УДК 004.056.55

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 2, pp. 142-148

ПОЛУТОРАБАЙТНЫЕ НЕЛИНЕЙНЫЕ ПРЕОБРАЗОВАНИЯ КОНСТРУКЦИИ НИБЕРГ

Д.А. Юровских, А.В. Соколов, Б.С. Троицкий

Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: radiosquid@gmail.com

Статья посвящена актуальным вопросам конструирования полуторабайтных S-блоков подстановки для повышения эффективности современных шифров. Построены полуторабайтные S-блоки конструкции Ниберг над всеми изоморфными представлениями поля $GF(2^{12})$, проведено их выборочное тестирование на соответствие основным критериям криптографического качества, которое показало, что полуторабайтные S-блоки обладают значительно лучшими криптографическими характеристиками, нежели однобайтные или полубайтные. Введен удобный для длинных S-блоков критерий удельного расстояния нелинейности, характеризующий «количество нелинейности» в элементе Q-последовательности либо значении булевой функции. Результаты работы позволяют утверждать, что построенные S-блоки могут быть эффективно использованы для модернизации современных шифров и построения новых перспективных криптоалгоритмов.

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

Введение

Повсеместное внедрение компьютерной техники во все сферы человеческой деятельности приводит к постоянному росту количества обрабатываемой, передаваемой и хранимой информации. Данное обстоятельство приводит к дальнейшей актуализации вопросов совершенствования методов защиты информации, в том числе, дальнейшего развития криптографических алгоритмов. В последнее время существенное распространение получили блочные криптоалгоритмы, что объясняется тем, что на сегодняшний день они обладают простой технической реализацией и высокими показателями криптографического качества.

Одним из важнейших этапов разработки любого современного симметричного блочного алгоритма шифрования является построение нелинейного преобразования — S-блока подстановки, характеристики которого во многом определяют характеристики конструируемого шифра. Так, в литературе достаточно много внимания уделяется проблеме построения высококачественных S-блоков, тем не менее, все они характеризуются длиной входного слова $k \le 10$ [1].

С другой стороны, результаты экспериментов [2] показывают, что криптографическое качество S-блоков подстановки и их способность противостоять атакам криптоанализа значительно улучшаются с ростом их длины $N = 2^k$. Данное обстоятельство четко прослеживается исторически в виде роста длины применяемых в криптоалгоритмах S-блоков. Так, на смену алгоритму DES, который использовал полубайтные S-блоки, пришел криптоалгоритм Rijndael (AES), который является ныне действующим стандартом шифрования США и использует S-блоки конструкции Ниберг с длиной входного слова $k = 8$ бит и, соответственно, с длиной Q-последовательности $N = 2^8 = 256$ (однобайтные). Исходя из этого, становится очевидно, что следующим шагом в конструировании новых криптоалгоритмов будет синтез и использование полуторабайтных S-блоков подстановки.

Процесс выбора S-блока является весьма трудоемким с вычислительной точки зрения, поэтому в современной криптографии принят подход, основанный на построении регулярных методов синтеза S-блоков с заранее определенными криптографическими характеристиками. Одним из таких методов является предложенная К. Нибергом конструкция, основанная на обращении элементов поля Галуа по модулю неприводимого полинома [3]. Тем не менее, в литературе S-блоки конструкции Ниберг синтезированы лишь для значений длины входного слова $k \le 10$, в то время как исследование характеристик более длинных S-блоков в литературе отсутствует.

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

Основная часть

Конструкция S-блоков подстановки классических блочных криптографических алгоритмов (например, ГОСТ 28147-89, Магма, Калина, BelT, DES, AES и др.) состоит из дешифратора, который преобразует *k*-разрядный двоичный сигнал в одноразрядный сигнал по модулю 2^k, системы внутренних связей (всего связей должно быть 2^k) и шифратора, который преобразует сигнал из одноразрядного 2^k -ичного в *k*-разрядный двоичный. Схема полуторабайтного S-блока представлена на рис. 1.

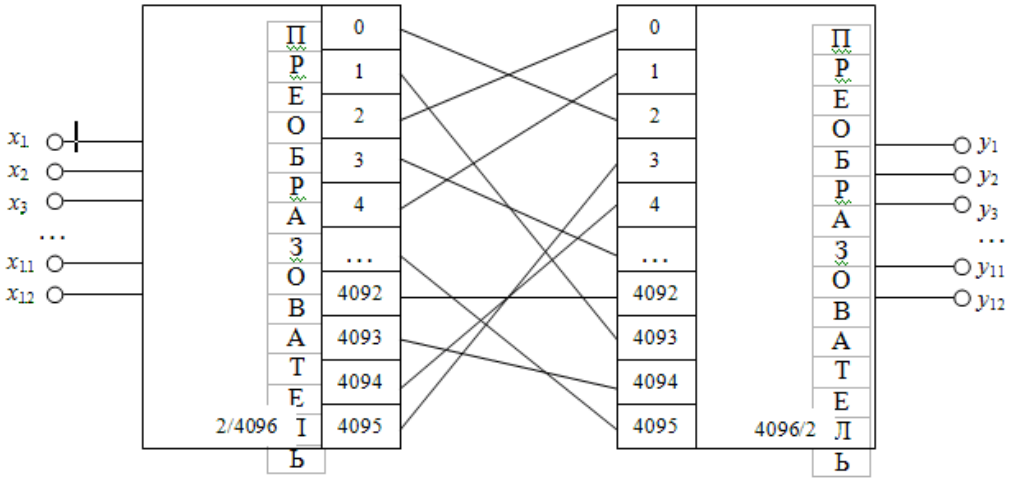

Рис. 1. Конструкция полуторабайтного S-блока подстановки

Очевидно, что S-блок подстановки определяет однозначное соответствие между электродами дешифратора и электродами шифратора или соответствующими ячейками памяти, которые реализуют блок программно. Данное правило часто записывают в виде кодирующей Q-последовательности, которая в свою очередь может быть представлена в виде k компонентных булевых функций. Криптографические свойства последних полностью определяют качество конструируемого S-блока.

S-блок называют биективным, если его кодирующая Q-последовательность содержит в своем составе все элементы тривиальной входной последовательности $\{0,1,...,2^{k-1}\}$, а все линейные комбинации компонентных булевых функций, соответственно, являются сбалансированными. Ясно, что всего биективных полуторабайтных S-блоков существует $J_{4096} = 2^k! = 4096!$, что является астрономической величиной. Данное обстоятельство полностью исключает

возможность поиска оптимальных структур Q-последовательностей переборными методами и диктует необходимость применения регулярных методов синтеза, одним из которых является ранее используемая для небольших длин S-блоков конструкция Ниберг [3].

Конструкция Ниберг, которая представляет собой отображение, задаваемое мультипликативно обратными элементами поля Галуа $GF(2^k)$ определяется следующим соотношением

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

скомбинированным вместе с аффинным преобразованием

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

где $f(z)$ – неприводимый над полем $GF(2^k)$ полином; A – невырожденная матрица аффинного преобразования; 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 как десятичные числа, либо двоичные векторы, либо полиномы степени $k-1$.

S-блоки, построенные в соответствии с выражениями (1) и (2) обладают высоким уровнем криптографического качества [4, 5]: высокой алгебраической степенью нелинейности, высоким расстоянием нелинейности, равномерной минимизацией коэффициентов корреляции. Существенным недостатком конструкции Ниберг является то, что количество различных структур высококачественных S-блоков равно количеству неприводимых полиномов над полем $GF(2^k)$, которое является весьма небольшим и определяется как [6]

$$|w_k| = \frac{1}{k} \sum_{\substack{d \\ d/k}} \mu(d) q^{(k/d)}, \tag{3}$$

где d – делители степени k; $\mu(d)$ – функция Мёбиуса; запись d/k означает, что d делит k нацело.

В случае небольших S-блоков подстановки данный недостаток удалось преодолеть за счет рассмотрения всех изоморфных представлений основного поля [1], однако, как показывают эксперименты, данный подход применим и для полуторабайтных S-блоков.

Так, основополагающая теорема полей Галуа гласит, что для каждого простого числа p и натурального k существует конечное алгебраическое поле порядка p^k, единственное с точностью до изоморфизма. Однако, оказывается, что свойства криптографических конструкций, ровно как и корректирующих кодов и шумоподобных сигналов, существенно зависят от выбора вида представления поля. Поэтому с прикладной точки зрения целесообразно различные представления поля порядка p^k рассматривать как различные поля.

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

$$GF(q^k) \Rightarrow GF(2^{12}) \Rightarrow GF(4^6) \Rightarrow GF(8^4) \Rightarrow GF(16^{13}) \Rightarrow GF(64^2). \tag{4}$$

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

$$y = x^{-1} \bmod dd\left[f_1(z), f_2(z), p\right], \quad y, x \in GF\left(q^k\right), \tag{5}$$

где $f_1(z)$ – неприводимый полином, определяющий операцию умножения в поле «нижнего уровня» $GF(q)$, $f_2(z)$ – в поле «верхнего уровня», т.е. расширении расширенного поля $GF(q^k)$.

Количества различных неприводимых полиномов [3] над различными представлениями основного поля (4), и соответственно, количества различных структур S-блоков подстановки, рассчитанные в соответствии с (3), приведены в табл. 1.

Таблица 1.

Количества различных неприводимых полиномов

Поле $GF(q^k)$	$GF(2^{12})$	$GF(4^6)$	$GF(8^4)$	$GF(16^3)$	$GF(64^2)$
Кол-во неприв. полиномов $f_1(z)$ в поле $GF(q)$	1	1	2	2	6
Кол-во неприв. полиномов $f_2(z)$ в поле $GF(q^k)$ для выбранного $f_1(z)$	335	670	1008	1360	2016
Общее кол-во неприв. полиномов 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, что является достаточным для использования данных высококачественных подстановочных конструкций в качестве долговременного ключа, а также для реализации концепции оперативной смены ключа.

В настоящей статье полученные полуторабайтные S-блоки были подвергнуты тестированию по следующим общепринятым критериям криптографического качества [4, 5]:

- алгебраическая степень нелинейности, определяемая как максимальная степень (наибольшее из количеств конъюнкций в терме) алгебраической нормальной формы представления компонентных булевых функций S-блока (минимум среди компонентных булевых функций);
- расстояние нелинейности, определяемое как минимальное расстояния Хэмминга от компонентных булевых функций S-блока до кодовых слов аффинного кода (минимум среди компонентных булевых функций);
- матрица коэффициентов корреляция, показывающая корреляционную взаимосвязь векторов выхода S-блока и векторов его входа.

Анализ криптографических свойств S-блоков большой длины, например, полуторабайтных представляет собой весьма сложную вычислительную задачу, что диктует необходимость проведения выборочного анализа на полном множестве построенных S-блоков. Результаты выборочного анализа криптографических свойств S-блоков подстановки на основе различных изоморфных представлений основных полей $GF(2^4)$, $GF(2^8)$, $GF(2^{12})$ приведены в табл. 2, где данные записаны в следующем порядке: алгебраическая степень нелинейности (расстояние нелинейности) максимум среди модулей коэффициентов корреляции.

Таблица 2.

Криптографические характеристики S-блоков подстановки

Поле	$GF(2^k)$	$GF(4^k)$	$GF(8^k)$	$GF(16^k)$	$GF(32^k)$	$GF(64^k)$
Полубайтные	3 / 4 / 0.25	3 / 4 /0.5	—	—	—	—
Однобайтные	7 / 112 / 0.125	7 / 112 / 0.125	—	7 / 112 / 0.125	—	—
Полуторабайтные	11 / 1984 / 0.0293	11 / 1984 / 0.0293	11 / 1984 / 0.0283	11 / 1984 / 0.0313	—	11 / 1984 / 0.0313

Анализ данных табл. 2 показывает существенный прирост в качестве построенных S-блоков, причем их качество является стабильным для различных изоморфных представлений основного поля.

Одним из наиболее показательных и практически ценных критериев является расстояние нелинейности. Так, расстояние нелинейности для конструкции Ниберг показывает значительный рост с увеличением их длины, что делает сравнительный анализ подстановочных конструкций неочевидным и затрудненным. Впервые, проведя оценку криптографических свойств S-блоков конструкции Ниберг столь большой длины $N = 2^k = 4096$, в настоящей работе авторами предлагается введение показателя удельного расстояния нелинейности

$$\eta_s = \frac{2 \cdot N_s}{N}, \eta_f = \frac{2 \cdot N_f}{N}, \tag{6}$$

где η_S — удельное расстояние нелинейности S-блока; η_f — удельное расстояние нелинейности булевой функции; N_s — расстояние нелинейности исследуемого S-блока; N_f — расстояние нелинейности исследуемой булевой функции; N — длина исследуемого S-блока или булевой функции.

Таким образом, по построению, удельное расстояние нелинейности показывает «количество нелинейности», содержащееся в одном элементе кодирующей *Q*-последовательности или в одном значении булевой функции. Так, нетрудно видеть, что для аффинных булевых функций $\eta = 0$, в то время как для бент-функций $\eta = \frac{2\left(2^{k-1} - 2^{(k/2)-1}\right)}{N} = \frac{2\left(2^{k-1} - 2^{(k/2)-1}\right)}{2^k}$ [7]. Нетрудно показать, что $\lim\limits_{k\to\infty} = \frac{2\left(2^{k-1} - 2^{(k/2)-1}\right)}{2^k} = \frac{2}{2} = 1$, таким образом удельное расстояние нелинейности бесконечно длинной булевой бент-функции достигает значения 1, в то время как $0 \le \eta_S < 1$, $0 \le \eta_f < 1$.

В виду схожести криптографических свойств S-блоков конструкции Ниберг над различными изоморфными представлениями основного поля $GF(2^k)$, а также с учетом результатов [8] построим на рис. 2 график эволюции удельного расстояния нелинейности

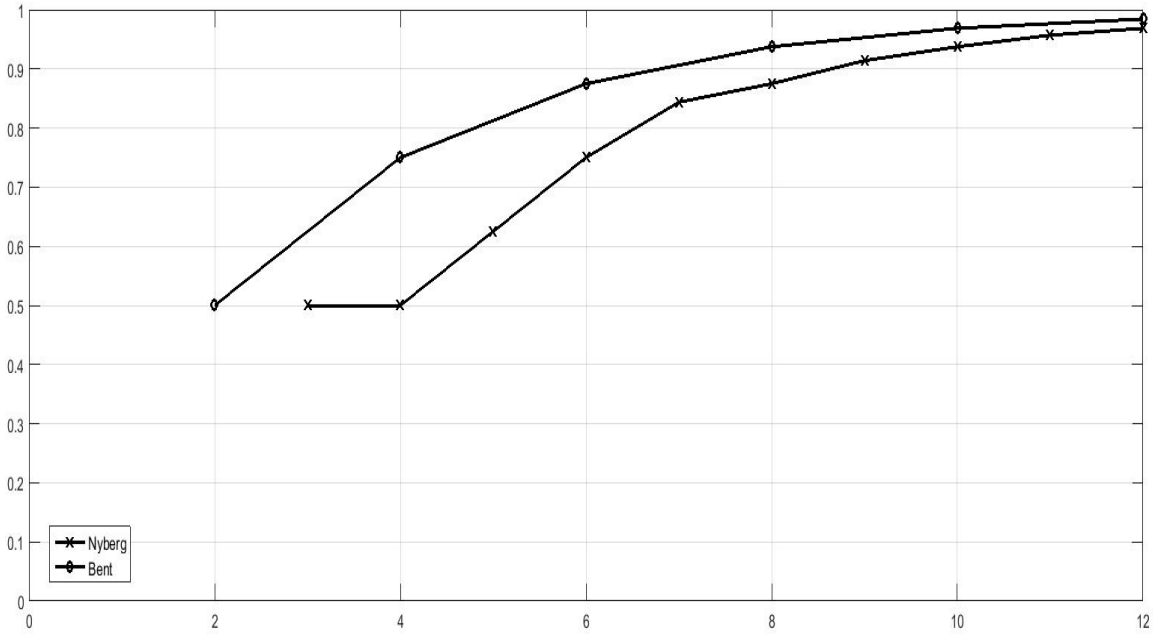

Рис. 2. Эволюция удельного расстояния нелинейности конструкции Ниберг и бент-функций

Детальный анализ данных рис. 2 показывает, что с увеличением длины S-блоков конструкции Ниберг их удельное расстояние нелинейности стремится к расстоянию нелинейности бент-функций. Так, для полуторабайтных S-блоков, отставание расстояния нелинейности S-блоков конструкции Нибрег от бент-функций составляет всего $\Delta_{12} = 0{,}0156{=}1{,}56\%$, в то время как для однобайтных S-блоков эта величина составляет $\Delta_8 = 0.0625 = 6.25\%$.

Выводы

1. Построен полный класс мощности $J{=}17837$ полуторабайтных S-блоков конструкции Ниберг над всеми изоморфными представлениями основного поля $GF(2^{12})$. Проведен выборочный анализ криптографического качества построенных S-блоков, который показал, что полуторабайтные S-блоки подстановки обладают значительно лучшим качеством, чем при длине входного слова полбайта или байт. При этом криптографическое качество является относительно стабильным в различных изоморфных представлениях основного поля.

2. Введен удобный для исследования длинных S-блоков критерий удельного расстояния нелинейности, показывающий «количество нелинейности», содержащееся в одном элементе кодирующей *Q*-последовательности или в одном значении булевой функции. Проведенный сравнительный анализ S-блоков конструкции Ниберг и бент-функций показал, что удельное расстояние нелинейности конструкции Ниберг приближается к удельному расстоянию нелинейности бент-функций с увеличением длины, при этом для полуторабайтных S-блоков величина отставания составляет $\Delta_{12} = 0{,}0156{=}1{,}56\%$.

3. Проведенные исследования подтверждают высокую перспективность применения полуторабайтных S-блоков подстановки конструкции Ниберг как для модернизации существующих криптоалгоритмов, так и для разработки новых криптоалгоритмов с большóй длиной блока.

Список литературы

1. Мазурков, М.И. Нелинейные S-блоки конструкции Ниберг с максимальным лавинным эффектом / М.И. Мазурков, А.В. Соколов // Известия высших учебных заведений. Радиоэлектроника. – 2014. – Т. 57. – N 6. – С. 47 – 55.
2. Ростовцев, А. Г. Большие подстановки для программных шифров / А.Г. Ростовцев // Проблемы инф. безопасности. Компьютерные системы. – СПб. – 2000. – № 3. – С. 31 – 34.
3. Nyberg, K. Differentially uniform mappings for cryptography. I Advances in cryptology / K. Nyberg // Proc. of EUROCRYPT'93. – Berlin, Heidelberg, New York. – 1994. – Vol.765. – Pp. 55 – 65.
4. Горбенко, І.Д. Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму RIJNDAEL (FIPS 197) / І.Д. Горбенко, О.В. Потій, Ю.А. Ізбенко // Радіотехніка: всеукр. міжвідом. наук.-техн. зб. – Харків, 2004 . – Т. 126. – С. 132 – 138.
5. Мазурков, М.И. Алгебраические свойства криптографических таблиц замен шифра Rijndael и шифра ГОСТ 28147-89 / М.И. Мазурков, А.В. Соколов. – Одесса: Труды СИЭТ. – 2012. – С. 149.
6. Берлекэмп, Э. Алгебраическая теория кодирования / Э. Берлекэмп // М: МИР. – 1971. – 477 с.
7. Токарева, Н.Н. Бент-функции: результаты и приложения. Обзор работ / Н.Н. Токарева // Приклад. дискрет. математика. – Томск, 2009. — №1(3). – С. 15–37.
8. Sokolov, A.V. Nyberg construction nonlinear transforms based on all isomorphic representations of the Galois field GF(512) [Электронный ресурс] / A.V. Sokolov // Проблеми телекомунікацій. – 2015. – № 2 (17). – С. 68 – 75. – Режим доступу: http://pt.journal.kh.ua/2015/2/1/152_sokolov_gf.pdf .

ПІВТОРАБАЙТНІ НЕЛІНІЙНІ ПЕРЕТВОРЕННЯ КОНСТРУКЦІЇ НІБЕРГ.

Д.А. Юровських, А.В. Соколов, Б.С. Троїцький

Одеський національний політехнічний університет,
просп. Шевченко, 1, Одеса, 65044, Україна; e-mail: radiosquid@gmail.com

Стаття присвячена актуальним питанням конструювання півторабайтних S-блоків підстановки для підвищення ефективності сучасних шифрів. Побудовано півторабайтні S-блоки конструкції Ніберг над усіма ізоморфними уявленнями поля $GF(2^{12})$, проведено їх вибіркове тестування на відповідність основним критеріям криптографічної якості, яке показало, що півторабайтні S-блоки мають значно кращі криптографічні характеристики у порівнянні з однобайтними або полубайтними. Введено зручний для довгих S-блоків критерій питомої відстані нелінійності, що характеризує «кількість нелінійності» в елементі Q-послідовності або значенні булевої функції. Результати роботи дозволяють стверджувати, що побудовані S-блоки можуть бути ефективно використані як для модернізації сучасних шифрів, так і для побудови нових перспективних криптоалгоритмів.

Ключові слова: S-блок підстановки, конструкція Ніберг, поле Галуа, ізоморфізм.

NIBERG CONSTRUCTION 12 BIT NONLINEAR TRANSFORMS.

D.A. Yurovsky, A.V. Sokolov, B.S. Troitsky

Odessa National Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: radiosquid@gmail.com

The article is devoted to the actual issues of the construction of 12 bit S-boxes in order to improve the effectiveness of modern ciphers. We built the full class of 12 bit S-boxes of Nyberg construction over all isomorphic representations of the field $GF(2^{12})$, performed their sample testing for compliance to the basic criteria of cryptographic quality, which showed that 12 bit S-boxes have much better cryptographic properties than 8 bit or 4 bit ones. We introduced new criterion of specific distance of nonlinearity for long S-boxes which characterizes "the number of non-linearity" in item of Q-sequence or single value of a Boolean function. The results suggest that the constructed S-boxes can be effectively used for the modernization of existing chipers and construction of modern promising cryptographic algorithms.

Keywords: S-box, Nyberg's construction, Galois field, isomorphism.