Somewhat homomorphic encryption schemes: which candidates and which expectations to have with this type of encryption schemes?

Vincent Migliore [1], Maria Méndez Real [1], Vianney Lapotre [1], Arnaud Tisserand [2], Caroline Fontaine [1], Guy Gogniat [1]

[1] Lab-STICC, Lorient

[2] Irisa, Rennes

Abstract

Somewhat homomorphic encryption schemes unlock the possibility to perform arithmetic's operations between ciphertexts, without the need of the secret key. This functionality is crucial in the domain of privacy due to the fact that the service provider, in charge of processing the private data, can't have access to the plaintext. In this study, we will briefly present the different trade-offs between the most popular encryption schemes, followed by a more detailed study of the best candidates for an hardware acceleration.