Крипто-кодовая система на модифицированных эллиптических кодах

Евсеев С.П.[1], Белодед И.В.[2]

[1]Доцент кафедри інформаційних систем, кандидат технічних наук, Харьковский национальный экономический университет им. С. Кузнеца, пр. Ленина, 9а, Харьков, Украина, Serhii.yevseiev@hneu.net
[2]Харьковский национальный экономический университет им. С. Кузнеца, пр. Ленина, 9а, Харьков, Украина, bilodid.vanya@gmail.com

Аннотация **- Рассматриваются криптосистемы с использованием алгебраических кодов. Предложены симметричные теоретико-кодовые схемы на модифицированных эллиптических кодах, получены аналитические выражения, связывающие параметры модифицированных эллиптических кодов и симметричных криптосхем на их основе.**

Ключевые слова: модифицированные эллиптические коды, криптостойкость, криптокодовые системы .

Crypto-code system on a modified elliptic codes

Yevseiev S.P.[1], Bilodid I.V.[2]

[1]assistant professor, Ph.D., Simon Kuznets Kharkiv National University of Economics, ave. Lenina, 9a, Kharkiv, Ukraine, Serhii.yevseiev@hneu.net
[2]Simon Kuznets Kharkiv National University of Economics, ave. Lenina, 9a, Kharkiv, Ukraine, bilodid.vanya@gmail.com

Abstract **- We consider the cryptosystem using the algebraic code. Proposed symmetrical theoretical coding scheme on the modified elliptic codes, analytical expressions relating the parameters of the modified elliptical codes and symmetrical cryptoschemes based on them.**

Keywords: modified elliptical codes, cryptostrength, cryptocode systems

ВВЕДЕНИЕ

Перспективным направлением в развитии криптографических методов обработки информации является разработка и исследование теоретико-кодовых схем с использованием алгебраических кодов [1-7]. Известные симметричные схемы Рао-Нама обладают существенным недостатком – большим объемом ключевых данных [1]. Предложенная в [3] модификация криптосхемы Рао-Нама позволяет снизить объем ключа, но криптостойкость такой схемы считается недостаточной [4-5]. Актуальной научно-технической задачей является разработка и исследование симметричных теоретико-кодовых схем с небольшим объемом ключа и обеспечивающих высокие показатели криптостойкости.

СИММЕТРИЧНЫЕ ТЕОРЕТИКО-КОДОВЫЕ СХЕМЫ РАО-НАМА И ИХ МОДИФИКАЦИИ.

Первым успешным результатом в разработке симметричных теоретико-кодовых схем является криптосистема Рао-Нама [1]. Основная идея, заложенная в эту конструкцию, состоит в использовании порождающей матрицы G алгебраического блокового (n, k, d) кода, замаскированного матицей X под случайный код:

$GX = G \cdot X$.

Криптограммой является вектор c* длины n, вычисляемый по правилу:

$$c^* = I * GX + e. \quad (1)$$

Т.е. криптограмма формируется кодированием информационной последовательности I длиной k информационных символов в кодовое слово длиной n кодовых символов и добавлении к нему случайного вектора ошибки e. Вес вектора e удовлетворяет ограничению $w(e) \square t$, где t – число ошибок, которое может исправить (n, k, d) блоковый код, $d = 2 * t + 1$.

На приемной стороне уполномоченный пользователь (знающий секретный ключ) дешифрует полученную криптограмму – декодирует кодовое слово с ошибками (n, k, d) алгебраического блокового кода. Задача декодирования алгебраического блокового кода (например, кода БЧХ, Рида-Соломона, и др.) – полиномиально разрешимая задача. Декодирование произвольного линейного кода (кода общего положения) является весьма сложной вычислительной задачей, сложность ее решения растет экспоненциально. Это положение лежит в основе симметричных криптосистем по схеме Рао-Нама: код с быстрым алгоритмом декодирования (полиномиальной сложности) маскируется под произвольный (случайный) линейный код, декодирование которого представляется как вычислительно сложная задача. Для уполномоченного пользователя криптосистемы (имеющего секретный ключ) декодирование - полиномиально разрешимая задача.

Проведем оценку параметров симметричной теоретико-кодовой схемы, построенной с использованием алгебраических (n, k, d) блоковых кодов над GF(2m): размерность секретного ключа (в битах); размерность информационного вектора (в битах) ll = k · m; размерность криптограммы (в битах) ; относительная скорость передачи.

Основным недостатком схемы Рао-Нама является большой объем ключа. Действительно, для хранения секретной порождающей матрицы (n, k, d) блочного кода над GF(q) необходимо хранить, в общем случае, n × k q-ичных символов.

Модифицированная симметричная теоретико-кодовая схема Рао-Нама, построенная с использованием альтернантных кодов, заданных через многочлен Гоппы впервые предложена в работе [2]. Основная идея состоит в построении схемы Рао-Нама на (n, k, d) кодах Гоппы, заданных с помощью многочлена Гоппы степени t, d = 2 * t + 1. При этом если (n, k, d) код Гоппы над GF(q) позволяет исправить t ошибок, то все кодовые слова могут быть однозначно заданы многочленом Гоппы степени t над GF(q). Следовательно, если вместо порождающей матрицы кода в качестве секретного ключа использовать многочлен Гоппы, то удается существенно сократить его объем. В общем случае, для однозначного определения многочлена Гоппы необходимо хранить t +1 q-ичных символов. Однако, как показано в работах [3-4] криптосхему с обобщенными кодами Рида-Соломона можно взломать алгоритмом полиномиальной сложности. Альтернантные коды строятся с использованием проверочной матрицы обобщенных кодов Рида-Соломона и, следовательно, криптосистемы на их основе так же потенциально уязвимы.

СИММЕТРИЧНЫЕ ТЕОРЕТИКО-КОДОВЫЕ СХЕМЫ С ИСПОЛЬЗОВАНИЕМ МОДИФИЦИРОВАННЫХ ЭЛЛИПТИЧЕСКИХ КОДОВ.

Известные методы модификации линейных блоковых кодов наиболее полно рассмотрены в [7-10]. На рис.1. представлены наиболее распространенные методы модификации.

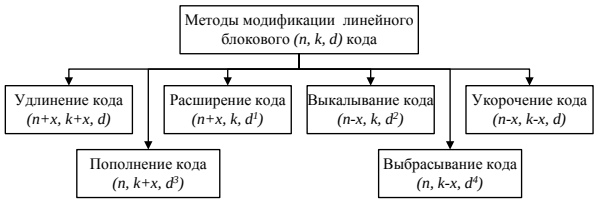

Рис. 1. Методы модификации линейных блоковых кодов

Наиболее простой и удобный метод модификации линейного блокового кода, не уменьшающий минимальное кодовое расстояние, состоит в укорочении его длины путем сокращения информационных символов. Пусть $I = (I_1, I_2, \ldots, I_k)$ – информационный вектор *(n, k, d)* блокового кода. Выберем подмножество h информационных символов, $|h| = x$, $x < k$. Поместим в информационный вектор I в подмножество h нули, т.е. $I_i = 0$, $\forall I_i \in h$. На остальных позициях вектора I поместим информационные символы. При кодировании информационного вектора символы множества h не участвуют (они нулевые) и их можно отбросить, а полученное кодовое слово будет короче на x кодовых символов. Для модификации (укорочения) эллиптических кодов будем использовать уменьшение набора точек кривой. Справедливо следующее утверждение.

Утверждение 4 [11-13]. Пусть *EC* – эллиптическая кривая в над *GF(q)*, $g = g(EC)$ - род кривой, *EC(GF(q))* - множество ее точек над конечным полем, $N = EC(GF(q))$ - их число. Пусть X и h – непересекающиеся подмножества точек, $X \cup h = EC(GF(q))$, $|h| = x$. Тогда *укороченный* эллиптический *(n, k, d)* код над *GF(q)*, построенный через отображение вида $\varphi: X \to P^{k-1}$, связан характеристиками $k + d \geq n$, причем:

$$n = 2\sqrt{q} + q + 1 - x,$$
$$k \geq \alpha - x, \qquad (2)$$
$$d \geq n - \alpha,\ \alpha = 3 \cdot degF.$$

Доказательство. Действительно, используя результаты утверждения 1 построим эллиптический код с параметрами: $n \leq 2\sqrt{q} + q + 1$, $k \geq \alpha - x$, $d \geq n - \alpha$, $\alpha = 3 \cdot degF$. Условие $n \leq 2\sqrt{q} + q + 1$ учитывает возможность построения эллиптических кодов на подмножестве точек кривой. Если это подмножество X, то получим равенство $n = 2\sqrt{q} + q + 1 - x$, а параметры эллиптического кода запишутся в виде (2).

Следствие 1. Зафиксируем подмножество $h_1 \subseteq h$, $|h_1| = x_1$. Пусть задан эллиптический *(n, k, d)* код над *GF(q)*, построенный через отображение вида $\varphi: X \to P^{k-1}$. Тогда параметры *удлиненного* на x_1 символов из *GF(q)* эллиптического кода, построенного через отображение вида $\varphi: (X \cup h_1) \to P^{k-1}$, будут связаны соотношениями: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \cdot degF$.

Доказательство. Если $x_1 < x$, то удлинение кода на x_1 эквивалентно укорочению исходного кода (утверждение 3) на $x - x_1$. Подставив эти параметры в выражение (2), получим результат следствия 1.

Следствие 2. Если известен вид эллиптической кривой (набор $a_1 \ldots a_6$, $\forall a_i \in GF(q)$), то подмножества h и h_1 полностью определяют модифицированные эллиптические *(n, k, d)* коды над *GF(q)*, построенные через отображения вида: $\varphi: X \to P^{k-1}$ и $\varphi: (X \cup h_1) \to P^{k-1}$.

Доказательство. Набор коэффициентов $a_1 \ldots a_6$, $\forall a_i \in GF(q)$ однозначно задает вид эллиптической кривой и, соответственно, набор ее точек *EC(GF(q))*. Используя отображение вида $\varphi: EC \to P^M$ и результаты утверждений 1-2 (см. раздел 2), построим эллиптический *(n, k, d)* код над *GF(q)*. Если известны символы укорочения

(удлинения), то построим укороченные (удлиненные) коды. По утверждению 5, это символы множеств h и h_1, которые полностью определяют модифицированный эллиптический (n, k, d) код над $GF(q)$.

Утверждение 5 [11-13]. *Укороченный* эллиптический (n, k, d) код над $GF(q)$, построенный через отображение вида $\varphi: X \to P^{r-1}$, связан характеристиками $k + d \geq n$, причем:

$$n = 2\sqrt{q} + q + 1 - x,$$
$$k \geq n - \alpha, \qquad (3)$$
$$d \geq \alpha,\ \alpha = 3 \cdot degF.$$

Доказательство. Используя результаты утверждения 2, построим эллиптический код с параметрами: $n \leq 2\sqrt{q} + q + 1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot degF$. Условие $n \leq 2\sqrt{q} + q + 1$ учитывает возможность построения эллиптических кодов на подмножестве точек кривой. Если это подмножество X, то получим равенство $n = 2\sqrt{q} + q + 1 - x$, а параметры эллиптического кода запишутся в виде (3).

Следствие 1. Зафиксируем подмножество $h_1 \subseteq h$, $|h_1| = x_1$. Пусть задан эллиптический (n, k, d) код над $GF(q)$, построенный через отображение вида $\varphi: X \to P^{r-1}$. Тогда параметры *удлиненного* на x_1 символов из $GF(q)$ эллиптического кода, построенного через отображение вида $\varphi: (X \cup h_1) \to P^{r-1}$, будут связаны соотношениями: $n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \cdot degF$.

Доказательство. Если $x_1 < x$, то удлинение кода на x_1 эквивалентно укорочению исходного кода (утверждение 4) на $x - x_1$. Подставив эти параметры в выражение (3) получим результат следствия 1.

Следствие 2. Если известен вид эллиптической кривой (набор $a_1 \ldots a_6$, $\forall a_i \in GF(q)$), то подмножества h и h_1 полностью определяют модифицированные эллиптические (n, k, d) коды над $GF(q)$, построенные через отображения вида: $\varphi: X \to P^{r-1}$ и $\varphi: (X \cup h_1) \to P^{r-1}$.

Доказательство. Набор коэффициентов $a_1 \ldots a_6$, $\forall a_i \in GF(q)$ однозначно задает вид эллиптической кривой и, соответственно, набор ее точек $EC(GF(q))$. Используя отображение вида $\varphi: EC \to P^M$ и результаты утверждений 1-2, построим эллиптический (n, k, d) код над $GF(q)$. Если известны символы укорочения (удлинения), то построим укороченные (удлиненные) коды. По утверждению 5, это символы множеств h и h_1, которые полностью определяют модифицированный эллиптический (n, k, d) код над $GF(q)$.

Результаты утверждений 4-5 и их следствия позволяют построить модифицированные (укороченные и удлиненные в пределах $n \leq 2\sqrt{q} + q + 1$) эллиптические (n, k, d) коды над $GF(q)$. Зададим следующий алгоритм построения модифицированных эллиптических кодов.

Используя результат утверждения 4 и его следствия, зададим симметричную теоретико-кодовую схему на модифицированных эллиптических кодах, построенных через отображения вида $\varphi: X \to P^{k-1}$ и $\varphi: (X \cup h_1) \to P^{k-1}$. Справедливо следующее утверждение.

Утверждение 6 [11-13]. Укороченный эллиптический (n, k, d) код над $GF(2^m)$, построенный через отображения вида $\varphi: X \to P^{k-1}$, определяет симметричную теоретико-кодовую схему с параметрами:

$$l_{K+} = x \cdot \left| log_2\left(2\sqrt{q} + q + 1\right) \right|; \qquad (4)$$
$$l_I = (\alpha - x) \cdot m; \qquad (5)$$
$$l_S = \left(2\sqrt{q} + q + 1 - x\right) \cdot m; \qquad (6)$$
$$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x\right). \qquad (7)$$

Удлиненный эллиптический (n, k, d) код над $GF(2^m)$, построенный через отображения вида $\varphi: (X \cup h_1) \to P^{k-1}$, определяет симметричную теоретико-кодовую схему с параметрами:

$$l_{K+} = (x - x_1) \cdot \left\lceil log_2\left(2\sqrt{q} + q + 1\right) \right\rceil; \qquad (8)$$
$$l_I = (\alpha - x + x_1) \cdot m; \qquad (9)$$
$$l_S = \left(2\sqrt{q} + q + 1 - x + x_1\right) \cdot m; \qquad (10)$$
$$R = (\alpha - x + x_1) / \left(2\sqrt{q} + q + 1 - x + x_1\right). \qquad (11)$$

Доказательство. Согласно результату утверждения 1, симметричная теоретико-кодовая схема, построенная с использованием порождающей матрицы алгебраического блокового (n, k, d) кода над $GF(2^m)$, обладает параметрами: размер секретного ключа $k \times n$ символов из $GF(2^m)$; информационный вектор длины k символов из $GF(2^m)$; длина криптограммы - n символов из $GF(2^m)$; относительная скорость передачи - $R = k / n$. Пронумеруем все точки кривой. Всего их $N \leq 2\sqrt{q} + q + 1$. Следовательно, для нумерации точек кривой необходимо $\left| log_2\left(2\sqrt{q} + q + 1\right) \right|$ бит. Если мощность подмножества символов укорочения $|h| = x$, то для обозначения всех символов укорочения потребуется $x \cdot \left| log_2\left(2\sqrt{q} + q + 1\right) \right|$ бит. Эти символы хранятся в секрете и задают объем ключевых данных – выражение (4). Если мощность подмножества символов удлинения $|h_1| = x_1$, то для обозначения всех символов модификации потребуется $(x - x_1) \cdot \left\lceil log_2\left(2\sqrt{q} + q + 1\right) \right\rceil$ бит. Эти символы хранятся в секрете и задают объем ключевых данных – выражение (8) .

Подставим параметры модифицированных (укороченных и удлиненных) эллиптических (n, k, d) кодов над $GF(q)$, построенных через отображения вида $\varphi: X \to P^{k-1}$ и $\varphi: (X \cup h_1) \to P^{k-1}$ (см. утверждение 4) получим, соответственно, выражения (4-7) и (8-11).

Используя результат утверждения 5 и его следствия, зададим симметричную теоретико-

кодовую схему на модифицированных эллиптических кодах, построенных через отображения вида $\varphi: X \to P^{r-1}$ и $\varphi: (X \cup h_1) \to P^{r-1}$. Справедливо следующее утверждение.

Утверждение 7 [11-13]. Укороченный эллиптический *(n, k, d)* код над $GF(2^m)$, построенный через отображения вида $\varphi: X \to P^{r-1}$, определяет симметричную теоретико-кодовую схему с параметрами:

- размерность секретного ключа определяется выражением (4);
- размерность информационного вектора (в битах):

$$l_1 = \left(2\sqrt{q} + q + 1 - \alpha\right) \cdot m; \qquad (12)$$

- размерность криптограммы определяется выражением (3.17);
- относительная скорость передачи:

$$R = \left(2\sqrt{q} + q + 1 - \alpha\right) / \left(2\sqrt{q} + q + 1 - x\right). \quad (13)$$

Удлиненный эллиптический *(n, k, d)* код над $GF(2^m)$, построенный через отображения вида $\varphi: (X \cup h_1) \to P^{r-1}$, определяет симметричную теоретико-кодовую схему с параметрами:

- размерность секретного ключа определяется выражением (8);
- размерность информационного вектора (в битах):

$$l_1 = \left(2\sqrt{q} + q + 1 - \alpha\right) \cdot m; \qquad (14)$$

- размерность криптограммы определяется выражением (10);
- относительная скорость передачи:

$$R = \left(2\sqrt{q} + q + 1 - \alpha\right) / \left(2\sqrt{q} + q + 1 - x + x_1\right). \quad (15)$$

Доказательство. Согласно результату утверждения 2, симметричная теоретико-кодовая схема, построенная с использованием проверочной матрицы алгебраического блокового *(n, k, d)* кода над $GF(2^m)$, обладает параметрами: информационный вектор длины *k* символов из $GF(2^m)$; длина криптограммы - *n* символов из $GF(2^m)$; относительная скорость передачи - $R = k / n$. Подставим параметры модифицированных (укороченных и удлиненных) эллиптических *(n, k, d)* кодов над *GF(q)*, построенных через отображения вида $\varphi: X \to P^{r-1}$ и $\varphi: (X \cup h_1) \to P^{r-1}$ (см. утверждение 5) получим, соответственно, выражения (12-13) и (14-15).

ВЫВОДЫ.

Результаты проведенных исследований позволяют задавать симметричные теоретико-кодовые схемы с использованием эллиптических кодов и их модификаций. Перспективным направлением является исследования криптостойкости предложенных теоретико-кодовых схем.

ЛИТЕРАТУРА REFERENCES

[1] T. R. N. Rao and K. H. Nam. Private-key algebraic-coded cryptosystem. Advances in Cryptology – CRYPTO 86, New York. – NY: Springer. – pp. 35-48.

[2] Халимов Г.З., Буханцов А.Д. Применение помехоустойчивого кодирования для обеспечения безопасности каналов передачи данных. // Труды международной НТК «Передача, обработка и отображение информации» / Под ред. А.В. Королева. Х.: НАНУ, ПАНИ. – 1994. – С.28.

[3] 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.

[4] Сидельников В.М. Криптография и теория кодирования. Материалы конференции «Московский университет и развитие криптографии в России», МГУ. – 2002. – 22с.

[5] Кузнецов А.А., Северинов А.В., Лысенко В.Н., Науменко И.В. Алгоритм помехоустойчивого кодирования с использованием кодов по кривым Эрмита // Системи обробки інформації. Збірник наукових праць. Вип. 6(28). – Харків: НАНУ, ПАНМ, ХВУ. - 2003. – С – 181-185.

[6] Кузнецов А.А., Евсеев С.П. Разработка теоретико-кодовых схем с использованием эллиптических кодов. // Системи обробки інформації. – Харків: ХВУ. –2004 – Вип. 5. – С. 127-132.

[7] Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.

[8] Коррекция ошибок в оптических накопителях информации // Типикин А.П., Петров В.В., Бабанин А.Г.; Отв. Ред. Додонов А.Г.; АН УССР. Ин-т проблем регистрации информации. – К.: Наукова думка, 1990. – 172 с.

[9] Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. – М.: Связь, 1979. – 744 с.

[10] Мутер В.М. Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат. Ленингр. отд-ние, 1990. – 288 с.

[11] Кузнецов А.А., Евсеев С.П., Лысенко В.Н., Житник В.Е. Симметричные теоретико-кодовые схемы на эллиптических кодах. // Східно-Європейський журнал передових технологій. – Харків: . – 2005. – Вип. 1 . – С. 37-43.

[12] Кузнецов А.А., Лысенко В.Н., Евсеев С.П. Симметричные криптосистемы с использованием эллиптических кодов. //Комп'ютерні системи та інформаційні технології. – Х.: ХАИ. – 2005. – Вип. 1 . – С. - 31-35.

[13] Кузнецов А.А., Лысенко В.Н., Евсеев С.П. Симметричные криптосистемы с использованием эллиптических кодов. //Материалы всеукраинской научно-технической конференции. – Х.: Н. – 2004. – С.70-71.