УДК 004.056.55

МОДИФИЦИРОВАННЫЙ ГЕНЕРАТОР КЛЮЧЕВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НА ОСНОВЕ ДУАЛЬНЫХ ПАР БЕНТ-ФУНКЦИЙ

К. т. н. А. В. Соколов, М. В. Ткаченко

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

Разработан модифицированный генератор псевдослучайных ключевых последовательностей на основе дуальных пар бент-функций, содержащий в своем составе два регистра сдвига с линейной обратной связью для любой длины используемых бент-функций, что упрощает аппаратную реализацию. Установлено высокое стохастическое и криптографическое качество разработанного генератора.

Ключевые слова: бент-функция, псевдослучайная последовательность, генератор.

Одним из ключевых объектов современной криптографии и теории информации в целом является генератор псевдослучайных ключевых последовательностей (ГПКП). ГПКП нашли свое применение в системах связи с расширенным спектром, теории синтеза сложных сигналов, моделировании, генерации инициализационных векторов и ключевой информации в блочных симметричных криптоалгоритмах. Кроме того, ГПКП, обладающие криптографической стойкостью, являются основным компонентом поточных алгоритмов шифрования.

Широкое распространение в практических приложениях получили ГПКП на основе регистров сдвига с линейной обратной связью (РСЛОС), примером которых является схема Геффа, схема Агафоновой, а также схема ГПКП на основе дуальных пар бент-функций, предложенная в [1].

ГПКП на основе дуальных пар бент-функций обладает многими практически ценными свойствами, в частности: высоким уровнем стохастического качества генерируемых последовательностей, легко масштабируемым числом уровней защиты, простотой конструктивных решений при программной и аппаратной реализации. Тем не менее, ГПКП на основе дуальных пар бент-функций не лишен существенного недостатка, связанного с большим количеством необходимых РСЛОС для его корректной работы. Так, для бент-функций длины N=16 требуется 5 РСЛОС, тогда как для бент-функций длины N=1024 потребуется уже 11 РСЛОС, причем каждый из них должен быть построен на основе первообразного полинома различной степени. Данный факт определяет сложности при аппаратной реализации ГПКП на основе дуальных пар бент-функций.

Целью настоящей работы является разработка модифицированного ГПКП на основе дуальных пар бент-функций, требующего два РСЛОС для любой длины используемых бент-функций.

Возможность построения ГПКП на основе дуальных пар бент-функций, содержащего два РСЛОС вне зависимости от длины применяемых бент-функций, лежит в плоскости использования математического аппарата q-функций [2], а также алгоритма построения первообразных полиномов над всеми изоморфными представлениями полей $GF(2^k)$ [3]. Так, на вход блока дуальной пары бент-функций должен быть подан один из N уровней, для генерации которых в [1] используется конкатенация $\log_2 N$ бит от $\log_2 N$ РСЛОС. В модифицированном ГПКП на основе дуальных пар бент-функций предлагается заменить $\log_2 N$ РСЛОС одним многозначным РСЛОС на основе полиномов [3]. Так, в случае бент-функций четырех переменных необходим РСЛОС, функционирующий на принципах 16-значной логики и использующий соответствующий полином.

Например, зададим первообразный полином третьей степени $z(x)=x^3+x+9$, существующий над арифметикой поля $GF(16)$, операции умножения в котором производятся по модулю первообразного полинома $h(x) = x^4 + x + 1$.

Полином $z(x)$ определяет схему 16-РСЛОС, представленную на рис. 1.

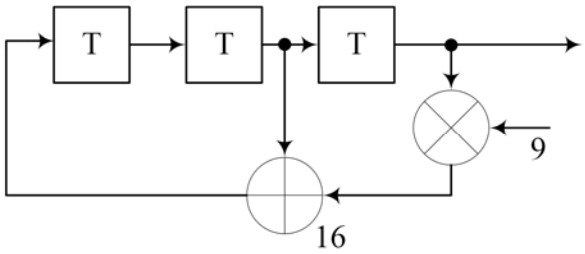

Рис. 1. 16-РСЛОС на основе полинома $z(x)$

С использованием схемы 16-РСЛОС построена модифицированная схема ГПКП на основе дуальных пар бент-функций, содержащая в своем составе всего два РСЛОС (рис. 2). Отметим, что в схему дополнительно введен Т-блок задержки на 1 такт, который в начале работы схемы инициализируются нулевым значением. Данное решение позволяет гарантировать безупречные корреляционные свойства генерируемой последовательности вне зависимости от конкретных параметров ГПКП.

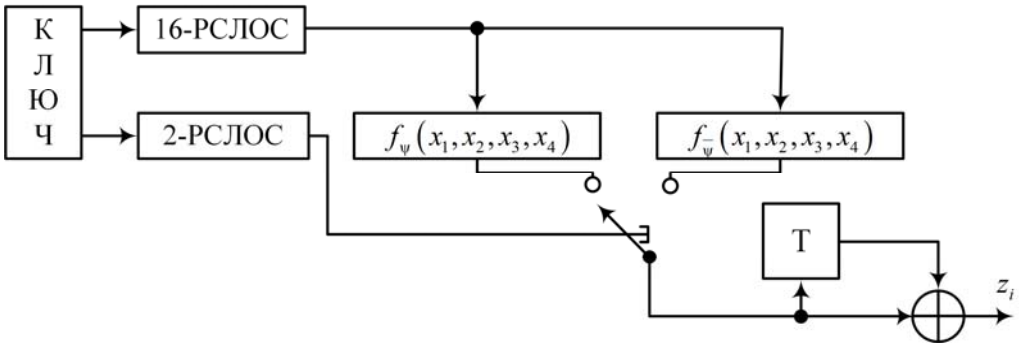

Рис. 2. Модифицированный ГПКП на основе дуальных пар бент-функций

Тестирование ГПКП, изображенного на рис. 2, показало высокое стохастическое качество генерируемых им последовательностей и их соответствие базовым критериям [1]. Модифицированный ГПКП на основе дуальных пар бент-функций обладает также хорошими криптографическими свойствами. Так, при используемом полиноме $f(x)$, а также полиноме $y(x)=x^{21}+x^2+1$ (для построения 2-РСЛОС) число уровней защиты определяется следующими величинами: исходные состояние РСЛОС ((16^3-1) и $(2^{21}-1)$), количество первообразных полиномов степени $\deg\{f(x)\}=3$ и $\deg\{y(x)\}=21$ над соответствующими полями ($2\cdot 576$ и 84672), число различных дуальных пар бент-функций (448^2), что в общем составляет $\Psi=(16^3-1)\cdot(2^{21}-1)\cdot 2\cdot 576\cdot 84672\cdot 448^2\simeq 1.68\cdot 10^{23}\approx 2^{77.154}$, и является достаточным с криптографической точки зрения. Отметим, что число уровней защиты может быть также легко масштабировано за счет выбора полиномов более высоких степеней для построения РСЛОС.

Таким образом, разработанный модифицированный ГПКП на основе дуальных пар бент-функций обладает высоким уровнем стохастического и криптографического качества, содержит в своем составе два РСЛОС для любой длины бент-функций, что упрощает его аппаратную реализацию.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Мазурков М.И., Барабанов Н.А., Соколов А.В. Генератор ключевых последовательностей на основе дуальных пар бент-функций.— Труды ОПУ, 2013.— Вып. 3 (42).— С. 150—156.

2. Жданов О.Н., Соколов А.В. Алгоритм построения оптимальных по критерию нулевой корреляции недвоичных блоков замен // Проблемы физики, математики и техники.— 2015,— № 3(24).— С. 94—97.

3. 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.

A.V. Sokolov, M.V. Tkachenko

Modified key sequences generator based on bent-function dual couples

The authors have developed a modified pseudo-random key sequences generator based on bent-function dual couples containing just two shift registers with linear feedback for any length of bent-functions, which simplifies hardware implementation. The high stochastic and cryptographic qualities of the sequences produced by the generator are confirmed.

Keywords: bent function, pseudo-random sequence, generator.