2. *Biere A.* Bounded Model Checking // Handbook of Satisfiability. Amsterdam: IOS Press, 2009. P. 457–481.
3. *Отпущенников И. В., Семёнов А. А.* Технология трансляции комбинаторных проблем в булевы уравнения // Прикладная дискретная математика. 2011. № 1 (11). С. 96–115.
4. *Otpuschennikov I., Semenov A., Gribanova I., et al.* Encoding cryptographic functions to SAT using TRANSALG system // Proc. 22nd European Conf. ECAI 2016. Frontiers in Artificial Intelligence and Applications. 2016. V. 285. P. 1594–1595.
5. *Цейтин Г. С.* О сложности вывода в исчислении высказываний // Записки научных семинаров ЛОМИ АН СССР. 1968. Т. 8. С. 234–259.
6. *Semenov A., Otpuschennikov I., Gribanova I., et al.* Translation of algorithmic descriptions of discrete functions to SAT with application to cryptanalysis problems // Log. Methods Comput. Sci. 2020. V. 16. Iss. 1. P. 29:1–29:42.
7. *Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем. М.: Наука, 1983.
8. *Агибалов Г. П.* Логические уравнения в криптоанализе генераторов ключевого потока // Вестник Томского госуниверситета. Приложение. 2003. № 6. С. 31–41.
9. *Semenov A., Zaikin O., Otpuschennikov I., et al.* On cryptographic attacks using backdoors for SAT // Proc. 32nd AAAI Conf. 2018. P. 6641–6648.
10. *Boros E. and Hammer P.* Pseudo-Boolean optimization // Discr. Appl. Math. 2002. V. 123. Iss. 1–3. P. 155–225.
11. *Glover F. and Laguna M.* Tabu Search. Norwell: Kluwer Academic Publishers, 1997.
12. *Антонов К. В., Семёнов А. А.* Применение метаэвристических алгоритмов псевдобулевой оптимизации к поиску линеаризующих множеств в криптоанализе криптографических генераторов // Материалы 6-й Междунар. школы-семинара «Синтаксис и семантика логических систем». Иркутск: ИГУ, 2019. С. 13–18.
13. *Pavlenko A., Semenov A., and Ulyantsev V.* Evolutionary computation techniques for constructing SAT-based attacks in algebraic cryptanalysis // LNCS. 2019. V. 11454. P. 237–253.
14. *De Canniere C.* Trivium: A stream cipher construction inspired by block cipher design principles // LNCS. 2006. V. 4176. P. 171–186.
15. *Dinur I. and Shamir A.* Cube attacks on tweakable black box polynomials // LNCS. 2009. V. 5479. P. 278–299.
16. ЦКП Иркутский суперкомпьютерный центр СО РАН. `http://hpc.icc.ru`.

УДК 519.7 DOI 10.17223/2226308X/13/35

## О ДИФФЕРЕНЦИАЛАХ ДЛЯ МОДИФИКАЦИИ ШИФРА SIMON НА ОСНОВЕ СХЕМЫ ЛАЯ — МЕССИ[1]

А. А. Белоусова, Н. Н. Токарева

Рассматриваются блочный итеративный шифр Simon 32/64, основанный на сети Фейстеля, и его модификации на основе схемы Лая — Месси. Получены оценки вероятностей дифференциалов 12 раундов исходного шифра и его модификаций.

**Ключевые слова:** *схема Лая — Месси, сеть Фейстеля, дифференциальный криптоанализ.*

[1]Работа выполнена в рамках государственного задания Института математики им. С. Л. Соболева СО РАН (проект № 0314-2019-0017) при поддержке РФФИ (проект № 18-07-01394) и Лаборатории криптографии JetBrains Research.

В работе рассматриваются блочные итеративные шифры, основанные на сети Фейстеля (рис. 1) и на альтернативной схеме — схеме Лая — Мэсси [1] (рис. 2). Для исследования выбран шифр Simon 32/64 [2], основанный на сети Фейстеля, и построены две его модификации подстановкой схемы Лая — Мэсси на место сети Фейстеля. Получены оценки вероятностей дифференциалов, построенных для 12 раундов исходной и модифицированных версий шифра Simon 32/64. Оценка вероятности дифференциалов для шифра Simon 32/64 взята из работы [3]: максимальная вероятность дифференциала после прохождения 12 раундов составляет $2^{-36}$.

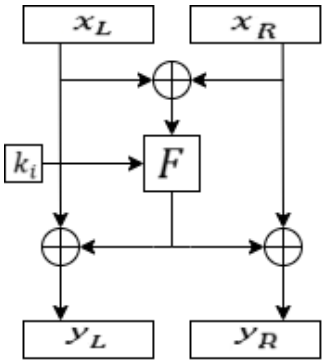


Рис. 1. Сеть Фейстеля

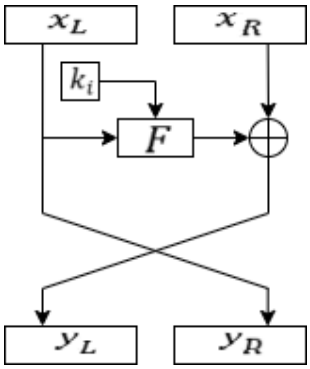


Рис. 2. Схема Лая — Месси

Один раунд схемы Лая — Мэсси в её оригинальном виде записывается как $(y_L, y_R) = (x_L \oplus F(x_L \oplus x_R), x_R \oplus F(x_L \oplus x_R))$, и в этом есть существенный недостаток: для любого входа $(x_L, x_R)$ выполняется соотношение $x_L \oplus x_R = y_L \oplus y_R$, где $(y_L, y_R)$ — выход раунда. В работе [4] отмечено, что для устранения этого недостатка к схеме необходимо добавить перестановку-ортоморфизм $\sigma$.

Пусть $\sigma\colon \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ — перестановка на $\mathbb{Z}_2^n$; $\sigma$ называется *ортоморфизмом* $\mathbb{Z}_2^n$, если $\sigma \oplus I$ — также перестановка на $\mathbb{Z}_2^n$, где $I$ — тождественная перестановка. Тогда один раунд схемы записывается как $(y_L, y_R) = (\sigma(x_L \oplus F(x_L \oplus x_R)), x_R \oplus F(x_L \oplus x_R))$, а разница текстов $y_L \oplus y_R = \sigma(x_L \oplus F(x_L \oplus x_R)) \oplus (x_R \oplus F(x_L \oplus x_R))$.

Проведено сравнение оценок вероятностей дифференциалов [5] оригинальной схемы Лая — Месси и схемы с добавлением ортоморфизма. Для этого написана программа, которая реализует перебор всех разностей открытых текстов. На каждой итерации шифра находится один из наиболее вероятных выходов на раунде с помощью построения строки таблицы дифференциалов, соответствующей входной разности. Далее найденные вероятности перемножаются для получения оценки максимальной вероятности дифференциалов.

После 12 раундов оценка для максимальной вероятности дифференциала для модернизированного шифра Simon32/64 без добавления ортоморфизма составляет $2^{-24}$, а с добавлением ортоморфизма находится в интервале между $2^{-24}$ и $2^{-63}$.

Таким образом, оценка максимальной вероятности дифференциала модернизации шифра Simon 32/64 без добавления ортоморфизма выше, чем у оригинального шифра. Компьютерные вычисления на части данных позволяют предположить, что модернизация с ортоморфизмом может быть более устойчивой, чем оригинальный шифр и модернизация без ортоморфизма.

## ЛИТЕРАТУРА

1. *Nakahara J.* Lai — Massey Cipher Designs. History, Design Criteria and Cryptanalysis. Springer Nature Switzerland AG, 2018.

2. *Beaulieu R., Shors D., Smith J., et al.* The Simon and Speck Families Of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013.
3. *Abed F., List E., Lucks S., and Wenzel J.* Differential and Linear Cryptanalysis of Reduced-Round Simon. ePrint Archive, Report 2013/526, 2013.
4. *Vaudenay S.* On the Lai — Massey Scheme // ASIACRYPT'99. LNCS. 1999. V. 1716. P. 8–19.
5. *Biham E. and Shamir A.* Differential Cryptanalysis of the Data Encryption Standard. Berlin; Heidelberg: Springer, 1993.

УДК 004.056.55 DOI 10.17223/2226308X/13/36

# КОДИРОВАНИЕ ИНФОРМАЦИИ МАТРИЦАМИ УОЛША

М. С. Беспалов, К. М. Малкова

Рассмотрено представление общей линейной группы $\mathrm{GL}(n,2)$ подгруппой автоморфизмов $\mathrm{GL}(N,2)$ при мультипликативной нотации в её действии в пространстве $\mathbb{R}^N$, где $N=2^n$. Каждая матрица как элемент группы $\mathrm{GL}(n,2)$ определяет упорядочения группы $\mathbb{Z}_2^n$ и её группы характеров, популярных при цифровой обработке информации в виде дискретных функций Уолша. На основе быстрого преобразования Уолша и данного соответствия создан программный прототип автоматической системы кодирования выходного сигнала в виде перестановки набора спектральных характеристик.

**Ключевые слова:** *дискретные функции Уолша, кодовая матрица, быстрое преобразование Уолша, кронекерово произведение.*

Для $\mathbb{Z}_2$ — аддитивной группы поля $\mathbb{F}_2$ — существуют разные представления, среди которых нас интересуют её мультипликативное представление $(\{1,-1\};\cdot)$ и векторное представление $(\{S,A\};\circ)$ с операцией умножения по Адамару векторов $S=(1\ 1)$, $A=(1\ -1)\in\mathbb{R}^2$. Для декартова произведения $\mathbb{Z}_2^n$ группы аддитивное представление рассматривается относительно операции $\oplus$ покоординатного сложения по модулю 2, а мультипликативное — относительно той же операции $\circ$ покоординатного умножения.

Популярные при цифровой обработке сигналов *дискретные функции Уолша* [1, 2] уровня $n$ в работе [3] определены без привлечения нумерации как кронекерово произведение векторов $S$ и $A$ в количестве $n$ сомножителей.

**Теорема 1.** Множество дискретных функций Уолша уровня $n$ составляет подгруппу $G$ мультипликативной группы $\mathbb{Z}_2^N$, где $N=2^n$, изоморфную группе $\mathbb{Z}_2^n$.

При декартовом произведении $\mathbb{Z}_2^n$ векторного представления $\mathbb{Z}_2=(\{S,A\};\circ)$ элементы будем записывать через разделительный знак $\otimes$, совпадающий с символом кронекерова произведения, что доказывает изоморфизм. Если перейдём к числам $S=(1\ 1)$ и $A=(1\ -1)$ и выполним кронекерово произведение, то получим элементы мультипликативной группы $\mathbb{Z}_2^N$. На основе свойства

$$(u\otimes v)\circ(w\otimes t)=(u\circ w)\otimes(v\circ t),$$

верного для $u,w\in\mathbb{R}^k$, $v,t\in\mathbb{R}^m$, устанавливается их групповое свойство.

Рассмотренная подгруппа $G\subseteq\mathbb{Z}_2^N$ составляет группу характеров конечной абелевой группы $\mathbb{Z}_2^n$, изоморфизм которых вытекает из теории двойственности Понтрягина [4].

Для решения задач цифровой обработки информации [2] эти группы нас интересуют в виде упорядоченных групп. В [5] подробно разбираются три известные нумерации