J. Math. Cryptol. **8** (2014), 297–303
DOI 10.1515/jmc-2013-0018

Security analysis of Modified Rivest Scheme

Deepthi Haridas, Sarma Venkataraman and Geeta Varadan

Communicated by Doug Stinson

Abstract. The Modified Rivest Scheme (MRS) is an additive homomorphic scheme recently used in many applications which demands third party processing of encrypted data. The present study carries out a comprehensive security analysis of MRS. We work out an attack from the category of known plaintext, chosen plaintext, chosen ciphertext where the adversary is having with him the pair of plaintext and its corresponding ciphertext. It is demonstrated that in such a scenario the adversary can compute the private key of the legitimate node causing threat to the security of the entire system. The novelty of the present study lies in the fact that any attack from the above mentioned category could be mounted on MRS (which is not being attacked so far), irrespective of the fact whether the modulus of the underlying MRS is kept private or made public.

Keywords. Data encryption, probabilistic methods, privacy homomorphism.

2010 Mathematics Subject Classification. 11T71, 43A22, 68P25, 94A60.

1 Introduction

Encryption is a well-known technique for preserving the privacy of sensitive information. The inherent limitation of the conventional encryption model is that an information system working on encrypted data can at most store or retrieve data for the user. With a conventional encryption model any further complicated operations on the encrypted data usually require the data be decrypted first before being operated on. In 1978, Rivest, Adleman and Dertouzous [8] addressed this problem. Privacy homomorphism/homomorphic encryption is the proposed solution toward encrypted data processing. As the internet is playing a crucial role in business network, homomorphic encryption is a prime cause of concern for security.

Our earlier work [3] presents a strengthened version of Iterated Hill Cipher (IHC), a homomorphic encryption scheme [2]. As an extension to [3] of analyzing the two homomorphic encryption schemes [2], the current study evaluates the security of the Modified Rivest Scheme (MRS); see [1, 2]. MRS is used in many applications, as it is an additive symmetric homomorphic scheme, so it is fast and, up to the present, it has not been cryptanalyzed successfully. Cheon,

Kim and Nam reported an attack on Domingo–Ferrer's additively homomorphic scheme [5, 6]. Many schemes based on MRS have been developed for Wireless Sensor Networks (WSN), which comprises of secure data aggregation scheme, secure key agreement scheme and strong key-predistribution scheme [4, 7, 9]. It has been observed that MRS is not secure with our proposed attack based on linear algebra.

The rest of the paper is structured as follows. The detailed MRS scheme is presented in Section 2. Section 3 gives the security analysis of MRS; Section 3.1 discusses the case for n being public and Section 3.2 the case for n being private. An example to illustrate the efficiency of the attack is given in Section 3.3. Finally, Section 4 concludes the interpretation for the known plaintext attack on MRS.

2 Modified Rivest Scheme

The Modified Rivest Scheme [1, 2] works as follows with the encryption function $\mathbb{E}_k : \mathbb{Z}_n \to (\mathbb{Z}_n * \mathbb{Z}_n)^d$:

Setup. To encrypt a message $m \in \mathbb{Z}_n$, $m = \sum_{i=1}^{d} m_i \bmod n$ where $d \in \mathbb{Z}$, the public parameter is (d, n) and the private key

$$K = (p, q, r_1, \ldots, r_i, \ldots, r_d, s_1, \ldots, s_i, \ldots, s_d),$$

where $r_i < p$ and $s_i < q$ are randomly selected for all $i \in [1, d]$. Note that r_i's and s_i's need to be different to avoid the attack due to the vulnerable form of encrypted zero's.

Encryption.

$$\begin{aligned}\mathbb{E}_{p,q,r_i,s_i}(m) &= \big((m_1 r_1 \bmod p, m_1 s_1 \bmod q), (m_2 r_2 \bmod p, m_2 s_2 \bmod q),\\ &\qquad \ldots, (m_d r_d \bmod p, m_d s_d \bmod q)\big)\\ &= \big((x_1, y_1), (x_2, y_2), \ldots, (x_d, y_d)\big).\end{aligned}$$

Decryption. Given a ciphertext $c = ((x_1, y_1), (x_2, y_2), \ldots, (x_d, y_d))$, decrypt c as follows:

- Multiply the components with the corresponding r_i^{-1} and s_i^{-1} in mod p and mod q, respectively:

$$\begin{aligned}&\big((x_1 r_1^{-1} \bmod p, y_1 s_1^{-1} \bmod q), (x_2 r_2^{-1} \bmod p, y_2 s_2^{-1} \bmod q),\\ &\qquad \ldots, (x_d r_d^{-1} \bmod p, y_d s_d^{-1} \bmod q)\big).\end{aligned}$$

- Use the Chinese Remainder Theorem to find $m_1, m_2, \ldots, m_d \bmod n$.
- Sum up m_i's to recover m.

Homomorphism. Let $\mathbb{E}_K(a) = ((x_1, y_1), \ldots, (x_d, y_d))$, $t \in \mathbb{Z}_n$ be a constant and $\mathbb{E}_K(b) = ((u_1, v_1), \ldots, (u_d, v_d))$, where $K = (p, q, r_i, s_i)$, $i \in [1, l]$ is the secret key. Addition and multiplication are defined as follows:

$$\mathbb{E}_K(a + b) = \big(((x_1 + u_1), (y_1 + v_1)), \ldots, ((x_d + u_d), (y_d + v_d))\big) \bmod n,$$
$$\mathbb{E}(t.a) = \big((tx_1, ty_1), \ldots, (tx_d, ty_d)\big) \bmod n.$$

3 Security analysis of MRS

Let us assume that the adversary holds

$$\big\{(m, E_K(m)) \mid m \in S \text{ and } K \text{ is the private key}\big\},$$

where S is the set of plaintext, E stands for MRS encryption and the private key K is known only to legitimate node. The present section demonstrates an attack based on linear algebra which successfully computes K for the adversary.

Theorem. *The Modified Rivest Scheme can be successfully attacked. If the modulus n is public, MRS can be attacked with $d + 1$ linearly independent plaintext-ciphertext pairs. If the modulus n is secret, MRS can be attacked with $d + 2$ linearly independent plaintext-ciphertext pairs.*

Proof. Let $m \in \mathbb{Z}_n$ be a plaintext such that

$$m \equiv m_1 + m_2 + \cdots + m_d \bmod n.$$

Then

$$\mathbb{E}_K(m) = \big((m_1 r_1 \bmod p, m_1 s_1 \bmod q), \ldots, (m_d r_d \bmod p, m_d s_d \bmod q)\big)$$
$$= \big((x_1, y_1), (x_2, y_2), \ldots (x_d, y_d)\big),$$

where $x_i = r_i m_i \bmod p$ and $y_i = s_i m_i \bmod q$.

For a subset S of $\mathbb{Z}_n$, if $\{(m, \mathbb{E}_p(m)) \mid m \in S\}$ and $\{(m, \mathbb{E}_q(m)) \mid m \in S\}$ (where $\mathbb{E}_p(m) = (x_1, \ldots, x_d)$ and $\mathbb{E}_q(m) = (y_1, \ldots y_d)$) are linearly independent as a module element of $\mathbb{Z}_n^{d+1}$ over $\mathbb{Z}_n$, then $\{(m, \mathbb{E}_K(m)) \mid m \in S\}$ is linearly independent over $\mathbb{Z}_n$.

Since p and q divide n, we have

$$m \equiv m_1 + m_2 + \cdots + m_d \bmod p. \tag{3.1}$$

Substituting $x_i = m_i r_i \bmod p$ and $y_i = m_i s_i \bmod q$ in (3.1), we get

$$-m + x_1 t_1 + x_2 t_2 + \cdots + x_d t_d \equiv 0 \bmod p,$$
$$-m + y_1 \hat{t}_1 + y_2 \hat{t}_2 + \cdots + y_d \hat{t}_d \equiv 0 \bmod q,$$

where $t_i = r_i^{-1} \bmod p$ and $\hat{t}_i = s_i^{-1} \bmod q$ for $i = 1, \ldots, d$.

3.1 Case 1: *n* is public

The adversary has $d + 1$ linearly independent plaintext-ciphertext pairs (M_i, C_i), $i = 1, 2, \ldots, d + 1$ over $\mathbb{Z}_n$. Let $C_i = ((x_{i1}, y_{i1}), (x_{i2}, y_{i2}), \ldots, (x_{id}, y_{id}))$. Then

$$-M_i + x_{i1} t_1 + x_{i2} t_2 + \cdots + x_{id} t_d \equiv 0 \bmod p \quad \text{for all } 1 \leq i \leq d + 1.$$

In matrix form:

$$\begin{bmatrix} M_1 & x_{11} & x_{12} & \ldots & x_{1d} \\ M_2 & x_{21} & x_{22} & \ldots & x_{2d} \\ \vdots & & & & \\ M_{d+1} & x_{d+11} & x_{d+12} & \ldots & x_{d+1d} \end{bmatrix} \begin{bmatrix} -1 \\ t_1 \\ \vdots \\ t_d \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \bmod p. \tag{3.2}$$

Since $d + 1$ pairs (M_i, C_i) are linearly independent, the homogeneous equation (3.2) has a non-trivial solution in $\mathbb{Z}_p^d$, the coefficient matrix A such that $\det(A) \neq 0$,

$$A = [M|C] = \begin{bmatrix} M_1 & x_{11} & x_{12} & \ldots & x_{1d} \\ M_2 & x_{21} & x_{22} & \ldots & x_{2d} \\ \vdots & & & & \\ M_{d+1} & x_{d+11} & x_{d+12} & \ldots & x_{d+1d} \end{bmatrix}.$$

Then $\gcd(\det(A) \bmod n, n) = p$, and hence q can be calculated from $q = n/p$. Solving the system of linear equations (3.2) over $\mathbb{Z}_p$, the components of secret key r_p, r_q can be computed, where p, q are known.

The entire private key set K can be computed using $d + 1$ linearly independent plaintext ciphertext pairs.

3.2 Case 2: *n* is secret

Assume $d + 2$ known plaintext-ciphertext pairs linearly independent over $\mathbb{Z}$, not in $\mathbb{Z}_n$. Each $d + 1$ pairs constitute a $(d + 1) \times (d + 1)$ coefficient matrix A_i for $i = 1, 2, \ldots, d + 2$ as in equation (3.2).

The probability of

$$\gcd\big(\det(A_1)/l, \det(A_2)/l, \ldots, \det(A_k)/l\big) = 1$$

can be estimated by approximately $1/\zeta$ with $\zeta(k) := \sum_{n=1}^{\infty} \frac{1}{n^k}$, where $l = m.p$, $2 \leq k \leq d + 2$. The approximate value of $1/\zeta(k)$ for $k = 2, 3, 4, \ldots, 101$ is $0.6078, 0.832, 0.9239, \ldots, 0.93$.

Once n is known, the other secret keys r_p and r_q can be obtained similarly to Section 3.1. In this manner the entire set of private keys K is determined. □

3.3 Example to illustrate the efficiency of the attack

The following example [2] illustrates the analysis worked out in the present study. Let $p = 7$ and $q = 11$, then $n = 77$. For simplicity, let $d = 2$, i.e., each plaintext message is split into two smaller parts. Let $r_1 = s_1 = 5$ and $r_2 = s_2 = 3$.

The encryption of the four plaintext numbers $a = 10$, $b = 7$, $c = 5$ and $e = 1$ are as follows:

$$\begin{aligned}
\mathbb{E}(a) &= \mathbb{E}(a_1, a_2) = \mathbb{E}(4, 6) = ((6, 9), (4, 7));\\
\mathbb{E}(b) &= \mathbb{E}(b_1, b_2) = \mathbb{E}(3, 4) = ((1, 4), (5, 1));\\
\mathbb{E}(c) &= \mathbb{E}(c_1, c_2) = \mathbb{E}(1, 4) = ((5, 5), (5, 1));\\
\mathbb{E}(e) &= \mathbb{E}(e_1, e_2) = \mathbb{E}(4, -3) = ((6, 9), (5, 2)).
\end{aligned}$$

For decryption:

$$\begin{aligned}
r_1^{-1} &= 5^{-1} \equiv 3 \bmod 7; \quad s_1^{-1} = 5^{-1} \equiv 9 \bmod 11;\\
r_2^{-1} &= 3^{-1} \equiv 5 \bmod 7; \quad s_2^{-1} = 3^{-1} \equiv 4 \bmod 11.
\end{aligned}$$

Case 1: *n* is public. Using the three plaintext-ciphertext pairs $\{(10, \mathbb{E}(10)), (7, \mathbb{E}(7)), (5, \mathbb{E}(5))\}$, the coefficient matrix is

$$A_1 = \begin{bmatrix} 10 & 6 & 4 \\ 7 & 1 & 5 \\ 5 & 5 & 5 \end{bmatrix}.$$

Then $\gcd(\det(A_1) \bmod n, n) = \gcd(14, 77) = 7 = p$.

Case 2: *n* is secret. Considering the fourth plaintext $e = 1$, the second coefficient matrix for plaintext-ciphertext pairs $\{(10, \mathbb{E}(10)), (7, \mathbb{E}(7)), (1, \mathbb{E}(1))\}$ is

$$A_2 = \begin{bmatrix} 10 & 6 & 4 \\ 7 & 1 & 5 \\ 1 & 6 & 5 \end{bmatrix}.$$

Then

$$\begin{aligned} \gcd(\det(A_1), \det(A_2)) = 14 &\implies t_1 = 5^{-1} \bmod 7 \implies r_1 = 5 \\ &\implies t_2 = 3^{-1} \bmod 7 \implies r_2 = 3 \end{aligned}$$

and

$$\begin{aligned} q = 11 &\implies \hat{t}_1 = 5^{-1} \bmod 11 \implies s_1 = 5 \\ &\implies \hat{t}_2 = 3^{-1} \bmod 11 \implies s_2 = 3. \end{aligned}$$

The present work (for $d = 2$) reveals all the parameters of the secret keys, i.e., $(p, q, r_1, r_2, s_1, s_2)$ of MRS using the proposed attack based on linear algebra.

4 Conclusion

The present work carries out a comprehensive security analysis of the Modified Rivest Scheme, a homomorphic scheme. An exhaustive mathematical analysis is carried out to demonstrate the vulnerability of MRS resulting in feasible computation of the private key by the adversary, using the attack based on linear algebra. It is an open problem whether there exist more algebraic privacy homomorphic schemes which could be cryptanalyzed on similar line of attack.

Bibliography

[1] A. C.-F. Chan, Distributed symmetric key management for mobile ad hoc networks, in: *Twenty-Third Annual Joint Conference of the IEEE Computer and Communications Societies* (INFOCOM 2004), 2414–2424.

[2] A. C.-F. Chan, Symmetric key homomorphic encryption for encrypted data processing, in: *IEEE International Conference on Communications* (ICC 2009), 1–5.

[3] D. Haridas, S. Venkatraman and G. Varadan, Strengthened iterated Hill cipher for encrypted processing, in: *2nd IEEE International Conference on Parallel Distributed and Grid Computing* (PDGC 2012), 491–496.

[4] T. Kim and G. Wang, A strong key pre-distribution scheme for wireless sensor networks, in: *Ubiquitous Intelligence and Computing*, Lecture Notes in Comput. Sci. 4159, Springer, Berlin (2006), 854–863.

[5] J. H. Cheon and H. S. Nam, A cryptanalysis of the original Domingo–Ferrer's algebraic privacy homomophism, preprint (2003), `https://eprint.iacr.org/2003/221.pdf`.

[6] J. H. Cheon, W.-H. Kim and H. S. Nam, Known-plaintext cryptanalysis of the Domingo–Ferrer algebraic privacy homomorphism scheme, *Inform. Process. Lett.* **97** (2006), 118–123.

[7] T. Kim, G. Wang and G. Cho, A secure key agreement scheme in low-energy wireless sensor networks, in: *Embedded and Ubiquitous Computing*, Lecture Notes in Comput. Sci. 4096, Springer, Berlin (2006), 79–88.

[8] R. L. Rivest, L. Adleman and M. L. Dertouzous, On data banks and privacy homomorphisms, in: *Foundations of Secure Computation*, Academic Press, London (1978), 169–179.

[9] M. K. Sandhya and K. Murugan, Secure data aggregation in wireless sensor networks using privacy homomorphism, *Commun. Comput. Inf. Sci.* **132** (2011), 482–490.

Received April 26, 2013; revised December 21, 2013; accepted March 7, 2014.

Author information

Deepthi Haridas, Advanced Data Processing Research Institute (ADRIN),
203. Akbar Road, Secunderabad, Andhra Pradesh, India.
E-mail: `haridasdeepthi@gmail.com`

Sarma Venkataraman, Advanced Data Processing Research Institute (ADRIN),
203. Akbar Road, Secunderabad, Andhra Pradesh, India.
E-mail: `kalk@adrin.res.in`

Geeta Varadan, Advanced Data Processing Research Institute (ADRIN),
203. Akbar Road, Secunderabad, Andhra Pradesh, India.
E-mail: `geetha@adrin.res.in`