УДК 004.056.55

СЛОЖНОСТЬ АППАРАТНОЙ РЕАЛИЗАЦИИ ПОЛНОГО КЛАССА ПОСЛЕДОВАТЕЛЬНОСТЕЙ ДЕ БРЕЙНА ДЛИНЫ 16

Н.А. Барабанов[1], А.В. Соколов[1], Н.А. Жданова[2]

[1]Одесский национальный политехнический университет;
[2]Одесская государственная академия строительства и архитектуры
Украина, Одесса
radiosquid@gmail.com

Проведена оптимизация аппаратной реализации криптографически ценного класса последовательностей де Брейна длины 16. Найден класс оптимальных с точки зрения аппаратной реализации последовательностей де Брейна, который может быть рекомендован к использованию в современных криптографических приложениях, требовательных к аппаратным ресурсам.

Ключевые слова: последовательность де Брейна, аппаратная реализация, QMC метод.

Криптографическая устойчивость и быстродействие большинства современных криптоалгоритмов во многом основываются и зависят от применяемых в них булевых функций. Современные тенденции к развитию криптографии все чаще используют совершенные алгебраические конструкции для решения задач повышения криптографической устойчивости алгоритмов как потокового [1] так и блочного [2] шифрования, что позволяет существенно повысить их защищенность и экономические характеристики.

Примером таких совершенных алгебраических конструкций являются последовательности де Брейна — последовательности длины $N = 2^k$, удовлетворяющие свойству k-граммного распределения, т.е. в которых каждая серия из k бит встречается на замкнутом цикле точно один раз. При этом в классе последовательностей де Брейна выделают подкласс образующих последовательностей, т.е. таких, каждая из которых не может быть получена путем циклического сдвига на величину τ другой последовательности из данного подкласса. В виду того, что свойство k-граммного распределения является инвариантным к циклическому сдвигу, число образующих последовательностей де Брейна в N раз меньше их общего количества.

Николасом де Брейном была найдена нижняя оценка количества образующих двоичных последовательностей де Брейна [3]

$$W_{\text{обр}} = 2^{2^{k-1}-2}. \quad (1)$$

Стоит отметить, что для произвольного значения n задача синтеза последовательностей де Брейна в настоящий момент является нерешенной, но, тем не менее, для некоторых n найдены эффективные алгоритмы синтеза их полных классов [2], свойства которых уже достаточно хорошо изучены [4]. Для многих практических приложений актуальной является не только задача получения полных классов данных сигналов, но также и задача обоснованного выбора наилучших его представителей с точки зрения их использования в тех или иных практических схемах. Так, во многих приложениях, требующих большого числа последовательных вычислений значения булевой функции, например, алгоритмах потокового шифрования, критичной часто является сложность аппаратной реализации.

В соответствии с определением Дж. фон Неймана [5] под сложностью аппаратной реализации булевой функции будем понимать число элементарных логических элементов (ЛЭ) для ее аппаратной реализации

$$N_{\text{ЛЭ}} = N_{\text{НЕ}} + N_{\text{И}} + N_{\text{ИЛИ}}, \tag{2}$$

где $N_{\text{НЕ}}$, $N_{\text{И}}$, $N_{\text{ИЛИ}}$ — количество элементов "НЕ", 'И" и 'ИЛИ" соответственно, реализующих операции отрицания, конъюнкции и дизъюнкции.

Логично считать, что число различных ЛЭ для реализации булевой функции равно числу соответствующих операций в записи логического выражения функции, но, тем не менее, для оценки сложности принято учитывать только число сумматоров и умножителей $N'_{\text{ЛЭ}} = N_{\text{И}} + N_{\text{ИЛИ}}$, как наиболее трудоемких при реализации.

В настоящей работе проведена минимизация всех $W = 256$ последовательностей де Брейна длины $N = 16$ с помощью современного QMC метода минимизации булевых функций [6], в результате чего было найдено распределение количества последовательностей де Брйена J, требующих для своей реализации заданное количество логических компонентов.

J	6	7	8	9	10	11	12	13	14	15	16	17	18
$N'_{\text{ЛЭ}}$	12	32	0	28	60	68	0	0	16	24	0	8	8

. (3)

Анализ (3) позволяет сделать вывод о существовании 12 оптимальных с точки зрения сложности аппаратной реализации последовательностей де Брейна, которые запишем в виде их минимальной дизъюнктивной формы (МДФ)

$$\begin{array}{l|l}
1.\left(\overline{x_1}\wedge\overline{x_3}\right)\vee\left(\overline{x_2}\wedge x_4\right)\vee\left(\overline{x_1}\wedge x_2\wedge\overline{x_4}\right) & 7.\left(\overline{x_2}\wedge x_4\right)\vee\left(x_1\wedge\overline{x_3}\right)\vee\left(x_1\wedge x_2\wedge\overline{x_4}\right) \\
2.\left(\overline{x_2}\wedge\overline{x_3}\right)\vee\left(\overline{x_2}\wedge x_4\right)\vee\left(\overline{x_1}\wedge x_3\wedge\overline{x_4}\right) & 8.\left(x_2\wedge\overline{x_3}\right)\vee\left(x_2\wedge x_4\right)\vee\left(\overline{x_1}\wedge x_3\wedge\overline{x_4}\right) \\
3.\left(\overline{x_2}\wedge\overline{x_4}\right)\vee\left(\overline{x_2}\wedge x_3\right)\vee\left(\overline{x_1}\wedge\overline{x_3}\wedge x_4\right) & 9.\left(x_2\wedge\overline{x_4}\right)\vee\left(x_2\wedge x_3\right)\vee\left(\overline{x_1}\wedge\overline{x_3}\wedge x_4\right) \\
4.\left(\overline{x_2}\wedge\overline{x_4}\right)\vee\left(\overline{x_2}\wedge x_3\right)\vee\left(x_1\wedge\overline{x_3}\wedge x_4\right) & 10.\left(x_2\wedge\overline{x_4}\right)\vee\left(x_1\wedge x_3\right)\vee\left(x_1\wedge\overline{x_2}\wedge x_4\right) \\
5.\left(\overline{x_2}\wedge\overline{x_3}\right)\vee\left(\overline{x_2}\wedge x_4\right)\vee\left(x_1\wedge x_3\wedge\overline{x_4}\right) & 11.\left(x_2\wedge\overline{x_4}\right)\vee\left(x_2\wedge x_3\right)\vee\left(x_1\wedge\overline{x_3}\wedge x_4\right) \\
6.\left(\overline{x_1}\wedge x_3\right)\vee\left(x_2\wedge\overline{x_4}\right)\vee\left(\overline{x_1}\wedge\overline{x_2}\wedge x_4\right) & 12.\left(x_2\wedge\overline{x_3}\right)\vee\left(x_2\wedge x_4\right)\vee\left(x_1\wedge x_3\wedge\overline{x_4}\right)
\end{array} \tag{4}$$

Таким образом, применение QMC метода к полному классу последовательностей де Брейна позволили выделить среди них 12 оптимальных с точки зрения аппаратной реализации последовательностей, которые могут быть рекомендованы к использованию в современных криптографических алгоритмах для повышения их быстродействия при сохранении криптографических характеристик на исходном уровне за счет сохранения свойства k -граммного распределения.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Барабанов, Н.А. Сложность аппаратной реализации полного класса бент-функций четырех переменных / Н.А. Барабанов, А.В. Соколов // Труды ОНПУ. — 2013. — №2(41). — С.227—231.

2. Мазурков, М.И. Методы синтеза двоичных псевдослучайных последовательностей со свойством k-граммного распределения / М.И. Мазурков, А.В. Соколов. — Одесса: Труды ОНПУ. — 2012. — С.188 — 198.

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

4. Мазурков, М.И. Автокорреляционные функции полного класса последовательностей со свойством k–граммного распределения / М.И. Мазурков, А.В. Соколов. — Одесса: Труды СИЭТ. — 2012. — С.148.

5. Блох, Э.Л. Обобщенные каскадные коды / Э.Л. Блох, В.В. Зяблов. — М.: Связь, 1976. — 240 с.

6. Савельев, А.Я. Основы информатики / А.Я. Савельев. — М.: МГТУ им. Н.Э. Баумана, 2001. — 328 с.

Nikolai Alexeevich Barabanov, Artem Victorovich Sokolov, Natalia Alexandrovna Zhdanova. Hardware realization complexity of the full class of de Bruijn sequences of length 16. The optimization of the hardware implementation of cryptographically important class of de Bruijn sequences of length 16 is performed. A class of the optimal de Bruijn sequences, which can be recommended for use in modern cryptographic applications, sensitive to hardware resources is found.