Cryptology ePrint Archive: Report 2011/191

On the Security of the Winternitz One-Time Signature Scheme

Johannes Buchmann and Erik Dahmen and Sarah Ereth and Andreas Hülsing and Markus Rückert

Abstract: We show that the Winternitz one-time signature scheme is existentially unforgeable under adaptive chosen message attacks when instantiated with a family of pseudo random functions. Compared to previous results, which require a collision resistant hash function, our result provides significantly smaller signatures at the same security level. We also consider security in the strong sense and show that the Winternitz one-time signature scheme is strongly unforgeable assuming additional properties of the pseudo random function. In this context we formally define several key-based security notions for function families and investigate their relation to pseudorandomness. All our reductions are exact and in the standard model and can directly be used to estimate the output length of the hash function required to meet a certain security level.

Category / Keywords: public-key cryptography / Hash-based signatures, post-quantum signatures, pseudorandom functions, security reductions.

Publication Info: Full version. An extended abstract of this paper appears in Proceedings of Africacrypt 2011

Date: received 13 Apr 2011

Contact author: huelsing at cdc informatik tu-darmstadt de