О. А. Козлитин, Параллельная декомпозиция неавтономных 2-линейных регистров сдвига,
Матем. вопр. криптогр., 2011, том 2, выпуск 3, 5–29

МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2011 Т. 2 № 3 С. 5–29

УДК: 512.62

Параллельная декомпозиция неавтономных 2-линейных регистров сдвига

О. А. Козлитин

ООО «Центр сертификационных исследований», Москва

Получено 10.V.2011

В статье рассматривается один из вариантов декомпозиции неавтономного 2-линейного регистра сдвига над кольцом Галуа. Показано, что неавтономный 2-линейный регистр сдвига над конечным полем представляется параллельным соединением регистров сдвига с неравномерным движением. Это позволяет применить к обсуждаемому узлу метод встречных атак, существенно снижающий оценку его криптографической стойкости.

Ключевые слова: 2-линейные регистры сдвига, регистры сдвига с неравномерным движением, кольца Галуа, конечные поля

Parallel decomposition of nonautonomous 2-linear shift registers

O. A. Kozlitin

LLC Certification Research Center, Moscow

Abstract. A variant of decomposition of nonautonomous 2-linear shift register over the Galois field is considered. It is shown that a nonautonomous 2-linear shift register over the finite field may be represented as a parallel system of clock-controlled shift registers. By means of this construction and the meet-in-the-middle attack the estimate of the cryptographic security of the register considered is lowered considerably.

Key words: 2-linear shift registers, clock-controlled shift registers, Galois ring, finite field

Citation: *Mathematical Aspects of Cryptography*, 2011, vol. 2, no. 3, pp. 5–29 (Russian).

Работа выполнена при поддержке гранта Президента РФ НШ-4.2010.10

1. Введение

Работа посвящена развитию одного из современных направлений теоретической криптографии — построению генераторов псевдослучайных последовательностей (ПСП) на основе так называемых *многомерных регистров сдвига* (*мультирегистров*). Многомерные регистры являются обобщением обыкновенных регистров: накопитель мультирегистра представляет собой многомерную фигуру («диаграмму Ферре»). На международных конкурсах последних лет отмечалось появление генераторов, использующих подобные узлы.

Впервые многомерный (точнее, двумерный) регистр сдвига возник в работе Nomura и Fukuda в 1971 г. [15]. Начиная с середины 90-х гг. проблему использования многомерных регистров сдвига в криптографии разрабатывают А. С. Кузьмин, В. Л. Куракин, А. А. Нечаев, А. В. Михалев и др. (см., например, [7, 11] и [13]). В частности, в работе [11] высказывалась мысль о возможности применения мультирегистров для построения нового класса криптографических генераторов. Были выделены два направления дальнейших исследований: использование мультирегистров в качестве *фильтрующих генераторов* [12] и при синтезе *узлов усложнения.*

По первому направлению необходимо отметить результаты А. С. Кузьмина, В. Л. Куракина и А. А. Нечаева (см., например, [7] и [8]), обобщающие на многомерный случай понятия периода линейного регистра сдвига и ранга линейной рекуррентной последовательности. Применение мультирегистра в качестве фильтрующего генератора подразумевает получение с его помощью одномерной ПСП, например, с использованием *автоматной модели* мультирегистра сдвига, предложенной А. А. Нечаевым в работе [11]. Возникающий при этом вопрос о связи свойств мультипоследовательности, вырабатываемой многомерным регистром, со свойствами выходной последовательности его автоматной модели изучен пока лишь в простейших случаях (см. [5] и [6]).

Второе направление — синтез узлов усложнения на основе мультирегистров — предполагает установление связей между свойствами входной (управляющей) последовательности, последовательности состояний и выходной последовательности неавтономного многомерного регистра сдвига. Насколько известно автору, эти вопросы в литературе не рассматривались.

Целью настоящей работы является развитие второго направления. Показано, что при определенных ограничениях неавтономный 2-линейный регистр сдвига (2-ЛРС) над кольцом Галуа R представляется параллельным соединением так называемых элементарных 2-ЛРС над некоторым расширением S кольца R (теорема 1). В случае поля элементарные 2-ЛРС изо-

морфны регистрам сдвига с неравномерным движением (теорема 4). Предложенная параллельная декомпозиция позволяет применить метод встречных атак [1], существенно снижающий трудоемкость восстановления начального заполнения регистра по входу и выходу в сравнении с методом тотального опробования.

2. Полилинейный регистр сдвига и его автоматная модель

Напомним некоторые понятия и обозначения из работ [5, 11] и [13].

Пусть $k \geq 1$. Любое конечное множество $\mathfrak{F} \subseteq \mathbb{N}_0^k$ назовем *полиэдром*. На множестве $\mathbb{N}_0^k$ рассмотрим покоординатное отношение «$\geq$»: для $\mathbf{i} = (i_0, i_1, \ldots, i_{k-1})$ и $\mathbf{j} = (j_0, j_1, \ldots, j_{k-1})$ будем писать $\mathbf{i} \geq \mathbf{j}$, если

$$\forall\, s \in \{0, 1, \ldots, k-1\}\colon i_s \geq j_s.$$

Полиэдр $\mathfrak{F}$ назовем *диаграммой Ферре, если для любых векторов* $\mathbf{i} \in \mathfrak{F}$ и $\mathbf{j} \in \mathbb{N}_0^k$ из того, что $\mathbf{i} \geq \mathbf{j}$, следует, что $\mathbf{j} \in \mathfrak{F}$.

Для всякого $s \in \mathbb{Z}_k$ положим $\mathbf{1}_s = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{N}_0^k$, где единице предшествуют s нулей. *Границей* диаграммы Ферре $\mathfrak{F}$ *по направлению* s назовем множество

$$\Delta_s(\mathfrak{F}) = (\mathbf{1}_s + \mathfrak{F}) \setminus \mathfrak{F}.$$

Полной границей диаграммы Ферре назовем множество

$$\Delta\mathfrak{F} = \bigcup_{s=0}^{k-1} \Delta_s(\mathfrak{F}).$$

Пусть R — коммутативное кольцо с единицей 1, $\mathfrak{F}$ — диаграмма Ферре, $\Omega = R^{\mathfrak{F}}$ — множество всех функций, заданных на $\mathfrak{F}$ и принимающих значения в R. Очевидно, Ω является левым модулем над R. Поэтому можно говорить о *линейных функциях*, заданных на Ω и принимающих значения в R.

Каждому $\mathbf{j} \in \Delta\mathfrak{F}$ сопоставим линейную функцию $r_{\mathbf{j}}\colon \Omega \to R$, а всякому $s \in \mathbb{Z}_k$ – преобразование φ_s множества Ω:

$$\forall\, \omega \in \Omega,\ \mathbf{j} \in \mathfrak{F}\colon \varphi_s(\omega)(\mathbf{j}) = \begin{cases} \omega(\mathbf{j} + \mathbf{1}_s), & \text{если} \quad \mathbf{j} + \mathbf{1}_s \in \mathfrak{F}, \\ r_{\mathbf{j}}\,(\omega[\mathfrak{F}]), & \text{если} \quad \mathbf{j} + \mathbf{1}_s \in \Delta\mathfrak{F}. \end{cases} \tag{1}$$

Обозначим $\mathcal{R} = \{r_{\mathbf{j}} \mid \mathbf{j} \in \Delta\mathfrak{F}\}$. Если выполняется соотношение

$$\forall\, s, t \in \mathbb{Z}_k\colon \varphi_s \cdot \varphi_t = \varphi_t \cdot \varphi_s, \tag{2}$$

где « $\cdot$ » — операция умножения отображений, то пара $(\mathcal{R}, \mathfrak{F})$ называется (коммутативным) *k-линейным регистром сдвига* (или *полилинейным регистром сдвига*, или линейным *мультирегистром сдвига*). Если соотношение (2) не выполняется, то пару $(\mathcal{R}, \mathfrak{F})$ называют *некоммутативным* линейным мультирегистром сдвига [9].

В [4] найдены условия на коэффициенты системы линейных функций $r_{\mathbf{j}}$, необходимые и достаточные для выполнения равенства (2). Они позволяют эффективно реализовать *автоматную модель* полилинейного регистра сдвига, предложенную в работе [11]. Опишем ее.

Каждому мультирегистру сдвига $(\mathcal{R}, \mathfrak{F})$ можно сопоставить конечный неавтономный автомат $\mathfrak{A}$ с множеством состояний Ω, входным алфавитом $\mathbb{Z}_k$, выходным алфавитом R, множеством частичных функций перехода $\Phi = \{\varphi_0, \varphi_1, \ldots, \varphi_{k-1}\}$ и некоторой линейной функцией выхода $\psi\colon \Omega \to R$. В алгебраической теории автоматов такой автомат принято [3] коротко обозначать

$$\mathfrak{A} = (\Omega, \mathbb{Z}_k, R, \Phi, \psi). \tag{3}$$

Автомат $\mathfrak{A}$ называется *автоматной моделью* мультирегистра $(\mathcal{R}, \mathfrak{F})$, или *неавтономным k-линейным регистром сдвига* (неавтономным k-ЛРС).

Обозначим через $e_{i,j}$ *матричную единицу*, т. е. $m \times m$-матрицу, где на пересечении строки i и столбца j стоит 1, а на остальных местах — 0 (счет строк и столбцов здесь начинается с нуля). Базис

$$e_{0,0}, \ldots, e_{0,m-1}, e_{1,0}, \ldots, e_{1,m-1}, \ldots, e_{m-1,0}, \ldots, e_{m-1,m-1}$$

R-бимодуля $R_{m,m}$ будем записывать столбцом и обозначать $e^{\downarrow}$. Всякому унитарному многочлену

$$F(x) = x^m - f_{m-1}x^{m-1} - f_{m-2}x^{m-2} - \cdots - f_1 x - f_0$$

сопоставим матрицу

$$S(F) = \begin{pmatrix} 0 & \cdots & 0 & 0 & f_0 \\ 1 & \cdots & 0 & 0 & f_1 \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 & f_{m-2} \\ 0 & \cdots & 0 & 1 & f_{m-1} \end{pmatrix}.$$

Такая матрица называется *сопровождающей* для $F(x)$ (см., например, [2]).

Пусть $n \in \mathbb{N}$, p — простое число, $q = p^r$. Всюду далее $R = GR(q^n, p^n)$ — кольцо Галуа мощности q^n и характеристики p^n, диаграмма Ферре $\mathfrak{F} \subset \mathbb{Z}^2$ — прямоугольник

$$\mathfrak{F} = \{0, 1, \ldots, m_0 - 1\} \times \{0, 1, \ldots, m_1 - 1\},$$

а частичные функции перехода φ_0 и φ_1 определены равенствами

$$\varphi_0(z) = \vec{z} \cdot (S(F_0) \otimes E) \cdot e^{\downarrow}, \qquad \varphi_1(z) = \vec{z} \cdot (E \otimes S(F_1)) \cdot e^{\downarrow}, \tag{4}$$

где $\vec{z}$ — строка координат матрицы z в базисе из матричных единиц, F_0 и F_1 — унитарные реверсивные многочлены над R степеней m_0 и m_1 соответственно, $S(F_0)$ и $S(F_1)$ — их сопровождающие матрицы, $\otimes$ — операция *тензорного* (*кронекерова*) *умножения* матриц, E — единичная матрица (соответствующих размеров). Следуя [5], будем называть такие автоматы *прямоугольными 2-линейными регистрами сдвига с элементарными характеристическими многочленами* (*э. х. м.*) F_0 *и* F_1.

Функционирование прямоугольного 2-ЛРС можно пояснить следующим образом. Пусть отображение $\mu\colon \mathbb{N}_0^2 \to R$ таково, что $\mu[\mathfrak{F}] = \omega(0)$, и в таблице

$\mu(0,0)$	$\mu(0,1)$	$\mu(0,2)$	$\ldots$	$\mu(0,j)$	$\ldots$
$\mu(1,0)$	$\mu(1,1)$	$\mu(1,2)$	$\ldots$	$\mu(1,j)$	$\ldots$
$\mu(2,0)$	$\mu(2,1)$	$\mu(2,2)$	$\ldots$	$\mu(2,j)$	$\ldots$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
$\mu(i,0)$	$\mu(i,1)$	$\mu(i,2)$	$\ldots$	$\mu(i,j)$	$\ldots$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$

каждый столбец есть линейная рекуррентная последовательность (ЛРП) с характеристическим многочленом F_0, а каждая строка — ЛРП с характеристическим многочленом F_1. Такая таблица называется *2-линейной рекуррентной последовательностью* (2-ЛРП) с э. х. м. F_0 и F_1 (см., например, [7]). По таблице под действием двоичной управляющей последовательности δ движется прямоугольное окно размерами $m_0 \times m_1$: если очередной знак $\delta(i)$ равен 0, то окно сдвигается на один шаг вниз, а если 1, то на один шаг вправо (в начальный момент времени окно располагается в левом верхнем углу таблицы). Текущее заполнение окна считается текущим заполнением регистра, а значение функции ψ от текущего заполнения окна — очередным знаком выходной ПСП.

В ситуации, когда $F_0(x) = F_1(x) = F(x)$ — многочлен максимального периода, прямоугольный 2-ЛРС $\mathfrak{A}$ изоморфен параллельному соединению так называемых элементарных 2-ЛРС. Об этом — следующий параграф.

3. Теорема о декомпозиции

Всюду в этом параграфе $F_0(x) = F_1(x) = F(x) \in R[x]$ — многочлен максимального периода степени $m \geq 2$.

Пусть $S = GR(q^{mn}, p^n)$. Положим

$$\Gamma(S) = \{x \in S \colon x^{q^m} = x\}.$$

Имеет место следующее *p-адическое разложение* всякого элемента $a \in S$:

$$a = a_0 + pa_1 + p^2 a_2 + \cdots + p^{n-1} a_{n-1},$$

где $a_i \in \Gamma(S)$ для $i \in \{0, 1, \ldots, n-1\}$. Рассмотрим автоморфизм φ кольца S, определенный равенством

$$\forall\, a \in S \colon \varphi(a) = \sum_{i=0}^{n-1} p^i a_i^q.$$

Тогда группа $\mathrm{Aut}(S/R)$ автоморфизмов кольца S, оставляющих элементы кольца R неподвижными, порождена автоморфизмом φ:

$$\mathrm{Aut}(S/R) = \langle \varphi \rangle.$$

Очевидно, $\operatorname{ord} \varphi = m$. Автоморфизм φ называют *автоморфизмом Фробениуса*.

Если θ — корень многочлена $F(x)$ в кольце $S = R[\theta]$, то

$$F(x) = (x - \varphi^0(\theta))(x - \varphi^1(\theta)) \ldots (x - \varphi^{m-1}(\theta)),$$

где φ^0 — тождественное преобразование, $\varphi^j = \varphi \cdot \varphi \cdot \cdots \cdot \varphi$ (j раз). При этом

$$S(F) \approx \operatorname{diag}(\varphi^0(\theta), \varphi^1(\theta), \ldots, \varphi^{m-1}(\theta)),$$

где $\approx$ — отношение подобия матриц.

Рассмотрим характеристический многочлен $\chi(x)$ матрицы $S(F) \otimes \otimes S(F)^{-1}$

$$\chi(x) = \prod_{i=0}^{m-1} \prod_{j=0}^{m-1} (x - \varphi^i(\theta) \cdot \varphi^j(\theta^{-1})). \tag{5}$$

Для элементов $a, b \in S$ будем писать $a \sim b$, если они лежат на одном цикле преобразования φ. Имеем

$$\varphi^i(\theta) \cdot \varphi^j(\theta^{-1}) = \varphi^j(\varphi^{i-j}(\theta)\theta^{-1}) \sim \varphi^{i-j}(\theta)\theta^{-1}. \tag{6}$$

Для всякого $j \in \{0, 1, \ldots, m-1\}$ положим $\vartheta_j = \varphi^j(\theta)\theta^{-1}$. Из (5) и (6) следует равенство

$$\chi(x) = \prod_{j=0}^{m-1} G_j(x), \tag{7}$$

где $G_j(x) = (x - \vartheta_j)(x - \varphi(\vartheta_j)) \ldots (x - \varphi^{m-1}(\vartheta_j)),\ j = 0, 1, \ldots, m-1$.

Унитарный многочлен $G(x) \in R[x]$ назовем *многочленом Галуа*, если результат $\overline{G}(x)$ его приведения по модулю радикала кольца R является неприводимым многочленом над полем $\overline{R} = GF(q)$.

Утверждение 1. *Многочлены $G_1(x), G_2(x), \ldots, G_{m-1}(x)$ суть попарно взаимно простые многочлены Галуа.*

Для всякого $t \in \mathbb{N}$ обозначим через $\rho_m(t)$ число со свойствами:

1. $1 \leq \rho_m(t) \leq q^m - 1$,
2. $\rho_m(t) \equiv t \pmod{q^m - 1}$.

Циклотомическим классом с представителем $x \in \{1, \ldots, q^m - 1\}$ назовем множество

$$C_m(x) = \{\rho_m(x \cdot q^i) \mid i \geq 0\}.$$

Каждому числу $a \in C_m(x)$ можно сопоставить его q-ичную запись длины m:

$$a = \sum_{i=0}^{m-1} \alpha_i q^i, \quad \alpha_i \in \{0, 1, \ldots, q-1\}, \quad i = 0, 1, \ldots, m-1.$$

Положим

$$l_q(a) = (\alpha_{m-1}, \alpha_{m-2}, \ldots, \alpha_1, \alpha_0).$$

Тогда множество $\{l_q(a) \mid a \in C_m(x)\}$ совпадает с множеством всех циклических сдвигов вектора $l_q(x)$. Отсюда следует, что для чисел $i, j \in \{1, 2, \ldots, m-1\}$ верна эквивалентность

$$C_m(q^i - 1) = C_m(q^j - 1) \Leftrightarrow i = j. \tag{8}$$

Теперь докажем утверждение 1.

Доказательство. Пусть $j \in \{1, 2, \ldots, m-1\}$. Для всякого $a \in S$ обозначим через $\overline{a}$ результат приведения a по модулю радикала кольца S. Тогда имеет место следующее разложение многочлена $\overline{G}_j(x)$ над полем $\overline{S} = GF(q^m)$:

$$\overline{G}_j(x) = (x - \overline{\vartheta}_j)(x - \overline{\vartheta}_j^{\,q}) \ldots (x - \overline{\vartheta}_j^{\,q^{m-1}})).$$

Чтобы доказать неприводимость $\overline{G}_j(x)$ над $\overline{R}$, достаточно показать, что длина цикла автоморфизма $\overline{\varphi}(x) = x^q$, на котором лежит вектор $\overline{\vartheta}_j$, равна m. От противного: пусть существует $k \in \{1, 2, \ldots, m-1\}$, такое, что $\overline{\vartheta}_j^{\,q^k} = \overline{\vartheta}_j$. Так как $\overline{\vartheta}_j = \overline{\theta}^{\,q^j - 1}$ и $\operatorname{ord} \overline{\theta} = q^m - 1$, имеем

$$q^k(q^j - 1) \equiv q^j - 1 \,(\operatorname{mod} q^m - 1).$$

Следовательно, циклический сдвиг на k шагов влево оставляет вектор $l_q(q^j - 1)$ неподвижным, что, очевидно, неверно. Итак, многочлен $\overline{G}(x)$ неприводим над $\overline{R}$.

Пусть теперь $1 \leq i < j \leq m-1$. Докажем, что $\overline{G}_i(x) \neq \overline{G}_j(x)$ (и, следовательно, $G_i(x)$ взаимно прост с $G_j(x)$). Достаточно показать, что $\overline{\vartheta}_i$ и $\overline{\vartheta}_j$ лежат на разных циклах автоморфизма $\overline{\varphi}$. От противного: пусть

$$\exists\, k \in \{0, 1, \ldots, m-1\} \colon \overline{\vartheta}_i^{\,q^k} = \overline{\vartheta}_j.$$

Тогда $q^k(q^i - 1) \equiv q^j - 1 \,(\operatorname{mod} q^m - 1)$, т. е.

$$C_m(q^i - 1) = C_m(q^j - 1).$$

Отсюда согласно (8) имеем $i = j$. Противоречие. □

Пусть автоморфизм σ R-бимодуля $R_{m,m}$ определен равенством

$$\sigma = \varphi_0 \cdot \varphi_1^{-1}. \tag{9}$$

Согласно (4) имеем

$$\sigma(z) = \vec{z} \cdot (S(F) \otimes S(F)^{-1}) \cdot e^{\downarrow},$$

где $\vec{z}$ — строка координат матрицы z в базисе из матричных единиц. По теореме Гамильтона – Кэли $\chi(\sigma) = 0$. В силу равенства $G_0(x) = (x-1)^m$ и утверждения 1 равенство (7) индуцирует следующее разложение R-бимодуля $R_{m,m}$ в прямую сумму ядер эндоморфизмов:

$$R_{m,m} = \operatorname{Ker} G_0(\sigma) \dotplus \operatorname{Ker} G_1(\sigma) \dotplus \ \ldots \ \dotplus \operatorname{Ker} G_{m-1}(\sigma). \tag{10}$$

При этом

$$\forall\, j \in \{0, 1, \ldots, m-1\}\colon |\operatorname{Ker} G_j(\sigma)| = |R|^{\deg G_j(x)} = |R|^m. \tag{11}$$

Равенство (10), в свою очередь, порождает однозначное разложение начального заполнения $w(0)$ 2-ЛРС $\mathfrak{A}$:

$$w(0) = w_0(0) + w_1(0) + \cdots + w_{m-1}(0), \tag{12}$$

где $w_j(0) \in \operatorname{Ker} G_j(\sigma)$, $j = 0, 1, \ldots, m-1$. Легко видеть, что подмодули $\operatorname{Ker} G_j(\sigma)$ инвариантны относительно частичных функций перехода φ_0 и φ_1. Поэтому дальнейшие усилия направлены на изучение компонент $w_j(0)$ в разложении (12) матрицы $w(0)$.

Пусть $\operatorname{Tr}\colon S \to R$ — функция «след» из S в R:

$$\forall\, x \in S\colon \operatorname{Tr}(x) = \sum_{i=0}^{m-1} \varphi^i(x).$$

Всякому $j \in \{0, 1, \ldots, m-1\}$ сопоставим отображение $\pi_j\colon S \to R_{m,m}$, определенное равенством

$$\forall\, x \in S\colon \pi_j(x) = \sum_{k=0}^{m-1} \sum_{l=0}^{m-1} \operatorname{Tr}([\varphi^j(\theta)]^k \theta^l x) e_{k,l}. \tag{13}$$

Утверждение 2. *Для всякого $j \in \{0, 1, \ldots, m-1\}$ отображение π_j задает изоморфизм R-бимодулей S и $\operatorname{Ker} G_j(\sigma)$.*

Доказательство. Покажем, что π_j — мономорфизм R-бимодулей S и $R_{m,m}$. Гомоморфность отображения π_j следует из свойств функции «след». Докажем его инъективнось.

Если $x, y \in S$ и $x \neq y$, то существует такое $l \in \{0, 1, \ldots, m-1\}$, что

$$\operatorname{Tr}(\theta^l x) \neq \operatorname{Tr}(\theta^l y).$$

Но тогда в силу (13) элементы, стоящие на пересечении нулевой строки и l-го столбца матриц $\pi_j(x)$ и $\pi_j(y)$, различны. Следовательно, $\pi_j(x) \neq \pi_j(y)$.

Из инъективности π_j и равенства (11) имеем

$$|\pi_j(S)| = |S| = |R|^m = |\operatorname{Ker} G_j(\sigma)|.$$

Осталось доказать включение

$$\pi_j(S) \subseteq \operatorname{Ker} G_j(\sigma). \tag{14}$$

Пусть $x \in S$. Положим $x_0 = x$ и $x_{i+1} = \varphi^j(\theta)x_i,\ i \in \{0, 1, \ldots, m-2\}$. Тогда в силу (13) верно равенство

$$\pi_j(x) = \sum_{k=0}^{m-1}\sum_{l=0}^{m-1} \operatorname{Tr}(x_k\theta^l)e_{k,l}. \tag{15}$$

Элементы θ и $\varphi^j(\theta)$ являются корнями многочлена $F(x)$. Поэтому ввиду (4) и (15) имеем

$$\varphi_0(\pi_j(x)) = \sum_{k=0}^{m-1}\sum_{l=0}^{m-1} \operatorname{Tr}(x_k\varphi^j(\theta)\theta^l)e_{k,l} = \pi_j(x\varphi^j(\theta)), \tag{16}$$

$$\varphi_1(\pi_j(x)) = \sum_{k=0}^{m-1}\sum_{l=0}^{m-1} \operatorname{Tr}(x_k\theta\theta^l)e_{k,l} = \pi_j(x\theta). \tag{17}$$

Заменив x на $x\theta^{-1}$ и применив φ_1^{-1} к обеим частям, имеем

$$\varphi_1^{-1}(\pi_j(x)) = \pi_j(x\theta^{-1}). \tag{18}$$

Из (9), (16) и (18) следует цепочка равенств:

$$\forall\, x \in S\colon \sigma(\pi_j(x)) = \pi_j(x\varphi^j(\theta)\theta^{-1}) = \pi_j(x\vartheta_j).$$

Отсюда, пользуясь гомоморфностью π_j, получаем

$$\forall\, x \in S\colon G_j(\sigma)(\pi_j(x)) = \pi_j(xG_j(\vartheta_j)) = 0.$$

Таким образом, включение (14) доказано. □

Разложение (10) сводит изучение 2-ЛРС $\mathfrak{A}$ вида (3) к изучению его подавтоматов

$$\mathfrak{A}(j) = (\operatorname{Ker} G_j(\sigma), \mathbb{Z}_2, R, \Phi, \psi), \quad j = 0, 1, \ldots, m-1,$$

где $\operatorname{Ker} G_j(\sigma)$ — множество состояний, $\mathbb{Z}_2$ — входной алфавит, R — выходной алфавит, Φ — множество частичных функций перехода, ψ — функция выхода. Действительно, в силу линейности функции ψ автомат внутренне изоморфен 2-ЛРС $\mathfrak{A}$. Изображенную на рис. 1 схему назовем *параллельным соединением* автоматов $\mathfrak{A}(j)$, $j = 0, 1, \ldots, m-1$, а изоморфизм запишем так:

$$\mathfrak{A} \cong \mathfrak{A}(0) \,||\, \mathfrak{A}(1) \,||\, \ldots \,||\, \mathfrak{A}(m-1). \tag{19}$$

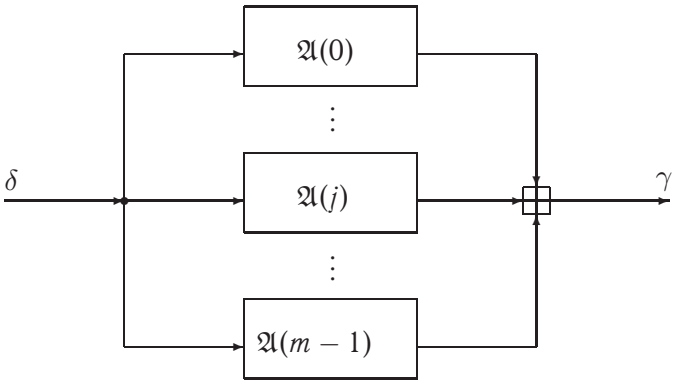

Рис. 1

Для $u, v \in S$ и функции выхода $f\colon S \to R$ рассмотрим неавтономный автомат

$$B(u, v, f) = (S, \mathbb{Z}_2, R, \{\phi_0, \phi_1\}, f), \tag{20}$$

частичные функции перехода ϕ_0 и ϕ_1 которого определены соотношением

$$\forall\, s \in \{0,1\},\ x \in S\colon \phi_s(x) = u^{1-s} \cdot x \cdot v^s.$$

Автомат (20) назовем *элементарным 2-линейным регистром сдвига*. Положим

$$\forall\, j \in \{0, 1, \ldots, m-1\}\colon \mathfrak{B}(j) = B(\varphi^j(\theta), \theta, \pi_j \cdot \psi).$$

Частичные функции перехода автомата $\mathfrak{B}(j)$ удовлетворяют соотношению

$$\forall\, s \in \{0,1\},\ x \in S\colon \phi_s(x) = \varphi^j(\theta^{1-s}) \cdot x \cdot \theta^s. \tag{21}$$

Утверждение 3. *Для всякого $j \in \{0, 1, \ldots, m-1\}$ отображение π_j задает внутренний изоморфизм автоматов $\mathfrak{B}(j)$ и $\mathfrak{A}(j)$.*

Доказательство. Выберем и зафиксируем $j \in \{0, 1, \ldots, m-1\}$. Согласно утверждению 2 отображение $\pi_j\colon S \to \operatorname{Ker} G_j(\sigma)$ биективно. Ввиду (16), (17) и (21) имеем

$$\forall\, s \in \{0,1\},\ x \in S\colon \varphi_s(\pi_j(x)) = \pi_j(\phi_s(x)).$$

Кроме того, $(\pi_j \cdot \psi)(x) = \psi(\pi_j(x))$ для всякого $x \in S$. $\square$

Рассмотрим следующее параллельное соединение элементарных 2-ЛРС:

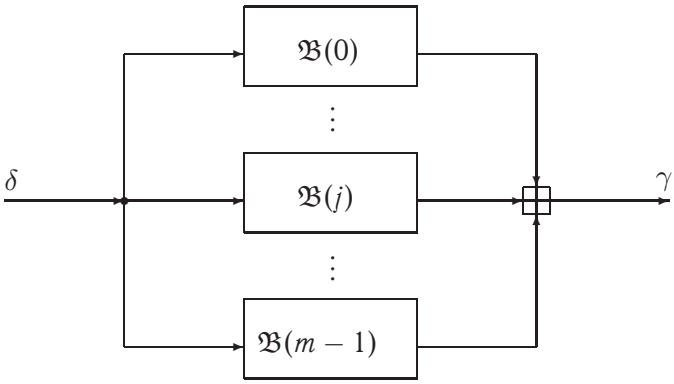

Рис. 2

Из утверждения 3 и соотношения (19) получаем цепочку внутренних изоморфизмов:

$$\mathfrak{B}(0)\,||\,\mathfrak{B}(1)\,||\,\ldots\,||\,\mathfrak{B}(m-1)\cong\mathfrak{A}(0)\,||\,\mathfrak{A}(1)\,||\,\ldots\,||\,\mathfrak{A}(m-1)\cong\mathfrak{A}. \tag{22}$$

Для всякого $j\in\{0,1,\ldots,m-1\}$ положим $\mathbf{e}_j=(0,\ldots,0,1,0,\ldots,0)\in R^m$, где единице предшествуют j нулей.

Теорема 1. *Имеет место внутренний изоморфизм*

$$\mathfrak{B}(0)\,||\,\mathfrak{B}(1)\,||\,\ldots\,||\,\mathfrak{B}(m-1)\cong\mathfrak{A}, \tag{23}$$

задающийся отображением

$$\pi\colon\ \sum_{j=0}^{m-1}x_j\mathbf{e}_j\mapsto\sum_{j=0}^{m-1}\pi_j(x_j),\quad x_j\in S,\quad j=0,1,\ldots,m-1.$$

Доказательство. Изоморфизм (23) следует из (22). Докажем, что он задается отображением π.

В силу утверждения 3 внутренний изоморфизм

$$\mathfrak{B}(0)\,||\,\mathfrak{B}(1)\,||\,\ldots\,||\,\mathfrak{B}(m-1)\cong\mathfrak{A}(0)\,||\,\mathfrak{A}(1)\,||\,\ldots\,||\,\mathfrak{A}(m-1)$$

задается отображением

$$\sum_{j=0}^{m-1}x_j\mathbf{e}_j\mapsto(\pi_0(x_0),\pi_1(x_1),\ldots,\pi_{m-1}(x_{m-1})). \tag{24}$$

Поскольку (10) есть разложение модуля состояний автомата $\mathfrak{A}$ в прямую сумму модулей состояний автоматов $\mathfrak{A}(j)$, $j = 0, 1, \ldots, m-1$, внутренний изоморфизм

$$\mathfrak{A}(0) \,||\, \mathfrak{A}(1) \,||\, \ldots \,||\, \mathfrak{A}(m-1) \cong \mathfrak{A}$$

задается отображением

$$(\pi_0(x_0), \pi_1(x_1), \ldots, \pi_{m-1}(x_{m-1})) \mapsto \sum_{j=0}^{m-1} \pi_j(x_j). \tag{25}$$

Осталось заметить, что π есть произведение отображений (24) и (25). □

Доказанная теорема позволяет представлять 2-ЛРС $\mathfrak{A}$ параллельным соединением элементарных 2-ЛРС (осуществлять его *параллельную декомпозицию*) при помощи отображения π^{-1}. Пусть теперь 2-ЛРС рассматривается как генератор ПСП, и начальное состояние $w(0)$ является его ключом. С точки зрения криптоанализа важно уметь оценивать трудоемкость применения отображений π и π^{-1}.

Теорема 2. *Отображение π^{-1} применяется за $O(m^4)$ операций сложения и умножения в кольце R. Если функция «след» протабулирована, то отображение π применяется за $O(m^4)$ операций сложения и умножения в кольце R.*

Сначала введем несколько обозначений. Базис

$$1, \theta, \theta^2, \ldots, \theta^{m-1} \tag{26}$$

R-бимодуля S можно отождествить с набором

$$[1]_F, [x]_F, [x^2]_F, \ldots, [x^{m-1}]_F$$

элементов факторкольца $R[x]/F(x)$. Поэтому базис (26) иногда называют полиномиальным. Пусть $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{m-1})$ — базис, *двойственный* к полиномиальному. Тогда если отображение $L\colon S \to R^m$ определено равенством

$$\forall\, x \in S\colon L(x) = \sum_{i=0}^{m-1} \mathrm{Tr}(x\theta^i)\mathbf{e}_i, \tag{27}$$

то обратное отображение $L^{-1}\colon R^m \to S$ удовлетворяет соотношению

$$\forall\, \mathbf{x} = \sum_{i=0}^{m-1} x_i\mathbf{e}_i \in R^m\colon L^{-1}(\mathbf{x}) = \sum_{i=0}^{m-1} x_i\varepsilon_i. \tag{28}$$

Теперь приступим к доказательству теоремы 2.

Доказательство. Пусть $A \in R_{m,m}$, и набор $(a_0, a_1, \ldots, a_{m-1}) \in S^m$ таков, что

$$\pi(a_0, a_1, \ldots, a_{m-1}) = A. \tag{29}$$

Тогда по определению отображения π

$$A = \sum_{j=0}^{m-1} \pi_j(a_j). \tag{30}$$

Выберем и зафиксируем $i, j \in \{0, 1, \ldots, m-1\}$, $x \in S$. Из (13) и (27) следует, что i-я строка матрицы $\pi_j(a_j)$ равна $L(\varphi^j(\theta^i)a_j)$. Если $\vec{A}_i$ есть i-я строка матрицы A (счет строк начинается с нуля), то в силу (30) верно равенство

$$\vec{A}_i = L\left(\sum_{j=0}^{m-1} \varphi^j(\theta^i)a_j\right).$$

Таким образом,

$$\sum_{j=0}^{m-1} [\varphi^j(\theta)]^i a_j = L^{-1}(\vec{A}_i), \quad i = 0, 1, \ldots, m-1. \tag{31}$$

Если рассматривать равенство (29) как уравнение от переменных $a_0, a_1, \ldots, a_{m-1}$, то (31) задает систему линейных уравнений (СЛУ), равносильную уравнению (29).

Исследуем СЛУ (31). Определитель матрицы этой системы есть определитель Вандермонда:

$$\left|\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} [\varphi^j(\theta)]^i e_{i,j}\right| = \prod_{0 \le l < k \le m-1} (\varphi^k(\theta) - \varphi^l(\theta)).$$

Поскольку система θ, $\varphi(\theta)$, $\ldots$, $\varphi^{m-1}(\theta)$ свободна над R, получаем, что при $l < k$ элемент $\varphi^k(\theta) - \varphi^l(\theta)$ обратим в кольце S. Следовательно, СЛУ (31) имеет единственное решение.

В силу (28) одно применение отображения L^{-1} требует $O(m)$ операций умножения элемента кольца R на элемент кольца S и $O(m)$ операций сложения в кольце S. Одна операция умножения элемента кольца R на элемент кольца S есть $O(m)$ операций умножения в R. Одна операция сложения в S есть $O(m)$ операций сложения в R. Поэтому применение L^{-1} требует $O(m^2)$

операций сложения и умножения в R. Чтобы вычислить столбец свободных коэффициентов в (31), необходимо m раз применить L^{-1}. Итак, трудоемкость вычисления столбца свободных коэффициентов составляет $m \cdot O(m^2) = O(m^3)$ операций сложения и умножения в R.

Если матрица

$$\left(\sum_{i=0}^{m-1} \sum_{j=0}^{m-1} [\varphi^j(\theta)]^i e_{i,j} \right)^{-1}$$

вычислена заранее, то трудоемкость решения системы (31) составляет $O(m^2)$ операций сложения и умножения в кольце S. Одна операция сложения в S есть $O(m)$ операций сложения в R. Одна операция умножения в S есть $O(m^2)$ операций сложения и умножения в R. Таким образом, трудоемкость решения системы (31) составляет $O(m^4)$ операций сложения и умножения в R.

Итоговая трудоемкость применения π^{-1} равна $O(m^3) + O(m^4) = O(m^4)$ операций сложения и умножения в R.

Отображение π будем применять так: сначала согласно (31) умножим матрицу на столбец $(a_0, a_1, \ldots, a_{m-1})^t$, а затем к полученному вектору покомпонентно применим L. Умножение матрицы на столбец требует $O(m^2)$ операций сложения и умножения в S, т. е. $O(m^4)$ операций сложения и умножения в R. По условию функция Tr протабулирована, поэтому в силу (27) одно применение отображения L требует $O(m)$ операций умножения в S, т. е. $O(m^3)$ операций сложения и умножения в R. Соответственно, m-кратное применение L осуществляется за $m \cdot O(m^3) = O(m^4)$ операций сложения и умножения в R. Итоговая трудоемкость применения π составляет $O(m^4)+O(m^4) = O(m^4)$ операций сложения и умножения в R. □

Итак, 2-ЛРС над кольцом Галуа эффективно представляется параллельным соединением элементарных 2-ЛРС. Этот факт позволяет построить метод восстановления начального заполнения 2-ЛРС по входной последовательности δ и выходной последовательности γ, трудоемкость которого ниже трудоемкости тотального перебора.

Пусть ключом 2-ЛРС $\mathfrak{A}$ является его начальное заполнение $w(0)$. Множество всех ключей обозначим через K. Очевидно,

$$|K| = |R_{m,m}| = q^{nm^2}.$$

Схема, изображенная на рис. 2, позволяет применить стандартный метод *встречных атак* [1, с. 255]. Этот метод снижает число перебираемых ключей с $|K|$ до $\sqrt{|K|}$. При опробовании одного ключа необходимо выработать

некоторое заранее определенное и не зависящее от m число знаков выходной последовательности. Для выработки одного знака необходимо осуществить $O(m^2)$ операций сложения и умножения в кольце R. Таким образом, трудоемкость метода встречных атак, выраженная в операциях кольца R, равна

$$O(m^2 \cdot \sqrt{|K|}) = O\Big(m^2 q^{\frac{nm^2}{2}}\Big), \quad m \to \infty.$$

Это существенно меньше трудоемкости тотального перебора, составляющей

$$O(m^2 \cdot |K|) = O\big(m^2 q^{nm^2}\big)$$

операций сложения и умножения в кольце R.

Все результаты этого параграфа были получены в ситуации, когда $F_0(x) = F_1(x)$. В случае поля это ограничение можно ослабить.

4. Параллельная декомпозиция 2-ЛРС над полем

В этом параграфе $n = 1$, т. е. $R = GF(q)$ — поле из q элементов, $S = GF(q^m)$, $\tau = q^m - 1$. Пусть F_0 и F_1 — многочлены максимального периода над R степени m, не обязательно равные, а λ и θ — их корни в S:

$$F_0(\lambda) = 0, \quad F_1(\theta) = 0.$$

Поскольку $\langle\lambda\rangle = \langle\theta\rangle = S^*$, существует такое $d \in \{1, 2, \ldots, \tau - 1\}$, что $\lambda = \theta^d$ и $(d, \tau) = 1$. Тогда имеют место равенства

$$F_1(x) = \prod_{i=0}^{m-1} (x - \varphi^i(\theta)), \quad F_0(x) = \prod_{i=0}^{m-1} (x - \varphi^i(\lambda)) = \prod_{i=0}^{m-1} (x - [\varphi^i(\theta)]^d). \quad (32)$$

Пусть $L_R(F_0, F_1)$ — множество всех 2-ЛРП с э. х. м. F_0 и F_1, $\mu \in L_R(F_0, F_1)$. Выберем и зафиксируем $l \geq 0$. Тогда существуют такие $\alpha_l \in S$ и корень λ_l многочлена F_0, что

$$\forall\, k \geq 0\colon \mu(k, l) = \mathrm{Tr}(\alpha_l \cdot \lambda_l^k).$$

В силу (32) существует такой корень θ_l многочлена F_1, что $\lambda_l = \theta_l^d$. Тогда

$$\forall\, k \geq 0\colon \mu(k, l) = \mathrm{Tr}(\alpha_l \cdot \theta_l^{dk}). \quad (33)$$

Поскольку $(d, \tau) = 1$, существует такое $t \in \{1, 2, \ldots, \tau - 1\}$, что $d \cdot t \equiv 1 \pmod{\tau}$. Рассмотрим отображение $\nu\colon \mathbb{N}_0^2 \to R$, определенное равенством

$$\forall\, k \geq 0,\ l \geq 0\colon \nu(k, l) = \mu(tk, l).$$

При фиксированном $k \geq 0$ последовательность $\nu(k, 0), \nu(k, 1), \ldots$ есть ЛРП с характеристическим многочленом F_1. С другой стороны, при всяком фиксированном $l \geq 0$ имеем

$$\forall\, k \geq 0\colon \nu(k, l) = \mathrm{Tr}(\alpha_l \cdot \theta_l^{dtk}) = \mathrm{Tr}(\alpha_l \cdot \theta_l^{k}). \tag{34}$$

Это означает, что последовательность $\nu(0, l)$, $\nu(1, l)$, $\nu(2, l)$, $\ldots$ также является ЛРП с характеристическим многочленом F_1. Итак,

$$\nu \in L_R(F_1, F_1). \tag{35}$$

Утверждение 4. *Существуют такие элементы* $a_0, a_1, \ldots, a_{m-1} \in S$, *что*

$$\forall\, k \geq 0,\ l \geq 0\colon \nu(k, l) = \sum_{j=0}^{m-1} \mathrm{Tr}([\varphi^j(\theta)]^k \theta^l a_j).$$

Доказательство. Напомним (см. параграф 2), что

$$\mathfrak{F} = \{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, m-1\}.$$

Из (10) и утверждения 2 следует существование таких элементов $a_0, a_1, \ldots, a_{m-1} \in S$, что

$$\nu[\mathfrak{F}] = \sum_{j=0}^{m-1} \pi_j(a_j).$$

Тогда в силу (13) верно равенство

$$\nu[\mathfrak{F}] = \sum_{k=0}^{m-1} \sum_{l=0}^{m-1} \sum_{j=0}^{m-1} \mathrm{Tr}([\varphi^j(\theta)]^k \theta^l a_j) e_{k,l}.$$

Расмотрим отображение $\widetilde{\nu}\colon \mathbb{N}_0^2 \to R$, определенное равенством

$$\forall\, k \geq 0,\ l \geq 0\colon \widetilde{\nu}(k, l) = \sum_{j=0}^{m-1} \mathrm{Tr}([\varphi^j(\theta)]^k \theta^l a_j).$$

Очевидно, что $\widetilde{\nu}[\mathfrak{F}] = \nu[\mathfrak{F}]$. Поскольку θ, $\varphi(\theta)$, $\varphi^2(\theta)$, $\ldots$, $\varphi^{m-1}(\theta)$ — корни многочлена F_1, имеем $\widetilde{\nu} \in L_R(F_1, F_1)$. Поэтому ввиду (35) верно равенство $\nu = \widetilde{\nu}$. $\square$

В силу (33) и (34) верно равенство

$$\forall\, k \geq 0,\ l \geq 0\colon \mu(k,l) = \nu(dk,l).$$

Отсюда по утверждению 4 имеем

$$\forall\, k \geq 0,\ l \geq 0\colon \mu(k,l) = \sum_{j=0}^{m-1} \operatorname{Tr}([\varphi^j(\theta^d)]^k \theta^l a_j) = \sum_{j=0}^{m-1} \operatorname{Tr}([\varphi^j(\lambda)]^k \theta^l a_j).$$

Поэтому

$$\mu[\mathfrak{F}] = \sum_{j=0}^{m-1}\sum_{k=0}^{m-1}\sum_{l=0}^{m-1} \operatorname{Tr}([\varphi^j(\lambda)]^k \theta^l a_j) e_{k,l} = \sum_{j=0}^{m-1} \pi'_j(a_j), \tag{36}$$

где

$$\forall\, x \in S\colon \pi'_j(x) = \sum_{k=0}^{m-1}\sum_{l=0}^{m-1} \operatorname{Tr}([\varphi^j(\lambda)]^k \theta^l x) e_{k,l}. \tag{37}$$

Поскольку $\mu \in L_R(F_0, F_1)$ было выбрано произвольно, из (36) следует равенство

$$R_{m,m} = \pi'_0(S) + \pi'_1(S) + \cdots + \pi'_{m-1}(S). \tag{38}$$

Пусть $j \in \{0, 1, \ldots, m-1\}$. Легко видеть, что отображение $\pi'_j\colon S \to$ $\to R_{m,m}$ инъективно и гомоморфно. Поэтому $\pi'_j(S)$ есть векторное пространство над R. Заметим, что пространство $\pi'_j(S)$ инвариантно относительно частичных функций перехода φ_0 и φ_1, определенных равенствами (4). Действительно, поскольку $\varphi^j(\lambda)$ — корень многочлена F_0, а θ – корень многочлена F_1, для любых $s \in \{0,1\}$, $x \in S$ имеем

$$\varphi_s(\pi'_j(x)) = \sum_{k=0}^{m-1}\sum_{l=0}^{m-1} \operatorname{Tr}([\varphi^j(\lambda)]^{k+1-s} \theta^{l+s} x) e_{k,l} = \pi'_j(\varphi^j(\lambda^{1-s}) \cdot x \cdot \theta^s). \tag{39}$$

Таким образом, (38) есть разложение пространства $R_{m,m}$ в сумму подпространств, инвариантных относительно частичных функций перехода 2-ЛРС $\mathfrak{A}$.

Утверждение 5. *Сумма* (38) *прямая.*

Доказательство. Выберем и зафиксируем $j \in \{0, 1, \ldots, m-1\}$. В силу инъективности π'_j верна цепочка равенств $|\pi'_j(S)| = |S| = |R|^m$, откуда

$$\dim \pi'_j(S) = m. \tag{40}$$

Рассмотрим векторное пространство

$$M_j = \pi'_0(S) + \cdots + \pi'_{j-1}(S) + \pi'_{j+1}(S) + \cdots + \pi'_{m-1}(S).$$

Поскольку $j \in \{0, 1, \ldots, m-1\}$ фиксировано произвольно, достаточно доказать, что

$$M_j \cap \pi'_j(S) = \{0\}.$$

По теореме Грассмана [2], а также ввиду (38) и (40) имеем

$$\dim(M_j \cap \pi'_j(S)) = \dim M_j + \dim \pi'_j(S) - \dim R_{m,m} \leq m(m-1) + m - m^2 = 0. \square$$

Итак, имеет место следующее разложение пространства $R_{m,m}$ в прямую сумму подпространств, инвариантных относительно частичных функций перехода 2-ЛРС $\mathfrak{A}$:

$$R_{m,m} = \pi'_0(S) \dotplus \pi'_1(S) \dotplus \ \ldots \ \dotplus \pi'_{m-1}(S). \tag{41}$$

Разложение (41) индуцирует параллельную декомпозицию неавтономного 2-ЛРС $\mathfrak{A}$. Рассмотрим следующие подавтоматы автомата $\mathfrak{A}$:

$$\mathcal{A}(j) = (\pi'_j(S), \mathbb{Z}_2, R, \Phi, \psi), \quad j = 0, 1, \ldots, m-1,$$

где $\pi'_j(S)$ — множество состояний, $\mathbb{Z}_2$ — входной алфавит, R — выходной алфавит, Φ — множество частичных функций перехода, ψ — функция выхода. В обозначениях §3 имеет место следующий внутренний изоморфизм:

$$\mathfrak{A} \cong \mathcal{A}(0) \,||\, \mathcal{A}(1) \,||\, \ldots \,||\, \mathcal{A}(m-1). \tag{42}$$

Для всякого $j \in \{0, 1, \ldots, m-1\}$ рассмотрим элементарный 2-ЛРС

$$\mathcal{B}(j) = B(\varphi^j(\lambda), \theta, \pi'_j \cdot \psi),$$

частичные функции перехода ϕ_0 и ϕ_1 которого определены соотношением

$$\forall\, s \in \{0,1\},\ x \in S\colon \phi_s(x) = \varphi^j(\lambda^{1-s}) \cdot x \cdot \theta^s. \tag{43}$$

В силу (39) и (43)

$$\forall\, s \in \{0,1\},\ x \in S\colon \varphi_s(\pi'_j(x)) = \pi'_j(\phi_s(x)).$$

Кроме того,

$$\forall\, x \in S\colon (\pi'_j \cdot \psi)(x) = \psi(\pi'_j(x)).$$

Таким образом, π'_j задает внутренний изоморфизм автоматов $\mathcal{B}(j)$ и $\mathcal{A}(j)$:

$$\forall\, j \in \{0,1,\dots,m-1\}\colon \mathcal{B}(j) \cong \mathcal{A}(j). \tag{44}$$

Теорема 3. *Имеет место внутренний изоморфизм*

$$\mathcal{B}(0)\,||\,\mathcal{B}(1)\,||\,\dots\,||\,\mathcal{B}(m-1) \cong \mathfrak{A}, \tag{45}$$

задающийся отображением

$$\pi'\colon \sum_{j=0}^{m-1} x_j \mathbf{e}_j \mapsto \sum_{j=0}^{m-1} \pi'_j(x_j), \quad x_j \in S, \quad j = 0,1,\dots,m-1.$$

Доказательство аналогично доказательству теоремы 1. Изоморфизм (45) следует из (42) и (44). Докажем, что он задается отображением π'.

Ввиду (44) внутренний изоморфизм

$$\mathcal{B}(0)\,||\,\mathcal{B}(1)\,||\,\dots\,||\,\mathcal{B}(m-1) \cong \mathcal{A}(0)\,||\,\mathcal{A}(1)\,||\,\dots\,||\,\mathcal{A}(m-1)$$

задается отображением

$$\sum_{j=0}^{m-1} x_j \mathbf{e}_j \mapsto (\pi'_0(x_0), \pi'_1(x_1), \dots, \pi'_{m-1}(x_{m-1})). \tag{46}$$

Поскольку (41) есть разложение пространства состояний автомата $\mathfrak{A}$ в прямую сумму пространств состояний автоматов $\mathcal{A}(j)$, $j = 0,1,\dots,m-1$, внутренний изоморфизм

$$\mathcal{A}(0)\,||\,\mathcal{A}(1)\,||\,\dots\,||\,\mathcal{A}(m-1) \cong \mathfrak{A}$$

задается отображением

$$(\pi'_0(x_0), \pi'_1(x_1), \dots, \pi'_{m-1}(x_{m-1})) \mapsto \sum_{j=0}^{m-1} \pi'_j(x_j). \tag{47}$$

Осталось заметить, что π' есть произведение отображений (46) и (47). □

Теорема 3 и теорема 1 говорят о возможности представления 2-ЛРС $\mathfrak{A}$ параллельным соединением элементарных 2-ЛРС вида (20). В обеих теоремах элементарные характеристические многочлены F_0 и F_1 являются многочленами максимального периода одной и той же степени m. Теорема 3 справедлива для 2-ЛРС над конечным полем, а теорема 1 — для 2-ЛРС над произвольным кольцом Галуа. Но в теореме 1 равенство $F_0 = F_1$ требуется, а в теореме 3 — нет.

Теорему 3 можно уточнить. С этой целью напомним еще одно понятие.

Пусть $\alpha, \beta \in \mathbb{N}$. Согласно [12] *генератором* «$\alpha - \beta$ *шагов*» с характеристическим многочленом $F_1(x)$ называется неавтономный регистр сдвига

$$\mathcal{R} = (R^m, \mathbb{Z}_2, R, H(\alpha, \beta), f), \tag{48}$$

где R^m — множество состояний, $\mathbb{Z}_2$ — входной алфавит, R — выходной алфавит, $H(\alpha, \beta) = \{h_0, h_1\}$ — набор частичных функций перехода, определенных равенством

$$\forall\, s \in \{0, 1\},\ \mathbf{x} \in R^m\colon h_s(\mathbf{x}) = \mathbf{x} \cdot S(F_1)^{(1-s)\alpha + s\beta}, \tag{49}$$

$f\colon R^m \to R$ — функция выхода. Иными словами, это обычный регистр, который при подаче 0 сдвигается на α, а при подаче 1 — на β шагов. В двоичном случае такие автоматы подробно изучены в литературе, в особенности генераторы «сто – вперёд» ($\alpha = 0,\ \beta = 1$) и «1–2 шага» (см., например, [14], [16] и [17]).

Всякому $j \in \{0, 1, \ldots, m-1\}$ сопоставим регистр

$$\mathcal{R}(j) = (R^m, \mathbb{Z}_2, R, H(q^j d, 1), f_j),$$

функция выхода f_j которого определена равенством

$$f_j = L^{-1} \cdot \pi_j' \cdot \psi. \tag{50}$$

Обозначим через L^m отображение $S^m \to R^{m^2}$, равное m-й декартовой степени отображения L:

$$L^m\left(\sum_{j=0}^{m-1} x_j \mathbf{e}_j\right) = (L(x_1), L(x_2), \ldots, L(x_m)), \quad x_j \in S, \quad j = 0, 1, \ldots, m-1.$$

Сформулируем центральный результат этого параграфа.

Теорема 4. *Пусть $F_0(x)$ и $F_1(x)$ — многочлены максимального периода степени $m \geq 2$. Тогда имеет место внутренний изоморфизм*

$$\mathfrak{A} \cong \mathcal{R}(0) \,||\, \mathcal{R}(1) \,||\, \ldots \,||\, \mathcal{R}(m-1), \tag{51}$$

задающийся отображением $[\pi']^{-1}L^m$.

Доказательство. Выберем и зафиксируем $j \in \{0, 1, \ldots, m-1\}$. Ввиду теоремы 3 достаточно показать, что отображение L задает внутренний изоморфизм автоматов $\mathcal{B}(j)$ и $\mathcal{R}(j)$. В силу равенств $\lambda = \theta^d$ (27), (43), (50) для любых $x \in S$ и $s \in \{0, 1\}$ имеем

$$L(\phi_s(x)) = L(\varphi^j(\lambda^{1-s}) \cdot x \cdot \theta^s) = L(x \cdot \theta^{(1-s)q^j d+s}) = \sum_{i=0}^{m-1} \mathrm{Tr}(x \cdot \theta^i \theta^{(1-s)q^j d+s})\mathbf{e}_i =$$

$$= \sum_{i=0}^{m-1} \mathrm{Tr}(x \cdot \theta^i)\mathbf{e}_i \cdot S(F_1)^{(1-s)q^j d+s} = L(x) \cdot S(F_1)^{(1-s)q^j d+s} = h_s(L(x)),$$

$$(\pi'_j \cdot \psi)(x) = (\pi'_j \cdot \psi)(L^{-1}(L(x))) = (L^{-1} \cdot \pi'_j \cdot \psi)(L(x)) = f_j(L(x)).$$

Гомоморфность L доказана. Биективность L уже отмечалась. □

Многочлен максимального периода над конечным полем называют также *примитивным* [10]. Из теоремы 4 следует, что всякий прямоугольный 2-линейный регистр сдвига над конечным полем с примитивными э. х. м. степени m представляется параллельным соединением m регистров сдвига с неравномерным движением.

Следующая теорема показывает, что изоморфизм $[\pi']^{-1}L^m$ и обратный к нему изоморфизм $[L^m]^{-1}\pi'$ эффективно вычислимы.

Теорема 5. *Если функция «след» протабулирована, то отображения*

$$[\pi']^{-1}L^m \quad \textit{и} \quad [L^m]^{-1}\pi'$$

применяются за $O(m^4)$ операций сложения и умножения в поле R.

Доказательство аналогично доказательству теоремы 2. Пусть $A \in$ $\in R_{m,m}$, и набор $(a_0, a_1, \ldots, a_{m-1}) \in S^m$ таков, что

$$\pi'(a_0, a_1, \ldots, a_{m-1}) = A. \tag{52}$$

Тогда по определению отображения π' имеем

$$A = \sum_{j=0}^{m-1} \pi'_j(a_j). \tag{53}$$

Выберем и зафиксируем $i, j \in \{0, 1, \ldots, m-1\}$, $x \in S$. Из (27) и (37) следует, что i-я строка матрицы $\pi'_j(a_j)$ равна $L(\varphi^j(\lambda^i)a_j)$. Если $\vec{A}_i$ есть i-я строка матрицы A (счет строк начинается с нуля), то в силу (53) верно равенство

$$\vec{A}_i = L\left(\sum_{j=0}^{m-1} \varphi^j(\lambda^i)a_j\right).$$

Таким образом,

$$\sum_{j=0}^{m-1} [\varphi^j(\lambda)]^i a_j = L^{-1}(\vec{A}_i), \quad i = 0, 1, \ldots, m-1. \tag{54}$$

Если рассматривать равенство (52) как уравнение от переменных $a_0, a_1, \ldots, a_{m-1}$, то (54) задает СЛУ, равносильную уравнению (52).

Исследуем СЛУ (54). Определитель матрицы этой системы есть определитель Вандермонда

$$\left|\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} [\varphi^j(\lambda)]^i e_{i,j}\right| = \prod_{0 \le l < k \le m-1} (\varphi^k(\lambda) - \varphi^l(\lambda)).$$

Поскольку система λ, $\varphi(\lambda)$, $\ldots$, $\varphi^{m-1}(\lambda)$ свободна над R, получаем, что при $l < k$ элемент $\varphi^k(\lambda) - \varphi^l(\lambda)$ обратим в поле S. Следовательно, СЛУ (54) имеет единственное решение.

При обосновании теоремы 2 было показано, что трудоемкость вычисления столбца свободных коэффициентов составляет $O(m^3)$ операций сложения и умножения в R. Если матрица

$$\left(\sum_{i=0}^{m-1}\sum_{j=0}^{m-1} [\varphi^j(\lambda)]^i e_{i,j}\right)^{-1}$$

вычислена заранее, то трудоемкость решения системы (54) составляет $O(m^2)$ операций сложения и умножения в S, т. е. $O(m^4)$ операций сложения и умножения в R. Итоговая трудоемкость применения отображения $[\pi']^{-1}$ равна $O(m^3) + O(m^4) = O(m^4)$ операций сложения и умножения в R.

Отображение π' будем применять так: сначала согласно (54) умножим матрицу на столбец $(a_0, a_1, \ldots, a_{m-1})^t$, а затем к полученному вектору покомпонентно применим L. Умножение матрицы на столбец требует $O(m^2)$ операций сложения и умножения в S, т. е. $O(m^4)$ операций сложения и умножения

в R. Как отмечалось при доказательстве теоремы 2, m-кратное применение L осуществляется за $O(m^4)$ операций сложения и умножения в R. Итоговая трудоемкость применения π' составляет $O(m^4) + O(m^4) = O(m^4)$ операций сложения и умножения в R.

Трудоемкость применения L^m равна трудоемкости m-кратного применения L, т. е. $O(m^4)$. Трудоемкость применения $[L^m]^{-1}$ равна трудоемкости вычисления столбца свободных коэффициентов, т. е. $O(m^3)$. □

5. Заключение

Перечислим основные результаты этой работы.

1. Для 2-ЛРС $\mathfrak{A}$ над произвольным кольцом Галуа R с одинаковыми элементарными характеристическими многочленами максимального периода степени $m \geq 2$ доказана возможность представления в виде параллельного соединения элементарных 2-ЛРС над S — расширением кольца R степени m (теорема 1).
2. Показано, что метод встречных атак [1] снижает трудоемкость восстановления начального заполнения прямоугольного 2-ЛРС по управляющей и выходной последовательностям с $O(m^2 q^{nm^2})$ до $O(m^2 q^{\frac{nm^2}{2}})$ операций в кольце R при $m \to \infty$.
3. Для любого конечного поля R результат пункта 1 обобщен на случай, когда элементарные характеристические многочлены являются многочленами максимального периода одинаковой степени $m \geq 2$, вообще говоря, различными. При этом элементарные 2-ЛРС изоморфны регистрам сдвига с неравномерным движением (теорема 4).

6. Благодарность

Автор выражает глубокую признательность профессору А. А. Нечаеву за постановку задачи, обсуждение полученных результатов и ценные замечания по тексту этой статьи.

Список литературы

1. *Бабаш А. В., Шанкин Г. П.* Криптография. — М.: Солон-Р, 2002. 512 с.
2. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. — М.: Гелиос АРВ, 2003. 749 с.
3. *Глушков В. М., Летичевский А. А.* Автоматов теория. — В кн.: Энциклопедия кибернетики, т.1. — Киев, 1975, с. 57–60.

4. *Горбатов Е. В., Нечаев А. А.* Конечные квазифробениусовы бимодули и полилинейные регистры сдвига. — В сб.: Труды по дискретной математике. Т. 9. — М.: Гелиос АРВ, 2006, с. 164–189.
5. *Козлитин О. А.* Периодические свойства простейшего 2-линейного регистра сдвига. — Дискретная математика, 2007, т. 19, вып. 3, с. 51–78.
6. *Козлитин О. А.* Свойства выходной последовательности простейшего самоуправляемого 2-линейного регистра сдвига. — Дискретная математика, 2007, т. 19, вып. 4, с. 70–96.
7. *Кузьмин А. С., Куракин В. Л., Нечаев А. А.* Псевдослучайные и полилинейные последовательности. — В сб.: Труды по дискретной математике. Т. 1. — М.: ТВП, 1997, с. 139–202.
8. *Куракин В. Л.* Линейная сложность полилинейных последовательностей. — Дискретная математика, 2001, т. 13, вып. 1, с. 3–55.
9. *Куракин В. Л.* Свободные регистры сдвига I. — В сб.: Труды по дискретной математике. Т. 9. — М.: Гелиос АРВ, 2006, с. 77–109.
10. *Лидл Р., Нидеррайтер Г.* Конечные поля. — М.: Мир, 1988. 818 с.
11. *Нечаев А. А.* Многомерные регистры сдвига и сложность мультипоследовательностей. — В сб.: Труды по дискретной математике. Т. 6. — М.: Физматлит, 2002, с. 150–164.
12. *Фомичёв В. М.* Дискретная математика и криптология. — М.: Диалог-МИФИ, 2003. 397 с.
13. *Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A.* Linear recurring sequences over rings and modules. — J. Math. Sci., 1995, v. 76, № 6, pp. 2793–2915.
14. *Beth T., Piper E.* The stop-and-go generator. — Eurocrypt'84, Lect. Notes Comput. Sci., 1985, v. 209, pp. 88–92.
15. *Nomura T., Fukuda A.* Linear recurring planes and two-dimensional cyclic codes. — Electronic Commun. Japan, 1971, v. 54, № 3, pp. 23–30.
16. *Nyffeler P.* Binary Automation und ihre linearen Rekursionen. — Ph. D. thesis, Univ. of Berne, 1975.
17. *Vogel R.* On the linear complexity of cascaded sequences. — Eurocrypt'84, Lect. Notes Comput. Sci., 1985, v. 209, pp. 99–109.