Cryptology ePrint Archive: Report 2011/607

Improving Additive and Multiplicative Homomorphic Encryption Schemes Based on Worst-Case Hardness Assumptions}

Carlos {Aguilar Melchor} and Slim Bettaieb and Philippe Gaborit and Javier Herranz

Abstract: In CRYPTO 2010, Aguilar et al. proposed a somewhat homomorphic encryption scheme, i.e. an encryption scheme allowing to compute a limited amount of sums and products over encrypted data, with a security reduction from LWE over general lattices. General lattices (as opposed to ideal lattices) do not have an inherent multiplicative structure but, using a tensorial product, Aguilar et al. managed to obtain a scheme allowing to compute products with a polylogarithmic amount of operands. In this paper we present an alternative construction allowing to compute products with polynomially-many operands while preserving the security reductions of the initial scheme. Unfortunately, despite this improvement our construction seems to be incompatible with Gentry's seminal transformation allowing to obtain fully-homomorphic encryption schemes.

Recently, Brakerski et al. used the tensorial product approach introduced by Aguilar et al. in a new alternative way which allows to radically improve the performance of the obtained scheme. Based on this approach, and using two nice optimizations, their scheme is able to evaluate products with exponentially-many operands and can be transformed into an efficient fully-homomorphic encryption scheme while being based on general lattice problems. However, even if these results outperform the construction presented here, we believe the modifications we suggest for Aguilar et al.'s schemes are of independent interest.

Category / Keywords: homomorphic encryption, secure function evaluation, lattices

Date: received 9 Nov 2011

Contact author: carlos aguilar at unilim fr

Available formats: PDF | BibTeX Citation

Version: 20111110:210555 (All versions of this report)

Discussion forum: Show discussion | Start new discussion
