Cryptology ePrint Archive: Report 2011/296

Short Signatures From Weaker Assumptions

Dennis Hofheinz and Tibor Jager and Eike Kiltz

Abstract: We provide constructions of (m,1)-programmable hash functions (PHFs) for m >= 2. Mimicking certain programmability properties of random oracles, PHFs can, e.g., be plugged into the generic constructions by Hofheinz and Kiltz (J. Cryptol. 2011) to yield digital signature schemes from the strong RSA and strong q-Diffie-Hellman assumptions. As another application of PHFs, we propose new and efficient constructions of digital signature schemes from weaker assumptions, i.e., from the (standard, non-strong) RSA and the (standard, non-strong) q-Diffie-Hellman assumptions. The resulting signature schemes offer interesting trade-off s between efficiency/signature length and the size of the public-keys. For example, our q-Diffie-Hellman signatures can be as short as 200 bits; the signing algorithm of our Strong RSA signature scheme can be as efficient as the one in RSA full domain hash; compared to previous constructions, our RSA signatures are shorter (by a factor of roughly 2) and we obtain a considerable efficiency improvement (by an even larger factor). All our constructions are in the standard model, i.e., without random oracles.

Category / Keywords: public-key cryptography / digital signatures, RSA assumption, q-DH assumption, programmable hash functions

Publication Info: Preliminary version appears in Proceedings of ASIACRYPT 2011. This is the full version.

Date: received 3 Jun 2011, last revised 4 Oct 2011

Contact author: eike kiltz at rub de