On realistic speedup and possible homomorphic operations of Somewhat Homomorphic Encryption Schemes in hardware.

Vincent Migliore[1], Maria Mendez Real[1], Arnaud Tisserand[3], Caroline Fontaine[2], and Guy Gogniat[1]

[1]Univ. Bretagne-Sud, UMR CNRS 6285, Lab-STICC, F-56100 Lorient, France, firstname.lastname@univ-ubs.fr
[2]Institut Mines-Telecom Telecom Bretagne, UMR CNRS 6285, Lab-STICC, Brest, France
[3]CNRS - IRISA - Univ. Rennes 1, Campus ENSSAT, 6 rue Kerampont, 22305 Lannion, France

Abstract

Since 2009, considerable progress has been done on Somewhat Homomorphic Encryption (SHE) Schemes, both in terms of software development and hardware development. These software and hardware implementations mainly accelerate the polynomial multiplication, which benefits to several elementary cryptographic operations like key generation, decryption and homomorphic multiplication. However, due to the fact that realistic security parameters have been unstable for a while, many implementations, comprising recent ones, are based on wrong setups, implying wrong estimation of speedup and wrong number of homomorphic operations achievable. By merging recent attacks, this talk proposes to clarify the situation of hardware acceleration of SHE schemes both in terms of speed-up and realistic homomorphic operations achievable.