Cryptology ePrint Archive: Report 2013/126

Direct Proof of Security of Wegman-Carter Authentication with Partially Known Key

Aysajan Abidin and Jan-Åke Larsson

Abstract: Information-theoretically secure (ITS) authentication is needed in Quantum Key Distribution (QKD). In this paper, we study security of an ITS authentication scheme proposed by Wegman\&Carter, in the case of partially known authentication key. This scheme uses a new authentication key in each authentication attempt, to select a hash function from an Almost Strongly Universal$_2$ hash function family. The partial knowledge of the attacker is measured as the trace distance between the authentication key distribution and the uniform distribution; this is the usual measure in QKD. We provide direct proofs of security of the scheme, when using partially known key, first in the information-theoretic setting and then in terms of witness indistinguishability as used in the Universal Composability (UC) framework. We find that if the authentication procedure has a failure probability ϵ and the authentication key has an ϵ' trace distance to the uniform, then under ITS, the adversary's success probability conditioned on an authentic message-tag pair is only bounded by $\epsilon+|\mT|\epsilon'$, where $|\mT|$ is the size of the set of tags. Furthermore, the trace distance between the authentication key distribution and the uniform increases to $|\mT|\epsilon'$ after having seen an authentic message-tag pair. Despite this, we are able to prove directly that the authenticated channel is indistinguishable from an (ideal) authentic channel (the desired functionality), except with probability less than $\epsilon+\epsilon'$. This proves that the scheme is ($\epsilon+\epsilon'$)-UC-secure, without using the composability theorem.

Category / Keywords: secret-key cryptography / Authentication, Strongly Universal hash functions, Partially known key, Trace distance, Universal Composability, Quantum Key Distribution.

Date: received 1 Mar 2013

Contact author: aysajan at isy liu se