УДК 510.5+681.3

В. В. Скобелев

Исследование структуры множества линейных БПИ-автоматов над кольцом $\mathcal{Z}_{p^k}$

(Представлено членом-корреспондентом НАН Украины А. А. Летичевским)

For linear information-lossless automata over the ring $\mathcal{Z}_{p^k}$, we have established conditions and estimated cardinalities for sets of automata characterized via basic characteristics of automata theory (the transition graph is complete with a loop at each vertex, permutation and reduced automata, automata with twin states). For the investigated automata, a criterion of equivalence is established, the problem of parametric identification is resolved, and the canonical presentations, in which all linear transformation are reduced to component-wise multiplication in the ring and to the application of reversible matrices, are designed.

1. Естественным обобщением линейных автоматов над конечным полем [1] являются линейные автоматы над конечным кольцом. Наличие в кольце делителей нуля и необратимых элементов требует тщательной проработки методов анализа и синтеза таких автоматов, так как происходит переход от структуры векторного пространства над конечным полем [2, 3] к модулю линейных форм над конечным кольцом [4]. Известно [5], что БПИ-автомат при каждом фиксированном начальном состоянии осуществляет взаимно-однозначное преобразование входной полугруппы в выходную. Поэтому БПИ-автоматы над конечным кольцом имеют нетривиальную область приложений, а именно: преобразование информации, в том числе и разработка методов защиты информации. Сказанное подтверждается тем, что модели и методы теории конечных полей присутствуют, практически, во всех современных стандартах шифрования [6, 7].

Зафиксируем кольцо $\mathcal{Z}_{p^k} = (\mathbf{Z}_{p^k}, \oplus, \circ)$ (p — простое число, $k \in \mathbf{N}$), где операции $\oplus$ и $\circ$ определены равенствами $a \oplus b = a + b (\mathrm{mod}\, p^k)$ и $a \circ b = a \cdot b (\mathrm{mod}\, p^k)$. В соответствии с [8] в качестве исследуемых моделей выберем инициальный автомат Мили

$$(M_1, \mathbf{q}_0)\colon \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_t \oplus D \circ \mathbf{x}_{t+1} \end{cases} \qquad (t \in \mathbf{Z}_+) \tag{1}$$

и инициальный автомат Мура

$$(M_2, \mathbf{q}_0)\colon \begin{cases} \mathbf{q}_{t+1} = A \circ \mathbf{q}_t \oplus B \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C \circ \mathbf{q}_{t+1} \end{cases} \qquad (t \in \mathbf{Z}_+), \tag{2}$$

где A, B, C и D — $(n \times n)$-матрицы над кольцом $\mathcal{Z}_{p^k}$, а $\mathbf{q}_t$, $\mathbf{x}_t$, $\mathbf{y}_t \in \mathbf{Z}_{p^k}^n$ — векторы-столбцы, представляющие, соответственно, состояние, входной и выходной символы в момент t.

Обозначим через $\mathcal{A}_{n,1}$ множество всех автоматов M_1, определяемых формулой (1), а через $\mathcal{A}_{n,2}$ — множество всех автоматов M_2, определяемых формулой (2).

Для того чтобы автоматы (1) и (2) были БПИ-автоматами (т. е. были обратимыми автоматами), необходимо и достаточно, чтобы для автомата (1) была обратимой матрица D, а для автомата (2) — матрицы B и C. При этом обратные автоматы имеют вид

$$(M_1^{-1}, \mathbf{q}_0)\colon \begin{cases} \mathbf{q}_{t+1} = A_1 \circ \mathbf{q}_t \oplus B_1 \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C_1 \circ \mathbf{q}_t \oplus D_1 \circ \mathbf{x}_{t+1} \end{cases} \qquad (t \in \mathbf{Z}_+),$$

где $A_1 = A \ominus B \circ D^{-1} \circ C$ ($\ominus$ — операция, обратная операции $\oplus$), $B_1 = B \circ D^{-1}$, $C_1 = \ominus D^{-1} \circ C$, $D_1 = D^{-1}$ и

$$(M_2^{-1}, \mathbf{q}_0)\colon \begin{cases} \mathbf{q}_{t+1} = B_1 \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = C_1 \circ \mathbf{q}_t \oplus D_1 \circ \mathbf{x}_{t+1} \end{cases} \qquad (t \in \mathbf{Z}_+)$$

($B_1 = C^{-1}$, $C_1 = \ominus A$, $D_1 = B^{-1} \circ C^{-1}$). Обозначим через $\mathcal{A}_{n,i}^{inv}$ $(i = 1, 2)$ множество всех обратимых автоматов $M_i \in \mathcal{A}_{n,i}$.

2. Исследуем конечно-автоматные характеристики автоматов $M \in \mathcal{A}_{n,i}^{inv}$ $(i = 1, 2)$.

Пусть M_n и M_n^{inv} — множество, соответственно, всех и всех обратимых $(n \times n)$-матриц над кольцом $\mathcal{Z}_{p^k}$. Ясно, что $|\mathsf{M}_n| = p^{k \cdot n^2}$. Так как $a \in \mathbf{Z}_{p^k}$ — обратимый элемент кольца $\mathcal{Z}_{p^k}$ тогда и только тогда, когда $a \neq 0 \pmod p$, то число обратимых и необратимых элементов кольца $\mathcal{Z}_{p^k}$ равно, соответственно, $(p-1) \cdot p^{k-1}$ и p^{k-1}. Из этих оценок вытекает

Теорема 1. *Для любого простого числа p при всех k, $n \in \mathbf{N}$*

$$n! \cdot (p-1)^n \cdot p^{-n^2} \cdot |M_n| \leqslant |M_n^{inv}| \leqslant (1 - p^{-n})^n \cdot |M_n|. \tag{3}$$

Следствие 1. *Для любого простого числа p при всех k, $n \in \mathbf{N}$*

$$(1 - (1 - p^{-n})^n) \cdot |M_n| \leqslant |M_n \setminus M_n^{inv}| \leqslant (1 - n! \cdot (p-1)^n \cdot p^{-n^2}) \cdot |M_n|. \tag{4}$$

Так как $|\mathcal{A}_{n,i}| = |\mathsf{M}_n|^{5-i}$ $(i = 1, 2)$, $|\mathcal{A}_{n,1}^{inv}| = |\mathsf{M}_n|^3 \cdot |\mathsf{M}_n^{inv}|$ и $|\mathcal{A}_{n,2}^{inv}| = |\mathsf{M}_n| \cdot |\mathsf{M}_n^{inv}|^2$, то из теоремы 1 вытекает

Теорема 2. *Для любого простого числа p при всех k, $n \in \mathbf{N}$*

$$(n! \cdot (p-1)^n \cdot p^{-n^2})^i \cdot |\mathcal{A}_{n,i}| \leqslant |\mathcal{A}_{n,i}^{inv}| \leqslant (1 - p^{-n})^{n \cdot i} \cdot |\mathcal{A}_{n,i}| \qquad (i = 1, 2). \tag{5}$$

Обозначим через $\mathsf{D}_n^{(1)}$ и $\mathsf{D}_n^{(2)}$ — множество диагональных $(n \times n)$-матриц, на главной диагонали которых расположены, соответственно, обратимые и необратимые элементы кольца $\mathcal{Z}_{p^k}$. Тогда $\mathsf{D}_n^{(1)} \subseteq \mathsf{M}_n^{inv}$ и $\mathsf{D}_n^{(2)} \subseteq \mathsf{M}_n \setminus \mathsf{M}_n^{inv}$, причем для любого простого числа p при всех k, $n \in \mathbf{N}$ истинны равенства

$$|\mathsf{D}_n^{(1)}| = (p-1)^n \cdot p^{(k-1) \cdot n}, \tag{6}$$

$$|\mathsf{D}_n^{(2)}| = p^{(k-1) \cdot n}. \tag{7}$$

Пусть $\mathcal{B}_{n,1}^{inv}$ — множество всех таких автоматов $M_1 \in \mathcal{A}_{n,1}^{inv}$, что $D \in \mathsf{D}_n^{(1)}$, а $\mathcal{B}_{n,2}^{inv}$ — множество всех таких автоматов $M_2 \in \mathcal{A}_{n,2}^{inv}$, что B, $C \in \mathsf{D}_n^{(1)}$. Из (6) вытекает, что для любого простого числа p при всех k, $n \in \mathbf{N}$

$$|\mathcal{B}_{n,i}^{inv}| = ((p-1)^n \cdot p^{(k-1-k \cdot n) \cdot n})^i \cdot |\mathcal{A}_{n,i}| \qquad (i = 1, 2). \tag{8}$$

Обозначим через $\mathcal{G}_{n,i}$ $(i = 1, 2)$ множество всех автоматов $M \in \mathcal{A}_{n,i}$, у которых граф переходов — полный граф с петлями, и $\mathcal{G}_{n,i}^{inv} = \mathcal{G}_{n,i} \bigcap \mathcal{A}_{n,i}^{inv}$ $(i = 1, 2)$. Из (1) и (2) вытекает, что если для автомата $M \in \mathcal{A}_{n,i}$ $(i = 1, 2)$ матрица B обратимая, то $M \in \mathcal{G}_{n,i}$. Следовательно, для любого простого числа p при всех k, $n \in \mathbf{N}$ истинны равенство $\mathcal{G}_{n,2}^{inv} = \mathcal{A}_{n,2}^{inv}$ и неравенства

$$((n!) \cdot (p-1)^n \cdot p^{-n^2})^2 \cdot |\mathcal{A}_{n,1}| \leqslant |\mathcal{G}_{n,1}^{inv}| \leqslant (1 - p^{-n})^{2 \cdot n} \cdot |\mathcal{A}_{n,1}|. \tag{9}$$

Пусть $\mathcal{C}_{n,i}^{inv}$ $(i = 1, 2)$ — множество всех перестановочных автоматов $M \in \mathcal{A}_{n,i}^{inv}$. Из (1) и (2) вытекает, что если для автомата $M \in \mathcal{A}_{n,i}$ $(i = 1, 2)$ матрица A обратимая, то M — перестановочный автомат, т. е. для любого простого числа p при всех k, $n \in \mathbf{N}$

$$|\mathcal{C}_{n,i}^{inv}| \geqslant (n! \cdot (p-1)^n \cdot p^{-n^2})^{i+1} \cdot |\mathcal{A}_{n,i}| \qquad (i = 1, 2). \tag{10}$$

Обозначим через $\mathcal{D}_{n,i}^{inv}$ $(i = 1, 2)$ множество всех приведенных автоматов $M \in \mathcal{A}_{n,i}^{inv}$. Из (1) и (2) вытекает, что:

1) если для автомата $M \in \mathcal{A}_{n,1}$ матрица C обратимая, то M — приведенный автомат, степень различимости [9] которого равна 1;

2) если для автомата $M \in \mathcal{A}_{n,2}$ матрицы A и C обратимые, то M — приведенный автомат, степень различимости которого равна 1. Следовательно, для любого простого числа p при всех k, $n \in \mathbf{N}$

$$|\mathcal{D}_{n,i}^{inv}| \geqslant (n! \cdot (p-1)^n \cdot p^{-n^2})^{i+1} \cdot |\mathcal{A}_{n,i}| \qquad (i = 1, 2). \tag{11}$$

Пусть $\mathcal{E}_{n,i}^{inv}$ $(i = 1, 2)$ — множество всех автоматов $M \in \mathcal{A}_{n,i}^{inv}$, имеющих состояния-близнецы. Из (1) и (2) вытекает, что:

1) если для автомата $M \in \mathcal{A}_{n,1}$ матрицы A и C необратимые и система уравнений

$$\begin{cases} A \circ \mathbf{u} = \mathbf{0}, \\ C \circ \mathbf{u} = \mathbf{0} \end{cases}$$

имеет ненулевое решение, то в автомате M существуют состояния-близнецы;

2) если для автомата $M \in \mathcal{A}_{n,2}$ матрица A необратимая, то в автомате M существуют состояния-близнецы. Следовательно, для любого простого числа p при всех k, $n \in \mathbf{N}$

$$|\mathcal{E}_{n,1}^{inv}| \geqslant n! \cdot (p-1)^n \cdot p^{-n^2} \cdot (1 - (1 - p^{-n})^n)^2 \cdot |\mathcal{A}_{n,1}|, \tag{12}$$

$$|\mathcal{E}_{n,2}^{inv}| \geqslant (1 - (1 - p^{-n})^n) \cdot (n! \cdot (p-1)^n \cdot p^{-n^2})^2 \cdot |\mathcal{A}_{n,2}|. \tag{13}$$

Обозначим через $\mathcal{F}_{n,1}^{inv}$ множество всех таких автоматов $M \in \mathcal{E}_{n,1}^{inv}$, что A, $C \in \mathsf{D}_n^{(2)}$, а $\mathcal{F}_{n,2}^{inv}$ — множество всех таких автоматов $M \in \mathcal{E}_{n,2}^{inv}$, что $A \in \mathsf{D}_n^{(2)}$. Из (3), (7) вытекает, что для любого простого числа p при всех k, $n \in \mathbf{N}$

$$|\mathcal{F}_{n,1}^{inv}| \geqslant n! \cdot (p-1)^n \cdot p^{-n^2} \cdot p^{2 \cdot n \cdot (k-1-k \cdot n)} \cdot |\mathcal{A}_{n,1}|, \tag{14}$$

$$|\mathcal{F}_{n,2}^{inv}| \geqslant p^{n \cdot (k-1-k \cdot n)} \cdot (n! \cdot (p-1)^n \cdot p^{-n^2})^2 \cdot |\mathcal{A}_{n,2}|. \tag{15}$$

Отметим, что параметр $k \in \mathbf{N}$ в (3)–(5), (9)–(13) не встречается в явном виде, а в (6)–(8), (14), (15) присутствует в явном виде. Следовательно, в первом случае доля соответствующих объектов не меняется при изменении параметра k, а во втором случае доля соответствующих объектов существенно зависит от параметра k.

3. Пусть M, $M' \in \mathcal{A}_{n,i}$ $(i = 1, 2)$, т. е. если $M = M_1$, то

$$M_1' \colon \begin{cases} \mathbf{q}_{t+1}' = A' \circ \mathbf{q}_t' \oplus B' \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1}' = C' \circ \mathbf{q}_t' \oplus D' \circ \mathbf{x}_{t+1} \end{cases} \qquad (t \in \mathbf{Z}_+),$$

а если $M = M_2$, то

$$M_2'\colon \begin{cases} \mathbf{q}'_{t+1} = A' \circ \mathbf{q}'_t \oplus B' \circ \mathbf{x}_{t+1} \\ \mathbf{y}'_{t+1} = C' \circ \mathbf{q}'_{t+1} \end{cases} \qquad (t \in \mathbf{Z}_+).$$

Автоматы M, $M' \in \mathcal{A}_{n,i}$ $(i = 1, 2)$ эквивалентные, если для любого $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ существует такое $\mathbf{q}'_0 \in \mathbf{Z}_{p^k}^n$ и, наоборот, для любого $\mathbf{q}'_0 \in \mathbf{Z}_{p^k}^n$ существует такое $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$, что инициальные автоматы $(M, \mathbf{q}_0)$ и $(M', \mathbf{q}'_0)$ реализуют один и тот же оператор [9].

Теорема 3. *Автоматы M, $M' \in \mathcal{A}_{n,1}$ эквивалентные тогда и только тогда, когда выполнены следующие условия:*

(i) $D = D'$;

(ii) $C' \circ \mathbf{q}'_0 \ominus C \circ \mathbf{q}_0 = \mathbf{0}$;

(iii) для любого $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ существует такое $\mathbf{q}'_0 \in \mathbf{Z}_{p^k}^n$ и, наоборот, для любого $\mathbf{q}'_0 \in \mathbf{Z}_{p^k}^n$ существует такое $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$, что $C' \circ (A')^j \circ \mathbf{q}'_0 \ominus C \circ A^j \circ \mathbf{q}_0 = \mathbf{0}$ $(j = 1, \ldots, 2 \cdot p^{k \cdot n} - 2)$;

(iv) $C' \circ (A')^j \circ B' \ominus C \circ A^j \circ B = O$ $(j = 1, \ldots, 2 \cdot p^{k \cdot n} - 3)$, где O — нулевая $(n \times n)$-матрица;

(v) $C' \circ B' \ominus C \circ B = O$.

Теорема 4. *Автоматы M, $M' \in \mathcal{A}_{n,2}$ эквивалентные тогда и только тогда, когда выполнены следующие условия:*

(i) $C' \circ B' \ominus C \circ B = O$, где O — нулевая $(n \times n)$-матрица;

(ii) для любого $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ существует такое $\mathbf{q}'_0 \in \mathbf{Z}_{p^k}^n$ и, наоборот, для любого $\mathbf{q}'_0 \in \mathbf{Z}_{p^k}^n$ существует такое $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$, что $C' \circ (A')^j \circ \mathbf{q}'_0 \ominus C \circ A^j \circ \mathbf{q}_0 = \mathbf{0}$ $(j = 1, \ldots, 2 \cdot p^{k \cdot n} - 1)$;

(iii) $C' \circ (A')^j \circ B' \ominus C \circ A^j \circ B = O$ $(j = 1, \ldots, 2 \cdot p^{k \cdot n} - 2)$.

4. Рассмотрим задачу параметрической идентификации автомата $M \in \mathcal{A}_{n,1}$.

Теорема 5. *Каждая из матриц C и D автомата $M \in \mathcal{A}_{n,1}$ идентифицируется единственным образом посредством n-кратного эксперимента высоты 1.*

Следствие 2. *Если в автомате $M \in \mathcal{A}_{n,1}$ матрица C обратимая, то автомат M идентифицируется единственным образом посредством двух n-кратных экспериментов высоты 1, двух n-кратных экспериментов высоты 2 и решения $2 \cdot n$ систем линейных уравнений n-го порядка над кольцом $\mathcal{Z}_{p^k}$.*

Если матрица C необратимая, то идентификация матриц A и B для автомата $M \in \mathcal{A}_{n,1}$ сводится к решению при известных матрицах C и D системы нелинейных уравнений

$$C \circ (A^i \circ \mathbf{q}_0 \oplus \bigoplus_{j=1}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_j \oplus B \circ \mathbf{x}_i) = \mathbf{y}_{i+1} \ominus D \circ \mathbf{x}_{i+1}$$

для всех $\mathbf{q}_0 \in \mathbf{Z}_{p^k}^n$ и $\mathbf{x}_1 \cdots \mathbf{x}_{i+1} \in (\mathbf{Z}_{p^k}^n)^{i+1}$ $(i = 1, \ldots, p^{n \cdot k} - 1)$.

Решение задачи параметрической идентификации автомата $M \in \mathcal{A}_{n,2}$ значительно сложнее, так как возникает необходимость решения системы нелинейных уравнений

$$C \circ (A^{i+1} \circ \mathbf{q}_0 \oplus \bigoplus_{j=0}^{i-1} A^{i-j} \circ B \circ \mathbf{x}_{j+1} \oplus B \circ \mathbf{x}_{i+1}) = \mathbf{y}_{i+1}$$

при неизвестной обратимой матрице C.

5. Построим каноническое представление автоматов (1) и (2). Множество $\mathbf{Z}_{p^k}^n$ представляет собой $\mathcal{Z}_{p^k}$-модуль линейных форм [4]. Следовательно, каждое линейное преобразование

$\mathbf{Z}_{p^k}^n$ в $\mathbf{Z}_{p^k}^n$, иными словами, каждая матрица $H \in \mathsf{M}_n$ с помощью элементарных операций (т. е. умножением слева и справа на соответствующие матрицы G, $F \in \mathsf{M}_n^{inv}$, может быть представлено в виде

$$G \circ H \circ F = \begin{pmatrix} U & O_{r,h} \\ O_{h,r} & V \end{pmatrix}, \tag{16}$$

где $U \in \mathsf{D}_r^{(1)}$, $V \in \mathsf{D}_h^{(2)}$ $(r+h=n)$, а $O_{r,h}$ — нулевая $(r \times h)$-матрица. Обозначим через $\mathsf{D}_n^{(1),(2)}$ множество всех матриц вида (16). Отметим, что матрица $X \in \mathsf{D}_n^{(1),(2)}$ осуществляет умножение компонент вектора $\mathbf{z} \in \mathbf{Z}_{p^k}^n$ на соответствующие элементы кольца $\mathcal{Z}_{p^k}$, а множество M_n^{inv} — группа, изоморфная подгруппе симметрической группы $S_{p^{k \cdot n}}$.

Будем говорить, что автомат $(M, \mathbf{q}_0)$ $(M \in \mathcal{A}_{n,1} \bigcup \mathcal{A}_{n,2})$ представлен в канонической форме, если все выполняемые в его представлении линейные преобразования — элементы множеств $\mathsf{D}_n^{(1),(2)}$ и M_n^{inv}. Канонические формы автоматов $(M_1, \mathbf{q}_0)$ и $(M_2, \mathbf{q}_0)$ имеют, соответственно, следующий вид:

$$(M_1, \mathbf{q}_0)\colon \begin{cases} F_1^{-1} \circ \mathbf{q}_{t+1} = R_1 \circ X_1 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus R_2 \circ X_2 \circ (F_2^{-1} \circ \mathbf{x}_{t+1}) \\ G_3 \circ \mathbf{y}_{t+1} = X_3 \circ R_3 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus R_4 \circ X_4 \circ (F_4^{-1} \circ \mathbf{x}_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{17}$$

$$(M_2, \mathbf{q}_0)\colon \begin{cases} F_1^{-1} \circ \mathbf{q}_{t+1} = R_1 \circ X_1 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus R_2 \circ X_2 \circ (F_2^{-1} \circ \mathbf{x}_{t+1}) \\ G_3 \circ \mathbf{y}_{t+1} = X_3 \circ R_3 \circ (F_1^{-1} \circ \mathbf{q}_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{18}$$

где $X_i \in \mathsf{D}_n^{(1),(2)}$ $(i = 1, \ldots, 4)$, G_i, $R_i \in \mathsf{M}_n^{inv}$ $(i = 1, \ldots, 4)$, причем $X_1 = G_1 \circ A \circ F_1$, $X_2 = G_2 \circ B \circ F_2$, $X_3 = G_3 \circ C \circ F_3$, $X_4 = G_4 \circ D \circ F_4$, $R_1 = F_1^{-1} \circ G_1^{-1}$, $R_2 = F_1^{-1} \circ G_2^{-1}$, $R_3 = F_3^{-1} \circ F_1$, а $R_4 = G_3 \circ G_4^{-1}$.

Для автомата $(M, \mathbf{q}_0)$ $(M \in \mathcal{A}_{n,1}^{inv} \bigcup \mathcal{A}_{n,2}^{inv})$ представления в канонической форме имеют более простой вид, а именно:

$$(M_1, \mathbf{q}_0)\colon \begin{cases} F_1^{-1} \circ \mathbf{q}_{t+1} = R_1 \circ X_1 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus R_2 \circ X_2 \circ (F_2^{-1} \circ \mathbf{x}_{t+1}) \\ G_3 \circ \mathbf{y}_{t+1} = X_3 \circ R_3 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus Y_1 \circ \mathbf{x}_{t+1} \end{cases} \quad (t \in \mathbf{Z}_+), \tag{19}$$

$$(M_2, \mathbf{q}_0)\colon \begin{cases} F_1^{-1} \circ \mathbf{q}_{t+1} = R_1 \circ X_1 \circ (F_1^{-1} \circ \mathbf{q}_t) \oplus Y_2 \circ \mathbf{x}_{t+1} \\ \mathbf{y}_{t+1} = Y_3 \circ (F_1^{-1} \circ \mathbf{q}_{t+1}) \end{cases} \quad (t \in \mathbf{Z}_+), \tag{20}$$

где $Y_1 = G_3 \circ D \in \mathsf{M}_n^{inv}$, $Y_2 = F_1^{-1} \circ B \in \mathsf{M}_n^{inv}$ и $Y_3 = C \circ F_1 \in \mathsf{M}_n^{inv}$.

В заключение отметим, что при логарифмическом весе [11] емкостная сложность представления элемента $\mathbf{z} \in \mathbf{Z}_{p^k}^n$ равна $n \cdot \lceil k \cdot \log p \rceil$, а емкостная сложность представления матрицей $W \in \mathsf{M}_n^{inv}$ подстановки, определенной на множестве $\mathbf{Z}_{p^k}^n$, равна $n^2 \cdot \lceil k \cdot \log p \rceil$. Перестановку на множестве $\mathbf{Z}_{p^k}^n$ назовем легко вычислимой, если при логарифмическом весе емкостная сложность ее представления и временная сложность ее применения к элементу $\mathbf{z} \in \mathbf{Z}_{p^k}^n$ равна $O(n \cdot \lceil k \cdot \log p \rceil)$. Изучение структуры множества таких подстановок — предмет дальнейших исследований.

1. *Гилл А.* Линейные последовательностные машины. – Москва: Наука, 1974. – 288 с.
2. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1. – Москва: Мир, 1988. – 394 с.

3. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 2. – Москва: Мир, 1988. – 428 с.
4. *ван дер Варден Б. Л.* Алгебра. – Москва: Наука, 1979. – 634 с.
5. *Курмит А. А.* Автоматы без потери информации конечного порядка. – Рига: Зинатне, 1972. – 266 с.
6. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. – Москва: ТРИУМФ, 2003. – 816 с.
7. *Харин Ю. С. и др.* Математические и компьютерные основы криптологии. – Минск: Новое знание, 2003. – 382 с.
8. *Глушков В. М.* Синтез цифровых автоматов. – Москва: Физматлит, 1962. – 476 с.
9. *Трахтенброт Б. А., Барздинь Я. М.* Конечные автоматы (поведение и синтез). – Москва: Наука, 1970. – 400 с.
10. *Коршунов А. Д.* О перечислении конечных автоматов // Проблемы кибернетики. Вып. 34. – Москва: Наука, 1978. – С. 5–82.
11. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. – Москва: Мир, 1979. – 536 с.

Институт прикладной математики и механики НАН Украины, Донецк

Поступило в редакцию 16.02.2007