УДК 681.3.06

МЕТОД СИНТЕЗА БЕНТ-ПОСЛЕДОВАТЕЛЬНОСТЕЙ В БАЗИСЕ ВИЛЕНКИНА-КРЕСТЕНСОНА

МАЗУРКОВ М. И., СОКОЛОВ А. В., БАРАБАНОВ Н. А.

Одесский национальный политехнический университет,
Украина, Одесса, 65044, пр. Шевченко 1

Аннотация. В статье разработан метод построения полного класса бент-последовательностей длины $N = 9$ в базисе Виленкина–Крестенсона, основанный на применении трех опорных конструкций. Первая конструкция допускает построение бент-последовательностей произвольной длины $N = 3^{2k}$, $k \in \mathbb{N}$. Полученные бент-последовательности могут использоваться как в приложениях криптографии, так и в качестве кодов постоянной амплитуды в технологии MC-CDMA. Предложена конструкция блока гаммирования графической и видеоинформации на основе бент-последовательностей в базисе Виленкина–Крестенсона.

Ключевые слова: бент-последовательность; преобразование Виленкина-Крестенсона; регулярный метод

В последние десятилетия совершенные алгебраические конструкции получили свои множественные применения в различных приложениях теории радиосвязи, передачи информации, криптографии [1]. Одними из наиболее применяемых совершенных алгебраических конструкций в области криптографии являются двоичные бент-последовательности, представляющие собой таблицы истинности бент-функций — наиболее нелинейных булевых функций, обладающих равномерным спектром Уолша–Адамара.

В литературе известны эффективные и быстродействующие генераторы псевдослучайных ключевых последовательностей (ГПКП) на основе дуальных пар бент-функций [2, 3], которые могут быть положены в основу алгоритмов поточного шифрования, блоков гаммирования блочных алгоритмов шифрования, а также применены для генерации ключевой информации.

Развитие принципов многозначной логики, в частности, разработка методов построения многозначных совершенных алгебраических конструкций является необходимой для повышения эффективности систем шифрования и скремблирования графической и видеоинформации.

Многие современные системы обработки графической информации основаны на принципе разделения потока данных на цветовые составляющие в соответствии с цветовой моделью. Чаще всего применяются цветовые модели RGB, основанные на представлении цветов в виде кортежей трех чисел, называемых цветовыми компонентами. Так, при выполнении операции гаммирования, данные кортежи объединяются в одно число, которое складывается с гаммой.

Таким образом, необходимая длина ключевой последовательности должна быть в 3 раза больше чем длина ключевой последовательности, необходимой для шифрования изо-

DOI: 10.20535/S0021347016110054

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Мазурков М. И.* Системы широкополосной радиосвязи / М. И. Мазурков. — Одесса :Наука и Техника, 2010. — 340 с. — ISBN 978-966-8335-95-2.

2. *Мазурков М. И.* Генератор ключевых последовательностей на основе дуальных пар бент-функций / М. И. Мазурков, Н. А. Барабанов, А. В. Соколов // Труды Одесского политехнического университета. — 2013. — № 3. — С. 150–156. — Режим доступа : http://pratsi.opu.ua/articles/show/1017.

3. *Соколов А. В.* Быстродействующий генератор ключевых последовательностей на основе клеточных автоматов / А. В. Соколов // Труды Одесского политехнического университета. — 2014 — № 1. — С. 180–186. — Режим доступа : http://pratsi.opu.ua/articles/show/1087.

4. *Амбросимов А. С.* Свойства бент-функций q-значной логики над конечными полями / А. С. Амбросимов // Дискрет. матем. — 1994. — Т. 6, № 3. — С. 50–60. — Режим доступа : http://mi.mathnet.ru/dm639.

5. *Paterson K. G.* Sequences for OFDM and multi-code CDMA: two problems in algebraic coding theory / Kenneth G. Paterson // Sequences and their applications : 2nd Int. Conf. Seta 2001, May 13–17, 2001, Bergen, Norway : proc. — Berlin : Springer, 2002. — P. 46–71. — DOI : 10.1007/978-1-4471-0673-9_4.

6. *Мазурков М. И.* О влиянии вида ортогонального преобразования на пик-фактор спектра сигналов в системах с CDMA / М. И. Мазурков, А. В. Соколов, Н. А. Барабанов // Информатика и математические методы в моделировании. — 2015. — Т. 5, № 1. — С. 28–37.

7. Метод оцінювання якості тритових псевдовипадкових послідовностей длякриптографічних застосувань / С. О. Гнатюк, Т. О. Жмурко, В. М. Кінзерявий, Н. А. Сєйл // Information Technology and Security. — 2015. — Т. 3, № 2. — С. 108–116. — Режим доступа : http://its.iszzi.kpi.ua/article/view/60891.

8. *Трахтман А. М.* Основы теории дискретных сигналов на конечных интервалах / А. М. Трахтман, В. А. Трахтман. — М. : Сов. радио, 1975. — 208 с.

9. *Соколов А. В.* О существовании троичных бент-последовательностей / А. В. Соколов, О. Н. Жданов, Н. А. Барабанов // Радиоэлектроника и молодежь в XXI веке : 19-й междунар. молодежный форум : сб. материалов форума. — Харьков : ХНУРЭ, 2015. — Т. 3. — С. 131–132.

10. *Токарева Н. Н.* Бент-функции: результаты и приложения. Обзор работ / Н. Н. Токарева // Приклад. дискрет. математика. — 2009. — № 1. — С. 15–37. — Режим доступа : http://journals.tsu.ru/pdm/&journal_page=archive&id=431&article_id=26255.

11. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер. — Триумф, 2013. — 816 с.

Поступила в редакцию 13.05.2015 После переработки 28.07.2016