Chapter 14
Fully Homomorphic Encryption Without Noise

Yacine Ichibane
Ecole Mohammadia d'Ingénieurs, Mohammed V University of Rabat, Rabat, Morocco

Youssef Gahi
Ibn Tofail University, Kenitra, Morocco

Mouhcine Guennoun
Cisco Systems, Ontario, Canada

Zouhair Guennoun
Ecole Mohammadia d'Ingénieurs, Mohammed V University of Rabat, Rabat, Morocco

ABSTRACT

In this paper, the authors present a novel fully homomorphic encryption scheme operating between Z_N and $\mathbb{Z}_N^h$ capable of arbitrarily performing additions and multiplications. The new scheme is compact and each operation (addition or multiplication) performed on any two ciphertexts produces a fresh ciphertext without any associated noise. Thus, the scheme does not need any bootstrapping procedure or noise reduction technique to refresh ciphertexts. In the absence, to the best of the knowledge of the authors, of any existing fully, partially or leveled homomorphic encryption scheme using Z_N as the set of plaintexts, the new cryptosystem has been implemented and has had its performance compared to the identity encoding.

INTRODUCTION

A homomorphic encryption scheme is a scheme that has a certain degree of a property called malleability. The malleability of an encryption scheme is the ability for one to use as input one or more ciphertexts and produce a new ciphertext representing an encryption of the result of a known function when applied to the plaintexts corresponding to the ciphertexts in play.

DOI: 10.4018/978-1-7998-7705-9.ch014

For instance, an encryption scheme which lets one compute an encryption of the sum of two plaintexts by computing a certain function f of two of their corresponding ciphertexts has a certain degree of malleability. Such scheme is known as an additively homomorphic scheme even if the used function f is a multiplication operation like in the case of the RSA cryptosystem (Rivest, Shamir, & Adleman, 1978). In the same manner, an encryption scheme that permits the computation of an encryption of the product of two plaintexts has also a certain degree of malleability and is known as a multiplicatively homomorphic scheme.

Many encryption schemes show one of these two types of malleability or homomorphism. Famous examples are Goldwasser-Micali (Goldwasser, & Micali, 1982) which is an additively homomorphic cryptosystem and ElGamal (ElGamal, 1985) which is a multiplicatively homomorphic cryptosystem, but rare are practical encryption schemes which present the two types of malleability at the same time. Such schemes which are both additively and multiplicatively homomorphic are called fully homomorphic encryption schemes because they enable one to compute arbitrary functions on encrypted data. This is the highest degree of malleability a scheme can aspire to have.

In this paper, the authors devise a novel fully homomorphic cryptosystem that has the property of performing an arbitrary number of additive and multiplicative operations without introducing noise to the resulting ciphertext. The rest of this paper is organized as follows. The Background section provides an overview of fully homomorphic encryption schemes and highlights both their strengths and weaknesses. The Scheme section presents a novel Noiseless Fully Homomorphic Encryption scheme (NFHE) and proves its homomorphic properties. The Security Analysis section analyzes the security of the proposed scheme, discusses the conditions under which the proposal is secure and presents some of the attacks that an adversary could try hoping to break the NFHE cryptosystem. The section that follows goes over a direct application of the proposed scheme in Private Information Retrieval. In the Performance Analysis section, the authors present the results of the comparison of their fully homomorphic encryption scheme to the identity encoding. Finally, the section that follows concludes this paper.

BACKGROUND

In this section, the authors present some of the works that addressed the subject of homomorphic encryption.

First Fully Homomorphic Encryption Scheme

The first fully homomorphic scheme has been presented by Craig Gentry in his Ph.D thesis in 2009 (Gentry, 2009a). The way Gentry constructed the very first homomorphic encryption scheme was later known as Gentry's blueprint and is for the moment being and to the best of the knowledge of the authors the only way to produce fully homomorphic encryption schemes. The blueprint is composed of two main steps described below.

Constructing a Noisy Somewhat Homomorphic Encryption Scheme

A Somewhat Homomorphic Encryption scheme, or SHE scheme, is a cryptosystem that has a limitation on the number of operations that can be performed on a ciphertext due to the fact that each ciphertext