Cryptology ePrint Archive: Report 2011/034

Secure Authentication from a Weak Key, Without Leaking Information

Niek J. Bouman and Serge Fehr

Abstract: We study the problem of authentication based on a weak key in the information-theoretic setting. A key is weak if its min-entropy is an arbitrary small fraction of its bit length. This problem has recently received considerable attention, with different solutions optimizing different parameters. We study the problem in an extended setting, where the weak key is as a one-time session key that is derived from a public source of randomness with the help of a (potentially also weak) long-term key. Our goal now is to authenticate a message by means of the weak session key in such a way that (nearly) no information on the long-term key is leaked. Ensuring privacy of the long-term key is vital for the long-term key to be re-usable. Previous work has not considered such a privacy issue, and previous solutions do not seem to satisfy this requirement. We show the existence of a practical four-round protocol that provides message authentication from a weak session key and that avoids non-negligible leakage on the long-term key. The security of our scheme also holds in the quantum setting where the adversary may have limited quantum side information on the weak session key. As an application of our scheme, we show the existence of an identification scheme in the bounded quantum storage model that is secure against a man-in-the-middle attack and that is truly password-based: it does not need any high entropy key, in contrast to the scheme proposed by Damgaard et al..

Category / Keywords: secret-key cryptography / authentication, privacy amplification, weak key, password-based identification, quantum cryptography

Publication Info: Full version of EUROCRYPT '11 paper

Date: received 19 Jan 2011, last revised 4 Feb 2011

Contact author: bouman at cwi nl

Available formats: PDF | BibTeX Citation

Note: Corrected a minor flaw in Sect 7.1

Version: 20110204:160439 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]