Front. Electr. Electron. Eng. China (2006) 3: 287–290
DOI 10.1007/s11460-006-0039-7

RESEARCH ARTICLE

JIANG Zheng-tao, SUN Xi, TIAN Lei, WANG Yu-min

Further research on public-key cryptosystems based on third-order recurrence sequence

Abstract Properties of third-order recurrence sequences were investigated and a new variant of the GH public-key cryptosystem, which was further improved to be a probabilistic public-key cryptosystem, was proposed. Then security analysis of the proposed scheme was provided and it was proved that the one-wayness of the proposed scheme is equivalent to partial discrete logarithm and its semantic security is equivalent to decisional Diffie-Hellman problem in ring extension. Finally, efficiency analysis of the proposed scheme was provided, and that these two encryption schemes need to transfer 2log N and 4log N bits data respectively.

Keywords public-key cryptosystem, third-order linear recurrence sequence, (trapdoor) discrete logarithm, integer factorization

1 Introduction

Since the notion of public-key cryptosystem was introduced by Diffie and Hellman [1], many researchers have deeply investigated this area. Rivest et al. proposed another cryptosystem, the RSA, based on integer factorization [2]. Presently, there is no proof for the equivalence between RSA and integer factorization [3].

Researches on the new intractable problem-based (or equivalent) cryptosystems enrich the theory of cryptography and promote the development of applied cryptography, as well as accelerate deep investigations on the related intractable problems in the area of mathematics. Based on second linear recursive sequences, Smith and Lennon proposed a public-key cryptosystem, the LUC, in 1994 [4]. In 1999 Gong et al. proposed another public-key encryption scheme the GH based on third-order linear feedback shift register sequence (3-LFSR) [5, 6], and they also provided an efficient algorithm to calculate this sequence.

Based on the problem of integer factorization, we attempt to construct another 3-LFSR-based cryptographic scheme, whose encryption/decryption procedures are different from GH. In order to analyze its security, this paper also defined two types of intractable problems, namely discrete logarithm problem based on third order linear recursive sequence (3-RS-DL), partial discrete logarithm problem based on third order linear recursive sequence (3-RS-PDL), and decisional discrete logarithm problem based on third order linear recursive sequence (3-RS-PDH). Similarly, one can present more accurate definitions for the related intractable problems of LUC and GH, which will facilitate the investigations on their security and their security relationships. Finally, it was proved that the one-wayness and semantic security of the proposed schemes are equivalent to 3-RS-PDL and 3-RS-DDH respectively.

Translated from *Journal on Communications*, 2005, 9(26): 9–12 (in Chinese)

JIANG Zheng-tao (✉)
National Key laboratory of Integrated service Networks,
Xidian University, Xi'an 710071, China
Present address: School of Computer Science, Beihang University,
Beijing 100083, China
E-mail: jiangzt@act.buaa.edu.cn

SUN Xi, WANG Yu-min
National Key Laboratory of Integrated Service Networks,
Xidian University, Xi'an 710071, China

TIAN Lei
Vocational College of Qingdao University, Qingdao 266101, China

2 Third order linear recursive sequences

Definition 1 Let the sequence $\overline{s} = \{s_k\}$ satisfy

$$s_j + c_1 s_{j-1} + c_2 s_{j-2} + c_3 s_{j-3} + d = 0, \quad j \geq 3 \tag{1}$$

then $\overline{s} = \{s_k\}$ is called third order recursive sequence.

Let the polynomial

$$f(x) = x^3 - ax^2 + bx - 1 \tag{2}$$

be an irreducible polynomial in $Z[x]$.

According to the Newton formula, if $d=0$, $c_1=-a$, $c_2=b$, $c_3=-1$ and $s_0=3$, $s_1=a$, $s_2=a^2-2b$, then $s_k=\alpha_1^k+\alpha_2^k+\alpha_3^k \quad k=0,1,\cdots$ where $\alpha_1,\alpha_2,\alpha_3$ are the three roots of $f(x)=0$.

In fact, Eq. (1) is

$$s_k=as_{k-1}-bs_{k-2}+s_{k-3}, \quad k=3,4,\cdots \tag{3}$$

where $s_0=3$, $s_1=a$, $s_2=a^2-2b$.

In finite field GF(p), if $f(x)$ in Eq. (2) is irreducible, it is easy to verify that each root of $f(x)=0$ satisfies $\alpha_i^{p^2+p+1}\equiv 1(\mathrm{mod}\ p)$, $i=1,2,3$.

So, $\{s_k\}$ is periodic in GF(p) satisfying

$$s_{p^2+p+1}\equiv 3(\mathrm{mod}\ p) \tag{4}$$

Let $N=n^2=p^2q^2$, where n is RSA modulus, $a,b\in Z_N$, and

$$f(x)=x^3-ax^2+bx-1 \tag{5}$$

is irreducible on Z_p, Z_q.

Let T_1 represent the period of $\overline{s}=\{s_k\}$ in Z_N. Apparently one has $T_1 | n(p^2+p+1)(q^2+q+1)$ (with respect of the security problem, T_1 should be large enough, such as $n(p^2+p+1)(q^2+q+1)=lT_1$, $l=1$ or a small positive integer). Knowing the factorization of n, one can calculate T_1; on the other hand, knowing T_1, one can also factorize n.

In fact, knowing T_1, since l is a small positive integer, one can get $\xi=(p^2+p+1)(q^2+q+1)$. With ξ, one can factorize n as follows:

$$\begin{aligned}\xi&=(p^2+p+1)(q^2+q+1)\\&=p^2q^2+p^2q+p^2+pq^2+pq+q^2+p+q+1\\&=(p+q+\frac{n+1}{2})^2-2pq-\left(\frac{n+1}{2}\right)^2+n^2+n+1\\&=(p+q+\frac{n+1}{2})^2-3n+\frac{3}{4}(n+1)^2\end{aligned}$$

In integer domain one calculates its square roots and gets $\xi_1=p+q$, so p, q are the two roots of the following equation $x^2-\xi_1 x+n=0$. Knowing p, q, one factorized n.

Remark 1 The relation analyzed between the period and the factorization of RSA modulus also applies to security analysis of GH cryptosystem [5, 6].

Let $T=T_1/n$, define the set Γ as follows:

$\Gamma:=\{(s_t, s_{-t})|\gamma\equiv 1 \mathrm{mod}\ n, t\in Z_n^*\}$

where γ is one root of $x^3-s_t x^2+s_{-t}x-1=0$.

L is a function, such that L: $\Gamma\rightarrow Z/n$

$$(s_k, s_{-k})\rightarrow\frac{s_{kT}-3}{n}(\mathrm{mod}\ n)$$

Definition 2 Let $(s_m,s_{-m})\in Z_N\times Z_N$ be the characteristic sequence of Eq. (5), and the problem of extracting $m\mathrm{mod}\ T_1$ from (s_m,s_{-m}) is called discrete logarithm problem based on third-order linear recursive sequences, 3-RS- DL(N). Extracting $m\mathrm{mod}\ n$ from (s_m,s_{-m}) is called partial discrete logarithm problem based on third order linear recursive sequences, 3-RS-PDL(N).

Definition 3 Given the cipher text $(s_{rn+m},s_{-(rn+m)})$, where r is random in Z_n, the problem of deciding whether m equals 1 is called decision of nth residusity problem based on the third order linear recursive sequences, 3-RS-DR$_n$.

Definition 4 For an encryption scheme E and for any pair of plaintexts m_0, m_1, choosing one to encrypt randomly, and get a ciphertext C. Based on the knowledge of m_0, m_1, C and other public parameters, the attacker can not determine which plaintext is corresponding to the ciphertext C in polynomial time, then the encryption scheme E is called semantically secure.

3 Third-order linear recursive sequences

3.1 Scheme description (scheme 1)

Let $m\in Z_n$ be the plaintext to encrypt, the encryption/ decryptioin processes of scheme 1 are as follows:

Public parameters: n, a, b (as in Eq. (5))

Private parameters: p, q

Encryption: $C_1\equiv s_m \mathrm{mod}\ N$, $C_2\equiv s_{-m} \mathrm{mod}\ N$

Ciphertext $C=(C_1, C_2)$

Decryption: $m=\dfrac{L(C_1,C_2)}{L(a,b)} \mathrm{mod}\ n$

3.2 Feasibility analysis

Theorem 1 Applying the decryption procedure of encryption scheme 1, one can extract the corresponding plaintext from ciphertext C.

Proof Since $a,b\in Z_N$, and $s_m=\alpha_1^m+\alpha_2^m+\alpha_3^m \mathrm{mod}\ N$, where $\alpha_1,\alpha_2,\alpha_3$ are the three roots of Eq. (5).

Obviously $\alpha_1^m,\alpha_2^m,\alpha_3^m$ are the three roots of

$$x^3-s_m x^2+s_{-m}x-1=0$$

Therefore,

$$\frac{L(C_1,C_2)}{L(a,b)}\equiv\frac{\dfrac{\alpha_1^{Tm}+\alpha_2^{Tm}+\alpha_3^{Tm}-3}{n}}{\dfrac{\alpha_1^{T}+\alpha_2^{T}+\alpha_3^{T}-3}{n}(\mathrm{mod}\ n)}\equiv m(\mathrm{mod}\ n)$$

3.3 Security analysis

The one-wayness of scheme 1 is the intractability of extracting $m\in Z_n$ from $(s_m,s_{-m})\in Z_N\times Z_N$, one gets the following theorem.

Theorem 2 Encryption scheme 1 is one-way if and only if 3-RS-PDL is intractable.

Since $f(x)$ is irreducible on Z_N, without losing generalization, let α be one of the roots of $f(x)=0$.

Until now, to our knowledge there is no detailed investigation on the partial discrete logarithm problem modulo a composite [7–10]. Among the present methods, the main method to extract the partial discrete logarithm modulo a composite is to factorize the module, calculate the order of $\alpha \bmod N$ or the period of the sequence.

Since the module is commonly RSA module, it is not feasible to extract 3-RS-PDL(N) by factorizing the composite module. The following two propositions briefly investigate the intractability of the other two approaches.

Proposition 1 If there exists an algorithm A, which can solve the problem of 3-RS-DL(N), then using this algorithm one can factorize the RSA modulus n, and attack the encryption scheme successfully.

Proof The attacker chooses a plaintext m such that $m>n(p^2+p+1)(q^2+q+1)$ to encrypt, and get the corresponding ciphertext $(s_m,s_{-m})\in Z_N\times Z_N$ using algorithm A, the attacker get $m_1=m \bmod n(p^2+p+1)(q^2+q+1)$. With these two "pliantexts" m and m_1, the attacker can get a multiple of the period T_1. According to Theorem 1 and the discussion above, the attacker can factorize the modulus n, and thus attack the encryption scheme successfully.

Similarly one gets the following:

Proposition 2 If there is an algorithm A_1, which calculates the period (or multiple period) of sequence $\overline{s}=\{s_k\}$ in Eq. (3), then using this algorithm one can factorize the RSA modulus.

Therefore, with a degree of confidence one cannot attack encryption scheme 1 by solving the problem of 3-RS-DL(N) based on the assumption of intractability of factorization problem.

4 Probabilistic public key encryption scheme based on third-order linear recursive sequences

4.1 Scheme description (scheme 2)

Let $m\in Z_n$ be the plaintext to encrypt. The encryption/ decryptioin processes of scheme 2 are as follows:

Public parameters: n, a, b (as in scheme 1)

Private parameters: p, q

Encryption: one randomly chooses $r\in Z_n$, and calculates

$C_1\equiv s_{rn+m} \bmod N$, $C_2\equiv s_{-(rn+m)} \bmod N$

Ciphertext $C=(C_1, C_2)$

Decryption: $m=\dfrac{L(C_1,C_2)}{L(a,b)} \bmod n$

From Theorem 1, applying the decryption procedure of encryption scheme 2 one can extract the corresponding plaintext from ciphertext C.

4.2 Security analysis

The one-wayness of encryption scheme 2 is exactly the intractability of extracting $m\in Z_n$ from $(s_{rn+m}, s_{-(rn+m)})\in Z_N\times Z_N$; in addition, since encryption scheme 2 includes a blinding parameter, it makes it more difficult for the analyzer to extract $m\in Z_n$. Thus it seems that the one-wayness of encryption scheme 2 is not lower than that of scheme 1.

Theorem 3 Encryption scheme 2 is semantically secure if and only if the problem of 3-RS-DR$_n$ is intractable.

Proof Let m_0 and m_1 be two plaintext, and randomly choose one of them to encrypt and get the ciphertext $(s_{rn+m}, s_{-(rn+m)})$. The analyzer calculates l, such that $lm_1\equiv$ mod n, and further calculates $(s_{(rn+m)l}, s_{-(rn+m)l})$.

In case of $m=m_0$ (similar for $m=m_1$), $(s_{(rn+m)l}, s_{-(rn+m)l})=(s_{r'n+1}, s_{-(r'n+1)})$, encryption scheme 2 is semantically secure if and ,only if the problem of 3-RS-DR$_n$ is intractable.

Remark 2 The one-wayness of encryption scheme is based on the intractability of extracting $m\in Z_n$ from $(s_m, s_{-m})\in Z_N\times Z_N$, while one-wayness of the GH scheme is based on extracting $d\in Z_{\varphi(n)}$ from $(s_d, s_{-d})\in Z_n\times Z_n$. With overwhelming probability, both d and m are smaller than $\varphi(n)$. In case m is smaller than $\varphi(n)$, one can denote both of the above array as $S_m\in Z_N\times Z_N$ and $S_m\in Z_n\times Z_n$ respectively. Obviously, one has $S_m=S_1+S_2n$, with S_1, $S_2\in Z_n\times Z_n$ satisfying $S_1=(s_m,s_{-m}) \bmod n$, $S_2=[(s_m, s_{-m})-(s_m,s_{-m}) \bmod n]/n$. If the GH scheme is insecure, one can extract m from $S_1=(s_m,s_{-m}) \bmod n$, and thus on the contrary, if encryption scheme 1 is not secure, similarly one can calculate S_2 from $S_1=(s_m,s_{-m}) \bmod n$, and thus attack the GH scheme successfully. The difference between one-wayness of encryption scheme 1 and that of GH is the intractability of calculating S_2 from $S_1=(s_m,s_{-m}) \bmod n$. What is exactly the difficulty about this problem needs further investigation.

The data of scheme 1 and 2 needed to be transferred are 2log N and 4log N respectively. Scheme 2 has the property of semantic security, which is guaranteed by a random number r. Brief comparisons with GH are as follows (Table 1).

Table 1 Comparisons of scheme 2 and GH

Encryption scheme	Computation	Transmission	Semantic scurity
GH	$(s_d, s_{-d}) \bmod n$	2 $\|n\|$	0
Scheme 2	$(s_{rn+m}, s_{-(rn+m)}) \bmod N$	4 $\|n\|$	$\|n\|$

Encryption scheme 2 and GH need two LFSR-index calculations over Z_N and Z_n respectively. And in encryption scheme 2, there are $|n|$ bits to guarantee its semantic security.

5 Conclusion remarks

The main motivation is to investigate new methods of constructing encryption schemes based on third order linear recursive sequences. The one-wayness and semantic security of the investigated encryption schemes are equivalent to partial discrete logarithm problem based on the third order linear recursive sequences and decision of the *n*th residusity problem based on the third order linear recursive sequences respectively.

Investigations over the above two new problems are related to the discrete logarithm problems in generic ring extensions including the security analysis of LUC and GH schemes, which will contribute in analyzing the security of Paillier-type cryptosystem as well [10] .

Acknowledgements This study was supported by the National Natural Science Foundation of China (No. 90412011), the Hi-Tech Research and Development Program of China (No. 2002AA143021)

References

1. Diffie W., Hellman M. E., New directions in cryptography, IEEE Transaction on Information Theory, 1976, IT-22(6): 644–654
2. Rivest R., Shamir A., Adleman L., A method for abstaining digital signatures and public-key cryptosystems, Comm. ACM 1978, 21(2): 120 –126
3. Muller S., Muller W. B., The security of public key cryptosystems bosed on integer factorization, Information Security and Privacy: Thiral Australasian Lonference-ACISP'98 LNCS 1438, Spring- Verlag, 1998: 9–23
4. Smith P., Lennon M., LUC: a new public-key system, Proceedings of the IFIP TC11, Ninth International Conference on Information Security: Computer Security, May 12-14, 1993: 103–117
5. Gong G., Harn L., Public-key cryptosystems based on cubic finite field extensions, IEEE Transaction on Information Theory,1999, IT- 45(7): 2601–2605
6. Gong G., Harn L., Wu H. P., The GH public-key cryptosystem, Selected Areas in Cryptography, 2001: 284–300
7. Paillier P., Public-key cryptosystems based on composite degree residuosity classes, Advances in Cryptology-Eurocrypt'99, LNCS 1592, Springer-Verlag, 1999: 223–238
8. Paillier P., Efficient public-key cryptosystem provably secure against active adversaries, Advances in Cryptology-ASIACRYPT'99, LNCS 1716, Springer-Verlag, 1999: 159–179
9. Catalano D., Gennaro R., Graham H., The bit security of Paillier's encryption scheme and its applications, Advances in Cryptology-EUROCRYPTO'01, LNCS 2045, 2001: 229–243
10. Jiang Zheng-tao, Yuan Chun-hua, Xu Wen-li et al., Analysis and improvement of a double-trapdoor encryption scheme, Journal on Communications, 2004, 9(25): 64–69 (in Chinese)