Chapter 59
About Fully Homomorphic Encryption Improvement Techniques:
NISS2018 Conference Paper

Ahmed El-Yahyaoui
Mohammed V University in Rabat, Morocco

Mohamed Daifr Ech-Cherif El Kettani
Mohammed V University, Rabat, Morocco

ABSTRACT

Fully homomorphic encryption schemes (FHE) are a type of encryption algorithm dedicated to data security in cloud computing. It allows for performing computations over ciphertext. In addition to this characteristic, a verifiable FHE scheme has the capacity to allow an end user to verify the correctness of the computations done by a cloud server on his encrypted data. Since FHE schemes are known to be greedy in term of processing consumption and slow in terms of runtime execution, it is very useful to look for improvement techniques and tools to improve FHE performance. Parallelizing computations is among the best tools one can use for FHE improvement. Batching is a kind of parallelization of computations when applied to an FHE scheme, it gives it the capacity of encrypting and homomorphically processing a vector of plaintexts as a single ciphertext. This is used in the context of cloud computing to perform a known function on several ciphertexts for multiple clients at the same time. The advantage here is in optimizing resources on the cloud side and improving the quality of services provided by the cloud computing. In this article, the authors will present a detailed survey of different FHE improvement techniques in the literature and apply the batching technique to a promising verifiable FHE (VFHE) recently presented by the authors at the WINCOM17 conference.

DOI: 10.4018/978-1-7998-7705-9.ch059

1. INTRODUCTION

Processing encrypted data in the cloud computing is today possible when data are encrypted with a fully homomorphic encryption scheme. This category of encryption has goal to allow computations in the ciphertext space without decrypting and without revealing the decryption key. Given its importance in cloud security and many other applications (El-yahyaoui & Ech-cherif El Kettani, 2017), (Armknecht, et al., 2015), (Damgård, Groth, & Salomonsen, 2002), it was early conjectured by Rivest et al. (Rivest, Adleman, & Dertouzos, 1978) under the name of privacy homomorphism. Gentry (Gentry, 2009) who gives it the famous name of fully homomorphic encryption solved this conjecture in 2009 after a breakthrough thesis work.

Simplification and improvement of fully homomorphic encryption schemes is the current occupation of many cryptographers. The majority of succeeding works (Smart & Vercauteren, 2009), (van Dijk, Gentry, Halevi, & Vaikuntanathan, 2009), (Vikuntanathan & Brakerski, 2011), (Brakerski, 2012), (Gentry & Halevi, 2011) after Gentry's breakthrough has as paramount objective to make simpler the design and ameliorate performances of fully homomorphic encryption algorithms. One of the significant ameliorations consists in adding new capacities to this class of algorithms (Gentry, Sahai, & Waters, 2013), (El-yahyaoui & Ech-cherif El kettani, 2017), (Asharov, et al., 2012), (Lopez-Alt, Tromer, & Vaikuntanathan, 2012). Verification capacity is one of the best characteristics that can hold a fully homomorphic encryption scheme.

A verifiable encryption scheme is a cryptosystem that permits us to prove some properties about a hidden value in a ciphertext without decrypting it. If the verification option is integrated with homomorphic capacities in the same encryption scheme, it becomes a verifiable fully homomorphic encryption scheme (VFHE). Consequently, a VFHE scheme is a particular case of FHE schemes for which the capacities of computing over encrypted data and delegating calculations on confidential data, to a remote cloud server, are given to the cloud client with the possibility of verifying the rightness of its outsourced computations.

In practice, FHE and VFHE schemes are costing. It generates a huge amount of noise and becomes ugly when evaluating multiplications on ciphertexts because the noise growth is square in general. As long as we add capacities to fully homomorphic encryption schemes (El-yahyaoui & Ech-cherif El kettani, 2017), (Gentry, Sahai, & Waters, 2013), (Lopez-Alt, Tromer, & Vaikuntanathan, 2012), it becomes uglier and costlier in practice.

Improvement of FHE has several techniques and tools. Each technique has its special impact on client or server side. Techniques that are recommended to client-side improvement allow enhancing the encryption runtime and take into consideration client processing powers. While server-side improvement techniques permit to reduce the client consumption in terms of processing and space storage in the cloud. This reduction minimizes the costumer's billing of cloud resources consumption.

Parallelize computations with fully homomorphic encryption schemes is one of the best techniques used for server-side improvement. It can be a good solution to improve performances of some homomorphic encryption schemes, with additional capacities like verification one. As it can be also an upturn of runtime improvement when processing operations for multiple clients by a cloud server. Batch a verifiable fully homomorphic encryption scheme entails evaluating functions over a vector of ciphertexts in the same time. Each component of this vector can be a ciphertext under the same algorithm but with a different encryption key, it implies that we can put in the same vector ciphertexts coming from different clients each client has its own encryption key.