УДК 621.391

ИССЛЕДОВАНИЕ СВОЙСТВ ПОТОЧНЫХ СИММЕТРИЧНЫХ КРИПТОСИСТЕМ НА ОСНОВЕ СВЕРТОЧНЫХ КОДОВ

И.Е. Кужель
(представил д.т.н., проф. Ю.В. Стасев)

Рассматриваются поточные симметричные теоретико-кодовые схемы, построенные на основе сверточных кодов. Исследуются их криптографические свойства, обосновываются требования к методам сверточного кодирования.

Введение. Одним из перспективных направлений развития современной криптографии являются методы, основанные на использовании алгебраических кодов [1 – 6]. С помощью маскирования алгебраического кода под случайный код (код общего положения) задача декодирования для злоумышленника представляется как вычислительно сложная. Не зная правило маскирования, злоумышленник вынужден использовать сложный декодер случайного кода, а весь процесс кодирования-декодирования в этом случае эквивалентен односторонней криптографической функции. В работе [6] предложены поточные криптосистемы, основанные на применении непрерывных кодов. **Целью** настоящей статьи является исследование свойств предложенных криптосхем, оценка потенциальных возможностей по обеспечению безопасности обрабатываемой и передаваемой информации, обоснование требований к используемым в них методам сверточного кодирования.

Основная часть. Рассмотрим поточные симметричные теоретико-кодовые схемы (ТКС), впервые предложенные в [6].

Зафиксируем некоторое правило f непрерывного кодирования, т.е. правило отображения информационного, в общем случае непрерывного, потока данных $I = \{I_1, I_2, \dots, I_k, \dots\}$ в непрерывный поток кодовых символов $c = \{c_1, c_2, \dots, c_n, \dots\}$. По определению, поточные ТКС – это симметричные криптосистемы, осуществляющие процесс поточного криптографического преобразования данных на основе использования непрерывного кода с замаскированным правилом f. Процесс криптографического преобразования записывается в виде

$$c^* = f(I)X + e,$$

где $c^* = \{c^*_1, c^*_2, \dots, c^*_n, \dots\}$ – непрерывный поток данных на выходе криптосхемы; X – оператор маскирования правила f; $e = \{e_1, e_2, \dots, e_n, \dots\}$ –

случайный поток ошибок, вес которого на длине l кадров не превосходит $t = \lfloor (d_\infty - 1)/2 \rfloor$. Величина l определяется из выражения $d_\infty = \max(d_l)$.

Проведем оценку параметров поточных криптосистем, построенных на основе теоретико-кодовых схем с использованием непрерывных кодов. Введем следующие обозначения: l_I – длина информационного кадра, поступающего на вход поточной теоретико-кодовой схемы (в битах); l_s – длина кадра криптограммы на выходе поточной теоретико-кодовой схемы (в битах); l_K – длина секретного ключа поточной криптосистемы (в битах); I_{K+} – сложность решения задачи криптоанализа (количество групповых операций); R – относительная скорость передачи, как отношение $R = l_I / l_s$.

Параметры сверточного (n, k, d_∞) кода связаны соотношениями: $k = (r + 1)\cdot k^0$; $n = (r + 1)\cdot n^0 = k\cdot n^0/k^0$; $\nu = r\cdot k^0$, где k^0 – длина информационного кадра; n^0 – длина кадра кодовых символов; r – длина регистра сдвига, на котором строиться сверточный кодер; ν – длина кодового ограничения. Следовательно, что для криптосистем, построенных на сверточных (n, k, d_∞) кодах над $GF(2^m)$ длина информационного кадра (в битах) запишется в виде $l_I = k^0\cdot m$, а длина кадра криптограммы на выходе поточной теоретико-кодовой схемы (в битах) запишется, соответственно, в виде: $l_s = n^0\cdot m$. Относительная скорость передачи в поточных теоретико-кодовых схемах на сверточных кодах всегда меньше единицы и определяется скоростью сверточного кода $R = l_I/l_s < 1$.

Длина секретного ключа поточной криптосистемы (в битах) определяется выражением $l_K = \log_2 N(f) = \log_2 q^{rk^0}$, где N(f) – мощность множества различных правил сверточного кодирования.

Сложность решения задачи криптоанализа определяется сложностью наилучшего алгоритма декодирования случайного непрерывного кода. Если задан вид сверточного кода, то криптоанализ сводится к его декодированию и не отличается по сложности от дешифрования уполномоченным пользователем. Если вид сверточного кода злоумышленнику не известен (хранится в секрете), то для эффективного криптоанализа противник должен каким-либо образом выяснить параметры искомого сверточного кода. Если стратегией противника является угадывание параметров случайного кода над GF(q), то ему потребуется перебрать $N(f) = mq^{rk^0}$ вариантов, т.е. криптоанализ эквивалентен подбору. Если принять условие о переборе одного ключа на каждой выполняемой операции, то выражение для сложности криптоанализа (в групповых операциях) запишется в виде

$$I_{K+} = mq^{rk^0}.$$

Основным параметром крипитосистемы, определяющим его стойкость, является сложность задачи криптоанализа. Воспользуемся последним выражением для определения потенциальной криптостойкости. На рис. 1 представлены зависимости $I_K + (v)$ для различных q при гипотетическом упрощенном варианте m = 1 (в реальных схемах m > 1, что только улучшит

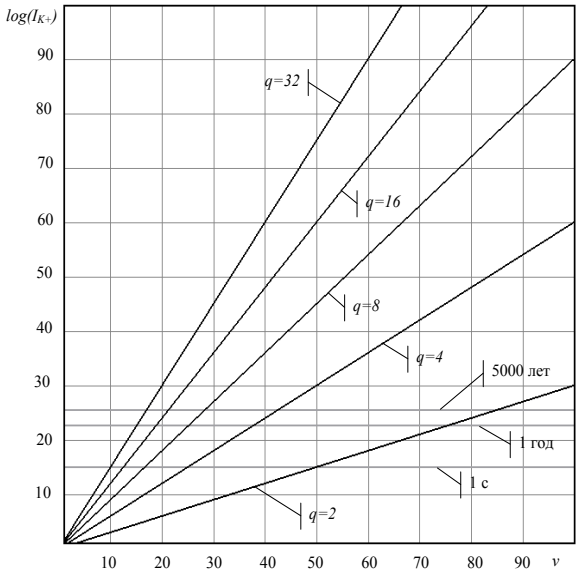

Рис. 1. Зависимость сложности подбора ключа от длины кодового ограничения в теоретико-кодовых схемах на сверточных кодах над GF(q)

е затраты, необходимые для полного перебора ключа при выполнении 10^{15} переборов в секунду.

Как следует из приведенных на рис. 1 зависимостей, для криптографической защиты информации в теоретико-кодовых схемах представляют интерес только сверточные коды с v > 80 бит. Действительно, двоичные сверточные коды с длиной кодового ограничения v > 80 бит позволяют реализовать потенциально стойкую поточную криптосхему со сложностью криптоанализа $I_K+ > 10^{22}$. В то же время, построение таких сверточных кодов сопряжено со значительными трудностями, состоящими в выборе порождающих многочленов кода. Кроме того, повышение длины кодового ограничения приводит к существенному росту затрат памяти на реализацию методов декодирования сверточных кодов.

Одним из возможных направлений в построении поточных теоретико-кодовых схем является разработка и исследование недвоичных сверточных кодов. Действительно, как следует из зависимостей, приведенных на рис. 1, увеличение мощности образующего поля позволяет существенно сократить длину кодового ограничения сверточного кода при сохранении потенциально высоких показателей стойкости.

Выводы. Таким образом, как показали проведенные исследования, мощный математический аппарат сверточного кодирования позволяет

задавать поточные теоретико-кодовые схемы для эффективной криптографической защиты информационного потока символов. Криптостойкость таких криптосистем зависит, в первую очередь, от длины кодового ограничения и определяется эффективностью методов построения сверточных кодов. Для определения криптографически стойкой поточной теоретико-кодовой схемы используемые в них методы сверточного кодирования должны удовлетворять следующим требованиям:

– легко описываться в полиномиальном и матричном виде;

– иметь возможность применения быстрых алгоритмов декодирования;

– иметь возможность формирования большого числа (по экспоненциальной зависимости) различных правил f сверточного кодирования при фиксированных (n, k, d_∞) параметрах и фиксированном v;

– иметь возможность алгебраического построения сверточных кодов с большой длиной кодового ограничения (десятки-сотни бит) для произвольного конечного поля GF(q).

Одним из **перспективных направлений дальнейших исследований** является разработка и исследование алгебраических методов построения сверточных кодов, удовлетворяющих указанным требованиям.

ЛИТЕРАТУРА

1. *McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory // DGN Progress Report 42–44, Jet Propulsi on Lab. Pasadena, 1978. – P. 114 – 116.*
2. *Niederreiter H. Knapsack-Type Cryptosystems and Algebraic Coding Theory // Probl. Control and Inform. Theory. – 1986. – V. 15. – P. 19 – 34.*
3. *Сидельников В.М. Криптография и теория кодирования // Материалы конференции «МГУ и развитие криптографии в России». – М.: МГУ. – 2002. – 22 с.*
4. *Халимов Г.З., Буханцов А.Д. Применение помехоустойчивого кодирования для обеспечения безопасности каналов передачи данных // Труды НТК «Передача, обработка и отображение информации». – Х.: НАНУ, ПАНИ. – 1994. – С. 28.*
5. *Кузнецов А.А., Евсеев С.П. Разработка теоретико-кодовых схем с использованием эллиптических кодов // Системи обробки інформації. – Х.: ХВУ.– 2004. – Вип. 5. – С. 127 – 132.*
6. *Кузнецов А.А., Приходько С.И., Кужель И.Е., Гусев С.А. Симметричные поточные криптосистемы на основе сверточных кодов // Авиационно-космическая техника и технология. – Х.: ХАИ. – 2004. – № 6. – С. 34 – 39.*

Поступила 7.10.2004

***КУЖЕЛЬ Игорь Евгеньевич**, научный сотрудник НИЛ ХУ ВС. Область научных интересов – криптографическое преобразование информации, алгебраическая теория кодов и их применение в системах передачи данных.*