Cryptology ePrint Archive: Report 2013/171

Confined Guessing: New Signatures From Standard Assumptions

Florian Böhl and Dennis Hofheinz and Tibor Jager and Jessica Koch and Christoph Striecks

Abstract: We put forward a new technique to construct very efficient and compact signature schemes. Our technique combines several instances of an only mildly secure signature scheme to obtain a fully secure scheme. Since the mild security notion we require is much easier to achieve than full security, we can combine our strategy with existing techniques to obtain a number of interesting new (stateless and fully secure) signature schemes. Concretely, we get:

* A scheme based on the computational Diffie-Hellman (CDH) assumption in pairing-friendly groups. Signatures contain O(1) and verification keys O(log(k)) group elements, where k is the security parameter. Our scheme is the first CDH-based scheme with such compact verification keys.

* A scheme based on the (non-strong) RSA assumption in which both signatures and verification keys contain O(1) group elements. Our scheme is significantly more efficient than existing RSA-based schemes.

* A scheme based on the Short Integer Solutions (SIS) assumption. Signatures contain O(log(k) m) and verification keys O(n m) Z_p-elements, where p may be polynomial in k, and n, m denote the usual SIS matrix dimensions. Compared to state-of-the-art SIS-based schemes, this gives very small verification keys, at the price of slightly larger signatures.

In all cases, the involved constants are small, and the arising schemes provide significant improvements upon state-of-the-art schemes. The only price we pay is a rather large (polynomial) loss in the security reduction. However, this loss can be significantly reduced at the cost of an additive term in signature and verification key size.

Category / Keywords: digital signatures, CDH assumption, pairing-friendly groups, RSA assumption, SIS assumption

Publication Info: A merge of this paper and http://eprint.iacr.org/2012/480 is accepted at Eurocrypt 2013.

Date: received 25 Mar 2013, last revised 27 Mar 2013

Contact author: florian boehl at kit edu