УДК 621.391

ИССЛЕДОВАНИЕ СТОЙКОСТИ К ВЗЛОМУ ПРОТИВНИКОМ КАСКАДНЫХ ТЕОРЕТИКО-КОДОВЫХ СХЕМ

А.А. Кузнецов[1], В.И. Грабчак[2], С.П. Евсеев[1]
([1]Харьковский университет Воздушных Сил,
[2]Сумской военный институт РвиА)

Рассматриваются секретные системы теоретической стойкости, построение которых основано на использовании алгебраических блоковых кодов (теоретико-кодовые схемы). Исследуется стойкость каскадных теоретико-кодовых схем к взлому противником методом оптимального статистического опробования.

системы теоретической стойкости, алгебраические блоковые коды, каскадные теоретико-кодовые схемы

Постановка проблемы в общем виде и анализ литературы. Важными требованиями к перспективной АСУВ являются достоверность и информационная скрытность обрабатываемых и передаваемых данных. Эти показатели характеризуют способность системы обеспечивать точное воспроизведение передаваемых сообщений в пунктах приема и противостоять раскрытию противником содержания передаваемой информации [1, 2].

В работах [3 – 5] показано, что обеспечить требуемые показатели достоверности и информационной скрытности возможно на основе применения теоретико-кодовых схем – секретных систем теоретической стойкости, построение которых основано на использовании алгебраических блоковых кодов. Перспективным направлением в их развитии является применение каскадных конструкций. Так, в работе [6] показано, что применение обобщенных каскадных кодов позволяет строить кодовые схемы защиты информации с небольшими размерами ключевых данных и низкой сложностью реализации. Актуальным направлением является исследование стойкости каскадных теоретико-кодовых схем к взлому противником.

Формирование каскадной теоретико-кодовой схемы. Для формирования каскадной теоретико-кодовой схемы воспользуемся алгебраическим определением обобщенных каскадных кодов. По определению алгебраически заданный обобщенный каскадный код порядка m одно-

значно определяется n_2 квадратными двоичными матрицами H_0^j, $j=\overline{1,n_2}$ порядка n_1 (задающих (n_1,k_i,d_{1i}) коды первой ступени) и $m+1$ групповыми над $GF(2^{a_i})$, $i=\overline{1,m+1}$ кодами второй ступени с параметрами (n_2,b_i,d_{2i}). В [6] показано, что формирование каскадной кодовой схемы осуществляется путем маскирования кодового слова обобщенного каскадного кода под случайный код. Существуют следующие варианты маскирования:

1) маскирование кодов первой ступени;
2) маскирование кодов второй ступени;
3) одновременное маскирование кодов первой и второй ступени.

В работе [6] показано, что при основном варианте построения (в качестве матриц H_0^j для всех $j=\overline{1,n_2}$ выбирается одна и та же треугольная матрица H_0 порядка n_1) при равновероятном выборе и случайном опробовании ключа противнику потребуется перебрать следующее число вариантов:

– при маскировке всех кодов первой ступени

$$\delta_1=\frac{|\Theta_1|}{|\Gamma_{A1}|}; \qquad (1)$$

– при маскировке всех кодов второй ступени, потребуется

$$\delta_2^{m+1}=\sum_{i=1}^{2^{n_1-1}}\prod_{j=1}^{m+1}\frac{\left|\Theta_{2_j^i}\right|}{\left|\Gamma_{A2_j^i}\right|}, \qquad (2)$$

где Θ_1 – множество различных матриц, задающих коды первой ступени; Γ_{A1} – группа автоморфизмов кода первой ступени; $\Theta_{2_j^i}$ – множество различных матриц, задающих (n_2,b_j,d_{2j}) коды над полем; $\Gamma_{A2_j^i}$ – группа автоморфизмов (n_2,b_j,d_{2j}) кода над полем $GF(2^{a_i})$.

Соответственно, объем необходимой памяти для хранения ключа l_K (длина ключа) составит (в битах):

– при маскировке всех кодов первой ступени

$$l_{K_1}=(n_1)^2; \qquad (3)$$

– при маскировке всех кодов второй ступени

$$l_{K_2} = n_2 \cdot \sum_{i=1}^{m+1} (b_i \cdot a_i). \qquad (4)$$

Проведем сравнительную оценку рассмотренных вариантов маскирования обобщенного каскадного кода, сравним потенциальную стойкость к раскрытию противником содержания передаваемой информации как число переборов при оптимальном статистическом опробовании при фиксированной длине ключа.

Исследование стойкости каскадных теоретико-кодовых схем. Длина ключа во всех рассмотренных вариантах маскирования кодового слова обобщенного каскадного кода однозначно определяется длиной кода соответственно первой и/или второй ступени. Потенциальная стойкость также зависит от длины кода, но определяется, прежде всего, порядком группы автоморфизма. Проведем оценку снизу.

Для блокового кода, построенного с использованием арифметики колец многочленов (например, коды БЧХ, РС коды) длины n символов мощность множества Θ определяется выражением

$$\Theta = (q-1)^n \cdot n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 = (q-1)^n \cdot n!.$$

В работе [3] показано, что порядок группы автоморфизмов (n, k, d) РС кода удовлетворяет неравенству:

$$\Gamma_A \le (q^{d-1}-1)\cdot(q^{d-1}-q)\cdot(q^{d-1}-q^2)\cdot\ldots\cdot(q^{d-1}-q^{d-2}).$$

Для оценки числа переборов сверху предположим, что $|\Gamma_A| = 1$.

Тогда, после подстановки в (1) и (2) получим:

$$(n_1!) \ge \delta_1 \ge \left(\frac{n_1!}{(2^{d_1-1}-1)\cdot(2^{d_1-1}-2)\cdot(2^{d_1-1}-2^2)\cdot\ldots\cdot(2^{d_1-1}-2^{d_1-2})} \right); \qquad (5)$$

$$\left(\sum_{i=1}^{2^{n_1-1}} \prod_{j=1}^{m+1} (2^{a_i}-1)^{n_2} \cdot n_2! \right) \ge \delta_2^{m+1} \ge$$

$$\ge \left(\sum_{i=1}^{2^{n_1-1}} \prod_{j=1}^{m+1} \frac{(2^{a_i}-1)^{n_2} \cdot n_2!}{\left(2^{a_i(d_{2_j}-1)}-1\right)\cdot\left(2^{a_i(d_{2_j}-1)}-2^{a_i}\right)\cdot\ldots\cdot\left(2^{a_i(d_{2_j}-1)}-2^{a_i(d_{2_j}-2)}\right)} \right). \qquad (6)$$

В случае маскировки всех кодов первой и второй ступеней обобщенного каскадного кода с сохранением в тайне от противника порядка обобщенного каскадного кода число переборов для оптимального статистического опробования будет лежать в пределах:

$$(n_1!)\cdot\left(\sum_{i=1}^{2^{n_1-1}}\prod_{j=1}^{m+1}(2^{a_i}-1)^{n_2}\cdot n_2!\right)\geq \delta_1\cdot\delta_2^{m+1}\geq$$

$$\geq\left(\frac{n_1!}{(2^{d_1-1}-1)\cdot(2^{d_1-1}-2)\cdot(2^{d_1-1}-2^2)\cdot\ldots\cdot(2^{d_1-1}-2^{d_1-2})}\right)\times \qquad (7)$$

$$\times\left(\sum_{i=1}^{2^{n_1-1}}\prod_{j=1}^{m+1}\frac{(2^{a_i}-1)^{n_2}\cdot n_2!}{\left(2^{a_i(d_{2_j}-1)}-1\right)\cdot\left(2^{a_i(d_{2_j}-1)}-2^{a_i}\right)\cdot\ldots\cdot\left(2^{a_i(d_{2_j}-1)}-2^{a_i(d_{2_j}-2)}\right)}\right).$$

Анализ выражений (5) – (7) показывает, что наибольшее число переборов, которые потребуется выполнить противнику при оптимальном статистическом опробовании, дает маскирование всех кодов первой и второй ступеней с сохранением в тайне от противника порядка обобщенного каскадного кода (см. выражение (7)), т.е. третий вариант маскирования. Среди остальных вариантов наибольшее число переборов дает маскирование всех кодов второй ступени.

Проведем сравнительные исследования вариантов маскирования и необходимых объемов ключевых данных. Для упрощения вычислений предположим, что используется основной вариант построения и для всех b_i и a_i выполняются равенства:

$$b_i=\frac{n_2}{2};\ a_i=\frac{n_1}{m+1};\ d_{2i}=n_2-b_i+1=\frac{n_2}{2}+1.$$

Тогда выражение (4) перепишется в виде

$$l_{K_2}=n_2\cdot\sum_{i=1}^{m+1}(b_i\cdot a_i)=\frac{(n_2)^2\cdot n_1}{2}\ \text{бит.}$$

Принимая во внимание, что

$$\left(\sum_{i=1}^{2^{n_1-1}}\prod_{j=1}^{m+1}(2^{a_i}-1)^{n_2}\cdot n_2!\right)=2^{n_1-1}\cdot\left(\left(2^{\frac{n_1}{(m+1)}}-1\right)^{n_2}\cdot n_2!\right)^{m+1}\approx 2^{n_1n_2+n_1-1}\cdot(n_2!)^{m+1}$$

оценим верхнюю границу числа переборов для оптимального статистического опробования.

На рис. 1 представлены зависимости числа переборов от длины ключа: а – $n_1=n_2$; б – $n_1=n_2/10$; в – $n_1=n_2\cdot 10$.

На рисунках представлены случаи:

1 – маскирование кода первой ступени обобщенного каскадного кода;

2 – маскирование кода второй ступени обобщенного каскадного кода нулевого порядка;

3 – маскирование кода второй ступени обобщенного каскадного кода пятого порядка;

4 – маскирование кода второй ступени обобщенного каскадного кода десятого порядка;

5 – маскирование кода второй ступени обобщенного каскадного кода двадцатого порядка.

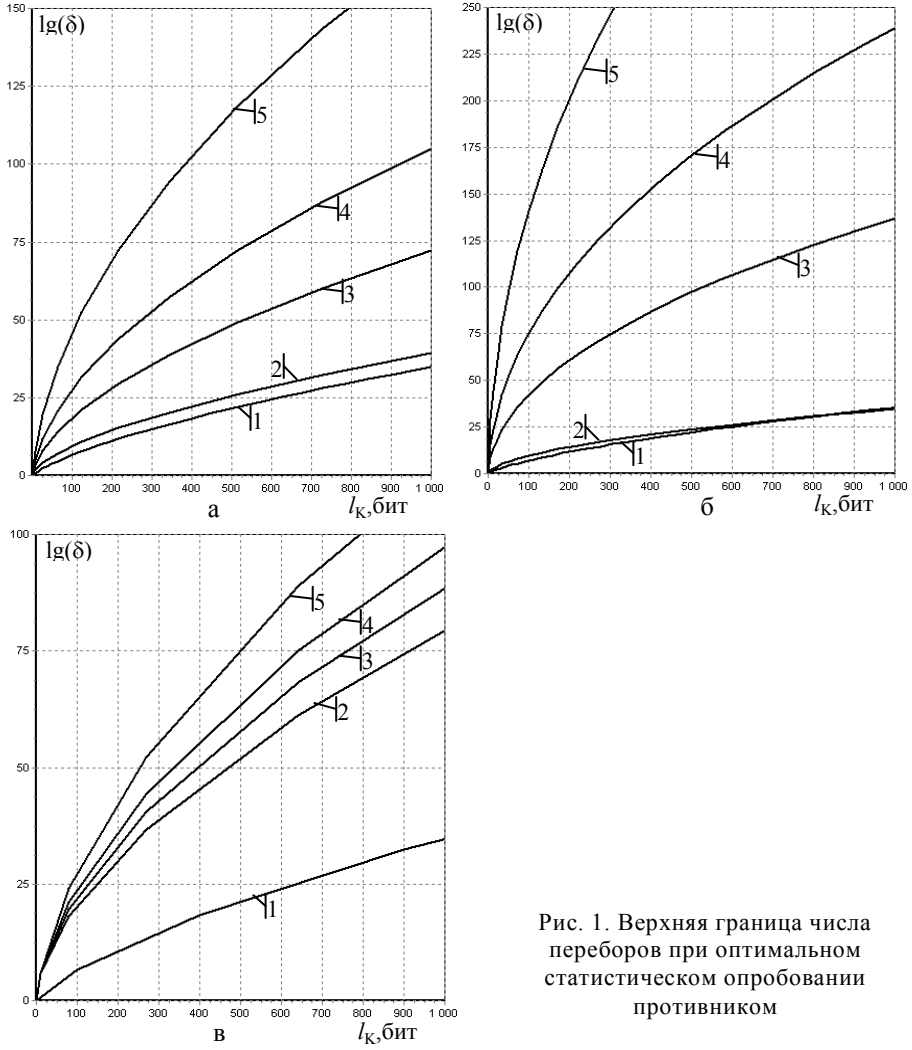

Рис. 1. Верхняя граница числа переборов при оптимальном статистическом опробовании противником

5

Как следует из приведенных на рис. 1 зависимостей, число переборов при оптимальном статистическом опробовании противником резко возрастает в случае маскирования кодов второй ступени и использования обобщенных каскадных кодов высокого порядка. Эта тенденция сохраняется для различных соотношений в длинах кодов первой и второй ступени обобщенного каскадного кода.

Выводы. Таким образом, проведенные исследования показали, что эффективным способом построения теоретико-кодовых схем с точки зрения соотношения длины ключа и числа переборов оптимального статистического опробования противником является маскирование кодов второй ступени в обобщенном каскадном коде высокого порядка. Перспективным направлением дальнейших исследований является разработка каскадных кодовых конструкций с алгеброгеометрическими кодами на внешнем каскаде обобщенного каскадного кода.

ЛИТЕРАТУРА

1. *Науменко М.І., Стасєв Ю.В., Кузнецов О.О. Теоретичні основи та методи побудови алгебраїчних блокових кодів: Монографія. – Х.: ХУ ПС, 2005. – 267 с.*
2. *ДСТУ В 3265-95. Зв'язок військовий. Терміни та визначення. – К.: УкрНДІССІ, 1995. – 23 с.*
3. *Сидельников В.М. Криптография и теория кодирования // Материалы конференции «Московский университет и развитие криптографии в России». – М.: МГУ, 2002. – 22 с.*
4. *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.*
5. *Стасев Ю.В., Кузнецов А.А. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов // Кибернетика и системный анализ: Международный научно-теоретический журнал. – К.: НАНУ. – 2005. – № 3. – С. 47-57.*
6. *Кузнецов А.А., Грабчак В.И., Евсеев С.П. Каскадные кодовые схемы защиты информации // Системи обробки інформації. – Х.: ХУ ПС. – 2005 – Вип. 9 (49). – С. 206-211.*

Поступила 5.01.2006

Рецензент: доктор технических наук, профессор Ю.В. Стасев,
Харьковский университет Воздушных Сил им. И. Кожедуба.