УДК 004.056.55

А. В. Соколов, М. И. Мазурков

Одесский национальный политехнический университет, Украина, Одесса

МЕТОДЫ СИНТЕЗА ЧЕТВЕРИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЕ БРЕЙНА ДЛЯ ЗАДАЧ КРИПТОГРАФИИ

Предлагается новый подход к разработке экономичных S-блоков подстановки, основанный на использовании четвертичных последовательностей де Брейна, что позволяет добиться значительного увеличения числа доступных экономичных S-блоков по сравнению с использованием двоичных последовательностей де Брейна. Получены криптографические характеристики экономичных S-блоков подстановки, установлено, что они обладают, по крайней мере, таким же криптографическим качеством, как и полные классы S-блоков подстановки.

Основным элементом блочных шифров, который определяет их скорость и надежность является криптографический *S*-блок подстановки. Качество *S*-блоков подстановки все чаще определяется не только требованиями к криптографической устойчивости конструкции, но и требованием экономии аппаратных ресурсов, простоты реализации, скорости работы и возможности параллельных вычислений.

Проблема разработки эффективных методов синтеза экономических *S*-блоков подстановки может быть решена за счет использования шумоподобных сигналов [1] – последовательностей де Брейна [2], методы синтеза которых, а также способ построения экономичных *S*-блоков подстановки на их основе нами предложен [3].

Применение двоичных последовательностей де Брейна позволяет добиться уменьшения количества ячеек памяти, требуемой для хранения *S*-блока подстановки в четыре раза [3] без существенного снижения важнейших показателей их криптографического качества. Однако недостатком данного метода является малая мощность классов двоичных последовательностей де Брейна, которая определяется следующим выражением:

$$W = [(q-1)!]^{q^k-1} q^{q^{k-1}-k}, \qquad (1)$$

где q – размерность алфавита последовательности, k – логарифм ее периода [2].

Устранение этого недостатка возможно за счет применения четвертичных последовательностей де Брейна, например, следующего вида для $q=4$ и $k=2$:

$$B = [3, 3, 1, 2, 2, 0, 1, 1, 0, 0, 2, 3, 0, 3, 2, 1], \qquad (2)$$

что, как видно из выражения (1) позволяет достичь существенного расширения набора доступных экономичных *S*-блоков подстановки за счет некоторого уменьшения эффекта экономии ячеек памяти.

Тем не менее задача разработки методов синтеза полных классов последовательностей де Брейна для $q>2$ не решена.

В данной работе в результате изучения особенностей построения последовательностей де Брейна были выделены базовые формы представления: алгебраическая и геометрическая, на основе свойств которых разработаны эффективные алгоритмы синтеза образующих и полных классов последовательностей де Брейна произвольного периода $N \geq 2$. Предложены методы размножения последовательностей де Брейна, основанные на одновременной перестановке элементов, позволяющие быстрое получение новых последовательностей де Брейна на основе ранее синтезированных.

В работе были изучены следующие криптографические свойства экономичных *S*-блоков подстановки на основе четвертичных последовательностей де Брейна:

1) отсутствие корреляционной связи между выходными и входными битами *S*-блока. Для оценки данного критерия требуется равномерность распределения элементов матрицы коэффициентов корреляции $|r_{\max}| \leq 1/\eta$, где η – размерность компонентной функции *S*-блока;

2) максимальное расстояние нелинейности $d_{S\max} \leq 2^{\eta-1} - 2^{(\eta/2)-1} - 2$;

3) максимальная длина циклов $T = \text{НОК}(i_1, i_2 \ldots)$, где i – соответствующие длины циклов;

4) строгий лавинный критерий $K_i(f) = \sum_{a_i} \left(f(x) \oplus f(x \oplus e_i) \right) = 2^{\eta-1}$.

5) экономия памяти таблиц подстановки $K_{\text{П}}$. Изучение данных таблицы подтверждает эффективность применения синтезированных четвертичных последовательностей де Брейна для существенного увеличения мощности класса доступных экономичных *S*-блоков подстановки.

Библиографические ссылки

1. Мазурков М. И. Системы широкополосной радиосвязи. Одесса : Наука и техника, 2010. С. 340.

2. De Bruijn N. G. A combitorial problem // Nederl. Akad. Wetensch. Proc. 1946. Vol. 49. P. 758–764.

3. Мазурков М. И., Соколов А. В. Методы синтеза двоичных псевдослучайных последовательностей со свойством *k*-граммного распределения для задач шифрования // Труды ОНПУ : науч. и производств.-практ. сб. Одесса, 2012. Вып. 1(38). С. 188–198.

Значения криптографически важных показателей *S*-блоков

Класс последовательностей де Брейна	Объем класса $W = 2^{N/2}$	Количество *S*-блоков, обладающих заданным параметром				
		$\lvert r_{\max} \rvert \le 1/\eta$	$d_S = 2^{\eta-1} - 2^{\frac{\eta}{2}-1} - 2$	T	$K_i(f) = 2^{\eta-1}$	$K_{\text{П}}$
Двоичный, $k = 4$	256	24	192	21 ($T \ge 60$)	0	4
Двоичный, $k = 5$	65 536	76	33 032	1 642 ($T \ge 1\,000$)	0	4
Четверичный, $k = 2$	331 776	23 008	218 688	2 281 ($T = 140$)	2176	2

A. V. Sokolov, M. I. Mazurkov

Odessa National Polytechnic University, Ukraine, Odessa

SYNTHESIS METHODS AND CRYPTOGRAPHIC APPLICATION OF QUATERNARY DE BRUIJN SEQUENCES

A new approach to the design of compact S-boxes based on the use of quaternary de Bruijn sequences is proposed. It allows the achievement of a substantial increase of available S-boxes compared to using binary de Bruijn sequences. The characteristics of the obtained compact cryptographic S-boxes are researched. These compact S-boxes are stated to have at least equivalent cryptographic quality compared to full-sized ones.

УДК 520.8.05

А. А. Сукиасян, И. А. Мисинева

Сибирский государственный аэрокосмический университет
имени академика М. Ф. Решетнева, Россия, Красноярск

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ПРЕДПРИЯТИЙ АЭРОКОСМИЧЕСКОЙ ОТРАСЛИ

Проблема защиты информации путем ее преобразования, исключающего ее прочтение посторонним лицом, волновала человеческий ум с давних времен. История криптографии – ровесница истории человеческого языка. Более того, первоначально письменность сама по себе была криптографической системой, так как в древних обществах ею владели только избранные.

Криптографические методы защиты информации – это специальные методы шифрования, кодирования или иного преобразования информации, в результате которого ее содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования. Криптографический метод защиты, безусловно, самый надежный, так как охраняется непосредственно сама информация, а не доступ к ней (например, зашифрованный файл нельзя прочесть даже в случае кражи носителя). Данный метод защиты реализуется в виде программ или пакетов программ.

Современная криптография включает в себя четыре крупных раздела:

– симметричные криптосистемы. В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ

– криптосистемы с открытым ключом. В системах с открытым ключом используются два ключа – открытый и закрытый, которые математически связаны друг с другом.

Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения;

– электронная подпись. Системой электронной подписи называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения;

– управление ключами. Это процесс системы обработки информации, содержанием которого является составление и распределение ключей между пользователями.

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи (например, электронная