Parameter Exploration for Homomorphic Encryption Schemes Analysis.

Cyrielle FERON[1], Vianney LAPOTRE[2], and Loïc LAGADEC[1]

[1]ENSTA Bretagne, UMR CNRS 6285, Lab-STICC, 29806 Brest Cedex 9, France
[2]Univ. Bretagne-Sud, UMR 6285, Lab-STICC, F-56100 Lorient, France

Homomorphic Encryption (HE) allows computing on ciphertexts: it enables to delegate sensitive encrypted data processing to third parties without loss of data confidentiality. Despite being promising, HE suffers from known issues, in particular regarding high complexity and memory cost. In recent years, researchers have created many HE schemes in order to find the golden one to be used in future applications. This multitude of schemes makes analyzing all of them a difficult task, all the more so as each scheme owns several input parameters which can largely impact its performances, preventing from a sound domain space exploration.

Yet, *PAnTHErS* (Prototyping and Analysis Tool for Homomorphic Encryption Schemes) [5] allows estimating performances of HE schemes. The tool start by modeling a HE scheme as a succession of functions. These functions are stored in the PAnTHErS library, so that they can be further reused in other scheme models. Then, PAnTHErS scores computational complexity and memory consumption of the designed scheme without requiring to execute the scheme. Still, despite offering some ordering metrics, these results remain theoretical. However, no more than few practical executions are required to calibrate the results : a calibration method [6] estimates HE scheme execution times and mebibytes (MiB) consumed for each set of input parameters requested.

This approach and PAnTHErS have been validated on different HE schemes based on Ring Learning With Error ([4], [1], [7], [3]) and a medical application [2]. Analyses produced by PAnTHErS allow a HE expert to choose the scheme and its input parameters that best fit an application for a given implementation (minoring execution time and memory consumption).

However, only an expert in HE schemes knows which parameter variations make sense when analyzing a scheme. As our intent is to provide to users of PAnTHErS, be they beginners or experts in HE, the most interesting scheme and input parameters for a given implementation, we have extended PAnTHErS by incorporating a domain space exploration feature. This exploration analyzes every sets of input parameters of every HE schemes for one application. According to PAnTHErS evaluations, one scheme along with one set of input parameters are returned, that ensure the best execution time versus memory cost ratio.

Future works will add extra analysis metrics to PAnTHErS, in particular, noise expansion. Then, PAnTHErS will automatically calculate the depth of HE schemes with no more need for the authors' depth equation.

References

[1] J. W. Bos, K. E. Lauter, J. Loftus, and M. Naehrig. Improved Security for a Ring-Based Fully Homomorphic Encryption Scheme. In *Cryptography and Coding IMA*, 2013.

[2] Sergiu Carpov, Thanh Hai Nguyen, Renaud Sirdey, Gianpiero Costantino, and Fabio Martinelli. Practical Privacy-Preserving Medical Diagnosis Using Homomorphic Encryption. In *CLOUD*, 2016.

[3] Yarkin Doröz and Berk Sunar. Flattening NTRU for evaluation key free homomorphic encryption. *IACR Cryptology ePrint Archive*, 2016.

[4] J. Fan and F. Vercauteren. Somewhat Practical Fully Homomorphic Encryption. *IACR Cryptology ePrint Archive*, 2012:144, 2012.

[5] Cyrielle Feron, Vianney Lapotre, and Loïc Lagadec. PAnTHErS: A Prototyping and Analysis Tool for Homomorphic Encryption Schemes. In *14th International Joint Conference on e-Business and Telecommunications (ICETE) - SECRYPT*, 2017.

[6] Cyrielle Feron, Vianney Lapotre, and Loïc Lagadec. Fast Evaluation of Homomorphic Encryption Schemes Based on Ring-LWE. In *9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018.

[7] Alhassan Khedr, P. Glenn Gulak, and Vinod Vaikuntanathan. SHIELD: Scalable Homomorphic Implementation of Encrypted Data-Classifiers. *IEEE Trans. Computers*, 2016.