2. *Rebeiro C., Selvakumar D., and Devi A. S. L.* Bitslice implementation of AES // Cryptology and Network Security. 2006. P. 203–212. https://link.springer.com/chapter/10.1007/11935070_14.
3. *Boss E., Grosso V., Tim Güneysu T., et al.* Strong 8-bit sboxes with efficient masking in hardware // J. Cryptographic Engineering. 2017. No. 7(2). P. 149–165.
4. *Kutzner S., Nguyen P. H., and Poschmann A.* Enabling 3-share threshold implementations for all 4-bit s-boxes // LNCS. 2013. V. 8565. P. 91–108.
5. *Canteaut A., Duval S., and Leurent G.* Construction of lightweight s-boxes using Feistel and MISTY structures (full version) // Cryptology ePrint Archive. 2015. No. 2015(711).
6. *Lim C. H.* CRYPTON: A New 128-bit Block Cipher — Specification and Analysis. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.52.5771. 1998.
7. *Gérard B., Grosso V., Naya-Plasencia M., and Standaert F.-X.* Block ciphers that are easier to mask: How far can we go? // LNCS. 2013. V. 8086. P. 383–399.
8. *Matsui M.* New block encryption algorithm MISTY // LNCS. 1997. V. 1267. P. 54–68.
9. *Grosso V., Leurent G., Standaert F.-X., and Varici K.* Ls-designs: Bitslice encryption for efficient masked software implementations // LNCS. 2014. V. 8540. P. 18–37.
10. *Standaert F.-X., Piret G., Rouvroy G., et al.* ICEBERG : An involutional cipher efficient for block encryption in reconfigurable hardware // LNCS. 2004. V. 3017. P. 279–299.
11. *Rijmen V. and Barreto P.* The Khazad Legacy-Level Block Cipher. https://www.researchgate.net/publication/228924670_The_Khazad_legacy-level_block_cipher. 2018.
12. *Lim C.-H.* A revised version of Crypton — Crypton v1.0 // LNCS. 1999. V. 1636. P. 31–45.
13. *Stallings W.* The Whirlpool secure hash function // Cryptologia. 2006. No. 30(1). P. 55–67.
14. *Perrin L., Udovenko A., and Biryukov A.* Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem (full version) // Cryptology ePrint Archive. 2016. No. 2016(539).
15. *De la Cruz Jiménez R. A.* On some methods for constructing almost optimal s-boxes and their resilience against side-channel attacks // Cryptology ePrint Archive. 2018. No. 2018(618).
16. *Fomin D.* New classes of 8-bit permutations based on a butterfly structure // CTCrypt'18. 2018. https://ctcrypt.ru/files/files/2018/09_Fomin.pdf
17. *Fomin D.* On the way of constructing $2n$-bit permutations from n-bit ones // CTCrypt'19. 2019 (в печати).
18. *Фомин Д. Б.* О подходах к построению низкоресурсных нелинейных преобразований // Обозрение прикладной и промышленной математики. 2018. Т. 25(4). С. 379–381.

УДК 519.17 DOI 10.17223/2226308X/12/40

О ПАРАМЕТРАХ ГЕНЕРАТОРА РАУНДОВЫХ КЛЮЧЕЙ АЛГОРИТМА 2-ГОСТ

В. М. Фомичев, А. М. Коренева, А. И. Тулебаев

Необходимость защиты информации в условиях ограниченных ресурсов определяет актуальность построения облегченных реализаций для известных криптографических алгоритмов. В 2014 г. была представлена низкоресурсная реализация ГОСТ 28147-89 под названием 2-ГОСТ. Несмотря на достоинства, схема имела потенциал в части усиления криптографической стойкости, в том числе за счёт модификации ключевого расписания. В 2018 г. предложен новый алгоритм генерации раундовых ключей для 2-ГОСТ на основе регистра сдвига длины 8 над множеством двоичных векторов длины 32. Вместе с тем параметры обратной свя-

зи регистра не были достаточно обоснованы. Работа посвящена определению наилучших (или близких к наилучшим) трёх точек съёма функции обратной связи регистра сдвига и обоснованию предложенного решения. Критерий качества поиска решения определяется характеристиками перемешивания исходных данных с помощью регистрового преобразования и экономичностью реализации, выраженной через «площадь реализации». В качестве характеристики перемешивания использован показатель локальной совершенности регистрового преобразования — число итераций (тактов работы генератора), после которых каждый бит сгенерированного раундового ключа существенно зависит от всех битов начального состояния (основного ключа алгоритма). Большее число точек съёма функции обратной связи не рассматривалось, так как эти варианты менее экономичны. Найдена наилучшая тройка точек съёма функции обратной связи регистра сдвига и проведено сравнение характеристик, определяющих качество ключевого расписания для предложенной и исходной схем. Установлено, что в исходной схеме значение показателя локальной совершенности наибольшее в классе всех функций обратной связи с тремя точками съёма (наихудший показатель с точки зрения перемешивания). Предложена альтернативная схема с наименьшим показателем локальной совершенности и аналогичной площадью реализации. Для исходной и альтернативной схемы проведено статистическое тестирование выходных последовательностей генератора.

Ключевые слова: *2-ГОСТ, генератор ключей, локальная совершенность, матрично-графовый подход, перемешивающие свойства, регистр сдвига.*

Введение

Ключевое расписание блочного шифра является важным компонентом строения, определяющим его криптографическую стойкость. Применение многих методов криптоанализа затруднено, если алгоритм развертывания ключа обеспечивает сложную нелинейную зависимость битов раундовых ключей от битов основного ключа. В 2014 г. представлена предназначенная для низкоресурсной реализации модификация блочного шифра ГОСТ 28147-89 под названием 2-ГОСТ [1]. Для усиления криптографических свойств в модификации предложена новая, более сложная по сравнению с ГОСТ 28147-89 схема ключевой развёртки на основе регистра сдвига длины 8 над множеством двоичных векторов длины 32 с функцией обратной связи, имеющей три точки съёма. Методы и результаты исследования предложенной схемы полностью представлены не были.

Цель данной работы — усилить криптографические характеристики схемы ключевой развёртки за счёт выбора наилучшей тройки точек съёма и представить обоснование выбранного решения. Для обоснования решения использован, в частности, математический аппарат, изложенный в [2].

Установлено [3], что предложенная в [4] модификация обладает не лучшими перемешивающими свойствами. С целью устранения недостатка выполнен перебор всех троек точек съёма вида $(0, i, j)$, где $0 < i, j \leqslant 7$, чтобы оценить для каждой тройки характеристики перемешивания, в том числе с использованием матрично-графового подхода (если 0 — не точка съёма, то реальная длина регистра меньше 8). Для регистровых преобразований получены значения локальных экспонентов их перемешивающих орграфов и экспериментально вычислены показатели локальной совершенности. Для оригинальной и предложенной схемы проведено статистическое тестирование выходных последовательностей генераторов.

1. Схема генератора 2-ГОСТ

Схема генератора построена на основе регистра сдвига длины 8 над множеством двоичных векторов длины 32 [4]. Преобразование $g_{i,j}$ множества 256-мерных двоичных векторов определено формулой (схема регистра при $(i,j)=(7,5)$ дана на рис.1)

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

где τ и S — определённые в [4] подстановки степени 32, обеспечивающие зависимость младших разрядов вектора $\tau(S(X_0\oplus X_i))\oplus X_j$ от старших разрядов.

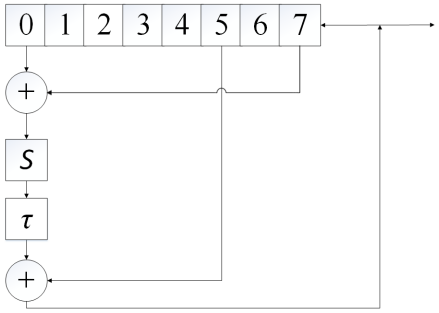

Рис. 1. Схема регистра сдвига при точках съема $(i,j)=(7,5)$

2. Оптимизация параметров генератора

Поиск наилучшей пары точек i,j выполнен с помощью перебора всех значений i,j, при которых перемешивающий орграф примитивный. Для каждой такой пары посчитана оценка γ локального (7,256)-экспонента перемешивающего орграфа $\Gamma(g)$ преобразования g, оценивающего число тактов, после которых каждый из 32-х разрядов вектора в ячейке 7 может зависеть от всех битов начального заполнения регистра, иначе говоря, все столбцы с номерами $225,\dots,256$ перемешивающей матрицы в степени γ не содержат нулей. Затем с учётом полученной оценки локального экспонента определён показатель $\gamma_7(i,j)$ локальной совершенности преобразования g (равный наименьшему числу итераций, после которых указанная зависимость необходимо имеется).

Пусть для краткости $g_{i,j}=g$. Обозначим g_k^t координатную k-ю функцию преобразования g^t, $k=1,\dots,256$, $t=1,2,\dots$ Экспериментально найдено наименьшее значение $\gamma_7(i,j)$ степени t преобразования g, при которой для $k=225,\dots,256$ и $l=1,\dots,256$ функция $g_k^t(x_1,\dots,x_{256})$ существенно зависит от x_l, то есть найдены векторы a, $a\oplus e_l$, где e_l — вектор веса 1, у которого l-я координата равна 1, $1\leqslant l\leqslant 256$, такие, что

$$g_k^{\gamma_7(i,j)}(a)\oplus g_k^{\gamma_7(i,j)}(a\oplus e_l)=1.$$

В таблице приведены значения показателей локальной совершенности преобразования g для всех указанных пар (i,j) точек съёма. Из таблицы видно, что для генератора, предложенного в [4], величина $\gamma_7(2,1)$ совпала с локальным (7,256)-экспонентом и равна 43, т. е. в оригинальной схеме с точками съёма (0,1,2) характеристики перемешивания наихудшие. Наилучшие характеристики перемешивания имеет модификация генератора с точками съёма (0,5,7) с наименьшим показателем локальной совершенности. При фиксации точек 7 и 5 (рис. 1) получено наименьшее значение $\gamma_7(7,5)=10$.

i,j	1,2	1,3	1,4	1,5	1,6	1,7	2,1	2,3	2,5	2,7	3,1	3,2	3,4	3,5	3,6	3,7	4,1
$\gamma_7(i,j)$	40	32	28	28	28	28	43	34	26	24	39	38	26	38	22	20	34
i,j	4,3	4,5	4,7	5,1	5,2	5,4	5,6	5,7	6,1	6,3	6,5	6,7	7,2	7,3	7,4	7,5	7,6
$\gamma_7(i,j)$	28	22	16	23	40	21	18	14	18	17	19	12	11	12	13	10	15

3. Статистическое тестирование выходных последовательностей генератора

Для оценки качества генерируемых последовательностей исходного и предложенного генераторов выполнено их статистическое тестирование. Для этого использован пакет NIST Statistical Test Suit (NIST STS) версии 2.1.2. Выбор параметров и интерпретация результатов осуществлялась в соответствии с рекомендациями NIST [5].

Для проверки статистических свойств генераторов при $(i,j)=(2,1)$ и $(i,j)=(7,5)$ сформированы файлы по $N=2048000000$ бит выходных данных, анализируемый материал разбивался на $m=100$ подпоследовательностей. Тестирование проводилось при нескольких наборах параметров, в каждом случае проведено по 188 тестов, уровень значимости $\alpha=0{,}05$. В результате тестирования подсчитаны:

— $C_1,\dots,C_{10}$ — количество значений p-value, попавших в соответствующий подынтервал (сумма значений $C_1,\dots,C_{10}$ равна m);
— P-VALUE — результирующее значение вероятности статистики теста (для всей последовательности длины N);
— PROPORTION — доля подпоследовательностей, прошедших тест с заданным уровнем значимости α.

При анализе результатов проверялись условия

$$\text{P-VALUE} \geqslant \alpha \text{ и } 0{,}9 \leqslant \text{PROPORTION}.$$

При начальном заполнении регистров значениями, полученными с качественного генератора псевдослучайных чисел, 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.

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 $\overline{0}=(0,\dots,0)\in V_{32}$, $\overline{1}=(1,\dots,1)\in V_{32}$, проверяемые файлы не прошли статистическое тестирование. Для $(i,j)=(2,1)$ не пройдено 180 тестов из 188, для $(i,j)=(7,5)$ — 181 тест из 188. Кроме того, при указанном начальном заполнении наблюдались повторы выходных значений.

Выводы

Исследован показатель локальной совершенности преобразований, связанных со схемой, представленной на РусКрипто'2018. Предложен альтернативный вариант точек съёма регистрового преобразования с аналогичной площадью реализации и наименьшим значением показателя совершенности (10 вместо 43 в оригинальной схеме). Это позволяет существенно сократить число тактов, необходимых для генерации раундовых ключей, каждый бит которых зависит от всех битов основного ключа.

Проведено статистическое тестирование выходных последовательностей обеих схем. Обнаружены начальные заполнения, при которых выходные последовательности имеют небольшую длину периода. Для гарантирования длины периода выходных последовательностей не меньше 2^{32} можно рекомендовать схемы на основе последова-

тельного соединения указанного регистра с полноцикловым линейным конгруэнтным генератором, использующим модуль 2^{32} и нечётный сдвиг [6, с. 156].

ЛИТЕРАТУРА

1. *Dmukh A. A., Dygin D. M., and Marshalko G. B.* A lightweight-friendly modification of GOST block cipher // Матем. вопр. криптогр. 2014. Т. 5. № 2. С. 47–55.
2. *Fomichev V. M., Avezova Ya. A., Koreneva A. M., and Kyazhin S. N.* Primitivity and local primitivity of digraphs and nonnegative matrices // J. Appl. Industr. Math. 2018. V. 12. No. 3. P. 453–469.
3. *Коренева А. М., Полеводин А. В.* Перемешивающие свойства генератора раундовых ключей алгоритма шифрования 2-ГОСТ // Информационная безопасность в банковско-финансовой сфере: Сб. научн. работ участников. М.: Прометей, 2018. С. 107–111.
4. *Дмух А., Трифонов Д., Чухно А.* О модификации отечественного низкоресурсного криптографического алгоритма 2-ГОСТ и вопросах его реализации на ПЛИС. Москва, РусКрипто-2018. `https://www.ruscrypto.ru/resource/archive/rc2018/files/02_Dmukh_Trifonov_Chukhno.pdf`.
5. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication (NIST SP) 800–22 Rev 1a. `https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-number-generators-cryptographic`.
6. *Фомичёв В. М.* Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010. 424 с.

УДК 519.17 DOI 10.17223/2226308X/12/41

О ПЕРЕМЕШИВАЮЩИХ СВОЙСТВАХ МОДИФИЦИРОВАННЫХ МНОГОМЕРНЫХ ЛИНЕЙНЫХ ГЕНЕРАТОРОВ

И. И. Хайруллин

Описан новый класс регистров сдвига длины n с r-битовыми ячейками, $n > 1$, $r > 1$, названных модифицированными многомерными линейными генераторами (ММЛГ). Проведено экспериментальное исследование перемешивающих свойств регистров сдвига длины 8 над V_{32} из класса ММЛГ, функция обратной связи которых построена на основе раундовой подстановки низкоресурсного блочного шифра SPECK. Для таких ММЛГ с различными множествами точек съёма $D \subseteq \{0, \ldots, 7\}$ рассчитаны локальные (0,256)-экспоненты перемешивающих матриц, то есть для каждой матрицы M определено наименьшее натуральное число γ, такое, что при любом натуральном $t \geqslant \gamma$ положительны все столбцы матрицы M^t с номерами 1,. . . ,32. Вычислены показатели 0-совершенности, то есть наименьшие значения степеней регистрового преобразования, при которых каждая координатная функция выхода существенно зависит от всех переменных входа. Для ММЛГ с точками съёма 0 и 7 значения локального экспонента и локального показателя совершенности равны 17. Полученные значения сравниваются с локальными экспонентами и локальными показателями совершенности для конструктивно схожих аналогов, построенных на основе модифицированных аддитивных генераторов. Сравнение показало, что генераторы обладают схожими перемешивающими свойствами, однако в отличие от рассмотренных схем класс ММЛГ представляет интерес для использования в условиях ограниченных ресурсов.

Ключевые слова: *модифицированный многомерный линейный генератор, пере-*