МАТЕМАТИЧЕСКИЕ ВОПРОСЫ КРИПТОГРАФИИ
2017 Т. 8 № 1 С. 69–80

УДК 519.719.2

Криптографически слабые функции усложнения для трехчленных линейных рекуррентных последовательностей

Ф. М. Малышев

Математический институт им. В. А. Стеклова Российской академии наук, Москва

Получено 30.IV.2014

Аннотация. Рассматриваются фильтрующие генераторы псевдослучайных последовательностей с входной двоичной трехчленной линейной рекуррентной последовательностью. Указано несколько классов булевых функций усложнения, допускающих построение линейных соотношений между начальными знаками рекуррентной последовательности при наличии специальных фрагментов в выходной последовательности. Допустимость использования таких функций в фильтрующих генераторах требует дополнительных обоснований.

Ключевые слова: рекуррентная последовательность, фильтрующий генератор, псевдослучайная последовательность

Cryptographically weak filter function for trinomial linear recurrent sequences

F. M. Malyshev

Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow

Abstract. We consider filter generators of pseudorandom sequences with binary input linear recurrent sequence having trinomial connection polynomial. Several classes of Boolean filter functions are described alowing to construct linear relations between the elements of input recurrent sequence by special subsets of output sequence. The admissibility of using such functions in the filter generators requires special justification.

Key words: recurrent sequence, filter generator, pseudo-random sequence

Citation: *Mathematical Aspects of Cryptography*, 2017, v. 8, № 1, pp. 69–80 (Russian)

Список литературы

[1] Шнайер Б., *Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си*, М.: ТРИУМФ, 2003, 816 с.

[2] Малышев Ф. М., “Сложность восстановления начальных знаков фильтрующих генераторов одного класса”, *Математические вопросы криптографии*, **6**:1 (2015), 109–116.

[3] Малышев Ф. М., “Порождающие наборы элементов рекуррентных последовательностей”, *Труды по дискретной математике*, **11**:2 (2008), 86–111.

[4] Балакин Г. В., “О возможности частичного восстановления некоторых последовательностей по наблюдениям”, *Математические вопросы криптографии*, **4**:4 (2013), 7–25.