

Cryptology ePrint Archive: Report 2011/713

A server-aided verification signature scheme without random oracles

Bin Wang and Qing Zhao

Abstract: Server-aided verification(SAV) signature is useful for power-constrained devices since a powerful server can assist in performing costly operations such as pairing operations. Wu et al. [13] defined three security notions for SAV protocol to prevent a server from convincing a verifier that an invalid signature is valid. Security against strong collusion attack provides the strongest security guarantee among these notions. They [13] constructed SAV protocols that meet the requirement of these notions respectively. But they did not provide concrete running time to show that the running time of a verifier in their SAV protocol is strictly less than that of a verifier in the original verification protocol. In addition, a problem left open by their work is to design SAV signature which is unforgeable without random oracles as well as sound against strong collusion attack. To address the above issues, we first choose to design a SAV protocol called SAV-Hofheinz for a short signature proposed by Hofheinz unforgeable in the standard model. Then we implement SAV-Hofheinz by the PBC library and shows that the running time of a verifier in SAV-Hofheinz is strictly less than that of a verifier in the verification protocol of Hofheinz short signature.

Category / Keywords: public-key cryptography /

Date: received 16 Dec 2011

Contact author: jxbin76 at yahoo cn

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20120102:202837 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]