Cryptology ePrint Archive: Report 2013/140

Limitations of the Meta-Reduction Technique: The Case of Schnorr Signatures

Marc Fischlin and Nils Fleischhacker

Abstract: We revisit the security of Fiat-Shamir signatures in the non-programmable random oracle model. The well-known proof by Pointcheval and Stern for such signature schemes (Journal of Cryptology, 2000) relies on the ability to re-program the random oracle, and it has been unknown if this property is inherent. Pailler and Vergnaud (Asiacrypt 2005) gave some first evidence of the hardness by showing via meta-reduction techniques that algebraic reductions cannot succeed in reducing key-only attacks against unforgeability to the discrete-log assumptions. We also use meta-reductions to show that the security of Schnorr signatures cannot be proven equivalent to the discrete logarithm problem without programming the random oracle. Our result also holds under the one-more discrete logarithm assumption but applies to a large class of reductions, we call *single-instance* reductions, subsuming those used in previous proofs of security in the (programmable) random oracle model. In contrast to algebraic reductions, our class allows arbitrary operations, but can only invoke a single resettable adversary instance, making our class incomparable to algebraic reductions.

Our main result, however, is about meta-reductions and the question if this technique can be used to further strengthen the separations above. Our answer is negative. We present, to the best of our knowledge for the first time, limitations of the meta-reduction technique in the sense that finding a meta-reduction for general reductions is most likely infeasible. In fact, we prove that finding a meta-reduction against a potential reduction is equivalent to finding a ``meta-meta-reduction" against the strong existential unforgeability of the signature scheme. This means that the existence of a meta-reduction implies that the scheme must be insecure (against a slightly stronger attack) in the first place.

Category / Keywords: public-key cryptography / Meta-Reduction, Random Oracle Model, Schnorr Signature

Publication Info: An extended abstract of this paper appears at Eurocrypt 2013.

Date: received 8 Mar 2013

Contact author: fleischhacker at cs uni-saarland de