for each $\alpha = 1, \dots, \tau$.

Step 3. *Eve sends the strings v^α for all $\alpha = 1, \dots, \tau$ (classical information) and the qubits of $|\psi_i\rangle$ corresponding to the key $\mathcal{K}$, i.e., the qubits containing the superposition of k's and the first qubit of each register containing the Bell states of the verification and the signed message, to the repository. The string v^α acts as the password for the packet of information regarding the α-th copy of the signature.*

Step 4. *The remaining qubits of all states $|\psi_i\rangle$ are sent to Alice using Protocol 5.*

Checking the honesty of Eve

Step 5. *Alice randomly chooses δ indices in $\{1, \dots, \tau\}$.*

Step 6. *For each $\alpha \in \{1, \dots, \tau\}$, Alice presents the relevant verification string v^α to the repository and is then allowed to extract the qubits in the repository corresponding to the states respective to $|\psi_\alpha\rangle$.*

Step 7. *By preparing the correct states that Eve should have created and using the quantum fingerprinting procedure discussed in Subsection 2.4, Alice checks the consistency of the states. If the results are all correct then Alice deems Eve honest, otherwise she aborts the protocol.*

Signing the message m

Step 8. *Alice picks $\tau - \delta$ elements $r_\alpha \in \{0,1\}^{\ell/2}$ at random and obtains the corresponding hash function h_{r_α} from the public collection. Let t be the binary string $t = m \odot r_\alpha \odot h_{r_\alpha}(m)$. Notice that t has the same size of s_α.*

Step 9. *For each copy α of the remaining systems received from Eve, Alice prepares the signed state by applying σ_x if $t_i \neq (s_\alpha)_i$ to each of the last ℓ qubits that are in her possession. Notice that the overall state of the α-th copy ($\alpha \in \{1, \dots, \delta\}$) is now of the form:*

$$|k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j^\alpha} |\Phi^+\rangle \right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{[m \odot r_\alpha \odot h_{r_\alpha}(m)]_i \oplus k_i} |\Phi^+\rangle \right].$$

Step 10. *Alice sends β of the states she has to Bob using Protocol 5, as well as their respective verification strings v^α.*

Verification Phase for Bob

Step 13. *Upon receiving the information from Alice, Bob randomly extracts ε qubits corresponding to $\mathcal{K}_1$ states from the repository that have not yet been used by Alice by presenting the relevant verification strings.*

Step 14. *For each of the ε states, Bob measures the register corresponding to $\mathcal{K}$ in the computational basis and determines k – the verification key.*

Step 15. *Using M on the registers from 2ℓ to 6ℓ he verifies the consistency of the results obtained with $k \oplus v^{\alpha}$.*

Step 16. *Using M on the last 4ℓ registers Bob collects $t = m \odot r_{\alpha} \odot h_{r_{\alpha}}(m)$ of all the ε states. If at least half of ε states are not consistent or give different messages m then Bob does not accept the message as valid.*

As we will see, for a fixed n, setting $\tau = 4n$, $\delta = 3n$, $\beta = n$ and $\varepsilon = n/2$ it is enough to have a considerable probability of success of the protocol. Notice that Bob keeps, at random, $n/2$ states in case of a message or signature disavowal by either Alice or Eve. Informally, Bob can then prove that Alice or Eve are being dishonest by checking that the measurements of at least $n/8$ states are valid and coincide with the message that is in jeopardy.

Remark 9. *Observe that the current protocol does not prevent Eve, if she was the recipient of the signed message at a later stage, from linking Alice's message to Alice herself by comparing verification strings (relevant for untraceable electronic money, where Eve is the bank, and other similar situations).*[1] *This issue can be solved by allowing the verification strings to be randomized after Alice extracted her states (or, in a more extreme case, after Bob's extraction as well). This means that Alice could then alter the quantum states composing the signature to reflect this change. Note also that a party must identify itself in order to extract information from the repository. If we did away with this requirement we would face an issue: Alice could extract information from the repository after she had sent the messages to Bob (and before Bob verified the message, if the verification strings were randomized after Bob's extraction as well), thus "deleting" the message before Bob was able to see it. Although this is not problematic in certain situations (like untraceable electronic money), it still is a negative property in general.*

Nevertheless, this issue can be solved by considering an additional quantum verification system between the repository and the verifier. Consider a verification string v and a system of 2ℓ Bell states $|\phi\rangle_i = \sigma_x^{v_i} |\Phi^+\rangle$, where $i = 1, \ldots, 2\ell$. The first qubit of each pair would belong to the party extracting information and the second qubit would belong to the repository. Besides presenting the relevant verification string v, they would also present the measurement results of their qubits on this new state. The repository would measure its qubits and recover the string v from the whole set of measurement results. Thus, someone would need to be in possession of these states in order to extract information and so Alice would not be able to delete her message after it has been sent to Bob. The randomization of verification strings could be taken into account by letting the repository and the extracting party apply the σ_x transformation to some of their qubits. Some procedures could be taken into account in order to test whether these systems were not tampered with. We do not discuss in detail these procedures and assume that Eve is not a possible verifier and that there is a secure authentication mechanism between the repository and the users.

Finally we discuss the blindness of the signature. Notice that Alice's message m will be unknown to Eve since, at the end of signing procedure, Eve's perception

[1] In the early stage of the work the idea was to describe a blind signature suitable to election or auctions where Eve would be a neutral entity that would just be responsible for the creation of the states and not an intervenient in the process. Later, we realized that the protocol could be, in fact, improved to achieve similar condition to untraceable money.

of the changed performed by Alice is null. In fact, since Alice after the signing procedure, there is not information sent to Eve and the change on the quantum system containing the signature is performed using only local operations over part of the qubits, and hence the description of the system for her does not change.

3.3 Proofs of correctness and security of the protocol

From the next theorem it follows that this scheme runs in polynomial time.

Theorem 3.2. *Protocol 8 runs in polynomial time.*

Proof. It follows from Theorem 3.1 that preparing the system

$$\frac{1}{\sqrt{2^{6\ell}}} \sum_{k\in\{0,1\}^{2\ell}} |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{k_i} |\Phi^+\rangle\right]$$

for each one of the $4n$ states from a system of zeros and a verification string v (this string differs from state to state) can be done in polynomial time in a quantum computer. Furthermore, each of Eve's final systems, i.e.,

$$\frac{1}{\sqrt{2^{6\ell}}} \sum_{k\in\{0,1\}^{2\ell}} |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{k_i \oplus (s_a)_i} |\Phi^+\rangle\right]$$

is obtained by applying $\otimes_{i=1}^{2\ell} (\sigma_x)^{s_i}$ to the last 2ℓ qubits of the system which is quantum polynomial time computable.

In order for Alice to transform the states received by Eve, she has to apply a similar operation on the last 2ℓ qubits. In particular she applies the quantum operator $\otimes_{i=1}^{2\ell} (\sigma_x)^{s_i \oplus [m\odot r_a \odot h_{r_a}(m)]_i}$ on the last 2ℓ qubits. Notice that computing the hash of a message and the concatenation of strings can be done in polynomial time too. □

Theorem 3.3. *If all the parties are honest and play fairly their role in the Protocol 8, then the probability of success, i.e., of reaching the end with Bob accepting the signature is exponentially close to 1.*

Proof. Notice that the term negligible used in the statement of the theorem is due to the fact that one-time-pad Protocol 5 used to transfer qubits has negligible probability to fail in transmitting the correct message.

For the rest of the argument, and without loss of generality, we assume that all the states were correctly transmitted. In order to prove this theorem we have to show:

1. The signing phase can be performed with certainty;
2. The unblinding phase can be done with probability 1;
3. The verification procedure has probability success 1;

The first item follows from Theorem 3.1.

The second item follows directly from the fact that unblinding the signature corresponds to applying the operation $\otimes_{i=1}^{2\ell} (\sigma_x)^{s_i \oplus [m\odot r\odot h_r(m)]_i}$ on the last 2ℓ qubits, which can be accomplished in a deterministic manner by a quantum computer.

To prove the last item, assume that Bob collected the relevant qubits from the repository and thus possesses states of the form:

$$\frac{1}{\sqrt{2^{6\ell}}} \sum_{k\in\{0,1\}^{2\ell}} |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{[m\odot r_a \odot h_{r_a}(m)]_i \oplus k_i} |\Phi^+\rangle\right].$$

For simplicity we provide the argument for a single system and extrapolate the conclusion for several systems. By measuring the first 2ℓ qubits in the computational basis, Bob recovers some $k \in \{0,1\}^{2\ell}$ and the resulting state is

$$\frac{1}{\sqrt{2^{4\ell}}} |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j} |\Phi^+\rangle \right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{[m \odot r_a \odot h_{r_a}(m)]_i \oplus k_i} |\Phi^+\rangle \right].$$

Using $M^{\otimes 4\ell}$ where $M = 0 \cdot P_{\Phi^+} + 1 \cdot P_{\Psi^+}$ and $P_{\Phi^+} = |\Phi^+\rangle \langle\Phi^+|$ and $P_{\Psi^+} = |\Psi^+\rangle \langle\Psi^+|$, Bob can recover, with probability 1, the strings $k \oplus v^\alpha$ and $[m \odot r_a \odot h_{r_a}(m)] \oplus k$ and hence verify the correctness of the message sent by Alice. All the systems have this property, and hence, the probability of Bob accepting the message is 1. □

Theorem 3.4. *Let n be a fixed integer and set $\tau = 4n$, $\delta = 3n$, $\beta = n$ and $\varepsilon = n/2$ in Protocol 8. Suppose that Eve is dishonest and prepares s cheating states and that Alice and Bob are honest. The probability of Alice accepting Eve's signature and Bob rejecting Alice's message is exponentially low on n.*

Proof. An informal line of reasoning goes as follows: in order for Bob to reject Alice's message Eve must prepare at least $n/4$ cheating states, and these must be quite different from the correct states or else Bob will classify them as valid states with high probability. On the other hand, if too many cheating states are highly distinct from the correct ones then Alice will catch them before Bob does and deem Eve dishonest. We prove that any strategy (defined for each n) that Eve employs has a negligible probability of being successful.

Let $s(n)$ be the number of cheating states created by Eve for each $n \in \mathbb{N}$. Recall that $s(n) \geq n/4$ in order for Bob to reject Alice's message. We can sort the cheating states in increasing order relative to each of their inner products with a correct state, i.e. if t is a correct state, the cheating states are sorted and indexed as $c_1, \ldots, c_{s(n)}$ satisfying $c_i \cdot t \leq c_j \cdot t$ if $i < j$. Let $\delta(n) = c_{\lfloor n/8 \rfloor} \cdot t$ and $K(n) = \{c_i : i \leq \lfloor n/8 \rfloor\}$.

Consider the following events:

- A - Alice deems Eve honest;
- B - Bob rejects Alice's message;
- E - Eve is dishonest and prepares $s(n) \geq n/4$ cheating states.

In order to prove the theorem we have to compute an upper bound for $\Pr(A \cap B|E)$. We proceed by cases:

Case 1: $\delta(n)$ is not exponentially close to 1 on n;

Define a random variable X that counts the number of states in $K(n)$ selected on $3n$ extractions out of a total population of $4n$ states, i.e., X counts the number of cheating states in $K(n)$ caught by Alice. Then X follows the hypergeometric distribution $\mathcal{H}(4n, |K(n)|, 3n)$. Hence the expected value of X is $E(X) = \frac{3|K(n)|}{4}$.

By Inequality (14) in Reference [23] (which is derived from bounds obtained in Reference [24]), we have, for some $t > 0$ that

$$\begin{aligned} \Pr(X > |K(n)|/2) &= 1 - \Pr(X \leq |K(n)|/2) && (1) \\ &= 1 - \Pr\left(X \leq \frac{3}{4}|K(n)| - \frac{|K(n)|}{12n} \cdot 3n\right) && (2) \\ &\geq 1 - e^{\frac{-2|K(n)|^2}{144n}}. && (3) \end{aligned}$$

Since $|K(n)| = \lfloor n/8 \rfloor$, then clearly the above probability increases exponentially to 1 with n.

On the other hand, by the quantum fingerprint result presented in Reference [22], we also have that

$$\Pr(A|X \geq |K(n)/2| \cap E) \leq \left(\frac{1+\delta(n)^2}{2}\right)^{|K(n)|}. \tag{4}$$

Since $\delta(n)$ is not exponentially high on n, the upper bound above is exponentially low on n for large enough n.

Putting together Inequalities 1 and 4 we conclude that $\Pr(A \cap B|E)$ is exponentially low on n for large enough n.

Case 2: $\delta(n)$ is exponentially close to 1 on n.

Define the random variable Y counting the number of measurements performed by Bob that yield a wrong result during his verification phase, assuming that each measurement produces the wrong result with probability $1-\delta(n)^2$ and that Bob has already detected all cheating states in $K(n)$. Then $Y \sim \mathbb{B}\mathbb{i}\mathbb{n}(n/2 - |K(n)|, 1-\delta(n)^2)$.

Notice that Y provides an upper bound on $\Pr(A \cap B|E)$ since Bob may not have detected all states in $K(n)$ and not all other chosen states may be cheating states. Additionally, if c is not in $K(n)$ then $c \cdot t \geq \delta(n)$.

Note that

$$\Pr\left(Y \geq \frac{n}{4} - |K(n)|\right) \leq e^{-\left(\frac{n}{2} - |K(n)|\right) \cdot H\left(\frac{n/4-|K(n)|}{n/2-|K(n)|}, 1-\delta(n)^2\right)}$$

where $H(p,q)$ is the Kullback-Leibler distance between two Bernoulli distributions with probabilities p and q. This bound is valid since, for large enough n, we have

$$1-\delta(n)^2 < \frac{n/4 - |K(n)|}{n/2 - |K(n)|}.$$

Furthermore, by Pinsker's inequality [25] we have that

$$H(p,q) \geq 2 \cdot |p-q|^2$$

and we can conclude that

$$\Pr\left(Y \geq \frac{n}{4} - |K(n)|\right) \leq e^{-\left(\frac{n}{2} - |K(n)|\right) \cdot 2 \cdot \left|\frac{n/4-|K(n)|}{n/2-|K(n)|} - (1-\delta(n)^2)\right|^2}.$$

Since $|K(n)| = \lfloor n/8 \rfloor$ we have that

$$\Pr\left(Y \geq \frac{n}{4} - |K(n)|\right) \leq e^{-\frac{3n}{4} \cdot \left|\frac{1}{3} - (1-\delta(n)^2)\right|^2}$$

and therefore $\Pr(A \cap B|E)$ is exponentially low on n for large enough n since $\delta(n)$ is exponentially close to 1 on n.

□

We now provide lines of reasoning for the impossibility of a third party successfully forging a signature or altering Alice's message after it has been prepared. Notice that the protocol is compromised if, during the interaction with Eve, the system is hacked and a third party impersonates Alice. We assume without loss of generality that the quantum key distribution protocol is implementable in such a way that Eve is ensured that she is communicating with Alice.

Theorem 3.5. *The probability of an adversary successfully forging a signature is negligible.*

Proof. Let Oscar be the opponent that tries to forge the message and assume that Eve is honest and prepares states of the form

$$|\psi_\alpha\rangle = \frac{1}{\sqrt{2^{6\ell}}} \sum_{k\in\{0,1\}^{2\ell}} |k\rangle \left[\bigotimes_{j=1}^{2\ell} (\sigma_x)^{k_j \oplus v_j^\alpha} |\Phi^+\rangle\right] \left[\bigotimes_{i=1}^{2\ell} (\sigma_x)^{s_i \oplus k_i} |\Phi^+\rangle\right].$$

Suppose that Oscar can provide Bob with valid verification strings (so that Bob can extract information from the repository), otherwise the attack would not be successful. Observe that the states created by Oscar are not entangled with the states extracted from the repository by Bob. Thus, regardless of whether Oscar knows the string s or $m \odot r \odot h_r(m)$, by Proposition 4, the measurements of the qubits extracted from the repository will be random with regards to Oscar's qubits. Thus, the probability of Oscar forging a signature is negligible.

Furthermore, even if Oscar is Alice then the only advantage it can have is to produce states that are valid for a different message. Notice that, in particular Alice cannot use the state in her possession to infer the possible $|k\rangle$ that is in the repository as the states are in a complete mixture. Hence, only with probability $1/k$ she is able, for each system of the signature, to produce a valid copy. □

Theorem 3.6. *The probability of an adversary successfully altering a signed message is negligible.*

Proof. First notice that, regardless of Alice's strategy (e.g. by entangling the signed message to some system she keeps for herself), she cannot alter her message after it has been sent to Bob. Furthermore, if an adversary intercepts Alice's signed message when it is being sent to Bob then he will not be able to alter it with non-negligible probability. Recall that the prepared message is $m \odot r_\alpha \odot h_{r_\alpha}(m)$, where r_α identifies, for each system that is a copy composing Alice's signature, is a function from a family of universal hash functions chosen at random for each copy of the signature. These indices r_α are known only to Alice and, at a later stage, by Bob, once he is in possession of the whole system composing the signature. Therefore, the index r_α are totally unknown to an adversary and, by the properties of universal hash families, the probability of an attacker successfully altering Alice's message in the remaining copies is negligible on ℓ. □

Remark 10. *Tampering with the validity of a signed message (by trying to alter the verification string) can be prevented in the same way we prevent adversaries from altering a signed message.*

In what follows, we stress that neither Alice nor Eve can disavow signed messages at a later stage.

Theorem 3.7. *The probability of either Alice or Eve successfully disavowing a signed message is negligible.*

Proof. Suppose that Alice attempts to disavow a signed message she had sent to Bob and that the protocol was carried out correctly. Recall that Bob has $n/2$ copies that were not used during the verification phase of the protocol. Bob can then show, by accessing the repository, retrieving the remaining states and publicly verifying that at least $n/8$ of the measurements are valid and coincide with the message Alice is trying to deny. Therefore, Bob can then show that Alice is being dishonest with probability exponentially close to 1.

Alternatively, Alice could prepare several different messages in an attempt to trigger Bob into accepting one of them (by measuring $n/2$ states and getting $n/4$ valid copies of the same message) but leading to, in the case of an eventual disavowal by Alice, failure in proving that Alice did in fact send the aforementioned message.[2] If we set the disavowal verification parameter to $n/8$ we can prove that the probability of Alice successfully disavowing the message is exponentially low.

Let $m_1, \ldots, m_t$ be messages prepared by Alice that are assigned to $k_1, \ldots, k_t$ states each. It is easy to see that, in order for Alice's strategy to be successful for a certain message $m_i = m$, i.e. Bob accepts m from Alice but is unable to later prove that Alice prepared that message, we must have

$$n/4 \leq k \leq 5n/8$$

where $k = k_i$. Let Y_k be the random variable that counts the number of states prepared with message m that are extracted by Bob out of $n/2$ extractions from a total population of n states, where k states are prepared with message m. Then $Y_k \sim H(n, n/2, k)$ and $E(Y_k) = k/2$. Therefore, the probability of Alice's strategy succeeding is

$$p(k) = \Pr(Y_k \geq \max(n/4, k - n/8)).$$

Define $f(k) = \max\{n/4, k - n/8\} - k/2$ for $n/4 \leq k \leq 5n/8$. It is easy to see that f has a minimum for $k = 3n/8$ and hence

$$p(k) \leq p(3n/8) = \Pr(Y \geq n/4) = \Pr(Y \geq E(Y) + n/16)$$

where $Y = Y_{3n/8}$. Again, by Inequality (14) in Reference [23] we conclude that

$$\Pr(Y \geq E(Y) + n/16) \leq e^{-2\frac{n/2}{8^2}}$$

and so we have the general upper bound

$$p(k) \leq e^{-n/64}.$$

Observe that the bound is independent of the message m_i and the number of states k_i. So we conclude that the probability of success of Alice's strategy is exponentially low.

Suppose now that the protocol was carried out correctly and that Eve attempts to disavow a signed message. The same strategy that was used against Alice can then be used against Eve.

Furthermore, Eve cannot prepare cheating states that are not caught by Alice and not accepted by Bob as shown in Theorem 3.4. Thus, there is no valid disavowal strategy for Eve. □

Making the aforementioned parallel with a PKI, an agent trusts a signature as much as he trusts the relevant PKI – in our protocol the same happens with the offline repository. The point of having the offline repository, or the PKI, is to get information that one can store for a future secure communication/signature. If such a PKI is not trustful, there is no point in using its services. Nevertheless, we incorporate in the next theorem the pathological case where Eve, the repository, and Alice try to cheat Bob. The other case, where Bob and the offline repository

[2]Furthermore, suppose that the disavowal verification parameter is $n/4$, i.e. Bob proves that Alice is dishonest by measuring the remaining $n/2$ states and verifying that at least $n/4$ states yield valid copies of the message that is being denied by Alice. In this case there is a clear attack: if Alice prepares $n/2$ states with message m and the remaining $n/2$ states with message $m' \neq m$, then Bob will accept one of the messages as valid but, if Alice attempts to disavow her message, Bob will not be able to prove that she is being dishonest.

cooperate, essentially means that Bob can decide what is and is not a valid signature for Alice. Such a scenario has absolutely no defense for Alice, as the repository is supposedly an honest party that, in case of disavowal from Alice, confirms to a judge whether Alice signed or did not sign a message. If Bob controls the repository, Alice cannot guarantee that her signature is accepted and may not be able to disavow a message as said before (note that the same would happen with a corrupted PKI).

Theorem 3.8. *If Alice and Eve are simultaneously dishonest, the probability of a signed message being successfully disavowed is negligible.*

Proof. Suppose that Alice and Eve are simultaneously dishonest. This means that Alice and Eve may cooperate in devising a strategy to successfully disavow a signed message with non-negligible probability.

In order to be disavowed, a message m sent by Alice must first be accepted by Bob. Afterwords, during the disavowal procedure, Bob must not be able to prove that he received the message m from Alice. Note that neither Alice nor Eve can tamper with the states composing the messages after they are sent to Bob or to the repository. The states can be prepared in arbitrary ways, but we require that each contains the same number of qubits, otherwise Bob could instantly deem the message as invalid. Nevertheless, every state received by Bob yields a certain bit string after its measurement, independently of the way in which the quantum state was prepared. Therefore, we can assume without loss of generality that for a fixed strategy devised by Alice and Eve, Bob extracts t messages $m_1, \ldots, m_t$ that are assigned to $k_1, \ldots, k_t$ states each. It is now possible to apply the exact same reasoning of Theorem 3.7 to conclude that the probability of success of the fixed strategy is negligible. □

All the above theorems show that Protocol 8 is correct and achieves perfect security.

4 Conclusions

In this paper we presented a scheme for a quantum blind signature based on offline trusted repositories. The scheme capitalizes on well established protocols for quantum key distribution and private classical and quantum communication. The scheme presented uses Bell states, Pauli operations and other simple realizable unitary operations as well as universal hash functions as mechanisms for creating a perfectly secure signature.

The main advantages of the protocol presented are the insurance of the impossibility of copying the states composing the signature as well as the fact that the sender must compromise to a single message. Thus, this scheme is especially useful for elections and certain auctions and secret negotiations. With some modifications concerning the behavior of the repository, this protocol may also be applied to situations where, at a later stage, the signer should not be able to link the signed message to its sender (e.g. untraceable electronic money).

Acknowledgments

This work was partially supported, under the PQDR (Probabilistic, Quantum and Differential Reasoning) initiative of SQIG at IT, CV-Quantum initiative of SQIG and Optical Communications and Photonics groups at IT, by FCT and EU FEDER, namely via the FCT PEst-OE/EEI/LA0008/2013, UID/EEA/50008/2013 and CaPri PTDC/EEI-TEL/6212/2014 projects, as well as by the European Union's

Seventh Framework Programme for Research (FP7). André Souto also acknowledges the FCT postdoc grant SFRH/BPD/76231/2011. João Ribeiro acknowledges the scholarship awarded by Fundação Calouste Gulbenkian through the program *Novos Talentos em Matemática* for undergraduate students.

References

[1] Diffie, W. & Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theor.* **22**, 644–654 (2006).

[2] Goldwasser, S., Micali, S. & Rivest, R. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM J. Comput.* **17**, 281–308 (1988).

[3] Rivest, R. L., Shamir, A. & Adleman, L. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **21**, 120–126 (1978).

[4] Lamport, L. Constructing digital signatures from a one-way function. Tech. Rep. (1979).

[5] Rabin, M. Digitalized signatures and public-key functions as intractable as factorization. Tech. Rep., Cambridge, MA, USA (1979).

[6] Merkle, R. A certified digital signature. In Brassard, G. (ed.) *Advances in Cryptology - CRYPTO' 89 Proceedings*, vol. 435 of *Lecture Notes in Computer Science*, 218–238 (Springer New York, 1990).

[7] Rivest, R., Shamir, A. & Tauman, Y. How to leak a secret. In *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ASIACRYPT '01, 552–565 (Springer-Verlag, London, UK, UK, 2001).

[8] Chaum, D. & Antwerpen, H. V. Undeniable signatures. In Brassard, G. (ed.) *CRYPTO*, vol. 435 of *Lecture Notes in Computer Science*, 212–216 (Springer, 1989).

[9] Chaum, D. Blind signatures for untraceable payments. In Chaum, D., Rivest, R. & Sherman, A. (eds.) *Advances in Cryptology Proceedings of Crypto 82*, 199–203 (1983).

[10] Shor, P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* **26**, 1484–1509 (1997).

[11] Bennett, C. & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, 175–179 (IEEE Press, New York, 1984).

[12] Nikolopoulos, G. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A* **77**, 032348 (2008).

[13] Gottesman, D. & Chuang, I. Quantum digital signatures. Tech. Rep. (2001).

[14] Lu, X. & Feng, D. Quantum digital signature based on quantum one-way functions. In *Advanced Communication Technology, 2005, ICACT 2005. The 7th International Conference on*, vol. 1, 514–517 (2005).

[15] P. Wallden, V. Dunjko, A. Kent & E. Andersson Quantum digital signatures with quantum key distribution components. Tech. Rep. (2014).

[16] Wang, M., Chen, X. & Yang, Y. A blind quantum signature protocol using the ghz states. *Science China Physics, Mechanics and Astronomy* **56**, 1636–1641 (2013).

[17] Nielsen, M. & Chuang, I. *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences)* (Cambridge University Press, 2004), 1 edn.

[18] Carter, J. & Wegman, M. Universal classes of hash functions. *J. Comput. Syst. Sci.* **18**, 143–154 (1979).

[19] Bennett, C. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.* **68**, 3121–3124 (1992).

[20] Ekert, A. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).

[21] Ambainis, A., Mosca, M., Tapp, A. & de Wolf, R. Private quantum channels. In *FOCS*, 547–553 (IEEE Computer Society, 2000).

[22] Buhrman, H., Cleve, R., Watrous, J. & Wolf, R. D. Quantum fingerprinting. *Physical Review Letters* **87**, 2001 (2001).

[23] Skala, M. Hypergeometric tail inequalities: ending the insanity. *ArXiv e-prints* (2013). `1311.5939`.

[24] Chvátal, V. The tail of the hypergeometric distribution. *Discrete Mathematics* **25**, 285 – 287 (1979).

[25] Pinsker, S. *Information and information stability of random variables and processes*. Holden-Day series in time series analysis (Holden-Day, 1964).