Alabama Journal of Mathematics
39 (2015)
ISSN 2373-0404

An Elementary Generalization on Modified Rivest Encryption

Emin Aygün
Department of Mathematics
Erciyes University

Erkam Lüy
Department of Mathematics
Erciyes University

Zekeriya Y. Karatas
Department of Mathematics
Tuskegee University

In this article, we construct a new cryptosystem by an elementary improvement on the famous Modified Rivest Encryption. This improvement allows us to build up a stronger system. We deceive the attackers by using a mod value other than the public key.

Introduction

The privacy homomorphism idea was first introduced in 1978 by Rivest, Adleman and Dertouzos in Rivest, Adleman, and Dertouzos (1978). In 1982, S. Goldwasser and S. Micali established Goldwasser-Micali cryptosystem Goldwasser and Micali (1982), and a generalization of this system, Pailler cryptosystem Pailler (1999), developed in 1999. In these cryptosystems, two operations were considered for homomorphism, addition and multiplication. Some cryptosystems are homomorphic according to a single operation. The famous well-known RSA and El-Gamal cryptosystems are homomorphic according to only multiplication, see Silverberg (2013). On the other hand, Pailler cryptosystem is only homomorphic according to addition. None of these cryptosystems provide the feature of being homomorphic with respect to two operations. They are homomorphic only for one operation, only addition or only multiplication.

The first fully homomorphic encryption scheme, homomorphic with respect to both addition and multiplication, was built by Gentry in 2009, see Gentry (2009). By this breakthrough result, homomorphic encryption gained its popularity again.

However, especially in electronic voting, additional homomorphic encryption schemes are systems of interest and sufficient for application. In Rivest et al. (1978), authors also introduced Modified Rivest Scheme which is homomorphic with respect to addition and scalar multiplication, and hence, this scheme is very useful for electronic voting. However, in Vizar and Vaudenay (2014), authors broke the Modified Rivest Scheme.

In this paper, we construct a homomorphic symmetric key encryption scheme similar to Modified Rivest Scheme by an elementary improvement. We also show that our scheme is homomorphic according to addition and scalar multiplication as well. After this elementary modification, we obtain a more secure scheme than Modified Rivest. Our modification depends on the usage of two different mod values, which will clearly mislead the attacker.

Corresponding Author Email: zkaratas@mytu.tuskegee.edu

Modified Rivest Scheme

The algorithm is as follows:
Keygen:

1. Choose two large prime p and q numbers, each almost same size.
2. Compute $n = pq$.
3. Choose two vectors $\mathbf{r} = (r_1, \dots, r_k) \in (\mathbb{Z}_p^*)^k$ and $\mathbf{s} = (s_1, \dots, s_k) \in (\mathbb{Z}_q^*)^k$.
4. Public key is n, and secret key is $(p, q, \mathbf{r}, \mathbf{s})$.

Encryption:

1. Choose a vector $(x_1, \dots, x_k)$ with $\sum_{i=1}^k x_i \equiv x \pmod{n}$, x being the plaintext.
2. Compute $(c_i, c_i') = (r_i x_i \pmod{p}, s_i x_i \pmod{q})$ for $i = 1, \dots, k$.
3. Ciphertext is $\mathbf{c} = ((c_1, c_1'), \dots, (c_k, c_k'))$.

Decryption:

1. Use Chinese Remainder Theorem to compute the systems of equations
   $x_i \equiv r_i^{-1} c_i \pmod{p}$
   $x_i \equiv s_i^{-1} c_i' \pmod{q}$ for $i = 1, \dots, k$.
2. The plaintext is $x \equiv \sum_{i=1}^k x_i \pmod{n}$.

Our Scheme

The algorithm is as follows:
Keygen:

1. Choose two large random positive integers l and m with a large greatest common divisor, each almost same size.
2. Compute $\gcd(l, m) = a$.
3. Compute $n = lm$.
4. Compute $\overline{n} = \frac{n}{a^2}$. Define $\overline{l} = \frac{l}{a}$, and $\overline{m} = \frac{m}{a}$.
5. Choose two vectors $\mathbf{r} = (r_1, \ldots, r_k) \in (\mathbb{Z}_l^*)^k$ and $\mathbf{s} = (s_1, \ldots, s_k) \in (\mathbb{Z}_m^*)^k$.
6. Public key is n, and secret key is $(l, m, \mathbf{r}, \mathbf{s})$.

Encryption:

1. Compute $\gcd(l, m) = a, \overline{n} = \frac{n}{a^2}$.
2. Choose a vector $(x_1, \ldots, x_k)$ with $\sum_{i=1}^{k} x_i \equiv x \pmod{\overline{n}}$, x being the plaintext.
3. Compute $(c_i, c_i') = (r_i x_i \pmod{l}, s_i x_i \pmod{m})$ for $i = 1, \ldots, k$.
4. Ciphertext is $\mathbf{c} = ((c_1, c_1'), \ldots, (c_k, c_k'))$.

Decryption:

1. Use Chinese Remainder Theorem to compute the systems of equations
 $x_i \equiv r_i^{-1} c_i \pmod{\overline{l}}$
 $x_i \equiv s_i^{-1} c_i' \pmod{\overline{m}}$ for $i = 1, \ldots, k$.
2. The plaintext is $x \equiv \sum_{i=1}^{k} x_i \pmod{\overline{n}}$.

Theorem 1. *The algorithm given above works.*

Proof. Note first that, $\overline{l} = \frac{l}{\gcd(l,m)}$, and $\overline{m} = \frac{m}{\gcd(l,m)}$ are obviously relatively prime. Moreover, by the choice of r_i's and s_i's, r_i^{-1} and s_i^{-1} exist for every i. Hence for each i, we obtain the system

$$x_i \equiv r_i^{-1} c_i \pmod{\overline{l}}$$
$$x_i \equiv s_i^{-1} c_i' \pmod{\overline{m}}$$

from $(c_i, c_i') = (r_i x_i \pmod{\overline{l}}, s_i x_i \pmod{\overline{m}})$. By, Chinese Remainder Theorem, this system has a unique solution $x_i \pmod{\overline{l}\overline{m}}$, which is $x_i \pmod{\overline{n}}$. So, we get $x \equiv \sum_{i=1}^{k} x_i \pmod{\overline{n}}$ our algorithm works correctly. □

Next, we investigate the homomorphic properties of the scheme. As in Modified Rivest Scheme, our scheme is additional homomorphic. Moreover, although it is not multipicative homomorphic, it is homomorphic with respect to scalar multiplication. Here is our theorem.

Theorem 2. *The scheme given above is homomorphic according to addition and scalar multiplication.*

Proof. Let $\mathbf{c}, \mathbf{d}$ be the ciphertexts of the plaintexts x, y respectively. Now, $\mathbf{c} + \mathbf{d} = ((c_1 + d_1, c_1' + d_1'), \ldots, (c_k + d_k, c_k' + d_k'))$. If we decrypt $\mathbf{c} + \mathbf{d}$ by our algorithm, we will have the system

$$z_i \equiv r_i^{-1}(c_i + d_i) \pmod{\overline{l}}$$
$$z_i \equiv s_i^{-1}(c_i' + d_i') \pmod{\overline{m}}\ ,$$

by using Chinese Remainder Theorem, we have the unique solution $z_i \equiv x_i + y_i \pmod{\overline{n}}$, since the systems

$$x_i \equiv r_i^{-1} c_i \pmod{\overline{l}}$$
$$x_i \equiv s_i^{-1} c_i' \pmod{\overline{m}}\ \text{, and}$$

$$y_i \equiv r_i^{-1} d_i \pmod{\overline{l}}$$
$$y_i \equiv s_i^{-1} d_i' \pmod{\overline{m}}$$

has unique solutions $x_i \pmod{\overline{n}}$ and $y_i \pmod{\overline{n}}$, respectively.

Similarly, by using the basic properties of congruences, we show that $t\mathbf{c}$ has decryption x, where t is an unencrypted constant in $\mathbb{Z}_{\overline{n}}$. □

An Example of Our Scheme

Keygen:

1. Choose two random positive integers $l = 8$ and $m = 10$.
2. Compute $\gcd(l, m) = (8, 10) = 2 = a$.
3. Compute $n = lm = 8 \cdot 10 = 80$.
4. Compute $\overline{n} = \frac{n}{a^2} = 20$. Define $\overline{l} = \frac{l}{a} = 4$, and $\overline{m} = \frac{m}{a} = 5$.
5. Choose two vectors $\mathbf{r} = (1, 3) \in (\mathbb{Z}_8^*)^2$ and $\mathbf{s} = (7, 9) \in (\mathbb{Z}_{10}^*)^2$.
6. Public key is $n = 80$, and secret key is $(l = 8, m = 10, \mathbf{r} = (1, 3), \mathbf{s} = (7, 9))$.

Encryption:

1. Compute $\gcd(l, m) = a = 2, \overline{n} = \frac{n}{a^2} = 20$.
2. Let $x = 5$ be the plaintext. Choose a vector $(x_1, x_2) = (2, 3)$ with $\sum_{i=1}^{2} x_i \equiv x \pmod{20}$,
3. Compute $(c_1, c_1') = (r_1 x_1 \pmod{8} = 1 \cdot 2 = 2 \pmod{8}, s_1 x_1 \pmod{10} = 7 \cdot 2 = 4 \pmod{10})$ and $(c_2, c_2') = (r_2 x_2 \pmod{8} = 3 \cdot 3 = 1 \pmod{8}, s_2 x_2 \pmod{10} = 9 \cdot 3 = 7 \pmod{10})$.

4. Ciphertext is $\mathbf{c} = ((2, 4), (1, 7))$.

Decryption:

1. Use Chinese Remainder Theorem to compute the systems of equations
   $x_1 \equiv r_1^{-1} c_1 = 1 \cdot 2 = 2 \pmod 4$
   $x_1 \equiv s_1^{-1} c_1' = 3 \cdot 4 = 2 \pmod 5$. So, if we solve this system, we obtain $x_1 \equiv 2 \pmod{20}$. With the same idea, we obtain $x_2 \equiv 3 \pmod{20}$.
2. The plaintext is $x \equiv \sum_{i=1}^{2} x_i \pmod{20} = 2 + 3 = 5$.

Security

Security of the Modified Rivest Scheme depends on large integer factorization problem. But in Vizar and Vaudenay (2014), authors broke the scheme with a known-plaintext, key recovery attack. Their attack do not use factorization, instead, they break the scheme with a vector produced by solving a matrix equation. Also, they use public key n while breaking the scheme. Here, it is clear that n must be public because of the property of homomorphic encryption. However, in our scheme, we do decryption with respect to mod $\overline{n}$, whereas we do encryption in mod n. Moreover, the attacker does not know $\overline{n}$. Hence, if the attack in Vizar and Vaudenay (2014) applied to our algorithm, the attacker will obtain a (chosen to be large) many plaintext instead of one. So, the attacker will not be sure about the correct one. Thus, security increases compared to the original scheme.

Conclusion

In this paper, we establish a homomorphic symmetric key encryption scheme similar to Modified Rivest Scheme by an elementary modification. Our scheme increases the security of the original scheme. Moreover, in Modified Rivest Scheme, encryption and decryption are done in public key mod n, however, we use n for encryption and $\overline{n}$ for decryption to deceive the attackers. This usage of two different mod values is a new idea and makes this algorithm more stronger. Our schemes is very simple and useful for applications like electronic voting.

References

Gentry, C. (2009). A fully homomorphic encryption scheme. *Ph.D. Thesis*. (Stanford University)

Goldwasser, S., & Micali, S. (1982). Probabilistic encryption and how to play mental poker keeping secret all partial information. *Proceedings of the 14th ACM Symposium on Theory of Computing*, 365–377.

Pailler, P. (1999). Public-key cryptosystems based on composite degree residuosity classes. *Advances in Cryptology, EUROCRYPT*, 223–238.

Rivest, R. L., Adleman, L. A., & Dertouzos, M. (1978). On data banks and privacy homomorphisms. *Foundations of Secure Computation*, 169–179.

Silverberg, A. (2013). Fully homomorphic encryption for mathematicians. *sponsored by DARPA under agreement numbers FA8750-11-1-0248 and FA8750- 13-2-0054*.

Vizar, D., & Vaudenay, S. (2014). Cryptanalysis of chosen symmetric homomorphic schemes. *EPFL CH*-1015. (Lausanne, Switzerland)