Cryptology ePrint Archive: Report 2011/087

On the Instantiability of Hash-and-Sign RSA Signatures

Yevgeniy Dodis and Iftach Haitner and Aris Tentes

Abstract: The hash-and-sign RSA signature is one of the most elegant and well known signatures schemes, extensively used in a wide variety of cryptographic applications. Unfortunately, the only existing analysis of this popular signature scheme is in the random oracle model, where the resulting idealized signature is known as the RSA Full Domain Hash signature scheme (RSA-FDH). In fact, prior work has shown several “uninstantiability” results for various ab- stractions of RSA-FDH, where the RSA function was replaced by a family of trapdoor random permutations, or the hash function instantiating the random oracle could not be keyed. These abstractions, however, do not allow the reduction and the hash function instantiation to use the algebraic properties of RSA function, such as the multiplicative group structure of Z&#8727;n. In contrast, the multiplicative property of the RSA function is critically used in many standard model analyses of various RSA-based schemes. Motivated by closing this gap, we consider the setting where the RSA function representation is generic (i.e., black-box) but multiplicative, whereas the hash function itself is in the standard model, and can be keyed and exploit the multiplicative properties of the RSA function. This setting abstracts all known techniques for designing provably secure RSA-based signatures in the standard model, and aims to address the main limitations of prior uninstantiability results. Unfortunately, we show that it is still impossible to reduce the security of RSA-FDH to any natural assumption even in our model. Thus, our result suggests that in order to prove the security of a given instantiation of RSA-FDH, one should use a non-black box security proof, or use specific properties of the RSA group that are not captured by its multiplicative structure alone. We complement our negative result with a positive result, showing that the RSA-FDH signatures can be proven secure under the standard RSA assumption, provided that the number of signing queries is a-priori bounded.

Category / Keywords: RSA Signature, Hash-and-Sign, Full Domain Hash, Random Oracle Heuristic, Generic Groups, Black-Box Reductions

Date: received 23 Feb 2011, last revised 29 Dec 2011

Contact author: tentes at cs nyu edu

Available formats: PDF | BibTeX Citation

Version: 20111229:151218 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]