Gentry, Craig; **Halevi, Shai**

Implementing Gentry's fully-homomorphic encryption scheme. (English) Zbl 1281.94026

Paterson, Kenneth G. (ed.), Advances in cryptology – EUROCRYPT 2011. 30th annual international conference on the theory and applications of cryptographic techniques, Tallinn, Estonia, May 15–19, 2011. Proceedings. Berlin: Springer (ISBN 978-3-642-20464-7/pbk). Lecture Notes in Computer Science 6632, 129-148 (2011).

Summary: We describe a working implementation of a variant of the first author's fully homomorphic encryption scheme [STOC 2009. New York, N.Y.: ACM, 169–178 (2009; Zbl 1257.68017)], similar to the variant used in an earlier implementation effort by *N. P. Smart* and *F. Vercauteren* [PKC 2010. Lect. Notes Comput. Sci. 6056, 420–443 (2010; Zbl 1281.94055)] who implemented the underlying "somewhat homomorphic" scheme, but were not able to implement the bootstrapping functionality that is needed to get the complete scheme to work. We show a number of optimizations that allow us to implement all aspects of the scheme, including the bootstrapping functionality.

Our main optimization is a key-generation method for the underlying somewhat homomorphic encryption, that does not require full polynomial inversion. This reduces the asymptotic complexity from $\tilde{O}(n^{2.5})$ to $\tilde{O}(n^{1.5})$ when working with dimension-n lattices (and practically reducing the time from many hours/days to a few seconds/minutes). Other optimizations include a batching technique for encryption, a careful analysis of the degree of the decryption polynomial, and some space/time trade-offs for the fully-homomorphic scheme.

We tested our implementation with lattices of several dimensions, corresponding to several security levels. From a "toy" setting in dimension 512, to "small," "medium," and "large" settings in dimensions 2048, 8192, and 32768, respectively. The public-key size ranges in size from 70 Megabytes for the "small" setting to 2.3 Gigabytes for the "large" setting. The time to run one bootstrapping operation (on a 1-CPU 64-bit machine with large memory) ranges from 30 seconds for the "small" setting to 30 minutes for the "large" setting.

For the entire collection see [Zbl 1214.94003].

MSC:

94A60 Cryptography

Cited in **4** Reviews
Cited in **37** Documents

Software:

NTL

Full Text: DOI