Cryptology ePrint Archive: Report 2011/215

Delegatable Homomorphic Encryption with Applications to Secure Outsourcing of Computation

M. Barbosa and P. Farshim

Abstract: In this work we propose a new cryptographic primitive called Delegatable Homomorphic Encryption (DHE). This allows a Trusted Authority to control/delegate the capability to evaluate circuits over encrypted data to untrusted workers/evaluators by issuing tokens. This primitive can be both seen as a public-key counterpart to Verifiable Computation, where input generation and output verification are performed by different entities, or as a generalisation of Fully Homomorphic Encryption enabling control over computations on encrypted data.

Our primitive comes with a series of extra features as follows: 1) there is a one-time setup procedure for all circuits; 2) senders do not need to be aware of the functions which will be evaluated on the encrypted data, nor do they need to register keys; 3) tokens are independent of senders and receiver; and 4) receivers are able to verify the correctness of computation given short auxiliary information on the input data and the function, independently of the complexity of the computed circuit.

We give a modular construction of such a DHE scheme from three components: Fully Homomorphic Encryption (FHE), Functional Encryption (FE), and a (customised) MAC. As a stepping stone, we first define Verifiable Functional Encryption (VFE), and then show how one can build a secure DHE scheme from a VFE and an FHE scheme. We also show how to build the required VFE from a standard FE together with a MAC scheme. All our results hold in the standard model.

Finally, we show how one can build a verifiable computation (VC) scheme generically from a DHE. As a corollary, we get the first VC scheme which remains verifiable even if the attacker can observe verification results.

Category / Keywords: Homomorphism Delegation. Homomorphic Encryption. Functional Encryption. Verifiable Computation. Public-Key Cryptography. Provable Security.

Date: received 3 May 2011, last revised 29 Aug 2011

Contact author: mbb at di uminho pt, pooya farshim@gmail com

Available formats: PDF | BibTeX Citation

Version: 20110829:142617 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]