Submission Received

Your submission has been received and will appear as follows.

Cryptology ePrint Archive: Submission xxxx/132

Compact E-Cash and Simulatable VRFs Revisited

Mira Belenkiy and Melissa Chase and Markulf Kohlweiss and Anna Lysyanskaya

Abstract: Efficient non-interactive zero-knowledge proofs are a powerful tool for solving many cryptographic problems. We apply the recent Groth-Sahai (GS) proof system for pairing product equations (Eurocrypt 2008) to two related cryptographic problems: compact e-cash (Eurocrypt 2005) and simulatable verifiable random functions (CRYPTO 2007).

We present the first efficient compact e-cash scheme that does not rely on a random oracle in its security proof. To this end we construct efficient GS proofs for signature possession, pseudo randomness and set membership. The GS proofs for pseudorandom functions give rise to a much cleaner and substantially faster construction of simulatable verifiable random functions (sVRF) under a weaker number theoretic assumption. We obtain the first efficient fully simulatable sVRF with a polynomial sized output domain (in the security parameter).

Category / Keywords: cryptographic protocols / electronic commerce and payment

Date: received 5 Mar 2009

Contact author: markulf kohlweiss at esat kuleuven be

Available formats: PDF |

Length of PDF file: 345206 bytes
Cksum of PDF file: 126

The password for your submission **xxxx/132** is **ofYMns**

Your submission will appear in the archive as shown above once it has been approved by the editor.

You will receive another email message with the number when your submission is posted in the archive. Until then, you can revise the submission using its password. If you submit the same article more than once, please add a message to the editor.

An email notification has also been sent to markulf.kohlweiss@esat.kuleuven.be.

[Cryptology ePrint Archive]