УДК 621.391

А.А. Кузнецов[1], В.И. Грабчак[2], С.П. Евсеев[1]

[1]*Харьковский университет Воздушных Сил им. И. Кожедуба*
[2]*Военный институт ракетных войск и артиллерии им. Б. Хмельницкого, Сумы*

РЕЗУЛЬТАТЫ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ КАСКАДНЫХ ТЕОРЕТИКО-КОДОВЫХ СХЕМ

Представлены результаты статистического тестирования безопасности каскадных теоретико-кодовых схем с алгеброгеометрическими кодами и кодами Рида-Соломона на внешней ступени обобщенного каскадного кода.

каскадные теоретико-кодовые схемы, статистическая безопасность, статистический портрет

Введение

Постановка проблемы в общем виде и анализ литературы. Теоретико-кодовые схемы для обеспечения безопасности информации впервые предложены в [1]. Их основное достоинство состоит в высокой скорости криптографического преобразования информации и интеграции помехоустойчивого кодирования с шифрованием [2]. В работах [3 – 5] показано, что построение теоретико-кодовых схем на каскадных кодах позволяет без ухудшения конструктивных параметров и снижения энергетического выигрыша от кодирования существенно (на несколько порядков) повысить их быстродействие. Важным вопросом практического использования каскадных теоретико-кодовых схем является исследование их статистической безопасности.

Целью статьи является исследование статистической безопасности каскадных теоретико-кодовых схем с кодами Рида-Соломона (РС) и алгеброгеометрическими кодами на внешней ступени обобщенного каскадного кода. Исследования проводились в соответствии с методикой тестирования NIST SP 800-22 [6], рекомендованной Национальным институтом по стандартизации и технологиям США.

Каскадные теоретико-кодовые схемы

Наиболее общим классом каскадных кодовых конструкций являются обобщенные каскадные коды. По определению алгебраически заданный обобщенный каскадный код порядка m однозначно 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 внутренней ступени и $m+1$ групповыми над $GF(2^{a_j})$, $j=\overline{1,m+1}$ кодами внешней ступени с параметрами (n_2,b_j,d_{2j}). При этом (n,k,d) параметры обобщенного каскадного кода удовлетворяют следующим соотношениям [7]:

$$n=n_1n_2;\ k=\sum_{i=1}^{m+1}a_ib_i;$$

$$d\ge\begin{cases}\min\left\{d_{1i}d_{2i}:i=\overline{1,m}\right\}\text{при } b_{m+1}=0,\\ \min\left\{d_{2m+1},d_{1i}d_{2i}:i=\overline{1,m}\right\}\text{при } b_{m+1}\ne 0.\end{cases}\quad(1)$$

Для построения кодов внутренней ступени используется треугольная проверочная матрица H_0 порядка n_1, которая в клеточной форме имеет вид

$$H_0=\begin{Vmatrix}I_{a_1}&&&&&\\P_{11}&I_{a_2}&&0&&\\P_{21}&P_{22}&I_{a_3}&&&\\\dots&\dots&\dots&\dots&\dots&\dots\\P_{m1}&P_{m2}&P_{m3}&\dots&P_{mm}&I_{a_{m+1}}\end{Vmatrix}=\begin{Vmatrix}\tilde H_0\\\tilde H_1\\\tilde H_2\\\dots\\\tilde H_m\end{Vmatrix},\quad(2)$$

где $\tilde H_0=\left\|I_{a_1}\ \ 0\right\|$; $\tilde H_i=\left\|P_{i_1}\ P_{i_2}\ \dots\ P_{i_i}\ I_{a_1}\ 0\ \dots\ 0\right\|$; $i=\overline{1,m}$; клетки P_{i_s} – двоичные матрицы размеров $a_{i+1}\times a_s$; I_{a_s} – единичная матрица порядка a_s.

Проверочная матрица H_i $(i=\overline{1,m})$ вида

$$H_i=\begin{Vmatrix}\tilde H_i\\\tilde H_{i+1}\\\dots\\\tilde H_m\end{Vmatrix}=\begin{Vmatrix}P_{i_1}&P_{i_2}&\dots&P_{i_i}&I_{a_{i+1}}&&0&\\P_{i+1_1}&P_{i+1_2}&\dots&P_{i+1_i}&P_{i+1_{i+1}}&I_{a_{i+2}}&&\\\dots&\dots&\dots&\dots&\dots&\dots&\dots&\dots\\P_{m_1}&P_{m_2}&\dots&P_{m_i}&P_{m_{i+1}}&\dots&P_{m_m}&I_{a_{m+1}}\end{Vmatrix};$$

полностью определяемая матрицей H_0 (состоит из $m-i+1$ клеточных строк матрицы H_0) задает i-й код первой ступени с параметрами (n_1,k_i,d_{1i}).

Зафиксируем каскадную теоретико-кодовую схему по обобщенному каскадному коду порядка m. Ее параметры задаются следующей теоремой [4 – 6].

Теорема 1. Пусть задана каскадная теоретико-кодовая схема по обобщенному каскадному коду порядка m путем маскировки всех его кодов второй ступени. Тогда объем ключа l_K, длина информационного блока данных l_M и длина кодограммы l_E (в битах) задаются следующими выражениями

$$l_K=n_2\sum_{j=1}^{m+1}b_j\cdot a_j;\ l_M=\sum_{j=1}^{m+1}b_j\cdot a_j;\ l_E=n_1\cdot n_2.\quad(2)$$

Для каскадных теоретико-кодовых схем с алгебро-геометрическими кодами справедлива теорема 2 [5].

Теорема 2. Зафиксируем m + 1 алгебраических кривых рода g_j, $j=\overline{1,m+1}$ и соответствующие алгеброгеометрические (n_2, b_j, d_{2j}) коды. Тогда параметры каскадной теоретико-кодовой схемы по обобщенному каскадному коду порядка m, построенной путем маскирования m + 1 алгеброгеометрических кодов внешней ступени над $GF(2^{a_j})$ задается выражениями:

$$l_K = (\alpha+1)\cdot n_2 \cdot n_1 - n_2 \sum_{j=1}^{m+1} g_j \cdot a_j;$$

$$l_M = (\alpha+1)\cdot n_1 - \sum_{j=1}^{m+1} g_j \cdot a_j;\ l_E = n_1 \cdot n_2, \qquad (3)$$

Теоремы 1, 2 устанавливают важную зависимость между параметрами обобщенного каскадного кода (1) с характеристиками каскадных теоретико-кодовых схем.

Исследование статистической безопасности каскадных теоретико-кодовых схем

Проведем исследования безопасности каскадных теоретико-кодовых схем с кодами РС над $GF(2^5)$ на внешней ступени обобщенного каскадного кода при m = 5. Зафиксируем 5 кодов РС над $GF(2^5)$ на внешней ступени обобщенного каскадного кода с параметрами (31,26,6), (31,24,8), (31,20,12), (31,16,16) и (31,8,24). В качестве кодов внутренней ступени используем коды БЧХ, задаваемыми треугольной проверочной матрицей вида (2) и имеющими следующие параметры: (31,5,16), (31,10,12), (31,15,8), (31,20) и (31,25,4). Тогда в соответствии с (1) имеем обобщенный каскадный код с параметрами: $n = 961$, $k = 470$, $d \ge 96$. По теореме 1 параметры каскадной теоретико-кодовой схемы с кодами РС над $GF(2^5)$ на внешней ступени обобщенного каскадного кода и кодами БЧХ на внутренней ступени будут иметь следующие значения: $l_K = 13020$; $l_M = 420$; $l_E = 961$.

Для проведения тестирования были взяты следующие параметры: длина тестируемой последовательности – 10^6 бит; количество тестируемых последовательностей – 100; уровень значимости $\alpha = 0{,}01$.

Таким образом, объем тестируемой выборки $N = 10^6 \times 100 = 10^8$ бит; количество (q) для разных длин q = 189, таким образом, статистический портрет генератора составляет 18900 значений вероятности P.

В результате тестирования двоичной последовательности формируется вектор значений вероятности $P = \{P_1, P_2, \ldots, P_{189}\}$. Анализ составляющих P_i этого вектора позволяет указать на конкретные дефекты случайной тестируемой последовательности.

На рис. 1 представлен статистический портрет каскадных теоретико-кодовых схем, построенных по кодам РС над $GF(2^5)$.

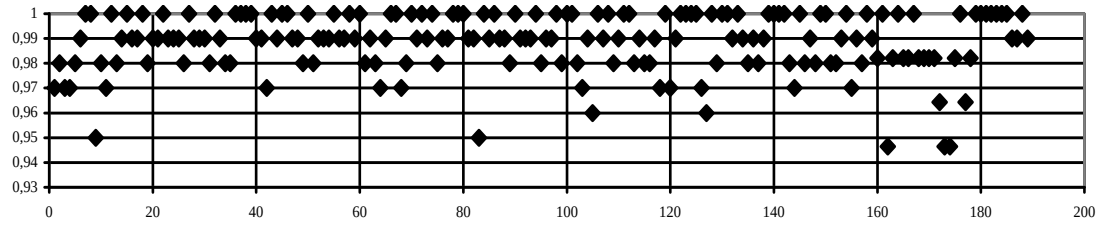

Рис. 1. Статистический портрет программной реализации каскадных теоретико-кодовых схем, построенных на кодах Рида-Соломона над $GF(2^5)$

Статистический портрет представляет собой диаграмму вероятностей прохождения соответствующих статистических тестов. Из представленного рисунка видно, что 184 статистических тестов каскадные теоретико-кодовые схемы, построенные по кодам РС успешно прошли с критерием $P_i > 0{,}96015$. Пять тестов по этому критерию не прошли, что является незначительным отклонением от нижней оценки. Повторное тестирование с другой сформированной последовательностью показало аналогичный результат. Кроме того, 66% тестов успешно прошли по критерию $P_i > 0{,}99$.

Проведем исследования безопасности каскадных теоретико-кодовых схем с алгеброгеометрическими кодами на внешней ступени обобщенного каскадного кода. Зафиксируем алгебраическую кривую $x^3 + y^2 z + yz^2 = 0$ рода $g_j = 1$ и следующие алгеброгеометрические коды над $GF(2^5)$: (31,26,5), (31,24,7), (31,20,11), (31,16,15) и (31,8,23). В качестве кодов внутренней ступени используем ту же треугольную проверочную матрицу H_0 порядка n_1 кода БЧХ. Для проведения статистических исследований выберем параметры, аналогичные предыдущему примеру. На рис. 2 представлен статистический портрет программной реализации каскадных теоретико-кодовых схем, построенных по алгебраической кривой $x^3 + y^2 z + yz^2 = 0$ над $GF(2^5)$. Из рисунка видно, что 187 статистических тестов каскадные теоретико-кодовые схемы, построенные по алгебраическим кривым успешно прошли с критерием $P_i > 0{,}96015$. Два теста под номером 9 и 83 по этому

критерию не прошли, оба имеют значения $P_{9,83} = 0,94 < 0,96015$. Повторное тестирование с другой сформированной последовательностью показало аналогичный результат. Кроме того, 68% тестов успешно прошли по критерию $P_i > 0,99$. Полученный результат имеет лучший статистический портрет по сравнению с каскадными теоретико-кодовыми схемами, построенными на кодах Рида-Соломона. Для примера на рис. 3. представлен статистический портрет программной реализации алгоритма блочного симметричного шифрования FIPS 197 в режиме счетчика.

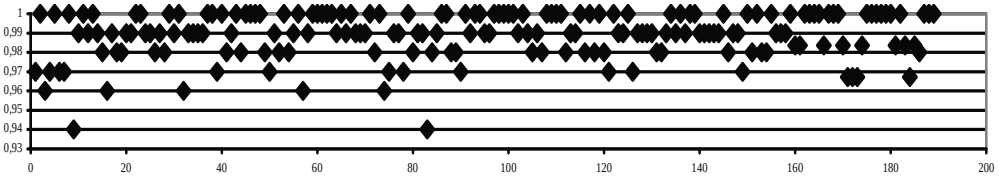

Рис. 2. Статистический портрет программной реализации каскадных теоретико-кодовых схем, построенных по алгебраической кривой $x^3 + y^2z + yz^2 = 0$ над $GF(2^5)$

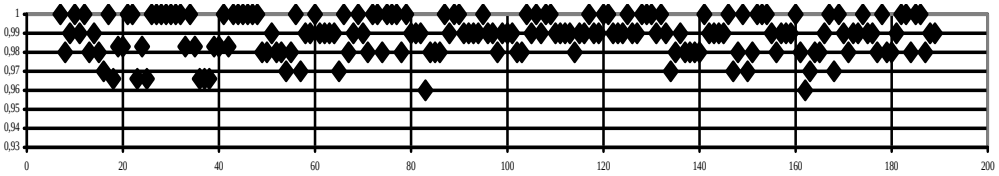

Рис. 3. Статистический портрет программной реализации FIPS 197

В табл. 1 сведены окончательные результаты тестирования программной реализации каскадных теоретико-кодовых схем, построенных по алгеброгеометрическим кодам, кодам РС, тестовой последовательности генератора псевдослучайных чисел BBS, рекомендуемой Национальным институтом по стандартизации и технологиям США, поставляемой вместе с пакетом тестов NIST SP 800-22 и программной реализации алгоритма блочного симметричного шифрования FIPS 197 в режиме счетчика (k_1 – количество тестов, в которых тестирование прошло ≥ 99% последовательностей, k_2 – количество тестов, в которых тестирование прошло больше ≥ 96% последовательностей).

Таблица 1

Результаты тестирования

Генератор	k_1	k_2
BBS	134 (71%)	189 (100%)
FIPS 197	126 (67%)	189 (100%)
Каскадные теоретико-кодовые схемы на алгебро-геометрических кодах	129 (68%)	187 (99%)
Каскадные теоретико-кодовые схемы на кодах РС	125 (66%)	184 (97%)

Как видно из данных, представленных в табл. 1, генераторы на каскадных теоретико-кодовых схемах обладают хорошими статистическими свойствами. Действительно, по результатам исследования статистической безопасности видно, что каскадные кодовые схемы защиты информации обеспечивают прохождение тестов с вероятностью, практически равной вероятности тестового генератора псевдослучайных чисел BBS и алгоритма блочного симметричного шифрования FIPS 197.

Выводы

Проведены экспериментальные исследования статистической безопасности каскадных теоретико-кодовых схем с кодами РС и алгеброгеометрическими кодами. Анализ полученных экспериментальных результатов позволяет сделать вывод о том, что каскадные теоретико-кодовые схемы с замаскированным алгеброгеометрическим кодом внешнего каскада, позволяют эффективно выполнять криптографическое преобразование данных – по своим показателям статистический портрет не уступает лучшим известным криптографическим алгоритмам, принятым в качестве национальных стандартов ведущих государств мира (FIPS 197). Практическое применение каскадных теоретико-кодовых схем на алгеброгеомнтрических кодах позволяет получить хорошие статистические свойства формируемых последовательностей и эффективно обеспечить информационную скрытность обрабатываемых и передаваемых данных.

Список литературы

1. *McEliece R.J. A Public-Key Criptosystem Based on Algebraic Theory // DGN Progres Report 42-44, Jet Propulsi on Lab. Pasadena, CA. January – February, – 1978. – P. 114-116.*
2. *Стасев Ю.В., Кузнецов А.А. Несимметричные теоретико-кодовые схемы с использованием алгеброгеометрических кодов // Кибернетика и системный анализ. – 2005. – №3. – С. 47-57.*
3. *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.*
4. *Стасев Ю.В., Кузнецов А.А., Грабчак В.И., Ковтун В.Ю. Разработка теоретико-кодовых схем на обобщенных каскадных кодах // Збірник наукових праць ХУПС. – Х.: ХУПС, 2006. – Вип. 2 (8). – С. 79-81.*
5. *Стасєв Ю.В., Кузнецов О.О., Грабчак В.І., Євсеєв С.П. Каскадні схеми захисту інформації на алгеброгеометричних кодах // Системи озброєння і військова техніка. – 2006. – № 1 (5). – С. 82-87.*
6. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22. – Washington: National Institute of Standards and Technology. – 2000. – P. 164.*

7. Блох Э.Л., Зяблов В.В. Обобщенные каскадные коды. – М.: Связь, 1976. – 240 с.

Поступила в редакцию 27.07.2006

Рецензент: д-р физ.-мат. наук, проф. С.В. Смеляков, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.