Quantum Digital Signatures

(Daniel Gottesman, Isaac L. Chuang)
quant-ph/0105032
Quantum digital signatures

basic properties

• combine the concepts of public-key cryptography and one-time signatures with the fundamental properties of quantum mechanics

• used for signing classical messages (a single bit in this scheme)

• analogical to Lamport one-time signature, using quantum one-way function instead of classical one

• employing quantum states as public keys

• quantum nature of the scheme provides various cheating possibilities
Lamport one-time signatures

Signing of a single bit

- choose private keys $k_0$ for bit $b = 0$ and $k_1$ for $b = 1$
- compute public keys $f_i$ under an appropriate one-way function $f$

$$f_i = f(k_i), \quad i = 0 \text{ or } 1$$

- publish public-key pairs $(0, f_0)$ and $(1, f_1)$
- *Signing of a bit b*: reveal private key $(b, k_b)$
- *Verification*: check that $k_b$ maps to $f_b$
Quantum one-way functions

- a classical bit string on input
- quantum state as output, thus public keys are quantum states
- an attacker cannot acquire the complete information about public keys, due to Holevo’s theorem
- a number of public keys in circulation has to be limited
Quantum one-way functions - continued

- input – all classical bit strings $k$ of length $L$

- to each $k$ a quantum state $|f_k\rangle$ of $n$ qubits is assigned

- $L$ can be much larger than $n$

- the mapping $k \mapsto |f_k\rangle$ is impossible to invert

- by Holevo’s theorem, we can extract only $n$ classical bits from $n$-qubit state

- if we have $T$ copies of $|f_k\rangle$, we can learn only $Tn$ bits of information about $k$ and when $L - Tn \gg 1$, the chance to guess $k$ remains small
Swap test for equality

- we need to have a test for equality, i.e. to find out, given two outputs $|f_k\rangle$ and $|f_{k'}\rangle$, if $k = k'$
- this is carried out by so-called swap test circuit

\[ |0\rangle \xrightarrow{\text{H}} \xrightarrow{\text{H}} \text{measurement} \]

- if $|f_k\rangle = |f_{k'}\rangle$ then the result will be always $|0\rangle$
- if $|f_k\rangle \neq |f_{k'}\rangle$, the result will be $|0\rangle$ with probability $(1 + \delta^2)/2$ and $|1\rangle$ with probability $(1 - \delta^2)/2$, in case the states satisfy the condition $|\langle f_k | f_{k'} \rangle| \leq \delta$
- if the states are the same, they always pass the test, while if they are different, they sometimes fail
Verifying an output of $f$

- given $k$, how to check that a state $|\phi\rangle = |f_k\rangle$

- we can perform the inverse operation to computing of the mapping $|k\rangle|0^{(n)}\rangle \mapsto |k\rangle|f_k\rangle$ and then measure the second register: if $|\phi\rangle \neq |f_k\rangle$, we will see a nonzero result with probability $1 - |\langle \phi |f_k\rangle|^2$

- it is again probabilistic
Specification of keys and parameters

• the signatory Alice prepares her private keys – pairs \( \{k_0^i, k_1^i\} \) of \( L \) - bit strings, \( 1 \leq i \leq M \).

• \( M \) keys are used for signing a single bit

• the public keys \( |f_{k_0^i}⟩, |f_{k_1^i}⟩ \) are computed under an appropriate quantum one-way function \( f \)

• \( T < L/n \) copies of each public key are available

• all participants will now how to implement the mapping \( k \mapsto |f_k⟩ \) and also choose the tresholds \( c_1 \) and \( c_2 \), for acceptance and rejection of the signature. The threshold \( c_1 \) reflects the noise of a channel (0 in the absence of noise) The gap \( c_2 - c_1 \) determines Alice’s chances of cheating.


Signing and verification

A single bit-message is sent by Alice this way:

1. Alice send the message $(b, k_b^1, k_b^2, \ldots, k_b^M)$ over an insecure classical channel.

2. Each recipient verifies that revealed public keys $k_b^i$ are mapped into $|f_{k_b^i}\rangle$ and recipient $R$ counts the number of incorrect keys. Let this number be $s_R$.

3. Recipent $R$ accepts the message as valid and transferable (1-ACC) if $s_R \leq c_1 M$, rejects it (REJ) if $s_R \geq c_2 M$ and accepts it without further transferability (0-ACC) if $c_1 M < s_R < c_2 M$.

4. Discard all used and used keys.

- **REJ** – we cannot safely say anything about the authenticity of the message.

- **1-ACC and 0-ACC** – imply the validity of the message but they differ in the following sense. The result 1-ACC means that the recipient is sure that any other recipient will also conclude the message is valid, whereas with the result 0-ACC the other recipient can conclude it as invalid.
Security - forgery

• The forger Eve is able to acquire at most only $Tn$ bits (Holevo’s theorem) of information about each of public keys (if she has access to all $T$ copies). Thus, she lacks at least $L - Tn$ bits of information and can guess correctly on about $G = \frac{2M}{2L - Tn}$ keys. If Eve did not guess a key correctly, she can claim that incorrect $k'$ is valid and the probability that the receiver’s measurement test will support this claim is no more than $\delta^2$.

• Each recipient finds out that at least $(1 - \delta^2)(M - G)$ of public keys will fail $\rightarrow$ we choose $c_2$, so that $(1 - \delta^2)(M - G) > c_2M$. 

Security - repudiation

- i.e. Alice wants to disagree Bob and Charlie about validity of a message
- we can use a trusted key distribution center with authenticated links to all recipients – it performs swap tests on public keys supplied by Alice and distribute public keys
- Alice can cheat by preparing the state $|\phi\rangle_B|\psi\rangle_C + |\psi\rangle_B|\phi\rangle_C$, which always passes swap test, but public keys go randomly to Bob and Charlie and she cannot control which of them gets the valid key
- it is unlikely that Bob and Charlie will get definite but differing result (1-ACC, REJ), the gap $c_1M$ and $c_2M$ protects them
Extensions

• key distribution without a trusted key distribution center

• distributed swap tests between the recipients can be used instead

• signing a multiple-bit message

• larger number of results (s-ACC) - levels of transferability