УДК 681.3.06

ПРИМЕНЕНИЕ ЛИНЕЙНЫХ РЕКУРРЕНТНЫХ РЕГИСТРОВ В ПОТОЧНЫХ ШИФРАХ

д.т.н., проф. Ю.В. Стасев, к.т.н. Ю.А. Избенко, к.т.н. Д.Е. Петрукович

Исследуются показатели стойкости линейных рекуррентных регистров, построенных над расширенным полем GF(2^q) и используемых в схемах поточного шифрования, даются рекомендации относительно выбора параметров схем.

Постановка проблемы. При построении схем поточного преобразования информации одной из составляющих данных схем являются линейные рекуррентные регистры (ЛРР), основанные на линейной рекурренте над GF(2). Следует отметить, что регистрам, построенным над GF(2), присущи следующие недостатки: операции сдвига, сложения и умножения являются эффективными в аппаратном исполнении на основе VLSI чипов, но не являются эффективными в программной реализации, особенно когда длина регистра превышает длину машинного слова; сравнительно низкое быстродействие – за один такт генерируется 1 бит, в то время как гораздо более сложные блочные схемы преобразования за тот же такт генерируют 64 бита (и более) управляющей последовательности. Для устранения указанных недостатков используются линейные рекуррентные регистры, построенные над расширенным полем GF(2^q).

Анализ литературы показывает [1], что использование данных регистров практикуется только последние несколько лет, вследствие чего данная область является недостаточно изученной. В связи с этим **важной научной задачей** является исследование стойкости таких регистров.

Целью статьи является исследование показателей стойкости ЛРР, построенных над GF(2^q), а также выработка рекомендаций относительно выбора параметров схем преобразования информации.

Основная часть. Известно, что основными показателями стойкости ЛРР являются период и сложность генерируемой последовательности [2].

ЛРР над GF(2^q) математически эквивалентен q параллельным сдвиговым регистрам над GF(2) [3], каждый длиной

$$L_{OP} = q \cdot n, \qquad (1)$$

но с различными начальными состояниями, где n – степень образующего примитивного полинома.

Период T_{OP} последовательности, генерируемой такими регистрами, с использованием образующего примитивного полинома степени n, равен [3]:

$$T_{OP} = 2^{L_{OP}} - 1. \quad (2)$$

Очевидно, что преимуществами регистров сдвига, построенных над $GF(2^q)$, являются:

– устранение присущего всем регистрам, построенным над GF(2), низкого быстродействия: за один такт на выход регистра поступает не один бит, а блок битов длиной в машинное слово (q бит);

– устранение зависимости быстродействия от вида образующего полинома обратной связи: как прореженный, так и плотный, образующие результирующие полиномы не влияют на быстродействие регистра в целом (при аппаратной реализации);

– возможность использования в качестве образующих полиномов хорошо известных прореженных примитивных полиномов, что позволяет избежать вычислительно трудоемкой задачи построения над V_n плотного примитивного полинома. Эффект "плотности" полинома достигается за счет осуществления арифметических операций по модулю неприводимого полинома, который, в свою очередь, является плотным;

– существенное увеличение одного из основополагающих показателей стойкости схемы преобразования – периода генерируемой последовательности. Увеличение периода, в свою очередь, позволяет уменьшить количество перезагрузок ключей, что повышает быстродействие системы в целом.

Другим показателем стойкости поточных схем, помимо периода управляющей последовательности, является линейная сложность Λ. Данный показатель определяет длину кратчайшего эквивалентного регистра, генерирующего последовательность, аналогичную последовательности, сгенерированной рассматриваемой схемой.

Линейная сложность $\Lambda(z)$ последовательности, генерируемой линейным рекуррентным регистром, построенным над $GF(2^q)$, с использованием в качестве образующего полинома примитивного полинома степени n, равна

$$\Lambda(z) = q \cdot L_{OP}. \quad (3)$$

Докажем данное утверждение. ЛРР, построенный над расширенным полем $GF(2^q)$, эквивалентен работе q ЛРР, построенных над GF(2) [3]. Поскольку в качестве образующего полинома выбран примитивный полином, каждый из q ЛРР длиной L_{OP} бит, построенных над GF(2), основан на примитивном полиноме. Следовательно, линейная сложность последовательности, генерируемой q параллельными ЛРР длиной L_{OP} бит, основанных на примитивном полиноме, равна $\Lambda(z) = q \cdot L_{OP}$.

На рис. 1 в качестве примера представлена зависимость линейной сложности последовательностей, генерируемых регистром алгоритма Snow (представленного на европейский конкурс NESSIE, степень образующего полинома n = 16, q = 32), от длины последовательности L.

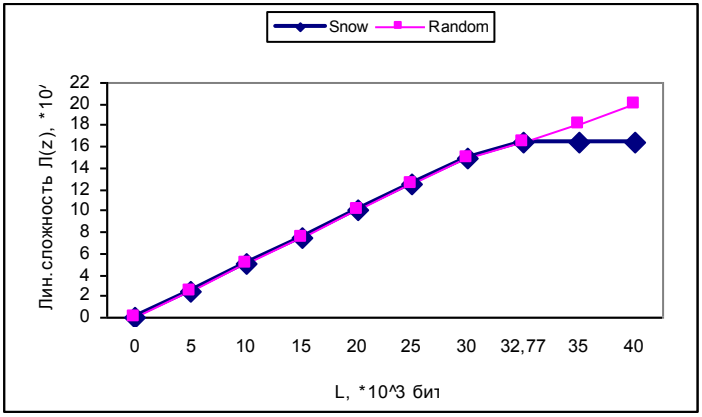

Рис. 1. Линейная сложность последовательностей ЛРР Snow

Согласно [4], верхняя граница линейной сложности $\Lambda(z)$ выходной последовательности z функции $f_i(x)$, имеющей алгебраическую степень d и использующей в качестве точек съема ячейки линейного регистра длиной L, определяется следующим образом:

$$\Lambda(z) \le L_d = \sum_{j=1}^{d} \binom{L}{j}. \qquad (4)$$

В [5] показано, что для ЛРР с примитивным образующим полиномом простой степени L доля P_n фильтр-генераторов, использующих в качестве нелинейного преобразования нелинейную функцию с алгебраической степенью d, генерирующих последовательности с линейной сложностью L_d, определяется как

$$P_n \approx e^{-L_d/L2^L} > e^{-1/L}. \qquad (5)$$

Как видно из (5), уже при $L > 100$ линейная сложность таких функций есть фактически L_d, определенная в (4). Однако из (1) следует, что степень L обобщенного регистра никогда не будет простой в силу того, что L – число составное. Следовательно, особенностью схем поточного преобразования информации на основе обобщенного регистра является тот факт, что верхняя граница линейной сложности является недостижимой. Кроме того, очевидно, что при фиксированной степени L единственным способом повышения линейной сложности является выбор нелинейных преобразований с максимально возможной алгебраической сте-

пенью d. Поэтому при разработке схем преобразования с использованием ЛРР, построенных над $GF(2^q)$, целесообразно подбирать степень примитивного полинома n таким образом, чтобы длина эквивалентного регистра L, построенного над GF(2), была достаточно большой для обеспечения высокой линейной сложности генерируемой последовательности.

Следует отметить, что поскольку регистр сдвига является линейным устройством, существует возможность на основе использования линейной зависимости выходных значений последовательности восстановления внутреннего состояния ЛРР. Для противостояния атакам подобного рода наиболее часто используются следующие приемы [5]: неравномерное усечение, применение нелинейной функции и использование составных сдвиговых регистров с последующим применением нелинейной функции.

Выводы. При использовании в схемах поточного шифрования регистров сдвига, построенных над расширенным полем $GF(2^q)$, следует помнить, что существенное увеличение таких показателей стойкости, как период и линейная сложность последовательности, не приводит к достижению верхней границы линейной сложности даже при использовании образующего примитивного полинома. В связи с этим целесообразным является использование нелинейных преобразований с максимально достижимой алгебраической степенью, а также введение различного рода узлов усложнения.

ЛИТЕРАТУРА

1. *Hawkes P., Rose G. The t-class of Sober stream ciphers. Technical report. – QUALCOMM Australia, suite 410. – 1999. – http://www.home.aone.net.au/qualcomm.*
2. *Golic J.D. On the security of nonlinear filter generators // Proceedings of Fast Software Encryption'96. – 1996. – Vol. 1039, Springer-Verlag. – P. 173 – 188.*
3. *Herlestam T. On functions of linear shift register sequences // In LNCS 219; Advances in Cryptology: Eurocrypt'85, Berlin: Springer-Verlag. – 1986. – P. 119 – 129.*
4. *Key E.L. An analysis of the structure and complexity of nonlinear binary sequence generators // IEEE Trans. Inform. Theory. – 1976. – Vol. IT-22, № 6. – P. 732 – 763.*
5. *Rueppel R.A. Analysis and Design of Stream Ciphers. Berlin, Springer-Verlag, 1986.*

Поступила 15.04.2004

***СТАСЕВ Юрий Владимирович**, д.т.н., проф., начальник факультета ХВУ. В 1981 году окончил ХВВКИУ РВ. Область научных интересов – помехоустойчивые системы связи, криптографическая защита информации.*

***ИЗБЕНКО Юрий Анатолиевич**, к.т.н., н.с. НИЛ кафедры ХВУ. В 1998 году окончил ХВУ. Область научных интересов – криптографическая защита информации.*

***ПЕТРУКОВИЧ Дмитрий Евгеньевич**, к.т.н., нач. отделения лаборатории ХВУ. В 1992 году окончил ХВККИУ РВ. Области научных интересов – компактное представле-*

ние видеоданных, криптографическая защита информации.