Building Algorithm-Hiding FHE Systems from Exotic Number Representations

Paulo Martins and Leonel Sousa

March 1, 2019

Abstract

Cloud computing providers maintain shared high-performance servers that are used by their clients as necessary. However, as attacks such as Meltdown and Spectre have shown, traditional isolation mechanisms are not sufficient to guarantee neither the secrecy of data nor the privacy of processing algorithms. With Fully Homomorphic Encryption (FHE), data may be processed encrypted in the cloud, making any leaked information look random to an attacker. While there has also been research on ensuring the confidentiality of the processing algorithm, this type of systems tries to emulate a computer architecture homomorphically, leading to impractical results. Rather than considering that FHE should offer the properties of a general-purpose processor, the most adequate number representations and their properties are herein investigated to achieve efficient domain-specific processors. More concretely, stochastic number representations and fixed-point arithmetic are considered, each with its own characteristics. Based on these representations, systems are proposed that allow to approximate a wide range of functions in a generic way, producing an encrypted description of them. In particular, we focus on functions whose approximation may be efficiently evaluated in an homomorphic manner, namely multivariate continuous functions, which might even be non-analytic, thus going beyond traditional Taylor series-based approaches. When processing the encrypted function descriptions, the homomorphic evaluator is not able to infer anything from the function except for how precisely it is being approximated. By having a larger number of functions that can be supported, security is being improved, since the amount of possibilities for the function that is being processed is also large. Moreover, since the algorithm inputs are encrypted, data disclosure is also prevented. As a byproduct, we achieve a mechanism to automatically translate the user code to the encrypted approximated descriptions. The translation treats the function in a black-box approach, which means that the user does not need to change his typical development flow, and that he or she can call other functions, use complex control flows, etc. Finally, a prototype of the system is presented, its applicability is verified in practice for commonly used applications, including image processing and machine learning, and the two aforementioned number representations are thoroughly compared.

Keywords: Fully Homomorphic Encryption; Stochastic Computing; Fixed-point Arithmetic