Chapter 18
A Secure Cloud Storage using ECC-Based Homomorphic Encryption

Daya Sagar Gupta
Indian Institute of Technology (ISM) Dhanbad, India

G. P. Biswas
Indian Institute of Technology (ISM) Dhanbad, India

ABSTRACT

This paper presents a new homomorphic public-key encryption scheme based on the elliptic curve cryptography (HPKE-ECC). This HPKE-ECC scheme allows public computation on encrypted data stored on a cloud in such a manner that the output of this computation gives a valid encryption of some operations (addition/multiplication) on original data. The cloud system (server) has only access to the encrypted files of an authenticated end-user stored in it and can only do computation on these stored files according to the request of an end-user (client). The implementation of proposed HPKE-ECC protocol uses the properties of elliptic curve operations as well as bilinear pairing property on groups and the implementation is done by Weil and Tate pairing. The security of proposed encryption technique depends on the hardness of ECDLP and BDHP.

1. INTRODUCTION

Public-key encryption (PKE) came into existence in the year 1976. Firstly, Diffie & Hellman (1976) asked whether it is possible to have two different keys; one for encryption (a public key *PK*) and another for decryption (a secret key *SK*) in their seminal paper entitled "New Directions in Cryptography". This paper includes the concepts of PKE to design a new homomorphic encryption technique mainly for cloud security. By homomorphic property, we mean that $E(m_1 \, o_m \, m_2) = E(m_1) \, o_c \, E(m_2)$ where E denotes the encryption and o_c / o_m denote the binary operations.

DOI: 10.4018/978-1-7998-1763-5.ch018

In this paper, the authors use the properties of the elliptic curves and bilinear map to secure the network communication. The security of ECC algorithms is independently given by Kapoor, Abraham & Singh (2008). The authors of this paper propose a new cryptographic encryption/decryption technique with homomorphic property based on the hardness assumptions Elliptic Curve Diffie-Hellman Problem (ECDHP) and Bilinear Diffie-Hellman Problem (BDHP). The cloud security is the main objective of this proposed paper. Thus, for security issues on the clouds, the authors of this paper include the homomorphic encryption technique. They have presented four algorithms: *key generation, encryption, decryption,* and *evaluation* to implement this proposed work. In the *key generation*, the key pair (public and private key) for their proposed scheme is generated. *Encryption* algorithm of this scheme simply encrypts the message using the public key of the receiver and the encrypted message is stored on the cloud storage. Since the stored messages are encrypted, a cloud server is not able to understand these messages, *i.e.* security to the stored messages is provided so that the cloud system could not see the original message. *Decryption* algorithm takes the encrypted message as input and uses receiver's private key to decrypt the encrypted message to get the authentic message. At last, the *evaluation* algorithm is mainly used to design the homomorphic property for the proposed protocol. For the evaluating process of the proposed work, an authentic user requests the cloud for encrypted data which includes the addition or multiplication of original authentic messages stored on cloud storage. The cloud system, in return, performs some computation on the files stored in it and responds with computed files. The authentic user, in turns, performs the decryption algorithm to generate the addition or multiplication of original files.

1.1. Literature Review

Gentry (2009) proposed a fully homomorphic encryption. He shows that his scheme computes a function on encrypted data and also homomorphism is preserved. He uses the hard lattices to design his protocol. He firstly designed a somewhat homomorphic "boostrappable" encryption scheme and later showed the how boostrappable encryption is converted into a fully homomorphic encryption. Van Dijk, Gentry, Halevi & Vaikuntanathan (2010) proposed a modular arithmetic based fully homomorphic encryption scheme. They use Gentry (2009)'s technique to include "boostrappable" somewhat encryption. Their scheme is based on the addition and multiplication on integers. Brakerski & Vaikuntanathan (2014) an LWE based fully homomorphic encryption scheme. Smart & Vercauteren (2010) presents a fully homomorphic encryption scheme in which the size of key and cipher text is smaller. Their scheme uses Gentry (2009) technique to design a somewhat encryption to a fully homomorphic encryption scheme. Gentry, Sahai & Waters (2013) proposed a new technique which is used to design a fully homomorphic encryption scheme. They called this new technique as approximate eigenvector method. Ducas & Micciancio (2015) proposed a fully homomorphic encryption which works on bit operations and continuously refresh it. Bendlin, Damgard, Orlandi & Zakarias (2011) proposed a semi-homomorphic encryption scheme. Bos, Lauter, Loftus & Naehrig (2013) designed a new fully homomorphic scheme which removes this non-standard assumption and based on lattice and circular security problems.

Coron, Lepoint & Tibouchi (2014) proposed a scheme which presented a key policy attribute-based encryption (ABE) using a fully homomorphic encryption scheme and security of their scheme is given by LWE problem. Wei (2016) provided the security to the cloud system using a pairing-based homomorphic encryption scheme. A faster fully homomorphic encryption is proposed by Stehlé & Steinfeld (2010). Their scheme described the improvement in Gentry's homomorphic encryption. They provide