ТРУДЫ

XIV МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И ЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ

27—31 мая 2013 г.
Украина, г. Одесса

Том I

ТРУДИ

XIV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

СУЧАСНІ ІНФОРМАЦІЙНІ ТА ЕЛЕКТРОННІ ТЕХНОЛОГІЇ

27—31 травня 2013 р.
Україна, м. Одеса
Том I

PROCEEDING

OF THE XIVth INTERNATIONAL SCIENTIFIC-PRACTICAL CONFERENCE

MODERN INFORMATION AND ELECTRONIC TECHNOLOGIES

27—31 May, 2013
Ukraine, Odessa
Volume I

В. М. Дмитриев, Т. Н. Зайченко, Ю. А. Шурыгин. Моделирование технических средств автоматизации и управления на базе метода компонентных цепей 157
С. А. Положаенко, Омар Муаяд Абдуллах. Мультимедийная информационная технология реализации средств математического моделирования диффузионных процессов 161
С. А. Положаєнко, Ю. В. Григоренко. Математичні моделі процесів та апаратів первинної обробки сирих вуглеводнів 163
Г. В. Шаповалов. Разработка программного комплекса для исследования оптимального расположения элементов электронной техники в трехмерном пространстве 165
В. А. Тудоран. Двумерное моделирование погружения жесткого контура произвольной формы с учетом брызговой струи по схеме Эйлера—Лагранжа 167
Г. М. Гайдаржи, А. С. Чебаненко, В. С. Ситников. Диверсификация методов анализа и обработки нестационарных рядов на основе самообучающейся нейронной сети 170
А. В. Никорак, А. А. Саченко, А. Ю. Рощупкин. Усовершенствованная подсистема стабилизации и маневрирования мобильного балансирующего робота 172
К. В. Защелкин, В. В. Калиниченко, Н. О. Ульченко. Комбинированный способ навигации автономного мобильного робота 174
В. С. Ситніков, Т. П. Яценко, А. М. Теплечук, І. С. Флоренко. Реалізація управління перебудовою вузла фільтрації у спеціалізованій комп'ютерній системі управління автомобільним двигуном 178

Секция 2

Защита информации в широкополосных системах и компьютерных сетях

А. А. Кобозева, О. В. Николаенко, В. С. Васьковец. Преобразование спектра симметричной матрицы как возможная основа стеганографического алгоритма для произвольного цифрового изображения-контейнера 182
И. И. Бобок, А. А. Кобозева. Алгоритм выявления нарушения целостности цифрового изображения 184
Б. В. Хлопов, Ю. С. Бондарев, Б. С. Лобанов, А. В. Шпак, А. Ю. Митягин. Устойчивость магнитных свойств материалов НЖМД при воздействии на них внешних магнитных полей 186
Б. С. Лобанов, Б. В. Хлопов, М. И. Самойлович, А. В. Шпак, А. Ю. Митягин, Я. Д. Ковалюк. Электромагнитная восприимчивость композитных метаматериалов на основе опаловых матриц в системах уничтожения информации 188
А. Я. Кулик, Ю. Ю. Іванов. Застосування гіперболічних функцій для роботи з турбокодами у розподілених комп'ютерних системах різного функціонального призначення 190
М. А. Мельник. Стеганографический алгоритм для контейнеров-изображений, устойчивый к атаке сжатием 193
Н. И. Кушниренко, В. Я. Чечельницкий. Аппаратный генератор перестановок 195
Р.М.Пелещак, А.А.Вельченко, С.А.Вельченко. Защита автоматизированной информационной системы с квантовым поляризационным кодированием на основе технологии плавающего кода 197
А. С. Сафронов, Н. А. Барабанов, Ю. И. Венедиктов. Анализ процессов развития систем информационной безопасности организации 201
А. В. Соколов. Множество нелинейных преобразований на основе конструкции Ниберг длиной N=256 204
М. И. Мазурков, А. В. Соколов. Синтез нелинейных преобразований на основе последовательностей де Брёйна над изоморфными представлениями поля GF(256) 208
О. О. Цисар, К. В. Защолкін. Методика приховування даних, яка заснована на використанні клітинно-автоматного підходу 212
К. В. Защелкин, А. И. Иващенко, Е. Н. Иванова. Усовершенствование метода скрытия данных Куттера—Джордана—Боссена 214

УДК 621.391.7

МНОЖЕСТВО НЕЛИНЕЙНЫХ ПРЕОБРАЗОВАНИЙ НА ОСНОВЕ КОНСТРУКЦИИ НИБЕРГ ДЛИНОЙ N=256

А. В. Соколов

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

Разработана методика размножения оптимальных криптографических S-блоков подстановки конструкции Ниберг, обладающих высочайшими показателями криптографического качества, что позволило увеличить их количество в 10^8 раз. Каждый полученный S-блок подстановки обладает гарантированными равнозначащими с конструкцией Ниберг свойствами нелинейности и корреляции выхода и входа.

Ключевые слова: S-блок подстановки, конструкция Ниберг, правила размножения.

Базовым компонентом современных алгоритмов блочного шифрования, а также хеширования являются нелинейные *S*-блоки подстановки [1], осуществляющие отображение группы входных битов x в другую группу выходных битов y по правилу, однозначно задаваемому кодирующей Q-последовательностью, полностью определяющей структурные и криптографические свойства *S*-блока подстановки [2]. Разработка методов синтеза больших множеств таких кодирующих Q-последовательностей, которые бы позволили получить высокие уровни показателей криптографического качества построенных на их основе *S*-блоков подстановки является актуальной задачей. Применение для синтеза Q-последовательностей переборных методов является невозможным, т. к. уже при длине *S*-блока подстановки N=256 число существующих Q-последовательностей достигает астрономического значения J=256!=1,17·10^{505}. При росте длины N существенно улучшаются корреляционные, дистанционные и периодические свойства *S*-блоков подстановки, поэтому синтез Q-последовательностей малой длины с помощью переборных методов, предложенный в [3], не является решением задачи построения криптографически качественных *S*-блоков подстановки даже в случае выбора разработчиками криптографического алгоритма малого значения N, что также исключает использование *S*-блоков подстановки в качестве долговременных ключевых элементов.

Из [4] известен метод построения *S*-блоков подстановки на базе обратных по умножению элементов над расширенными полями $GF(q)$, где $q=p^m$ по модулю неприводимого полинома $f(z)$:

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

Выражение (1) вместе с аффинным преобразованием вида

$$y = Ax + a, \tag{2}$$

где A — невырожденная матрица аффинного преобразования размера $k \times k$;

a — вектор сдвига, причем $a \in V_k$, где V_k — линейное векторное пространство порядка k,

представляют собой конструкцию Ниберг, используемую в шифре Rijndael/AES [5], обладающую такими криптографическими качествами, как равномерная минимизация элементов матрицы коэффициентов корреляции

$$\max\{|r_{ij}|\} \approx 1/k \tag{3}$$

и высокий уровень нелинейности компонентных булевых функций *S*-блоков подстановки

$$N_s \approx 2^{k-1} - 2^{k/2-1} - 2; \quad \deg\{f_i\} = k-1. \tag{4}$$

Однако оказывается, что подобных подстановочных конструкций обладающих уникальной структурой, может существовать ровно столько, сколько существует неприводимых q-ичных полиномов заданной степени k

$$\left|f_q^k\right| = \frac{1}{k}\sum_{\substack{d \\ d|k}} \mu(d)\cdot q^{(k/d)}, \tag{5}$$

где d — делители числа k, $\mu(d)$ — функция Мёбиуса, а запись $d|k$ означает, что d делит k.

Из них количество первообразных полиномов определяется как

$$\left|V_q^k\right| = \frac{\varphi\left(q^k-1\right)}{k}. \tag{6}$$

Например, для степени неприводимого первообразного полинома $k=8$, применяемой в криптопреобразовании Rijndael, в соответствии с выражением (2) существует $\left|f_2^8\right|=30$ неприводимых полиномов, представленных ниже в виде своих десятичных эквивалентов:

$$\left(f_i(z)\right)_{10} = \left\{\begin{matrix} 283,\ \mathbf{285},\ \mathbf{299},\ \mathbf{301},\ 313,\ 319,\ \mathbf{333},\ \mathbf{351},\ \mathbf{355},\ \mathbf{357},\ \mathbf{361},\ \mathbf{369},\ 375,\ 379, \\ \mathbf{391},\ 395,\ \mathbf{397},\ 415,\ 419,\ \mathbf{425},\ 433,\ 445,\ \mathbf{451},\ \mathbf{463},\ 471,\ 477,\ \mathbf{487},\ 499, \\ \mathbf{501},\ 505 \end{matrix}\right\}, \tag{7}$$

где первообразные неприводимые полиномы, которых при $k=8$ существует $\left|V_2^8\right|=16$, выделены жирным шрифтом своих десятичных эквивалентов. Таким образом, мощность класса доступных высококачественных криптографических S-блоков подстановки является очень малой, что делает невозможной идею их применения в качестве долговременных ключей для увеличения числа уровней защиты шифра.

Проведенные исследования показали, что значительное увеличение мощности класса оптимальных S-блоков подстановки конструкции Ниберг, обладающих аппроксимировано максимальным расстоянием нелинейности, а также практически равномерным распределением элементов матрицы коэффициентов корреляции, возможно за счет применения следующих правил

1. Новые $k!$ S-блоков подстановки могут быть получены путем всех возможных перестановок компонентных булевых функций S-блоков подстановки конструкции Ниберг. Причем при применении данного правила размножения сохраняются такие свойства блока, как расстояние нелинейности, алгебраическая степень нелинейности, матрица коэффициентов корреляции.

2. Новые 2^k S-блоков подстановки могут быть получены путем всех возможных вариантов инверсии компонентных булевых функций данного S-блока подстановки на основе МЛРП. При применении данного правила также сохраняются свойства, приведенные в Правиле 1.

Применение вышеприведенных правил позволяет нарастить мощность класса оптимальных криптографических S-блоков подстановки до значения

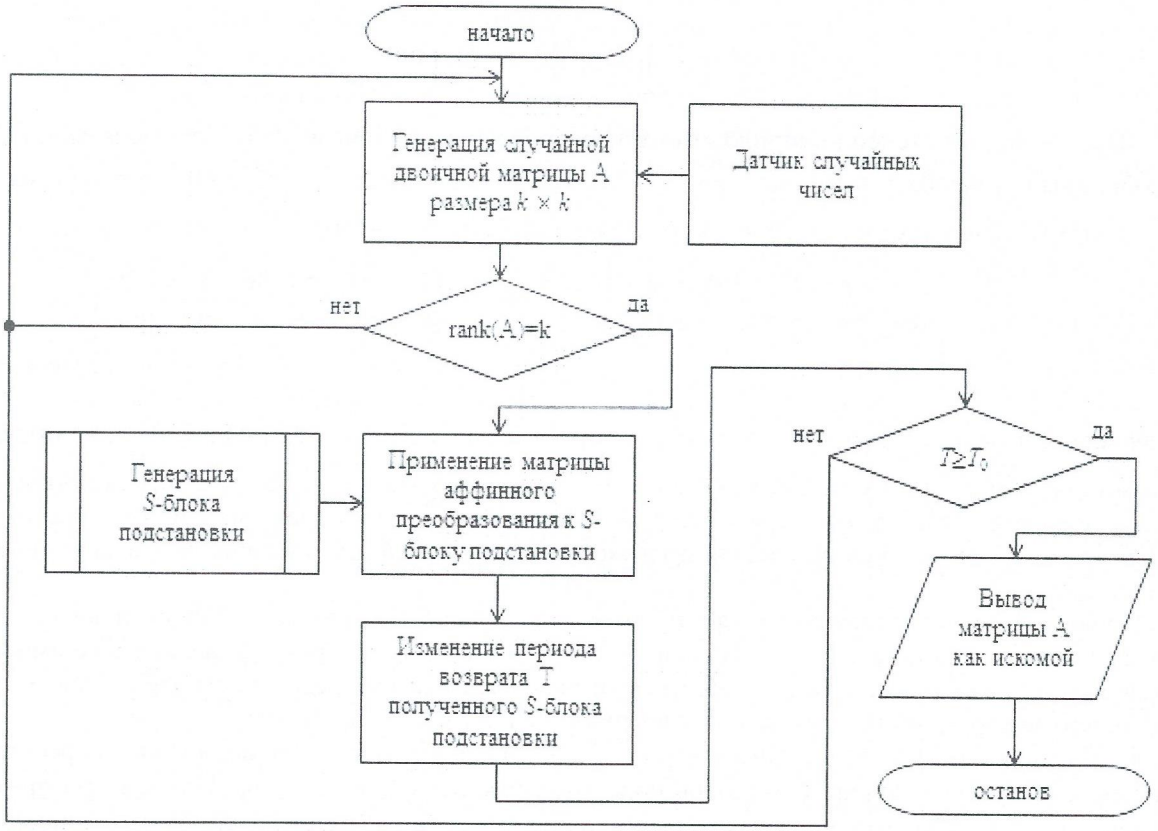
$$J = \left|f_2^8\right|\cdot k!\cdot 2^k, \tag{8}$$

что для значения $k=8$ (что соответствует шифру Rijndael) позволяет получить $J \simeq 3\cdot 10^8$ S-блоков подстановки с корреляционными свойствами, а также свойствами нелинейности, абсолютно идентичными конструкции Ниберг.

Недостатком всех S-блоков подстановки конструкции Ниберг является недостаточно большие периоды возврата блока в исходное состояние. Устранение данного недостатка возможно за счет установки на выходе S-блока подстановки блока аффинного преобразования (2) со специально подобранной матрицей A, обеспечивающей максимизацию увеличения расстояния нелинейности. Матрица A — невырожденная матрица, количество $\left|W_A\right|_k$ которой определяется как [6]

$$\left|W_A\right|_k = \prod_{i=0}^{k-1}\left(2^k - 2^i\right). \tag{9}$$

Например, для $k=8$ $|W_A|_8 \approx 5{,}3 \cdot 10^{18}$, что является существенно величиной. Оптимальная матрица аффинного преобразования A, обеспечивающая наибольший период возврата, подбирается индивидуально для каждого вида неприводимого полинома $f(z)$, на основе которого строится конструкция Ниберг. В виду того, что выбор матрицы аффинного преобразование индивидуален и зависит от конкретного вида *S*-блока подстановки, а мощность множества аффинных матриц $|W_A|_k$ является существенной и стремительно растет при росте k можно предложить алгоритм подбора матриц аффинного преобразования, изображенный на рисунке.



Блок схема алгоритма генерации матрицы аффинного преобразования

Здесь видно, что из вышеприведенного рисунка, данный алгоритм представим в виде следующих шагов:

Шаг 1. Случайно выбирается матрица A размером $k \times k$, проверяется, является ли она невырожденной. Если да, то процедура генерации матрицы аффинного преобразования завершена. Если нет, генерация случайных матриц A продолжается до тех пор, пока не будет найдена невырожденная матрица (на данном шаге возможно применение алгоритма Ростовцева [7] для синтеза невырожденных матриц).

Шаг 2. Матрица аффинного преобразования применяется к выбранному *S*-блоку подстановки, в результате чего образуется новый *S*-блок подстановки, свойства нелинейности которого совпадают с исходным, однако период возврата является иным.

Шаг 3. Измеряется период возврата *T*, полученного *S*-блока подстановки. Если величина периода возврата *T* является большей или равной заранее заданной величине T_0 — желаемому значению периода возврата *S*-блока подстановки в исходное состояние, достигаемой с помощью аффинного преобразования A, то алгоритм генерации подходящей матрицы аффинного преобразования завершен. Если значение фактического периода возврата T меньше T_0, то происходит возврат на Шаг 1, и алгоритм повторяется снова.

Применение предложенного алгоритма, даже при значении $k=8$ позволяет найти матрицу аффинного преобразования A, увеличивающую период возврата до значения $T_0=10\,000\,000$ за минимальное время.

Отметим основные результаты проведенных исследований:

1. Разработанные методы размножения криптографически качественных *S*-блоков подстановки конструкции Ниберг позволяют увеличить объем доступных блоков на 8 порядков уже для $k=8$, причем величина доступных блоков с оптимальными значениями криптографического качества стремительно растет при росте значения k.

2. Устранен недостаток конструкции Ниберг, связанный с ее малыми значениями периодов возврата в исходное состояние. Предложенный алгоритм позволяет найти оптимальные матрицы аффинного преобразования, существенно увеличивающие периоды возврата конструкции Ниберг.

Таким образом, был увеличен объем множества оптимальных *S*-блоков подстановки конструкции Ниберг, а также предложен алгоритм нахождения аффинных преобразований для увеличения периодов возврата *S*-блоков подстановки данной конструкции, что делает ее применение в новейших криптографических алгоритмах более обоснованным.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Горбенко, І. Д., Потій О. В., Ізбенко Ю. А. Дослідження аналітичних і статистичних властивостей булевих функцій криптоалгоритму RIJNDAEL (FIPS 197) // Всеукраїнський міжвідомчий науково-технічний збірник "Радіотехніка".— Харків, 2004 .— Т. 126.— С. 132—138.
2. Мазурков М. И., Соколов А. В. Методы синтеза двоичных псевдослучайных последовательностей со свойством k-граммного распределения.— Одесса: Труды ОНПУ.— 2012.— С.188 — 198.
3. Яковлєв, С. В. Збалансовані критерії якості довгострокових ключових елементів алгоритму ГОСТ 28147-89 // Київ: Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія».— 2009.— С. 5—12.
4. Nyberg K. Differentially uniform mappings for cryptography. I Advances in cryptology // Proceedings of EUROCRYPT'93 (1994) vol.765, Lecture Notes in Compuer Springer-Verlag, Berlin, Heidelberg, New York. P. 55—65.
5. FIPS 197. Advanced encryption standard // см. http://csrc.nist.gov/publications/
6. OEIS. A002884. - N. J. A. Sloane // http://oeis.org/A002884. - 06.02.13
7. Ростовцев А. Г., Маховенко Е. Б. Теоретическая криптография // СПб.: НПО «ПРОФЕССИОНАЛ».— 2004.

A. V. Sokolov

The set of non-linear transformations based on the Nyberg construction with the lengh of N = 256.

The method of reproduction of the optimal cryptographic substitution S-boxes of Nyberg construction, delivering the highest performance of cryptographic quality, which increases the number of them by a factor of 10^8 has been developed. Each obtained substitution S-box has the guaranteed equal properties with the Nyberg construction of nonlinearity and correlation between output and input.

Keywords: *substitution S-box, Nyberg construction, rules of reproduction.*