Chapter 10
Design of Public-Key Algorithms Based on Partial Homomorphic Encryptions

Marwan Majeed Nayyef
Anbar University, Baghdad, Iraq

Ali Makki Sagheer
University of Anbar, Baghdad, Iraq

ABSTRACT

With the rapid development of cloud computing, which has become a key aspect to maintain the security of user information that may be highly confidential and maintained during transport and storage process. The reliance on traditional algorithms that are used to encrypt data are not secure enough because we cannot process the data only after decrypt. In this article is proposed the use of homomorphic encryption to solve this problem because it can deal with encrypted data without the decryption, which can lead to ensuring confidentiality of the data. A number of public-key algorithms are explained, which is based on the concept of homomorphic encryption. In this article an algorithm is proposed based on HE and it is similar to Menesez-EC but with one digit as a secret key according to its advantage, whereby reducing the cost of communication, and storage and provides high processing speed when compared with other algorithms. This algorithm provides enough security for a bank's customer information and then compared with ECC, each of RSA and Piallier algorithms as evaluated.

1. INTRODUCTION

Early on, many researcher studies began on homomorphic encryption more in-depth. Homomorphic encryption was simplified and through advances in research, most of the research appeared to focus their efforts toward homomorphic encryption due to its importance in more aspects spatially in the field of the cloud computing in order to provide information security and maintaining that information from penetrating by the hackers (Chen, Ben, & Huang, 2014). Homomorphic Encryption is an important

DOI: 10.4018/978-1-7998-7705-9.ch010

kind of encryption in computational science, it provides many techniques such as partially, somewhat and fully homomorphic encryption with the purpose of the securely store, transfer and dealing with ciphertext in a way that maintains the confidentiality and integrity of the data (Ogburn, Turner, & Dahal, 2013). Homomorphic encryption can be classified into partially and fully homomorphic encryption, with partial Homomorphic Encryption (PHE) use one operation in ciphertext whereas Fully Homomorphic Encryption (FHE) can use all operations in the ciphertext, and it is one of the most common new topics which make more of the researcher to deal with those concepts because of providing more security for data especially in the cloud environment (Suveetha & Manju, 2016).

There are two main general cryptosystems they are symmetric and asymmetric cryptosystem. AES, DES are symmetric-key algorithm and Elgamal, paillier and RSA are asymmetric cryptosystem, in this paper, we work in the public key encryption algorithms.

In section 1, we would explain the concepts, functions and properties of homomorphic encryption. In section 2, Elliptic curve Cryptography is described, in section 3, describe encryption algorithms such as (RSA, Paillier, Elgamal, Goldwasser-Micali and Boneh-Goh-Nissim (BGN)) are based on homomorphic encryption properties. In section 4, we would explain the limitation of PHE. In section 5, we would describe comparison between different algorithms of homomorphic encryption that give a general idea of all the algorithms. In section 6, the proposed algorithm is described, in section 7, we explain the experimental result of the proposed algorithm and compare ECC with other algorithms.

2. BACKGROUND

In 2012 Li Li, Ahmed A.Abd, XiamuNiu proposed new scheme with additive homomorphism property based on ElGamal-Elliptic Curve (ElGamal-EC) for transferring secret images over a channel which is unsecured instead of using ElGamal and RSA scheme. In this paper, the proposed scheme uses a shorter key to better performance than schemes based on ElGamal or RSA. Therefore, decryption of images requires lower processing compared with the method that uses the other additively homomorphic property in ElGamal-EC. Experimental results and analysis show that the proposed method is faster and has superior performance for RSA and ElGamal (Li, Abd El-Latif, & Xiamu, 2012).

In 2015, Kamal Kumar Chauhan; Amit K.S. Sanger, A. Verma, a secure method was developed for keeping data, Data security is an important aspect, especially when data transfer and storage over the internet (cloud computing), therefore various methods of standard encryption algorithm provide security for data in storage and transmission. In the traditional state data to be processed must be decrypted first, but this state makes data understandable to a cloud provider. Standard encryption algorithms are not sufficient to make data more secure. In this paper various schemes are proposed such as (Pillar, RSA, and Boneh-Goh-Nissim (BGN)) based on homomorphic encryption in cloud computing in order to secure data through processing state because of Homomorphic encryption allows the service provider to operate on ciphertext without decryption. The implementation of these schemes helps to provide security for data stored in cloud computing (Chauhan, Sanger, & Verma, 2015).

In 2016, Tannishk Sharma creates a voting system in order to solve the problem of the time consuming, obstruction and disruption which may happen. The development of Information Technology led us to propose an E - voting system to solve all these problems, E-voting system helps us to vote from any place. In this paper, an E-voting system proposed based on Paillier Homomorphic Encryption scheme in order to provide security for those systems through processing and transferring data in ciphertext form.