УДК 004.056.55

ПОЛУТОРАБАЙТНЫЕ НЕЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ КОНСТРУКЦИИ НИБЕРГ

Д. А. Юровских, к. т. н. А. В. Соколов, А. О. Шипунова

Одесский национальный политехнический университет
Украина, г. Одесса
radiosquid@gmail.com

Настоящая работа посвящена актуальным вопросам конструирования полуторабайтных S-блоков подстановки для повышения эффективности современных шифров. Построены S-блоки подстановки конструкции Ниберг над всеми изоморфными представлениями поля $GF(2^{12})$, оценено их соответствие основным критериям криптографического качества.

Ключевые слова: S-блок подстановки, конструкция Ниберг, поле Галуа, изоморфизм.

Одним из важнейших этапов разработки любого современного симметричного алгоритма шифрования является построение нелинейного преобразования — S-блока подстановки, характеристики которого во многом обуславливают характеристики конструируемого шифра. Актуальность данного вопроса определяет значительное внимание к нему со стороны исследователей.

Результаты экспериментов [1] показывают, что криптографическое качество S-блоков подстановки и их способность противостоять атакам криптоанализа значительно улучшаются с ростом их длины N. Данное обстоятельство четко прослеживается исторически в виде роста длины применяемых в криптоалгоритмах S-блоков. Известный сегодня криптоалгоритм Rijndael (AES), который является стандартом шифрования США и одним из самых распространенных блочных шифров, использует S-блоки конструкции Ниберг с длиной входного слова k=8 бит, соответственно, с длиной кодирующей последовательности $N=2^k=256$. Исходя из этого, становится очевидным, что следующим шагом в истории развития нелинейных преобразований будет синтез и использование полуторабайтных S-блоков подстановки.

Целью настоящей работы является построение S-блоков подстановки конструкции Ниберг с длиной входного слова k=12 (полуторабайтных) над всеми изоморфными представлениями поля Галуа $GF(2^{12})$.

Конструкция Ниберг представляет собой отображение, задаваемое мультипликативно обратными элементами поля Галуа $GF(2^k)$:

$$y = x^{-1} \bmod[f(z), p], \quad y, x \in GF(2^k), \tag{1}$$

скомбинированное вместе с аффинным преобразованием

$$\mathbf{b} = \mathbf{A} \cdot \mathbf{y} + \mathbf{a}, \quad \mathbf{a}, \mathbf{b} \in GF(2^k), \tag{2}$$

где $f(z) = z^8 + z^4 + z^2 + z + 1$ — неприводимый над полем $GF(2^k)$ полином;

$\mathbf{A}$ — невырожденная матрица аффинного преобразования;

$\mathbf{a}$ — вектор сдвига;

$p = 2$ — характеристика расширенного поля Галуа, $0^{-1} \equiv 0$ — принято;

a, b, x, y — элементы расширенного поля Галуа $GF(2^k)$; рассматриваются либо как десятичные числа, либо двоичные векторы, либо полиномы степени k–1.

Основополагающая теорема полей Галуа гласит, что для каждого простого числа p и натурального n существует конечное алгебраическое поле порядка p^n, единственное с точностью до изоморфизма. Однако заметим, что методы синтеза кодов, ансамблей шумоподобных сигналов, стоимость аппаратуры генерации и обработки кодов и сигналов существенно зависят от выбора вида представления поля. Поэтому с прикладной точки зрения целесообразно различные представления поля порядка p^n рассматривать как различные поля [2].

Основное поле $GF(2^{12})$, рассматриваемое в данной работе, имеет следующие свои изоморфные представления:

$$GF(q^k) \Rightarrow GF(2^{12}) \Rightarrow GF(4^6) \Rightarrow GF(8^4) \Rightarrow GF(16^3) \Rightarrow GF(64^2). \quad (3)$$

Таким образом, исходя из (3), выражение (1) принимает вид

$$y = x^{-1}\text{moddd}[f_1(z), f_2(z), p], \quad y, x \in GF(2^k), \quad (4)$$

где $f_1(z)$ — неприводимый полином, определяющий операцию мультипликативного обращения в поле «нижнего уровня» $GF(q)$, $f_2(z)$ — то же самое, но в поле «верхнего уровня», т. е. расширение расширенного поля $GF(q^k)$.

Количества различных неприводимых полиномов [2] и, соответственно, количества различных структур S-блоков подстановки приведены в табл. 1.

Таблица 1

Количества различных неприводимых полиномов в поле $GF(q^k)$

Вид полинома	$GF(2^{12})$	$GF(4^6)$	$GF(8^4)$	$GF(16^3)$	$GF(64^2)$
$f_1(z)$ в поле $GF(q)$	1	1	2	2	6
$f_2(z)$ в поле $GF(q^k)$ для выбранного $f_1(z)$	335	670	1008	1360	2016
Все неприводимые полиномы в поле $GF(q^k)$	335	670	2016	2720	12096

Таким образом, общее количество S-блоков подстановки конструкции Ниберг, которые могут быть построены над всеми изоморфными представлениями поля $GF(2^{12})$, составляет J=17837. Результаты выборочного анализа криптографических свойств S-блоков подстановки на основе различных изоморфных представлений основного поля $GF(2^{12})$ приведены в табл. 2, где данные записаны в следующем порядке: алгебраическая степень нелинейности / расстояние нелинейности / максимум среди модулей коэффициентов корреляции.

Таблица 2

Криптографические характеристики построенных S-блоков подстановки

$GF(2^{12})$	$GF(4^6)$	$GF(8^4)$	$GF(16^3)$	$GF(64^2)$
11 / 1984 / 0,0293	11 / 1984 / 0,0293	11 / 1984 / 0,0283	11 / 1984 / 0,0313	11 / 1984 / 0,0313

Проведенные исследования показывают, что качество полуторабайтных S-блоков подстановки конструкции Ниберг значительно лучше, чем блоков длиной полбайта или байт. При этом криптографическое качество является относительно стабильным в различных изоморфных представлениях основного поля. Следовательно, применение полуторабайтных S-блоков подстановки конструкции Ниберг в симметричных шифрах является перспективным.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Соколов А. В. Новые методы синтеза нелинейных преобразований современных шифров.— Гамбург: Lambert Academic Publishing, 2015. — 100 с.

2. Мазурков, М. И., Соколов А. В. Нелинейные S-блоки конструкции Ниберг с максимальным лавинным эффектом // Известия ВУЗов. Радиоэлектроника, 2014. — Т. 57, № 6. — С. 47—55.

D. A. Yurovskykh, A. V. Sokolov, A. O. Shipunova

12-bit nonlinear transforms of Nyberg design

This paper is devoted to topical issues of construction of 12-bit substitution boxes for improvement in efficiency of modern ciphers. Substitution boxes of Nyberg's construction over all isomorphic representations of the $GF(2^{12})$ field were built and assessed for their compliance with basic criteria of cryptographic quality.

Keywords: S-box substitution, Nyberg design, Galois field, isomorphism.