Математичні Моделі Модифікованої Несиметричної Крипто-Кодової Системи Мак-Еліса на Модифікованих Еліптичних Кодах

Євсеєв Сергій
Кафедра інформаційних систем
Харківський національний економічний університет ім. С. Кузнеця
Харків, Україна
Serhii.Yevseiev@hneu.net

Mathematical Models of the Modified Asymmetric Crypto-Code System of McElice on Modified Elliptic Codes

Serhii Yevseiev
Information Systems Department
Simon Kuznets Kharkiv National University of Economics
Kharkiv, Ukraine
Serhii.Yevseiev@hneu.net

***Анотація*—Математичні моделі модифікованих засобів захисту інформації розроблені на основі теоретико-кодової схеми Мак-Еліса з використанням алгеброгеометричних блокових кодів з укороченням і подовженням інформаційного простору**

***Abstract*—Mathematical models of modified crypto-code information protection tools are developed on the basis of the McElis theoretical-code scheme using algebraic geometric block codes with shortening and extension of the information premise**

Ключові слова— несиметрична крипто-кодова система, теоретико-кодові схеми, модифіковані коди з виправленням помилок

Keywords—asymmetric crypto-code system, theoretical-code system, modified error-correcting codes

I. Введення і аналіз літератури

Розвиток телекомунікаційних систем і технологій, бурхливе зростання обчислювальної техніки висувають нові вимоги до основних критеріїв якості обслуговування клієнтів (уповноважених користувачів). Основними показниками за результатами аналізу стандартів в цій галузі є забезпечення достовірності (надійності) передачі даних і забезпечення безпеки всього циклу обробки і зберігання даних [1, 2, 3]. Для забезпечення достовірності використовуються механізми перешкодостійкого кодування, а для забезпечення безпеки – криптографічні механізми на основі методів симетричної і несиметричної криптографії. Перспективним напрямком, на наш погляд, є використання несиметричних криптосистем на основі теоретико-кодових схем Мак-Еліса, що забезпечують інтегровано (одним механізмом) показники достовірності на рівні $2^9 – 2^{12}$ і криптостійкості – $2^{30} – 2^{35}$ групових операцій при її побудові над полем $GF(2^{10})$. Дана криптосистема отримала широке застосування з розвитком обчислювальних можливостей комунікаційних пристроїв і їх програмного забезпечення.

В роботі [4] автори пропонують використовувати криптосистему Мак-Еліса в програмному забезпеченні Sequitur, яка дозволяє інтегровано вирішувати завдання швидкодії і безпеки при передачі конфіденційної інформації. У роботах [5, 6, 7] криптосистему Мак-Еліса пропонують використовувати для забезпечення основних послуг безпеки: конфіденційності і цілісності в стегасистемі на основі звукових файлів MPEG Layer-III або MP3, для забезпечення доступності та цифрового підпису при передачі конфіденційної медичної інформації. Разом з тим, проведений в роботі [8] аналіз програмної реалізації несиметричної крипто-кодової системи на ТКС Нідеррайтера показав на значні складності реалізації, що істотно ускладнює використання теоретико-кодових схем для побудови криптостійкі несиметричних систем. В роботі [9] розглянуто нові підходи до злому криптосистеми Мак-Еліса на основі

рандомізованих зчеплених кодів.

Для забезпечення необхідних показників криптостійкості і збільшення обсягу переданих даних автором пропонується модифікована несиметрична крипто-кодова система (МНККС) Мак-Еліса на модифікованих (скорочених/подовжених) еліптичних кодах, що є перспективним напрямком у вирішенні даної науково-технічної задачі. Проведений аналіз в роботі [10] швидкості криптоперетворень в модифікованих несиметричних крипто-кодових системах Мак-Еліса порівняння з блоково-симетричними шифрами, але забезпечує математичну доказову криптостійкість на основі теоретико-складної задачі – декодування випадкового коду.

II. Основна частина

В роботі [10] автором розглянуті основні принципи модифікації завадостійких кодів, та запропонований математичний апарат модифікації алгеброгеометричних кодів на еліптичних кривих (модифікованих еліптичних кодів, МЕС).

На основі запропонованих модифікацій МЕС пропонуються математичні моделі модифікованої несиметричної крипто-кодової системи (МНККС) Мак-Еліса на МЕС (подовжених/скорочених кодів).

Математична модель НККС з використанням ТКС Мак-Еліса на основі укорочення (скорочення інформаційних символів) формально задається сукупністю наступних елементів [9]:

– множина відкритих текстів

$$M = \{M_1, M_2, ..., M_{q^k}\},$$

де $M_i = \{I_0, I_{h_1}, .. I_{h_j}, I_{k-1}\}$, $\forall I_j \in GF(q)$ h_j – інформаційні символи рівні нулю, $|h| = \frac{1}{2}k$, т. е. $I_i = 0$, $\forall I_i \in h$;

– множина закритих текстів (кодограм)

$$C = \{C_1, C_2, ..., C_{q^k}\},$$

де $C_i = (c^*_{X_0}, c^*_{h_1}, ..., c^*_{h_j}, c^*_{X_{n-1}})$, $\forall c^*_{X_j} \in GF(q)$;

– множина прямих відображень (на основі використання відкритого ключа – породжувальної матриці):

$$\varphi = \{\varphi_1, \varphi_2, ..., \varphi_s\},$$

де $\varphi_i : M \to C_{k-h_j}$, $i = 1,2,...,s$;

– множина зворотних відображень (на основі використання закритого (особистого) ключа – матриць маскування):

$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_s^{-1}\}$, где $\varphi_i^{-1} : C_{k-h_j} \to M$, $i = 1,2,...,s$;

– множина ключів, параметрізірующіх прямі відображення (відкритий ключ уповноваженого користувача):

$$K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G_X^{EC_1}{}_{a_i}, G_X^{EC_2}{}_{a_i}, ..., G_X^{ECs}{}_{a_i}\}$$

де $G_X^{ECi}{}_{a_i}$ – яка породжує $n \times k$ матриця замаскованого під випадковий код алгеброгеометричного блокового (n, k, d) коду з елементами з $GF(q)$ тобто $\varphi_i : M \xrightarrow{K_{ia_i}} C_{k-h_j}$; $i = 1,2,...,s$; a_i – набір коефіцієнтів багаточлена кривої $a_1 ... a_6$, $\forall a_i \in GF(q)$, однозначно ставить конкретний набір точок кривої з простору P^2.

– множина ключів, які параметрізують зворотні відображення (особистий (закритий) ключ уповноваженого користувача):

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, ..., \{X,P,D\}_s\},$$

$$\{X,P,D\}_i = \{X^i, P^i, D^i\},$$

де X^i – маскуюча невироджена випадково рівноймовірно сформована джерелом ключів $k \times k$ матриця з елементами з $GF(q)$; P^i – перестановочна випадково рівноймовірно сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$; D^i – діагональна сформована джерелом ключів матриця з елементами з $GF(q)$, тобто

$$\varphi_i^{-1} : C \xrightarrow{K_i^*} M, \; i = 1,2,...,s,$$

складність виконання зворотного відображення φ_i^{-1} без знання ключа $K_i^* \in K^*$ пов'язане з рішенням теоретико-складної задачі декодування випадкового коду (коду загального положення).

Вихідними даними при опису розглянутої несиметричної крипто-кодової системи захисту інформації є:

– алгеброгеометричний блоковий (n, k, d) код C_{k-h_j} над $GF(q)$, тобто множина кодових слів $C_i \in C_{k-h_j}$ таких, що виконується рівність $C_i H^T = 0$ де H – перевірочна матриця алгеброгеометричного блокового коду;

– a_i – набір коефіцієнтів багаточлена кривої $a_1 ... a_6$, $\forall a_i \in GF(q)$, однозначно ставить конкретний набір точок кривої з простору P^2 для формування матриці, яка породжує;

– h_j – інформаційні символи, рівні нулю, $|h| = 1/2k$, т. е. $I_i = 0$, $\forall I_i \in h$;

– маскуючі матричні відображення, задані безліччю матриць $\{X,P,D\}_i$, де X – невироджена $k \times k$ матриця над $GF(q)$, P – переставна $n \times n$ матриця над $GF(q)$ з одним ненульовим елементом в кожному рядку і в кожному стовпці матриці, D – діагональна $n \times n$ матриця над $GF(q)$ з ненульовими елементами на головній діагоналі.

У несиметричній крипто-кодовій системі на основі ТКС Мак-Еліса модифікований (укорочений) алгеброгеометричний (n, k, d) код C_{k-h_j} з швидким алгоритмом розкодування маскується під випадковий

(n, k, d) код C_{k-h_j}* за допомогою множення породжувальної матриці G^{EC} код C_{k-h_j} на збережені в секреті маскуючі матриці X^u, P^u і D^u, [10], що забезпечує формування відкритого ключа уповноваженого користувача:

$$G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u, \; u \in \{1,2,...,s\},$$

де G^{EC} – породжувальна $k \times n$ матриця алгеброгеометричного блокового (n,k,d) коду з елементами з *GF(q)*, побудовану на основі використання вибраних користувачем коефіцієнтів багаточлена кривої $a_1 ... a_6$, $\forall a_i \in GF(q)$, однозначно, які задають конкретний набір точок кривої з простору P^2.

Формування закритого тексту $C_j \in C_{k-h_j}$ по введеному відкритому тексту $M_i \in M$ і заданому відкритому ключу $G_X^{ECu}{}_{a_i}$, $u \in \{1,2,...,s\}$ здійснюється шляхом формування кодового слова замаскованого коду з додаванням до нього випадково сформованого вектору $e = (e_0, e_1, ..., e_{n-1})$

$$C_j = \varphi_u\left(M_i, G_X^u\right) = M_i \cdot \left(G_X^u\right)^T + e,$$

причому вага Хемінга (число ненульових елементів) вектору e не перевищує виправляючої здатності використовуваного алгебраїчного блокового коду:

$$0 \le w(e) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor,$$

$\lfloor x \rfloor$ – ціла частина дійсного числа *x*.

Для кожного закритого тексту, який формується $C_j \in C_{k-h_j}$ відповідний вектор $e = (e_0, e_1, ..., e_{n-1})$ виступає в якості одноразового сеансового ключа, тобто для конкретного E_j вектор e формується випадково, рівноймовірно і незалежно від інших закритих текстів.

У канал зв'язку надходить $C_j^* = C_j - C_{k-h_j}$.

На приймальній стороні уповноважений користувач, який знає правило маскування, кількість і місця нульових інформаційних символів може скористатися швидким алгоритмом розкодування алгеброгеометричного коду (поліноміальної складності) для відновлення відкритого тексту [10]:

$$M_i = \varphi_u^{-1}\left(C_j^*, \{X, P, D_u\}\right).$$

Для відновлення відкритого тексту уповноважений користувач додає нульові інформаційні символи $C_j^* = C_j + C_{k-h_j}$ з відновленого закритого тексту C_j знімає дію секретних перестановної і діагональної матриць P^u і D^u:

$$C = C_j^* \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \left(M_i \cdot \left(G_X^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$
$$= \left(M_i \cdot \left(X^u \cdot G \cdot P^u \cdot D^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$
$$= M_i \cdot \left(X^u\right)^T \cdot (G)^T \cdot \left(P^u\right)^T \cdot \left(D^u\right)^T \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$
$$= M_i \cdot \left(X^u\right)^T \cdot (G)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

розкодує отриманий вектор за алгоритмом Берлекемпа-Месси [10]:

$$C = M_i \cdot \left(X^u\right)^T \cdot \left(G^{EC}\right)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

тобто позбувається від другого доданку і від співмножника $(G)^{EC^T}$ в першому доданку в правій частині рівності, після чого знімає дію матриці маскування X^u. Для цього отриманий результат розкодування $M_i \cdot \left(X^u\right)^T$ слід помножити на $\left(X^u\right)^{-1}$: $\left(M_i \cdot \left(X^u\right)^T\right) \cdot \left(X^u\right)^{-1} = M_i$. Отримане рішення – суть відкритий текст M_i.

Математична модель модифікованої несиметричної крипто-кодової системи захисту інформації з використанням алгеброгеометричних блокових кодів на основі теоретико-кодової схеми Мак-Еліса на основі подовження (збільшення інформаційних символів) формально задається сукупністю наступних елементів

– множина відкритих текстів

$M = \{M_1, M_2, ..., M_{q^k}\}$, де $M_i = \{I_0, I_{h_1}, .. I_{h_{rj}}, I_{k-1}\}$, $\forall I_j \in GF(q)$, h_j – інформаційні символи рівні нулю, |h| = $\frac{1}{2}k$, тобто $I_i = 0, \forall I_i \in h$; h_r – інформаційні символи подовження k, |h| = $\frac{1}{2}k$;

– множина закритих текстів (кодограм)

$$C = \{C_1, C_2, ..., C_{q^k}\},$$

де $C_i = (c_{X_0}^*, c_{h_{r1}}^*, ..., c_{h_{rj}}^*, c_{X_{n-1}}^*)$, $\forall c_{X_j}^* \in GF(q)$;

– множина прямих відображень (на основі використання відкритого ключа - породжує матриці)

$\varphi = \{\varphi_1, \varphi_2, ..., \varphi_s\}$, де $\varphi_i : M \to C_{h_r}$, $i = 1,2,...,s$;

– множина зворотних відображень (на основі використання закритого (особистого) ключа - матриць маскування)

$\varphi^{-1} = \{\varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_s^{-1}\}$, де $\varphi_i^{-1} : C_{h_r} \to M$, $i = 1,2,...,s$;

– множина ключів, які параметрізують прямі відображення (відкритий ключ уповноваженого користувача))

$$K_{a_i} = \{K_{1_{a_i}}, K_{2_{a_i}}, ..., K_{s_{a_i}}\} = \{G_X^{EC1}{}_{a_i}, G_X^{EC2}{}_{a_i}, ..., G_X^{ECs}{}_{a_i}\},$$

де $G_{X\ a_i}^{ECi}$ – породжувальна $n \times k$ матриця замаскованого під випадковий код алгеброгеометричного блокового (n,k,d) коду з елементами з $GF(q)$, тобто

$$\varphi_i : M \xrightarrow{K_{i a_i}} C_{h_r}; i = 1,2,...,s;$$

a_i – набір коефіцієнтів багаточлена кривої $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, однозначно ставить конкретний набір точок кривої з простору P^2.

– множина ключів, які параметрізують зворотні відображення (особистий (закритий) ключ уповноваженого користувача))

$$K^* = \{K_1^*, K_2^*, ..., K_s^*\} = \{\{X,P,D\}_1, \{X,P,D\}_2, ..., \{X,P,D\}_s\},$$

$$\{X,P,D\}_i = \{X^i, P^i, D^i\},$$

де X^i – маскуюча невироджена випадково рівноймовірно сформована джерелом ключів $k \times k$ матриця з елементами з $GF(q)$; P^i – перестановочна випадково рівноймовірно сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$; D^i – діагональна сформована джерелом ключів $n \times n$ матриця з елементами з $GF(q)$, тобто

$$\varphi_i^{-1} : C \xrightarrow{\mathrm{K_i^*}} M, i = 1,2,...,s,$$

складність виконання зворотного відображення φ_i^{-1} без знання ключа $K_i^* \in K^*$ пов'язане з рішенням теоретико-складної задачі декодування випадкового коду (коду загального положення).

Вихідними даними при описі розглянутої несиметричної крипто-кодової системи захисту інформації є параметри, описані в попередній моделі.

У несиметричній крипто-кодовій системі на основі ТКС Мак-Еліса модифікований (подовжений) алгеброгеометричний (n, *k, d*) код C_{h_r} з швидким алгоритмом розкодування маскується під випадковий (*n, k, d*) код C_{h_r}* за допомогою множення породжує матрицю G^{EC} коду C_{k-h_j} на маскують матриці, які зберігаються в секреті X^u, P^u і D^u, що забезпечує формування відкритого ключа уповноваженого користувача: $G_X^{ECu} = X^u \cdot G^{EC} \cdot P^u \cdot D^u$, $u \in \{1,2,...,s\}$,

де G^{EC} – яка породжує $n \times k$ матрицю алгеброгеометричного блокового (n,k,d) коду з елементами з $GF(q)$, побудована на основі використання вибраних користувачем коефіцієнтів багаточлена кривої $a_1 \ldots a_6$, $\forall a_i \in GF(q)$, однозначно задають конкретний набір точок кривої з простору P^2.

Формування закритого тексту $C_j \in C_{h_r}$ по введеному відкритому тексту $M_i \in M$ і заданому відкритому ключу $G_{X\ a_i}^{ECu}$, $u \in \{1,2,...,s\}$ здійснюється шляхом формування укороченого кодового слова, а потім подовження замаскованого коду з додаванням до нього випадково сформованого вектору $e = (e_0, e_1, ..., e_{n-1})$:

$$C_j = \varphi_u\left(M_i, G_X^u\right) = M_i \cdot \left(G_X^u\right)^T + e$$

Для кожного формованого закритого тексту $C_j \in C_{h_r}$ відповідний вектор $e = (e_0, e_1, ..., e_{n-1})$ виступає в якості одноразового сеансового ключа, тобто формується випадково, рівноймовірно і незалежно від інших закритих текстів.

У канал зв'язку надходить $C_j^* = C_j - C_{k-h_j} + C_{h_r}$

На приймальній стороні, уповноважений користувач, який знає правило маскування, кількість і місця нульових інформаційних символів може скористатися швидким алгоритмом розкодування алгеброгеометричного коду (поліноміальної складності) для відновлення відкритого тексту: $M_i = \varphi_u^{-1}\left(C_j^*, \{\mathrm{X,P,D}\}_\mathrm{u}\right)$.

Для відновлення відкритого тексту уповноважений користувач заміняє символи подовження на нульові інформаційні символи: $C_j^* = C_{h_r} \to C_{k-h_j}$,

з відновленого закритого тексту C_j знімає дію секретних перестановної і діагональної матриць P^u и D^u:

$$C = C_j^* \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} = \left(M_i \cdot \left(G_X^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= \left(M_i \cdot \left(X^u \cdot G \cdot P^u \cdot D^u\right)^T + e\right) \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= M_i \cdot \left(X^u\right)^T \cdot (G)^T \cdot \left(P^u\right)^T \cdot \left(D^u\right)^T \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} =$$

$$= M_i \cdot \left(X^u\right)^T \cdot (G)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

розкодує отриманий вектор за алгоритмом Берлекемпа-Месси [10]:

$$C = M_i \cdot \left(X^u\right)^T \cdot \left(G^{EC}\right)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1},$$

тобто позбавляється від другого доданку і від співмножника $(G)^{EC^T}$ в першому доданку в правій частині рівності, після чого знімає дію матриці маскування X^u. Для цього отриманий результат розкодування $M^*{}_i$ слід помножити на $\left(X^u\right)^{-1}$:

$$M^*{}_i \cdot \left(X^u\right)^{-1} = M_i.$$

Отримане рішення – відкритий текст M_i, до якого додаються символи подовження: $M_j = M_i + h_r$ – суть переданого повідомлення.

В роботах [8, 10] проведений аналіз оцінки енергетичних витрат на програмну реалізацію і складності кодоперетворень в МНККС Мак-Еліса. Для оцінки часових і швидкісних показників прийнято використовувати одиницю виміру *cpb* (*cycles per byte*) – кількість тактів

процесора, який необхідно витратити для обробки 1 байту інформації. Складність алгоритму обчислимо за виразом:

$$Per = Utl * CPU\_clock / Rate ,$$

де Utl – утилізація ядра процесора (%), $Rate$ – пропускна здатність алгоритму (байт/с).

В табл. 1 наведені результати досліджень залежності довжини кодової послідовності алгеброгеометричного коду в МНККС Мак-Еліса від кількості тактів процесора на виконання елементарних операцій в програмній реалізації модифікованих крипто-кодових систем. В табл. 2 результати досліджень оцінки тимчасових і швидкісних показників процедур формування і розкодування інформації в несиметричних крипто-кодових системах на основі ТКС Мак-Еліса.

ТАБЛИЦЯ 1 РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ ЗАЛЕЖНОСТІ ДОВЖИНИ КОДОВОЇ ПОСЛІДОВНОСТІ КОДУ В НККС МАК-ЕЛІСА І МОДИФІКОВАНОЇ НККС ВІД КІЛЬКОСТІ ТАКТІВ ПРОЦЕСОРА

Довжина кодової послідовності		**MacElis на укорочених кодах**			**MacElis на подовжених кодах**			**MacElis**		
		10	***100***	***1000***	***10***	***100***	***1000***	***10***	***100***	***1000***
Кількість викликів функцій, що реалізовують елементарні операції	Читання символу	10 294 397	28 750 457	76 759 874	11 432 131	33 460 317	82 473 442	11 018 042	30 800 328	80 859 933
	Порівняння рядків	3 406 921	9 246 748	25 478 498	3 673 756	12 119 867	29 469 389	3 663 356	10 199 898	26 364 634
	Конкатенація рядків	1 705 544	5 045 748	12 379 422	1 947 681	6 114 478	14 456 729	1 834 983	5 125 564	13 415 329
Сума		15 406 862	43 042 953	114 617 794	17 053 568	17 053 568	51 694 662	126 399 560	46 125 790	120 639 896
Тривалість виконання функцій * в тактах процесора	Читання символу	295 374	810 478	2 001 167	300 479	843 705	2 745 148	297 487	831 609	2 183 218
	Порівняння рядків	178 814	531 379	1 248 684	213 478	561 754	1 739 170	197 821	550 794	1 423 690
	Конкатенація рядків	544 990	1 328 114	3 586 486	578 174	1 647 638	4 007 883	544 990	1 522 293	3 984 353
Сума		1 006 781	2 749 548	7 247 488	109 157	109 157	1 092 131	3 053 097	2 904 696	7 591 261
Тривалість виконання ** в мс		0,52	1,37	3,4	0,56	0,56	1,55	4,1	1,53	4

ПРИМІТКА: * тривалість 1000 операцій в тактах процесора: читання символу – 27 тактів, порівняння рядків – 54 такту, конкатенація рядків – 297 тактів; ** для розрахунку взято процесор з тактовою частотою 2 ггц з урахуванням завантаження операційної системою 5 %

ТАБЛИЦЯ 2 РЕЗУЛЬТАТИ ДОСЛІДЖЕНЬ ОЦІНКИ ТИМЧАСОВИХ І ШВИДКІСНИХ ПОКАЗНИКІВ ПРОЦЕДУР ФОРМУВАННЯ І РОЗКОДУВАННЯ ІНФОРМАЦІЇ

Показники	***Довжина кодової послідовності***	***Пропускна здатність алгоритму, Rate, (байт / с)***	***Утилізація ядра процесора,%***	***Складність алгоритму, Per (cpb)***
MacElis	100	46 125 790	56	61,5
	1000	120 639 896	56	62,0
MacElis на укорочених кодах	100	52 721 778	56	61,5
	1000	127 389 928	56	62,1
MacElis на подовжених кодах	100	51 694 662	56	61,7
	1000	126 399 560	56	62,2

Проведений аналіз табл. 1, 2 підтверджує необхідність використання модифікованих НККС для зменшення енергетичних витрат.

Таким чином, передача ключовий послідовності при використанні модифікованої несиметричної крипто-кодової системи Мак-Еліса на основі укорочених кодів дозволяє використовувати відкриті канали зв'язку комунікаційних систем і суттєво знизити обсяги ключових послідовностей, що зберігаються у користувачів даної системи. Використання подовжених еліптичних кодів дозволяє збільшити обсяг переданих даних на h_r символів, забезпечуючи при цьому стійкість криптосистеми при її формуванні в поле $GF\ (2^6 – 2^8)$, що істотно знижує енергетичні витрати на її реалізацію.

ЛІТЕРАТУРА REFERENCES

[1] S.G. Semenov, Modeli i metody upravlenija setevymi resursami v informacionno-telekommunikacionnyh sistemah [Tekst] : monografija / S. G. Semenov, A. A. Smirnov, E. V. Meleshko – Har'kov : NTU "HPI", 2011. – 212 s.

[2] H.N. Rzaev, Analiz sostojanija i putej sovershenstvovanija protokolov bezopasnosti sovremennyh telekommunikacionnyh setej [Tekst] : monografija / H. N. Rzaev, O. G. Korol' // Informacionnye tehnologii v upravlenii, obrazovanii, nauke i promyshlennosti: monografija/– H. : Izdatel' Rozhko S. G. 2016. – S.217 – 234.

[3] Telekommunikacionnye uslugi v mirovoj jekonomike [Jelektronnyj resurs] : – Rezhim dostupa : http://www.gumer.info/bibliotek_Buks/Econom/world_econom/30.php.

[4] Transmission of Picturesque content with Code Base Cryptosystem [Elektronnyj resurs] : – Rezhim dostupa : https://doaj.org/article/6714b60516cc4aa79e56d0c421febaf3.

[5] Steganography application program using the ID3v2 in the MP3 audio file on mobile phone [Jelektronnyj resurs] : – Rezhim dostupa : https://doaj.org/article/707a6506be9e49698fd75323fcc1302c.

[6] Space-Age Approach To Transmit Medical Image With Codebase Cryptosystem Over Noisy Channel [Jelektronnyj resurs] : – Rezhim dostupa : https://doaj.org/article/5c7da3a1e3ec4f83b552199034bd3241.

[7] An Authenticated Transmission of Medical Image with Codebase Cryptosystem over Noisy Channel [Jelektronnyj resurs] : – Rezhim dostupa : https://doaj.org/article/39a3ac65d5b24b348f069dfc82eb6248.

[8] S.P. Evseev, Analiz programmnoj realizacii prjamogo i obratnogo preobrazovanija po metodu nedvoichnogo ravnovesnogo kodirovanija / S.P. Evseev, H.N. Rzaev, A.S. Cyganenko // Naukovo-tehnichnij zhurnal «Bezpeka informacii». tom.22. № 2. Kiïv. – 2016. – s. 196 – 203

[9] On the Usage of Chained Codes in Cryptography [Jelektronnyj resurs] : – Rezhim dostupa : https://doaj.org/article/c0f40bdb1f6149f4ac107d44a95c9531.

[10] S.P. Evseev, Razrabotka modificirovannoj nesimmetrichnoj kripto-kodovoj sistemy Mak-Jelisa na ukorochennyh jellipticheskih kodah / S.P. Evseev, H.N. Rzaev, O.G. Korol, Z.R. Imanova // Vostochno-evropejskij zhurnal peredovyh tehnologij. – Har'kov. – 2016. – tom 4. 9(82). – S. 18-26.