Cryptology ePrint Archive: Report 2011/703

Waters Signatures with Optimal Security Reduction

Dennis Hofheinz and Tibor Jager and Edward Knapp

Abstract: Waters signatures (Eurocrypt 2005) can be shown existentially unforgeable under chosen-message attacks under the assumption that the computational Diffie-Hellman problem in the underlying (pairing-friendly) group is hard. The corresponding security proof has a reduction loss of O(l*q), where l is the bitlength of messages, and q is the number of adversarial signature queries. The original reduction could meanwhile be improved to O(\sqrt{l}*q) (Hofheinz and Kiltz, Crypto 2008); however, it is currently unknown whether a better reduction exists. We answer this question as follows:

(a) We give a simple modification of Waters signatures, where messages are encoded such that each two encoded messages have a suitably large Hamming distance. Somewhat surprisingly, this simple modification suffices to prove security under the CDH assumption with a reduction loss of O(q).

(b) We also show that any black-box security proof for a signature scheme with re-randomizable signatures must have a reduction loss of at least \Omega(q), or the underlying hardness assumption is false. Since both Waters signatures and our variant from (a) are re-randomizable, this proves our reduction from (a) optimal up to a constant factor.

Understanding and optimizing the security loss of a cryptosystem is important to derive concrete parameters, such as the size of the underlying group. We provide a complete picture for Waters-like signatures: there is an inherent lower bound for the security loss, and we show how to achieve it.

Category / Keywords: public-key cryptography / Digital signatures, Waters signatures, provable security, black-box reductions

Publication Info: PKC 2012

Date: received 23 Dec 2011, last revised 18 Sep 2012

Contact author: tibor jager at kit edu