Cryptology ePrint Archive: Report 2011/018

Homomorphic Signatures for Polynomial Functions

Dan Boneh and David Mandell Freeman

Abstract: We construct the first homomorphic signature scheme that is capable of evaluating multivariate polynomials on signed data. Given the public key and a signed data set, there is an efficient algorithm to produce a signature on the mean, standard deviation, and other statistics of the signed data. Previous systems for computing on signed data could only handle linear operations. For polynomials of constant degree, the length of a derived signature only depends logarithmically on the size of the data set.

Our system uses ideal lattices in a way that is a ``signature analogue'' of Gentry's fully homomorphic encryption. Security is based on hard problems on ideal lattices similar to those in Gentry's system.

Category / Keywords: public-key cryptography / homomorphic signatures, ideals, lattices

Date: received 10 Jan 2011, last revised 5 Apr 2011

Contact author: dabo at cs stanford edu

Available formats: PDF | BibTeX Citation

Note: An extended abstract of this work will appear in Eurocrypt 2011. This is the full version.

Version: 20110405:220158 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]