

- в)  $\delta_H$  в первом случае принимает значения, приблизительно равные  $\delta$  функций классов  $\mathcal{P}_{n,k}$  (очень редко получаются значения лучше или хуже), а во втором случае сохраняется значение  $2^n$  (как у функций класса  $\mathcal{S}_{n,k}$ );
- г)  $N(H)$  в обоих случаях может принимать разные значения, в основном они лучше, чем наихудшие значения у функций, используемых в композициях.

## ЛИТЕРАТУРА

1. *Pankratova I. A.* Construction of invertible vectorial Boolean functions with coordinates depending on given number of variables // Материалы Междунар. науч. конгресса по информатике: Информационные системы и технологии. Республика Беларусь, Минск, 24–27 окт. 2016. Минск: БГУ, 2016. С. 519–521.
2. *Agibalov G. P.* Substitution block ciphers with functional keys // Прикладная дискретная математика. 2017. № 38. С. 57–65.
3. *Панкратова И. А.* Об обратимости векторных булевых функций // Прикладная дискретная математика. Приложение. 2015. № 8. С. 35–37.
4. *Carlet C.* Vectorial Boolean Functions for Cryptography. Cambridge: Cambridge University Press, 2010. 93 p.
5. *Canteaut A.* Lecture Notes on Cryptographic Boolean Functions. Paris: Inria, 2016. 48 p.
6. *Nyberg K.* Differentially uniform mappings for cryptography // LNCS. 1994. V. 765. P. 55–64.
7. *Киселева Н. М., Лунатова Е. С., Панкратова И. А., Трифонова Е. Е.* Алгоритмы вычисления криптографических характеристик векторных булевых функций // Прикладная дискретная математика. 2019. № 46. С. 78–87.
8. *Кнут Д.* Искусство программирования. Т. 2. Получисленные алгоритмы. М.: Вильямс, 2007. 832 с.

УДК 519.7

DOI 10.17223/2226308X/13/7

## КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА ОРТОМОРФИЗМОВ<sup>1</sup>

Ю. П. Максимлюк

Рассмотрены взаимно однозначные отображения  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ , называемые ортоморфизмами, такие, что отображения  $G(x) = F(x) \oplus x$  также являются взаимно однозначными. Они используются в схеме Лая — Месси в качестве перемешивающего элемента между раундами, а также для построения криптографически стойких S-блоков. Исследованы основные криптографические свойства: нелинейные характеристики и дифференциальная равномерность. Выявлено, что ортоморфизмы от малого числа переменных не устойчивы к линейному и дифференциальному криптоанализам.

**Ключевые слова:** ортоморфизм, таблица линейного преобладания, таблица дифференциалов.

В симметричной криптографии часто используются отображения множества  $\mathbb{Z}_2^n$ , состоящего из двоичных наборов длины  $n$ , на себя. В частности, в [1] в шифрах FOX (IDEA NXT), использующих схему Лая — Месси, предлагается использовать отображение, называемое ортоморфизмом.

<sup>1</sup>Работа выполнена при поддержке Математического центра в Академгородке (г. Новосибирск), соглашение с Министерством науки и высшего образования Российской Федерации № 075-15-2019-1613, и Лаборатории криптографии JetBrains Research.

Ортоморфизм  $\mathbb{Z}_2^n$  — это взаимно однозначное отображение  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ , такое, что отображение  $G(x) = F(x) \oplus x$  также является взаимно однозначным.

В литературе в основном освещаются перемешивающие свойства ортоморфизмов. Например, в [2] ортоморфизмы характеризуются свойством отображать каждую максимальную подгруппу группы двоичных наборов длины  $n$  наполовину в себя и наполовину в своё дополнение.

В рамках данной работы разработан и программно реализован рекурсивный алгоритм построения всех ортоморфизмов для заданного  $n$ . Алгоритм перебирает все значения для  $k$ -го элемента и проверяет выполнение определения ортоморфизма. Если проверка успешна, то переходим к  $(k + 1)$ -му элементу, иначе проверяем следующее значение  $k$ -го. Когда проверены все возможные значения для  $k$ -й позиции, происходит возврат к дальнейшей проверке значений для позиции  $k - 1$ .

С помощью этой программы получены все ортоморфизмы для малых значений  $n$  и один ортоморфизм для  $n = 16$  для исследования модификации шифра Simon 32/64 [3], где вместо сети Фейстеля использована схема Лая — Мессе.

Получено, что:

- при  $n = 2$  существует 8 ортоморфизмов;
- при  $n = 3$  существует 384 ортоморфизма;
- при  $n = 4$  существует 244744192 ортоморфизма.

Для всех полученных ортоморфизмов экспериментально исследованы основные криптографические свойства: нелинейные характеристики и дифференциальная равномерность.

Обозначим вход и выход функции  $F : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$  через  $x = (x_1, \dots, x_n)$  и  $y = (y_1, \dots, y_n)$  соответственно. Для линейного криптоанализа строится таблица линейного преобладания, где на пересечении строки  $u \in \mathbb{Z}_2^n$  и столбца  $v \in \mathbb{Z}_2^n$  находится число  $\lambda$ , такое, что соотношение  $\langle u, x \rangle = \langle v, y \rangle$  выполняется с вероятностью  $(2^{n-1} + \lambda)/2^n$ , где  $\langle u, x \rangle = u_1x_1 \oplus \dots \oplus u_nx_n$ .

**Утверждение 1.** При  $n = 2, 3$  и 4 таблицы линейного преобладания ортоморфизмов состоят из значений 0 и  $\pm 2^{n-1}$ .

Для дифференциального криптоанализа в таблице дифференциалов на пересечении строки  $u \in \mathbb{Z}_2^n$  и столбца  $v \in \mathbb{Z}_2^n$  находится число  $\lambda$ , такое, что равенство  $F(x \oplus u) \oplus F(x) = v$  выполняется в точности для  $\lambda$  различных  $x$ .

**Утверждение 2.** При  $n = 2, 3$  и 4 таблицы дифференциалов ортоморфизмов состоят из значений 0 и  $2^n$ .

Для полученного ортоморфизма при  $n = 16$  также исследовались таблицы линейного преобладания и дифференциалов. Таблица линейного преобладания состоит из значений 0 и  $\pm 2^{n-1}$ , а таблица дифференциалов — из 0 и  $2^n$ .

Утверждения 1, 2 и точечное исследование ортоморфизма для  $n = 16$  позволяют предположить, что для любого значения  $n$  таблицы дифференциалов и линейного преобладания ортоморфизмов имеют вид, описанный выше. Из этого следует, что ортоморфизмы не устойчивы к линейному и дифференциальному криптоанализам и должны использоваться в шифрах в качестве вспомогательных элементов для построения более устойчивых к криптоанализу перемешивающих отображений.

## ЛИТЕРАТУРА

1. Nakahara J. Jr. Lai-Massey Cipher Designs. History, Design Criteria and Cryptanalysis. Springer, 2018. 726 p.

2. *Mittenthal L.* Block substitutions using orthomorphic mappings // *Adv. Appl. Math.* 1995. V. 16. Iss. 1. P. 59–71.
3. *Beaulieu R., Shors D., Smith J., et al.* The Simon and Speck Families Of Lightweight Block Ciphers. *Cryptology ePrint Archive*, Report 2013/404, 2013.

УДК 519.7

DOI 10.17223/2226308X/13/8

## О РАЗЛОЖЕНИИ ВЕКТОРНОЙ БУЛЕВОЙ ФУНКЦИИ В КОМПОЗИЦИЮ ДВУХ ВЕКТОРНЫХ ФУНКЦИЙ<sup>1</sup>

Г. М. Пинтус

Исследуется возможность представления векторной булевой функции в виде композиции двух векторных булевых функций меньшей алгебраической степени. Вводится понятие разложимости векторной булевой функции. Изучен вопрос сохранения разложимости при расширенном аффинном преобразовании. Представлена конструкция векторной булевой функции третьей степени от произвольного числа переменных, являющейся разложимой. Проведён вычислительный эксперимент, в результате которого показано, что все кубические векторные булевы функции от трёх переменных являются разложимыми.

**Ключевые слова:** векторная булева функция, декомпозиция, пороговая реализация.

Атаки по сторонним каналам [1] — вид атак, целью которых является нахождение уязвимостей в реализации криптографической системы. На данный момент эти атаки являются одними из наиболее эффективных среди всех видов криптоанализа. В атаках по сторонним каналам используется информация, полученная при отслеживании перепадов напряжений, времени выполнения процессов, электромагнитного излучения или звуков при проводимых алгоритмом вычислениях.

Пороговая реализация [2] является контрмерой по отношению к атакам по сторонним каналам, она разделяет наборы входных данных и используемые векторные булевы функции на части, позволяя скрыть различия между операциями. Таким образом, если разбиение удовлетворяет ряду условий, при работе алгоритма не происходит утечки информации, которая может быть использована в атаке по сторонним каналам.

В данном методе необходимо построить разбиение для векторной булевой функции определённым образом, что не всегда удаётся сделать. Однако придуман способ решения проблемы, использующий построение разбиения для более простых функций, композицией которых является исходная векторная булева функция.

В настоящей работе анализируется возможность представления векторных булевых функций в виде композиции векторных булевых функций меньших степеней. Рассмотрены векторные булевы функции от трёх переменных с алгебраической степенью равной трём и возможность их представления в виде композиции двух векторных булевых функций алгебраической степени два.

Так как важно сохранение свойств при преобразованиях, а одним из наиболее распространённых является расширенное аффинное преобразование, мы исследуем вопрос сохранения разложимости векторной булевой функции при расширенной аффинной эквивалентности.

*Векторной булевой функцией*  $((n, m)$ -функцией)  $F$  называется произвольное отображение  $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ . В случае  $m = 1$  говорят, что  $F$  — *булева функция от  $n$  переменных*.

<sup>1</sup>Работа выполнена при поддержке Лаборатории криптографии JetBrains Research.