ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/22/1

УДК 519.7

ПОДСТАНОВКИ, ИНДУЦИРОВАННЫЕ РАЗРЯДНО-ИНЪЕКТИВНЫМИ ПРЕОБРАЗОВАНИЯМИ МОДУЛЯ НАД КОЛЬЦОМ ГАЛУА

А. В. Аборнев

ООО «Центр сертификационных исследований», г. Москва, Россия

E-mail: abconf.c@gmail.com

Для произвольного кольца Галуа $R = \mathrm{GR}(q^2, p^2)$, $q = p^r$, построен большой класс $m \times 2m$-матриц над R, называемых разрядно-инъективными (РИ-матрицами), которым соответствует нелинейная подстановка π на модуле R^m. В качестве криптографической характеристики таких подстановок изучаются свойства множества $\Sigma\pi$, где Σ — регулярное представление группы $(R^m, +)$ в симметрической группе $S(R^m)$. В случаях $R = \mathrm{GR}(q^2, p^2)$, $p > 2$, $m = 1$ и $R = \mathrm{GR}(q^2, 4)$, $m > 1$ описаны классы разрядно-инъективных матриц с минимально возможным показателем 2-транзитивности множества подстановок $\Sigma\pi$ равным 4. В случае $R = \mathbb{Z}_{p^2}$, $m = 1$ показано также, что группа, порождённая множеством $\Sigma\pi$, содержит знакопеременную группу подстановок.

Ключевые слова: *разрядно-инъективная матрица, РИ-матрица, подстановка, кольцо Галуа.*

Введение

Пусть $R = \mathrm{GR}(q^2, p^2)$ — кольцо Галуа с полем вычетов $\overline{R} = R/pR = \mathrm{GF}(q)$, $q = p^r$. В частности, при $r = 1$ имеем $R = \mathbb{Z}_{p^2}$. Подмножество $P = \Gamma(R) = \{a \in R : a^q = a\}$ называют *p-адическим координатным множеством* или *координатным множеством Тейхмюллера* кольца R. Будем называть его также *разрядным* множеством.

Каждый элемент $a \in R$ однозначно представляется в виде

$$a = a_0 + pa_1, \quad a_i \in P, \quad i \in \{0, 1\},$$

называемом *p-адическим разложением элемента a*. Отображения

$$\gamma_i \colon R \to P, \quad \gamma_i(a) = a_i, \quad i \in \{0, 1\},$$

будем называть *разрядными функциями в разрядном множестве* P, а элементы $a_i = \gamma_i(a)$ — *p-адическими разрядами элемента a*. Алгебра $(P, \oplus, \cdot)$ с операцией сложения $a \oplus b = \gamma_0(a + b)$, $a, b \in P$, является полем.

Понятия p-адического разложения и значения функции γ_i естественным образом (поэлементно) распространяются на матрицы $A \in R_{m \times m}$, при этом используется обозначение $A_i = \gamma_i(A)$. Так же естественным образом операции $\oplus$ и $\cdot$ распространяются на матрицы и векторы над полем P, при этом операция умножения матриц обозначается через $\odot$.

Назовём матрицу W размеров $m \times n$ над кольцом Галуа R *разрядно-инъективной* (*РИ-матрицей*), если любая ненулевая строка $\mathbf{a} \in R^m$ однозначно восстанавливается по строке $\gamma_1(\mathbf{a}W)$.

Каждой РИ-матрице соответствует эффективно реализуемая нелинейная подстановка на модуле ${}_R R^m$, определяемая равенством

$$\pi(\mathbf{x}) = \gamma_1(\mathbf{x}W)Z,$$

где $Z = (E \mid pE)^T$ — $2m \times m$-матрица над R.

В работе построен большой класс РИ-матриц вида

$$K = U(E \mid E + 2G), \tag{1}$$

где $U, G \in R_{m,m}$ — обратимые матрицы. Соответствующую матрице K подстановку на модуле R^m обозначим через π.

В качестве криптографического приложения изучается блочный шифр, реализующий подстановки из множества $(\Sigma\pi)^k$, где Σ — регулярная подгруппа группы $S(R^m)$. Изучаются следующие характеристики, определяющие криптографические свойства данного шифра:

1) показатель 2-транзитивности $d_2(\Sigma\pi)$ — минимальное k, для которого множество $(\Sigma\pi)^k$ 2-транзитивно;
2) группа, порождаемая множеством подстановок $\Sigma\pi$.

В случаях $R = \mathrm{GR}(q^2, p^2)$, $p > 2$, $m = 1$ и $R = \mathrm{GR}(q^2, 4)$, $m > 1$ описаны классы РИ-матриц с оптимальным значением показателя 2-транзитивности соответствующего множества подстановок $\Sigma\pi$, то есть минимального $k \in \mathbb{N}$, для которого множество $(\Sigma\pi)^k$ 2-транзитивно. Для кольца $R = \mathbb{Z}_{p^2}$ и циклической группы Σ показано, что группа $\langle\Sigma\pi\rangle$, порождённая множеством $\Sigma\pi$, содержит знакопеременную группу подстановок.

1. Построение разрядно-инъективных матриц

Из определения РИ-матрицы $K_{m\times n}$ следует, что её размеры должны удовлетворять условию $n \geqslant 2m$. Профессором А. А. Нечаевым предложен следующий способ построения большого класса РИ-матриц размера $m \times 2m$.

Теорема 1. Если $U_{m\times m}$ — обратимая матрица над кольцом R, $G_{m\times m}$ — обратимая матрица над полем P, то матрица $W_{m\times 2m}$ над кольцом R вида

$$W = U(E \mid E + pG) = (U \mid V) \tag{2}$$

является разрядно-инъективной.

Доказательство. Покажем, что для любой ненулевой строки $\mathbf{x} \in R^m$ по строке $\mathbf{y}$, равной

$$\mathbf{y} = \gamma_1(\mathbf{x}W), \tag{3}$$

можно однозначно восстановить строку $\mathbf{x}$.

Приведём алгоритм восстановления. Подставляя (2) в (3), получаем

$$\mathbf{y} = (\gamma_1(\mathbf{x}U) \mid \gamma_1(\mathbf{x}V)) = (\gamma_1(\mathbf{x}_0U_0) \oplus \mathbf{x}_1 \odot U_0 \oplus \mathbf{x}_0 \odot U_1 \mid \gamma_1(\mathbf{x}_0V_0) \oplus \mathbf{x}_1 \odot V_0 \oplus \mathbf{x}_0 \odot V_1). \tag{4}$$

Так как ввиду (2) справедливы равенства $V_0 = U_0$, $V_1 = U_1 \oplus (U_0 \odot G)$, то из (4) имеем

$$\gamma_1(\mathbf{x}V) \ominus \gamma_1(\mathbf{x}U) = \mathbf{x}_0 \odot U_0 \odot G.$$

Таким образом по строке $\mathbf{y}$ однозначно восстанавливается строка $\mathbf{x}_0$:

$$\mathbf{x}_0 = (\gamma_1(\mathbf{x}V) \ominus \gamma_1(\mathbf{x}U)) \odot G^{-1} \odot U_0^{-1}.$$

После этого по строке $\mathbf{y}$ и известным $U, \mathbf{x}_0$ однозначно восстанавливается из (4) строка $\mathbf{x}_1$: $\mathbf{x}_1 = (\gamma_1(\mathbf{x}U) \ominus \gamma_1(\mathbf{x}_0U_0) \ominus \mathbf{x}_0U_1) \odot U_0^{-1}$. ■

Расширить класс разрядно-инъективных матриц позволяет

Утверждение 1. Пусть $W_{m\times n}$ — разрядно-инъективная матрица над кольцом R, $D = \mathrm{diag}(c_1, \ldots, c_n)$ — диагональная обратимая матрица над полем P, Π — подстановочная матрица размеров $n \times n$. Тогда матрицы K_1 и K_2, заданные равенствами

$$K_1 = WD, \quad K_2 = W\Pi,$$

являются разрядно-инъективными.

Доказательство. Пусть $\mathbf{x} = (x_1, \ldots, x_m)$ — произвольная ненулевая строка над кольцом R. Для доказательства утверждения достаточно доказать равенства

$$\gamma_1(\mathbf{x}D) = \gamma_1(\mathbf{x}) \odot D; \tag{5}$$
$$\gamma_1(\mathbf{x}\Pi) = \gamma_1(\mathbf{x}) \odot \Pi. \tag{6}$$

Рассмотрим i-й элемент h_i строки $\gamma_1(\mathbf{x}D)$: $h_i = \gamma_1(x_ic_i)$. Воспользовавшись свойствами функции γ_1, получаем

$$h_i = \gamma_1(x_i)\gamma_0(c_i) = \gamma_1(x_i)c_i = (\gamma_1(\mathbf{x}) \odot D)_i.$$

Равенство (5) доказано. Равенство (6) очевидно. ■

Следствие 1. Матрица $K_{m\times 2m} = WD\Pi$ над кольцом R (W, D, Π определены выше) является разрядно-инъективной.

2. Алгоритм блочного шифрования

Приведём описание криптографического примитива, построенного на основе разрядно-инъективной матрицы:

1) $U_{m\times m}$ — обратимая матрица над кольцом R;
2) $G_{m\times m}$ — обратимая матрица над полем P;
3) $K = U(E \mid E + pG)$ — матрица размера $m \times 2m$ над кольцом R;
4) $Z = (E \mid pE)^T$, где E — единичная матрица размера $m \times m$[1];
5) $\mathbf{c}_0, \mathbf{c}_1, ..., \mathbf{c}_{n-1} \in R^m$ — набор раундовых ключей;
6) $\mathbf{x} = \mathbf{x}_0$ — открытый текст;
7) раундовое преобразование определим равенством $\pi(\mathbf{x}) = \gamma_1(\mathbf{x}K)Z$. Тогда преобразование текста на i-м шаге, $i \in \{0, \ldots, n-1\}$, задается формулой

$$\mathbf{x}^{(i+1)} = \gamma_1((\mathbf{x}^{(i)} + \mathbf{c}_i)K)Z = \pi(\mathbf{x}^{(i)} + \mathbf{c}_i). \tag{7}$$

В качестве криптографического примитива рассматривается преобразование открытого текста $\mathbf{x}$ путём n-кратного применения преобразований (7).

[1]Заметим, что умножение произвольного вектора $\mathbf{x} = (\mathbf{x}' \mid \mathbf{x}'') \in P^{2m}$ на матрицу Z даёт вектор $\mathbf{x}' + p\mathbf{x}'' \in R^m$.

3. Криптографические свойства примитива

Пусть $\Sigma = (\Omega, \cdot)$ — регулярное представление группы $(R^m, +)$, $|\Omega| = N$ и подстановка $\pi : R^m \to R^m$ задана равенством

$$\pi(\mathbf{x}) = \gamma_1(\mathbf{x}K)Z. \tag{8}$$

Далее считается, что раундовые ключи $\mathbf{c}_0, \ldots, \mathbf{c}_{n-1}$ выбираются независимо, случайно и равновероятно. Тогда с помощью описанного выше криптографического примитива нетрудно реализовать подстановки из множества $(\Sigma\pi)^k$. Свойства данного множества, согласно [1], определяют криптографические характеристики изучаемого примитива.

Показателем 2-транзитивности $d_2(\Sigma\pi)$ называют минимальную степень k, в которой множество $(\Sigma\pi)^k$ является 2-транзитивным. Интерес представляют подстановки с минимальным значением данного параметра. Известно [1, 2], что для произвольной подстановки $g \in S(\Omega)$ верна оценка $d_2(\Sigma g) \geqslant 3$. Заметим, что подстановочная матрица $\mathcal{P}_2(\pi)$ не влияет на показатель 2-транзитивности и скорость сходимости последовательности степеней матриц переходных вероятностей биграмм к предельной.

Согласно [1], достаточно рассмотреть матрицу Q_π переходов ненулевых разностей биграмм вида

$$(Q_\pi)_{N-1\times N-1} = \frac{1}{N}(\nu_{\mathbf{ab}})_{\mathbf{a},\mathbf{b}\in R^m\setminus\mathbf{0}},$$

где $\nu_{\mathbf{ab}} = |\{\mathbf{x} \in R^m : \pi(\mathbf{x}+\mathbf{a}) - \pi(\mathbf{x}) = \mathbf{b}\}|$. Заметим, что для нахождения показателя 2-транзитивности достаточно описать степени матрицы Q_π, поскольку $d_2(\Sigma\pi) = k$ тогда и только тогда, когда $Q_\pi^{k-1} > 0$.

Для оценки элементов $\nu_{\mathbf{ab}}$ матрицы Q_π используем

Утверждение 2. Элемент $\nu_{\mathbf{ab}}$ для матрицы Q_π равен числу решений системы нелинейных уравнений

$$\begin{cases} \mathbf{b}_0 = \gamma_1(\mathbf{a}U) \oplus \gamma_1(\mathbf{x}_0 + \gamma_0(\mathbf{a}U)), \\ \mathbf{b}_1 = \gamma_0(\mathbf{a}U) \odot G \oplus \mathbf{b}_0 \ominus \gamma_1(\mathbf{x}_1 + \mathbf{b}_0) \end{cases}$$

относительно $\mathbf{x}_0, \mathbf{x}_1 \in P^m$.

Доказательство. Для произвольной матрицы K из (1), по определению, элемент $\nu_{\mathbf{a},\mathbf{b}}$ есть число решений уравнения

$$\mathbf{b} = \pi(\mathbf{y}+\mathbf{a}) - \pi(\mathbf{y}) = \gamma_1(\mathbf{y}K + \mathbf{a}K)Z - \gamma_1(\mathbf{y}K)Z \tag{9}$$

относительно $\mathbf{y} \in R^m$.

Пусть $\mathbf{y}K = (\mathbf{y}' \mid \mathbf{y}'')$, $\mathbf{a}K = (\mathbf{a}' \mid \mathbf{a}'')$. Пользуясь определением матрицы Z, из (9) для нулевого и первого разрядов $\mathbf{b}_0, \mathbf{b}_1$ строки $\mathbf{b}$ получаем равенства

$$\begin{aligned} \mathbf{b}_0 &= \gamma_0(\gamma_1(\mathbf{y}' + \mathbf{a}' \mid \mathbf{y}'' + \mathbf{a}'')Z - \gamma_1(\mathbf{y}' \mid \mathbf{y}'')Z) = \\ &= \gamma_0((\gamma_1(\mathbf{y}' + \mathbf{a}') + p\gamma_1(\mathbf{y}'' + \mathbf{a}'')) - (\gamma_1(\mathbf{y}') + p\gamma_1(\mathbf{y}'')) = \\ &= \gamma_1(\mathbf{y}' + \mathbf{a}') \ominus \gamma_1(\mathbf{y}') = \gamma_1(\mathbf{y}'_0 + \mathbf{a}'_0) \oplus \mathbf{y}'_1 \oplus \mathbf{a}'_1 \ominus \mathbf{y}'_1; \\ \mathbf{b}_1 &= \gamma_1(\gamma_1(\mathbf{y}' + \mathbf{a}') + p\gamma_1(\mathbf{y}'' + \mathbf{a}'') - \gamma_1(\mathbf{y}') - p\gamma_1(\mathbf{y}'')) = \\ &= \gamma_0(\mathbf{y}''_1 \oplus \mathbf{a}''_1 \oplus \gamma_1(\mathbf{y}''_0 + \mathbf{a}''_0) \ominus \mathbf{y}''_1) \oplus \gamma_1((\mathbf{y}'_1 \oplus \mathbf{b}_0) - \mathbf{y}'_1). \end{aligned}$$

Окончательно получаем

$$\begin{aligned} \mathbf{b}_0 &= \gamma_1(\mathbf{y}'_0 + \mathbf{a}'_0) \oplus \mathbf{a}'_1, \\ \mathbf{b}_1 &= \mathbf{a}''_1 \oplus \gamma_1(\mathbf{y}''_0 + \mathbf{a}''_0) \oplus \gamma_1((\mathbf{y}'_1 \oplus \mathbf{b}_0) - \mathbf{y}'_1). \end{aligned}$$

Заметим, что $\mathbf{y}'_0 = \mathbf{y}''_0$ и $\mathbf{a}'_0 = \mathbf{a}''_0$, откуда

$$\begin{aligned} \mathbf{b}_0 &= \mathbf{a}'_1 \oplus \gamma_1(\mathbf{y}'_0 + \mathbf{a}'_0), \\ \mathbf{b}_1 &= \mathbf{a}'_1 \oplus \mathbf{a}''_1 \oplus \mathbf{b}_0 \oplus \gamma_1((\mathbf{y}'_1 \oplus \mathbf{b}_0) - \mathbf{y}'_1). \end{aligned}$$

Преобразуем второе равенство. Пусть $a, b \in \Gamma(R)$, тогда значение $\gamma_1((a \oplus b) - a)$ можно получить, используя равенство $a + b = (a \oplus b) + p\gamma_1(a + b)$. Имеем $a \oplus b - a = b - p\gamma_1(a+b)$, откуда $\gamma_1((a \oplus b) - a) = \gamma_1(b) \ominus \gamma_1(a+b)$. Заметим также, что $\mathbf{a}'_1 \oplus \mathbf{a}''_1 = \mathbf{a}'_0 G$. Следовательно,

$$\begin{aligned} \mathbf{b}_0 &= \mathbf{a}'_1 \oplus \gamma_1(\mathbf{y}'_0 + \mathbf{a}'_0), \\ \mathbf{b}_1 &= \mathbf{a}'_0 G \oplus \mathbf{b}_0 \ominus \gamma_1(\mathbf{y}'_1 + \mathbf{b}_0). \end{aligned}$$

Подставим значение $\mathbf{a}' = \mathbf{a}U$ и сделаем замену $\mathbf{x} = \mathbf{y}' = \mathbf{y}U$. Получим искомую систему уравнений. ■

Приведём оценку снизу показателя 2-транзитивности $d_2(\Sigma\pi)$ для класса подстановок π вида (8).

Теорема 2. Пусть π — подстановка на R^m, определённая равенством (8). Тогда $d_2(\Sigma\pi) \geqslant 4$.

Доказательство. Достаточно показать, что матрица Q_π^2 содержит нулевые элементы. Элементы $\nu_{\mathbf{ac}}^{(2)}$ матрицы Q_π^2 опишем, используя утверждение 2. Заметим, что

$$\nu_{\mathbf{ac}}^{(2)} = \frac{1}{N^2} \sum_{\mathbf{b} \in R^m} \nu_{\mathbf{ab}} \nu_{\mathbf{bc}}$$

и, согласно утверждению 2, произведение $\nu_{\mathbf{ab}}\nu_{\mathbf{bc}}$ равно числу решений $(\mathbf{x}_0, \mathbf{x}_1, \mathbf{y}_0, \mathbf{y}_1) \in (P^m)^4$ системы

$$\begin{cases} \mathbf{b}_0 = \gamma_1(\mathbf{a}U) \oplus \gamma_1(\mathbf{x}_0 + \gamma_0(\mathbf{a}U)), \\ \mathbf{b}_1 = \gamma_0(\mathbf{a}U) \odot G \oplus \mathbf{b}_0 \ominus \gamma_1(\mathbf{x}_1 + \mathbf{b}_0), \\ \mathbf{c}_0 = \gamma_1(\mathbf{b}U) \oplus \gamma_1(\mathbf{y}_0 + \gamma_0(\mathbf{b}U)), \\ \mathbf{c}_1 = \gamma_0(\mathbf{b}U) \odot G \oplus \mathbf{c}_0 \ominus \gamma_1(\mathbf{y}_1 + \mathbf{c}_0), \end{cases} \tag{10}$$

а $\nu_{\mathbf{ac}}^{(2)}$ равно числу решений системы (10) относительно системы независимых переменных $(\mathbf{x}_0, \mathbf{x}_1, \mathbf{y}_0, \mathbf{y}_1, \mathbf{b}_0, \mathbf{b}_1) \in (P^m)^6$. При этом условие $\nu_{\mathbf{ac}}^{(2)} > 0$ равносильно совместности системы (10) относительно последнего набора неизвестных.

Покажем, что в матрице Q_π^2 всегда есть нулевые элементы. Пусть $\mathbf{a}_0 = \mathbf{c}_0 = \mathbf{0}$. Заметим, что $\gamma_0(\mathbf{b}U) = \mathbf{b}_0 \odot U_0$. Первое и последнее уравнения системы (10) примут вид

$$\begin{cases} \mathbf{b}_0 = \gamma_1(\mathbf{a}U), \\ \mathbf{c}_1 = \mathbf{b}_0 \odot U_0 \odot G. \end{cases}$$

Следствием данной системы является уравнение $\mathbf{c}_1 = \mathbf{a}_1 \odot U_0^2 \odot G$. Пусть $\mathbf{a}_1, \mathbf{c}_1 \in P^m$ выбраны так, что последнее равенство не выполняется. Тогда для $\mathbf{a} = p\mathbf{a}_1, \mathbf{c} = p\mathbf{c}_1$ элемент $\nu_{\mathbf{ac}}^{(2)}$ равен нулю. ■

Далее показано, что в ряде случаев указанная оценка достижима.

4. Примитив над кольцом $R = \mathrm{GR}(q^2, p^2)$ на основе разрядно-инъективной матрицы K размера 1×2

Пусть $R = \mathrm{GR}(q^2, p^2)$, $P = \Gamma(R)$, $q = p^r$, $m = 1$, $p > 2$. В этом случае преобразование одного раунда шифрования будем записывать в виде

$$\pi(x) = \gamma_1(xu(e \mid e + pg))Z = \gamma_1(xu) + p(\gamma_1(xu) \oplus x_0 u_0 g_0), \tag{11}$$

где $u \in R^*$; $g \in \Gamma(R)$.

Заметим, что всегда справедливо включение $\{\gamma_1(a + e) \ominus \gamma_1(b + e) : a, b \in P\} \subset P$. Следующая теорема описывает кольца Галуа при $p > 2$, для которых любая нетривиальная РИ-матрица индуцирует 2-транзитивное множество подстановок с минимально возможным показателем 2-транзитивности.

Теорема 3. Пусть для кольца Галуа $R = \mathrm{GR}(q^2, p^2)$, $p > 2$, выполнено условие

$$\{\gamma_1(a + e) \ominus \gamma_1(b + e) : a, b \in P\} = P. \tag{12}$$

Тогда для любой подстановки π вида (11) выполнено равенство $d_2(\Sigma\pi) = 4$.

Доказательство. Как было замечено в п. 3, достаточно доказать, что $Q_\pi^3 > 0$. Опишем элементы $\nu_{ad}^{(3)}$ матрицы Q_π^3, используя утверждение 2. Заметим, что

$$\nu_{ad}^{(3)} = \frac{1}{N^3} \sum_{b,c \in R} \nu_{ab}\nu_{bc}\nu_{cd}$$

и, согласно утверждению 2, произведение $\nu_{ab}\nu_{bc}\nu_{cd}$ равно числу решений $(x_0, x_1, y_0, y_1, z_0, z_1) \in P^6$ системы

$$\begin{cases} b_0 = \gamma_1(au) \oplus \gamma_1(x_0 + \gamma_0(au)), \\ b_1 = \gamma_0(au)g \oplus b_0 \ominus \gamma_1(x_1 + b_0), \\ c_0 = \gamma_1(bu) \oplus \gamma_1(y_0 + \gamma_0(bu)), \\ c_1 = \gamma_0(bu)g \oplus c_0 \ominus \gamma_1(y_1 + c_0), \\ d_0 = \gamma_1(cu) \oplus \gamma_1(z_0 + \gamma_0(cu)), \\ d_1 = \gamma_0(cu)g \oplus d_0 \ominus \gamma_1(z_1 + d_0), \end{cases} \tag{13}$$

а $\nu_{ad}^{(3)}$ равно числу решений системы (13) относительно системы независимых переменных $(x_0, x_1, y_0, y_1, z_0, z_1, b_0, b_1, c_0, c_1) \in P^{10}$. При этом условие $\nu_{ad}^{(3)} > 0$ равносильно совместности системы (13) относительно последнего набора неизвестных. Покажем, что при условии (12) неравенство $\nu_{ad}^{(3)} > 0$ выполняется при всех $a, d \in R \setminus \{0\}$.

Покажем, что из пятого и шестого уравнений системы (13) можно выразить переменные c_1, c_0 соответственно через остальные переменные.

Поскольку $m = 1$, справедливо равенство $\gamma_1(cu) = c_0u_1 \oplus c_1u_0$, и пятое уравнение системы (13) равносильно уравнению

$$c_1 = (d_0 \ominus \gamma_1(z_0 + c_0u_0)) \ominus c_0u_1)u_0^{-1}. \tag{14}$$

Заметим, что последнее уравнение системы (13) имеет вид

$$d_1 = c_0u_0g \oplus d_0 \ominus \gamma_1(z_1 + d_0),$$

откуда $c_0 = (d_1 \ominus d_0 \oplus \gamma_1(z_1 + d_0))g^{-1}u_0^{-1}$.

Преобразуем (13) следующим образом. Заметим, что третье уравнение системы имеет вид

$$c_0 = b_0u_1 \oplus b_1u_0 \oplus \gamma_1(y_0 + \gamma_0(bu)).$$

Подставив в него выражение для b_1 из второго уравнения системы (13), получим

$$c_0 \ominus b_0(u_0 \oplus u_1) \ominus \gamma_0(augu) = \gamma_1(y_0 + b_0u_0) \ominus \gamma_1(x_1 + b_0)u_0.$$

Подставив выражение для c_1 из (14) в четвёртое уравнение системы (13), получим

$$d_0 \ominus c_0(u_0 \oplus u_1) \ominus \gamma_0(bugu) = \gamma_1(z_0 + c_0u_0) \ominus \gamma_1(y_1 + c_0)u_0.$$

Из приведённых рассуждений следует, что система (13) равносильна системе уравнений

$$\begin{cases} \gamma_1(y_0 + b_0u_0) \ominus \gamma_1(x_1 + b_0)u_0 = c_0 \ominus b_0(u_0 \oplus u_1) \ominus \gamma_0(augu), \\ \gamma_1(z_0 + c_0u_0) \ominus \gamma_1(y_1 + c_0)u_0 = d_0 \ominus c_0(u_0 \oplus u_1) \ominus \gamma_0(bugu), \\ b_0 = \gamma_1(au) \oplus \gamma_1(x_0 + \gamma_0(au)), \\ c_0 = (d_1 \ominus d_0 \oplus \gamma_1(z_1 + d_0))g^{-1}u_0^{-1}, \\ b_1 = \gamma_0(au)g \oplus b_0 \ominus \gamma_1(x_1 + b_0), \\ c_1 = (d_0 \ominus \gamma_1(z_0 + c_0u_0)) \ominus c_0u_1)u_0^{-1} \end{cases} \tag{15}$$

и совместна тогда и только тогда, когда совместна система из первых четырёх уравнений системы (15).

Лемма 1. Пусть $a \in R \setminus \{0\}$ — произвольный элемент. Тогда в уравнении

$$b_0 = \gamma_1(au) \oplus \gamma_1(x_0 + \gamma_0(au))$$

найдётся $x_0 \in P$, при котором $b_0 \neq \mathbf{0}$.

Доказательство. Для доказательства рассмотрим два случая. Пусть $a_0 = \mathbf{0}$, тогда $b_0 = \gamma_1(au) \neq \mathbf{0}$, так как $a \neq \mathbf{0}$.

Если же $a_0 \neq \mathbf{0}$, то существование искомого x_0 следует из того, что функция γ_1 не является константой. ■

Лемма 2. Пусть $d \in R \setminus \{0\}$ — произвольный элемент. Тогда в уравнении

$$c_0 = (d_1 \ominus d_0 \oplus \gamma_1(z_1 + d_0))g^{-1}u_0^{-1}$$

найдётся $z_1 \in P$, при котором $c_0 \neq \mathbf{0}$.

Доказательство. Лемма 2 доказывается аналогично лемме 1. ■

Зафиксируем произвольные $a, d \in R \setminus \{0\}$. По леммам 1 и 2 элементы $x_0, z_1 \in P$ выберем так, чтобы выполнялось условие $b_0 \neq 0$, $c_0 \neq 0$.

Нам понадобятся свойства функции переноса γ_1. Известно [3], что для $x, y \in \Gamma(R)$ она имеет вид

$$\gamma_1(x + y) \equiv \sum_{j=1}^{p-1} \frac{1}{j!(p-j)!} x^{rj} y^{r(p-j)} \pmod{p}.$$

Данный многочлен является однородным, поэтому при $y \neq 0$ верно сравнение $\gamma_1(x + y) \equiv y\gamma_1(x/y + e) \pmod{p}$.

В системе (15) сделаем замену переменных $y_0' = \dfrac{y_0}{b_0u_0}, x_1' = \dfrac{x_1}{b_0}, z_0' = \dfrac{z_0}{c_0u_0}, y_1' = \dfrac{y_1}{c_0}$.

Тогда условие $\nu_{ad}^{(3)} > 0$ выполняется в том и только в том случае, когда для данных a, d, b_0, c_0, x_0, z_1 существует решение $(x_1', y_0', y_1', z_0') \in P^4$ системы уравнений

$$\begin{cases} \gamma_1(y_0' + e) \ominus \gamma_1(x_1' + e) = (c_0 \ominus b_0(u_0 \oplus u_1) \ominus \gamma_0(augu))u_0^{-1}b_0^{-1}, \\ \gamma_1(z_0' + e) \ominus \gamma_1(y_1' + e) = (d_0 \ominus c_0(u_0 \oplus u_1) \ominus \gamma_0(bugu))u_0^{-1}c_0^{-1}. \end{cases} \tag{16}$$

Если выполнено условие (12), то очевидно, что система (16) совместна. Таким образом, доказано, что все элементы матрицы Q_π^3 положительны. ■

Замечание. Экспериментально подтверждено, что равенство (12) справедливо для $\mathbb{Z}_{p^2}$, где $p \leqslant 283$, а также для колец Галуа $\mathrm{GR}(9^2, 3^2)$, $\mathrm{GR}(27^2, 3^2)$. Описание колец Галуа, для которых выполнено условие (12), остаётся открытой задачей. Примеров, когда оно не выполняется, не найдено.

Утверждение 3. Пусть $p = 3$, $R = \mathrm{GR}(q^2, p^2)$. Тогда выполнено (12).

Доказательство. Функция переноса в первый разряд имеет вид

$$\gamma_1(x+e) = \sum_{j=1}^{p-1} \frac{(-1)^j}{j} x^j.$$

Отсюда $\gamma_1(a+e) \ominus \gamma_1(b+e) = \left(\dfrac{a^2}{2} \ominus a\right) \ominus \left(\dfrac{b^2}{2} \ominus b\right) = 2^{-1}((a \ominus e)^2 \ominus (b \ominus e)^2)$. Достаточно показать, что при любом $c \in P$ уравнение

$$x^2 \ominus y^2 = c \tag{17}$$

имеет решение в P. Пусть $y = x \ominus e$. Тогда $x^2 \ominus (x \ominus e)^2 = 2x \ominus e$, и решением уравнения (17) будет пара $\left(\dfrac{c \oplus e}{2}, \dfrac{c \ominus e}{2}\right)$. ■

В предположении, что верна S-гипотеза (все конечные простые группы известны [4]), удаётся описать свойства группы $\langle \Sigma\pi \rangle$.

Утверждение 4. Пусть верна S-гипотеза, $R = \mathbb{Z}_{p^2}$. Если множество Σ содержит полный цикл $t(x) \equiv x + 1 \pmod{p^2}$, то $\langle \Sigma\pi \rangle \supseteq A_{p^2}$.

Доказательство. Из теоремы 3 следует 2-транзитивность группы $\langle \Sigma\pi \rangle$. Из справедливости S-гипотезы следует, что все 2-транзитивные группы известны, и поэтому список таких групп в [4, 5] является исчерпывающим. Так как группа $\langle \Sigma\pi \rangle$ примарна, то либо она подгруппа аффинной группы, либо содержит знакопеременную.

Однако известно, что $t \notin AGL(2, p)$. Тогда, согласно списку 2-транзитивных групп, $\langle \Sigma\pi \rangle \supseteq A_{p^2}$. ■

5. Примитив над кольцом $R = \mathrm{GR}(q^2, 4)$ на основе разрядно-инъективной $m \times 2m$-матрицы

Пусть далее $R = \mathrm{GR}(q^2, 4)$, $P = \Gamma(R)$.

Теорема 4. Пусть $R = \mathrm{GR}(q^2, 4)$, $P = \Gamma(R)$, $m \in \mathbb{N}$, подстановка π вида (8) выбрана так, что все миноры матрицы U_0 отличны от нуля. Тогда $d_2(\Sigma\pi) = 4$.

Доказательство. Достаточно доказать, что $Q_\pi^3 > 0$. Опишем элементы $\nu_{\mathbf{ad}}^{(3)}, \mathbf{a}, \mathbf{d} \in R^m$ матрицы Q_π^3, используя утверждение 2. Заметим, что

$$\nu_{\mathbf{ad}}^{(3)} = \frac{1}{N^3} \sum_{\mathbf{b},\mathbf{c} \in R^m} \nu_{\mathbf{ab}} \nu_{\mathbf{bc}} \nu_{\mathbf{cd}}$$

и, согласно утверждению 2, произведение $\nu_{\mathbf{ab}}\nu_{\mathbf{bc}}\nu_{\mathbf{cd}}$ равно числу решений $(\mathbf{x}_0, \mathbf{x}_1, \mathbf{y}_0, \mathbf{y}_1, \mathbf{z}_0, \mathbf{z}_1) \in (P^m)^6$ системы

$$\begin{array}{l} \mathbf{b}_0 = \gamma_1(\mathbf{a}U) \oplus \gamma_1(\mathbf{x}_0 + \gamma_0(\mathbf{a}U)), \\ \mathbf{b}_1 = \gamma_0(\mathbf{a}U) \odot G \oplus \mathbf{b}_0 \ominus \gamma_1(\mathbf{x}_1 + \mathbf{b}_0), \\ \mathbf{c}_0 = \gamma_1(\mathbf{b}U) \oplus \gamma_1(\mathbf{y}_0 + \gamma_0(\mathbf{b}U)), \\ \mathbf{c}_1 = \gamma_0(\mathbf{b}U) \odot G \oplus \mathbf{c}_0 \ominus \gamma_1(\mathbf{y}_1 + \mathbf{c}_0), \\ \mathbf{d}_0 = \gamma_1(\mathbf{c}U) \oplus \gamma_1(\mathbf{z}_0 + \gamma_0(\mathbf{c}U)), \\ \mathbf{d}_1 = \gamma_0(\mathbf{c}U) \odot G \oplus \mathbf{d}_0 \ominus \gamma_1(\mathbf{z}_1 + \mathbf{d}_0), \end{array} \tag{18}$$

а $\nu^{(3)}_{\mathbf{ad}}$ равно числу решений системы (18) относительно системы независимых переменных $(\mathbf{x}_0, \mathbf{x}_1, \mathbf{y}_0, \mathbf{y}_1, \mathbf{z}_0, \mathbf{z}_1, \mathbf{b}_0, \mathbf{b}_1, \mathbf{c}_0, \mathbf{c}_1) \in (P^m)^{10}$. При этом условие $\nu^{(3)}_{\mathbf{ad}} > 0$ равносильно совместности системы (18) относительно последнего набора неизвестных. Покажем, что при условии теоремы неравенство $\nu^{(3)}_{\mathbf{ad}} > 0$ выполняется при всех $\mathbf{a}, \mathbf{d} \in R^m \setminus \{\mathbf{0}\}$.

Покажем, что из пятого и шестого уравнений системы (18) можно выразить переменные $\mathbf{c}_1, \mathbf{c}_0$ соответственно через остальные переменные.

Из равенства $\gamma_1(\mathbf{c}U) = \mathbf{c}_0 \odot U_1 \oplus \mathbf{c}_1 \odot U_0 \oplus \gamma_1(\mathbf{c}_0U_0)$ следует, что пятое уравнение системы (18) равносильно уравнению

$$\mathbf{c}_1 = (\mathbf{d}_0 \ominus \gamma_1(\mathbf{z}_0 + \mathbf{c}_0 \odot U_0)) \ominus \mathbf{c}_0 \odot U_1 \ominus \gamma_1(\mathbf{c}_0U_0)) \odot U_0^{-1}. \tag{19}$$

Заметим, что последнее уравнение системы (18) имеет вид

$$\mathbf{d}_1 = \mathbf{c}_0 \odot U_0 \odot G \oplus \mathbf{d}_0 \ominus \gamma_1(\mathbf{z}_1 + \mathbf{d}_0),$$

откуда

$$\mathbf{c}_0 = (\mathbf{d}_1 \ominus \mathbf{d}_0 \oplus \gamma_1(\mathbf{z}_1 + \mathbf{d}_0)) \odot G^{-1} \odot U_0^{-1}.$$

Преобразуем систему (18) следующим образом. Заметим, что третье уравнение системы имеет вид

$$\mathbf{c}_0 = \mathbf{b}_0 \odot U_1 \oplus \mathbf{b}_1 \odot U_0 \oplus \gamma_1(\mathbf{b}_0U_0) \oplus \gamma_1(\mathbf{y}_0 + \gamma_0(\mathbf{b}U)).$$

Подставив в него выражение для $\mathbf{b}_1$ из второго уравнения, получим

$$\mathbf{c}_0 \ominus \mathbf{b}_0 \odot (U_0 \oplus U_1) \ominus \gamma_0(\mathbf{a}UGU) \ominus \gamma_1(\mathbf{b}_0U_0) = \gamma_1(\mathbf{y}_0 + \mathbf{b}_0 \odot U_0) \ominus \gamma_1(\mathbf{x}_1 + \mathbf{b}_0) \odot U_0.$$

Подставив выражение для $\mathbf{c}_1$ из (19) в четвёртое уравнение системы, получим

$$\mathbf{d}_0 \ominus \mathbf{c}_0 \odot (U_0 \oplus U_1) \ominus \gamma_0(\mathbf{b}UGU) \ominus \gamma_1(\mathbf{c}_0U_0) = \gamma_1(\mathbf{z}_0 + \mathbf{c}_0 \odot U_0) \ominus \gamma_1(\mathbf{y}_1 + \mathbf{c}_0) \odot U_0.$$

Из приведённых рассуждений следует, что система (18) равносильна системе уравнений

$$\begin{cases} \gamma_1(\mathbf{y}_0 + \mathbf{b}_0 \odot U_0) \ominus \gamma_1(\mathbf{x}_1 + \mathbf{b}_0) \odot U_0 = \mathbf{c}_0 \ominus \mathbf{b}_0 \odot (U_0 \oplus U_1) \ominus \gamma_0(\mathbf{a}UGU) \ominus \gamma_1(\mathbf{b}_0U_0), \\ \gamma_1(\mathbf{z}_0 + \mathbf{c}_0 \odot U_0) \ominus \gamma_1(\mathbf{y}_1 + \mathbf{c}_0) \odot U_0 = \mathbf{d}_0 \ominus \mathbf{c}_0 \odot (U_0 \oplus U_1) \ominus \gamma_0(\mathbf{b}UGU) \ominus \gamma_1(\mathbf{c}_0U_0), \\ \mathbf{b}_0 = \gamma_1(\mathbf{a}U) \oplus \gamma_1(\mathbf{x}_0 + \gamma_0(\mathbf{a}U)), \\ \mathbf{c}_0 = (\mathbf{d}_1 \ominus \mathbf{d}_0 \oplus \gamma_1(\mathbf{z}_1 + \mathbf{d}_0)) \odot G^{-1} \odot U_0^{-1}, \\ \mathbf{b}_1 = \gamma_0(\mathbf{a}U) \odot G \oplus \mathbf{b}_0 \ominus \gamma_1(\mathbf{x}_1 + \mathbf{b}_0), \\ \mathbf{c}_1 = (\mathbf{d}_0 \ominus \gamma_1(\mathbf{z}_0 + \mathbf{c}_0 \odot U_0)) \ominus \mathbf{c}_0 \odot U_1 \ominus \gamma_1(\mathbf{c}_0U_0)) \odot U_0^{-1} \end{cases} \tag{20}$$

и совместна тогда и только тогда, когда совместна система из первых четырёх уравнений системы (20).

Лемма 3. Пусть $\mathbf{a}\in R^m\setminus\{\mathbf{0}\}$ — произвольный вектор. Тогда в уравнении

$$\mathbf{b}_0=\gamma_1(\mathbf{a}U)\oplus\gamma_1(\mathbf{x}_0+\gamma_0(\mathbf{a}U))$$

найдётся $\mathbf{x}_0\in P^m$, при котором $\mathbf{b}_0\neq\mathbf{0}$.

Доказательство. Для доказательства рассмотрим два случая. Пусть $\mathbf{a}_0=\mathbf{0}$, тогда $\mathbf{b}_0=\gamma_1(\mathbf{a}U)\neq\mathbf{0}$, так как $\mathbf{a}\neq\mathbf{0}$.

Если же $\mathbf{a}_0\neq\mathbf{0}$, то существование искомого $\mathbf{x}_0$ следует из того, что функция γ_1 не является константой. ■

Лемма 4. Пусть $\mathbf{d}\in R^m\setminus\{\mathbf{0}\}$ — произвольный вектор. Тогда в уравнении

$$\mathbf{c}_0=(\mathbf{d}_1\ominus\mathbf{d}_0\oplus\gamma_1(\mathbf{z}_1+\mathbf{d}_0))\odot G^{-1}\odot U_0^{-1}$$

найдётся $\mathbf{z}_1\in P^m$, при котором $\mathbf{c}_0\neq\mathbf{0}$.

Доказательство. Лемма 4 доказывается аналогично лемме 3. ■

Зафиксируем произвольные $\mathbf{a},\mathbf{d}\in R^m\setminus\{\mathbf{0}\}$. По леммам 3 и 4 векторы $\mathbf{x}_0,\mathbf{z}_1\in P^m$ выберем так, чтобы выполнялось условие $\mathbf{b}_0\neq\mathbf{0},\mathbf{c}_0\neq\mathbf{0}$.

Следовательно, достаточно показать, что для произвольных $\mathbf{a},\mathbf{d}$ и произвольных ненулевых $\mathbf{b}_0,\mathbf{c}_0$ при условии теоремы система уравнений

$$\begin{cases}\gamma_1(\mathbf{y}_0+\mathbf{b}_0\odot U_0)\ominus\gamma_1(\mathbf{x}_1+\mathbf{b}_0)\odot U_0=\mathbf{c}_0\ominus\mathbf{b}_0\odot(U_0\oplus U_1)\ominus\gamma_0(\mathbf{a}UGU)\ominus\gamma_1(\mathbf{b}_0U_0),\\ \gamma_1(\mathbf{z}_0+\mathbf{c}_0\odot U_0)\ominus\gamma_1(\mathbf{y}_1+\mathbf{c}_0)\odot U_0=\mathbf{d}_0\ominus\mathbf{c}_0\odot(U_0\oplus U_1)\ominus\gamma_0(\mathbf{b}UGU)\ominus\gamma_1(\mathbf{c}_0U_0)\end{cases}\tag{21}$$

относительно неизвестных $(\mathbf{y}_0,\mathbf{x}_1,\mathbf{z}_0,\mathbf{y}_1)$ совместна.

Поскольку правые части уравнений системы (21) при фиксированных $\mathbf{a},\mathbf{d},\mathbf{b}_0,\mathbf{c}_0$ являются постоянными векторами, преобразуем отдельно левые части.

Пусть $U_0=(u_{ij})$, $\mathbf{b}_0=(b_1^{(0)},\ldots,b_m^{(0)})$ и $\mathbf{y}_0=(y_1^{(0)},\ldots,y_m^{(0)})$, $\mathbf{x}_1=(x_1^{(1)},\ldots,x_m^{(1)})$. Заметим, что первое уравнение системы (21) равносильно системе уравнений относительно независимых переменных $(y_1^{(0)},\ldots,y_m^{(0)},x_1^{(1)},\ldots,x_m^{(1)})\in P$ с матрицей

$$M=\begin{pmatrix}\sum\limits_{i=1}^m b_i^{(0)}s_{i1} & 0 & \cdots & 0 & 0 & b_1^{(0)}s_{11} & \ldots & b_m^{(0)}s_{m1}\\ & & \ddots & & & \vdots & & \vdots\\ 0 & 0 & \ldots & 0 & \sum\limits_{i=1}^m b_i^{(0)}s_{im} & b_1^{(0)}s_{1m} & \ldots & b_m^{(0)}s_{mm}\end{pmatrix}.$$

Покажем, что если все миноры матрицы U_0 ненулевые, то $\operatorname{rank}M=m$ при любом ненулевом векторе $\mathbf{b}_0$.

Из определения максимально-рассеивающей матрицы $U_0\in P_{m,m}$ следует, что если вектор $\mathbf{b}_0\in P^m$ имеет вес k, то $\|\mathbf{b}_0U_0\|\geqslant m-k+1$.

Пусть $\|\mathbf{b}_0\|=k$. Можно считать, что $\mathbf{b}_0=(b_1^{(0)},\ldots,b_k^{(0)},0,\ldots,0)$. Тогда последние $m-k$ столбцов матрицы M ненулевые и все миноры, соответствующие подматрицам, содержащимся в этих столбцах, также ненулевые. Следовательно, $\|\mathbf{b}_0U_0\|\geqslant m-k+1$. Это означает, что

$$\left\|\left(\sum_{i=1}^m b_i^{(0)}s_{i1},\ldots,\sum_{i=1}^m b_i^{(0)}s_{im}\right)\right\|\geqslant m-k+1.$$

Получаем, что все строки матрицы M линейно независимы, т. е. $\operatorname{rank}M=m$.

Аналогичные рассуждения справедливы и для второго уравнения системы (21). Поэтому система (21) совместна относительно неизвестных $(\mathbf{y}_0,\mathbf{x}_1,\mathbf{z}_0,\mathbf{y}_1)$, т. е. $\nu_{\mathbf{ad}}^{(3)}>0$ при всех $\mathbf{a},\mathbf{d}\in R^m\setminus\{\mathbf{0}\}$. ■

6. Реализация

Опишем представление элементов кольца Галуа $R = \mathrm{GR}(q^2, p^2)$, $q = p^r$, операции сложения и умножения, а также способ вычисления разрядной функции γ_1 в разрядном множестве $\Gamma(R)$.

Имеет место изоморфизм $R \cong \mathbb{Z}_{p^2}[x]/(F(x))$, где $F(x)$ — многочлен Галуа над $\mathbb{Z}_{p^2}$, в соответствии с которым элементу $a \in R$ сопоставлен многочлен $a(x) \in \mathbb{Z}_{p^2}[x]$ степени $r-1$.

Сумма $c = a + b$ и произведение $d = ab$ реализуются с помощью равенств

$$c(x) = a(x) + b(x), \quad d(x) = a(x)b(x) \pmod{F(x)}.$$

Из описания разрядных функций, приведённых в работе [3], следует, что $\gamma_0(a) = a^q$. Поэтому для нахождения первого разряда $\gamma_1(a)$ вычислим многочлен $t(x)$ из равенства $a(x) - a(x)^q = pt(x) \pmod{F(x)}$. Тогда $t(x)^q \pmod{F(x)}$ есть многочлен, соответствующий элементу $\gamma_1(a)$ кольца R.

Заметим, что возведение в степень $q = p^r$ реализуется с помощью не более чем $\log_2 q$ возведений многочлена в квадрат по модулю многочлена $F(x)$ степени r.

Заключение

Полученные в работе результаты показывают, что, используя только линейные преобразования модуля и разрядные функции кольца Галуа, можно строить эффективно реализуемые нелинейные подстановки большой степени, которые порождают множество с малым показателем 2-транзитивности. В дальнейшем представляет интерес изучение других криптографических свойств описанных примитивов и построение новых классов РИ-матриц.

Автор выражает искреннюю благодарность профессору А. А. Нечаеву за постановку задачи и внимание к проводимым исследованиям.

ЛИТЕРАТУРА

1. *Глухов М. М.* О 2-транзитивности произведения регулярных групп подстановок // Труды по дискретной математике. М.: Физматлит, 2000. С. 37–52.
2. *Глухов М. М., Зубов А. Ю.* О длинах симметрических и знакопеременных групп подстановок в различных системах образующих (обзор) // Математические вопросы кибернетики. 1999. Вып. 8. С. 2–32.
3. *Кузьмин А. С., Нечаев А. А.* Линейные рекуррентные последовательности над кольцами Галуа // Алгебра и логика. 1995. Т. 34. № 2. С. 169–189.
4. *Cameron P. J.* Finite permutation groups and finite simple groups // Bull. London Math. Soc. 1981. V. 13. No. 1. P. 1–22.
5. *Погорелов Б. А.* Основы теории групп подстановок. Ч. I. Общие вопросы. М., 1986. 316 с.