**Следствие 3.** В условиях теоремы 1 существует $n_0$, такое, что для любых $\varepsilon_1, \varepsilon_2 > 0$, $n > n_0$ верны неравенства

$$(1-\varepsilon_1)\exp_2\left(m2^n - T(n,m,k) + (m-1)N(n,1,k)\right) < |R(m,n,k)| <$$
$$< (1+\varepsilon_2)\exp_2\left(m2^n - T(n,m,k) + (m-2)N(n,m,k) + N(n,1,k)\right).$$

Данные оценки уточняют или улучшают результаты работ [1, 4] в связи с [8].

ЛИТЕРАТУРА


1. *Панков К. Н.* Асимптотические оценки для чисел двоичных отображений с заданными криптографическими свойствами // Математические вопросы криптографии. 2014. № 4. С. 73–97.
2. *Логачев О. А., Сальников А. А., Смышляев С. В., Ященко В. В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2012.
3. *Carlet C.* Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Encyclopedia of Mathematics and its Applications. V. 134. N.Y.: Cambridge University Press, 2010. P. 398–472.
4. *Денисов О. В.* Локальная предельная теорема для распределения части спектра случайной двоичной функции // Дискретная математика. 2000. № 1. С. 82–95.
5. Словарь криптографических терминов. М.: МЦНМО, 2006.
6. *Сачков В. Н.* Курс комбинаторного анализа. Ижевск: НИЦ «Регулярная и хаотическая динамика», 2013.
7. *Панков К. Н.* Оценки скорости сходимости в предельных теоремах для совместных распределений части характеристик случайных двоичных отображений // Прикладная дискретная математика. 2012. № 4. С. 14–30.
8. *Canfield E. R., Gao Z., Greenhill C., et al.* Asymptotic enumeration of correlation-immune Boolean functions // Cryptography and Communications. 2010. No. 1. P. 111–126.


УДК 519.7 DOI 10.17223/2226308X/10/21

# КОМПОНЕНТНАЯ АЛГЕБРАИЧЕСКАЯ ИММУННОСТЬ S-БЛОКОВ, ИСПОЛЬЗУЮЩИХСЯ В НЕКОТОРЫХ БЛОЧНЫХ ШИФРАХ

Д. П. Покрасенко

Установлено точное значение компонентной алгебраической иммунности S-блоков, которые используются в работе известных блочных шифров. Получено, что такие шифры, как DES, CAST-256, KASAMI, PRESENT не обладают максимальной иммунностью и потенциально являются менее стойкими к алгебраическому криптоанализу.

**Ключевые слова:** *векторная булева функция, компонентная алгебраическая иммунность, S-блоки, DES, AES, PRESENT, KUZNYECHIK.*

Известно, что любой шифр можно представить в виде системы булевых уравнений, которые описывают его работу. Данная система строится на основе известного алгоритма шифрования и позволяет связать между собой биты открытого текста, ключа и шифротекста. Решение систем булевых уравнений в общем случае является NP-трудной задачей. Существуют различные алгоритмы решения таких систем, но большинство из них решают только линейные системы либо нелинейные при достаточно низком значении степени уравнений, трудоёмкость нахождения решения в таком случае слишком велика. Подробнее с методами решения систем булевых уравнений можно ознакомиться в [1].

В 2003 г. N. Courtois и W. Meier [2] предложили новый метод криптоанализа шифров, который был назван алгебраическим криптоанализом. Основная его идея заключается в процессе линеаризации булевых систем уравнений и сведении их к уравнениям меньшей степени, решение которых — менее сложная задача. Появление нового вида атаки привело к необходимости исследования свойств булевых функций, наличие которых позволяет затруднить применение данного критоанализа.

В 2004 г. W. Meier, E. Pasalic и C. Carlet [3] ввели понятие алгебраической иммунности $\mathrm{AI}(f)$ для булевых функций. В частности, было установлено, что высокая алгебраическая иммунность позволяет противостоять алгебраическим атакам. *Алгебраической иммуностью* $\mathrm{AI}(f)$ булевой функции $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется минимальное число $d$, такое, что существует булева функция $g$ степени $d$, не тождественно равная нулю, для которой $fg = 0$ или $(f \oplus 1)g = 0$.

Данное понятие различными способами обобщено на векторный случай. Одним из наиболее естественных обобщений является понятие компонентной алгебраической иммунности, введённое C. Carlet [4]. *Компонентной алгебраической иммунностью* $\mathrm{AI}_{\mathrm{comp}}(F)$ векторной булевой функции $F : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ называется минимальная алгебраическая иммунность компонентных функций $b \cdot F$ ($b \in \mathbb{Z}_2^m$, $b \neq 0$), т. е. $\mathrm{AI}_{\mathrm{comp}}(F) = \min\{\mathrm{AI}(b \cdot F) : b \in \mathbb{Z}_2^m, b \neq 0\}$, где $b \cdot F = b_1 f_1 \oplus \ldots \oplus b_m f_m$.

Наличие высокой компонентной алгебраической иммунности способствует наилучшему противостоянию различным методам алгебраических атак. В [5] установлено, что в случае нечётного $n$ если векторная булева функция обладает максимальной компонентной алгебраической иммунностью, то она является сбалансированной, и построены примеры функций с максимальной компонентной иммунностью для малых значений $n, m$.

Основу блочных шифров составляют S-блоки, которые и являются векторными булевыми функциями. В данной работе проведён анализ компонентной алгебраической иммунности S-блоков, использующихся в различных блочных шифрах.

Ниже приведена таблица, в которой указан год создания шифра, его название, размер S-блока, значение компонентной алгебраической иммунности и максимально возможное значение компонентной алгебраической иммунности при данных параметрах $n, m$. Будем обозначать через $n \to m$ векторную булеву функцию (S-блок), действующий из $\mathbb{Z}_2^n$ в $\mathbb{Z}_2^m$.

| Год | Шифр | Размер блока | $\mathrm{AI}_{\mathrm{comp}}(F)$ | Max |
|---|---|---|---|---|
| 1977 | DES | $6 \to 4$ | 2 | 3 |
| 1989 | ГОСТ 28147-89 | $4 \to 4$ | 2 | 2 |
| 1996 | CAST-256 | $8 \to 32$ | 2 | 4 |
| 1997 | SQUARE | $8 \to 8$ | 2 | 4 |
| 1998 | CRYPTON | $8 \to 8$ | 4 | 4 |
| 1998 | AES | $8 \to 8$ | 4 | 4 |
| 1998 | KASAMI | $7 \to 7$ | 3 | 4 |
| 2006 | SM4 | $8 \to 8$ | 4 | 4 |
| 2007 | PRESENT | $4 \to 4$ | 1 | 2 |
| 2013 | FIDES | $6 \to 6$ | 3 | 3 |
| 2015 | KUZNYECHIK | $8 \to 8$ | 4 | 4 |

Видно, что далеко не все шифры обладают максимальной компонентной алгебраической иммунностью. Такие шифры потенциально являются менее стойкими к алгебраическому криптоанализу.

ЛИТЕРАТУРА

1. *Агибалов Г. П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник Томского государственного университета. Приложение. 2006. № 17. С. 4–9.
2. *Courtois N. and Meier W.* Algebraic attacks on stream ciphers with linear feedback // Eurocrypt 2003. LNCS. 2003. V. 2656. P. 345–359.
3. *Meier W., Pasalic E., and Carlet C.* Algebraic attacks and decomposition of Boolean functions // Eurocrypt 2004. LNCS. 2004. V. 3027. P. 474–491.
4. *Carlet C.* On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions // Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes. Amsterdam: IOS Press, 2009. P. 104–116.
5. *Покрасенко Д. П.* О максимальной компонентной алгебраической иммунности векторных булевых функций // Дискретный анализ и исследование операций. 2016. Т. 23. № 2. С. 88–99.

УДК 512.13 DOI 10.17223/2226308X/10/22

# СПОСОБ ПРЕДСТАВЛЕНИЯ ПОДСТАНОВОК $S_{16}$ С ПОМОЩЬЮ АЛГЕБРАИЧЕСКИХ ПОРОГОВЫХ ФУНКЦИЙ

Д. А. Сошин

Предлагается алгоритм представления подстановок на множестве элементов $\{0, 1, \ldots, 15\}$ с помощью линейных комбинаций алгебраических пороговых функций. Получаемые задания могут быть использованы для эффективной реализации на перспективной оптической элементной базе нелинейных преобразований узлов переработки информации.

**Ключевые слова:** *алгебраические пороговые функции, геометрические типы, подстановки, блочные шифры.*

**Определение 1.** Функцию $k$-значной логики $f : \Omega_k^n \to \Omega_k$ назовём *алгебраической пороговой* (АПФ), если существуют целочисленные наборы $\mathbf{c} = (c_0, c_1, \ldots, c_n)$, $\mathbf{b} = (b_0, b_1, \ldots, b_k)$ и натуральный модуль $m$, такие, что для любого $\alpha \in \Omega_k$ выполняется

$$f(x_1, x_2, \ldots, x_n) = \alpha \quad \Leftrightarrow \quad b_\alpha \leqslant r_m(c_0 + c_1x_1 + c_2x_2 + \ldots + c_nx_n) < b_{\alpha+1},$$

где $r_m(x)$ — функция взятия остатка числа $x$ по модулю $m$, $r_m(x) \in \{0, 1, \ldots, m-1\}$; $\Omega_k = \{0, 1, \ldots, k-1\}$. Тройку $(\mathbf{c}, \mathbf{b}, m)$ будем называть *структурой функции* $f$.

В случае двузначной логики АПФ будем задавать следующим образом:

$$f = 1 \quad \Leftrightarrow \quad r_m(c_0 + c_1x_1 + c_2x_2 + \cdots + c_nx_n) \geqslant b$$

и писать $f : ((c_0, c_1, c_2, \ldots, c_n); b; m)$.

В [1] исследован вопрос реализации булевых функций трёх переменных функциями из класса АПФ. Для этого доказана замкнутость данного класса относительно операций перестановки переменных, инвертирования переменных и инвертирования функции (геометрическая замкнутость). *Геометрическим типом функции* $f$ назовём класс эквивалентности относительно указанных преобразований. Для булевых функций от трёх переменных доказано, что только геометрический тип с представителем $f^*(x_1, x_2, x_3) = x_1x_3 \vee x_2\overline{x_3}$ не задаётся через АПФ. Для булевых функций от четырёх