where $s(k)$ is any function such that $1 \leq s(k) \leq k$. Encoding and decoding require

$$T = O(ks(k) + k \log k)$$

bit operations and the area is

$$A = O(s^3(k) + k)$$

memory bits. If, for example, we let $s(k) = \log_2 k$, then the proposed scheme has the same complexity as the codes given in [10] and a redundancy of

$$N(k) - k = 3 \log_2 k + 2.5 \log_2 \log_2 k + O(\log \log \log k)$$

which is slightly better than the redundancy of the method in [10]. But if we allow a little bit more computational effort with $s(k) = k^{1/3}$, then the proposed scheme has a complexity of $T = O(k \cdot k^{1/3})$ and $A = O(k)$, and a redundancy of

$$\begin{aligned} N(k) - k &= (3 - 1/6) \log_2 k + O(\log \log k) \\ &= 2.83 \cdot \log_2 k + O(\log \log k). \end{aligned}$$

This is definitely better than the redundancy of the method in [10]. Finally, note that if the balanced code used in step S1 of the encoding algorithm is optimal (thus requiring approximately $0.5 \log_2 k$ redundant bits) then the redundancy of the proposed code will be

$$N(k) - k = 2.5 \log_2 k + O(\log \log k).$$

Currently, the most efficient way to realize optimal balanced codes is by using an enumerative encoding technique [5], [7, p. 117] which requires $T = O(k^2)$ bit operations and $A = O(k^3)$ bits. Thus at present, the use of optimal balanced codes will result in quite high complexity.

ACKNOWLEDGMENT

The authors wish to thank the anonymous reviewers for their many valuable inputs. The proof of the nonexistence of the systematic q-OSN code with rate greater than $1/2$ was given by Reviewer A.

REFERENCES

[1] S. Al-Bassam and B. Bose, "On balanced codes," *IEEE Trans. Inform. Theory*, vol. 36, pp. 406–408, Mar. 1990.
[2] ——, "Design of efficient balanced codes," *IEEE Trans. Comput.*, vol. 43, pp. 362–365, Mar. 1994.
[3] B. Bose and T. R. N. Rao, "Theory of unidirectional error correcting/detecting codes," *IEEE Trans. Comput.*, vol. C-31, pp. 23–32, June 1982.
[4] B. Bose, "On unordered codes," *IEEE Trans. Comput.*, vol. 40, pp. 125–131, Feb. 1991.
[5] T. M. Cover, "Enumerative source encoding," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 73–77, Jan. 1973.
[6] K. A. S. Immink, "Spectrum shaping with DC^2-constrained channel codes," *Philips J. Res.*, vol. 40, pp. 40–53, 1985.
[7] ——, *Coding Techniques for Digital Recorders.* London, U.K.: Prentice-Hall, 1991.
[8] R. Karabed and P. H. Siegel, "Matched spectral-null codes for partial-response channels," *IEEE Trans. Inform. Theory*, vol. 37, pp. 818–855, May 1991.
[9] D. E. Knuth, "Efficient balanced codes," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 51–53, Jan. 1986.
[10] R. M. Roth, P. H. Siegel, and A. Vardy, "High-order spectral-null codes—Constructions and bounds," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1826–1840, Nov. 1994.
[11] V. Skachek, T. Etzion, and R. M. Roth, "Efficient encoding algorithm for third-order spectral-null codes," *IEEE Trans. Inform. Theory*, vol. 44, pp. 846–851, Mar. 1998.
[12] N. R. Saxena and J. P. Robinson, "Accumulator compression testing," *IEEE Trans. Comput.*, vol. C-35, pp. 317–321, Apr. 1986.
[13] L. G. Tallini, R. M. Capocelli, and B. Bose, "Design of some new efficient balanced codes," *IEEE Trans. Inform. Theory*, vol. 42, pp. 790–802, May 1996.
[14] L. Tallini, "Design of efficient constant weight codes," Ph.D. dissertation, Dep. Comput. Sci., Oregon State Univ., Corvallis, Nov. 1996.
[15] ——, "On efficient m-ary q-th order spectral-null codes," in *Proc. 1998 IEEE Int. Symp. Information Theory*, Aug. 1998, p. 112.
[16] L. G. Tallini and U. Vaccaro, "Efficient m-ary balanced codes," *Discr. Appl. Math.*, vol. 92, no. 1, pp. 17–56, Mar. 1999.

Public-Key Cryptosystems Based on Cubic Finite Field Extensions

Guang Gong and Lein Harn

***Abstract*—The cryptographic properties of third-order linear feedback shift-register (LFSR) sequences over GF(p) are investigated. A fast computational algorithm for evaluating the kth term of a characteristic sequence of order 3 is presented. Based on these properties, a new public-key distribution scheme and an RSA-type encryption algorithm are proposed. Their security, implementation, information rate, and computational cost for the new schemes are discussed.**

***Index Terms*— Characteristic sequence, cubic finite field extension, linear feedback shift-register sequence, public-key exchange scheme, RSA-type encryption.**

I. INTRODUCTION

With the rapid development of Internet applications, information security in today's world is more important than that in any previous eras. Designing cryptosystems that meet requirements of communication bandwidth, information rate, computational speed, and various security strategies has become a very challenging task for researchers.

In the most widely used modern cryptosystems, such as the RSA [18], the Diffie–Hellman public-key distribution scheme [3], the ElGamal cryptosystem [5], and DSS [16], increasing the size of the modulus is necessary in order to strengthen their security.

From the point of the linear feedback shift-register (LFSR) sequences, the exponential function which used in the RSA encryption, the Diffie–Hellman (DH) public-key exchange scheme [3], and the ElGamal digital signature scheme is a first-order LFSR sequence over GF(p) or Z_n, where n is a product of two prime numbers. In the literature, there is another family of public-key cryptosystems similar to RSA, DH, and ElGamal public-key cryptosystems, which

Manuscript received March 8, 1998; revised October 15, 1998.

G. Gong was with the Communication Sciences Institute, University of Southern California, Electrical Engineering Systems, EEB#500, Los Angeles, CA 90089-2565 USA. She is now with the Department of Combinatoris and Optimization, University of Waterloo, Waterloo, Ont., Canada N2L 3G1 (e-mail: ggong@cacr.math.uwaterloo.ca).

L. Harn is with the Department of Computer Networking, University of Missouri–Kansas City, Kansas City, MO 64110-2499 USA (e-mail: harn@cstp.umkc.edu).

Communicated by D. R. Stinson, Associate Editor for Complexity and Cryptography.

Publisher Item Identifier S 0018-9448(99)06026-5.

are called the Dickson polynomial scheme [13]–[15] or LUC [20], [21], respectively. The mathematical function used in this family of the public-key cryptosystems is the second-order LFSR sequence over GF(p) or Z_n with a special initial state. This kind of LFSR sequences are *coset constant* [8]. We will give their definition in Section II. (Note: throughout of this correspondence, we will use the term LFSR sequences over GF(p) or Z_n instead of linear recurring sequences over GF(p) or Z_n, since the term of initial state is related to an LFSR.)

In this correspondence, we will explore to construct public-key cryptosystems by using third-order LFSR sequences over GF(p) or Z_n. First, we will investigate the cryptographic properties of third-order LFSR sequences and propose a fast computational algorithm to evaluate the kth term of a third-order characteristic sequence. Based on these properties, we will construct two public-key cryptographic algorithms. One is a public-key distribution scheme that can reduce the size of the modulus while speeding up the computation. The security is based on the difficulty of solving the discrete logarithm in GF(p^3). Another one is a RSA-type encryption algorithm whose security is based on the difficulty of factoring a large composite integer. We will also discuss their security, implementation, information rate, and computational cost.

For the theory of LFSR sequences, the reader is refereed to [8], [12], and for the fundamental theory of finite fields, see [12].

II. Rhird-Order Characteristic Sequences

Let $F = \mathrm{GF}(p)$, where p is a prime and

$$f(x) = x^3 - ax^2 + bx - 1, \qquad a, b \in F \tag{1}$$

be a polynomial over F. A sequence $\boldsymbol{s} = \{s_k\}$ is said to be a third-order LFSR sequence with a characteristic polynomial $f(x)$ if the elements of s satisfy

$$s_k = as_{k-1} - bs_{k-2} + s_{k-3}, \qquad k \geq 3. \tag{2}$$

If $\boldsymbol{s}$ has the initial state $s_0 = 3$, $s_1 = a$, and $s_2 = a^2 - 2b$, then $\boldsymbol{s} = \{s_k\}$ is called *the characteristic sequence generated by* $f(x)$. We denote s_k as $s_k(a, b)$ or $s_k(f)$, and $\boldsymbol{s}$ as $\boldsymbol{s}(a, b)$ or $\boldsymbol{s}(f)$.

Assume that $\alpha_1, \alpha_2, \alpha_3$ are all three roots of $f(x)$ in the splitting field of $f(x)$ over F. According to Newton's formula, the elements of $\boldsymbol{s}$ can be represented by the symmetric kth-power sum of the roots as follows:

$$s_k = \alpha_1^k + \alpha_2^k + \alpha_3^k, \qquad k = 0, 1, \cdots. \tag{3}$$

Let us denote the period of $f(x)$ as $\mathrm{per}(f)$. Notice that if $f(x)$ is irreducible over F, then the period of $\boldsymbol{s}(f)$ is equal to $\mathrm{per}(f)$.

Lemma 1: Let $f(x) = x^3 - ax^2 + bx - 1$ be a polynomial over F, $\alpha_1, \alpha_2, \alpha_3$ be three roots of $f(x)$ in the splitting field of $f(x)$ over F, and $\boldsymbol{s}$ be the characteristic sequence generated by $f(x)$. Let

$$f_k(x) = \left(x - \alpha_1^k\right)\left(x - \alpha_2^k\right)\left(x - \alpha_3^k\right). \tag{4}$$

i) $f_k(x) = x^3 - s_k(a, b)x^2 + s_{-k}(a, b)x - 1$, where $s_{-k}(a, b) = s_k(b, a)$.
ii) $f(x)$ and $f_k(x)$ have the same period if and only if $(\mathrm{per}(f), k) = 1$.
iii) If $(\mathrm{per}(f), k) = 1$, then $f(x)$ is irreducible over F if and only if $f_k(x)$ is irreducible over F.

Proof: i) It follows from Newton's formula of (3). ii) Note that the minimal polynomials of α_i^k and α_i have the same period if and only if $(\mathrm{per}(f), k) = 1$. Hence $\mathrm{per}(f(x)) = \mathrm{per}(f_k(x))$ if and only if $(\mathrm{per}(f), k) = 1$. iii) It follows from ii).

Remark: Let $f^{-1}(x) = x^3 - bx^2 + ax - 1$. Then $f^{-1}(x)$ is the reciprocal polynomial of $f(x)$ and $\{s_{-k}(a, b)\}$ is the characteristic sequence over F generated by $f^{-1}(x)$. We also call $\{s_{-k}(a, b)\}$ the reciprocal sequence of $\{s_k(a, b)\}$.

Lemma 2: Let $f(x) = x^3 - ax^2 + bx - 1$ be a polynomial over F, and let $\boldsymbol{s}$ be the characteristic sequence generated by $f(x)$. Then for all positive integers k and e

$$s_k(s_e(a, b), s_{-e}(a, b)) = s_{ke}(a, b). \tag{5}$$

Proof: From Lemma 1

$$\begin{aligned} f_e(x) &= (x - \alpha_1^e)(x - \alpha_2^e)(x - \alpha_3^e) \\ &= x^3 - s_e(a, b)x^2 + s_{-e}(a, b)x - 1. \end{aligned} \tag{6}$$

Thus

$$\begin{aligned} s_k(s_e(a, b), s_{-e}(a, b)) &= (\alpha_1^e)^k + (\alpha_2^e)^k + (\alpha_3^e)^k \\ &= \alpha_1^{ek} + \alpha_2^{ek} + \alpha_3^{ek} = s_{ke}(a, b). \end{aligned}$$ Q.E.D.

Note: If we consider a and b as variables in F and k as a fixed integer, then $s_k(a, b)$ and $s_{-k}(a, b)$ are Waring polynomials. From [12, Theorem 7.46], we have the following fact.

Fact 1: Let k be a fixed positive integer. If k satisfies $(k, p^i - 1) = 1$, $i = 1, 2, 3$, then for any $u, \nu \in F$, the system of equations

$$s_k(a, b) = u \quad \text{and} \quad s_{-k}(a, b) = v$$

has a unique solution $(a, b) \in F \times F$. In other words, $s_k(a, b)$ and $s_{-k}(a, b)$ are orthogonal in F in variables a and b.

We denote that $Q = p^2 + p + 1$. A positive integer r is called a *coset leader* modulo Q if r is the smallest integer in the set $\{tp^i \bmod Q | i = 0, 1, 2\}$, where t is a positive integer.

Theorem 1: Let $f(x) = x^3 - ax^2 + bx - 1$ be an irreducible polynomial over F of the period $Q = p^2 + p + 1$ and $\boldsymbol{s} = \{s_k\}$ be the characteristic sequence generated by $f(x)$. Let k and k' be different coset leaders modulo Q, and both k and k' are relatively prime to Q. Then

$$(s_k, s_{-k}) \neq (s_{k'}, s_{-k'}).$$

Proof: If $(s_k, s_{-k}) = (s_{k'}, s_{-k'})$, then

$$\begin{aligned} f_k(x) &= x^3 - s_k x^2 + s_{-k}x - 1 \\ &= x^3 - s_{k'}x^2 + s_{-k'}x - 1 = f_{k'}(x). \end{aligned}$$

Thus $f_k(x)$ also has $\alpha_i^{k'}$, $1 \leq i \leq 3$, as its roots. From Lemma 1, $f_k(x)$ is irreducible over F. Therefore, α_i^k and $\alpha_i^{k'}$ are conjugate of each other. In other words, there exists an integer t, $0 \leq t \leq 2$, such that

$$k' \equiv kp^t \pmod{Q}.$$

This contradicts the fact that k and k' are different coset leaders modulo Q. Q.E.D.

Remark: Lemma 2 and Theorem 1 will play key roles in constructing a public-key distribution scheme, since the former guarantees the commutative property and the later provides a one-to-one correspondence between the private key space and the public key space. Fact 1, together with Lemma 2, will be used to construct an RSA-type encryption scheme.

III. Fast Computational Method

In [7], there is an algorithm to calculate the kth term of any linear recurring sequences. Here we will provide a much more efficient algorithm to calculate the kth term of a third-order characteristic sequence.

Lemma 3: Let $\{s_k\}$ be the third-order reciprocal characteristic sequence over F with the characteristic polynomial $f(x)$, defined by (1), and $\{s_{-k}\}$, its reciprocal sequence. Then for any positive integers n and m

i) $s_{2n} = s_n^2 - 2s_{-n}$, and

ii) $s_n s_m - s_{n-m}s_{-m} = s_{n+m} - s_{n-2m}, \qquad n \neq m.$

Proof: From (2), we have

$$s_{2n} = \alpha_1^{2n} + \alpha_2^{2n} + \alpha_3^{2n} \qquad \text{and} \quad s_n^2 = (\alpha_1^n + \alpha_2^n + \alpha_3^n)^2.$$

Notice that $\alpha_1\alpha_2\alpha_3 = 1$. Then

$$\begin{aligned} s_n^2 &= \alpha_1^{2n} + \alpha_2^{2n} + \alpha_3^{2n} + 2\sum_{1\le i<j\le 3} \alpha_i^n \alpha_j^n \\ &= s_{2n} + 2\sum_{i=1}^{3} \alpha_i^{-n} \\ &= s_{2n} + 2s_{-n} \end{aligned}$$

which gives i). The same argument can be applied to ii). Q.E.D.

Let $k = \sum_{i=0}^{r} k_i 2^{r-i}$ be the binary representation of k, $T_0 = k_0 \neq 0$, and $T_j = k_j + 2T_{j-1}$, $1 \le j \le r$. So, $T_r = k$. From Lemma 3, the recurrence can be described by the following formulas.

For $k_j = 0$

$$s_{T_j-1} = s_{T_{j-1}} s_{T_{j-1}-1} - bs_{-T_{j-1}} + s_{-(T_{j-1}+1)} \tag{7}$$

$$s_{T_j} = s_{T_{j-1}}^2 - 2s_{-T_{j-1}} \tag{8}$$

and

$$s_{T_j+1} = s_{T_{j-1}} s_{T_{j-1}+1} - as_{-T_{j-1}} + s_{-(T_{j-1}-1)}. \tag{9}$$

For $k_j = 1$

$$s_{T_j-1} = s_{T_{j-1}}^2 - 2s_{-T_{j-1}} \tag{10}$$

$$s_{T_j} = s_{T_{j-1}} s_{T_{j-1}+1} - as_{-T_{j-1}} + s_{-(T_{j-1}-1)} \tag{11}$$

$$s_{T_j+1} = s_{T_{j-1}+1}^2 - 2s_{-(T_{j-1}+1)}. \tag{12}$$

Since $\{s_k\}$ and $\{s_{-k}\}$ are symmetric in (7)–(12) and the probability that k_j equals 0 or 1 is $1/2$, therefore, we obtain the following result.

Theorem 2: With the same $f(x)$, $\{s_k\}$, and $\{s_{-k}\}$ as in Lemma 3. Using (7)–(12) to calculate a pair of the kth terms s_k and s_{-k} needs $9 \log k$ modulo p multiplications on average.

Note: This method is much more efficient than the algorithm using modulo polynomial [7]. The algorithm provided in [7] requires $O(\mu(n) \log k)$ arithmetic operations to calculate the kth term of an LFSR sequence of order n over F where $\mu(n)$ is the total number of arithmetic operations required to multiply two polynomials of degree $n-1$. In case of $n = 3$, μ (3) is the total number of multiplications modulo p required to multiply two polynomials of degree 2 over $F(= \mathrm{GF}(p))$ and reduce it by modulo $f(x)$. Notice that multiplying two polynomials of degree 2 over F without reduction by modulo $f(x)$ already requires nine multiplications modulo p. So, by using the algorithm in [7] to calculate the kth term s_k requires at least $9 \log k$ multiplications modulo p. Consequently, the total computational cost for calculating a pair of the kth term s_k and s_{-k} needs at least $18 \log k$ multiplications modulo p.

IV. A Public-Key Distribution Scheme

In this section, we will present a public-key distribution (GH-PKD) scheme that is constructed by a pair of third-order characteristic sequences and discuss its security.

A. GH-PKD Scheme

Key-Generation Phase:

- System public parameters: p is a prime number, and $f(x) = x^3 - ax^2 + bx - 1$ is an irreducible polynomial over $\mathrm{GF}(p)$ with the period $Q = p^2 + p + 1$.
- User Alice selects e that satisfies $0 < e < Q$ and $\gcd(e, Q) = 1$ as her private key. She then computes (s_e, s_{-e}) as her public key from the system public key p and $f(x) = x^3 - ax^2 + bx - 1$.
- User Bob selects r that satisfies that $0 < r < Q$ and $\gcd(r, Q) = 1$ as his private key. He then computes (s_r, s_{-r}) as his public key from the system public key p and $f(x) = x^3 - ax^2 + bx - 1$.

Key-Distribution Phase: (See the bottom of this page.)

According to Lemma 2

$$s_e(s_r, s_{-r}) = s_{er} = s_r(s_e, s_{-e}),$$

and

$$s_{-e}(s_r, s_{-r}) = s_{-er} = s_{-r}(s_e, s_{-e}).$$

Namely, their common key is (s_{er}, s_{-er}).

Example: Let $p = 11$, and $f(x) = x^3 + 4x - 1$ be an irreducible polynomial over $\mathrm{GF}(11)$ of period $133 = 7 \times 19$.

Alice: Selects $e = 9$ as her private key. Her public key is $(s_9, s_{-9}) = (10, 6)$.

Bob: Selects $r = 13$ as private key. His public key is $(s_{13}, s_{-13}) = (7, 1)$.

Key-Distribution Phase:

Alice:

$$s_e(s_r, s_{-r}) = s_9(7, 1) = 8$$

and

$$s_{-e}(s_r, s_{-r}) = s_{-9}(7, 1) = s_{124}(7, 1) = 5.$$

So she obtains the key $(8, 5)$.

Bob:

$$s_r(s_e, s_{-e}) = s_{13}(10, 6) = 8$$

and

$$s_{-13}(10, 6) = s_{120}(10, 6) = 5.$$

He obtains the same key $(8, 5)$ as Alice.

Remark:

i) In the Key-Distribution Phase, this scheme does not involve the system public key $f(x) = x^3 - ax^2 + bx - 1$.

ii) The spaces of the private keys and public keys are the sets consisting of all coset leaders modulo $p^2 + p + 1$ relatively prime to $p^2 + p + 1$ and all irreducible polynomials over $\mathrm{GF}(p)$ of degree 3 with the period $p^2 + p + 1$, respectively. According to Theorem 1, the map $k :\to (s_k, s_{-k})$ from the space of the

Alice		Bob
computing:	$\xrightarrow{(s_e,\, s_{-e})}$	computing:
$s_e(s_r, s_{-r})$ and $s_{-e}(s_r, s_{-r})$	$\xleftarrow{(s_r,\, s_{-r})}$	$s_r(s_e, s_{-e})$ and $s_{-r}(s_e, s_{-e})$

private keys to the space of the public keys is bijective. Thus there will be different public keys corresponding to different private keys in GH-PKD. Moreover, the size of the space of private (or public) keys is $\phi(p^2+p+1)/3$ where $\phi(\cdot)$ is the Euler function.

iii) In each key exchange session, the computational cost for each user is $9\log p$ modulo p multiplications on average.

B. Security of GH-PKD

The security for GH key distribution scheme is based on the difficulty of solving the discrete logarithm in $\mathrm{GF}(p^3)$. If an attacker tries to compute Alice's private key e from her public key (s_e, s_{-e}), a polynomial $f_e(x) = x^3 - s_e x^2 + s_{-e}x - 1$ can be formed. Since $f(x) = x^3 - ax^2 + bx - 1$ is irreducible over F, according to Lemma 1, $f_e(x)$ is also irreducible over F. Assume that α and β are the roots of $f(x)$ and $f_e(x)$ in the extension $\mathrm{GF}(p^3)$ of F, respectively. They then can be derived by solving roots of $f(x) = x^3 - ax^2 + bx - 1$ and $f_e(x) = x^3 - s_e x^2 + s_{-e}x - 1$ in $\mathrm{GF}(p^3)$. Then $\beta = \alpha^e$. As a result, once α and β are known, solving the exponent e is equivalent to solving the discrete logarithm in $\mathrm{GF}(p^3)$. According to [1], [2], [6], [9], and [11], solving the discrete logarithm in $\mathrm{GF}(p^3)$ is much harder than solving discrete logarithm in the $\mathrm{GF}(p)$ for the same p.

V. An RSA-Type Encryption Scheme

In this section, we will propose an RSA-type public-key cryptosystem by using a pair of third-order characteristic sequences over Z_n, which is an integer ring modulo n.

A. An RSA-Type Encryption Algorithm

1) **Public keys**: e and n, where $n = pq$, p and q are primes, and $\gcd(e, p^i - 1) = 1$, $i = 2, 3$.
2) **Private keys** d_i, $1 \le i \le 9$, where d_i's are given by Table I.
3) **Enciphering**: For a message $m = (m_1, m_2)$ where $0 < m_1, m_2 < n$, the sender computes $c_1 = s_e(m_1, m_2)$ and $c_2 = s_{-e}(m_1, m_2)$. The ciphertext $c = (c_1, c_2)$.
4) **Deciphering**: First, the receiver computes three functions (14)–(16) of the ciphers c_1, c_2 in order to choose a proper decryption key d, in the set $\{d_i, 1 \le i \le 9\}$ in Table I. Then he computes $m_1 = s_d(c_1, c_2)$ and $m_2 = s_{-d}(c_1, c_2)$ using the selected key d.

Note that all computations here are performed in Z_n.

Remark: According to Fact 1 and the Chinese Remainder Theorem, the map

$$(m_1, m_2) \to (s_e(m_1, m_2), s_{-e}(m_1, m_2))$$

is a bijective map from the message space to the ciphertext space.

Next we will show how to construct decryption keys. For a third-order characteristic sequence $\boldsymbol{s}$ over $F = \mathrm{GF}(p)$ generated by $f(x) = x^3 - ax^2 + bx - 1$, its period, $\mathrm{per}(\boldsymbol{s})$, may be one of three cases as listed below:

Case 1: $f(x)$ is reducible over $F \Leftrightarrow \mathrm{per}(\boldsymbol{s}) | p - 1$.

Case 2: $f(x) = (x - \alpha) f_1(x)$ where $f_1(x)$ is irreducible over F and $\alpha \in F \Leftrightarrow \mathrm{per}(\boldsymbol{s}) | p^2 - 1$ and $\mathrm{per}(\boldsymbol{s})$ is not a factor of $p - 1$.

Case 3: $f(x)$ is irreducible over $F \Leftrightarrow \mathrm{per}(\boldsymbol{s}) | p^2 + p + 1$.

According to the method for solving a cubic equation in a finite field in [17], substituting $x = y + 3^{-1}a$ into $f(x)$, then

$$f(x) = g(y) = y^3 + C(a, b)y + D(a, b) \tag{13}$$

TABLE I
A Construction for the Deciphering Keys

Condition	Multiplier of the Period	Deciphering Key
$\Gamma(1,p) \wedge \Gamma(1,q)$	$\delta_1 = R_{1,p} \cdot R_{1,q}$	$d_1 e \equiv 1 \pmod{\delta_1}$
$\Gamma(1,p) \wedge \Gamma(2,q)$	$\delta_2 = R_{1,p} \cdot R_{2,q}$	$d_2 e \equiv 1 \pmod{\delta_2}$
$\Gamma(1,p) \wedge \Gamma(3,q)$	$\delta_3 = R_{1,p} \cdot R_{3,q}$	$d_3 e \equiv 1 \pmod{\delta_3}$
$\Gamma(2,p) \wedge \Gamma(1,q)$	$\delta_4 = R_{2,p} \cdot R_{1,q}$	$d_4 e \equiv 1 \pmod{\delta_4}$
$\Gamma(2,p) \wedge \Gamma(2,q)$	$\delta_5 = R_{2,p} \cdot R_{2,q}$	$d_5 e \equiv 1 \pmod{\delta_5}$
$\Gamma(2,p) \wedge \Gamma(3,q)$	$\delta_6 = R_{2,p} \cdot R_{3,q}$	$d_6 e \equiv 1 \pmod{\delta_6}$
$\Gamma(3,p) \wedge \Gamma(1,q)$	$\delta_7 = R_{3,p} \cdot R_{1,q}$	$d_7 e \equiv 1 \pmod{\delta_7}$
$\Gamma(3,p) \wedge \Gamma(2,q)$	$\delta_8 = R_{3,p} \cdot R_{2,q}$	$d_8 e \equiv 1 \pmod{\delta_8}$
$\Gamma(3,p) \wedge \Gamma(3,q)$	$\delta_9 = R_{3,p} \cdot R_{3,q}$	$d_9 e \equiv 1 \pmod{\delta_9}$

where

$$C(a, b) = 3^{-1}a^2 + b$$

and

$$D(a, b) = -2 \cdot 3^{-3}a^3 + 3^{-1}ab - 1. \tag{14}$$

The discriminate of the cubic (14) is defined as

$$\Delta(a, b) = -4C^3(a, b) - 27D^2(a, b). \tag{15}$$

Let $x \in \{p, q\}$,

$$\gamma(a, b) = \left(\frac{-27D(a, b) + \sqrt{-27\Delta(a, b)}}{-27D(a, b) - \sqrt{-27\Delta(a, b)}} \right)^{2N} \tag{16}$$

where $N \in \{(x-1)/6, (x+1)/6\}$, and

$$\left(\frac{i}{x}\right), \text{ the Legendre symbol of an integer } i \text{ with respect to the prime } x. \tag{17}$$

Now we are in a position to give a definition for a logic function $\Gamma(j, x)$, which is related to the ciphertext (c_1, c_2), where $j \in \{1, 2, 3\}$ and $x \in \{p, q\}$.

$\Gamma(1, x)$ is true $\Leftrightarrow \Delta(c_1, c_2) \pmod{x} = 0$ or $\Delta(c_1, c_2) \pmod{x} \neq 0$, $(\Delta(c_1, c_2)/x) = 1$ and $\gamma(c_1, c_2) \pmod{x} = 1$.

$\Leftrightarrow$ Case 1

$\Gamma(2, x)$ is true $\Leftrightarrow \Delta(c_1, c_2) \pmod{x} \neq 0$ and $(\Delta(c_1, c_2)/x) = -1$.

$\Leftrightarrow$ Case 2

$\Gamma(3, x)$ is true $\Leftrightarrow \Delta(c_1, c_2) \pmod{x} \neq 0$, $(\Delta(c_1, c_2)/x) = 1$ and $\gamma(c_1, c_2) \pmod{x} \neq 1$.

$\Leftrightarrow$ Case 3

We denote $R_{1,x} = x - 1$, $R_{2,x} = x^2 - 1$, and $R_{3,x} = x^2 + x + 1$. From Lemma 1, two polynomials $x^3 - m_1 x^2 + m_2 x - 1$ and $x^3 - c_1 x^2 + c_2 x - 1$ have the same period. So the receiver can select a proper deciphering key based on the polynomial constructed by the ciphertext (c_1, c_2). Table I gives the construction of these deciphering keys.

B. Security

It is clear that the security of the scheme is based on the difficulty of factoring a large composite integer.

C. Computational Cost

As in the RSA public-key system, we can choose a small e such that the computational cost for computing the eth terms of the third-order characteristic sequence with $f(x) = x^3 - m_1x^2 + m_2x - 1$ and its reciprocal polynomial is low. For example, by taking $e = 5$, we compute

$$s_0 = 3,\ s_1 = m_1 \quad \text{and} \quad s_2 = m_1 - 2m_2$$
$$s_3 = m_1s_2 - m_2s_1 + s_0$$
$$s_4 = s_2^2 - 2s_{-2} \quad \text{and} \quad s_5 = m_1s_4 - m_2s_3 + s_2.$$

So $c_1 = s_5$. Similarly,

$$s_0 = 3, s_{-1} = m_2 \quad \text{and} \quad s_{-2} = m_2 - 2m_1$$
$$s_{-3} = m_2s_{-2} - m_1s_{-1} + s_0$$
$$s_{-4} = s_{-2}^2 - 2s_2 \quad \text{and} \quad s_{-5} = m_2s_{-4} - m_1s_{-3} + s_{-2}.$$

We get $c_2 = s_{-5}$. Totally, we only need 10 modulo n multiplications for enciphering a $2\log n$-bit message. For deciphering process, first we need to decide a proper deciphering key d, i.e., we need to compute three functions. $\Delta(c_1, c_2) (\mathrm{mod}\, x)$ requires 8 modulo n multiplications. For $(\Delta(c_1, c_2)/x)$ and $\gamma(c_1, c_2) (\mathrm{mod}\, x)$, each of the last two functions requires $1.5 \log p$ modulo p multiplications and $1.5 \log q$ modulo q multiplications, respectively. Second, we need to compute the dth terms of the third-order characteristic sequence with $x^3 - c_1x^2 + c_2x - 1$ and its reciprocal polynomial, which needs $9 \log n$ modulo n multiplications on average. Therefore, the total computational cost in the deciphering process is $12 \log n$ modulo n multiplications on average.

VI. Conclusion and Discussion

As we have shown, we can conclude that the proposed public-key distribution scheme (GH-PKD) and the RSA-type encryption scheme are practical efficient public-key cryptosystems. Especially, GH-PKD is successful in reducing the size of the modulus while speeding up the computation. Note that from current literatures [19], [22], [23], only a few of public-key cryptosystems have been put into practical use.

The method presented here can lead to the construction of public-key cryptosystems by using nth-order characteristic sequences over GF(p) of any degree $n > 3$.

Acknowledgment

The authors wish to thank the referees for their valuable comments and suggestions.

References

[1] L. M. Adleman and J. DeMarrais, "A subexponential algorithm for discrete logarithms over all finite fields," in *Proc. Crypto'93* (Lecture Notes in Computer Science, no. 773). Berlin, Germany: Springer-Verlag, 1994, pp. 147–158.

[2] L. M. Adleman and M. A. Huang, "Function field sieve method for discrete logarithms over finite fields," Dec. 1997, preprint.

[3] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT–22, pp. 644–654, Nov. 1976.

[4] P. Donnelly and G. Grimmett, "On the asymptotic distribution of large prime factors," *J. London Math. Soc. (2)*, vol. 47, pp. 395–404, 1993.

[5] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inform. Theory*, vol. IT- 31, pp. 469–472, July 1985.

[6] ——, "A subexponential-time algorithm for computing discrete logarithms over GF (p^2)," *IEEE Trans. Inform. Theory*, vol. IT–32, 1985.

[7] C. M. Fiduccia, "An efficient formula for linear recurrences," *SIAM J. Comput.*, vol. 14, pp. 106–112, 1985.

[8] S. W. Golomb, *Shift Register Sequences.* Laguna Hills, CA: Aegean Park, 1982.

[9] D. Gordon, "Discrete logarithms in GF (p) suing the number field sieve," *SIAM J. Discr. Math.*, vol. 6, pp. 124–138, 1993.

[10] D. E. Knuth, *The Art of Computer Programming*, vol. 2, *Seminumerical Algorithms.* Reading, MA: Addison-Wesley, 1969.

[11] A. K. Lenstra and H. W. Lenstra, Jr., Eds., *The Development of the Number Field Sieve* (Lecture Notes in Mathematics, no. 1554). Berlin, Germany: Springer-Verlag, 1993.

[12] R. Lidl and H. Niederreiter, "Finite fields," in *Encyclopedia of Mathematics and Its Applications*, vol. 20. Reading, MA: Addison-Wesley, 1983.

[13] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics 65.* New York: Wiley, 1993.

[14] W. B. Müller and W. Nöbauer, "Cryptanalysis of the Dickson-scheme," in *Proc. Eurocrypt'85.* Berlin, Germany: Springer-Verlag, 1986, pp. 71–76.

[15] W. Nöbauer, "Cryptanalysis of a public-key cryptosystem based on Dickson polynomials," *Math. Slovaca*, vol. 38, pp. 309–323, 1989.

[16] NIST, "A proposed federal information processing standard for digital signature standard (DSS)," *Federal Register*, vol. 56, pp. 42980–42982, 1991.

[17] L. Rédei, *Algebra.* Leipzig, Germany: Geest & Portig, 1959; London, U.K.: Pergamon, 1967.

[18] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public key cryptosystems," *ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[19] B. Schneier, *Applied Cryptography*, 2nd ed. New York: Wiley, 1996.

[20] P. Smith, "LUC public-key encryption," *Dr. Dobb's J.*, pp. 44–49, Jan. 1993.

[21] P. Smith and C. Skinner, "A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms," in *Proc. Asiacrypt'94*, Nov. 1994, pp. 298–306.

[22] D. R. Stison, *Cryptography, Theory and Practice.* Boca Raton, FL: CRC, 1995.

[23] W. Stallings, *Network and Internetwork Security Principles and Practice.* New York: IEEE, 1995.