Cryptology ePrint Archive: Report 2011/311

Targeted Malleability: Homomorphic Encryption for Restricted Computations

Dan Boneh and Gil Segev and Brent Waters

Abstract: We put forward the notion of targeted malleability: given a homomorphic encryption scheme, in various scenarios we would like to restrict the homomorphic computations one can perform on encrypted data. We introduce a precise framework, generalizing the foundational notion of non-malleability introduced by Dolev, Dwork, and Naor (SICOMP '00), ensuring that the malleability of a scheme is targeted only at a specific set of "allowable" functions.

In this setting we are mainly interested in the efficiency of such schemes as a function of the number of repeated homomorphic operations. Whereas constructing a scheme whose ciphertext grows linearly with the number of such operations is straightforward, obtaining more realistic (or merely non-trivial) length guarantees is significantly more challenging.

We present two constructions that transform any homomorphic encryption scheme into one that offers targeted malleability. Our constructions rely on standard cryptographic tools and on succinct non-interactive arguments, which are currently known to exist in the standard model based on variants of the knowledge-of-exponent assumption. The two constructions offer somewhat different efficiency guarantees, each of which may be preferable depending on the underlying building blocks.

Category / Keywords: foundations / Homomorphic encryption, non-malleable encryption

Publication Info: Innovations in Theoretical Computer Science (ITCS), 2012.

Date: received 10 Jun 2011, last revised 2 Jan 2012

Contact author: gil segev at microsoft com

Available formats: PDF | BibTeX Citation

Version: 20120102:174847 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]