УДК 621.391.7:512.772

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ КОДОВЫХ СТРУКТУР КРИВОЙ ЭРМИТА НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

В.В. ПАНЬКОВА, С.Б. САЛОМАТИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 16 октября 2013

Построение систем защиты информации на базе алгебро-геометрических кодов возможно с применением различных алгебраических структур, обладающих криптографической стойкостью. Приведены результаты исследования свойства кодовых последовательностей, построенных на кривой Эрмита в поле *GF*(16), проведено тестирование на предмет требований, предъявляемых к криптографическим преобразованиям. Криптографический анализ выполнен с использованием спектральных преобразований. Оцениваются такие показатели качества шифрованных последовательностей, как нелинейность, сбалансированность, линейная сложность.

Ключевые слова: алгебро-геометрический код, кривая Эрмита, криптографический анализ, нелинейность, сбалансированность, линейная сложность.

Введение

Безопасность информационных систем предполагает комплекс мероприятий по защите информации от несанкционированного доступа. В [1, 2] рассмотрены преимущества криптографической защиты, использующей в качестве помехоустойчивых кодов алгебро-геометрические. Первоначально конструкции кодов, основанных на методах алгебраической геометрии, были предложены В. Д. Гоппой. В дальнейшем найдены и другие способы алгебро-геометрического кодирования, позволяющие строить с помощью специальных кривых длинные недвоичные блоковые коды, обладающие асимптотически хорошими параметрами [3, 4]. Кодовые структуры, используемые как компоненты систем защиты информации, должны обладать стойкостью к вскрытию, а значит, удовлетворять требованиям, предъявляемым к криптографическим алгоритмам. Оценка свойств шифрующей последовательности позволяет выявить возможный дисбаланс в способе ее формирования и оценить приемлемость с точки зрения устойчивости к криптоанализу. Методы анализа криптографических систем с использованием теории дискретных функций рассмотрены в [5]. Построение систем защиты информации на базе алгебро-геометрических кодов возможно с применением различных алгебраических структур, обладающих криптографической стойкостью. В статье исследуются свойства кодовых последовательностей, построенных на кривой Эрмита, проводится их тестирование на предмет требований, предъявляемых к криптографическим преобразованиям.

Моделирование кодовых структур кривой Эрмита

Алгебро-геометрические коды определяются алгебраическими кривыми над конечными полями. Кривой на аффинной плоскости $\chi_f(F)$, заданной многочленом $f(x,y)=0$ с коэффициентами из поля F, называют множество точек аффинного пространства $(x,y)\in A^2(F)$, включая точки на бесконечности. Кривая Эрмита задается уравнением $x^{r+1}-y^r-y=0$ над конечным полем $GF(q)$, где r –степень простого числа и $q=r^2$. Эта

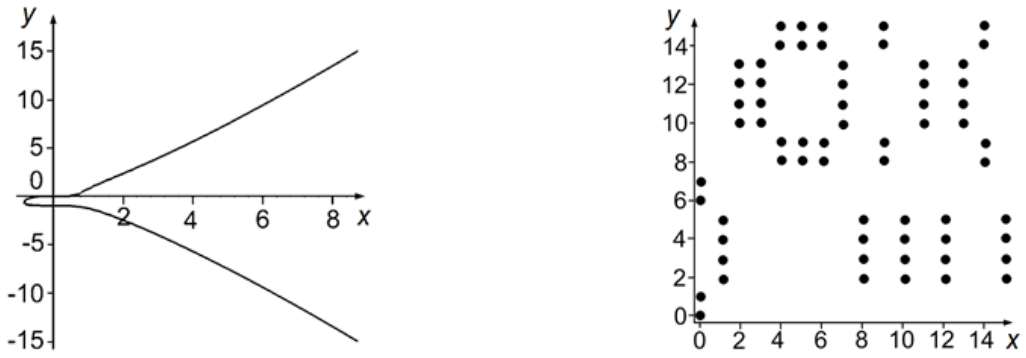
кривая является регулярной и содержит $N = r^3$ рациональных точек. Геном g регулярной кривой, заданной многочленом степени m, можно определить как $g = (m-1)\cdot(m-2)/2$.

Пусть $P_1, P_2, ..., P_n$ – рациональные точки кривой Эрмита, j – натуральное число, для которого $m-2 \le j \le \left\lfloor \frac{n-1}{m} \right\rfloor$, $\varphi_0(x,y), \varphi_1(x,y), ..., \varphi_\mu(x,y)$ –одночлены $x^a y^b$, упорядоченные относительно порядка общей степени $(\le_T)$, где $(1,0) <_T (0,1)$, так что $(a,b) \le_T (0,j)$. Все расчеты проводятся по модулю многочлена, задающего кривую, так что все многочлены могут быть представлены базисом, заданным множеством одночленов $\Phi = \{x^a y^b \mid 0 \le a \le q, 0 \le b\}$. В соответствии с [6], код $C^*(j)$, заданный матрицей

$$\begin{pmatrix} \varphi_0(P_1) & \dots & \varphi_0(P_n) \\ \varphi_1(P_1) & \dots & \varphi_1(P_n) \\ \dots & \dots & \dots \\ \varphi_\mu(P_1) & \dots & \varphi_\mu(P_n) \end{pmatrix},$$

имеет параметры $k = n - (mj - g + 1)$ и $d_{\min} \ge d^* = mj - 2g + 2$, где d^* – конструктивное расстояние кода. Уникальность генераторной матрицы кода определена набором точек $P_1, P_2, ..., P_n$, в которых вычисляются значения генераторных функций (одночленов $x^a y^b$), смена которых, при заданных конструктивных характеристиках кода (n,k,d), приводит к изменению структуры кодового слова.

Исследуемые конструкции алгебро-геометрического кода образованы кривой Эрмита, которая задается уравнением $f = y^4 + y - x^5$ и в поле $GF(16)$ содержит 64 рациональные точки. Кривая Эрмита и ее точки представлены на рис. 1.



а *б*

Рис. 1. Кривая Эрмита в поле $GF(16)$ (*а*) и ее точки (*б*)

Исследуются кодовые конструкции $C^*(j)$, заданные базисом генераторных функций $x^a y^b$:

1) $C^*(10)$, $(64,19,40)$, $a+b \le 6$;

2) $C^*(10)$, $(64,19,40)$, $a+b \le 10$;

3) $C^*(7)$, $(64,30,25)$, $a+b \le 10$;

4) $C^*(5)$, $(64,44,15)$, $a+b \le 10$;

5) $C^*(5)$, $(64,44,15)$, $a+b \le 14$.

Анализ криптографических свойств кодовых структур проводится на основе выборки из $i = 100$ сформированных случайным образом шифропоследовательностей каждой кодовой конструкции, полученных как произведение информационного вектора-строки на порождающую матрицу.

Исследование свойств кодированных последовательностей кривой Эрмита

Одним из основных критериев, предъявляемых к разработке и исследованию эффективности криптографических алгоритмов, является такой показатель, как нелинейность преобразований. В качестве основного аппарата анализа и изучения особенностей критериев используется спектральное преобразование Уолша БФ (булевой функции) $W_f(\omega) = \sum_{x \in GF(2)^t} f(x) \cdot (-1)^{\langle x,\omega \rangle}$, где $f(x)$ – БФ двоичных переменных; $x = (x_1, x_2, ..., x_t)$, $\omega = (\omega_1, \omega_2, ..., \omega_t)$ – наборы длиной t над полем $GF(2)$; $\langle x, \omega \rangle = \sum_{i=1}^{t} x_i \omega_i$ – скалярное произведение наборов.

Спектральное преобразование Уолша СФ (сопряженной функции) $\breve{f}(x)$: $W_{\breve{f}}(\omega) = \sum_{x \in GF(2)^t} (-1)^{f(x)+\langle x,\omega \rangle}$.

Нелинейность БФ, реализующих некоторое преобразование, показывает степень удаленности БФ от множества аффинных или линейных БФ. В терминах спектрального преобразования значение нелинейности оценивается как

$$N_f = 2^{t-1} - \frac{1}{2} \max_{\omega \in GF(2^t)} \left| W_{\breve{f}}(\omega) \right|. \quad (1)$$

Для оценки нелинейности БФ следует определить максимальное значение компонент спектра Уолша-Адамара [5]. Верхняя граница значения нелинейности определяется выражением

$$N_f \le \left\lfloor 2^{t-1} - 2^{t/2-1} \right\rfloor. \quad (2)$$

Спектральные преобразования позволяют оценить сбалансированность криптографической функции. Для противодействия прямым статистическим атакам на криптоалгоритмы необходимо, чтобы все компоненты БФ, реализующие преобразование, были сбалансированы, а преобразование в целом носило регулярный характер. Количество единиц в таблице истинности сбалансированной БФ равно количеству нулей [5]. В терминах преобразования Уолша-Адамара сбалансированность эквивалентна выполнению условий $W_{\breve{f}}(\omega) = 0$, $W_f(\omega) = 2^{t-1}$, где $\omega = (0,...,0)$. Степень отклонения БФ от сбалансированности определяет значение спектра Уолша-Адамара в точке "0" [5].

Исследование таких критериев как уровень нелинейности и сбалансированность основано на формировании спектра Уолша-Адамара для каждой кодированной последовательности (рис. 2.).

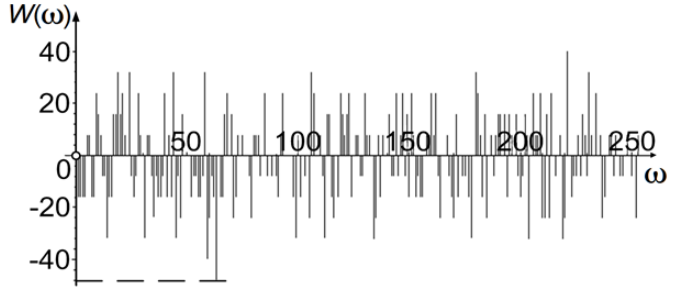


Рис. 2. Спектр Уолша-Адамара кодированной последовательности

Оценка уровня нелинейности использует максимальное значение компонент спектра (рис. 3.), полученных для всех последовательностей каждого исследуемого кода. В соответствии с формулой (1) лучшие показатели уровня нелинейности имеют вектора с меньшим значением максимальной компоненты спектра. Все шифропоследовательности отличает высокий уровень нелинейности (92…110) при верхней границе равной 120, согласно (2). Основная часть кодированных последовательностей расположена в диапазоне от 102 до 108. В табл. 1 приведены полученные при моделировании данные о величине максимальных компонент и соответствующем уровне нелинейности основной части шифропоследовательностей.

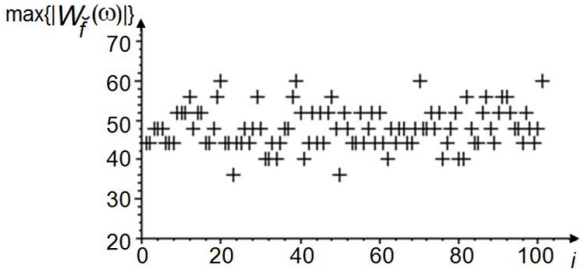


Рис. 3. Значения максимальных компонент спектра Уолша-Адамара кода $C^*(7)$

Таблица 1. **Показатели уровня нелинейности шифрованных последовательностей**

N_f	$\max\{\lvert W_{\bar{f}}(\omega)\rvert\}$	Количество шифропоследовательностей кода,%				
		$C^*(10)$ (64,19,40) $a+b\le 6$	$C^*(10)$ (64,19,40) $a+b\le 10$	$C^*(7)$ (64,30,25) $a+b\le 10$	$C^*(5)$ (64,44,15) $a+b\le 10$	$C^*(5)$ (64,44,15) $a+b\le 14$
108	40	6	6	9	8	11
106	44	22	21	31	25	26
104	48	29	33	27	28	30
102	52	23	24	20	17	19

Уровень нелинейности кодированных последовательностей выше, если конструктивно они образованы кодами с большей скоростью и генераторными функциями более высоких степеней. Каждый код в своем составе имеет вектора с уровнем нелинейности ниже среднего, т.е. последовательности с диапазоном нелинейности от 100 до 92. При использовании кодов в криптосистемах, в зависимости от конкретных задач, вектора, не удовлетворяющие требованиям к уровню нелинейности, могут отбраковываться как слабые. В целом отмечен высокий уровень нелинейности, что характеризует высокую степень удаленности последовательностей от линейных, а значит, высокую степень устойчивости к линейному криптоанализу при их использовании в криптосистемах.

Оценка сбалансированности использует значение нулевой компоненты спектра. Нулевая компонента сбалансированной шифропоследовательности равна «0», любое другое значение определяет степень отклонения функции от сбалансированности (рис. 4.).

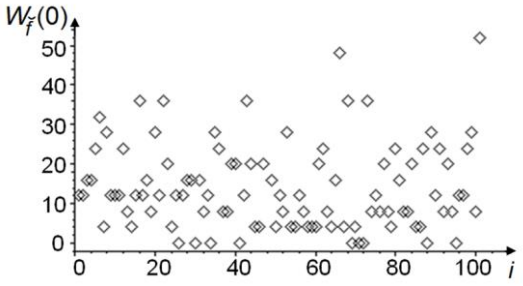


Рис. 4. Значения нулевых компонент спектра Уолша-Адамара кода $C^*(7)$

Полученные при моделировании данные о нулевых компонентах исследуемых кодовых структур занесены в табл. 2.

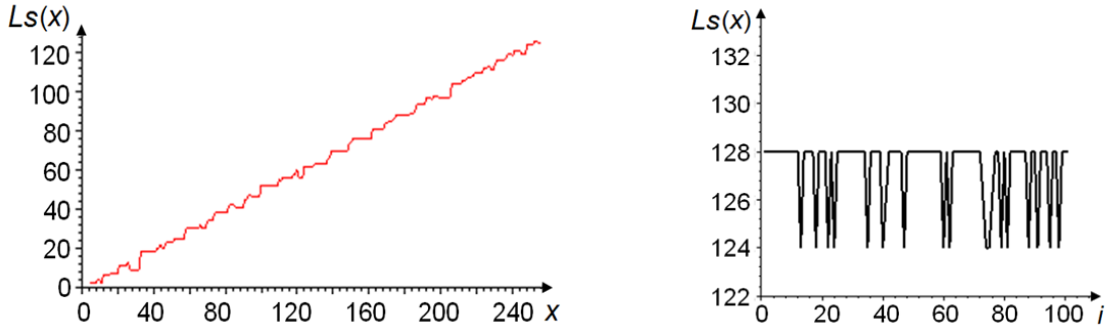
Таблица 2. **Показатели сбалансированности шифрованных последовательностей**

Количество кодовых слов с нулевой компонентой спектра $W_{\bar{f}}(0)=0$	Исследуемые кодовые структуры				
	$C^*(10)$ (64,19,40) $a+b\le 6$	$C^*(10)$ (64,19,40) $a+b\le 10$	$C^*(7)$ (64,30,25) $a+b\le 10$	$C^*(5)$ (64,44,15) $a+b\le 10$	$C^*(5)$ (64,44,15) $a+b\le 14$
%	8	8	9	8	7

Из 100 кодовых структур каждого исследуемого кода только для 7–9 % выполнено свойство сбалансированности, т.е. менее десятой части векторов имеет нулевую компоненту

спектра равную «0». Можно заключить, что в общем случае свойство сбалансированности не выполнено, а это означает слабость в противодействии прямым статистическим атакам на криптографические преобразования, если не выполнено добалансирование векторов.

Линейную сложность шифрующей последовательности можно оценить с помощью алгоритма Берлекемпа-Месси (БМ). Под линейной сложностью последовательности понимают длину самого короткого регистра сдвига с линейной обратной связью (РСЛОС), способного породить эту последовательность. Любая последовательность, сформированная конечным аппаратом над конечным полем, имеет конечную линейную сложность. С помощью алгоритма БМ можно воссоздать РСЛОС. Алгоритм БМ позволяет вычислить профиль линейной сложности, который определяет линейную сложность $Ls(x)$ последовательности по мере ее удлинения. Используя значения ее уровней для 100 векторов каждого исследуемого кода, можем оценить линейную сложность криптопоследовательностей (рис. 5.).



а *б*

Рис. 5. Профиль линейной сложности кодированной последовательности (*а*) и уровень линейной сложности кода $C^*(7)$ (*б*)

Графики профилей исследуемых кодовых структур носят линейную зависимость, а линейная сложность меняется в пределах 120…132 со средним значением уровня равным 128. Результаты моделирования сведены в табл. 3.

Таблица 3. **Линейная сложность шифрованных последовательностей**

Значения уровней линейной сложности $Ls(x)$	Исследуемые кодовые структуры				
	$C^*(10)$ (64,19,40) $a+b\le 6$	$C^*(10)$ (64,19,40) $a+b\le 10$	$C^*(7)$ (64,30,25) $a+b\le 10$	$C^*(5)$ (64,44,15) $a+b\le 10$	$C^*(5)$ (64,44,15) $a+b\le 14$
	124–132	124–132	124–128	120–128	124–132

Каждая бинарная последовательность имеет высокую степень линейной сложности и может быть сформирована с помощью РСЛОС с полиномом обратной связи степени не меньше 120. На рис. 6 приведен усредненный профиль линейной сложности последовательности АГ-кода, который, как видно, совпадает с последовательностью *BBS* [5], тестовой для *NIST*.

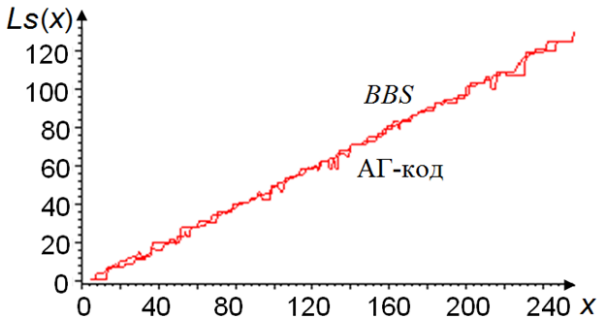


Рис. 6. Усредненный профиль линейной сложности АГ-кода и *BBS*

Высокая степень линейной сложности означает, что криптосистемы, использующие подобные шифропоследовательности, устойчивы к вскрытию, и криптоаналитик не может предсказать ни следующий, ни предыдущий бит последовательности.

Заключение

Криптографический анализ исследуемых кодовых структур кривой Эрмита в поле *GF*(16) выполнен с использованием спектральных преобразований. Оценены такие показатели качества шифрованных последовательностей, как нелинейность, сбалансированность, линейная сложность. Высокий уровень нелинейности предполагает высокую степень устойчивости к линейному криптоанализу и приемлемость применения подобных структур в криптоситемах. В общем случае свойство сбалансированности остается не выполненным, а значит, возможность противодействия прямым статистическим атакам требует добалансировки криптографических преобразований. Высокая степень линейной сложности и близость к криптографическим стандартам *BBS* и *AES* означает устойчивость к вскрытию и возможность применения таких криптографических алгоритмов в системах защиты информации.

CRYPTOGRAPHIC ANALYSIS OF THE CODE STRUCTURES OF HERMITE CURVE FOR COMPLIANCE WITH THE REQUIREMENTS OF INFORMATION SECURITY SYSTEMS

V.V. PANKOVA, S.B. SALOMATIN

Abstract

Building security systems based on the algebraic-geometric codes is possible with the use of various algebraic structures with cryptographic security. This paper investigates the properties of the code sequences, built on the Hermite curve in the field GF(16), their testing on the subject of the requirements for cryptographic transformations was conducted. Cryptographic analysis is performed using spectral transformations. Encrypted sequences quality metrics such as nonlinearity, balance, linear complexity are evaluated.

Список литературы

1. *Грабчак В.И., Мельник А.П.* // Вісник СумДУ. Сер. технічні навукі. 2009. № 4. С. 94–100.
2. *Онанченко Е.Л.* // Системи обробки інформації. 2007. № 7. С. 53–58.
3. *Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А.* Алгебро-геометрические коды. Основные понятия. М., 2003.
4. *Niebuhr R.* Application of algebraic-geometric codes in cryptography. Darmstadt, 2006.
5. *Саломатин С.Б.* Поточные криптосистемы. Минск, 2006.
6. *Justesen J., Larsen K., Havemose A. e.t al* // *IEEE Transactions Information Theory.* July 1989. P. 811–821.