УДК 681.3.06

А. В. СОКОЛОВ

ПРОЦЕССОРНО-ОРИЕНТИРОВАННЫЕ НЕЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ НА ОСНОВЕ ПОЛНЫХ КЛАССОВ ИЗОМОРФНЫХ И АВТОМОРФНЫХ ПРЕДСТАВЛЕНИЙ ПОЛЕЙ GF(512) И GF(1024)

Одесский национальный политехнический университет, Одесса, Украина

В статье построены полные множества многоуровневых линейных рекуррентных последовательностей над всеми изоморфными и автоморфными представлениями полей Галуа GF(512) и GF(1024). Разработаны конструкции криптографически высококачественных S-блоков подстановки процессорно-ориентированных длин N = {512, 1024}. Мощности множеств S-блоков подстановки составляют соответственно $J_{GF(512)} = 1.104 \cdot 10^{18}$ *и* $J_{GF(1024)} = 1.01 \cdot 10^{19}$*, что позволяет использовать их в качестве долговременного ключа для модернизации существующих блочных симметричных криптографических алгоритмов и при разработке новых.*

Ключевые слова*: МЛРП, поле Галуа, S-блок подстановки, автоморфизм, изоморфизм; MLRP, Galois field, S-box, automorphism, isomorphism.*

Введение

Основным компонентом современных блочных симметричных криптографических алгоритмов является их нелинейное преобразование – *S*-блок подстановки, которое определяет их резистивность к атакам криптоанализа, а также быстродействие.

S-блок подстановки представляет собой правило отображения группы входных элементов x_i в группу выходных элементов y_i, которое однозначно определяется кодирующей *Q*-последовательностью задающей структуру *S*-блока подстановки. Построение высоконадежного, с криптографической точки зрения, *S*-блока подстановки требует построения определяющей его структуру *Q*-последовательности, которая соответствует базовым критериям криптографического качества, таким как: высокая нелинейность, отсутствие корреляционной связи между векторами выхода и входа, хороший лавинный эффект, периодические свойства [1].

Причем с ростом длины *N* *Q*-последовательностей существенно улучшается и криптографическое качество *S*-блоков подстановки на их основе, а соответственно растет и эффективность криптографических алгоритмов, использующих данные преобразования [2]. Рост длины *Q*-последовательностей также позволяет существенно увеличить количество доступных высококачественных, с криптографической точки зрения, структур *Q*-последовательностей, что открывает возможность их использования в качестве долговременного ключа.

Ясно, что задача поиска подходящих структур *Q*-последовательностей может решаться переборным путем, однако мощность множества всех существующих *Q*-последовательностей стремительно растет с ростом их длины *N* как факториальная величина $J = N!$. Данное обстоятельство делает актуальной задачу поиска регулярных правил синтеза больших множеств *Q*-последовательностей, обладающих хорошими криптографическими свойствами.

Одной из конструкций, решающей задачу синтеза оптимальных, с криптографической точки зрения, *Q*-последовательностей является конструкция *К*. Ниберг [3], основанная на расширенных полях Галуа и используемая в криптопреобразовании Rijndael/AES. Тем не менее, на основе правил, предложенных *К*. Ниберг, могут быть синтезированы лишь небольшие множества *S*-блоков подстановки, так

при $N = 256$ мощность множества оптимальных S-блоков подстановки составляет лишь $J = 30$ [4].

Концепция использования структур расширенных полей Галуа получила дальнейшее развитие в работе [5], где были предложены правила синтеза S-блоков подстановки длины $N = 256$ на основе Многоуровневых Линейных Рекуррентных Последовательностей (МЛРП) по правилу

$$Q = \{0 \mid \text{МЛРП}\}, \quad (1)$$

где | – оператор горизонтальной конкатенации, а последовательности МЛРП генерируются над всеми изоморфными и автоморфными представлениями поля $GF(256)$.

Применение данного подхода позволило достигнуть высокого криптографического качества генерируемых S-блоков подстановки, а также большой мощности их полного множества, достигающей $J = 55296$, для которой также были предложены эффективные правила размножения [5].

Тем не менее задачи построения новых поколений симметричных блочных криптографических алгоритмов требуют улучшения криптографических свойств, применяемых в них S-блоков подстановки, а также дальнейшее наращивание доступных их объемов, что осуществимо путем увеличения длины Q-последовательности N. Таким образом, большой интерес представляет разработка S-блоков подстановки бóльшей длины N, соответствующих базовым критериям криптографического качества.

Целью настоящей статьи является построение нелинейных преобразований на основе всех изоморфных и автоморфных представлений полей GF(512) и GF(1024).

1. Построение нелинейных преобразований над всеми изоморфными и автоморфными представлениями поля *GF*(512)

Рассмотрим исходное поле $GF(512)$, которое имеет свои следующие изоморфные представления

$$\text{GF}(q^k): \quad \text{GF}(2^9) \Rightarrow \text{GF}(8^3).$$

Структура и свойства МЛРП, на основе которой может быть построен криптографически высококачественный S-блок подстановки определяются парой $[f(x), \theta]$ – первообразный полином, первообразный элемент.

В каждом из приведенных изоморфных представлений может быть построено свое множество первообразных полиномов, количество которых определяется как [6]

$$\left|f_q^k\right| = \varphi(q^k - 1)/k, \quad (2)$$

и, соответственно, первообразных элементов

$$\left|\theta_q^k\right| = \varphi(q^k - 1), \quad (3)$$

где $\varphi(\bullet)$ – фи-функция Эйлера.

На основе выражений (2), (3), несложно установить, что количество первообразных полиномов в изоморфном представлении $\left|f_2^9\right| = 48$, в то время как расширение расширенного поля $GF(8^3)$ может быть построено на основе арифметик двух существующих над полем $GF(8)$ первообразных полиномов

$$\begin{cases} g_1(x) = x^3 + x^1 + 1; \\ g_2(x) = x^3 + x^2 + 1. \end{cases}$$

Таким образом, общее количество первообразных полиномов над полем $GF(8^3)$ определяется как $2 \cdot \left|f_8^3\right| = 2 \cdot 144 = 288$. Общее число всех первообразных полиномов над всеми изоморфными представлениями поля $GF(512)$

$$\varepsilon_{GF(512)} = 48 + 288 = 336.$$

Очевидно, что в соответствии с (3) общее количество первообразных элементов, существующих над изоморфными представлениями поля $GF(512)$ определяется как $\left|\theta_2^9\right| = \left|\theta_8^3\right| = 432$.

Стало быть, общее число различных структур МЛРП, которые могут быть построены над всеми автоморфными и изоморфными представлениями поля $GF(512)$

$$\Psi_{GF(512)} = \varepsilon_{GF(512)} \cdot \left|\theta_2^9\right| = 336 \cdot 432 = 145152. \quad (4)$$

Представим метод построения каждого S-блока подстановки из множества (4) в виде конкретных шагов.

Шаг 1. Построить расширенное поле $GF(q^k)$, используя заданный первообразный полином $g_i(x)$ и первообразный элемент $\theta = x$.

Шаг 2. Используя алгоритмы [7] выполнить построение полного множества из $\left|f_q^k\right|$ первообразных полиномов над полем $GF(q^k)$.

Шаг 3. В соответствии с требуемыми параметрами криптографического качества осуществить выбор первообразного полинома.

Шаг 4. Построить МЛРП в соответствии с формулой

```
000 001 008 040 00A 050 08A 044 02A 150 0A9 15C 0C9 056 0BA 1C4 01D 0E8 15E 0D9
0D6 0AE 164 109 06B 152 0B9 1DC 0DD 0F6 1AE 147 011 088 054 0AA 144 009 048 04A
05A 0DA 0CE 06E 17A 1F9 1F5 195 09F 0EC 17E 1D9 0F5 1B6 187 00F 078 1CA 06D 162
139 1EB 165 101 02B 158 0E9 156 099 0DC 0FE 1EE 14D 041 002 010 080 014 0A0 114
083 00C 060 10A 073 192 0A7 12C 143 031 188 077 1B2 1A7 10F 05B 0D2 08E 064 12A
173 1B1 1BF 1CF 045 022 110 0A3 10C 043 012 090 094 0B4 1B4 197 08F 06C 16A 179
1E1 135 18B 06F 172 1B9 1FF 1C5 015 0A8 154 089 05C 0EA 14E 059 0C2 00E 070 18A
067 132 1B3 1AF 14F 051 082 004 020 100 023 118 0E3 106 013 098 0D4 0BE 1E4 11D
0CB 046 03A 1D0 0BD 1FC 1DD 0D5 0B6 1A4 117 09B 0CC 07E 1FA 1ED 155 081 01C 0E0
11E 0D3 086 024 120 123 13B 1FB 1E5 115 08B 04C 06A 15A 0F9 1D6 08D 07C 1EA 16D
141 021 108 063 112 0B3 18C 057 0B2 184 017 0B8 1D4 09D 0FC 1FE 1CD 055 0A2 104
003 018 0C0 01E 0F0 19E 0C7 026 130 1A3 12F 15B 0F1 196 087 02C 160 129 16B 171
1A1 13F 1DB 0E5 136 193 0AF 16C 149 061 102 033 198 0F7 1A6 107 01B 0D8 0DE 0EE
16E 159 0E1 116 093 08C 074 1AA 167 111 0AB 14C 049 042 01A 0D0 09E 0E4 13E 1D3
0A5 13C 1C3 025 128 163 131 1AB 16F 151 0A1 11C 0C3 006 030 180 037 1B8 1F7 185
01F 0F8 1DE 0CD 076 1BA 1E7 105 00B 058 0CA 04E 07A 1DA 0ED 176 199 0FF 1E6 10D
04B 052 09A 0C4 03E 1F0 1BD 1DF 0C5 036 1B0 1B7 18F 04F 072 19A 0E7 126 113 0BB
1CC 05D 0E2 10E 053 092 084 034 1A0 137 19B 0EF 166 119 0EB 146 019 0C8 05E 0FA
1CE 04D 062 11A 0F3 186 007 038 1C0 03D 1E8 17D 1C1 035 1A8 177 191 0BF 1EC 15D
0C1 016 0B0 194 097 0AC 174 189 07F 1F2 1AD 15F 0D1 096 0A4 134 183 02F 178 1E9
175 181 03F 1F8 1FD 1D5 095 0BC 1F4 19D 0DF 0E6 12E 153 0B1 19C 0D7 0A6 124 103
03B 1D8 0FD 1F6 18D 05F 0F2 18E 047 032 190 0B7 1AC 157 091 09C 0F4 1BE 1C7 005
028 140 029 148 069 142 039 1C8 07D 1E2 12D 14B 071 182 027 138 1E3 125 10B 07B
1D2 0AD 17C 1C9 075 1A2 127 11B 0FB 1C6 00D 068 14A 079 1C2 02D 168 169 161 121
12B 17B 1F1 1B5 19F 0CF 066 13A 1F3 1A5 11F 0DB 0C6 02E 170 1A9 17F 1D1 0B5 1BC
1D7 085 03C 1E0 13D 1CB 065 122 133 1BB 1EF 145
```

Рисунок

$$N_i = \sum_{\nu=1}^{k} \alpha_{k-\nu}^{(i)} q^{k-\nu},\ i = \overline{0, q^k - 2},$$

где

$\theta^i \operatorname{modd}(f(x), q) = \alpha_{k-1}^{(i)} x^{k-1} + \alpha_{k-2}^{(i)} x^{k-2} + \ldots + \alpha_0^{(i)}$ – i-й элемент поля.

Шаг 5. Сформировать Q-последовательность, определяющую структуру S-блока подстановки в соответствии с (1).

Например, выбрав изоморфное представление поля $GF(8^3)$, а также неприводимый над полем $GF(8)$ полином $g_1(x)$, а также неприводимый над полем $GF(8^3)$ полином $\xi(x) = x^3 + x + 2$, получаем соответственно S-блок подстановки, представленный в виде шестнадцатеричного кода своей Q-последовательности (рисунок).

Сведем в табл. 1 криптографические характеристики [8] построенных на основе поля $GF(512)$ S-блоков подстановки, где приняты следующие условные обозначения:

- $\max\left\{\left|r_{i,j}\right|\right\}$ – максимальный по абсолютной величине элемент матрицы коэффициентов корреляции;
- K^0 – количество нулей в матрице коэффициентов корреляции;
- N_s – расстояние нелинейности;
- $\min\left\{\deg\left(F_i\right)\right\}$ – наименьшая степень среди алгебраических степеней нелинейности компонентных булевых функций;
- T – период возврата S-блока подстановки в исходное состояние [9].

Результаты, представленные в табл. 1 демонстрируют высокое качество построенных над полем $GF(512)$ S-блоков подстановки.

2. Построение нелинейных преобразований над всеми изоморфными и автоморфными представлениями поля *GF*(1024)

Исходное расширенное поле $GF(1024) = GF(2^{10})$ может быть представлено в виде следующих своих изоморфных представлений

$$GF(q^k):\quad GF(2^{10}) \Rightarrow GF(4^5) \Rightarrow GF(32^2).$$

Таким образом, в поле $GF(2^{10})$ существует $\left|f_2^{10}\right| = 60$ первообразных полиномов; в поле $GF(4^5)$ существует $\left|f_4^5\right| = 120$ первообразных полиномов; и в поле $GF(32^2)$ соответственно $\left|f_{32}^2\right| = 300$. С другой стороны, в последнем случае исходное расширенное поле $GF(32)$ также может иметь свои различные изоморфные представления в соответствии с выбранным первообразным полиномом $f(x)$, и соот-

Таблица 1

Поле	Количество первообразных полиномов	$\max\{\lvert r_{i,j}\rvert\}$	K^0	N_s	$\min\{\deg(F_i)\}$	T
$GF(2^9)$	48	0.0625...0.1094	0...16	198...222	7...8	412...14429940
$GF(8^3)$	144, по модулю полинома $g_1(x)$	0.0625...0.1016	0...13	206...222	7...8	2...3540900
	144, по модулю полинома $g_2(x)$	0.0547...0.1016	0...10	202...222	7...8	3...2810109

ветственно, различные структуры таблиц умножения. Так, в поле $GF(32) = GF(2^5)$ существует 6 первообразных полиномов

$$\begin{cases} f_1(x) = x^5 + x^2 + 1; \\ f_2(x) = x^5 + x^3 + 1; \\ f_3(x) = x^5 + x^3 + x^2 + x^1 + 1; \\ f_4(x) = x^5 + x^4 + x^2 + x^1 + 1; \\ f_5(x) = x^5 + x^4 + x^3 + x^1 + 1; \\ f_6(x) = x^5 + x^4 + x^3 + x^2 + 1. \end{cases}$$

Следовательно, общее количество различных структур первообразных полиномов в поле $GF(32)$ определяется как $6 \cdot \left| f_{32}^2 \right| = 1800$.

В соответствии с (2) количество первообразных элементов определяется как $\left|\theta_2^{10}\right| = \left|\theta_4^5\right| = \left|\theta_{32}^2\right| = 600$.

Общее множество первообразных полиномов во всех изоморфных представлениях поля $GF(1024)$ может быть найдено как сумма всех найденных выше первообразных полиномов по всех изоморфных представлениях данного поля

$$\varepsilon = \left| f_2^{10} \right| + \left| f_4^5 \right| + 6 \left| f_{32}^2 \right| = 120 + 300 + 1800 = 2220.$$

Таким образом, общее количество различных структур МЛРП в поле $GF(1024)$ определяется как

$$\Psi_{GF(1024)} = \varepsilon \left| \theta_2^{10} \right| = 2220 \cdot 600 = 1332000.$$

В табл. 2 рассчитаны значения основных криптографических параметров построенных на основе поля $GF(1024)$ криптографических S-блоков подстановки.

Следовательно, данные табл. 2 демонстрируют наличие во всех изоморфных и автоморфных представлениях поля $GF(1024)$ существенного количества S-блоков подстановки, обладающих высоким уровнем криптографического качества.

3. Правила размножения нелинейных преобразований и обобщение результатов

Отметим, что для S-блоков подстановки построенных над всеми изоморфными и автоморфными представлениями поля $GF(1024)$ применимы правила размножения [5]:

- нулевой элемент может быть добавлен в Q-последовательность 1023 различными способами, при этом формируя различные структуры S-блоков подстановки;
- каждая Q-последовательность допускает перестановку своих компонентных булевых функций 10! различными способами;
- путем знаковых кодирований компонентных булевых функций 2^{10} различными способами;
- путем рассмотрения Q-последовательности как частотно-кодирующей последовательности (ЧКП), так и время-кодирующей последовательности (ВКП), что позволяет удвоить их количество [10].

Таким образом, общее количество построенных S-блоков подстановки над всеми изоморфными и автоморфными представлениями поля $GF(512)$ составляет

$$J_{GF(512)} = 145152 \cdot 1023 \cdot 10! \cdot 1024 \cdot 2 = 1.104 \cdot 10^{18},$$

в то время как для поля $GF(1024)$ этот показатель составляет

$$J_{GF(1024)} = 1332000 \cdot 1023 \cdot 10! \cdot 1024 \cdot 2 = 1.01 \cdot 10^{19},$$

что является дост аточно существенной величиной. Так, при использовании S-блока подстановки длины $N = 1024$ в качества элемента ключа, длина ключа достигнет ~ 64 бита.

На основе данных [5] может быть проведен сравнительный анализ (табл. 3) динамики основных показателей криптографического ка-

Таблица 2

Поле	Количество первообразных полиномов	$\max\{\lvert r_{i,j}\rvert\}$	K^0	N_s	$\min\{\deg(F_l)\}$	T
1	2	3	4	5	6	7
$GF(2^{10})$	60	0.0469...0.0781	0...18	422...462	9	1010...539965270
$GF(4^5)$	120	0.0469...0.0781	0...12	422...462	8...9	2...339437110
$GF(32^2)$	300, по модулю полинома $f_1(x)$	0.043...0.0781	0...14	410...464	9	2...90350990
	300, по модулю полинома $f_2(x)$	0.043...0.0781	0...15	410...462	9	2...2081380170
	300, по модулю полинома $f_3(x)$	0.0351...0.0781	0...13	410...462	9	3...72116040
	300, по модулю полинома $f_4(x)$	0.0468...0.0781	0...15	410...466	9	3...1287763560
	300, по модулю полинома $f_5(x)$	0.0468...0.0781	0...16	410...462	9	2...28502469
	300, по модулю полинома $f_6(x)$	0.0429...0.0781	0...18	410...464	9	2...1205547720

Таблица 3

N	Объем J	Наилучшие показатели криптографического качества				
		$\max\{\|r_{i,j}\|\}$	K^0	N_s	$\min\{\deg(F_i)\}$	T
256	$7.4518\cdot10^{16}$	0.0781	17	108	7	113050
512		0.0547	16	222	8	14429940
1024	$1.01\cdot10^{19}$	0.0351	18	466	9	2081380170

чества с увеличением длины *S*-блоков подстановки на основе всех изоморфных и автоморфных представлений полей *GF*(256), *GF*(512), *GF*(1024).

Анализ данных табл. 3 показывает стремительный рост с увеличением длины N таких важнейших параметров криптографического качества как расстояние нелинейности N_s, алгебраическая степень нелинейности $\min\{\deg(F_i)\}$ и период возврата *S*-блока подстановки в исходное состояние. При этом умеренно падает корреляционная связь выхода и входа *S*-блока подстановки, что показывает, соответственно $\max\{|r_{i,j}|\}$. Таким образом, табл. 3 подтверждает эффективность использования метода построения *S*-блоков подстановки над всеми изоморфными и автоморфными представлениями полей Галуа при больших длинах $N = \{512, 1024\}$.

Заключение

- дальнейшее развитие получил метод синтеза процессорно-ориентированных *S*-блоков подстановки на основе МЛРП в рамках чего построены полные классы МЛРП над всеми изоморфными и автоморфными представлениями полей *GF*(512) и *GF*(1024), мощностей $\Psi_{GF(512)} = 145152$ и $\Psi_{GF(1024)} = 1332000$. При этом классы высоконелинейных *S*-блоков подстановки на основе МЛРП имеют мощности $J_{GF(512)} = 1.104\cdot10^{18}$ и $J_{GF(1024)} = 1.01\cdot10^{19}$, что является существенными величинами с криптографической точки зрения;
- найденные криптографические свойства построенного класса *S*-блоков подстановки показали тотальное улучшение криптографического качества *S*-блоков подстановки на основе всех изоморфных и автоморфных представлений полей *GF*(512) и *GF*(1024) по отношению к *S*-блокам подстановки над полем *GF*(256);
- полученная мощность класса криптографически качественных *S*-блоков подстановки позволяет рекомендовать их к использованию в качестве элементов ключа шифра, при этом необходимый прирост ключа для хранения номера выбранного *S*-блока подстановки составляет до 64 бит для длины $N = 1024$.

Отметим, что практический интерес представляет задача дальнейшего расширения ансамбля доступных длин оптимальных с точки зрения криптографического качества *S*-блоков подстановки, которые могут быть использованы для повышения эффективности существующих криптографических алгоритмов, а также для построения новых алгоритмов шифрования с бóльшими длинами блока данных.

Литература

1. Горбенко, І. Д. Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму RIJNDAEL (FIPS 197) / І. Д. Горбенко, О. В. Потій, Ю. А. Ізбенко // Харків: Всеукраїнський міжвідомчий науково-технічний збірник «Радіотехніка». – 2004. – Том 126. – С. 132–138.

2. Ростовцев А. Г. Большие подстановки для программных шифров /А. Г. Ростовцев // Проблемы инф. безопасности. Компьютерные системы. – СПб.. – 2000. – № 3. – С. 31–34.

3. Nyberg, K. Differentially uniform mappings for cryptography. I Advances in cryptology / K. Nyberg // Proc. of EUROCRYPT'93. – Berlin, Heidelberg, New York. – 1994. – vol.765, Lecture Notes in Compuer Springer-Verlag. – P. 55–65.

4. Мазурков, М. И. Алгебраические свойства криптографических таблиц замен шифра Rijndael и шифра ГОСТ 28147-89 / М. И. Мазурков, А. В. Соколов. – Одесса: Труды СИЭТ. – 2012. – С. 149.

5. Мазурков, М. И. Нелинейные преобразования на основе полных классов изоморфных и автоморфных представлений поля GF(256) / М. И. Мазурков, А. В. Соколов // Известия высших учебных заведений. Радиоэлектроника. – 2013. – Т. 56, N 11. – С. 16–24.

6. Берлекэмп, Э. Алгебраическая теория кодирования / Э. Берлекэмп. – М: МИР, 1971. – 477 с.

7. Мазурков М. И. Семейства линейных рекуррентных последовательностей на основе полных множеств изоморфных полей Галуа / Мазурков М. И., Конопака Е. А // Радиоэлектроника. — 2005. – № 11. – С. 58–65. (Изв. вузов).

8. Соколов, А. В. Новые методы синтеза нелинейных преобразований современных шифров / А. В. Соколов. – Lap Lambert Academic Publishing, Germany 2015. – 100 с.

9. Зайко, Ю. Н. Криптография глазами физика // Изв. Саратовского ун-та. – Т. 9 вып. 2. – С. 34–48. – 2009.

10. Мазурков, М. И. Системы широкополосной радиосвязи / М. И. Мазурков – Одесса: Наука и Техника, 2010. – с. 340. – ISBN 978-966-8335-95-2.

Поступила 10.07.15

A. V. Sokolov

PROCESSOR-ORIENTED NONLINEAR TRANSFORM BASED ON THE FULL CLASSES OF ISOMORPHIC AND AUTOMORPHIC REPRESENTATIONS OF GALOIS FIELDS GF(512) AND GF(1024)

The full sets of multilevel linear recurring sequences over all isomorphic and automorphic representations of Galois fields GF(512) and GF(1024) are built. Constructions of cryptographically high quality S-box of processor-oriented lengths N = {512, 1024} are developed. The cardinality of sets of S-boxes are $J_{GF(512)} = 1.104 \cdot 10^{18}$ *and* $J_{GF(1024)} = 1.01 \cdot 10^{19}$ *which allows to use them as a long-term key to upgrade existing block of symmetric cryptographic algorithms and for development of new ones.*