Parameter Optimization & Larger Precision for (T)FHE

Ilaria Chillotti*[1] and Damien Ligier*[1]

[1]Zama – Zama – France

Résumé

In theory, Fully Homomorphic Encryption schemes allow users to compute any operation over encrypted data. However in practice, one of the major difficulties lies into determining secure cryptographic parameters that minimize the computational cost of evaluating a circuit. In this paper, we propose a solution to solve this open problem. Even though it mainly focuses on TFHE, the method is generic enough to be adapted to all the current FHE schemes.

TFHE is particularly suited, for small precision messages, from Boolean to 5-bit integers. It is possible to instantiate bigger integers with this scheme, however the computational cost quickly becomes unpractical. By studying the parameter optimization problem for TFHE, we observed that if one wants to evaluate operations on larger integers, the best way to do it is by encrypting the message into several ciphertexts, instead of considering bigger parameters for a single ciphertext. In the literature, one can find some constructions going in that direction, which are mainly based on radix and CRT representations of the message. However, they still present some limitations, such as inefficient algorithms to evaluate generic homomorphic lookup tables and no solution to work with arbitrary modulus for the message space. We overcome these limitations by proposing two new ways to evaluate homomorphic modular reductions for any modulo in the radix approach, by introducing on the one hand a new hybrid representation, and on the other hand by exploiting a new efficient algorithm to evaluate generic lookup tables on several ciphertexts. The latter is not only a programmable bootstrapping but does not require any padding bit, as needed in the original TFHE bootstrapping. We additionally provide benchmarks to support our results in practice. Finally, we formalize the parameter selection as an optimization problem, and we introduce a framework based on it enabling easy and efficient translation of an arithmetic circuit into an FHE graph of operation along with its optimal set of cryptographic parameters. This framework offers a plethora of features: fair comparisons between FHE operators, study of contexts that are favorable to a given FHE strategy/algorithm, failure probability selection for the entire use case, and so on.

*Intervenant