Chapter 17
A Pairing-based Homomorphic Encryption Scheme for Multi-User Settings

Zhang Wei
Engineering University of Chinese Armed Police Force, China

ABSTRACT

A new method is presented to privately outsource computation of different users. As a significant cryptographic primitive in cloud computing, homomorphic encryption (HE) can evaluate on ciphertext directly without decryption, thus avoid information leakage. However, most of the available HE schemes are single-user, which means that they could only evaluate on ciphertexts encrypted by the same public key. Adopting the idea of proxy re-encryption, and focusing on the compatibility of computation, the authors provide a pairing-based multi-user homomorphic encryption scheme. The scheme is a somewhat homomorphic one, which can do infinite additions and one multiplication operation. Security of the scheme is based on subgroup decision problem. The authors give a concrete security model and detailed security analysis.

1. INTRODUCTION

Aiming on storage and computation outsourcing, cloud computing is revolutionizing the entire field of information technology. Clients outsource their data to the cloud to take advantage of the unlimited virtualized storage space and the low management cost. And the mighty computation ability can greatly alleviate the user's load. But the cloud is also posing new security and privacy challenges. Users want to gain reliability and availability for the remotely stored data, thus gives system designer a new challenge to provide security and credit, without service quality slacking.

During the past several years, since the first fully homomorphic encryption (FHE) scheme presented by Gentry (Gentry, 2009), homomorphic encryption has been a vibrant domain in cryptography. As a useful cryptographic primitive, homomorphic encryption can allow specific types of computations to be carried

DOI: 10.4018/978-1-7998-1763-5.ch017

out on ciphertexts and obtain an encrypted result which matches the result of operations performed on the plaintext after decryption. The idea of HE first presented by Rivest, Adleman and Dertouzos (Rivest, Adleman & Dertouzos, 1978), they found that some of the classical public key cryptosystem, such as RSA and ElGamal, are multiplication homomorphic, which means we can multiply two ciphertexts, and get the ciphertext of two plaintexts' multiplication.While RSA cannot permit addition on ciphertexts. This property is called semi-homomorphic, means only permit one operation (addition or multiplication).

BGN scheme was brought forward by Boneh, Goh and Nissim (Boneh, Goh & Nissim, 2005), it was the first semantic secure somewhat homomorphic encryption scheme that allows both addition and multiplication. This type is called *somewhat homomorphic*, because the time of multiplications is strictly limited, often once.If an encryption system permits unlimited additions and multiplications, then it is called *fully homomorphic*. During the past 30 years, the problem of constructing fully homomorphic encryption (FHE) schemes remains open. After the breakthrough work of Gentry in 2009, there has been numerous works on FHE. Some candidate schemes (Gentry, 2013, Yagisawa, 2015, Brakerski 2011) have been constructed, with security and efficiency been carefully analyzed.

However, most of the available HE or FHE schemes could only operate on ciphertexts of the same user. But in the practical world, it is often needed to operate on ciphertexts that was encrypted by different keys. In other word, we are facing such a scenario:

Suppose there are n clients that store their data in clouds. They wish to use these data as input to compute a function, with no personal information revealed. This is called *secure multiparty cloud computation* (SMCC), which is different from secure multiparty computation and server-aided multiparty computation in that it emphasizes that the server could not decrypt, yet the bulk computation should carry on the server.

SMCC is formulated as the following (Zheng & Zhang, 2012).

Secure Multiparty Cloud Computation (SMCC) Consider that k clients $p_1,\ldots,p_k$, store their data $x_1,\ldots,x_k$ in clouds in an encrypted form, they wish to cooperate together in order to efficiently and securely compute the function $f(x_1,\ldots,x_k)$ by utilizing the computation capability of clouds.

This process is described in Figure 1.

Homomorphic encryption can be used to solve the problem of SMCC, however, the solution involves homomorphic evaluation on ciphertexts encrypted by different encryption keys, namely multi-key homomorphic encryption. The idea of multi-key homomorphic encryption is first presented by López-Alt, Tromer and Vaikuntanathan (López-Alt, Tromer & Vaikuntanathan, 2012). They constructed a multi-key fully homomorphic encryption (FHE) scheme from NTRU, and indicated that in theory, most of the existing FHE schemes can be changed into multi-key schemes, but in the resulting scheme, the size of ciphertext grows exponentially, thus cannot use in practice anyway. In 2014, Clear and McGoldrick (Clear & McGoldrick, 2014) put forward a multi-key leveled FHE basing on LWE assumption. They also point out that the ciphertext sizes of the multi-key FHE schemes are too long to be use in practice.

In addition to the above work, there's another way to obtain multi-key homomorphic encryption. That is, using the idea of proxy re-encryption to build an encryption scheme that can evaluate on two or more user's ciphertexts. The concept of proxy re-encryption, with a goal of securely enabling the re-encryption of ciphertexts from one key to another, first comes from the work of Blaze, Bleumer and Strauss (Blaze, Bleumer & Strauss, 1998).In 2005, Ateniese et.al. proposed a few new re-encryption schemes and discussed its several potential applications. Since then, many excellent schemes have been proposed, including re-encryption schemes in certificate based setting, in identity based setting and in hybrid setting (Wang et al, 2012, Matsuo,2007, Chandran,2015, Srinivasan & Rangan, 2014) .In 2012,