World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:16, No:07, 2022

Parameter Selection for Computationally Efficient Use of the Bfvrns Fully Homomorphic Encryption Scheme

Authors : Cavidan Yakupoglu, Kurt Rohloff

Abstract : In this study, we aim to provide a novel parameter selection model for the BFVrns scheme, which is one of the prominent FHE schemes. Parameter selection in lattice-based FHE schemes is a practical challenges for experts or non-experts. Towards a solution to this problem, we introduce a hybrid principles-based approach that combines theoretical with experimental analyses. To begin, we use regression analysis to examine the parameters on the performance and security. The fact that the FHE parameters induce different behaviors on performance, security and Ciphertext Expansion Factor (CEF) that makes the process of parameter selection more challenging. To address this issue, We use a multi-objective optimization algorithm to select the optimum parameter set for performance, CEF and security at the same time. As a result of this optimization, we get an improved parameter set for better performance at a given security level by ensuring correctness and security against lattice attacks by providing at least 128-bit security. Our result enables average ~ 5x smaller CEF and mostly better performance in comparison to the parameter sets given in [1]. This approach can be considered a semiautomated parameter selection. These studies are conducted using the PALISADE homomorphic encryption library, which is a well-known HE library. The abstract goes here.

Keywords : lattice cryptography, fully homomorphic encryption, parameter selection, LWE, RLWE
Conference Title : ICCSP 2022 : International Conference on Cryptography, Security and Privacy
Conference Location : Istanbul, Türkiye
Conference Dates : July 28-29, 2022