УДК 621.391

А.А. КУЗНЕЦОВ, канд. техн. наук,
С.П. ЕВСЕЕВ (г. Харьков),
В.И. ГРАБЧАК (г. Сумы)

РЕЗУЛЬТАТЫ СТАТИСТИЧЕСКОГО ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ ТЕОРЕТИКО-КОДОВЫХ СХЕМ НА ЭЛЛИПТИЧЕСКИХ КОДАХ

Представлені результати статистичного тестування безпеки теоретико-кодових схем, побудованихна еліптичних кодах. Проведені порівняльні дослідження статистичної безпеки теоретико-кодових схем, побудованих на кодах Рида-Соломона і на еліптичних кодах.

The results of the statistical testing of safety of the theoretic-codes charts built on elliptic codes are presented. Comparative researches of statistical safety of the theoretic-codes charts built on the codes of Reed-Solomon and on elliptic codes are conducted.

Постановка проблемы в общем виде и анализ литературы. Одним из перспективных направлений развития теории и методов обеспечения безопасности информации являются теоретико-кодовые схемы, построенные на алгебраических кодах [1 – 6]. В основе их построения лежит маскировка блокового кода под случайный код, соответственно их стойкость базируется на сложности декодирования случайного кода.

Исходя из общетеоретических положений теории секретных систем, потенциально стойкими являются системы, у которых символы криптограммы статистически не зависимы от символов открытого текста [7]. Для оценки таких зависимостей используются статистические тесты [8].

Целью статьи является статистическое исследование безопасности несимметричных теоретико-кодовых схем, построенных на эллиптических кодах.

Основная часть. Теоретико-кодовые схемы для безопасности информации впервые предложены в [1, 2]. Их основное достоинство состоит в высокой скорости криптографического преобразования информации [3, 4] и интеграции помехоустойчивого кодирования с шифрованием [5, 6]. Построенные теоретико-кодовые схемы на эллиптических кодах [5, 6] обладают высокими показателями эффективности: их применение позволяет обеспечить несимметричную обработку информации для эффективной защиты передаваемых данных от случайного или преднамеренного воздействия и обеспечить требуемые показатели достоверности и безопасности информации.

Важным вопросом практического использования теоретико-кодовых схем на эллиптических кодах для обеспечения защиты передаваемой информации является исследование их безопасности.

Исследования безопасности теоретико-кодовых схем проводились в соответствии с методикой тестирования NIST SP 800-22, рекомендованной Национальным институтом по стандартизации и технологиям США.

Для проведения тестирования были взяты следующие параметры:

- длина тестируемой последовательности $n = 106$ бит;
- количество тестируемых последовательностей $m = 100$;
- уровень значимости $\alpha = 0{,}01$.

Таким образом, объем тестируемой выборки составляет:

- $N = 106 \times 100 = 10600$ бит;
- количество (q) для разных длин $q = 189$, таким образом, статистический портрет генератора составляет 18900 значений вероятности P.

Результаты тестирования теоретико-кодовых схем на эллиптических кодах сведены в табл. 1.

Таблица 1

	Теоретико-кодовые схемы на эллиптических кодах	Теоретико-кодовые схемы на кодах Рида-Соломона	BBS	FIPS 197
Количество тестов, в которых тестирование прошло 99% последовательностей	141	132	134	126
Количество тестов, в которых тестирование прошло 96% последовательностей	189	188	189	189
Количество тестов, в которых значение вероятности P <=0,01	2	2		0
Количество тестов, в которых значение вероятности P <=0,001	1	0		0
Количество тестов, в которых значение вероятности P <=0,05	13	8		8
Допустимое значение доли прохождения теста для выборки размером 100 двоичных	0,96015			

последовательностей равняется	
Допустимое значение доли прохождения теста для выборки размером 71 двоичных последовательностей для тесту Random-Excursion равняется	0,954575

В табл. 1 приведены так же результаты статистического исследования теоретико-кодовых схем на кодах Рида – Соломона, подробно рассмотренные в [3, 4], и результаты исследования алгоритма блочного симметричного шифрования FIPS 197. В графе BBS приведены данные, которые соответствуют тестовой последовательности генератора псевдослучайных чисел BBS, рекомендуемой Национальным институтом по стандартизации и технологиям США и поставляемой вместе с пакетом тестов NIST SP 800-22.

На рис. 1 представлен статистический портрет программной реализации теоретико-кодовых схем, построенных по эллиптической кривой $y^2 + xy = x^3 + x^2 + 1$ над $GF(2^8)$.

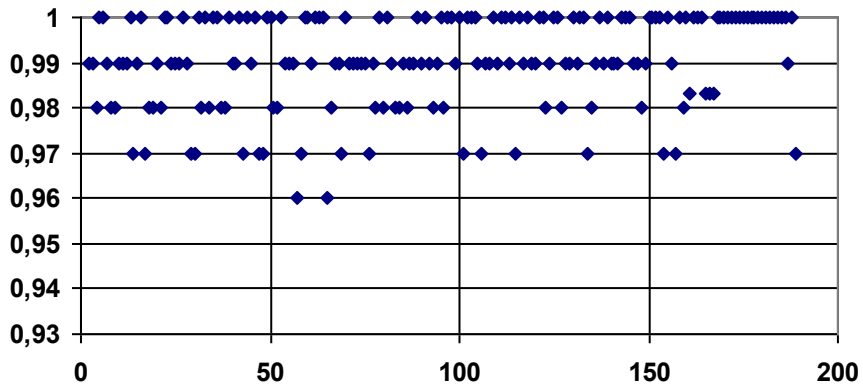

Рис. 1. Статистический портрет программной реализации теоретико-кодовых схем, построенных по эллиптической кривой $y^2 + xy = x^3 + x^2 + 1$ над $GF(2^8)$

Статистический портрет представляет из себя диаграмму вероятностей прохождения соответствующих статистических тестов. Из представленного рисунка видно, что статистический портрет программной реализации теоретико-кодовых схем, построенных по эллиптической кривой, соответствует предъявляемым требованиям – по всем тестам положительно прошло более 96% последовательностей.

На рис. 2. представлен статистический портрет программной реализации теоретико-кодовых схем, построенных по кодам Рида-Соломона над $GF(2^8)$. Более детальное исследование статистической безопасности кодовых схем защиты информации на кодах Рида-Соломона проведено в [9].

Для примера на рис. 3 представлен статистический портрет программной реализации алгоритма блочного симметричного шифрования FIPS 197 в режиме счетчика.

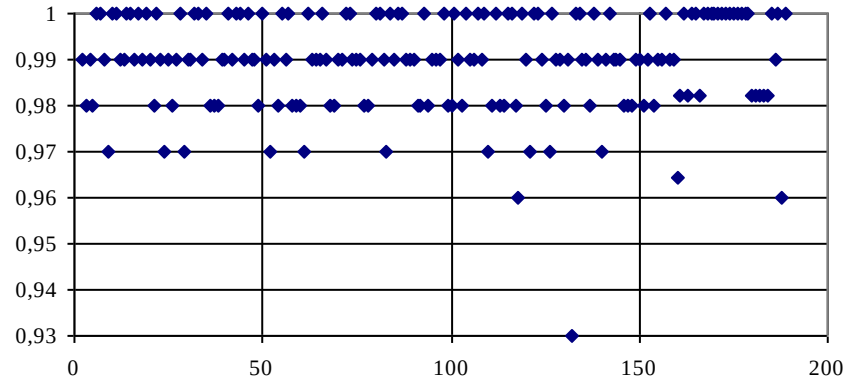

Рис. 2. Статистический портрет программной реализации теоретико-кодовых схем, построенных на кодах Рида-Соломона

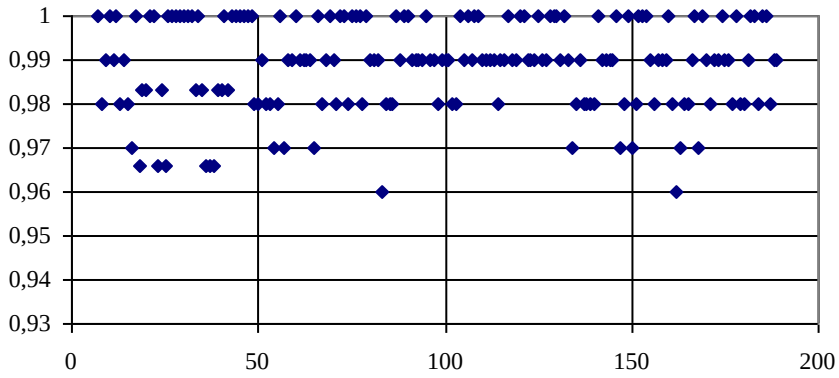

Рис. 3. Статистический портрет программной реализации FIPS 197

В табл. 2 сведены окончательные результаты тестирования программной реализации несимметричных теоретико-кодовых схем, построенных по эллиптическим кодам, кодам Рида-Соломона, тестовой последовательности генератора псевдослучайных чисел BBS и программной реализации алгоритма блочного симметричного шифрования FIPS 197 в режиме счетчика. Как видно из представленных данных в табл. 2, генераторы на теоретико-кодовых схемах обладают хорошими статистическими свойствами. Действительно, по результатам исследования статистической безопасности видно, что кодовые схемы защиты информации обеспечивают прохождение тестов с большей вероятностью, чем тестовый генератор псевдослучайных чисел BBS и алгоритм блочного симметричного шифрования FIPS 197.

Таблица 2

Генератор	Количество тестов, в которых тестирование прошло больше 99% последовательностей	Количество тестов, в которых тестирование прошло больше 96% последовательностей
BBS	134 (71%)	189 (100%)
FIPS 197	126 (67%)	189 (100%)
Теоретико-кодовые схемы на эллиптических кодах	141 (74%)	189 (100%)
Теоретико-кодовые схемы на кодах Рида-Соломона	132 (69%)	188 (99%)

Выводы. Проведены экспериментальные исследования статистической безопасности кодовых схем, построенных с использованием теоретико-кодовых схем на эллиптических кодах. При этом все 189 статистических тестов (согласно методике тестирования NIST SP 800-22) несимметричные теоретико-кодовые схемы, построенные по эллиптическим кривым, успешно прошли с критерием $P_i > 0{,}96015$. Кроме того 74% тестов успешно прошли по критерию $P_i > 0{,}99$, что является лучшим результатом, по сравнению с генератором BBS и алгоритмом блочного шифрования FIPS 197.

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.** *Niederreiter H.* Knapsack-Type Cryptosystems and Algebraic Coding Theory // Probl. Control and Inform. Theoty. – 1986. – V.15. – P. 19–34. **3.** *Сидельников В.М.* Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22 с. **4.** *Сидельников В.М., Шестаков С.О.* О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона // Дискретная математика. – 1992. – Т. 4. – № 3. – С. 57–63. **5.** *Кузнецов А.А., Лысенко В.Н., Евсеев С.П.* Исследование свойств несимметричных теоретико-кодовых схем с эллиптическими кодами // Системи обробки інформації. – Харків: ХВУ. – 2004. – Вип. 9 (37). – С. 79-84. **6.** *Кузнецов А.А., Евсеев С.П.* Несимметричные криптосистемы на основе теоретико-кодовых схем на эллиптических кодах // IV науково-технічна конференція молодих вчених Харківського військового університету 16–17 квітня 2004. – Харків: ХВУ. – 2004. – С. 64. **7.** *Шеннон К.* Теория связи в секретных системах / *Шеннон К.* Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – С. 333–402. **8.** *Методика* статистического тестирования NIST STS и математические доказательства тестов. – Харків: Інститут информационных технологий, 2004. – 62 с. **9.** *Кузнецов А.А., Евсеев С.П., Грабчак В.И.* Дослідження статистичної безпеки кодових схем захисту інформації, що будуються на кодах Ріда-Соломона // Збірник наукових праць ХУПС. – Харків: ХУПС. – 2005. – Вип. 5. – С. 84–86.

Поступила в редакцию 14.10.2005.