Advances in Engineering and Applied Science Research, ISSN 2617-1023

2021 International Conference on Intelligent Manufacturing Technology and Information Technology

Vol. 11, 2021, pp. 49-53

On the Security of Polynomial Rsa over Finite Field F_p and the New Simulation of Rsa

Dandan Su

Foshan Polytechnic, Foshan, Guandong 528137, China

ABSTRACT. In modern cryptography, the periodic property of polynomial is very important to the security of cryptosystems. RSAI, one of the most famous public key cryptosystems, has been extended to algebraic integer rings and integer matrix rings. In this paper, the factorization of polynomials over finite fields is discussed, and the number of irreducible polynomials and primitive polynomials over finite fields, the judgment of primitive polynomials, and the method of constructing high-order irreducible polynomials by using lower-order irreducible polynomials are given. The simulated RSA public key cryptosystem is improved, and the problem of ciphertext expansion is solved by properly selecting parameters. The security of the improved system is discussed, and a new simulation of RSA is given, which has no ciphertext expansion and is closer to the standard RSA concept.

KEYWORDS: Rsa, Security, Finite field

1. Introduction

Information plays an increasingly important role in modern society, and it has become an important strategic resource for social development. The elliptic curve cryptosystem is a public key cryptosystem based on algebraic curve, which has the characteristics of “short key and high security”. In 1978, Rivest, Shamir and Adleman constructed the famous RSA public key cryptosystem. Over the past 40 years, people have not only made various improvements on it, but also put forward many public key cryptography algorithms based on other difficult problems, including ElGamal cryptosystem, RSA new simulation based on finite fields and elliptic curve cryptosystem [2-3]. For example, Guo et al. [4], Li et al. [5] and He et al. [6] considered the simulation of RSA in algebraic integer ring, especially in general quadratic domain. This simulation is undoubtedly a new contribution to modern cryptography. In this article, we will give the conic simulation of the original SRA system and the improved SRA system. The discussion shows that the original RSA conic simulation can resist the attack of small public key exponent, and the improved RSA conic simulation includes some existing large integer systems.

2. Security of Polynomial Rsa over Finite Field F_p

A class of finite fields composed of residual classes in integer rings, for example, for any prime number p, the residual class ring $E_p = E/(q)$ of module q forms a finite field F_p with p elements. This is a very important finite field, because any field characterized by p must contain a subdomain isomorphic to F_p, so it can be regarded as an extended field. This result is the basis of the classification and construction of finite fields.

If $f(x) \in F_p(x)$ is an irreducible first polynomial of degree n, and a is a root of $f(x)$, then $F_p(a) = F_{k^n}$, $f(x)$ is called the minimal polynomial of a. But a is not necessarily the primitive of F_{k^n}. We call the minimal polynomial whose root is primitive.

Definition 2.1[7] Let $f(x)$ be an irreducible first polynomial of degree n over a finite field F_p. If the root a of $f(x)$ is the primitive element of F_{k^n}, $f(x)$ is called the primitive polynomial in $F_p(x)$.

Definition 2.2[7]: let $f(x) \in F_k(x)$, $f(0) \neq 0$ make

DOI: 10.23977/IMTIT2021012

$$f(x) \mid x^b - 1 \quad (1)$$

The minimum positive integer b is the period or order of polynomial $f(x)$, which is denoted as $\prod(f(x)) = \prod f(x) = b$.

If the number of rational points on an elliptic curve can be given to construct an elliptic curve E/F_p, it can be quickly judged whether it is a non-supersingular elliptic curve. The general algorithm for constructing this elliptic curve E/F_p is given below.

(1)Select a large prime number I so that all prime factors of $\frac{I-1}{2}$ are greater than or equal to S;

(2)Choose $H \in F_p$ so that it is $(\frac{-H}{I}) = 1$, where $(\frac{-H}{I})$ represents Legendre symbol;

(3)Check whether the integers o and z satisfy $4I = o^2 + Hz^2$, and if not, return to the second step;

(4) Let $S = I + 1 - o$ and $\overline{S} = I + 1 + o$ check whether $S = I + 1 - o$ or $\overline{S} = I + 1 + o$ can be divisible by large prime numbers, if not, turn to the second step;

Calculate a class polynomial $P_{H(z')^2}(X)$, which is uniquely determined by $H(z')^2$, z' is an integer and $z' \mid z$, and solve the equation:

$$P_{H(z')^2}(X) \equiv 0 (\bmod p)$$

Let m_0 be a solution of congruence equation $P_{H(z')^2}(X) \equiv 0 (\bmod p)$, and take m_0 as m invariant to construct elliptic curve E/F_p, then its order #E/F_p is equal to S or $\overline{S}$ which can be divisible by large prime numbers. The algorithm ends.

In order to embed the elliptic curve discrete logarithm problem on F_p into the general discrete logarithm problem on field F_p^k, the following formula should hold:

$$p^k \equiv 1 \bmod m$$

The $m = \# E(F_p)$ here.

Theorem 2.3 (Euler Theorem): For any $o \in Z_m$, there are:

$$o^{\gamma(m)} \equiv 1 \bmod m$$

In which $Z_m = \{x \in Z_m \mid \gcd(x, m) = 1\}$ and $\gamma()$ represent Euler functions.

Theorem 2.4 [8] Let RSA modulus $V = pq$ be a positive integer of v bits, $\tau = 1, 0 < \sigma < \delta < 1$. If the high ($\delta - \sigma$) v bits of d are known, and σ and δ satisfy any of the following three relationships

$$\sigma < \frac{5}{6} - \frac{\sqrt{6\delta + 1}}{3} \quad (1)$$

$$\sigma < \frac{4}{15}, \delta \le \frac{10}{15} \qquad (2)$$

$$\sigma < \frac{\delta+1}{3} - \frac{\sqrt{4\sigma^2+3\sigma-1}}{3}, \sigma \ge \frac{10}{15} \qquad (3)$$

There is a polynomial time algorithm that can decompose V.

Theorem 2.5 [8] Let RSA modulus $V = pq$ be a positive integer of v bits, $\tau = 1, 0 < \sigma < \delta < 1$. If the low ($\delta - \sigma$)$v$ bit of d is known, and σ and δ satisfy the following relationship

$$\sigma < \frac{4}{7} - \frac{\sqrt{5\delta+2}}{4}$$

There is a polynomial time algorithm that can decompose V.

Theorem 2.6 [8] Let RSA modulus $V = pq$ be a positive integer with v bits, $\delta = 1, 0 < \sigma < \tau < 1$. If the high ($\delta - \sigma$)$v$ bits of d is known, and σ and δ satisfy the following relationship

$$\sigma < \frac{\tau+3}{5} = \frac{\sqrt{3\tau^2+5\tau-1}}{5}$$

There is a polynomial time algorithm that can decompose V.

In addition to attacking common RSA cryptographic algorithms, based on lattice reduction theory, RSA algorithms with special parameters and special implementations can also be attacked.

3. A New Simulation of RSA

(1)Selecting n different prime numbers $u_1, u_2, \cdots, u_n,\ u_1 < u_2 <, \cdots, < u_n$ (secret) and $k = u_1 u_2, \cdots, u_n$ (public);

(2)Select a polynomial $l(x)$ (open) of degree j whose first coefficient is 1 on the Z ring of whole coefficient, so that there is a decomposition formula on F_{u_1}.

$$l(x) = l_1^{(1)}(x) l_2^{(1)}(x) \cdots l_{k1}^{(1)}(x)$$

Here $l_m^{(1)}(x)$ is an irreducible polynomial $(m = 1 - k_1)$ of degree $h_m^{(1)}$ which is different from each other on F_{u_1}; There is a decomposition formula on F_{u_2}

$$l(x) = l_1^{(2)}(x) l_2^{(2)}(x) \cdots l_{k2}^{(2)}(x)$$

Here, $l_m^{(2)}(x)$ is an irreducible polynomial of degree $h_m^{(2)}$ which is different from each other on F_{u_2}, and $(m = 1 - k_2)$ has a decomposition on F_{u_n}

$$l(x) = l_1^{(n)}(x) l_2^{(n)}(x) \cdots l_{kn}^{(n)}(x)$$

Where $l_m^{(n)}(x)$ is an irreducible polynomial $(m = 1 - k_n)$ of degree $h_m^{(n)}$ different from F_{u_n} on each other.

$$\phi_k(l(x)) = \phi_{u_1}(l(x))\phi_{u_2}(l(x))\cdots\phi_{u_n}(l(x)) = k^h \prod_{m=1}^{k_1}(1-1/u_1^{h_m^{(1)}})\cdots\prod_{m=1}^{k_n}(1-1/u_n^{h_m^{(n)}})$$

Encryption algorithm: let plaintext $(a_{m-1}, a_{m-2}, \cdots, a_0) \in Z_k^m$. Calculation

$$\left\langle (a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_0)^e \right\rangle l(x) = b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots + b_0$$

Here, $\langle f(x) \rangle l(x)$ represents the remainder of polynomial $f(x)$ module $l(x)$, and its coefficient module k, so $(b_{m-1}, b_{m-2}, \cdots, b_0)$

As ciphertext.

Decryption algorithm: known $(b_{m-1}, b_{m-2}, \cdots, b_0) \in Z_k^m$, calculation

$$\left\langle (b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + \cdots + b_0)^e \right\rangle l(x) = a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_0$$

Recover plaintext $(a_{m-1}, a_{m-2}, \cdots, a_0) \in Z_k^m$.

$e_1 = e_2 = e$ is taken from RSAC1, and d_1, d_2 is satisfied by Euclid algorithm

$ed_1 \equiv 1(\mathrm{mod}\,\phi_p(l(x))), \quad 1 < d_1 < \phi_p(l(x))$

$ed_2 \equiv 1(\mathrm{mod}\,\phi_q(l(x))), \quad 1 < d_2 < \phi_q(l(x))$

Theorem 3.1 The improved encryption algorithm is injective.

Proof:

Let $\left\langle (a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_0)^e \right\rangle l(x) = \left\langle (a'_{m-1}x^{m-1} + a'_{m-2}x^{m-2} + \cdots + a'_0)^e \right\rangle l(x)$. At the same time, treat $a_{m-1}, a_{m-2}, \cdots, a_0, a'_{m-1}, a'_{m-2}, \cdots, a'_0$ as the remaining class representative of modulo p and modulo q, respectively, in $F_p(x)$

$$\left\langle (a_{m-1}x^{m-1} + \cdots + a_0)^{ed_1} \right\rangle l(x) = \left\langle (a_{m-1} \right\rangle_p x^{m-1} + \cdots + \left\langle a_0 \right\rangle_p$$

$$\left\langle (a_{m-1}x^{m-1} + \cdots + a_0)^{ed_1} \right\rangle l(x) = \left\langle (a'_{m-1} \right\rangle_p x^{m-1} + \cdots + \left\langle a'_0 \right\rangle_p$$

Therefore, there is $\left\langle a_j \right\rangle_p = \left\langle a'_j \right\rangle_p$ for $j = 0,1,-m-1$, where $\left\langle a_j \right\rangle_p$ is the remainder of module p of a_j. similarly, there is $\left\langle a_j \right\rangle_p = \left\langle a'_j \right\rangle_p$ for $j = 0,1,-m-1$, which can be known from grandson's theorem $(a_{m-1}, a_{m-2}, \cdots, a_0) = (a'_{m-1}, a'_{m-2}, \cdots, a'_0) \in Z_j^m$. therefore, the encryption algorithm is injective.

4. Conclusion

The foundation of establishing elliptic curve cryptosystem over finite field F_p is to choose a good elliptic curve suitable for establishing cryptosystem. Based on the properties of polynomials over finite field, this paper presents a new system in the form of polynomials over finite field, which has higher security.The new simulation of RSA proposed in this paper is a cryptographic system with high security, and it is also easy to implement. Especially, it is convenient to use them to construct key escrow and threshold key escrow schemes. The improved system has no ciphertext expansion, and a new simulation of RSA is proposed. Its security is based on the decomposition of large integers, just like the original system, but whether it is equivalent to the decomposition of large integers is still an unsolved problem.

References

[1] Gong Linming, Li Shundong, Dou Jiawei, et al. RSA encryption scheme against CPA and CCA2 under standard model. Acta Electronica Sinica, No. 8, pp. 1938-1946, 2018.

[2] Gong Linming, Li Shundong, Dou Jiawei, et al. RSA-type Encryption Schemes Against CPA and CCA2 in Standard Model. Acta Electronica Sinica, Vol. 46, No. 8, pp. 1938-1946, 2018.

[3] Ren Yanbing. Integer decomposition and RSA security. Journal of Network and Information Security, Vol. 3, No. 005, pp. 62-69, 2017.

[4] Guo Shengnan, Jiang Xueqin. Research and implementation of RSA-based information security encryption system. Network Security Technology and Application, Vol. 205, No. 01, pp. 35-35, 2018.

[5] Li Yunfei, Liu Jukun, Liu Qing. Security analysis of improved RSA algorithm. Computer Applications and Software, Vol. 35, No. 06, pp. 315-318, 2018.

[6] He Jian, Jiang Lin, Liao Qing, et al. Research on the security of RSA-PKCS#1 encryption algorithm based on JSON. Microcomputer and Application, Vol. 037, No. 001, pp. 25-29, 2018.

[7] Liu Jinhui, Zhang Huanguo, Jia Jianwei, et al. Analysis of HKKS key exchange protocol. Chinese Journal of Computers, Vol. 39, No. 003, pp. 516-528, 2016.

[8] Chen Chunling, Qi Nianqiang, Yu Han. Research and improvement of RSA algorithm. Computer Technology and Development, Vol. 026, No. 008, pp. 48-51, 2016.