Cryptology ePrint Archive: Report 2013/128

Attribute-Based Encryption for Circuits from Multilinear Maps

Sanjam Garg and Craig Gentry and Shai Halevi and Amit Sahai and Brent Waters

Abstract: In this work, we provide the first construction of Attribute-Based Encryption (ABE) for general circuits. Our construction is based on the existence of multilinear maps. We prove selective security of our scheme in the standard model under the natural multilinear generalization of the BDDH assumption. Our scheme achieves both Key-Policy and Ciphertext-Policy variants of ABE.

Our scheme and its proof of security directly translate to the recent multilinear map framework of Garg, Gentry, and Halevi.

This paper is the result of a merge of the works of Garg, Genry, and Halevi and of Sahai and Waters, and subsumes both these works.

Category / Keywords: public-key cryptography / Attribute-Based Encryption

Date: received 2 Mar 2013, last revised 2 Mar 2013

Contact author: amitsahai at gmail com

Available formats: PDF | BibTeX Citation

Note: This paper is the result of a merge of the works of Garg, Genry, and Halevi and of Sahai and Waters, and subsumes both these works.

Version: 20130307:151704 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]