Cryptology ePrint Archive: Report 2011/277

Fully Homomorphic Encryption without Bootstrapping

Zvika Brakerski and Craig Gentry and Vinod Vaikuntanathan

Abstract: We present a radically new approach to fully homomorphic encryption (FHE) that dramatically improves performance and bases security on weaker assumptions. A central conceptual contribution in our work is a new way of constructing leveled fully homomorphic encryption schemes (capable of evaluating arbitrary polynomial-size circuits), {\em without Gentry's bootstrapping procedure}.

Specifically, we offer a choice of FHE schemes based on the learning with error (LWE) or ring-LWE (RLWE) problems that have $2^\secparam$ security against known attacks. For RLWE, we have:

1. A leveled FHE scheme that can evaluate L-level arithmetic circuits with $\tilde{O}(\secparam \cdot L^3)$ per-gate computation -- i.e., computation {\em quasi-linear} in the security parameter. Security is based on RLWE for an approximation factor exponential in L. This construction does not use the bootstrapping procedure.

2. A leveled FHE scheme that uses bootstrapping {\em as an optimization}, where the per-gate computation (which includes the bootstrapping procedure) is $\tilde{O}(\secparam^2)$, {\em independent of L}. Security is based on the hardness of RLWE for {\em quasi-polynomial} factors (as opposed to the sub-exponential factors needed in previous schemes).

We obtain similar results for LWE, but with worse performance. We introduce a number of further optimizations to our schemes. As an example, for circuits of large width -- e.g., where a constant fraction of levels have width at least $\secparam$ -- we can reduce the per-gate computation of the bootstrapped version to $\tilde{O}(\secparam)$, independent of L, by {\em batching the bootstrapping operation}. Previous FHE schemes all required $\tilde{\Omega}(\secparam^{3.5})$ computation per gate.

At the core of our construction is a much more effective approach for managing the noise level of lattice-based ciphertexts as homomorphic operations are performed, using some new techniques recently introduced by Brakerski and Vaikuntanathan (FOCS 2011).

Category / Keywords: fully homomorphic encryption, cryptography

Date: received 28 May 2011, last revised 11 Aug 2011

Contact author: craigbgentry at gmail com

Available formats: PDF | BibTeX Citation

Version: 20110811:062108 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]