Cryptology ePrint Archive: Report 2011/484

XMSS - A Practical Forward Secure Signature Scheme based on Minimal Security Assumptions

Johannes Buchmann, Erik Dahmen, and Andreas Hülsing

Abstract: We present the hash-based signature scheme \xmss. It is the first provably (forward) secure and practical signature scheme with minimal security requirements: a pseudorandom and a second preimage resistant (hash) function family. Its signature size is reduced to less than 25\% compared to the best provably secure hash based signature scheme.

Category / Keywords: public-key cryptography / digital signature, practical, minimal security assumptions, hash-based signatures, forward security, provable security

Publication Info: An extended abstract appears in Proceedings of PQCrypto 2011

Date: received 8 Sep 2011, last revised 25 Nov 2011

Contact author: huelsing at cdc informatik tu-darmstadt de