Quantum Pseudosignatures

J. Müller-Quade
Arbeitsgruppe Quantum Computing *Prof. Beth,*
E.I.S.S., Fakultät für Informatik, Universität Karlsruhe
(August 29^{th}, 2001)

A pseudosignature is a piece of evidence with which the receiver of a message can prove to other players the identity of the originator of that message. In contrast to a signature a pseudosignature has a restricted *transferability* [5].

The full paper presents the first quantum pseudosignature scheme where the resulting pseudosignature and the verification procedures are classical. Therefore no long term quantum storage is needed for this scheme.

For an unconditionally secure pseudosignature scheme the signature verification procedure is either a quantum procedure (see the quantum digital signatures of [2]) or all classical verification procedures of the different players must be different [1,5,4].

In the scheme of [1,5] all players anonymously send m random numbers to the signer. The signer authenticates his message with each random number. Each player can only verify a part of the signature, but it is impossible for the signer to generate a signature which is accepted by the receipient of the signed document.

This abstract considers *resilient* protocols for pseudosignatures.

Definition 1 *A pseudosignature scheme is called* resilient *if no collusion not containing the signer can keep the signer from generating a valid pseudosignature. Furthermore if a collusion containing the signer aborts the protocol the signer will be detected cheating.*

We show that in the classical three party case the signer can abort the anonymous data transfer without being identified as a cheater (compare [3]). The basic idea, explained in a three party setting, is that the signer refuses to cooperate with the player who is not the recepient of the signature, then the classical anonymous channel protocol (the dining cryptographers protocol) cannot work any more, but the recepient of the signature does not know who is cheating. The protocol is aborted but not all honest players know that it was aborted by the signer. The implementation is not *resilient.* Our contribution is a new anonymous data transfer based on quantum cryptography. Using this anonymous channel in the scheme of [1,5] we obtain resilient quantum pseudosignatures which are impossible classically.

We will not give the protocol for pseudosignatures here, but we will focus on the anonymous channels used. We will state a protocol for anonymous key exchange in the three party setting below. Proofs as well as the generalization to more than three parties are omitted here. This anonymous key exchange can be extended to an anonymous channel, but in the form below it is sufficient to be used in the schemes of [1,5] to give a resilient protocol.

Anonymous Quantum Key Exchange of {Bob, Carol} with Alice via Carol

Bob and Carol agree on a string $b_1 \dots b_l$ unknown to Alice

`FOR ALL` $i \in \{1, \dots, l\}$ `DO`

> `IF` $b_i = 0$ `THEN` Carol performs a quantum key exchange with Alice where she and Alice use the broadcast channel instead of the authenticated classical channel.
>
> `ELSE` Bob performs a quantum key exchange with Alice, but sends the quantum states to Carol before Carol forwards them to Alice, Bob lets Carol broadcast everything which is supposed to be sent over the authenticated classical channel to Alice, and Alice broadcasts all her classical messages.

`OD`

---

[1] D. Chaum and S. Roijakkers. Unconditionally secure digital signatures. In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology: Crypto '90*, volume 537 of *LNCS*, pages 206–215. Springer-Verlag, Berlin, 1990.

[2] D. Gottesman and I. Chuang. Quantum digital signatures. Appeared as Los Alamos preprint quant-ph/0105032.

[3] J. Müller-Quade and H. Imai. More robust multiparty protocols with oblivious transfer. Technical Report of ISEC 11 Technical Meeting, Tokyo, also as Los Alamos preprint quant-ph/0101020, October 2000.

[4] T. Nishioka, G. Hanaoka, and H. Imai. A new digital signature scheme on id-based key sharing infrastructures. In *Proc. of 1999 International Information Security Workshop (ISW'99)*, volume 1729 of *LNCS*, pages pp. 259–270. Springer-Verlag, 1999.

[5] B. Pfitzmann and A. Waidner. Unconditional byzantine agreement for any number of faulty processors. In *Proc. STACS'92*, volume 577 of *LNCS*, pages 339–350. Springer-Verlag, Berlin, 1992. This paper generalizes the result of [1].