Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

On the invertibility of finite k-tray automata

Ali Saeidi Rashkolia [1,*], Mohammad Mahdi Zahedi [1], Masoud Hadian Dehkordi [2]

[1]*Department of Mathematics, Graduate University of Advanced Technology, Kerman, Iran*
[2]*School of Mathematics, Iran University of Science and Technology, Tehran, Iran*

ARTICLE INFO

Article history:
Received 7 May 2016
Received in revised form
27 June 2016
Accepted 27 June 2016

Keywords:
Finite k-tray Automaton
k-tray Complex Inverse
k-invertible

ABSTRACT

In this paper a generalization of the notion and the related results of invertibility of finite automata are given. In this regard, first the notion of finite k-tray automata is introduced. Then three different compositions between any two finite k-tray automata are introduced. After that some theorems related to the complex inverse and complex invertible finite k-tray automata are presented.

1. Introduction

Automata theory is a mathematical theory to investigate behavior, structure and their relationship to discrete and digital systems such as algorithms, nerve nets, digital circuits, and so on. The first investigation of automata theory goes back to A. M. Turing in 1936 for the formulation of the informal idea of algorithms. Finite automata model the discrete and digital systems with finite "memory", for example, digital circuits. The theory of finite automata has received considerable attention and found applications in areas of computer, communication, automatic control, and biology, since the pioneering works of Kleene et al. (1956). Among others, autonomous finite automata including shift registers are used to generate pseudo-random sequences, and finite automata with invertibility are used to model encoders and decoders for error correcting and cipher as well as to solve topics in pure mathematics such as the Burnside problem for torsion groups (Tao, 2007; Even, 1965; Kleene, 1956; Kurmit, 1974).

It can be considered as a natural model of cryptosystems. Since up to now, in studying the cryptosystem based on automata, the invertibility of finite automata has a main role, for example in studying the public key cryptosystem FAPKC3 and FAPKC4, we can observe this (Tao et al., 1997; Tao and Chen, 1999). All of these cryptosystems based on invertibility theory of finite automaton, in which their securities rest on the difficulties of inversion of nonlinear finite automata. For more information about the invertibility of finite automata, the reader may be referred to (Tao and Chen, 2000; Bao, 1993; Bao et al., 1996; Chen, 1981; Chen, 1986; Chen and Tao 1987; Chen and Tao, 1992; Dai, 1994; Dai and Ye, 1995; Gao and Bao, 1994; Lu, 1991).

Now in this paper first we introduce the finite k-tray automata, which is a generalization of finite automata, and then we give different compositions between any two finite k-tray automata. After that we present some theorems related to complex inverse finite k-tray automata and complex ivertible finite k-tray automata.

The main purpose of this work is to give the generalization of automata. We will introduce cryptosystems based on this generalization in the future works in which the security is greater than before ones.

2. Preliminaries

As usual, for a finite set X, we denote by X^n the set of words of length n, with $n \in N_0$, and $X^0 = \{\varepsilon\}$, where ε denotes the empty word. We will also use $X^* = \cup_{n\geq 0} X^n$, the set of all finite words, and X^ω will denote the set of infinite words.

Definition 1. (Tao, 2007) *A finite automata is a quintuple* $(X, Y, S, \delta, \lambda)$*, where:*
1. X is a nonempty finite set called the input alphabet of the finite automaton;
2. Y is a nonempty finite set called the output alphabet of the finite automaton;
3. S is a nonempty finite set called the set of states of the finite automaton;
4. δ is a function from $S \times X$ to S called the state transition function of the finite automaton;
5. λ is a function from $S \times X$ to Y called the output function.

* Corresponding Author.
Email Address: a-saeidi@kgut.ac.ir (A.S. Rashkolia), zahedi_mm@kgut.ac.ir (M.M. Zahedi),mhadian@iust.ac.ir (M.H. Dehkordi)

Let $A = (X, Y, S, \delta, \lambda)$ be a finite automaton. The state transition function δ and the output function λ can be extended to words, i.e. elements of $X^{\hat{\mathrm{I}}}$ recursively, as follows:

$$\delta(s, \varepsilon) = s, \delta(s, ||_{i=0}^{n}x_i) = \delta(\delta(s, x_0), ||_{i=1}^{n}x_i), \lambda(s, \varepsilon)$$
$$= \varepsilon, \lambda(s, ||_{i=0}^{n}x_i)$$
$$= \lambda(\delta(s, x_0), ||_{i=1}^{n}x_i),$$

where $s \in S$, $n \in N$ and $||_{i=0}^{n}x_i \in X^{n+1}$, where $||_{i=1}^{n}x_i = x_1x_2 \ldots x_n$. In an analogous way, λ may be extended to X^{ω}.

Definition 2. (Tao, 2007) *Let $A_i = (X_i, Y_i, S_i, \delta_i, \lambda_i)$ for $i = 1,2$ be two finite automata. For any $s_i \in S_i$, $i = 1,2$, s_1 and s_2 are said to be equivalent, denoted by $s_1 : s_2$, if $X_1 = X_2$ and for any $\alpha \in X_1^*$, $\lambda_1(s_1, \alpha) = \lambda_2(s_2, \alpha)$ holds.*

Suppose that k is an integer number and greater than one and $X_1, X_2, \ldots, X_k$ be nonempty finite sets, by $||_{i=1}^{k}X_k$ we mean the cartesian product $X_1 \times X_2 \times \ldots \times X_k = \{(x_1, x_2, \ldots, x_k) | x_i \in X_i, i = 1,2, \ldots, k\}$, and also to simplify the notions we use $||_{i=1}^{k}x_i$ instead of $(x_1, x_2, \ldots, x_k)$.

3. Finite k-tray Automata

Definition 3. *Let $||_{i=1}^{k}X_i$ and $||_{i=1}^{k}Y_i$ be nonempty finite sets. Then a finite automaton $A = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S, \delta, \lambda)$ is called finite k-tray automaton.*

Example 1. *Suppose that S is a set of all n-ary permutations from the set $\{0,1, \ldots, n\}$. Let $X_1 = \{0,1\}$, $X_2 = \{0,1,2\}, \ldots, X_k = \{0,1, \ldots, k\}$, and $Y_1 = Y_2 = \cdots = Y_k = \{0,1\}$ such that:*

$$\delta((p_1p_2 \ldots p_n), (||_{i=1}^{k}x_i))$$
$$= x_1p_2x_3p_4 \ldots x_{k-1}p_kp_{k+1} \ldots p_n,$$
$$\lambda((p_1p_2 \ldots p_n), ||_{i=1}^{k}x_i) = y_1y_2 \ldots y_k,$$
$$y_j = x_j \oplus p_{n-j+1},$$
$$j = 1,2, \ldots, k,$$

where $k \leq n$ and " $\oplus$ " denotes the XOR operation, i.e., componentwise addition modulo 2. Then $(||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S, \delta, \lambda)$ is a finite k-tray automaton.

Definition 4. *Let $A_1 = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Z_i, S_1, \delta_1, \lambda_1)$ and $A_2 = (||_{i=1}^{k}Z_i, ||_{i=1}^{k}Y_i, S_2, \delta_2, \lambda_2)$ be two finite k-tray automata and suppose that $A = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S_1 \times S_2, \delta, \lambda)$, where*

$$\delta((s_1, s_2), ||_{i=1}^{k}x_i)$$
$$= (\delta_1(s_1, ||_{i=1}^{k}x_i), \delta_2(s_2, \lambda_1(s_1, ||_{i=1}^{k}x_i))),$$
$$\lambda((s_1, s_2), ||_{i=1}^{k}x_i) = \lambda_2(s_2, \lambda_1(s_1, ||_{i=1}^{k}x_i)), s_1 \in S, s_2$$
$$\in S_2.$$

Then A is called the k-superposition of A_1 and A_2. We use $C_{\ k}(A_1, A_2)$ to denote the k-superposition of A_1 and A_2.

Definition 5. *Suppose that f_k be a single-valued mapping from $(||_{i=1}^{k}Y_i)^r \times (||_{i=1}^{k}X_i)^{t+1}$ to $||_{i=1}^{k}Y_i$, where t and r are nonnegative integers. Then we mean A_{f_k} to denote a finite automaton defined by:*

$$||_{j=1}^{k}y_i^j = f(||_{j=1}^{r}||_{p=1}^{k}y_{i-j}^{p}, ||_{j=0}^{t}||_{p=1}^{k}x_{i-j}^{p}), i = 0,1, \ldots .$$

More precisely,

$$A_{f_k} = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, (||_{i=1}^{k}Y_i)^r \times (||_{i=1}^{k}X_i)^t, \delta, \lambda),$$

where

$$\delta((||_{j=1}^{k}y_{-1}^{j}, \ldots, ||_{j=1}^{k}y_{-r}^{j}, ||_{j=1}^{k}x_{-1}^{j}, \ldots, ||_{j=1}^{k}x_{-t}^{j}), ||_{j=1}^{k}x_0)$$
$$= (||_{j=1}^{k}y_0^j, ||_{j=1}^{k}y_{-1}^{j}, \ldots, ||_{j=1}^{k}y_{-r+1}^{j},$$
$$||_{j=1}^{k}x_0^j, ||_{j=1}^{k}x_{-1}^{j}, \ldots, ||_{j=1}^{k}x_{-t+1}^{j}),$$

$$\lambda((||_{j=1}^{k}y_{-1}^{j}, \ldots, ||_{j=1}^{k}y_{-r}^{j}, ||_{j=1}^{k}x_{-1}^{j}, \ldots, ||_{j=1}^{k}x_{-t}^{j}), ||_{j=1}^{k}x_0) = ||_{j=1}^{k}y_0^j$$

and

$$||_{j=1}^{k}y_0^j = f(||_{j=1}^{k}y_{-1}^{j}, \ldots, ||_{j=1}^{k}y_{-r}^{j}, ||_{j=1}^{k}x_0^j, ||_{j=1}^{k}x_{-1}^{j}, \ldots, ||_{j=1}^{k}x_{-t}^{j}).$$

A_{f_k} is called the (t, r)-order memory finite k-tray automaton determined by f_k. If $r = 0$, then A_{f_k} is called the t-order input memory finite k-tray automaton determined byf_k.

Definition 6. *Let f_k be a single-valued mapping from $(||_{i=1}^{k}X_i)^{t+1}$ to $||_{i=1}^{k}Y_i$ and g_k be a single-valued mapping from $(||_{i=1}^{k}Z_i)^r \times (||_{i=1}^{k}Y_i)^{P+1}$ to $||_{i=1}^{k}Z_i$ and*

$A_{f_k} = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, (||_{i=1}^{k}X_i)^t, \delta_{f_k}, \lambda_{f_k})$ a t-order input memory finite k-tray automaton determined by f_k and $A_{g_k} = (||_{i=1}^{k}Y_i, ||_{i=1}^{k}Z_i, (||_{i=1}^{k}Z_i)^r \times (||_{i=1}^{k}Y_i)^p, \delta_{g_k}, \lambda_{g_k})$ a $(p,\ r)$-order memory finite k-tray automata determined by g_k and also suppose that

$$A' =$$
$$(||_{i=1}^{k}X_i, ||_{i=1}^{k}Z_i, (||_{i=1}^{k}Z_i)^r \times (||_{i=1}^{k}X_i)^{p+t}, \delta', \lambda'),$$

where

$$\delta'((||_{i=1}^{k}z_{-1}^{i}, \ldots, ||_{i=1}^{k}z_{-r}^{i}, ||_{i=1}^{k}x_{-1}^{i}, \ldots, ||_{i=1}^{k}x_{-p-t}^{i}), ||_{i=1}^{k}x_0^i)$$
$$=$$
$$(||_{i=1}^{k}z_0^i, \ldots, ||_{i=1}^{k}z_{-r+1}^{i}, \ldots, ||_{i=1}^{k}x_0^i, \ldots, ||_{i=1}^{k}x_{-p-t+1}^{i}),$$

$$\lambda'((||_{i=1}^{k}z_{-1}^{i}, \ldots, ||_{i=1}^{k}z_{-r}^{i}, ||_{i=1}^{k}x_{-1}^{i}, \ldots, ||_{i=1}^{k}x_{-p-t}^{i}), ||_{i=1}^{k}x_0^i) = ||_{i=1}^{k}z_0^i$$

and

$$||_{i=1}^{k}z_0^i =$$
$$g_k(||_{i=1}^{k}z_{-1}^{i}, \ldots, ||_{i=1}^{k}z_{-r}^{i}, f(||_{i=1}^{k}x_0^i, \ldots, ||_{i=1}^{k}x_{-t}^{i}), \ldots,$$
$$f(||_{i=1}^{k}x_{-p}^{i}, \ldots, ||_{i=1}^{k}x_{-p-t}^{i})).$$

Then A' is called the k-combination of A_{f_k}, A_{g_k}. We use $C'_k(A_{f_k}, A_{g_k})$ to denote the k-combination of A_{f_k} and A_{g_k}.

Definition 7. *A finite k-tray automaton* $A = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S, \delta, \lambda)$ *is said to be k-invertible with delay t, where t being a nonnegative integer, if for any s in S and any* $||_{j=1}^{k}x_i^j$ *in* $||_{r=1}^{k}X_r$, $i = 0, \ldots, t$, $||_{j=1}^{k}x_0^j$ *can be uniquely determined by* $\lambda(s, ||_{i=0}^{t}||_{j=1}^{k}x_i^j)$, *that is, for any* s, s' *in S and any* $||_{j=1}^{k}x_i^j, ||_{j=1}^{k}{x_i'}^j$ *in* $||_{r=1}^{k}X_r$,
$i = 0, \ldots, t, \lambda(s, ||_{i=0}^{t}||_{j=1}^{k}x_i^j) = \lambda(s', ||_{i=0}^{t}||_{j=1}^{k}{x_i'}^j)$,
gives $x_0^j = {x_0'}^j$, $j = 1, \ldots, k$.

Definition 8. *A finite k-tray automaton* $A = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S, \delta, \lambda)$ *is said to be weakly k-invertible with delay t, t being a nonnegative integer, if for any s in S and any* $||_{j=1}^{k}x_i^j$ *in* $||_{r=1}^{k}X_r$, $i = 0, \ldots, t$, $||_{j=1}^{k}x_0^j$ *can be uniquely determined by s and* $\lambda(s, ||_{i=0}^{t}||_{j=1}^{k}x_i^j)$, *that is, for any s in S and any* $||_{j=1}^{k}x_i^j, ||_{j=1}^{k}{x_i'}^j$ *in* $||_{r=1}^{k}X_r$,
$i = 0, \ldots, t, \lambda(s, ||_{i=0}^{t}||_{j=1}^{k}x_i^j) = \lambda(s, ||_{i=0}^{t}||_{j=1}^{k}{x_i'}^j)$,
implies that $x_0^j = {x_0'}^j$, $j = 1, \ldots, k$.

Definition 9. *Let* $A = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S, \delta, \lambda)$ *and* $A' = (||_{i=1}^{k}Y_i, ||_{i=1}^{k}X_i, S', \delta', \lambda')$ *be two finite k-tray automata, and t be a nonnegative integer. Then if for any pair* $(s', s) \in S' \times S$ *and for any* β *in* $(||_{i=1}^{k}X_i)^{\omega}$ *there exists* β_0 *in* $(||_{i=1}^{k}X_i)^{*}$ *such that* $|\beta_0| = kt$, $\lambda'(s', \lambda(s, \beta)) = \beta_0\beta$, *then* (s', s) *is called a k-tray match pair with delay t.*

Definition 10. *Let* $A = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S, \delta, \lambda)$ *and* $A' = (||_{i=1}^{k}Y_i, ||_{i=1}^{k}X_i, S', \delta', \lambda')$ *be two finite k-tray automata. A′ is called a k-tray weak inverse whit delay t of A, if for any* $s \in S$ *there exists* $s' \in S'$ *such that* (s', s) *is k-tray match pair with delay t.*

Definitions 3-10 are extension of compliments in (Tao, 2007), and also the assumption of $k = 1$.

Theorem 1. *If A is weakly k-invertible with delay t, then there exist a finite k-tray automaton A′ such that it is k-tray weak inverse whit delay t of A.*

Proof. Since for $k = 1$, this theorem coincides completely with Theorem 1.4.4. of [1], so that proof is similar to the proof of that theorem, by imposing the suitable change.

Definition 11. *Let* $U_1, \ldots, U_k$ *be non empty finite sets, and* $\alpha = ||_{j=1}^{k}u_{1j}||_{j=1}^{k}u_{2j} \ldots ||_{j=1}^{k}u_{nj} \ldots$ in $(||_{i=1}^{k}U_i)^{\omega}$. The member $\beta = ||_{j=k}^{1}u_{1j}||_{j=k}^{1}u_{2j} \ \ldots ||_{j=k}^{1}u_{nj} \ldots$ of $(||_{i=k}^{1}U_i)^{\omega}$ is said to be the k-tray complex of α and is denoted by $\beta = \ k - TC\ (\alpha)$.

Definition 12. *Let* $A = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S, \delta, \lambda)$ *and* $A' = (||_{i=1}^{k}Y_i, ||_{i=k}^{1}X_i, S', \delta', \lambda')$ *be two finite k-tray automata, and t be a nonnegative integer. Then if for any pair* $(s', s) \in S' \times S$ *and for any* θ *in* $(||_{i=1}^{k}X_i)^{\omega}$ *there exists* θ_0 *in* $(||_{i=1}^{k}X_i)^{*}$ *such that* $|\theta_0| = kt$, $\lambda'(s', \lambda(s, \theta)) = (\ k - TC\ (\theta_0))(\ k - TC\ (\theta))$,\$ *then* (s', s) *is called a k-tray complex match pair with delay t.*

Definition 13. *Let* $A = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S, \delta, \lambda)$ *and* $A' = (||_{i=1}^{k}Y_i, ||_{i=k}^{1}X_i, S', \delta', \lambda')$, *if for any* (s, s') *in* $S \times S'$, (s', s) *be a k-tray complex match pair with delay t. Then A′ is called a k-tray complex inverse with delay t of A,*

Definition 14. *Let* $A = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S, \delta, \lambda)$ *and* $A' = (||_{i=1}^{k}Y_i, ||_{i=k}^{1}X_i, S', \delta', \lambda')$, *if for any s in S there exists s′ in S′, such that* (s', s) *is a k-tray complex match pair with delay t, Then A′ is called a weak k-tray complex inverse with delay t of A.*

Theorem 2. *Suppose that A be a finite k-tray automaton. If A is k-invertible with delay t, then there exists a t-order input-memory finite k-tray automaton A′ such that it is a k-tray complex inverse with delay t of A.*

Proof. Assume that $A = (||_{i=1}^{k}X_i, ||_{i=1}^{k}Y_i, S, \delta, \lambda)$ be k-tray invertible with delay t. We define a single-valued mapping f_k from $(||_{i=1}^{k})^{t+1}$ to $||_{i=k}^{1}X_i$ as follows.

For $s \in S$ and $||_{j=1}^{k}x_0^j, \ldots, ||_{j=1}^{k}x_t^j$ *in* $||_{i=1}^{k}X_i$ if $\lambda(s, ||_{i=0}^{t}||_{j=1}^{k}x_i^j) = ||_{i=0}^{t}||_{j=1}^{k}y_i^j$, then

$f_k(||_{j=1}^{k}y_t^j, \ldots, ||_{j=1}^{k}y_0^j) = ||_{j=k}^{1}x_0^j$. Since A is k-tray invertible with delay t, thus $||_{j=1}^{k}x_0^j$ can be uniquely determined by $\lambda(s, ||_{i=0}^{t}||_{j=1}^{k}x_i^j)$, hence f_k is well define.

Let $A' = (||_{i=1}^{k}Y_i, ||_{i=k}^{1}X_i, (||_{i=1}^{k}Y_i)^t, \delta', \lambda')$ be the t-order input-memory finite k-tray automaton A_{f_k}. For any $s \in S$ and $s' = (||_{j=1}^{k}y_{-1}^j, ||_{j=1}^{k}y_{-2}^j, \ldots, ||_{j=1}^{k}y_{-t}^j)$ in $(||_{i=1}^{k}Y_i)^t$, let $\lambda(s, ||_{i=0}^{\infty}||_{j=1}^{k}x_i^j) = ||_{i=0}^{\infty}||_{j=1}^{k}y_i^j$. Now we have:

1. $\lambda'(s', ||_{j=1}^{k}y_0^j) = f_k(||_{j=1}^{k}y_0^j, ||_{j=1}^{k}y_{-1}^j, \ldots, ||_{j=1}^{k}y_{-t}^j) = ||_{j=k}^{1}x_{-t}^j$,
2. $\lambda'\big(\delta'(s', ||_{j=1}^{k}y_0^j), ||_{j=1}^{k}y_1^j\big) =$
$\lambda'((||_{j=1}^{k}y_0^j, ||_{j=1}^{k}y_{-1}^j, \ldots, ||_{j=1}^{k}y_{-t+1}^j), ||_{j=1}^{k}y_1^j)$
$= f_k(||_{j=1}^{k}y_1^j, ||_{j=1}^{k}y_0^j, \ldots, ||_{j=1}^{k}y_{-t+1}^j) =$
$||_{j=k}^{1}x_{-t+1}^j, \ldots,$
3. $\lambda'\big(\delta'(s', ||_{i=0}^{t-1}||_{j=1}^{k}y_i^j), ||_{j=1}^{k}y_t^j\big) =$
$\lambda'((||_{j=1}^{k}y_{t-1}^j, ||_{j=1}^{k}y_{t-2}^j, \ldots, ||_{j=1}^{k}y_0^j), ||_{j=1}^{k}y_t^j)$
$= f(||_{j=1}^{k}y_t^j, ||_{j=1}^{k}y_{t-1}^j, \ldots, ||_{j=1}^{k}y_0^j) = ||_{j=k}^{1}x_0^j$,
4. $\lambda'\big(\delta'(s', ||_{i=0}^{t}||_{j=1}^{k}y_i^j), ||_{j=1}^{k}y_{t+1}^j\big) =$
$\lambda'((||_{j=1}^{k}y_t^j, ||_{j=1}^{k}y_{t-1}^j, \ldots, ||_{j=1}^{k}y_1^j), ||_{j=1}^{k}y_{t+1}^j) =$
$f_k(||_{j=1}^{k}y_{t+1}^j, ||_{j=1}^{k}y_t^j, \ldots, ||_{j=1}^{k}y_1^j) = ||_{j=k}^{1}x_1^j \ , \ldots$.

Consequently,

$\lambda'(s',\lambda(s,\|_{i=0}^{\infty}\|_{j=1}^{k}x_i^j)) = \|_{i=-t}^{\infty}\|_{j=k}^{1}x_i^j$. Therefore for all $s \in S$, $s' \in (\|_{i=1}^{k}Y_i)^t, (s', s)$ is k-tray complex mach pair with delay t.

Corollary 1. Suppose that A be a finite k-tray automaton. Then A is k-invertible with delay t if and only if there exists a finite k-tray automaton A′ such that it is a k-tray complex inverse with delay t of A.

Theorem 3. Let A be a finite k-tray automaton. If A is weakly k-invertible with delay t, then there exists a finite k-tray automaton A′ such that it is a weak k-tray complex inverse with delay t of A.

Proof. Assume that $A = (\|_{i=1}^{k}X_i, \|_{i=1}^{k}Y_i, S, \delta, \lambda)$ be weakly k-tray invertible with delay t. We consider a single-valued mapping g_k from $S \times (\|_{i=1}^{k}Y_i)^{t+1}$ to $\|_{i=k}^{1}X_i$ satisfying the condition: For $s \in S$ and $\|_{j=1}^{k}x_0^j, \dots, \|_{j=1}^{k}x_t^j$ *in* $\|_{i=1}^{k}X_i$ if $\lambda(s, \|_{i=0}^{t}\|_{j=1}^{k}x_i^j) = \|_{i=0}^{t}\|_{j=1}^{k}y_i^j$, then $g_k(s, \|_{i=t}^{0}\|_{j=1}^{k}y_i^j) = \|_{j=k}^{1}x_0^j$. Since A is weakly k-tray invertible with delay t, thus $\|_{j=1}^{k}x_0^j$ can be uniquely determined by s and $\lambda(s, \|_{i=0}^{t}\|_{j=1}^{k}x_i^j)$, hence g_k is well define. Let $A' = (\|_{i=1}^{k}Y_i, \|_{i=k}^{1}X_i, S', \delta', \lambda')$ be a finite k-tray automaton, where

$$S' = \{(c, s, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t}^j) | c = 0,1, \dots, t, s \in S, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t}^j \in \|_{i=1}^{k}Y_i\},$$

$$\delta'((c, s, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t}^j), \|_{j=1}^{k}y_0^j)$$

$$= \begin{cases} (c+1, s, \|_{j=1}^{k}y_0^j, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t+1}^j), & if 0 \le c < t, \\ (c, s^*, \|_{j=1}^{k}y_0^j, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t+1}^j), & if c = t, \end{cases}$$

Where

$$s^* = \delta(s, k - TC\ (g_k(s, \|_{j=1}^{k}y_0^j, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t}^j)))$$

and

$$\lambda'((c, s, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t}^j), \|_{j=1}^{k}y_0^j) = g_k(s, \|_{j=1}^{k}y_0^j, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t}^j).$$

Here $s_0 \in S$ and $s_0' = (0, s_0, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t}^j) \in S'$.

We show that $\lambda'(s_0', \lambda(s_0, \|_{i=0}^{\infty}\|_{j=1}^{k}x_i^j)) = \|_{i=-t}^{\infty}\|_{j=k}^{1}x_i^j$. Let $\lambda(s_0, \|_{i=0}^{\infty}\|_{j=1}^{k}x_i^j) = \|_{i=0}^{\infty}\|_{j=1}^{k}y_i^j$. thus

$$\begin{aligned} \lambda'(s_0', \lambda(s_0, \|_{i=0}^{\infty}\|_{j=1}^{k}x_i^j)) &= \lambda'(s_0', \|_{i=0}^{\infty}\|_{j=1}^{k}y_i^j) \\ &= \lambda'(s_0', y_0^1y_0^2)\lambda'(\delta'(s_0', |\|_{j=1}^{k}y_0^j), |\|_{j=1}^{k}y_1^j) \\ &\quad \lambda'(\delta'(s_0', \|_{i=0}^{1}\|_{j=1}^{k}y_i^j), \|_{j=1}^{k}y_2^j) \dots \\ &= \lambda'(s_0', |\|_{j=1}^{k}y_0^j)\lambda'(s_1', |\|_{j=1}^{k}y_1^j)\lambda' \\ &\quad (s_2', \|_{j=1}^{k}y_2^j)\lambda'(s_3', \|_{j=1}^{k}y_3^j) \dots, \end{aligned}$$

where

$$\begin{aligned} s_1' &= \delta'(s_0', \|_{j=1}^{k}y_0^j) \\ &= \delta'((0, s_0, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t}^j), \|_{j=1}^{k}y_0^j) \\ &= (1, s_0, \|_{j=1}^{k}y_0^j, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t+1}^j), \\ s_2' &= \delta'(s_1', \|_{j=1}^{k}y_1^j) \\ &= \delta'((1, s_0, \|_{j=1}^{k}y_0^j, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t+1}^j), \|_{j=1}^{k}y_1^j) \\ &= (2, s_0, \|_{j=1}^{k}y_1^j, \|_{j=1}^{k}y_0^j, \dots, \|_{j=1}^{k}y_{-t+2}^j), \end{aligned}$$

hence if $i \le t$ then $s_i' = (i, s_0, \|_{j=1}^{k}y_{i-1}^j, \|_{j=1}^{k}y_{i-2}^j, \dots, \|_{j=1}^{k}y_{i-t}^j)$ and

$$\begin{aligned} s_{t+1}' &= \delta'(s_t', \|_{j=1}^{k}y_t^j) \\ &= \delta'((t, s_0, \|_{j=1}^{k}y_{t-1}^j, \dots, \|_{j=1}^{k}y_0^j), \|_{j=1}^{k}y_t^j) \\ &= (t, \delta(s_0, k - TC\ (g_k(s_0, \|_{j=1}^{k}y_t^j, \|_{j=1}^{k}y_{t-1}^j, \dots, \|_{j=1}^{k}y_0^j))), \\ &\qquad \|_{j=1}^{k}y_t^j, \|_{j=1}^{k}y_{t-1}^j, \dots, \|_{j=1}^{k}y_1^j) \\ &= (t, \delta(s_0, k - TC\ (\|_{j=k}^{1}x_0^j)), \|_{j=1}^{k}y_t^j, \|_{j=1}^{k}y_{t-1}^j, \dots, \|_{j=1}^{k}y_1^j) \\ &= (t, s_1, \|_{j=1}^{k}y_t^j, \|_{j=1}^{k}y_{t-1}^j, \dots, \|_{j=1}^{k}y_1^j), \end{aligned}$$

hence if $i \ge t$ then $s_i' = (t, s_{i-t}, \|_{j=1}^{k}y_{i-1}^j, \|_{j=1}^{k}y_{i-2}^j, \dots, \|_{j=1}^{k}y_{i-t}^j)$. Now we have

$$\begin{aligned} &\lambda'(s_0', \|_{j=1}^{k}y_0^j) \\ &= \lambda'((0, s_0, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t}^j), \|_{j=1}^{k}y_0^j) \\ &= g_k(s_0, \|_{j=1}^{k}y_0^j, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t}^j) = \|_{j=k}^{1}x_{-t}^j, \\ &\lambda'(s_1', \|_{j=1}^{k}y_1^j) \\ &= \lambda'((1, s_0, \|_{j=1}^{k}y_0^j, \|_{j=1}^{k}y_{-1}^j, \dots, \|_{j=1}^{k}y_{-t+1}^j), \|_{j=1}^{k}y_1^j) \\ &= g_k(s_0, \|_{j=1}^{k}y_1^j, \|_{j=1}^{k}y_0^j, \dots, \|_{j=1}^{k}y_{-t+1}^j) = \\ &\|_{j=k}^{1}x_{-t+1}^j, \dots, \lambda'(s_t', \|_{j=1}^{k}y_t^j) = \|_{j=k}^{1}x_{-t+t}^j \\ &= \|_{j=k}^{1}x_0^j, \quad \lambda'(s_{t+1}', \|_{j=1}^{k}y_{t+1}^j) \\ &= \lambda'((t, s_1, \|_{j=1}^{k}y_t^j, \|_{j=1}^{k}y_{t-1}^j, \dots, \|_{j=1}^{k}y_1^j), \|_{j=1}^{k}y_{t+1}^j) \\ &= g_k(s_1, \|_{j=1}^{k}y_{t+1}^j, \|_{j=1}^{k}y_t^j, \dots, \|_{j=1}^{k}y_1^j) = \|_{j=k}^{1}x_1^j, \dots . \end{aligned}$$

In the other words $\lambda'(s_{t+j}', \|_{j=1}^{k}y_{t+j}^j) = \|_{j=k}^{1}x_p^j$, $p = -t, -t+1, \dots$.

Corollary 2. Suppose that A be a finite k-tray automaton. Then A is a weakly k-invertible automaton with delay t if and only if there exists a finite k-tray automaton A′ such that it is a weak k-tray complex inverse with delay t of A.

Theorem 4. Suppose that $\mathrm{A} = (\mathrm{X}^\mathrm{k}, \mathrm{Y}^\mathrm{k}, \mathrm{S}, \delta, \lambda)$ and $\mathrm{A}' = (\mathrm{Y}^\mathrm{k}, \mathrm{X}^\mathrm{k}, \mathrm{S}', \delta', \lambda')$ be two finite k-tray automata and $\mathrm{X} = \mathrm{Y}$ and $\mathrm{k}-\ \mathrm{TC}(\lambda(\mathrm{s},\alpha)) = \lambda(\mathrm{s},\mathrm{k}-\ \mathrm{TC}(\alpha))$ for all $\mathrm{s} \in \mathrm{S}, \alpha \in \mathrm{X}^{\mathrm{k}}$ and also $\mathrm{k}-\ \mathrm{TC}(\lambda'(\mathrm{s}',\gamma)) = \lambda'(\mathrm{s}',\mathrm{k}-\ \mathrm{TC}(\gamma))$ for all $\mathrm{s}' \in \mathrm{S}', \gamma \in \mathrm{Y}^{\mathrm{k}}$. Then A is a k-tray complex inverse with delay zero of A′ if and only if A′ is a k-tray complex inverse with delay zero of A.

Proof. Suppose that (s',s) be a $k-tray$ complex match pair with delay zero, we prove by reduction to absurdity that (s,s') is a finite $k-tray$ complex match pair with delay zero. If for some sequence $||_{j=1}^{k} y_0^j, ||_{j=1}^{k} y_1^j, \ldots \in Y^k,\ \lambda(s,\lambda'(s',||_{i=0}^{\infty}||_{j=1}^{k} y_i^j)) = ||_{i=0}^{\infty}||_{j=k}^{1} y_i^{\prime j}$ and

$||_{i=0}^{\infty}||_{j=1}^{k} y_i^j \neq\ k-TC\ (||_{i=0}^{\infty}||_{j=k}^{1} y_i^{\prime j})$, then there exist $n \geq 0$, such that $||_{i=0}^{n}||_{j=1}^{k} y_i^j \neq ||_{i=0}^{n}||_{j=1}^{k} y_i^{\prime j}$. Since (s',s) is a k-tray complex match pair with delay zero, then

$$\begin{aligned}\lambda'(s',||_{i=0}^{n}||_{j=1}^{k} y_i^{\prime j}) &= \lambda'(s',k-TC\ (||_{i=0}^{n}||_{j=k}^{1} y_i^{\prime j})) \\ &= \lambda'(s',k \\ &\quad -TC\ (\lambda(s,\lambda'(s',||_{i=0}^{n}||_{j=1}^{k} y_i^j)))) \\ &= \lambda'(s',\lambda(s,k-TC\ (\lambda'(s',||_{i=0}^{n}||_{j=1}^{k} y_i^j)))) \\ &= \lambda'(s',||_{i=0}^{n}||_{j=1}^{k} y_i^j).\end{aligned}$$

From $X = Y$ it implies $\lambda'(s',Y^{kn+k}) \neq X^{kn+k}$, thus there exists $||_{i=0}^{n}||_{j=1}^{k} x_i^{\prime\prime j}\ \ in\, X^{kn+k} - \lambda'(s',Y^{kn+k})$. Suppose $\lambda(s,k-TC\ (||_{i=0}^{n}||_{j=1}^{k} x_i^{\prime\prime j})) = ||_{i=0}^{n}||_{j=k}^{1} y_i^{\prime\prime j}$. Since (s',s) is a k-tray complex match pair with delay zero, we have $\lambda'(s',||_{i=0}^{n}||_{j=k}^{1} y_i^{\prime\prime j}) = ||_{i=0}^{n}||_{j=1}^{k} x_i^{\prime\prime j}$. In other words $||_{i=0}^{n}||_{j=1}^{k} x_i^{\prime\prime j}$ is in $\lambda'(s',Y^{kn+k})$. This is a contradiction. From symmetry the theorem is proved.

Definition 15. Let $\mathrm{f_k}$ be a single-valued mapping from $(||_{\mathrm{i}=1}^{\mathrm{k}} \mathrm{Y_i})^{\mathrm{t}+1}$ to $||_{\mathrm{i}=1}^{\mathrm{k}} \mathrm{Z_i}$, $\mathrm{g_k}$ be a single-valued mapping from $(||_{\mathrm{i}=1}^{\mathrm{k}} \mathrm{Z_i})^{\mathrm{r}+1}$ to $||_{\mathrm{i}=\mathrm{k}}^{1} \mathrm{X_i}$. Also, suppose that

$A_0 = (||_{i=1}^{k} X_i, ||_{i=1}^{k} Z_i, S_0, \delta_0, \lambda_0)$, $A_1 = (||_{i=1}^{k} Z_i, ||_{i=1}^{k} Y_i, S_1, \delta_1, \lambda_1)$ be two finite k-tray automata, $A_0^* = (||_{i=1}^{k} Z_i, ||_{i=k}^{1} X_i, (||_{i=1}^{k} Z_i)^r, \delta_0^*, \lambda_0^*)$ be an r-order input memory finite k-tray automaton determined by g_k, $A_1^* = (||_{i=1}^{k} Y_i, ||_{i=1}^{k} Z_i, (||_{i=1}^{k} Y_i)^t, \delta_1^*, \lambda_1^*)$ be a t-order input memory finite k-tray automaton determined by f_k and $A^* = (||_{i=1}^{k} Y_i, ||_{i=k}^{1} X_i, (||_{i=1}^{k} Y_i)^{t+r}, \delta^*, \lambda^*)$ be a $(t+r)$-order input memory finite k-tray automaton determined by g_k, where

$$\begin{aligned} &g_k(f_k(||_{j=1}^{k} y_p^j, \ldots, ||_{i=j}^{k} y_{p-t}^j), \\ &\ldots, f_k(||_{j=1}^{k} y_{p-r}^j, \ldots, ||_{j=1}^{k} y_{p-r-t}^j)) = ||_{j=k}^{1} x_p^{\prime j}, p \\ &= 0,1 \ldots\ .\end{aligned}$$

Then A^* is called the k-tray complex combination of A_1^* and A_0^*. We use $C\,''_{k-com}(A_1^*, A_0^*)$ to denote the k-tray complex combination of A_1^* and A_0^*.

By considering the above definition we give the following theorem:

Theorem 5. *Suppose that A_0^* be a k-tray complex inverse automaton with delay r of A_0, A_1^* be a k-tray weak inverse automaton with delay t of A_1 and*

$A = (||_{i=1}^{k} X_i, ||_{i=1}^{k} Y_i, S_0 \times S_1, \delta, \lambda)$ such that $A = C_k(A_0, A_1)$. Then A^* is a k-tray complex weak inverse automaton with delay $t+r$ of A, where $A^* = C''_{k-com}(A_1^*, A_0^*)$.

Proof. Suppose that (s_0, s_1) be a state of A. Then there exist, s_1^* of A_1^* such that (s_1^*, s_1) is a k-tray complex match pair with delay t. Consider $s_1^* = (||_{j=1}^{k} y_{-1}^j, \ldots, ||_{j=1}^{k} y_{-t}^j)$ and suppose that $s^* = (||_{j=1}^{k} y_{-1}^j, \ldots, ||_{j=1}^{k} y_{-r-t}^j)$ be a state of A^*. We show that s^* and (s_0, s_1) are k-tray complex match pair with delay $r+t$.

Let $\lambda_1(s_1, ||_{i=0}^{\infty}||_{j=1}^{k} z_i^j) = ||_{i=0}^{\infty}||_{j=1}^{k} y_i^j$. Since A_1^* is a k-tray weak invers of A_1, from the proof of Theorem 1, we get that:

$$||_{j=1}^{k} z_{p-t}^j = f_k(||_{j=1}^{k} y_p^j, \ldots, ||_{j=1}^{k} y_{p-t}^j),\ p = t, t+1, \ldots, \tag{1}$$

and since (s_1^*, s_1) is a k-tray complex match pair with delay t, then

$$\lambda_1^*(s_1^*, \lambda_1(s_1, ||_{i=0}^{\infty}||_{j=1}^{k} z_i^j)) = ||_{i=-t}^{\infty}||_{j=1}^{k} z_i^j.$$ Now let

$$\lambda^*(s^*, ||_{i=0}^{\infty}||_{j=1}^{k} y_i^j) = ||_{i=0}^{\infty}||_{j=k}^{1} x_i^{\prime j}. \tag{2}$$

Since A^* is a $(t+r)$-order input memory finite k-tray automaton determined by g_k, Definition 6 implies that:

$$\begin{aligned} &||_{j=k}^{1} x_p^{\prime j} \\ &= g_k(f_k(||_{j=1}^{k} y_p^j, \ldots, ||_{j=1}^{k} y_{p-t}^j), \ldots, f_k(||_{j=1}^{k} y_{p-r}^j, \ldots, ||_{j=1}^{k} y_{p-r-t}^j)), \\ &p = 0,1, \ldots,\end{aligned}$$

thus from (1) we conclude that:

$$||_{j=k}^{1} x_p^{\prime j} = g_k(||_{j=1}^{k} z_{p-t}^j, \ldots, ||_{j=1}^{k} z_{p-r-t}^j),\quad p = r+t, \ldots\ . \tag{3}$$

If $\lambda_0(s_0, ||_{i=0}^{\infty}||_{j=1}^{k} x_i^j) = ||_{i=0}^{\infty}||_{j=1}^{k} z_i^j$, then since A_0^* is a r-order input memory finite k-tray automaton we have $||_{j=k}^{1} x_{p-r}^j = g_k(||_{j=1}^{k} z_p^j, \ldots, ||_{j=1}^{k} z_{p-r}^j)),\ p = r, \ldots$. But we know that A_0^* is a k-tray complex inverse with delay r of A_0, so for any $s_0^* = (||_{j=1}^{k} z_{-r}^j, \ldots, ||_{j=1}^{k} z_{-1}^j)$ of A_0^* there exists $||_{j=k}^{1} x_{-r}^j, \ldots, ||_{j=1}^{k} x_{-1}^j$ in $||_{i=k}^{1} X_i$ such that $\lambda_0^*(s_0^*, ||_{i=0}^{\infty}||_{j=1}^{k} z_i^j) = \lambda_0^*((||_{j=1}^{k} z_{-r}^j, \ldots, ||_{j=1}^{k} z_{-1}^j), \lambda_0(s_0, ||_{i=0}^{\infty}||_{j=1}^{k} x_i^j)) = ||_{i=-r}^{\infty}||_{j=k}^{1} x_i^j$. Thus from the proof Theorem 1. we have

$$||_{j=k}^{1} x_{p-r-t}^j = g_k(||_{j=1}^{k} z_{p-t}^j, \ldots, ||_{j=1}^{k} z_{p-r-t}^j)), p = r+t, \ldots\ . \tag{4}$$

Therefore (3) and (4) imply that: $||_{j=k}^{1} x_p^{\prime j} = ||_{j=k}^{1} x_{p-r-t}^j,\ p = r+t, \ldots.$ Thus from (2) we get that:

$\lambda^*(s^*, ||_{i=0}^{\infty}||_{j=1}^{k} y_i^j) = ||_{i=-r-t}^{\infty}||_{j=k}^{1} x_i^j$. On the other hand

$$\begin{aligned} ||_{i=0}^{\infty}||_{j=1}^{k} y_i^j &= \lambda_1(s_1, ||_{i=0}^{\infty}||_{j=1}^{k} z_i^j) \\ &= \lambda_1(s_1, \lambda_0(s_0, ||_{i=0}^{\infty}||_{j=1}^{k} x_i^j)) \\ &= \lambda((s_1, s_0), ||_{i=0}^{\infty}||_{j=1}^{k} x_i^j). \end{aligned}$$

Hence s^* and (s_0, s_1) are k-tray complex match pair with delay $r + t$.

4. Conclusion

In this paper, we presented the notion of the finite k-tray automata and then we obtained some properties of it. In the time to come we introduce an improvement on FAPKC3 Tao et al. (1997) based on the notions and results of this paper, in which its security is greater than before.

References

Bao F (1993). Two results about the decomposition of delay step of weakly invertible finite automata. Chinese Journal of Computers, 16(8): 629-632.

Bao F, Igarashi Y and Yu X (1996). Some results on decomposition of weakly invertible finite automata. IEICE T INF SYST, 79(1): 1-7.

Chen SH (1981). On the structure of weak inverses of a weakly invertible linear finite automaton. IEICE Transactions on Information and Systems, 4(4): 409-419.

Chen SH (1986). On the structure of finite automata of which M' is an (weak) inverse with delay τ. Journal of Computer Science and Technology, 1(2): 54-59.

Chen SH, Tao RJ (1987). The structure of weak inverses of a finite automaton with bounded error propagation. Chinese science bulletin (Kexue tongbao), 32(10): 713-714.

Chen SH, Tao RJ (1992). Invertibility of quasi-linear finite automata. Advances in Cryptology — CHINACRYPT'92, Science Press, Beijing, 77–86, (in Chinese).

Dai ZD (1994). Invariants and invertibility of linear finite automata. Advances in Cryptology - CHINACRYPT'94, Science Press, Beijing: 127-134, (in Chinese).

Dai ZD, Ye DF (1995). Weak invertibility of nonlinear finite automata over commutative rings. Chinese Science Bulletin, 40: 1357–1360, (in Chinese).

Even S (1965). On information lossless automata of finite order. IEEE Transactions on Electronic Computers, 14(4): 561-569.

Gao X, Bao F (1994). Decomposition of binary weakly invertible finite automata. Chinese Journal of Computers, 17(5): 330-337.

Kleene SC (1956). Representation of events in nerve nets and finite automata. in Automata Studies, Annals of Mathematical Studies 34, Princeton University Press, Princeton: 3-41.

Kurmit AA (1974). Information Lossless Automata of Finite Order. John Wiley, New York.

Lu SZ (1991). Some results on the invertibility of linear finite automata over a ring. Chinese Journal of Computers, 14(8): 570-578.

Tao R (2007). Finite Automata and Application to Cryptography. TSI NGHUA University Press, Springer.

Tao R, Chen S (1999). The generalization of public key cryptosystem FAPKC4. Chinese Science Bulletin, 44(9): 784-790.

Tao R, Chen S (2000). Constructing finite automata with invertibility by transformation method. Journal of Computer Science and Technology, 15(1): 10-26.

Tao R, Chen S, Chen X (1997). FAPKC3: a new fnite automaton public key cryptosystem. Journal of Computer science and Technology, 12(4): 289-305.