Brakerski, Zvika; **Vaikuntanathan, Vinod**

Fully homomorphic encryption from ring-LWE and security for key dependent messages.

(English) Zbl 1290.94051

Rogaway, Phillip (ed.), Advances in cryptology – CRYPTO 2011. 31st annual cryptology conference, Santa Barbara, CA, USA, August 14–18, 2011. Proceedings. Berlin: Springer (ISBN 978-3-642-22791-2/pbk). Lecture Notes in Computer Science 6841, 505-524 (2011).

Summary: We present a somewhat homomorphic encryption scheme that is both very simple to describe and analyze, and whose security (quantumly) reduces to the worst-case hardness of problems on ideal lattices. We then transform it into a fully homomorphic encryption scheme using standard "squashing" and "bootstrapping" techniques introduced by *C. Gentry* [Proceedings of the 41st annual ACM symposium on theory of computing, STOC 2009, New York: ACM, 169–178 (2009; Zbl 1304.94059)].

One of the obstacles in going from "somewhat" to full homomorphism is the requirement that the somewhat homomorphic scheme be circular secure, namely, the scheme can be used to securely encrypt its own secret key. For all known somewhat homomorphic encryption schemes, this requirement was not known to be achievable under any cryptographic assumption, and had to be explicitly assumed. We take a step forward towards removing this additional assumption by proving that our scheme is in fact secure when encrypting polynomial functions of the secret key.

Our scheme is based on the ring learning with errors (RLWE) assumption that was recently introduced by *V. Lyubashevsky, C. Peikert* and *O. Regev* [Eurocrypt 2010, Lect. Notes Comput. Sci. 6110, 1–23 (2010; Zbl 1279.94099), also J. ACM 60, No. 6, Paper No. 4, 35 p. (2013; Zbl 1281.68140)]. The RLWE assumption is reducible to worst-case problems on ideal lattices, and allows us to completely abstract out the lattice interpretation, resulting in an extremely simple scheme. For example, our secret key is s, and our public key is $(a, b = as + 2e)$, where s, a, e are all degree $(n-1)$ integer polynomials whose coefficients are independently drawn from easy to sample distributions.

For the entire collection see [Zbl 1219.94002].

MSC:

94A60 Cryptography

Keywords:

ring learning with errors (RLWE)

Software:

SWIFFT; NTRU

Full Text: DOI