Journal of Information Security and Applications 34 (2017) 233–242

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Fully Enhanced Homomorphic Encryption algorithm of MORE approach for real world applications

Khalil Hariss*, Hassan Noura, Abed Ellatif Samhat

Faculty of Engineering-CRSI, Lebanese University, Hadath Campus, Hadath, Lebanon

ARTICLE INFO

Article history:
Available online 21 February 2017

Keywords:
Fully Homomorphic Encryption scheme
MORE
Dynamic diffusion and permutation primitives
Security analysis

ABSTRACT

The design of a Homomorphic Encryption (HE) algorithm that allows computation over the encrypted data is required in real world modern applications to preserve the privacy. Such applications include Cloud Computing, shared storage, processing resources, etc. The existing solutions are not practical for real world applications. Asymmetric approaches suffer from high computation overhead, while symmetric approaches suffer from low immunity against attacks such as chosen and known plaintext attack. In this paper, we consider symmetric approaches and we focus on Matrix Operation for Randomization and Encryption (MORE) approach to build a new algorithm overcoming the drawbacks of MORE. The proposed algorithm is explained in details and evaluated. The security performance results show that the proposed approach can prevent the strong attacks without degradation of the system performances in term of latency and energy consumption.

1. Introduction

Encryption is one of the most common techniques used for preserving users data privacy, but sometimes users are enforced to reveal their secret encryption keys to some parties for processing operations over their sensitive data. Homomorphic Encryption (HE) is new cryptographic research topic that was introduced to help users in preserving their data confidentiality and privacy by allowing untrusted parties to process computations over encrypted data. HE becomes an important need in real world modern applications such as Cloud Computing, Data aggregation in wireless sensor network scenario, Electronic Voting, Spam filters, etc.

In such applications, HE will allow the creation of new techniques capable to run over encrypted inputs to produce encrypted outputs without knowing any information about the primitive data, once they are used by untrusted parties. Thus users privacy is guaranteed.

Several homomorphic ideas have been introduced in the literature. A state of art of the existing HE algorithms is given in [1–3]. RSA explained in [4] is the first HE Cryptosystem. Gentry examined also a Fully Homomorphic Encryption (FHE) in [5,6] based on ideal lattices. DGHV another FHE was presented by Van Dijk et al. in [7].

The MORE (Matrix Operation for Randomization and Encryption) and the PORE (Polynomial Operation for Randomization and Encryption) two FHE algorithms based on linear transformations are explained in [8–10], and Josepeh Domingo Ferrer also talked in [11,12] about a FHE approach based on polynomial calculations. Two additive HE schemes Iterated Hill Cipher (IHC) and Modified Rivest Scheme (MRS) are presented in [13,14]. The implementation of the Homomorphic Pallier cryptosystem in a cloud scenario is given in [15].

All the existing algorithms are not efficient for real world applications due to computational complexity such as asymmetric ones like Gentry [5,6], DGHV [7]. Symmetric ones such as MORE [9] and PORE [10] are introduced with an encryption process satisfying the homomorphic properties. However they encounter some drawbacks including the storage overhead and the weakness against chosen/known plaintext attack.

To understand the concept of HE, we define C to be a circuit that performs a certain operation (querying, downloading a file from the INTERNET, comparing two values, adding two values, etc.). Any circuit C can be written as a Boolean function and any Boolean function can be written as a polynomial form. We know that any polynomial form is merely a set of addition and multiplication operations. A scheme is defined to be Fully Homomorphic Encryption (FHE) scheme if it satisfies the two following basic properties of addition and multiplication:

$$[Enc_K(x_1) + Enc_K(x_2)] mod N = [Enc_K([x_1 + x_2]\ mod N)] mod(N) \quad (1)$$

* Corresponding author.
E-mail addresses: Khalilharis87@hotmail.com (K. Hariss), hnnoura@gmail.com (H. Noura), samhat@ul.edu.lb (A.E. Samhat).

http://dx.doi.org/10.1016/j.jisa.2017.02.001
2214-2126/

$$[Enc_K(x_1) \times Enc_K(x_2)]modN = [Enc_K([x_1 \times x_2]\ modN)]mod(N) \quad (2)$$

where x_1, x_2 are two plaintexts in a ring Z_N, Enc is the encryption algorithm and K is the symmetric key.

In addition, the evaluation function is introduced where all computations are related to the circuit C. It is defined in a symmetric scenario with circuit C by:

1. $\Psi\mapsto$ evaluate$(K, C, \theta_1, \theta_2, \theta_3, \ldots, \theta_t)$ where $\theta_i = Enc_K(m_i)$, m_i is a plaintext, K is the symmetric key and $i = 1, 2, 3, \ldots, t$.
2. Any encryption algorithm is evaluated as homomorphic if $\Psi = En_K(C(m_1, m_2, .., m_t))$.

To our knowledge there is no efficient FHE scheme practical for real world applications. We consider in this paper the MORE approach and we build a new encryption algorithm (Enhanced MORE) that provides a dynamic implementation and high immunity against attack. The proposed enhancement are evaluated and Enhanced MORE algorithm performs better than MORE and PORE when studying the security analysis.

The rest of this paper is organized as follows, Section 2 explains the MORE and PORE Approaches. Section 3 introduces Enhanced MORE, i.e. our enhancement steps for the MORE approach. Security analysis and performances of Enhanced MORE algorithm are given in Section 4 in addition to a comparison with the MORE and PORE approaches. Conclusions are drawn in Section 5.

2. MORE and PORE approaches

2.1. MORE approach

In [9,10], a matrix idea called MORE (Matrix Operation for Randomization and Encryption) is investigated for building a FHE scheme (an example of the MORE Approach is given in Appendix A). The proposed method is defined by the following matrix equation:

$$E(m,k) = K^{-1}\begin{bmatrix} m & 0 \\ 0 & r \end{bmatrix}K \quad (3)$$

where m the plaintext, r is a random integer in a ring Z_N, K is an invertible matrix in Z_N (2x2) and K^{-1} its corresponding inverse one.

The decryption process is simply the inverse of the encryption process by applying:

$$D(m,k) = KE(m,k)K^{-1} = \begin{bmatrix} m & 0 \\ 0 & r \end{bmatrix} \quad (4)$$

The introduced encryption algorithm provides additive and multiplicative properties:

$$\begin{aligned} E(m_1) + E(m_2) &= K^{-1}\begin{bmatrix} m_1 & 0 \\ 0 & r_1 \end{bmatrix}K + K^{-1}\begin{bmatrix} m_2 & 0 \\ 0 & r_2 \end{bmatrix}K \\ &= K^{-1}\begin{bmatrix} m_1+m_2 & 0 \\ 0 & r_1+r_2 \end{bmatrix}K \\ &= E(m_1+m_2) \end{aligned} \quad (5)$$

$$\begin{aligned} E(m_1) \times E(m_2) &= K^{-1}\begin{bmatrix} m_1 & 0 \\ 0 & r_1 \end{bmatrix}K \times K^{-1}\begin{bmatrix} m_2 & 0 \\ 0 & r_2 \end{bmatrix}K \\ &= K^{-1}\begin{bmatrix} m_1 \times m_2 & 0 \\ 0 & r_1 \times r_2 \end{bmatrix}K = E(m_1 \times m_2) \end{aligned} \quad (6)$$

One can see that the MORE approach is FHE because it satisfies the both homomorphic properties. But this approach presents high storage overhead and in [16] a key recovery attack on MORE that requires only side channel information on plaintext is given. Thus providing an inefficient FHE algorithm.

Table 1
PORE approach.

Secret key	$K = (v_1, v_2)$
Public parameters	$b = -(v_1 + v_2)mod(N)$ $c = (v_1 v_2)mod(N)$
Plaintext space	set of x in a ring Z_N.
Encryption process	$Enc(x) = (a, d)$ that satisfies $\begin{matrix} av_1 + d = x \\ av_2 + d = r \end{matrix}$ r is a random integer
Ciphertext space	set of $(a, d) \in Z_N \times Z_N$
Decryption process	$x = (av_1 + d)mod(N)$
Fully Homomorphic	b and c should be exposed to the cloud.

2.2. PORE approach

The PORE approach which stands for Polynomial Operation for Randomization and Encryption is proposed in [10]. It is a FHE Algorithm that satisfies both properties, Addition and Multiplication. A summary of this FHE algorithm is given in Table 1, as we implement it to achieve the comparison with our Enhanced MORE.

3. Building the Enhanced MORE

Based on the MORE Approach, Enhanced MORE is built without altering its homomorphic behavior. The different enhancement steps are illustrated in Fig. 1 and will be explained below:

3.1. Dynamic key generation (DK)

The two end hosts should agree on two secret parameters: a secret key and an initial vector (IV). Using a secure hash algorithm, a dynamic key (DK) of 64 bytes is created. Three different keys are picked and used to form three different cipher layers as follows (Fig. 1) :

- DK_p: Dynamic Key for Permutation formed of 23 bytes.
- DK_d: Dynamic Key for Diffusion formed of 16 bytes.
- DK_s: Dynamic Key for Selection formed of 23 bytes.

3.2. Permutation box

Using DK_p, a permutation box is generated and applied over the input plaintext. In our Enhanced MORE implementation, the creation of a permutation box is done similar to [17]. The key dependent permutation technique is employed because it preserves the homomorphic properties [17],[18]. The interpretation of the homomorphic behavior of a permutation box is shown as follows:

Suppose that we have a permutation box called π of dimension N defined by: $\pi = [p_i]_{1\le i\le N}$.

Two plaintexts X and Y of dimension N are given: $X = [x_i]_{1\le i\le N}$ and $Y = [y_i]_{1\le i\le N}$.

After permutation $\pi(X) = [x_{p_i}]_{1\le i\le N}$ and $\pi(Y) = [y_{p_i}]_{1\le i\le N}$.

Suppose that $\odot$ is a law defined over the plaintexts by:

$X \odot Y = [x_i]_{1\le i\le N} \odot [y_i]_{1\le i\le N} = [x_i \odot y_i]_{1\le i\le N} = [z_i]_{1\le i\le N} = Z$.

$\pi(X \odot Y) = \pi(Z) = [z_{p_i}]_{1\le i\le N} = [x_{p_i} \odot y_{p_i}]_{1\le i\le N}$.

And $\pi(X) \odot \pi(Y) = [x_{p_i}]_{1\le i\le N} \odot [y_{p_i}]_{1\le i\le N} = [x_{p_i} \odot y_{p_i}]_{1\le i\le N}$.

Since $\pi(X \odot Y) = \pi(X) \odot \pi(Y)$, we can deduce the homomorphic behavior of π.

3.3. Dynamic block encryption

After the Permutation box, the permuted plaintexts of dimension l is divided into H blocks, where $H = \left\lceil \frac{l}{n} \right\rceil$, n is the block size as shown in Fig. 2. Each block of dimension n is encrypted with