О параметрах генератора раундовых ключей алгоритма 2-ГОСТ

Фомичёв Владимир Михайлович[1] Коренева Алиса Михайловна[2]
Тулебаев Азат Ирикович[3]

[1]д.ф.-м.н., научный консультант ООО «Код Безопасности», профессор НИЯУ МИФИ, профессор Финансовый университет при Правительстве РФ, в.н.с. ФИЦ ИУ РАН, fomichev.2016@yandex.ru

[2]к.ф.-м.н., ведущий системный аналитик ООО «Код Безопасности», a.koreneva@securitycode.ru

[3]программист ООО «Код Безопасности», a.tulebaev@securitycode.ru

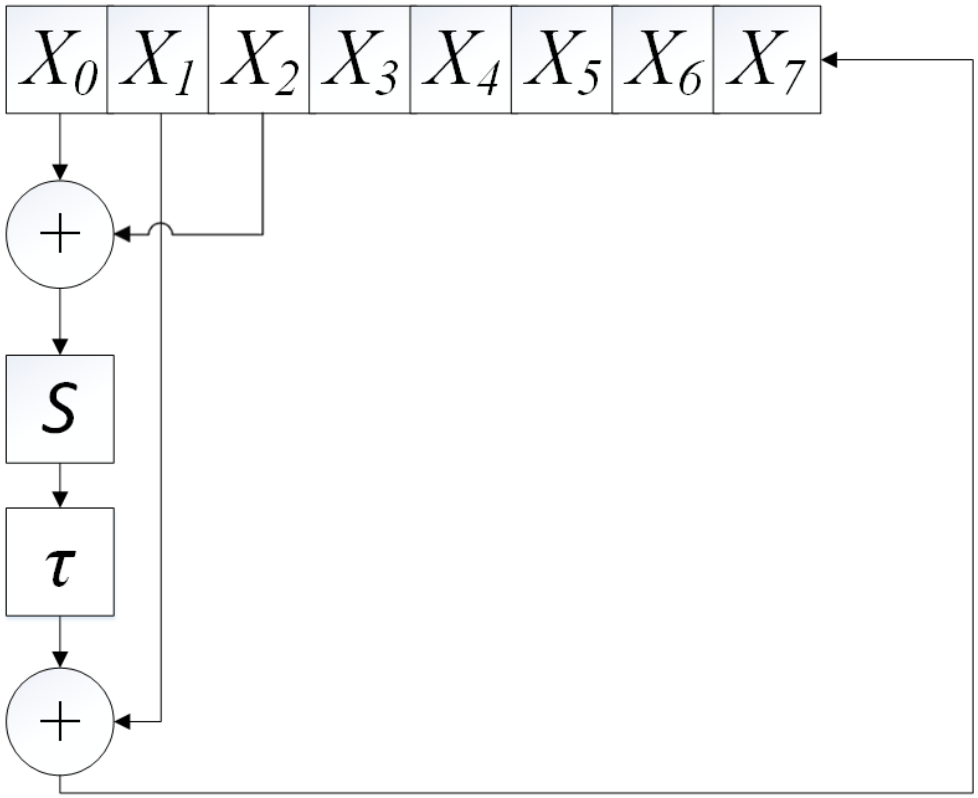
Актуальность

- Алгоритм 2-ГОСТ – низкоресурсная модификация ГОСТ 28147-89;
- Усиление криптографических свойств 2-ГОСТ за счет модификации ключевого расписания;
- На конференции РусКрипто'2018 предложен новый алгоритм генерации раундовых ключей для 2-ГОСТ [1].

[1] – А. Дмух, Д. Трифонов, А. Чухно, О модификации отечественного низкоресурсного криптографического алгоритма 2-ГОСТ и вопросах его реализации на ПЛИС, РусКрипто'2018.

Способ выбора раундовых ключей алгоритма 2-ГОСТ (РусКрипто'2018)

Регистр состоит из 8 ячеек $X_j \in V_{32}, j = 0, \ldots, 7$.



Нелинейная рекуррента генерации раундовых ключей

Функционирование регистра в i-такт, $i = 1, \ldots, 32$:

$$X_7(i) = \tau(S[X_0(i-1) \oplus X_2(i-1)]) \oplus X_1(i-1),$$

$$X_j(i) = X_{j+1}(i-1), j = 0, \ldots, 6.$$

- $S(a) = S(a_7, \ldots, a_0) = (\pi(a_7), \ldots, \pi(a_0)), a \in V_{32}, a_i \in V_4$.
  Преобразование $\pi\colon V_4 \to V_4$ задано следующим образом:

$$\pi = (0, 8, 6, 13, 5, 15, 7, 12, 4, 14, 2, 3, 9, 1, 11, 10)$$

- $\tau \in \mathbb{S}_{32}$ – подстановка на множестве $\{0, \ldots, 31\}$.

$$\tau = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 & 31 \\ 4 & 13 & 22 & 31 & 8 & 17 & 26 & 3 & 12 & 21 & 30 & 7 & 16 & 25 & 2 & 11 & 20 & 29 & 6 & 15 & 24 & 1 & 10 & 19 & 28 & 5 & 14 & 23 & 0 & 9 & 18 & 27 \end{pmatrix}$$

Цели работы

- Определить наилучшие с точки зрения перемешивания знаков начального заполнения точки съема функции обратной связи регистра сдвига;
- Предложить альтернативную схему генератора ключевого расписания алгоритма 2-ГОСТ, усиливающую криптографические характеристики прототипа.

Объект исследования

Объект исследования – класс нелинейных рекуррент, порождаемый семейством регистров сдвига длины 8 с 3 точками съема $(0, i, j), 0 < i, j \leq 7$.

Преобразование $g_{i,j} : V_{256} \to V_{256}$ определим формулой:

$$g_{i,j}(X_0, \ldots, X_7) = (X_1, \ldots, X_7, \tau(S(X_0 \oplus X_i)) \oplus X_j),$$

где τ и S – подстановки из работы [1].

[1] – А. Дмух, Д. Трифонов, А. Чухно, О модификации отечественного низкоресурсного криптографического алгоритма 2-ГОСТ и вопросах его реализации на ПЛИС, РусКрипто'2018.

Исследование параметров регистра

Поиск наилучшей пары точек съема (i, j) регистрового преобразования $g_{i,j}$ осуществлялся с помощью:

- оценочного МГП;
- вычислительного эксперимента по проверке свойства локальной совершенности функций, отображающих начальные заполнения в выходные векторы рекурренты.

МГП заключается в исследовании локальных экспонентов перемешивающих матриц и орграфов исследуемых преобразований. Были определены все пары (i, j), при которых матрица перемешивания примитивна.

Экспонент

Экспонент примитивной перемешивающей $(0,1)$-матрицы M – наименьшее натуральное число t такое, что матрица M^t состоит только из положительных элементов.

Значением экспонента оценивается снизу число тактов работы регистра, необходимое для возможного достижения свойства совершенности – зависимости каждого бита текущего состояния от всех битов начального состояния.

Локальный экспонент

Локальный I-экспонент матрицы M, где $I \subseteq \{1, \ldots, 256\}$ – наименьшнее натуральное t такое, что столбцы с номерами из I состоят из положительных элементов.

В рамках нашего исследования $I = \{225, \ldots, 256\}$ и каждый бит $X_7(i)$ может зависеть от всех битов начального заполнения.

Проверка свойства совершенности

Практический подход нахождения локальной совершенности преобразования $g_{i,j}$. Для удобства $g_{i,j} = g$

- $g_k^t(x_1, \ldots, x_{256})$ – k-я координатная функция преобразования g^t, $k = 225, \ldots, 256, t = 1, 2, \ldots$
- Поиск наименьшего значения $\gamma_7(i,j)$ степени t преобразования g, для которой будут найдены векторы $a, a \oplus e_\ell \in V_{256}$, где e_ℓ – вектор веса 1, у которого ℓ-я координата 1, $1 \le \ell \le 256$, такие что:

$$g_k^{\gamma_7(i,j)}(a) \oplus g_k^{\gamma_7(i,j)}(a \oplus e_\ell) = 1, \quad 225 \le k \le 256.$$

Результаты эксперимента

Значения показателя локальной совершенности для всех пар (i, j) точек съема.

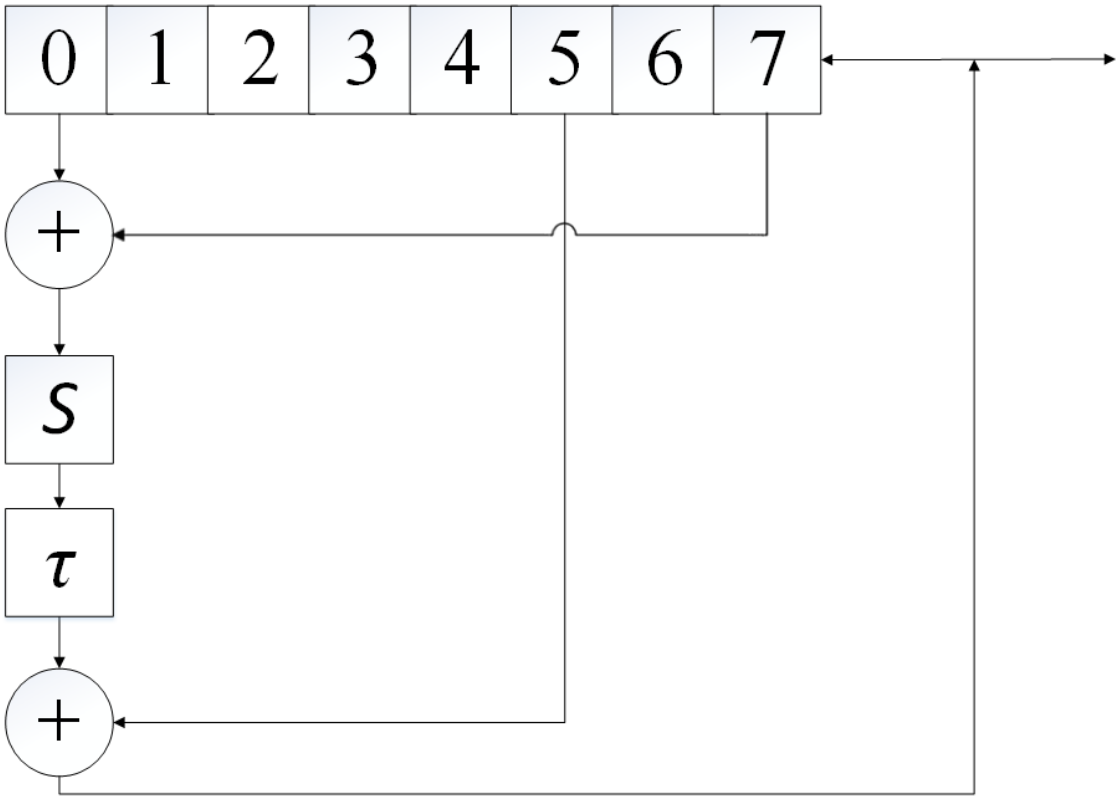
i \ j	1	2	3	4	5	6	7
1	-	40	32	28	28	28	28
2	43	-	34		26		24
3	39	38	-	26	38	22	20
4	34		28	-	22		16
5	23	40		21	-	18	14
6	18		17		19	-	12
7		11	12	13	10	15	-

– показатель локальной совершенности для регистра из [1]
– пары (i, j), при которых перемешивающая матрица непримитивна
– наименьший показатель локальной совершенности

[1] – А. Дмух, Д. Трифонов, А. Чухно, О модификации отечественного низкоресурсного криптографического алгоритма 2-ГОСТ и вопросах его реализации на ПЛИС, РусКрипто'2018

Регистр с улучшенными перемешивающими свойствами

Близкие к наилучшим перемешивающие свойства достигаются при $(i, j) = (7, 5)$. Регистр имеет вид:



Дополнительное исследование

- Проверка статистических свойств генераторов при $(i, j) = (2, 1)$ и $(i, j) = (7, 5)$;
- Изучение длин периодов выходных последовательностей генераторов при некоторых начальных заполнениях.

Для статистического тестирования выходных последовательностей использовался пакет статистических тестов NIST STS версии 2.0. Настройка параметров тестирования произведена в соответствии с рекомендациями NIST.

Статистическое тестирование

При начальном заполнении регистров значениями, полученными с качественного ПДСЧ, проверяемые файлы успешно прошли статистическое тестирование. Доля непройденных тестов невелика:

- для $(i, j) = (2, 1)$ — не более 9 из 188;
- для $(i, j) = (7, 5)$ – не более 4 из 188.

Периодичность нелинейной рекурренты при некоторых начальных заполнениях

При начальном заполнении регистров значением с регулярной структурой, например,

$$(X_0, X_1, X_2, X_3, X_4, X_5, X_6, X_7) = (\overline{0}, \overline{1}, \overline{0}, \overline{1}, \overline{0}, \overline{1}, \overline{0}, \overline{1}),$$

где $\overline{0} = (0, \ldots, 0) \in V_{32}, \overline{1} = (1, \ldots, 1) \in V_{32}$, проверяемые файлы не прошли статистическое тестирование.

- Для $(i, j) = (2, 1)$ – не пройдено 180 тестов из 188;
- для $(i, j) = (7, 5)$ – не пройден 181 тест из 188.

Повторы гаммы

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E
00000000	AA	AA	AA	AA	AA	AA	AA	AA	11	11	11	11	CC	CC	CC
00000010	CC	CC	CC	CC	66	66	66	66	88	88	88	88	00	00	00
00000020	99	99	99	99	66	66	66	66	DD	DD	DD	DD	EE	EE	EE
00000030	33	33	33	33	FF	FF	FF	FF	88	88	88	88	EE	EE	EE
00000040	33	33	33	33	99	99	99	99	55	55	55	55	BB	BB	BB
00000050	CC	CC	CC	CC	00	00	00	00	DD	DD	DD	DD	FF	FF	FF
00000060	EE	EE	EE	EE	33	33	33	33	55	55	55	55	FF	FF	FF
00000070	88	88	88	88	77	77	77	77	22	22	22	22	77	77	77
00000080	00	00	00	00	CC	CC	CC	CC	EE	EE	EE	EE	CC	CC	CC
00000090	55	55	55	55	22	22	22	22	11	11	11	11	33	33	33
000000A0	77	77	77	77	EE	EE	EE	EE	FF	FF	FF	FF	EE	EE	EE
000000B0	77	77	77	77	99	99	99	99	44	44	44	44	66	66	66
000000C0	AA	AA	AA	AA	FF	FF	FF	FF	AA	AA	AA	AA	BB	BB	BB
000000D0	44	44	44	44	EE	EE	EE	EE	DD	DD	DD	DD	44	44	44
000000E0	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	00	BB	BB	BB
000000F0	00	00	00	00	FF	FF	FF	FF	22	22	22	22	CC	CC	CC
00000100	55	55	55	55	55	55	55	55	BB	BB	BB	BB	55	55	55
00000110	99	99	99	99	FF	FF	FF	FF	00	00	00	00	BB	BB	BB
00000120	EE	EE	EE	EE	BB	BB	BB	BB	33	33	33	33	BB	BB	BB
00000130	11	11	11	11	55	55	55	55	00	00	00	00	EE	EE	EE
00000140	AA	AA	AA	AA	33	33	33	33	DD	DD	DD	DD	AA	AA	AA
00000150	DD	DD	DD	DD	33	33	33	33	CC	CC	CC	CC	BB	BB	BB
00000160	FF	FF	FF	FF	33	33	33	33	AA	AA	AA	AA	33	33	33
00000170	BB	BB	BB	BB	88	88	88	88	66	66	66	66	BB	BB	BB
00000180	CC	CC	CC	CC	AA	AA	AA	AA	BB	BB	BB	BB	88	88	88

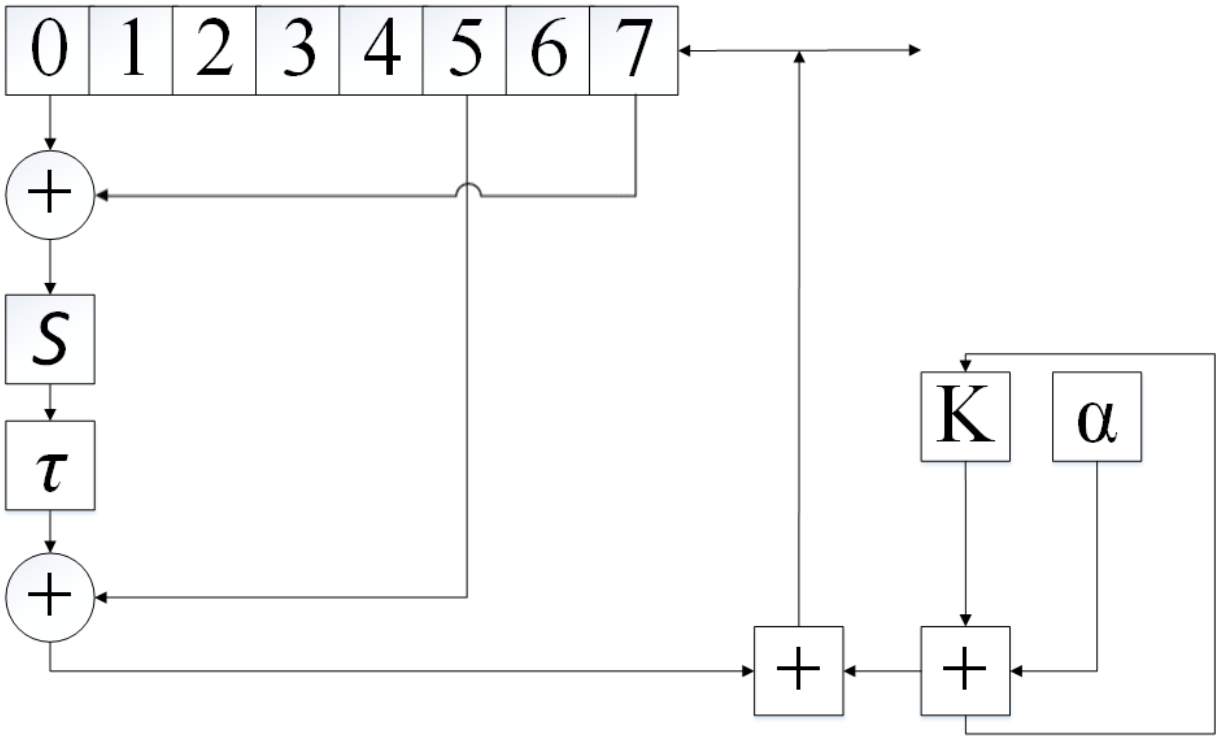
Регистр $g_{2,1}$

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	CC	CC	CC	CC	22	22	22	22	44	44	44	44	77	77	77	77
00000010	EE	EE	EE	EE	44	44	44	44	66	66	66	66	11	11	11	11
00000020	55	55	55	55	AA	AA	AA	AA	AA	AA	AA	AA	44	44	44	44
00000030	88	88	88	88	33	33	33	33	BB	BB	BB	BB	AA	AA	AA	AA
00000040	99	99	99	99	66	66	66	66	33	33	33	33	55	55	55	55
00000050	77	77	77	77	66	66	66	66	44	44	44	44	CC	CC	CC	CC
00000060	99	99	99	99	EE	EE	EE	EE	DD	DD	DD	DD	DD	DD	DD	DD
00000070	CC	CC	CC	CC	FF	FF	FF	FF	EE	EE	EE	EE	AA	AA	AA	AA
00000080	22	22	22	22	77	77	77	77	88	88	88	88	DD	DD	DD	DD
00000090	FF	FF	FF	FF	88	88	88	88	AA	AA	AA	AA	FF	FF	FF	FF
000000A0	99	99	99	99	11	11	11	11	11	11	11	11	00	00	00	00
000000B0	BB	BB	BB	BB	CC	CC	CC	CC	77	77	77	77	FF	FF	FF	FF
000000C0	BB	BB	BB	BB	55	55	55	55	AA	AA	AA	AA	99	99	99	99
000000D0	33	33	33	33	00	00	00	00	55	55	55	55	11	11	11	11
000000E0	22	22	22	22	99	99	99	99	CC	CC	CC	CC	DD	DD	DD	DD
000000F0	22	22	22	22	AA	AA	AA	AA	77	77	77	77	55	55	55	55
00000100	66	66	66	66	DD	DD	DD	DD	DD	DD	DD	DD	66	66	66	66
00000110	88	88	88	88	BB	BB	BB	BB	FF	FF	FF	FF	AA	AA	AA	AA
00000120	22	22	22	22	55	55	55	55	EE	EE	EE	EE	66	66	66	66
00000130	EE	EE	EE	EE	11	11	11	11	DD	DD	DD	DD	22	22	22	22
00000140	11	11	11	11	88	88	88	88	55	55	55	55	CC	CC	CC	CC
00000150	EE	EE	EE	EE	FF	FF	FF	FF	AA	AA	AA	AA	AA	AA	AA	AA
00000160	CC	CC	CC	CC	FF	FF	FF	FF	88	88	88	88	99	99	99	99
00000170	33	33	33	33	11	11	11	11	AA	AA	AA	AA	33	33	33	33
00000180	BB	BB	BB	BB	FF	FF	FF	FF	FF	FF	FF	FF	CC	CC	CC	CC

Регистр $g_{7,5}$

Рекомендации по увеличению длины периода

Последовательное соединение с ЛКГ: $K \in V_{32}, \alpha \in \mathbb{Z}_{2^{32}}$ – нечетный сдвиг.



Таким образом гарантируется длина периода выходных последовательностей не менее 2^{32}.

Выводы

- Исследованы перемешивающие свойства нелинейных рекуррент, порождаемых регистрами сдвига длины 8 с 3 точками съема;
- Определены точки съема регистра, при которых перемешивающие свойства наилучшие с точки зрения МГП;
- Проведен сравнительный анализ результатов статистического тестирования регистровых преобразований $g_{2,1}$ и $g_{7,5}$;
- Предложена схема на основе последовательного соединения полноциклового линейного конгруэнтного генератора (ЛКГ) и исследуемых регистров. Для такого класса автоматов гарантируется длина периода выходных последовательностей не менее 2^{32}.

Спасибо за внимание!