Cryptology ePrint Archive: Report 2013/109

Shorter Quasi-Adaptive NIZK Proofs for Linear Subspaces

Charanjit S. Jutla and Arnab Roy

Abstract: We define a novel notion of quasi-adaptive non-interactive zero knowledge (NIZK) proofs for probability distributions on parametrized languages. It is quasi-adaptive in the sense that the common reference string (CRS) generator can generate the CRS depending on the language parameters. However, the simulation is required to be uniform, i.e., a single efficient simulator should work for the whole class of parametrized languages. For distributions on languages that are linear subspaces of vector spaces over bilinear groups, we give quasi-adaptive NIZKs that are shorter and more efficient than Groth-Sahai NIZKs. For many cryptographic applications quasi-adaptive NIZKs suffice, and our constructions can lead to significant improvements in the standard model. Our construction can be based on any k-linear assumption, and in particular under the Symmetric eXternal Diffie Hellman (SXDH) assumption our proofs are even competitive with Random-Oracle based Σ-protocol NIZK proofs.

We also show that our system can be extended to include integer tags in the defining equations, where the tags are provided adaptively by the adversary. This leads to applicability of our system to many applications that use tags, e.g. applications using Cramer-Shoup projective hash proofs. Our techniques also lead to the shortest known (ciphertext) fully secure identity based encryption (IBE) scheme under standard static assumptions (SXDH).

Category / Keywords: public-key cryptography / NIZK, Groth-Sahai, bilinear pairings, signatures, dual-system IBE, DLIN, SXDH

Date: received 24 Feb 2013, last revised 25 Feb 2013

Contact author: csjutla at us ibm com