Quantum digital signatures with smaller public keys

Boris Škorić

Eindhoven University of Technology

b.skoric@tue.nl

Information-theoretically secure signatures

All practical signature schemes depend on assumptions about the computational hardness of certain problems. *Unconditionally secure* signatures have been designed [1, 2, 3], but they require a fixed set of participants and involve a large amount of communication. Furthermore, they require either a trusted third party or secret channels between pairs of participants.

Gottesman and Chuang [4] introduced *quantum digital signatures*, which are also unconditionally secure but alleviate some of these disadvantages. Mind you, now the verifiers are supposed to have long-term quantum memory. At some point in the future this may become realistic.

Our contribution is a variant of the Gottesman-Chuang scheme that requires less quantum memory. It is based on a different use of *fingerprinting states* and a generalisation to non-binary alphabets.

1. The Lamport signature

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

- Private key k_0, k_1. 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_0, k_1 is classical. 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 $\mathcal{H}$ be a d-dimensional Hilbert space with basis $|0\rangle, \cdots, |d-1\rangle$. Let $x \in \{0,1\}^d$. The fingerprinting state $|F(x)\rangle$ is defined as [6]

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

This state is created using d classical bits of information, but at most $\log \dim \mathcal{H} = \log d$ 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 $m \in \{0,1\}^K$. Error-correcting code with codewords in $\{0,1\}^N$. Codeword c_m.

- The bits of c_m are individually signed as above; verifiers hold only one copy of each $|P\rangle$.
- Verifier counts number of '0' projection outcomes. Must be sufficiently low.

$d_{\rm min} \approx T \log T$, with T = number of verifiers.

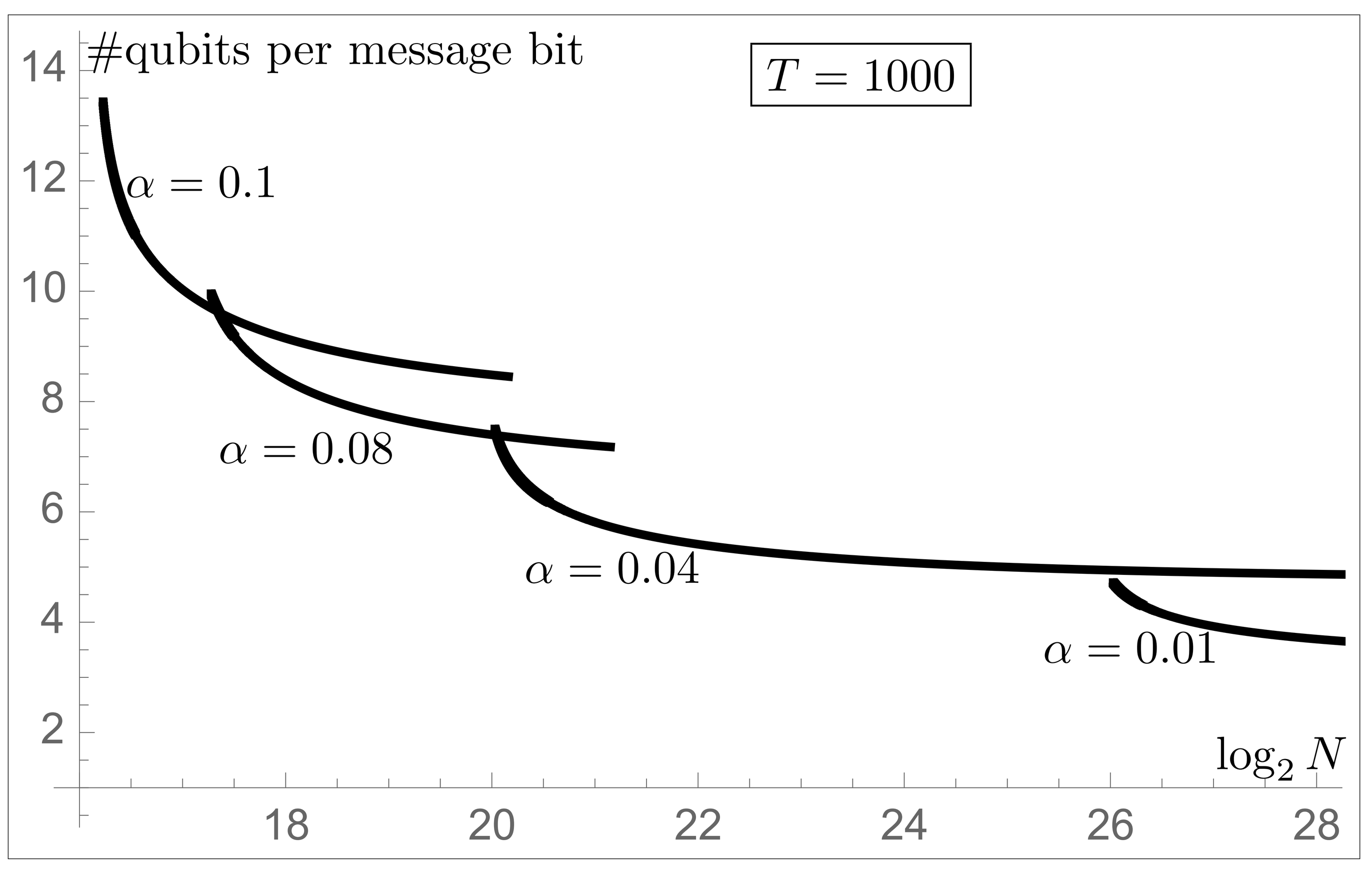
#qubits spent per message bit: more than $\log(T \log T)$.

5. Our scheme

Alphabet $\mathcal{S} = \{0, \ldots, S-1\}$. Message $m \in \mathcal{S}^K$. Codeword $C_m \in \mathcal{S}^N$.

- Private key $k_1, \ldots, k_N$, with $k_i \in \{0,1\}^d$. Public key $|P_1\rangle \cdots |P_N\rangle$, with $|P_i\rangle = |F(k_i)\rangle$.
- **Signing**: For each $i \in \{1, \ldots, N\}$ reveal *part of* k_i. If $C_m[i] = s$ then reveal k_i except for a small window of width d/S at 'position' s. The choice of window encodes a symbol in $\mathcal{S}$.
- **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.

$$d_{\rm min} \approx ST \log ST \qquad \frac{\#\text{qubits}}{\text{msg. bit}} > \frac{\log(ST \log ST)}{\log S} \tag{2}$$



$\alpha = 1/S$. Each curve was created by varying d. For comparison: Gottesman-Chuang spends > 13.3 qubits per message bit at $T = 1000$ verifiers.

Discussion

- **Increasing the data density by a <u>factor</u> log S only adds a <u>term</u> 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 $d_{\rm min} \approx ST \log ST$, 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

[1] D. Chaum and S. Roijackers. Unconditionally-secure digital signatures. In *Crypto 1990*, volume 537 of *LNCS*, pages 206–214. Springer-Verlag Berlin Heidelberg, 1991.

[2] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai. Unconditionally secure digital signature schemes admitting transferability. In *Asiacrypt 2000*, volume 1976 of *LNCS*, pages 130–142, 2000.

[3] C.M. Swanson and D.R. Stinson. Unconditionally secure signature schemes revisited. In *Information Theoretic Security (ICITS) 2011*, volume 6673 of *LNCS*, pages 100–116.

[4] D. Gottesman and I.L. Chuang. Quantum digital signatures, 2001. `https://arxiv.org/abs/quant-ph/0105032`.

[5] L. Lamport. Constructing digital signatures from a one-way function, 1979. Technical Report CSL-98, SRI International.

[6] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum fingerprinting. *Physical Review Letters*, 87(16):167902, 2001.

[7] B. Škorić. Quantum digital signatures with smaller public keys, 2020. `https://arxiv.org/abs/2012.15493`.