ПРИКЛАДНАЯ ТЕОРИЯ АВТОМАТОВ

УДК 519.7 DOI 10.17223/20710410/66/7

О СВОЙСТВАХ КОНЕЧНО-АВТОМАТНОГО ГЕНЕРАТОРА[1]

А. О. Бахарев*, Р. О. Запанов*, С. Е. Зинченко*, И. А. Панкратова**, Е. С. Прудников**

*Новосибирский государственный университет, г. Новосибирск, Россия
**Томский государственный университет, г. Томск, Россия

E-mail: a.bakharev@g.nsu.ru, rinchinzapanov@yandex.ru, s.zinchenko@alumni.nsu.ru, pank@mail.tsu.ru, egorprudnikov71@gmail.com

Рассматриваются периодические свойства двухкаскадного конечно-автоматного криптографического генератора. Сформулированы некоторые необходимые условия того, что выходная последовательность генератора имеет период максимально возможной длины. Получены также достаточные условия, на основании которых предложен способ построения такого генератора. Доказано, что для любой двоичной последовательности, период которой равен степени двойки, существует генератор, выдающий её.

Ключевые слова: *конечный автомат, криптографический генератор, криптоавтомат, период последовательности.*

ON THE PROPERTIES OF A FINITE-STATE GENERATOR

A. O. Bakharev*, R. O. Zapanov*, S. E. Zinchenko*, I. A. Pankratova**, E. S. Prudnikov**

*Novosibirsk State University, Novosibirsk, Russia
**Tomsk State University, Tomsk, Russia

The periodic properties of a two-stage finite-state generator $G = A_1 \cdot A_2$ are studied, where $A_1 = (\mathbb{F}_2^n, \mathbb{F}_2, g_1, f_1)$ (it is autonomous), $A_2 = (\mathbb{F}_2, \mathbb{F}_2^m, \mathbb{F}_2, g_2, f_2)$, $n, m \geqslant 1$. Some necessary conditions for such a generator with the maximum period of 2^{n+m} have been formulated, namely: 1) the output sequence of A_1 is purely periodic and the period length is 2^n; 2) the substitution G_u transforming any initial state $y(1)$ of the automaton A_2 into the state $y(2^n+1)$ is a full-cycle substitution; 3) the function f_1 has an odd weight; 4) the substitutions $g(0,\cdot)$ and $g(1,\cdot)$ have different parities. Some sufficient conditions have been also formulated, for example, in addition to conditions 1–4, the function $g_2(u, y)$ must be injective in u and the weight of the function f_2 must be odd. Two methods for constructing a generator having maximum period have been proposed. It has been proved that, for any binary sequence whose period is a power of two, there exists a generator that produces it.

Keywords: *finite state machine, cryptographic generator, cryptoautomaton, sequence period.*

[1]Работа первого автора выполнена при поддержке Математического центра в Академгородке, соглашение с Министерством науки и высшего образования РФ № 075-15-2022-282.

Введение

В работе [1] Г.П. Агибаловым введено понятие криптоавтомата как класса автоматных сетей с ключом, который может включать в себя начальные состояния компонент сети и их функции переходов и выходов. Этому определению криптоавтомата соответствуют различные криптографические примитивы: генераторы ключевого потока MUGI [2] и KNOT [3] — в поточных шифрах, симметричный конечно-автоматный шифр Закревского [4], конечно-автоматные криптосистемы с открытым ключом для шифрования и цифровой подписи семейства FAPKC [5] и другие.

Рассматриваемый в данной работе генератор является, с одной стороны, частным случаем последовательной композиции $A_1 \cdot A_2$ в модели [1] (A_1 — автомат Мура); с другой — обобщением конечно-автоматного генератора (δ, τ)-шагов [6] (функция переходов автомата A_2 произвольна). В [7] изучены некоторые задачи криптоанализа генератора, в [8] — его периодические свойства. В продолжение этих исследований в работе получены условия максимальности периода выходной последовательности генератора и предложены способы построения генераторов с таким свойством.

1. Базовые определения и обозначения

Пусть $\mathbb{F}_2 = \{0, 1\}$; *весом* $\mathrm{wt}(f)$ булевой функции $f : \mathbb{F}_2^n \to \mathbb{F}_2$, $n \in \mathbb{N}$, будем называть

$$\mathrm{wt}(f) = |\,\{x \in \mathbb{F}_2^n : f(x) = 1\}\,|.$$

Последовательность $\{u_i : 1, 2, \dots\}$, $u_i \in \mathbb{F}_2$, называется *периодической*, если для некоторых $i_0, t \in \mathbb{N}$ выполнено $u_i = u_{i+t}$ для всех $i \geqslant i_0$. Минимальное t с таким свойством называется *периодом* последовательности. Периодическая последовательность называется *чисто периодической*, если $i_0 = 1$.

Пусть $\sigma \in \mathbb{S}_n$ — подстановка степени n, $\sigma = \tau_1 \circ \dots \circ \tau_k$ — произвольное разложение σ в произведение транспозиций. Число $\mathsf{sgn} = (-1)^k$ называется *знаком* σ, полностью определяется подстановкой σ и не зависит от способа разложения в произведение транспозиций.

Лемма 1 [9]. Пусть $\sigma \in \mathbb{S}_n$ и c — число попарно независимых циклов в σ. Тогда $\mathsf{sgn}(\sigma) = (-1)^{n-c}$.

2. Конечно-автоматный генератор

Схема двухкаскадного конечно-автоматного криптографического генератора $G = A_1 \cdot A_2$ представлена на рис. 1: это последовательное соединение автономного автомата $A_1 = (\mathbb{F}_2^n, \mathbb{F}_2, g_1, f_1)$ (с функцией переходов $g_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ и функцией выходов $f_1 : \mathbb{F}_2^n \to \mathbb{F}_2$) и автомата $A_2 = (\mathbb{F}_2, \mathbb{F}_2^m, \mathbb{F}_2, g_2, f_2)$ (с функцией переходов $g_2 : \mathbb{F}_2 \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ и функцией выходов $f_2 : \mathbb{F}_2 \times \mathbb{F}_2^m \to \mathbb{F}_2$), $n, m \geqslant 1$.

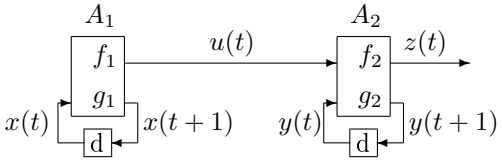

Рис. 1. Схема генератора G

В каждый момент времени $t = 1, 2, \dots$ автомат A_1, находясь в состоянии $x(t) \in \mathbb{F}_2^n$, выдаёт выходной символ $u(t) = f_1(x(t))$ и переходит в следующее состояние $x(t+1) = g_1(x(t))$, а автомат A_2, находясь в состоянии $y(t) \in \mathbb{F}_2^m$, принимает от A_1 символ $u(t)$,

выдаёт на выход генератора символ $z(t) = f_2(u(t), y(t))$ и переходит в следующее состояние $y(t+1) = g_2(u(t), y(t))$. Ключом генератора может быть любое непустое подмножество множества $\{x(1), y(1), f_1, g_1, f_2, g_2\}$.

Периодом генератора назовём период его выходной последовательности $z(1)z(2)\ldots$ В [8] доказано, что период генератора не превосходит 2^{n+m}. Сформулируем условия достижения верхней оценки.

3. Необходимые условия максимальности периода генератора

Обозначим через $g_2^\delta = g_2(\delta, \cdot)$, $\delta \in \{0, 1\}$, подфункции функции g_2.

Утверждение 1 [8]. Если период генератора G равен 2^{n+m}, то:

1) функция g_1 является полноцикловой подстановкой;
2) подфункции g_2^0 и g_2^1 являются подстановками;
3) $y(2^n i + j) \neq y(2^n k + j)$ для всех $i, k \in \{0, \ldots, 2^m - 1\}$, $i \neq k$, $j = 1, \ldots, 2^n$;
4) выходная последовательность $z(1)z(2)\ldots$ генератора чисто периодическая.

Дополним список необходимых условий:

Утверждение 2. Если период генератора G равен 2^{n+m}, то последовательность $u(1)u(2)\ldots$ чисто периодическая и её период равен 2^n.

Доказательство. Из [10, утверждение 6.1, п. 2], п. 1 утверждения 1 и формулы $u(t) = f_1(g_1(t))$ следует, что последовательность $\{u(t) : t = 1, 2, \ldots\}$ чисто периодическая и её минимальный период s делит 2^n. Предположим, что $s < 2^n$, тогда $s \,|\, 2^{n-1}$ и $u(j) = u(2^{n-1} i + j)$ для всех i, j.

По п. 3 утверждения 1 для любого j, $1 \leqslant j \leqslant 2^n$, значения $y(2^n i + j)$, $i = 0, \ldots, 2^m - 1$, попарно различны, а всего таких значений 2^m. Значит, для $j = 2^{n-1} + 1$ найдётся i, такое, что $y(1) = y(2^n i + 2^{n-1} + 1) = y(2^{n-1} k + 1)$, где $k = 2i + 1$. Из того, что $u(1) = u(2^{n-1} k + 1)$, и описания функционирования генератора заключаем, что $z(1) = z(2^{n-1} k + 1)$ и $y(2) = y(2^{n-1} k + 2)$. Продолжая по индукции, получим: $z(j) = z(2^{n-1} k + j)$ для всех j, т. е. период генератора делит $2^{n-1} k = 2^n i + 2^{n-1} \leqslant$ $\leqslant 2^n (2^m - 1) + 2^{n-1} = 2^{n+m} - 2^{n-1}$, что противоречит условию. ■

Для $u = u(1)u(2)\ldots u(2^n)$ обозначим через $G_u : \mathbb{F}_2^m \to \mathbb{F}_2^m$ композицию подстановок

$$G_u = g_2^{u(1)} \circ \ldots \circ g_2^{u(2^n)},$$

другими словами, $G_u(y(1)) = y(2^n + 1)$ для всех $y(1) \in \mathbb{F}_2^m$, т. е. G_u — это подстановка на множестве состояний автомата A_2, переводящая любое его начальное состояние в то, в которое автомат перейдёт после одного цикла последовательности на входе.

В следующем утверждении приведено, в том числе (в п. 2), решение задачи 9 из второго раунда десятой Международной олимпиады по криптографии Non-Stop University CRYPTO [11, 12].

Утверждение 3. Если период генератора G равен 2^{n+m}, то:

1) подстановка G_u полноцикловая;
2) вес функции f_1 нечётный;
3) подстановки g_2^0 и g_2^1 имеют разную чётность.

Доказательство.

1) Следует из п. 3 утверждения 1.

2) Пусть $\mathrm{wt}(f_1) = k$. Из утверждения 2 следует, что в отрезке $u = u(1)u(2)\ldots u(2^n)$ содержатся значения функции f_1 на всех наборах значений её аргументов, т. е. k единиц и $2^n - k$ нулей. Следовательно,

$$\mathsf{sgn}(G_u) = \mathsf{sgn}(g_2^1)^k \cdot \mathsf{sgn}(g_2^0)^{2^n-k}. \tag{1}$$

С другой стороны, по лемме 1 и ввиду п. 1

$$\mathsf{sgn}(G_u) = (-1)^{2^m-1} = -1. \tag{2}$$

Это возможно только при нечётном k.

3) Если $\mathsf{sgn}(g_2^0) = \mathsf{sgn}(g_2^1)$, то $\mathsf{sgn}(G_u) = \mathsf{sgn}(g_2^0)^{2^n} = 1$ — противоречие с (2). ■

Условия утверждений 1–3 не являются достаточными для максимальности периода генератора, в частности, потому, что не накладывают никаких ограничений на функцию выходов автомата A_2. В следующем пункте эти условия дополняются ещё двумя, что даёт достаточные (но теперь не необходимые) условия максимальности периода.

4. Достаточные условия максимальности периода генератора

Утверждение 4. Пусть для генератора G выполнены следующие условия:

1) последовательность $u(1)u(2)\ldots$ чисто периодическая с периодом 2^n;
2) подфункции g_2^0 и g_2^1 — подстановки, их композиция $G_u = g_2^{u(1)} \circ \ldots \circ g_2^{u(2^n)}$ — полноцикловая подстановка;
3) функция $g_2(u, y) : \mathbb{F}_2 \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ инъективна по переменной u.

Тогда период последовательности состояний $(y(t) : t \in \mathbb{N})$ равен 2^{n+m}, а отображение

$$\psi_G : \mathbb{F}_2^n \times \mathbb{F}_2^m \to \mathbb{F}_2^n \times \mathbb{F}_2^m,\ \big(x(t), y(t)\big) \mapsto \big(x(t+1), y(t+1)\big),$$
$$\big(x(t+1), y(t+1)\big) = \big(g_1(x(t)), g_2(f_1(x(t)), y(t))\big)$$

является полноцикловой подстановкой.

Доказательство. Обозначим через π период последовательности $(y(t) : t \in \mathbb{N})$. Из условий 1 и 3 ввиду [10, следствие 1 теоремы 7.5] получаем, что $2^n \,|\, \pi$. Условие 2 означает, что значения $y(1), y(2^n + 1), \ldots, y(2^n(2^m - 1) + 1)$ попарно различны. Следовательно, $\pi \geqslant 2^{n+m}$. Неравенство $\pi \leqslant 2^{n+m}$ очевидно в силу формулы $y(t+1) = g_2(f_1(x(t)), y(t))$ и того, что количество разных пар $(x(t), y(t))$ равно 2^{n+m}.

Поскольку $u(t) = f_1(x(t))$, из условия 1 следует, что период последовательности $(x(t) : t \in \mathbb{N})$ равен 2^n. Тогда по [10, утверждение 6.2, п. 1] получаем, что период последовательности $\big((x(t), y(t)) : t \in \mathbb{N}\big)$ равен $\mathrm{НОК}(2^n, 2^{n+m}) = 2^{n+m}$, т. е. отображение ψ_G — полноцикловая подстановка. ■

Утверждение 5. Если генератор G удовлетворяет условиям утверждения 4 и вес функции f_2 нечётный, то период генератора равен 2^{n+m}.

Доказательство. Обозначим: $k = \mathrm{wt}(f_1)$; N — количество единиц в отрезке $z = z(1)z(2)\ldots z(2^{n+m})$; π — период этой последовательности; N_0 и N_1 — веса подфункций $f_2(0, y)$ и $f_2(1, y)$ соответственно. Из условия и формул (1) и (2) следует, что k нечётно; из того, что нечётен вес $\mathrm{wt}(f_2) = N_0 + N_1$, заключаем, что числа N_0 и N_1 имеют разную чётность.

Период последовательности $\big((x(t), y(t)) : t \in \mathbb{N}\big)$ равен 2^{n+m} (следует из утверждения 4). Тогда ввиду $z(t) = f_2(f_1(x(t)), y(t))$ выполняется

$$N = (2^n - k)N_0 + kN_1,$$

т. е. N нечётно. По [10, утверждение 6.1, п. 2] имеем $\pi \,|\, 2^{n+m}$; при $\pi < 2^{n+m}$ период повторяется в отрезке z чётное число раз, следовательно, и число N должно быть чётным. Значит, $\pi = 2^{n+m}$. ■

Условия утверждений 4 и 5 являются достаточными, но не необходимыми для максимальности периода генератора; так, в примере 1 функция g_2 не инъективна по u и вес функции f_2 чётный, однако период генератора равен 2^{n+m}.

Пример 1. Пусть $n = 1$, $m = 2$, $g_1(x) = x \oplus 1$, $f_1(x) = x$, $x(1) = 0$, $y(1) = 00$, функции g_2 и f_2 заданы табл. 1 и 2.

Таблица 1
Функция g_2

$u(t)$	$y(t)$			
	00	01	10	11
0	01	10	11	00
1	01	10	00	11

Таблица 2
Функция f_2

$u(t)$	$y(t)$			
	00	01	10	11
0	0	1	0	0
1	0	0	1	0

Тогда $(u(t) : t = 1, 2) = (0, 1)$, $(y(t) : t = 1, \ldots, 8) = (00, 01, 10, 11, 11, 00, 01, 10)$, $G_u = (00, 10, 11, 01)$ — полноцикловая; $(z(t) : t \in \mathbb{N}) = 00000011\ldots$ — периодическая с периодом $8 = 2^{n+m}$.

5. Построение генераторов максимального периода

Утверждение 6. Если $\mathrm{wt}(f_1) = k$ — нечётное число, то для любых $n, m \geqslant 1$ существуют такие функции g_1, g_2, f_2, что период генератора G равен 2^{n+m}.

Доказательство. Сопоставим векторам $x \in \mathbb{F}_2^n$ и $y \in \mathbb{F}_2^m$ числа из $\mathbb{Z}_{2^n}$ и $\mathbb{Z}_{2^m}$, двоичными представлениями которых они являются, и определим функции

$$g_1(x) = (x + 1) \bmod 2^n, \quad g_2(u, y) = (y + u) \bmod 2^m, \quad f_2(u, y) = \mathbb{I}[y = 0],$$

где $\mathbb{I}$ — функция-индикатор. Отметим, что g_1 и g_2^1 являютя полноцикловыми подстановками, g_2^0 — тождественное отображение. Пусть, без ограничения общности, $y(1) = 0$ и, следовательно, $z(1) = 1$; период генератора G (последовательности $(z(t) : t \in \mathbb{N})$) обозначим через π.

По построению $z(t) = z(t + 2^{n+m})$, $t \in \mathbb{N}$. Тогда $\pi = 2^p$ для $p \leqslant n + m$; $z(1 + 2^p) = 1$, а значит,

$$y(1 + 2^p l) = 0, \quad l \in \mathbb{N}. \tag{3}$$

Поскольку за 2^n тактов работы генератора последовательность u на входе автомата A_2 пробегает значения функции f_1 на всех наборах, имеем $y(1 + 2^n) = k \bmod 2^m$ и $y(1 + 2^n) \neq 0$ ввиду нечётности k.

Если $p < n$, то $y(1 + 2^n) = y(1 + 2^p 2^{n-p}) = 0$ по (3) — противоречие.

Если $p > n$, то $y(1 + 2^p) = y(1 + 2^n 2^{p-n}) = 2^{p-n}k = 0 \bmod 2^m$, что невозможно при нечётном k и $p < n + m$. Следовательно, $\pi = 2^{n+m}$. ■

Замечание 1. Для функции f_2, построенной в доказательстве утверждения 6, не выполнены условия утверждения 5, так как $\mathrm{wt}(f_2) = 2$ — чётное число.

Утверждения 1 (п. 1) и 3 (п. 2) задают необходимые требования к автомату A_1 для построения генератора максимального периода. Для функции переходов g_2 автомата A_2 должны выполняться условия 2 и 3 утверждения 4, при этом условие 2 зависит от выходной последовательности автомата A_1. Опишем способ построения такой функции g_2, что условия утверждения 4 выполнены для любого автомата A_1, удовлетворяющего необходимым условиям.

Утверждение 7. Пусть функция $g_2(u, y) : \mathbb{F}_2 \times \mathbb{F}_2^m \to \mathbb{F}_2^m$ такова, что g_2^0 — полноцикловая подстановка, g_2^1 — любая её чётная степень (или наоборот). Тогда:

1) функция $g_2(u, y)$ инъективна по u;
2) композиция $G_u = g_2^{u(1)} \circ \ldots \circ g_2^{u(2^n)}$ — полноцикловая подстановка для любой последовательности $u = u(1) \ldots u(2^n)$ нечётного веса.

Доказательство. Как и при доказательстве утверждения 6, будем отождествлять векторы $y \in \mathbb{F}_2^m$ и числа из $\mathbb{Z}_{2^m}$. Пусть, без ограничения общности, $g_2^0(y) = (y+1) \bmod 2^m$ и $g_2^1 = (g_2^0)^l$, l — чётное. Тогда $g_2^1(y) = (y+l) \bmod 2^m$.

1) При чётном l для любого $y \in \mathbb{F}_2^m$ имеем

$$g_2(0, y) = (y+1) \bmod 2^m \neq (y+l) \bmod 2^m = g_2(1, y).$$

Следовательно, функция $g_2(u, y)$ инъективна по u.

2) Пусть последовательность u содержит k единиц. Тогда $G_u = (g_2^0)^s$, где $s = 2^n - k + lk$ — нечётное в силу чётности l и нечётности k. Рассмотрим r-ю степень этой подстановки: $G_u^r = (g_2^0)^{sr}$; и уравнение $G_u^r(y) = y$:

$$G_u^r(y) = y + sr = y \pmod{2^m},$$

которое верно только при $r = 0 \pmod{2^m}$. Следовательно, G_u — полноцикловая. ■

Из утверждений 4, 5 и 7 получаем метод построения генератора G, имеющего максимальный период (алгоритм 1).

Алгоритм 1. Построение генератора G максимального периода

Вход: $n, m \in \mathbb{N}$.
Выход: функции переходов и выходов автоматов A_1 и A_2.
Выбрать:
1: $g_1 : \mathbb{F}_2^n \to \mathbb{F}_2^n$ — произвольная полноцикловая подстановка;
2: $f_1 : \mathbb{F}_2^n \to \mathbb{F}_2$ — произвольная функция нечётного веса;
3: $g_2^0 : \mathbb{F}_2^m \to \mathbb{F}_2^m$ — произвольная полноцикловая подстановка;
g_2^1 — любая её чётная степень (или наоборот);
4: $f_2 : \mathbb{F}_2^{m+1} \to \mathbb{F}_2$ — произвольная функция нечётного веса.

Алгоритм 1, очевидно, не обладает свойством полноты (с его помощью нельзя построить все возможные генераторы максимального периода), поскольку условия, на которые он опирается, не являются необходимыми. Однако, если не фиксировать значения n и m, то для любой двоичной последовательности, период которой равен степени двойки, можно предложить генератор, выдающий её.

Утверждение 8. Для любых $l \geqslant 2$ и $z = z(1) \ldots z(2^l) \in \mathbb{F}_2^l$ существует двухкаскадный конечно-автоматный генератор, выходная последовательность которого равна $z \cdot z \cdot \ldots$ (здесь «$\cdot$» — операция конкатенации).

Доказательство. Опишем способ построения генератора G.

Положим $n = 1$, $m = l - 1$; как и прежде, будем отождествлять векторы из $\mathbb{F}_2^m$ и числа из $\mathbb{Z}_{2^m}$. Зададим функции автомата A_1 как $g_1(x) = x \oplus 1$, $f_1(x) = x$, начальное состояние $x(0) = 0$; тогда на вход автомата A_2 поступит последовательность $u = 010101 \ldots$

Определим функцию $g_2(u, y) = (y + u) \bmod 2^m$ и начальное состояние $y(0) = 0$. Тогда пара «вход/состояние» автомата A_2 за первые 2^l шагов будет пробегать значения

$$(0,0),\ (1,0),\ (0,1)\ (1,1),\ \ldots,\ (0, 2^m - 1),\ (1, 2^m - 1).$$

Для получения последовательности z на выходе генератора осталось положить $f_2(0, y) = z(2y + 1)$ и $f_2(1, y) = z(2y + 2)$, $y = 0, 1, \ldots, 2^m - 1$. ■

Замечание 2. Если последовательность z в утверждении 8 апериодична, то способом, описанным в его доказательстве, получим генератор максимального периода.

Заключение

Рассмотрены условия, при которых двухкаскадный конечно-автоматный генератор имеет максимальный период; дополнен список необходимых условий и получены некоторые достаточные, на основании которых предложен простой метод построения такого генератора. Однако найденные необходимые условия не являются достаточными и наоборот, т. е. критерий максимальности периода генератора не сформулирован.

Некоторые из результатов работы докладывались на конференции SIBECRYPT'24, их краткое изложение можно найти в [13].

ЛИТЕРАТУРА

1. *Агибалов Г. П.* Криптоавтоматы с функциональными ключами // Прикладная дискретная математика. 2017. № 36. С. 59–72.
2. *Watanabe D., Furuya S., Yoshida H., et al.* A new keystream generator MUGI // LNCS. 2002. V. 2365. P. 179–194.
3. *Joux A. and Muller F.* Loosening the KNOT // LNCS. 2003. V. 2887. P. 87–99.
4. *Закревский А. Д.* Метод автоматической шифрации сообщений // Прикладная дискретная математика. 2009. № 2(4). С. 127–137.
5. *Tao R.* Finite Automata and Application to Cryptography. TSINGHUA University Press, 2009. 406 p.
6. *Агибалов Г. П., Панкратова И. А.* О двухкаскадных конечно-автоматных криптографических генераторах и методах их криптоанализа // Прикладная дискретная математика. 2017. № 35. С. 38–47.
7. *Боровкова И. В., Панкратова И. А., Семенова Е. В.* Криптоанализ двухкаскадного конечно-автоматного генератора с функциональным ключом // Прикладная дискретная математика. 2018. № 42. С. 48–56.
8. *Обухов П. К., Панкратова И. А.* Периодические свойства конечно-автоматного генератора // Прикладная дискретная математика. Приложение. 2023. № 16. С. 141–143.
9. *Кострикин А. И.* Введение в алгебру. Ч. 1: Основы алгебры: учебник для вузов. М.: Физматлит, 2000. 272 с.
10. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
11. *Idrisova V. A., Tokareva N. N., Gorodilova A. A., et al.* Mathematical problems and solutions of the Ninth International Olympiad in Cryptography NSUCRYPTO // Прикладная дискретная математика. 2023. № 62. С. 29–54.
12. `https://nsucrypto.nsu.ru/`
13. *Прудников Е. С.* Конечно-автоматные генераторы максимального периода // Прикладная дискретная математика. Приложение. 2024. № 17. С. 152–154.

REFERENCES

1. *Agibalov G. P.* Kriptoavtomaty s funktsional'nymi klyuchami [Cryptautomata with functional keys]. Prikladnaya Diskretnaya Matematika, 2017, no. 36, pp. 59–72. (in Russian)
2. *Watanabe D., Furuya S., Yoshida H., et al.* A new keystream generator MUGI. LNCS, 2002, vol. 2365, pp. 179–194.

3. *Joux A. and Muller F.* Loosening the KNOT. LNCS, 2003, vol. 2887, pp. 87–99.
4. *Zakrevskiy A. D.* Metod avtomaticheskoy shifratsii soobshcheniy [The method for messages automatic encryption]. Prikladnaya Diskretnaya Matematika, 2009, no. 2(4), pp. 127–137. (in Russian)
5. *Tao R.* Finite Automata and Application to Cryptography. TSINGHUA University Press, 2009. 406 p.
6. *Agibalov G. P. and Pankratova I. A.* O dvukhkaskadnykh konechno-avtomatnykh kriptograficheskikh generatorakh i metodakh ikh kriptoanaliza [About 2-cascade finite automata cryptographic generators and their cryptanalysis]. Prikladnaya Diskretnaya Matematika, 2017, no. 35, pp. 38–47. (in Russian)
7. *Borovkova I. V., Pankratova I. A., and Semenova E. V.* Kriptoanaliz dvukhkaskadnogo konechno-avtomatnogo generatora s funktsional'nym klyuchom [Cryptanalysis of 2-cascade finite automata generator with functional key]. Prikladnaya Diskretnaya Matematika, 2018, no. 42, pp. 48–56. (in Russian)
8. *Obukhov P. K. and Pankratova I. A.* Periodicheskie svoystva konechno-avtomatnogo generatora [Periodic properties of a finite automaton generator]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2023, no. 16, pp. 141–143. (in Russian)
9. *Kostrikin A. I.* Vvedenie v algebru. Ch. 1: Osnovy algebry [Introduction to Algebra. P. 1: Fundamentals of Algebra. Textbook for Universities.] Moscow, Fizmatlit Publ., 2000. 272 p. (in Russian)
10. *Fomichev V. M.* Metody diskretnoy matematiki v kriptologii [Methods of Discrete Mathematics in Cryptology]. Moscow, Dialog-MIFI Publ., 2010. 424 p. (in Russian)
11. *Idrisova V. A., Tokareva N. N., Gorodilova A. A., et al.* Mathematical problems and solutions of the Ninth International Olympiad in Cryptography NSUCRYPTO. Prikladnaya Diskretnaya Matematika, 2023, no. 62, pp. 29–54.
12. `https://nsucrypto.nsu.ru/`
13. *Prudnikov E. S.* Konechno-avtomatnye generatory maksimal'nogo perioda [Finite-state generators with maximal period]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2024, no. 17, pp. 152–154. (in Russian)