On finite automaton one-key cryptosystems

Tao Renji
Institute of Software,Academia Sinica,Beijing 100080,PRC

Abstract

This paper reviews some works on finite automaton one-key cryptosystems and related topics such as autonomous finite automata and Latin arrays.

It is well known that shift registers are important sequence generators in stream ciphers. But shift registers are merely a special kind of autonomous finite automata. Finite automata were considered as suitable mathematical models of cryptosystems from structural viewpoint long ago [1, 2, 3, 4, 5]. And invertibility theory of finite automata had been used to design one-key, two-key and identity-based cryptosysatems [6, 7, 8, 9, 10, 11, 12, 13, 14, 15]. In this paper we give a survey of some works of ours on finite automaton one-key cryptosystems and related topics such as autonomous finite automata and Latin arrays. In §1 we recite some basic definitions and results in invertibility theory of finite automata. We then in §2 mention two important results on bounded error propagation and feedforward invertibility. In §3 we explain a canonical form for one-key cryptosystems implemented by finite automata without expansion of the plaintext and with bounded propagation of decoding errors. §4 is devoted to Latin arrays. And §5 deals with autonomous finite automata.

1 Basic definitions and results

Recall some definitions. A *finite automaton,* say M, is a quintuple $< X, Y, S, \delta, \lambda >$, where X is a nonempty finite set (the *input alphabet* of M), Y a nonempty finite set (the *output alphabet* of M), S a nonempty finite set (the *state alphabet* of M), $\delta : S \times X \to S$ a single-valued mapping (the *next state function* of M), and $\lambda : S \times X \to Y$ a single-valued mapping (the *output function* of M).

For any set A, by A^* denote the set of all words (finite sequences) over A including the *empty word* ε, and by A^ω the set of all infinite-length words (infinite sequences) over A. Expand the domains of δ and λ to $S \times X^*$ and $S \times (X^* \cup X^\omega)$, respectively, as follows.

$$\begin{aligned} &\delta(s, \varepsilon) = s, \quad && \delta(s, \alpha x) = \delta(\delta(s, \alpha), x), \\ &\lambda(s, \varepsilon) = \varepsilon, \quad && \lambda(s, x\alpha') = \lambda(s, x)\lambda(\delta(s, x), \alpha'), \\ & && s \in S,\ x \in X,\ \alpha \in X^*,\ \alpha' \in X^* \cup X^\omega. \end{aligned}$$

In other words, on an initial state $s(0)$ of M an input sequence $x(0), x(1), \ldots$ of M causes a state sequence $s(0), s(1), \ldots$ of M and an output sequence $y(0), y(1), \ldots$ of M according

to

$$\begin{aligned} s(i+1) &= \delta(s(i), x(i)), \\ y(i) &= \lambda(s(i), x(i)), \\ i &= 0, 1, \ldots. \end{aligned}$$

Let $M =< X, Y, S, \delta, \lambda >$ and $M' =< Y, X, S', \delta', \lambda' >$ be two finite automata, and τ a nonnegative integer.

In his seminal paper [1] D.Huffman introduced the concept of τ-order information-lossless that we call weakly invertible with delay τ. M is said to be *weakly invertible with delay* τ (or *τ-order information-lossless*) if for any s in S and x_i in X, $i = 0, 1, \ldots, \tau$, x_0 can be uniquely determined by s and $\lambda(s, x_0 \ldots x_\tau)$.

M is said to be *weakly invertible* if for any s in S and α in X^ω, α can be uniquely determined by s and $\lambda(s, \alpha)$.

Proposition 1 (a). *If M is weakly invertible with delay τ, then M is weakly invertible.*

(b). *If M is weakly invertible , then there exists a nonnegative integer τ such that M is weakly invertible with delay τ.*

For any states $s \in S$ and $s' \in S'$, if

$$(\forall \alpha)_{X^\omega}(\exists \alpha_0)_{X^*}[\lambda'(s', \lambda(s, \alpha)) = \alpha_0 \alpha \& |\alpha_0| = \tau],$$

then (s', s) is said to be a *match pair with delay* τ or say that s' *τ-matches* s.

M' is said to be a *weak inverse with delay* τ of M if for any s in S there exists s' in S' such that (s', s) is a match pair with delay τ.

Proposition 2 *M is weakly invertible with delay τ if and only if there exists a finite automaton M' such that M' is a weak inverse with delay τ of M.*

In an unpublished paper [16] we introduced the concept of invertible with delay τ which occurs in public literature [17]. M is said to be *invertible with delay* τ if for any s in S and x_i in X, $i = 0, 1, \ldots, \tau$, x_0 can be uniquely determined by $\lambda(s, x_0 \ldots x_\tau)$.

M is said to be *invertible* if for any s in S and α in X^ω, α can be uniquely determined by $\lambda(s, \alpha)$.

Proposition 3 (a). *If M is invertible with delay τ, then M is invertible.*

(b). *If M is invertible , then there exists a nonnegative integer τ such that M is invertible with delay τ.*

M' is said to be an *inverse with delay* τ of M if for any s in S and any s' in S', (s', s) is a match pair with delay τ.

If φ is a mapping from $Y^k \times X^{h+1}$ to Y, and a finite automaton $M =< X, Y, Y^k \times X^h, \delta, \lambda >$ can be defined by

$$y(i) = \varphi(y(i-1), \ldots, y(i-k), x(i), \ldots, x(i-h)), \quad i = 0, 1, \ldots,$$

i.e.,

$$\begin{aligned} \delta(< y_{-1}, \ldots, y_{-k}, x_{-1}, \ldots, x_{-h} >, x_0) &= < y_0, \ldots, y_{-k+1}, x_0, \ldots, x_{-h+1} >, \\ \lambda(< y_{-1}, \ldots, y_{-k}, x_{-1}, \ldots, x_{-h} >, x_0) &= y_0, \\ y_0 &= \varphi(y_{-1}, \ldots, y_{-k}, x_0, x_{-1}, \ldots, x_{-h}), \end{aligned}$$

then M is said to be an (h,k)-*order memory finite automaton*, denoted by M_φ. In case of $k=0$, M_φ is said to be an h-*order input-memory finite automaton* .

Proposition 4 *M is invertible with delay τ if and only if there exists a τ-order input-memory finite automaton M' such that M' is an inverse with delay τ of M, if and only if there exists a finite automaton M' such that M' is an inverse with delay τ of M.*

2 Bounded error propagation and feedforward invertibility

In [18], J.L. Massey and M.K. Sain introduced the concept of feedforward invertible for linear finite automata . For the general case, we introduced the concept of feedforward invertible with delay τ in [7] to pursue the structural character on bounded error propagation .

A finite automaton $M =< X, Y, S, \delta, \lambda >$ is said *autonomous*, if for any $s \in S$ and any $x, x' \in X$, $\delta(s,x) = \delta(s,x')$ and $\lambda(s,x) = \lambda(s,x')$ hold. We use $< Y, S, \delta, \lambda >$ to denote an autonomous finite automaton, where domains of δ and λ are S.

Let $M^* =< Y, X, S^*, \delta^*, \lambda^* >$ be a finite automaton. M^* is said to be a *c-order semi-input-memory finite automaton* if there exists an autonomous finite automaton $M_a =< Y_a, S_a, \delta_a, \lambda_a >$ and a single-valued mapping $f : Y^{c+1} \times \lambda_a(S_a) \to X$ such that

$$\begin{aligned} S^* &= Y^c \times S_a, \\ \delta^*(< y_0, \ldots, y_{c-1}, s >, y_c) &= < y_1, \ldots, y_c, \delta_a(s) >, \\ \lambda^*(< y_0, \ldots, y_{c-1}, s >, y_c) &= f(y_0, \ldots, y_c, \lambda_a(s)). \end{aligned}$$

Denote M^* by $C(M_a, f)$.

A finite automaton M is said to be *feedforward invertible with delay* τ if there exists a finite order semi-input-memory finite automaton M' such that M' is a weak inverse with delay τ of M.

Let $M' =< Y, X, S', \delta', \lambda' >$ be a weak inverse with delay τ of $M =< X, Y, S, \delta, \lambda >$. If there exists a nonnegative integer c such that

$$\begin{aligned} &(\forall s)_S (\exists s')_{S'} [(\ (s', s) \text{ is a match pair with delay } \tau) \& \\ &\quad (\forall \alpha)_{X^\omega} (\forall \beta)_{Y^\omega} (\forall k)_{>0} (\beta =_k \lambda(s,\alpha) \to \lambda'(s',\beta) =_{(k+c)} \lambda'(s', \lambda(s,\alpha)))], \end{aligned}$$

then we say that *propagation of weakly decoding errors of M' for M is bounded*, where $a_0 a_1 \ldots =_n b_0 b_1 \ldots$ means $a_n a_{n+1} \ldots = b_n b_{n+1} \ldots$.

The following Theorem gives a characterization in structure for bounded error propagation [7].

Theorem 1 *A finite automaton M is feedforward invertible with delay τ if and only if there exists a finite automaton M' such that M' is a weak inverse with delay τ of M and the propagation of decoding errors of M' for M is bounded.*

A finite automaton M' is said to be a *feedforward inverse with delay* τ if there exists a finite automaton M such that M' is a feedforward inverse with delay τ of M.

We obtained a characterization for structure of feedforward inverses with small delay [8, 19, 38]. In case of delay free, we have the following [8].

Theorem 2 *Let* $M^* =< Y, X, S^*, \delta^*, \lambda^* >$ *be a c-order semi-input-memory finite automaton* $C(M_a, f)$, *where* $M_a =< Y_a, S_a, \delta_a, \lambda_a >$ *is an autonomous finite automaton,* $f : Y^{c+1} \times \lambda_a(S_a) \to X$ *a single-valued mapping. Let* $\tau \leq c$. *If the cardinal number of* X *is the same as of* Y, *then* M^* *is a feedforward inverse with delay free if and only if there exist* $p_1, \ldots, p_k \in S_a$ *such that* $\delta_a(p_i) = p_{i+1}$, $i = 1, \ldots, k-1$, $\delta_a(p_k) = p_1$, *and the cardinal number of* $f(y_0, \ldots, y_{c-1}, Y, \lambda_a(p_i))$ *is the same as of* X *for any* $i = 1, \ldots, k$ *and any* $y_0, \ldots, y_{c-1} \in Y$.

3 Canonical form for finite automaton one-key cryptosystems

Using Theorem 2, for one-key cryptosystems implemented by finite automata without expansion of the plaintext and with bounded propagation of decoding errors, we give a kind of canonical form as follows [10].

The decoder $M' =< Y, X, S', \delta', \lambda' >$ is a c-order semi-input-memory finite automaton $C(M_a, f)$, where $X = Y$, $M_a =< Y_a, S_a, \delta_a, \lambda_a >$ is an autonomous finite automaton, $f : Y^{c+1} \times \lambda_a(S_a) \to X$ a single-valued mapping such that the cardinal number of $f(y_0, \ldots, y_{c-1}, Y, \lambda_a(s_a))$ is the same as of X for any $s_a \in S_a$ and any $y_0, \ldots, y_{c-1} \in Y$. For any $y_a \in \lambda_a(S_a)$ and any $y_0, \ldots, y_{c-1} \in Y$, define $f_{y_0,\ldots,y_{c-1},y_a} : Y \to X$

$$f_{y_0,\ldots,y_{c-1},y_a}(y_c) = f(y_0, \ldots, y_c, y_a).$$

Clearly, $f_{y_0,\ldots,y_{c-1},y_a}$ is a permutation on Y (or X). Then there exists a single-valued mapping $h : Y^c \times \lambda_a(S_a) \to W$ such that

$$f(y_0, \ldots, y_{c-1}, y_c, y_a) = g^{-1}_{h(y_0,\ldots,y_{c-1},y_a)}(y_c),$$

$$y_a \in \lambda_a(S_a), y_0, \ldots, y_c \in Y$$

for some finite set W and some permutation family $\{g_w^{-1} : Y \to X, w \in W\}$. Fig.1 (b) gives a pictorial form of the decoder M'. For any initial state

$$s'(0) =< y(-1), \ldots, y(-c), s_a(0) >$$

and any input sequence (ciphertext)

$$y(0), \ldots, y(l-1)$$

of M', the output sequence (plaintext) $x(0), \ldots, x(l-1)$ of M' can be computed by

$$\begin{aligned} s_a(i+1) &= \delta_a(s_a(i)), \\ y_a(i) &= \lambda_a(s_a(i)), \\ w(i) &= h(y(i-c), \ldots, y(i-1), y_a(i)), \\ x(i) &= g^{-1}_{w(i)}(y(i)), \\ & \quad i = 0, 1, \ldots, l-1. \end{aligned}$$

Corresponding encoder may be chosen as a finite automaton $M =< X, Y, Y^c \times S_a, \delta, \lambda >$ of which a pictorial form is given by Fig.1 (a), where

$$\begin{aligned}
\delta(< y_{-1}, \ldots, y_{-c}, s_a >, x_0) &= < y_0, y_{-1}, \ldots, y_{-c+1}, \delta_a(s_a) >, \\
\lambda(< y_{-1}, \ldots, y_{-c}, s_a >, x_0) &= y_0, \\
y_0 &= g_{w_0}(x_0), \\
w_0 &= h(y_{-c}, \ldots, y_{-1}, \lambda_a(s_a)), \\
&\quad < y_{-1}, \ldots, y_{-c}, s_a > \in Y^c \times S_a,\ x_0 \in X.
\end{aligned}$$

That is to say, for any initial state $s(0) =< y(-1), \ldots, y(-c), s_a(0) >$ and any input sequence (plaintext) $x(0), \ldots, x(l-1)$ of M, the output sequence (ciphertext) $y(0), \ldots, y(l-1)$ of M can be computed by

$$\begin{aligned}
s_a(i+1) &= \delta_a(s_a(i)), \\
y_a(i) &= \lambda_a(s_a(i)), \\
w(i) &= h(y(i-c), \ldots, y(i-1), y_a(i)), \\
y(i) &= g_{w(i)}(x(i)), \\
&\quad i = 0, 1, \ldots, l-1.
\end{aligned}$$

As a special case ($c = 0$), for one-key cryptosystems implemented by finite automata without expansion of the plaintext and without propagation of decoding errors, the canonical form is as follows [21].

The decoder $M' =< Y, X, S_a, \delta', \lambda' >$ is a 0-order semi-input-memory finite automaton $C(M_a, g^{-1})$, where $X = Y$,

$$\begin{aligned}
\delta'(s_a, y) &= \delta_a(s_a), \\
\lambda'(s_a, y) &= g_w^{-1}(y), \\
w &= \lambda_a(s_a), \\
&\quad s_a \in S_a,\ y \in Y,
\end{aligned}$$

$M_a =< W, S_a, \delta_a, \lambda_a >$ is an autonomous finite automaton, $g_w^{-1} : Y \to X$ is a permutation on Y, $w \in W$, and $g_w^{-1}(y) = g^{-1}(w, y)$. For any initial state $s_a(0)$ and any input sequence (ciphertext) $y(0), \ldots, y(l-1)$ of M', the output sequence (plaintext) $x(0), \ldots, x(l-1)$ of M' can be computed by

$$\begin{aligned}
s_a(i+1) &= \delta_a(s_a(i)), \\
w(i) &= \lambda_a(s_a(i)), \\
x(i) &= g_{w(i)}^{-1}(y(i)), \\
&\quad i = 0, 1, \ldots, l-1.
\end{aligned}$$

Corresponding encoder may be chosen as a finite automaton $M =< X, Y, S_a, \delta, \lambda >$, where $X = Y$,

$$\begin{aligned}
\delta(s_a, x) &= \delta_a(s_a), \\
\lambda(s_a, x) &= g_w(x), \\
w &= \lambda_a(s_a), \\
&\quad s_a \in S_a,\ x \in X.
\end{aligned}$$

That is to say, $M =< X, Y, S_a, \delta, \lambda >$ is also a 0-order semi-input-memory finite automaton $C(M_a, g)$, where $g(w, x) = g_w(x)$. For any initial state $s_a(0)$ and any input sequence (plaintext) $x(0), \ldots, x(l-1)$ of M, the output sequence (ciphertext) $y(0), \ldots, y(l-1)$ of M can be computed by

$$\begin{aligned} s_a(i+1) &= \delta_a(s_a(i)), \\ w(i) &= \lambda_a(s_a(i)), \\ y(i) &= g_{w(i)}(x(i)), \\ & i = 0, 1, \ldots, l-1. \end{aligned}$$

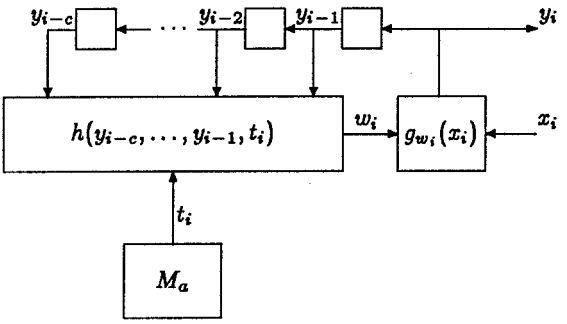

Fig.1 (a). Encoder M

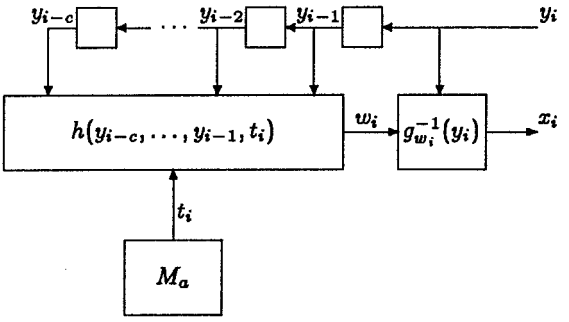

Fig.1 (b). Decoder M'

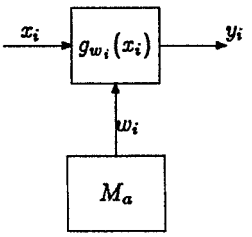

Fig.2 (a). Encoder M

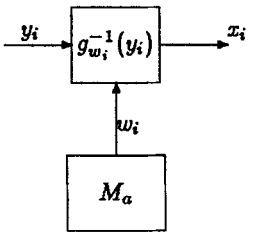

Fig.2 (b). Decoder M'

Block ciphers, rotor ciphers and stream ciphers (in a narrow sense) are special cases of above canonical form. For block ciphers, δ_a is the identity function. For binary stream ciphers , $g_w(x) = w \oplus x$, where $\oplus$ stands for addition modulo two, i.e., exclusive OR.

Example. Let X and Y be 256 bytes. Take $c = 6$. M_a consists of a binary shift register with characteristic polynomial $x^{128} \oplus x^8 \oplus x$ and an autonomous finite automaton with identity next stat function. w_i ranges over 16 bits words. $g_{w_1 w_2}(x) = \varphi(w_1 - (w_2 \oplus (w_1 - \varphi(x))))$, where φ is a permutation on X, and $-$ stands for subtraction modulo 256. The key consists of the initial state of M_a and φ.

4 Latin array

The problem of designing one-key cryptosystems which can be implemented by finite automata without expansion of the plaintext and with bounded propagation of decoding errors lies on choosing suitable parameters such as the size of alphabets and the length c of ciphertext history and designing three components in above canonical form (Fig.1) – an autonomous finite automaton M_a, a transformation h and a permutation family g_w – such that the systems are both efficient and also secure.

For studying the family of permutations used in previous canonical form, we introduced the concept of Latin arrays and investigated their enumeration and generation problems [22, 23].

Let g_w, w in W, be a family of permutations on X. For resisting the known plaintext attack, a natural requirement is to possess the property 1.

Property 1. For any x, y in X , $|\{w|w \text{ in } W, g_w(x) = y\}| = \text{constant}$.

From the viewpoint of uniformity of permutations , it is desirable to have the property 2 additionally.

Property 2. For any w' in W, $|\{w|w \text{ in } W, g_w = g_{w'}\}| = \text{constant}$.

Specify an order for elements of X and of W, say $x_1, \cdots, x_n$ and $w_1, \cdots, w_m$, respectively. Let $A = (a_{ij})$ be an $n \times m$ matrix, where $a_{ij} = g_{w_j}(x_i)$. Then each column of A is a permutation of elements of X. Clearly, fixing orders of elements for X and W, the family of permutations g_w, w in W, is one-one correspondent with A. Corresponding to property 1 and to properties 1–2, we introduced the following concepts.

Let A be an $n \times nk$ matrix on $N = \{1, \cdots, n\}$. If each element of N occurs exactly once in each column of A and k times in each row of A, then A is said to be an (n,k)-*Latin array*.

Let A be an (n,k)-Latin array. If each column of A occurs exactly r times in columns of A repeatedly, then A is said to be an (n,k,r)-*Latin array*.

Latin arrays is a kind of generalization of Latin squares.

Let A and B be $n \times m$ matrices on N. If B can be obtained from A by rearranging rows, rearranging columns and renaming elements, then A and B is said to be *isotopic*.

Clearly, if A is an (n,k)-Latin array and isotopic with B, then B is an (n,k)-Latin array; and if A is an (n,k,r)-Latin array and isotopic with B, then B is an (n,k,r)-Latin array.

For (n,k)-Latin arrays or (n,k,r)-Latin arrays, the equivalence class partitioned by isotopy relation is called *isotopy class*.

By $U(n,k)$ denote the number of all (n,k)-Latin arrays, $U(n,k,r)$ the number of all (n,k,r)-Latin arrays, $I(n,k)$ the number of all isotopy classes of (n,k)-Latin arrays, and $I(n,k,r)$ the number of all isotopy classes of (n,k,r)-Latin arrays. We have [22,23]

Proposition 5 (a). $I(n,k,r) = I(n,k/r,1)$;
(b). $U(n,k,r) = U(n,k/r,1)(nk)!/(nk/r)!(r!)^{nk/r}$.

Proposition 6 *Let* $1 \le k < (n-1)!$. *We then have :*
(a). $I(n,k,1) = I(n,(n-1)!-k,1)$;
(b). $U(n,(n-1)!-k,1) = U(n,k,1)(n!-nk)!/(nk)!$;
(c). $I(n,(n-1)!,1) = 1, U(n,(n-1)!,1) = (n!)!$.

Theorem 3

$$I(2,k) = 1,\ U(2,k) = (2k)!/(k!)^2, \qquad I(2,1,1) = 1,\ U(2,1,1) = 2;$$

$$I(3,1,1) = 1,\ U(3,1,1) = 12,$$

$$I(3,k) = \begin{cases} (k+1)/2 & \text{if } k \text{ is odd} \\ k/2+1 & \text{otherwise,} \end{cases} \qquad U(3,k) = \textstyle\sum_{h=0}^{k} (3k)!/(h!(k-h)!)^3,$$

$$I(4,1) = 2,\ U(4,1) = (4!)^2, \qquad I(4,1,1) = 2,\ U(4,1,1) = (4!)^2,$$

$$I(4,2) = 11,\ U(4,2) = 12640320, \qquad I(4,2,1) = 6,\ U(4,2,1) = 10281600,$$

$$I(4,3) = 46,\ U(4,3) = 805929062400, \qquad I(4,3,1) = 11,\ U(4,3,1) = 306561024000,$$

$$I(4,4) = 201, \qquad U(4,4) = 87285061904040000,$$

$$I(4,4,1) = 6, \qquad U(4,4,1) = 10281600 \times 16!/8!.$$

Among others, some of useful permutation family corresponding to $(2^r, 2^r)$-Latin arrays are $g_{w_1 w_2}(x) = \varphi(w_1 - (w_2 \oplus (w_1 - \varphi(x))))$, $g_{w_1 w_2}(x) = \varphi(w_1 \oplus (w_2 - (w_1 \oplus \varphi(x))))$, $g_{w_1 w_2}(x) = w_1 \oplus \varphi(w_2 - \varphi(w_1 \oplus x))$, $g_{w_1 w_2}(x) = w_1 - \varphi(w_2 \oplus \varphi(w_1 - x))$, etc.. In case of involution φ, such g_w are involutions and corresponds to so-called *involutional Latin arrays*[24].

Example. An m-sequence plus (4,4)-Latin array cipher [25].

In Fig.2, let X and Y be $\{0,1\}^2$. M_a is an m-sequence generator. g_w corresponds to (4,4)-Latin array ($w \in \{0,1\}^4$). The key consists of g_w, M_a and its initial state. Contrary to the case of $g_w(x) = w \oplus x$, this cipher seems secure.

For larger alphabets, we can choose so-called *linear independent Latin array*[26,27] and the initial state of M_a as key.

5 Autonomous finite automata

Autonomous finite automata are considered as sequence generators. For the general case, the set of output sequences of an autonomous finite automaton are consisted of ultimately periodic sequences and closed under translation operation. From mathematical viewpoint, such sets have clearly characterized, although such a characterization is not very useful to cryptology. On the other hand, nonlinear autonomous finite automata can be linearized. So we confine ourself to linear case in this section. Notice that each linear autonomous finite automaton with output dimension 1 is equivalent to a linear shift register. And linear shift registers as a special case of linear autonomous finite automata have been so intensively and extensively studied. Hereafter, we focus our attention on the case of arbitrary output dimension.

Let $M =< Y, S, \delta, \lambda >$ be a linear autonomous finite automaton, where Y and S are column vector space of dimension m and n over $GF(q)$ respectively, $\delta(s) = As$, and $\lambda(s) = Cs$. A and C are referred as the state transition matrix and the output matrix of M respectively, and m, n the structure parameters of M. If the state transition matrix of M is a companion matrix of some monic polynomial over $GF(q)$, then M is said to be a *shift register*.

For any $s \in S$, the infinite output sequence $y_0 y_1 \ldots y_i \ldots\ldots$, where $y_i = \lambda(\delta^i(s))$ for $i \geq 0$, is denoted by $\Phi(s)$, and its z-transformation $\sum_{i=0}^{\infty} y_i z^i$ by $\Phi(s, z)$. Denote $\Phi_M = \{\Phi(s), s \in S\}$ and $\Phi_M(z) = \{\Phi(s, z), s \in S\}$. Clearly, Φ_M and $\Phi_M(z)$ are linear spaces over $GF(q)$ and isomorphic. It is known that for any linear autonomous finite automaton M over $GF(q)$, there exist some linear autonomous shift registers M_i over $GF(q)$, $i = 1, \ldots, h$ such that $\Phi_M = \Phi_{M_1} \oplus \cdots \oplus \Phi_{M_h}$.

We turn on autonomous shift register. Let $M =< Y, S, \delta, \lambda >$ be a linear shift register over $GF(q)$, where A and $C = [c_{ik}]_{m \times n}$ are the state transition matrix and the output matrix of M respectively, and m, n the structure parameters of M.

Consider (generalized) polynomial over $GF(q)$. Let $\psi(z) = \sum_{i=k}^{h} a_i z^i$, where $h \geq k$ are integers, and $a_i \in GF(q)$, $i = h, h+1, \ldots, k$. $\max i[a_i \neq 0]$ is referred as the *high degree* of ψ, and $\min i[a_i \neq 0]$ is referred as the *low degree* of ψ. In case of zero polynomial, its high degree is ∞ and low degree is $-\infty$. For any polynomial ψ and nonzero polynomial φ, there exist uniquely polynomials $q(z)$ and $r(z)$ such that

$$\psi(z) = q(z)\varphi(z) + r(z),$$

$r(z) = 0$ or the low degree of $r(z) \geq$ the low degree of $\varphi(z)$, and $q(z) = 0$ or the high degree of $q(z) < 0$. Denote the unique $r(z)$ by $\mathrm{Res}'(\psi(z), \varphi(z))$.

Let $f(z)$ be the characteristic polynomial of M, i.e., $|zE - A|$. Let

$$c_i(z) = \sum_{k=1}^{n} c_{ik} z^{1-k}, \ i = 1, \ldots, m.$$

$c_i(z), i = 1, \ldots, m$ is said to be the *output polynomials* of M. And

$$f'(z) = f(z) / \gcd(f(z), c_1(z^{-1}), \ldots, c_m(z^{-1}))$$

is said to be the *second characteristic polynomial* of M.

Theorem 4 *Let M be a shift register over $GF(q)$ with structure parameters m, n. Let $f(z)$ be the characteristic polynomial and $c_k(z), k = 1, \ldots, m$ the output polynomials of M, and $g(z) = z^n f(z^{-1})$. Denote the degree of the second characteristic polynomial of M by n'. Then the dimension of $\Phi_M(z)$ is n', and*

$$\rho_k(z) = \begin{bmatrix} \mathrm{Res}'(c_1(z)z^{n-n'+k}, g(z))/g(z) \\ \vdots \\ \mathrm{Res}'(c_m(z)z^{n-n'+k}, g(z))/g(z) \end{bmatrix}, \quad k = 0, 1, \ldots, n'-1$$

is a basis of $\Phi_M(z)$.

This basis is said to be a *polynomial basis* of $\Phi_M(z)$. For any $s \in S$, if $\Phi_M(s, z) = \sum_{k=0}^{n'-1} h'_k \rho_k(z)$ for some $h'_0, \ldots, h'_{n'-1} \in GF(q)$, then $[h'_0, \ldots, h'_{n'-1}]^T$ is said to be the *polynomial coordinate* of $\Phi_M(s, z)$. It can be computed as follows. Denote $f(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0$. Then $\sum_{i=0}^{n'-1} h'_i z^{n'-1-i} = \sum_{i=0}^{n-1} h_i z^{n-1-i} \pmod{f'(z)}$, where

$$\begin{bmatrix} h_0 \\ \vdots \\ h_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & & & \\ a_{n-1} & \ddots & & \\ \vdots & \ddots & \ddots & \\ a_1 & \cdots & a_{n-1} & 1 \end{bmatrix} s.$$

Assume that $GF(q^*)$ is a splitting field of the second characteristic polynomial $f'(z)$ of M. Let M^* be an extension of M over $GF(q^*)$, i.e., A and C are the state transition matrix and the output matrix of M^*, respectively. Let

$$f'(z) = z^{l_0} \prod_{i=1}^{r} f'_i(z)^{l_i} = z^{l_0} \prod_{i=1}^{r} \prod_{j=1}^{n_i} (z - \varepsilon_i^{q^{j-1}})^{l_i}, \tag{1}$$

where $f'_i(z)$ is a monic irreducible polynomial over $GF(q)$ with nonzero constant term, n_i is its degree, $\varepsilon_i \in GF(q^*)$ is its root, $f'_1(z), \ldots, f'_r(z)$ are coprime, and $l_0 \geq 0$, $l_1 > 0$, $\ldots$, $l_r > 0$. Let

$$\begin{aligned} \Gamma_0(z) &= \begin{bmatrix} 1 \\ z \\ \vdots \\ z^{l_0-1} \end{bmatrix}, \\ \Gamma_{ij}(z) &= \begin{bmatrix} 1/(1-\varepsilon_i^{q^{j-1}}z) \\ \vdots \\ 1/(1-\varepsilon_i^{q^{j-1}}z)^{l_i} \end{bmatrix}, \\ i &= 1, \ldots, r, \\ j &= 1, \ldots, n_i. \end{aligned} \tag{2}$$

Then there exist uniquely n' column vectors of dimension m over $GF(q^*)$, R_{0k}, $k = 1, \ldots, l_0$, R_{ijk}, $i = 1, \ldots, r$, $j = 1, \ldots, n_i$, $k = 1, \ldots, l_i$ such that

$$\begin{bmatrix} c_1(z)z^{n-1}/g(z) \\ \vdots \\ c_m(z)z^{n-1}/g(z) \end{bmatrix} = \sum_{k=1}^{l_0} R_{0k} z^{k-1} + \sum_{i=1}^{r} \sum_{j=1}^{n_i} \sum_{k=1}^{l_i} R_{ijk}/(1-\varepsilon_i^{q^{j-1}}z)^k. \tag{3}$$

Theorem 5 *Assume that the second characteristic polynomial $f'(z)$ of the autonomous shift register M has the decomposition as* (1). *Assume that* (3) *holds. Let*

$$R_0(k) = [R_{0(l_0+1-k)} \dots R_{0l_0} 0 \dots 0]_{m \times l_0}, \quad k = 1, \dots l_0,$$

$$R_{ij}(k) = [R_{ij(l_i+1-k)} \dots R_{ijl_i} 0 \dots 0]_{m \times l_i}, \quad i = 1, \dots, r, j = 1, \dots, n_i, k = 1, \dots, l_i.$$

Then $R_0(k)\Gamma_0(k), k = 1, \dots, l_0$, $R_{ij}(k)\Gamma_{ij}(z)$, $i = 1, \dots, r$, $j = 1, \dots, n_i$, $k = 1, \dots, l_i$ is a basis of $\Phi_{M^*}(z)$, where $\Gamma_0(z)$ and $\Gamma_{ij}(z)$ are defined by (2).

This basis is said to be a $(\varepsilon_1, \dots, \varepsilon_r)$ *root basis* of $\Phi_{M^*}(z)$. For any state s of M^*, if there exist $\beta_k \in GF(q^*)$, $k = 0, \dots, l_0$, $\beta_{ijk} \in GF(q^*)$, $i = 1, \dots, r$, $j = 1, \dots, n_i$, $k = 1, \dots, l_i$ such that

$$\Phi_{M^*}(s, z) = \sum_{k=1}^{l_0} \beta_{k-1} R_0(k)\Gamma_0(z) + \sum_{i=1}^{r} \sum_{j=1}^{n_i} \sum_{k=1}^{l_i} \beta_{ijk} R_{ij}(k)\Gamma_{ij}(z),$$

then

$$\beta = [\beta_0, \dots, \beta_{l_0-1}, \beta_{111}, \dots, \beta_{1n_1 1}, \dots, \beta_{11l_1}, \dots, \beta_{1n_1 l_1}, \dots\dots, \beta_{r11}, \dots, \beta_{rn_r 1}, \dots, \beta_{r1l_r}, \dots, \beta_{rn_r l_r}]^T$$

is said to be the $(\varepsilon_1, \dots, \varepsilon_r)$ *root coordinate* of $\Phi_{M^*}(s, z)$.

Notice that if the $(\varepsilon_1, \dots, \varepsilon_r)$ root coordinate of $\Phi_{M^*}(s, z)$ is β, then the τth coefficient of $\Phi_{M^*}(s)$ is

$$\sum_{k=\tau+1}^{l_0} \beta_{l_0+\tau-k} R_{0k} + \sum_{i=1}^{r} \sum_{j=1}^{n_i} \sum_{h=1}^{l_i} \left(\sum_{k=h}^{l_i} \beta_{ij(l_i+h-k)} R_{ijk} \right) \binom{\tau+h-1}{h-1} \varepsilon_i^{\tau q^{j-1}}$$

for $\tau = 0, 1, \dots$.

Theorem 6 *Let $\Omega(z) \in \Phi_{M^*}(z)$. Then $\Omega(z) \in \Phi_M(z)$ if and only if in the $(\varepsilon_1, \dots, \varepsilon_r)$ root coordinate β of $\Omega(z)$, $\beta_k \in GF(q)$, $k = 0, \dots, l_0$, $\beta_{ijk} \in GF(q^{n_i})$ and $\beta_{ijk} = \beta_{ij1}^{q^{j-1}}$, $i = 1, \dots, r$, $j = 1, \dots, n_i$, $k = 1, \dots, l_i$.*

For any nonnegative integer c, the *c-translation* of a infinite sequence $(a_0, a_1, \dots)$ means the infinite sequence $(a_c, a_{c+1}, \dots)$. Correspondingly, $\sum_{i=0}^{\infty} a_{i+c} z^i$ is said to be the *c-translation* of $\sum_{i=0}^{\infty} a_i z^i$.

Theorem 7 *Let β and*

$$\beta' = [\beta'_0, \dots, \beta'_{l_0-1}, \beta'_{111}, \dots, \beta'_{1n_1 1}, \dots, \beta'_{11l_1}, \dots, \beta'_{1n_1 l_1}, \dots\dots, \beta'_{r11}, \dots, \beta'_{rn_r 1}, \dots, \beta'_{r1l_r}, \dots, \beta'_{rn_r l_r}]^T$$

be the $(\varepsilon_1, \dots, \varepsilon_r)$ root coordinate of $\Omega(z)$ and $\Omega'(z)$ in $\Phi_{M^*}(z)$, respectively. Then $\Omega'(z)$ is the c-translation of $\Omega(z)$ if and only if

$$\beta'_k = \beta_{c+k}, \quad k = 0, 1, \dots, l_0 - c - 1,$$
$$\beta'_k = 0, \quad k = l_0 - c, \dots, l_0 - 1,$$
$$\beta'_{ijh} = \sum_{k=h}^{l_i} \binom{k-h+c-1}{k-h} \beta_{ijk} \varepsilon_i^{cq^{j-1}},$$
$$i = 1, \dots, r, j = 1, \dots, n_i, h = 1, \dots, l_i.$$

For the $(\varepsilon_1, \ldots, \varepsilon_r)$ root coordinate β, let $l_{ij} = \min h\ [h \geq 0,\ \beta_{ijk} = 0 \text{ if } h < k \leq l_i],\ i = 1, \ldots, r,\ j = 1, \ldots, n_i.\ \max\{l_{ij},\ i = 1, \ldots, r,\ j = 1, \ldots, n_i\}$ is said to be the *efficient multiplicity* of β. Let the different elements in $\{i |\ \exists j_1 \leq j \leq n_i (l_{ij} > 0),\ 1 \leq i \leq r\}$ are $i_1, \ldots, i_{r_1}$. Denote the order of ε_i by $e_i,\ i = 1, \ldots, r.\ \mathrm{lcm}(e_{i_1}, \ldots, e_{i_{r_1}})$ is said to be the *basic period* of β.

Theorem 8 *Assume that the state transition matrix of M is nonsingular. Then any $\Omega(z) \in \Phi_{M^*}(z)$ is periodic and its period is ep^a, where p is the characteristic of $GF(q)$, e is the basic period of the $(\varepsilon_1, \ldots, \varepsilon_r)$ root coordinate β of $\Omega(z)$, $a = \lceil \log_p l \rceil$ and l is the efficient multiplicity of β.*

Notice that if the $(\varepsilon_1, \ldots, \varepsilon_r)$ root coordinate of a periodic $\Omega(z)$ in $\Phi_M(z)$ is β, then the linear complexity of Ω equals to $\sum_{i=1}^{r} n_i l_{i1}$, where the linear complexity of Ω means the minimal state space dimension of linear shift registers over $GF(q)$ which generate Ω.

The detail proofs of above results are in [6, chapter 3]. Topics on linearization of linear feedback autonomous finite automata and decimation of linear shift register sequences, reader is referred to [6,28].

References

[1] D.A. Huffman, Canonical forms for information-lossless finite-state logical machines, *IRE Trans. on Circuit Theory*, **6**(1959), special supplement, 41–59.

[2] J.E. Savage, Some simple self-synchronizing digital data scrambles, *Bell System Technical J.*, **46**(1967), no.2, 449–487.

[3] F.P. Preparata, Convolutional transformation and recovery of binary sequences, *IEEE Trans. on Computers*, **17**(1968), no.7, 649–655.

[4] S.R. Reddy and M.J. Ashjaee, A class of serial cyphers, in *Proceedings of the 1975 Conference on Information Sciences and Systems*, 396–400.

[5] A. Ecker, Abstrakte Kyptographische Maschinen, *Angewandte Informatik*, 1975, no.5, 201–295.

[6] Tao Renji, *Invertibility of Finite Automata,* Science Press, Beijing, 1979.

[7] Tao Renji, Relationship between bounded error propagation and feedforward invertibility, *Kexue Tongbao*, **27**(1982), no.6, 680–682; Chinese Edition, **27**(1982), no.7, 406–408.

[8] Tao Renji, Some results on the structure of feedforward inverses, *Scientia Sinica* (ser.*A*), **27**(1984), no.2, 157–162; Chinese Edition, **26**(1983), no. 12, 1073–1078.

[9] Chen Shihua and Tao Renji, Invertibility of quasi-linear finite automata, *Advances in Cryptology–CHINACRYPT'92*, 77–86, Science Press, Beijing, 1992.

[10] Tao Renji, Cryptology and mathematics, *Nature Journal*, **7**(1984), no.7, 527–534.

[11] Yan Zhanqing and Zuou Tongheng, The implementation of a FA(finite automaton) cryptosystem, *Computer Research and Development*, **22**(1985), no.3, 29–35, 59.

[12] Qi Yulu,Chen Shihua and Tao Renji, A finite automaton cryptosystem and its software implementation, *International Conference on Computer and Communications Proceedings*, 550–557, Beijing, October 1986.

[13] Tao Renji and Chen Shihua, A finite automaton public key cryptosystem and digital signatures, *Chinese J. of Computers,* **8**(1985),401–409.

[14] Tao Renji and Chen Shihua, Two varieties of finite automaton public key cryptosystem and digital signatures, *J. of Computer Science and Technology,* **1**(1986),9–18.

[15] Tao Renji and Chen Shihua, An implementation of identity-based cryptosystems and signature schemes by finite automaton public key cryptosystems, *Advances in Cryptology–CHINACRYPT'92,* 87–104, Science Press, Beijing, 1992.

[16] Chen Shihua and Tao Renji, On the decision of invertible finite automata with delay τ and τ-inverses, Institute of Computing Technology, Academia Sinica, 1967.

[17] Tao Jen-chi(Tao Renji), Invertible linear finite automata, *Scientia Sinica,* **16**(1973), no.4, 565–581; Chinese Edition, **16**(1973), no.4, 454–467.

[18] J.L. Massey and M.K. Sain, Inverse of linear sequential circuits, *IEEE Trans. on Computer,* **17**(1968), no.4, 330–337.

[19] Zhu Xinjie, On the structure of binary feedforward inverses with delay 2, *J. of Computer Science and Technology,* **4**(1989), no.2, 163–171.

[20] Bao Feng, Some results of self-synchronous invertibility and feedforward inverses, thesis, Institute of Software, Academia Sinica, 1986.

[21] Tao Renji and Chen Shihua, On cryptosystems without error propagation, *Proceedings of the 3rd National Colloquium on Cryptology,* 16–20, Xian, 1988.

[22] Tao Renji and Chen Shihua, Enumeration of Latin arrays (I) – case $n \leq 3$, *Science in China,* ser.*A*, **33**(1990), no.12, 1430–1438; Chinese Edition, ser.*A*, **33**(1990), no.8, 803–809.

[23] Tao Renji and Chen Shihua, Enumeration of Latin arrays (II) – case $n = 4$, $k \leq 4$, *Science in China,* ser.*A*, **34**(1991), no.1, 20–29; Chinese Edition, ser.*A*, **33**(1990), no.9, 930–937.

[24] He Mingqiu, Enumeration of involution Latin arrays, thesis, Institute of Software, Academia Sinica, 1991.

[25] Tao Renji, An application of (4,4)-Latin arrays to cryptography, *Chinese J. of Computers,* **14**(1991), no.6, 423–431.

[26] Tao Renji and Chen Shihua, A generation method for a kind of linear independent Latin arrays, presented at *CHINACRYPT'90,* Beijing, December 1990.

[27] Tao Renji and Chen Shihua, Generation of some linear independent permutations and involutions, presented at *CHINACRYPT'90,* Beijing, December 1990.

[28] Tao Renji, Linear feedback shift register sequences, *Computer Application and Applied Mathematics*, 1975, no.11, 21–51.

[29] Tao Renji, Output sequences of autonomous shift registers, presented at the *Workshop on Pseudo Codes,* Huangshan, July 1977.

[30] Tao Renji, A survey of invertibility of finite automata, presented at the *Workshop on Pseudo Codes,* Huangshan, July 1977.

[31] Tao Renji and Chen Shihua, Some properties on the structure of invertible and inverse finite automata with delay τ, *Chinese J. of Computers*, **3**(1980), no.4, 289–297.

[32] Chen Shihua, On the structure of inverses of a weakly invertible linear finite automaton, *Chinese J. of Computers*, **4**(1981), no.6, 409–419.

[33] Zuou Shanyou, On the weakly invertibility of type I abelian FGHSS, *Chinese J. of Computers*, **5**(1982), no.3, 220–221.

[34] Tao Renji, *Introduction to Automata Theory*, series of computer science, Science Press, Beijing, 1986.

[35] Chen Shihua, On the structure of finite automata of which M' is an (weak) inverse with delay τ, *J. of Computer Science and Technology,* **1**(1986), no.2, 54–59.

[36] Chen Shihua, On the structure of (weak) inverses of an (weakly) invertible finite automaton, *J. of Computer Science and Technology,* **1**(1986), no.3, 92–100.

[37] Chen Shihua and Tao Renji, The structure of weak inverses of a finite automaton with bounded error propagation, *Kexue Tongbao*, **32**(1987), no.10, 713–714; Chinese Edition, **31**(1986), no.20, 1594–1595; full paper in *Advances in Chinese Computer Science*, Vol.**1**, 205–211, World Scientific, Singapore,1988.

[38] Tao Renji, Some mathematical problems in cryptology, *Chinese Quarterly J. of Mathematics*, **2**(1987), no.1, 73–90.

[39] Tao Renji, Invertibility of linear finite automata over a ring, *Automata,Languages and Programming*, Lecture Notes in Computer Science **317**, 489–501, Springer-Verlag, 1988.

[40] Bao Feng, Limited error-propagation, self-synchronization and finite input memory FSM as weak inverses, *Advances in Chinese Computer Science*, Vol.**3**, 1–24, World Scientific, Singapore,1991.

[41] Lü Shuzhi, Some results on the invertibility of linear finite automata over a ring, *Chinese J. of Computers*, **14**(1991), no.8, 570–578.