Quantum Digital Signatures

Dominic Moylett*
Quantum Engineering Centre for Doctoral Training
University of Bristol
(Dated: May 2, 2016)

While classical cryptography has relied on the assumed existence of one-way functions for proofs of security, quantum cryptography has given us information theoretically secure secret sharing. This has been achieved via quantum key distribution, utilising the uncertainty principle to limit what an eavesdropper can discover about a shared private key. Another application where we can have provably secure primitives is that of quantum digital signatures, which are used for authenticating that a message did come from a specific user. In this essay, we summarise the theoretical and experimental achievements in quantum digital signatures, and discuss their current limitations.

I. INTRODUCTION

II. PRELIMINARIES

Definition II.1. *A function* $f : \mathbb{N} \to \mathbb{R}$ *is negligible iff* $\forall\ c > 0\ \exists\ n_0 \in \mathbb{N}$ *such that* $\forall\ n \geq n_0, |f(n)| < \frac{1}{n^c}$.

The most common example of negligible functions are functions of the form $2^{-p(n)}$ for some positive polynomial p.

III. DEFINITION OF DIGITAL SIGNATURES

A digital signature scheme consists of the following stages:

Key Sharing: Alice generates a signing key sk and a verification key vk. The signing key is kept to herself, while the verification key is shared with other parties.

Message Signing: Alice takes a message m and her signing key sk and produces a signature for that message s_m.

Message Verification: Another party, Bob, takes a message m, Alice's verification key vk and a signature s_m and accepts if they think the message was sent and signed by Alice, otherwise they reject.

Another definition of verification used in, for example, [1] has three different options for Bob. In this definition Bob can output:

1-ACC: He thinks the message-signature pair is valid and other parties will also find the message to be valid.

0-ACC: He thinks the message-signature pair is valid and other parties will not find the message to be valid.

REJ: He thinks the message-signature pair is invalid.

For security, we care about two properties with digital signatures:

Repudiation: The probability that Alice is able to convince Bob that a message-signature pair is valid and convince another party Charlie that the same pair is invalid is negligible in terms of the security parameter (often the length of the signature).

Forgery: The probability that Bob can in polynomial time create a valid message-signature pair he has not previously seen sent by Alice is negligible in terms of the security parameter.

IV. LAMPORT'S ONE-TIME DIGITAL SIGNATURE

The original quantum digital signature was inspired from a classical family of digital signatures. This family of signatures were first published by Lamport[2], and are reliant on the existence of one-way functions, defined below.

Definition IV.1. *Let* $\mathcal{X}, \mathcal{Y}$ *be arbitrary sets. A function* $f : \mathcal{X} \to \mathcal{Y}$ *is one-way iff* f *can be computed in polynomial time, but for any polynomial-time randomised adversary* $f^{-1} : \mathcal{Y} \to \mathcal{X}$ *and uniformly selected* $x \in \mathcal{X}, \Pr[f(f^{-1}(x)) = f(x)]$ *is negligible in terms of the length of* x *in bits.*

For a one-way function f, then Lamport's one-time digital signature scheme is defined as follows for Alice signing an m-bit message:

Key Sharing: Alice generates m pairs of uniformly selected random integers (k_0^i, k_1^i). These will act as Alice's signing key, while the verification key will be the pairs $(f(k_0^i), f(k_1^i))$ for $i \in \{0, ..., m-1\}$.

Message Signing: For each bit m_i of Alice's message, she sends $k_{m_i}^i$ as her signature for that bit.

* dominic.moylett@bristol.ac.uk

Message Verification: Given Alice's verification key (v_0^i, v_1^i) and her signature $k_{m_i}^i$, her message m_i can be verified by accepting if $v_{m_i}^i = f(k_{m_i}^i)$ and rejecting otherwise.

Because this signature scheme is classical and deterministic, it is trivial for any verifying parties to share their copies of the message and verification keys and thus impossible for Alice to repudiate the message. As for forgery, if it is possible for an adversary to forge a message given only one message from Alice then it is possible to invert f, thus f is not a one-way function.

Note that this signature scheme can only be used for verifying a single m-bit message. This is because if an attacker has signatures for two different messages M, M' then they can construct the valid signature for the new message $m_0 m_1 ... m_i' ... m_{m-1}$, where $m_i \neq m_i'$.

V. QUANTUM DIGITAL SIGNATURES

VI. EXPERIMENTAL ACHIEVEMENTS

VII. CURRENT LIMITATIONS

VIII. CONCLUSION

[1] D. Gottesman and I. Chuang, "Quantum digital signatures," (2001), arXiv:quant-ph/0105032.
[2] L. Lamport, Technical Report SRI-CSL-98 (1979).