Cryptology ePrint Archive: Report 2011/566

Fully Homomorphic Encryption with Polylog Overhead

Craig Gentry and Shai Halevi and Nigel P. Smart

Abstract: We show that homomorphic evaluation of (wide enough) arithmetic circuits can be accomplished with only polylogarithmic overhead. Namely, we present a construction of fully homomorphic encryption (FHE) schemes that for security parameter $\secparam$ can evaluate any width-$\Omega(\secparam)$ circuit with t gates in time $t\cdot polylog(\secparam)$.

To get low overhead, we use the recent batch homomorphic evaluation techniques of Smart-Vercauteren and Brakerski-Gentry-Vaikuntanathan, who showed that homomorphic operations can be applied to "packed" ciphertexts that encrypt vectors of plaintext elements. In this work, we introduce permuting/routing techniques to move plaintext elements across these vectors efficiently. Hence, we are able to implement general arithmetic circuit in a batched fashion without ever needing to "unpack" the plaintext vectors.

We also introduce some other optimizations that can speed up homomorphic evaluation in certain cases. For example, we show how to use the Frobenius map to raise plaintext elements to powers of~p at the "cost" of a linear operation.

Category / Keywords: public-key cryptography / Homomorphic encryption, Bootstrapping, Batching, Automorphism, Galois group, Permutation network

Date: received 19 Oct 2011, last revised 10 Nov 2011

Contact author: shaih at alum mit edu

Available formats: PDF | BibTeX Citation

Version: 20111110:102242 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]