Quantum digital signatures with smaller public keys

Boris Škorić
Eindhoven University of Technology
b.skoric@tue.nl

Information-theoretically secure signatures

1. The Lamport signature

How to sign a bit; based on one-way function \( f \) [5].

- Private key \( k_i \), \( k_i \). Public key \((P_0, P_1)\) with \( P_i = f(k_i) \).
- Signing a message \( m \in \{0,1\} \): publish \( k_m \).
- Verification: check if hashing the published \( k_m \) yields \( P_m \).
- Keys are discarded after a single use.

The security is based on the assumption that \( f \) is difficult to invert. Quantum digital signatures are inspired by the Lamport scheme, but they make use of information-theoretic one-wayness.

2. Gottesman-Chuang signature

How to sign a bit; based on the one-wayness of quantum state preparation [4].

- Private key \( k_i \), \( k_i \). Public key \((|P_0\rangle, |P_1\rangle)\) consists of two quantum states. \( |P_0\rangle = |f(k_0)\rangle \), \( |P_1\rangle = |f(k_1)\rangle \). Here \( F \) is a mapping that embeds a bitstring in a Hilbert space (e.g., fingerprinting states).
- Signing a message \( m \in \{0,1\} \): publish \( k_m \).
- Verification: Project state \(|P_m\rangle\) onto direction \( F(k_m) \) and check if result is ‘1’.
- Keys are discarded after a single use.

In order to reduce false positives, each verifier gets multiple copies of the public key.

3. Fingerprinting states

Let \( H \) be a d-dimensional Hilbert space with basis \(|0\rangle, \ldots, |d-1\rangle \). Let \( x \in \{0,1\}^d \). The fingerprinting state \(|F(x)\rangle\) is defined as [6]

\[
|F(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} (-1)^j |j\rangle.
\]

This state is created using \( d \) classical bits of information, but at most \( \log \dim H = \log d \) bits can be learned via measurement. \(|F(x)\rangle\) is a compact representation of \( x \) that hides \( x \).

4. Efficient Gottesman-Chuang

More efficient use of resources than public key repetition [4]. Message \( m \in \{0,1\}^S \). Error-correcting code with codewords in \( \{0,1\}^S \). Codeword \( c_m \).

- The bits of \( c_m \) are individually signed as above; verifiers hold only one copy of each \( |P_i\rangle \).
- Verifier counts number of ‘0’ projection outcomes. Must be sufficiently low.
- \( d_{\text{min}} \approx T \log T \), with \( T = \text{number of verifiers} \).
- \#qubits spent per message bit: more than \( \log(T \log T) \).

5. Our scheme

Alphabet \( S = \{0, \ldots, S-1\} \). Message \( m \in \mathcal{S}^S \). Codeword \( c_m \in \mathcal{S}^S \).

- Private key \( k_0, \ldots, k_{S-1} \). Public key \((|P_0\rangle, \ldots, |P_{S-1}\rangle)\), with \(|P_i\rangle = |F(k_i)\rangle \).
- Signing: For each \( i \in \{1, \ldots, N\} \) reveal \( k_i \).
- If \( c_m[k_i] = s \) then reveal \( k_i \), except for a small window of width \( d/S \) at ‘position’ \( s \).
- Choice of window encodes a symbol in \( S \).
- Verification: Project \(|P_i\rangle\) onto the sum of all \( 2^d/S \) fingerprinting states that are consistent with the revealed part of \( k_i \). Number of ‘0’ outcomes must be sufficiently low.

\[
d_{\text{min}} \approx S T \log ST
\]

\[
\frac{\#\text{qubits per message bit}}{\text{msg. bit}} > \frac{\log(S T \log ST)}{\log S}
\]

Discussion

- Increasing the data density by a factor \( \log S \) only adds a term \( \log S \) to the size of a public key.
- The improvement factor \( 1/\log S \) in (2) due to the increased alphabet is hampered slightly by the growing \( d_{\text{min}} \approx ST \log ST \), but overall it is favorable to increase \( S \).
- The effect of allowing \( k \) to be opened in multiple ways is that forgery becomes easier. This has to be counteracted by increasing the message length in order to achieve distinguishability between an attacker’s error rate and the genuine error rate.

References