Comment on "Improved Secure RSA Cryptosystem (ISRSAC) for Data Confidentiality in Cloud"

Chenglian Liu[1,2] and Chieh-Wen Hsu[3]

(Corresponding author: Chenglian Liu)

Department of Computer Engineering, Dongguan Polytechnic Institute[1]
Dongguan 523808, China
(Email: chenglian.liu@gmail.com)
School of Computing, Neusoft Institute of Guangdong[2]
Foshan 528225, China
Economics and Management College, Zhaoqing University[3]
Zhaoqing 526061, China

(Received Apr. 15, 2018; Revised and Accepted Aug. 16, 2018; First Online Mar. 17, 2019)

Abstract

Data storage in the cloud is a very popular storage method because of the cost savings resulting from the user not needing hardware, software or space. However, data storage in the cloud has unique requirements because the current technical and environment. On March 2018, Thangavel and Varalakshmi proposed an "Improved Secure RSA cryptosystem (ISRSAC) for Data Confidentiality in Cloud". They modified the RSA algorithm into another one called MRSAC. In this paper, the author will examine the flaw from that scheme.

Keywords: Flaw; MRSAC; RSA

1 Introduction

Thangavel *et al.* [4] proposed the ESRKGS scheme in 2005, which stemmed from their RSA modification. The $\phi(n)$ of RSA [2] used two prime numbers, and Thangavel used four primes to generate its $\phi(n)$. Lüy *et al.* [1] discussed the vulnerability of Thangavel's scheme, and also gave an example. Thangavel and Varalakshmi [3] modified the ESRKGS algorithm to ISRSAC scheme. Unfortunately, there is a flaw in ISRSAC scheme, we would describe this situation on next section.

2 ISRASC Algorithm

RSA cryptosystem consists of three phases: Prime key generation, encryption and decryption. The problem is that RSA is not secure against a brute force attack. The security of RSA cryptosystem depends on the large prime number because it is difficult to break. Hence a modified version of RSA for secure key generation is used to generate the public and private keys. The resulting algorithm is known as ISRSAC. To start the algorithm, we randomly choose two large primes p and q where where $p \neq q, p > 3, q > 3$, and find

$$\begin{aligned} n &= p \cdot q \cdot (p-1) \cdot (q-1) \\ m &= p \cdot q. \end{aligned}$$

An integer r is randomly selected where $p > 2^r > q$, which generates $\alpha(n)$

$$\alpha(n) = \frac{(p-1)(q-1)(p-2^r)(q-2^r)}{2^r}$$

The public key e is satisfying $1 < e < \alpha(n)$ where $\gcd(e, \alpha(n)) = 1$

$$e \cdot d \equiv 1 \pmod{\alpha(n)}.$$

The public key pair is (e, n), and private key pair is (d, m).

Encryption: Suppose the M is plaintext or digitize message. We get ciphertext C by

$$C \equiv M^e \pmod{n}.$$

Decryption: We recovery message by

$$M \equiv C^d \pmod{m}.$$

3 Our Comment

3.1 The Parameter 2^r Problem

As known 2^r where

$$p > 2^r < q.$$

There are four types as follow:

Type 1: $p = 4n + 1$ and $q = 4m + 1$ forms.

Type 2: $p = 4n + 3$ and $q = 4m + 1$ forms.

Type 3: $p = 4n + 1$ and $q = 4m + 3$ forms.

Type 4: $p = 4n + 3$ and $q = 4m + 3$ forms.

Proof.

The Type 1. Since

$$4m + 1 < 2^r < 4n + 1,$$

we get

$$\begin{aligned} 4m + 1 < 2^r \quad &\Rightarrow \quad m < \frac{2_r - 1}{4} \\ 4n + 1 > 2^r \quad &\Rightarrow \quad n > \frac{2_r - 1}{4} \end{aligned}$$

The Type 2. Since

$$4m + 1 < 2^r < 4n + 3,$$

we get

$$\begin{aligned} 4m + 1 < 2^r \quad &\Rightarrow \quad m < \frac{2_r - 1}{4} \\ 4n + 3 > 2^r \quad &\Rightarrow \quad n > \frac{2_r - 3}{4} \end{aligned}$$

The Type 3. Since

$$4m + 3 < 2^r < 4n + 1,$$

we get

$$\begin{aligned} 4m + 3 < 2^r \quad &\Rightarrow \quad m < \frac{2_r - 3}{4} \\ 4n + 1 > 2^r \quad &\Rightarrow \quad n > \frac{2_r - 1}{4} \end{aligned}$$

The Type 4. Since

$$4m + 3 < 2^r < 4n + 3,$$

we get

$$\begin{aligned} 4m + 3 < 2^r \quad &\Rightarrow \quad m < \frac{2_r - 3}{4} \\ 4n + 3 > 2^r \quad &\Rightarrow \quad n > \frac{2_r - 3}{4} \end{aligned}$$

By Type 1 and Type 2, we get

$$m < \frac{2^r - 1}{4} \tag{1}$$

By Type 3 and Type 4, we get

$$m < \frac{2^r - 3}{4} \tag{2}$$

Suppose Equation (1) ∩ Equation (2), we know

$$m < \frac{2^r - 3}{4}$$

By Type 1 and Type 3, we get

$$n > \frac{2^r - 1}{4} \tag{3}$$

By Type 2 and Type 4, we get

$$n > \frac{2^r - 3}{4} \tag{4}$$

Suppose Equation (3) ∩ Equation (4), we obtain

$$n > \frac{2^r - 1}{4}$$

When $n > \frac{2^r-1}{4}$ and $m < \frac{2^r-3}{4}$ where $r \in \mathbb{Z}^+$, we get

$$q < 2^r < p.$$

□

3.2 The Core Algorithm

As known

$$\alpha(n) = \frac{(p-1)(q-1)(p-2^r)(q-2^r)}{2^r}.$$

p, q are both primes. If $r > 2, r \in \mathbb{Z}^+$, $\alpha(n)$ is not an integer.

Proposition 1. *From $\alpha(n)$ above, p, q are both primes. p or q can be written three forms as follows:*

Case 1. *$p = 4n + 3$ and $q = 4n + 3$ forms.*

Case 2. *$p = 4n + 1$ and $q = 4n + 3$ forms.*

Case 3. *$p = 4n + 1$ and $q = 4n + 1$ forms.*

We first consider Case 1.

$$\begin{aligned} (p-1)(q-1) &= (4n+2)(4m+2) \\ &= 4[4mn + 2(m+n) + 1]. \\ (p-2^r)(q-2^r) &= pq - 2^r p - 2^r q + 2^{2r}. \end{aligned}$$

$$\begin{aligned} \alpha(n) &= 4[4mn + 2(m+n) + 1](\frac{p \cdot q}{2^r} - p - q + 2^r) \\ &= \frac{pq4[4mn + 2(m+n) + 1]}{2^{r-2}} \\ &\quad -4(p + q - 2^r)[4mn + 2(m+n) + 1] \end{aligned}$$

since p, q and $[4mn+2(m+n)+1]$ are odd, therefore the product of $p \cdot q \cdot (4mn+2(m+n)+1)$ is also odd. This equation is not divisible by 2^{r-2} where 2^{r-2} is even. And

$$(p + q) - 2^r(4mn + 2(m+n) + 1)$$

is an integer. Thus, while r greater than $2, r \in \mathbb{Z}^+$, the $\alpha(n)$ is not an integer (a solution).

We then discuss Case 2, namely $p = 4n + 1$ and $q = 4m + 3$. Since

$$(p-1)(q-1) = 16mn + 8n = 8n(2m+1),$$

then

$$(p-2^r)(q-2^r) = pq - 2^r p - 2^r q + 2^{2r}.$$

We get

$$\begin{aligned}\alpha(n) &= 8n(2m+1)(\frac{pq}{2^r} - p - q + 2^r) \\ &= \frac{pqn(2m+1)}{2^{r-3}} - 8n(2m+1)(p+q-2^r)\end{aligned}$$

1) If n is odd since p, q, n and $(2m+1)$ are odd, the product of $p \cdot q \cdot n(2m+1)$ is also odd. We obtain

$$8n(2m+1)(p+1)(p+q-2^r)$$

is not divisible by 2^{r-3} if $r > 3$. Therefore, $\alpha(n)$ is not possible an integer.

2) If n is even where $n = a \cdot 2^i, i \in \mathbb{Z}^+$, a is odd. We get

$$\alpha(n) = \frac{p \cdot q \cdot a(2m+1)}{2^{r-i-3}} - 8n(2m+1)(p+q-2^r).$$

Since p, q, a and $(2m+1)$ are odd, the product of $p \cdot q \cdot a \cdot (2m+1)$ is also odd and is not divisible by 2^{r-i-3} when $r > i + 3, i \in \mathbb{Z}^+$.

By above Items 1) and 2), we know the $\alpha(n)$ is not an integer when $r > i + 3, i \in \mathbb{Z}_0^+$.

We keep discussing Case 3, namely $p = 4n + 1$ and $q = 4m + 1$.

$$\begin{aligned}(p-1)(q-1) &= 16mn \\ (p-2^r)(q-2^r) &= pq - 2^r p - 2^r q + 2^{2r} \\ \alpha(n) &= 16mn(\frac{p \cdot q}{2^r}) - p - q + 2^r \\ &= \frac{p \cdot q \cdot m \cdot n}{2^{r-4}} \\ &\quad -16mn(p+q-2^r).\end{aligned}$$

1) If m, n are odd, and p, q are odd, the product of $m \cdot n \cdot p \cdot q$ is odd and is not divisible by 2^{r-4}.

2) We start with $m \cdot n$ is even this is true under following condition m is odd and n is even, or m is even and n is odd.

Suppose

$$m \cdot n = b \cdot 2^j,$$

where b is odd, $j \in \mathbb{Z}^+$. We get

$$\alpha(n) = \frac{b \cdot p \cdot q}{2^{r-j-4}} - 16mn(p+q-2^r),$$

since b, p, q are odd, the product of $b \cdot p \cdot q$ is odd. Therefore it will not be divisible by 2^{r-j-4} when $r > 4 + j, j \in \mathbb{Z}^+$. From above Items 1) and 2), when $r > 4 + j$, $j \in \mathbb{Z}_0^+$, the $\alpha(n)$ is not an integer.

Summary of Cases 1, 2 and 3.

1) $p = 4n + 3$, $q = 4m + 3$, $\alpha(n)$ is not an integer when $r > 2, r \in \mathbb{Z}^+$.

2) $p = 4n + 1$, $q = 4m + 3$, $\alpha(n)$ is not an integer when $r > 3 + j, j \in \mathbb{Z}_0^+$.

3) $p = 4n + 1$, $q = 4m + 1$, $\alpha(n)$ is not an integer when $r > 4 + j, j \in \mathbb{Z}_0^+$.

4 Conclusion

Thangavel and Varalakshmi proposed ISRSAC scheme by RSA modification algorithm. From our comment, $\alpha(n) = \frac{(p-1)(q-1)(p-2^r)(q-2^r)}{2^r}$ where p and q are primes, and $r > 3, r \in \mathbb{Z}^+$, then the $\alpha(n)$ is not a integer. On their scheme, it is not possible to generate the public key e randomly. On other hand, it is also impossible satisfied $e \cdot d \equiv 1 \pmod{\alpha(n)}$ where $1 < e < \alpha(n)$ and $\gcd(e, \alpha(n)) = 1$. Therefore, the ISRSAC algorithm has a certain theoretical defect.

Acknowledgement

The authors would like to thank the anonymous reviewers for their useful comments. This work is partially supported from Neusoft Institute of Guangdong under the project number NUIT2018-001, and school project grant number 2018ZXB09 of Zhaoqing University. This work also partially supported by student innovation training program under the grant number PDJH2018B0579 and PDJH2019B0569.

References

[1] E. Lüy, Z. Y. Karatas, and H. Ergin, "Comment on "An enhanced and secured rsa key generation scheme (ESRKGS)"," *Journal of Information Security and Applications*, vol. 30, pp. 1–2, 2016.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communincation of ACM*, vol. 21, pp. 120–126, Feb. 1978.

[3] M. Thangavel and Varalakshmi P., "Improved secure rsa cryptosystem (ISRSAC) for data confidentiality in cloud," *International Journal of Information Systems and Change Management*, 2018. In press.

[4] M. Thangavel, P. Varalakshmi, Mukund Murrali, and K. Nithya, "An enhanced and secured rsa key generation scheme (ESRKGS)," *Journal of Information Security and Applications*, vol. 20, pp. 3–10, 2015.

Biography

Chenglian Liu received his B.S degree in information management from National Union University in 1992

and the MSc degree in National Defense from National Defense University in 2004. He studied his doctorate course at Royal Holloway, University of London from 2006 to 2009 under the supervised by Chris Mitchell. He is with a distinguished associate professor at Huizhou University since 2014. His research interests are in Information Security, Number Theory and Goldbach's Conjecture so on.

Chieh-Wen Hsu received his B.S degree in department of mathamatics from Tamkang University in 1992 and the Master degree in National Cheng Kung University in 1994. He completed his Ph.D in 2010 in National Kaohsiung University of Science nd Technology in Taiwan. His research interests are in Probability and Statistics , Number Theory and Cryptanalysis so on.