Cryptology ePrint Archive: Report 2011/300

One-round Strongly Secure Key Exchange with Perfect Forward Secrecy and Deniability

Cas Cremers and Michele Feltz

Abstract: Traditionally, secure one-round key exchange protocols in the PKI setting have either achieved perfect forward secrecy, or forms of deniability, but not both. On the one hand, achieving perfect forward secrecy against active attackers seems to require some form of authentication of the messages, as in signed Diffie-Hellman style protocols, that subsequently sacrifice deniability. On the other hand, using implicit authentication along the lines of MQV and descendants sacrifices perfect forward secrecy in one round and achieves only weak perfect forward secrecy instead.

We show that by reintroducing signatures, it is possible to satisfy both a very strong key-exchange security notion, which we call eCK-PFS, as well as a strong form of deniability, in one-round key exchange protocols. Our security notion for key exchange is stronger than, e.g., the extended-CK model, and captures perfect forward secrecy. Our notion of deniability, which we call peer-and-time deniability, is stronger than that offered by, e.g., the SIGMA protocol.

We propose a concrete protocol and prove that it satisfies our definition of key-exchange security in the random oracle model as well as peer-and-time deniability. The protocol combines a signed-Diffie-Hellman message exchange with an MQV-style key computation, and offers a remarkable combination of advanced security properties.

Category / Keywords: cryptographic protocols / Key Exchange, Perfect Forward Secrecy, Deniability, PKI

Date: received 6 Jun 2011, last revised 26 Oct 2011

Contact author: cas cremers at inf ethz ch