УДК 681.3.06
DOI: 10.15587/2313-8416.2019.189621

МОДИФІКАЦІЇ КРИПТО-КОДОВОЇ КОНСТРУКЦІЇ НІДЕРАЙТЕРА

О. С. Циганенко

Дослідження крипто-кодової конструкції Нідерайтера на МЕС дозволили виявити основну причину неможливості практичної реалізації алгоритмів розкодування при використанні недвійковий кодів в класичній схемі. Встановлено, що потрібно фіксування підмножини відкритих текстів, для яких процедура локалізації помилки, при обраних відправником матрицях маскування X, P і D (особистий ключ) не може бути виконана. Розроблений модифікований алгоритм за допомогою укорочення інформаційної посилки і фіксації допустимих позиційних векторів перетворення відкритого тексту на основі рівноважного кодування.

Ключові слова: *модифікована крипто-кодова конструкція Нідерайтера, модифіковані укорочені еліптичні коди, рівноважне кодування, інформаційна скритність.*

1. Вступ

Обчислювальні можливості в останні десятиліття дозволяють людству вийти на абсолютно новий рівень обробки інформації, що, в свою чергу, висуває нові вимоги до надійності та забезпечення безпеки даних. Разом з технічним прогресом росте і комп'ютерна злочинність, з'являються нові види атак і нові види кібертероризму. Збільшення оброблюваних обсягів даних в критичних системах ЛВС (ГВС) висуває нові вимоги до забезпечення надійності і продуктивності комп'ютерних систем, безпеки і достовірності переданих і оброблюваних даних. Проведені дослідження в області впливу квантових обчислень, що використовують явища квантової суперпозиції та квантової заплутаності для передачі та обробки даних, показали, що квантові комп'ютери, які використовують спеціальні алгоритми (наприклад, алгоритм Шора), будуть здатні до факторизації чисел за поліноміальний час. Отже, криптографічні системи RSA, ECC, DSA будуть вразливі до атак "грубої сили" (brute force attacks) з використанням повномасштабного квантового комп'ютера. Тому основні дослідження і розробки криптографічних засобів захисту інформації (КЗЗІ) в нинішній час спрямовані на пошуки рішень, що не мали б вразливостей щодо квантових обчислень і були б одночасно стійкими до атак за допомогою звичайних комп'ютерів. Такі алгоритми відносяться до розділу квантово-стійкої криптографії (quantum safe cryptography або quantum resistant cryptography). Через швидку появу нових схем не приділяється достатня увага давно відомим, несиметричним крипто-кодовим системам (НККС) на основі ТКС Мак-Еліса і Нідерайтера, що також є квантово-стійкими. У комп'ютерних мережах з вирішальною зворотним зв'язком для інтегрованого забезпечення вимог як достовірності так і оперативності даних пропонується використовувати несиметричну крипто-кодову системи Нідеррайтера на еліптичних кодах.

2. Літературний огляд

У роботі [1] було запропоновано комбіновану схему Мак-Еліса-Нідерайтера, однак, як і традиційна схема Нідерайтера, авторами розглядається рівноважове кодування в схемі Нідерайтера на бінарних кодах, що не дозволяє створити криптосистеми з необхідними рівнями криптостійкості. Це підтверджують результати досліджень у роботі [2]. Доповнення до використання в двох варіантах - вимушений шаг на шляху до робочих можливостей описаної конструкції, який спричинив зменшення швидкості і збільшення енергоємності.

У роботі [2] показано атаку на схеми Мак-Еліса та Нідерайтера на основі дрібно-лінійних перетворень, які дозволяють знайти породжуючу (перевірочну) матрицю і зламати криптосистему. Таким чином, перспективним рішенням є розробка схеми Мак-Еліса та Нідерайтера на алгеброгеометричних кодах (кодах на основі параметрів еліптичних кривих) або каскадних кодах.

У роботі [3] була згадана можливість практичної реалізації несиметричної крипто-кодової системи Нідерайтера на еліптичних кодах, але вона вимагає збільшення швидких криптоперетворень.

У роботі [4, 5] запропоновано підходи для здійснення ККК Мак-Еліса в умовах постквантової криптографії.

У роботі [6] запропоновано підходити до реалізації МККК Нідерайтера на МЕС. Незважаючи на це, незначне зменшення енерговитрат.

У роботі [7, 8] запропоновано метод рівноважового кодування на основі м-ного коду (коду Рида-Соломона), однак недоліком є відсутність практичних алгоритмів разкодування синдрому на приймаючій стороні та можливості злому на основі переставного декодера.

У роботі [9] автори підтверджують складність практичної реалізованої системи Нідерайтера та розглядають можливість використання криптосистем у VPN-

каналі. У роботі [10] автори пропонують використовувати коди Ріда-Соломона (РС) для побудови несиметричної крипто-кодової системи на основі схем Мак-Еліса. Однак автори не розглянули можливості злому криптосистеми на основі дрібно-лінійних перетворень.

3. Мета та задачі досліджень

Метою дослідження є розробка математичного апарату та практичних алгоритмів НККС Нідерайтера на еліптичних кодах з урахуванням особливостей реалізації та необхідних змін.

Основними завданнями дослідження визначено такі:

– розробка математичної моделі НККС Нідерайтера,

– розробка практичних алгоритмів НККС Нідерайтера

– дослідження властивостей НККС Нідерайтера

4. Матеріали і методи досліджень

В роботі [7] вперше запропонована кодова криптосистема, заснована на маскуванні перевірочної матриці алгебраїчного блокового коду. Основна перевага НККС Нідеррайтера полягає у високій швидкості перетворення інформації (відносна швидкість кодування близька до 1).

Основними характеристиками є: (рис 1.) особистий ключ: G – породжувальна матриця лінійного (n, k, d) коду над GF (q) з поліноміальною складністю декодування, X – невироджена k×k – матриця над GF (q), D – діагональна матриця з ненульовими на діагоналі елементами, P – переставна матриця розміру n × n. Відкритим ключ: матриця GX=X×G×P×D, отримана шляхом перемноження породжувальної матриці лінійного (n, k, d) коду над GF (q) на матриці маскування (X, P, D).

Під час експериментального дослідження було визначено, що використання недвійкових кодів з класичною НККС Нідерайтера потребує доробок, а саме фіксування підмножини відкритих текстів для яких процедура локалізації помилки, при обраних *X, P* і *D*, не може бути виконана. Нехай $Mc = \left\{M_1, M_{2,}...M_{q^k}\right\}$, множина всіх відкритих текстів (*n, k, d*) блокового коду. Визначимо підмножину зафіксованих відкритих текстів $Mf = \left\{M_1, M_{2,}...M_n\right\}$, де $M_i^u \cdot P^u \cdot D^u ! =$

$= M_i \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1} \cdot P^u \cdot D^u$.

При кодуванні, елементи множини зафіксованих відкритих текстів не беруть участь, а множина придатних відкритих текстів є $M = M_c - M_f$.

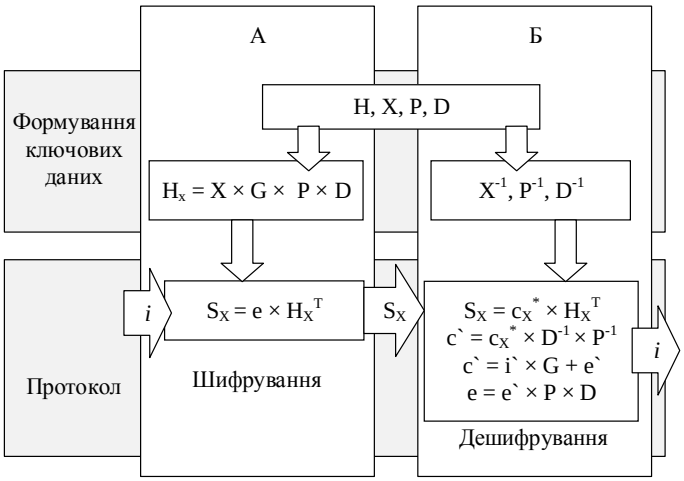

Рис. 1. Алгоритм взаємодії абонентів в МККС Нідерайтера

Розглянемо формальний опис математичної моделі НККС Нідерайтера. Математична модель задається сукупністю таких елементів [**Ошибка! Источник ссылки не найден.**]:

– множина всіх відкритих текстів $Mc = \left\{M_1, M_{2,}...M_{q^k}\right\}$, де $M_i = \left\{e_0, e_{h_1,}...e_{h_k}, e_{e-1}\right\}$, $\forall e_e \in GF(q)$, h_e – символи вектора помилки, що дорівнюють нулю, $|h| = \frac{1}{2}e$, тобто $e_i=0, \forall e_i \in h$;

– множина зафіксованих відкритих текстів $Mf = \left\{M_1, M_{2,}...M_n\right\}$, тоді множина придатних відкритих текстів $M = Mc - Mf$;

– множина закритих текстів $S = \left\{S_0, S_1,...S_{q^r}\right\}$, де $S_i = \left\{S^*_{X_0}, S^*_{h_1},...S^*_{h_j}, S^*_{X_r}\right\}$, $\forall S_{X_r} \in GF(q)$;

– множина прямих відображень (на основі використання відкритого ключа – перевірочної матриці еліптичного коду (*EC*): $\varphi = \left\{\varphi_1, \varphi_2, ..., \varphi_r\right\}$,

де $\varphi_i : M \to S_{r-h_e}, i = 1,2,...,e$ – множина обернених відображень (на основі використання закритого (особистого) ключа – матриць маскування). $\varphi^{-1} = \left\{\varphi_1^{-1}, \varphi_2^{-1}, ..., \varphi_r^{-1}\right\}$,

де $\varphi_i^{-1} : S_{r-h_e} \to M, i = 1,2,...,e$.

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

$$KU_{a_i} = \left\{KU_{1_{a_i}}, KU_{2_{a_i}}, ..., KU_{r_{a_i}}\right\} = \left\{H_{x_{a_i}}^{EC_1}, H_{x_{a_i}}^{EC2}, ..., H_{x_{a_i}}^{ECr}\right\}$$

де $H_{x_{a_i}}^{EC_i}$ – перевірочна $r \times n$ матриця замаскованого під випадковий код алгеброгеометричного блокового (n, k, d) коду з елементами $GF(q)$, тобто $\varphi_i : M \xrightarrow{KU_{i_{a_i}}} S^*_{r-h_e}$, $i = 1,2,...,e$, a_i – набір коефіцієнтів многочлена кривої $a_1 ... a_6$, $\forall a_i \in GF(q)$, однозначно задає конкретний набір точок кривої з простору P^2;

– множина ключів, які параметризують обернені відображення (особистий (закритий) ключ уповноваженого користувача):

$$KR = \left\{KR_1, KR_2, ..., KR_r\right\} = \left\{\begin{matrix}\left\{X, P, D\right\}_1, \\ \left\{X, P, D\right\}_2, ..., \left\{X, P, D\right\}_r\end{matrix}\right\},$$

$\left\{X, P, D\right\}_i = \left\{X^i, P^i, D^i\right\}$, де X^i – маскуюча невироджена випадково рівноймовірно сформована джерелом ключів $k \times k$ матриця з елементами зі $GF(q)$; 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 $\varphi_i^{-1} : S^*_{r-h_e} \xrightarrow{KR_i} M$, $i = 1,2,...,s$. Складність виконання оберненого відображення ϕ_i^{-1} без знання ключа $K_i^* \in K^*$ пов'язана з розв'язанням теоретико-складної задачі декодування випадкового коду (коду загального положення).

Вихідними даними при описі розглянутої несиметричною крипто-кодової системи захисту інформації є:

– недвійковий рівноважний код над $GF(q)$, тобто множина послідовностей довжини n та ваги $w(\varepsilon_i)$;

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

– маскуючі матричні відображення, задані множиною матриць $\{X, P, D\}_i$, де X – невироджена $k \times k$ матриця над $GF(q)$, P – перестановочна $n \times n$ 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;

– r – деякий параметр $r \in_R Z_{q^m}$, $Z_{q^m} = \left\{0,1,...2^n - 1\right\}$,

n – деякий параметр $n \in_R Z_{q^n}$, $Z_{q^n} = \left\{1,...2^n\right\}$;

На основі рівноважного кодування формується закритий текст $C_j \in C$ за введеним відкритим текстом $M_i \in M$ і заданим ключем H_X^{ECu}, $u \in \{1,2,...,s\}$. Це здійснюється шляхом формування синдромної (в термінах завадостійкого кодування) послідовності S_{X_j}, що відповідає рівноважній послідовності $M_i = e = \{e_0, e_1, ..., e_{n-1}\}$:

$S_{X_j} = \phi_u\left(M_i, H_X^{ECu}\right) = M_i \times \left(H_X^{ECu}\right)^T$, причому вага Гемінга (кількість ненульових елементів) вектора e не перевищує виправної здатності використовуваного алгебраїчного блокового (n,k,d) коду:

$$\forall i : 0 \le w(M_i) \le t = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Потужність множин M та C визначається допустимим спектром ваг $w(M_i)$, тобто в загальному випадку (для всіх допустимих значень $w(M_i)$) маємо:

$m = \sum_{i=0}^{t} (q-1)^i \times C_n^i$, де C_n^i – біноміальний коефіцієнт, $C_n^i = \frac{n!}{i! \cdot (n-1)!}$.

Найбільш доцільно величину $w(M_i)$ вибирати відповідно до необхідного значенням безпеки передачі інформації.

Тоді для $w(M_i) = const = w(e)$ маємо:

$$m = (q-1)^{w(e)} \times C_n^{w(e)},$$

а послідовність $M_i = \{e_0, e_1, ..., e_{n-1}\}$ з множини $M = \{M_1, M_2, ..., M_m\}$ формується як результат деякого відображення ψ, реалізованого шляхом надлишкового кодування недвійковими рівноважними кодами ненадлишкових інформаційних послідовностей.

Сформований закритий текст $C_j \in C$ однозначно відповідає вектору $M_i = \{e_0, e_1, ..., e_{n-1}\}$.

Сформуємо вектор ініціалізації $IV = EC - h_j$, де h_j – інформаційні символи, що дорівнюють нулю, $|h| = \frac{1}{2}k$, тобто. $I_i = 0$, $\forall I_i \in h$.

Відкритий ключ формується шляхом множення перевірочної матриці алгеброгеометричного коду на матриці маскування:

$$H_X^{ECu} = X^u \cdot H \cdot P^u \cdot D^u, \quad u \in \{1,2,...,s\},$$

де H^{EC} – перевірочна $n \times (n-k)$ матриця алгеброгеометричного блокового (n,k,d) коду з елементами з $GF(q)$. В канал зв'язку поступає синдромна послідовність: $S^*_{r-h_e} = (e_n - h_e) \times H_X^{EC^T}$.

На стороні прийому уповноважений користувач, який знає маскування (набір матриць $\{X, P, D\}_u = \{X^u, P^u, D^u\}$) і вектори ініціалізації (кількість і місця нульових символів вектора помилки) формує кодову послідовність як одне (будь-яке) з можливих рішень рівняння:

$$S^*_{r-h_e} = c^*_{X_i} \cdot H^T_{X_j},$$

тобто знаходить такий вектор $c^*_{X_i}$, який розкладається на суму: $c^*_{X_i} = c_{X_i} + M_i$, де c_{X_i} – одне (будь-яке) з можливих кодових слів замаскованого коду з перевірочної матрицею $H^T_{X_j}$, тобто $c_{X_i} \times H^T_{X_j} = 0$.

Далі уповноважений користувач, використовуючи набір матриць $\{X,P,D\}_u=\{X^u,P^u,D^u\}$, формує вектор: $\bar{c}^*=c_X^*\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}$, тобто демаскує кодову послідовність $c_{X_i}^*$.

Після підстановки отримаємо рівність:

$$\bar{c}^*=c_X^*\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}=\left(c_{X_i}+M_i\right)\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}=$$

$$=c_{X_i}\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}+M_i\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}.$$

Уповноважений користувач, який сформував вектор, має можливість застосувати швидкий (поліноміальної складності) алгоритм завадостійкого декодування і сформувати таким чином вектор $\bar{c}^*=c_X^*\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}$ та вектор $M_i^u=M_i\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}$.

Для відновлення інформаційної рівноважної послідовності M_i достатньо знову помножити вектор M_i^u на матриці маскування D^u та P^u, але в іншому порядку:

$$M_i=M_i^u\cdot P^u\cdot D^u=M_i\cdot\left(D^u\right)^{-1}\cdot\left(P^u\right)^{-1}\cdot P^u\cdot D^u=M_i.$$

5. Результати досліджень

В роботах [11, 12] наведені детальні результаті дослідження, тому звернемо увагу тільки на ті показники, що відрізняються від проаналізованих джерел, з розділу 2.

На рис. 2 наведені результати досліджень складності розкодування криптограми в різних *GF(2^m)*.

Аналіз рис. 2, показав, що в подальше зменшення потужності поля Галуа призводить до значного зменшення складності формування (≈ в 3 разів) і розкодування (≈ в 5 разів) криптограми.

На рис. 3 наведені результати досліджень складності злому алгоритмом переставного декодування в різних GF(2^m).

Аналіз рис. 3 показав, що зменшення потужності поля до 2^6 не привело до істотного зниження складності злому криптограми методом переставного декодування.

На рис. 4 наведені результати досліджень складності злому і складності кодування для різних швидкостей R в різних GF(2^m).

На рис. 5 наведені залежності обсягу відкритих ключових даних для різних показників стійкості.

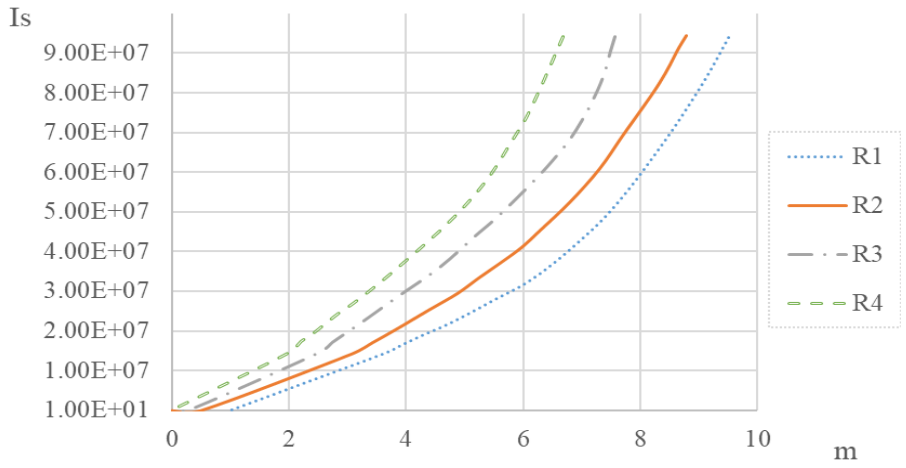

Рис. 2. Залежність складності розкодування криптограми в різних GF(2m)

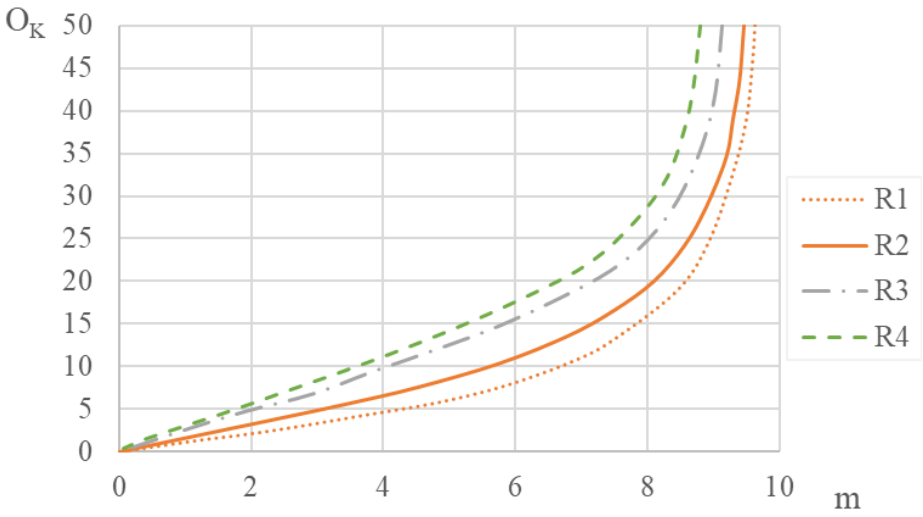

Рис. 3. Залежність складності злому над GF(2m) (переставне декодування)

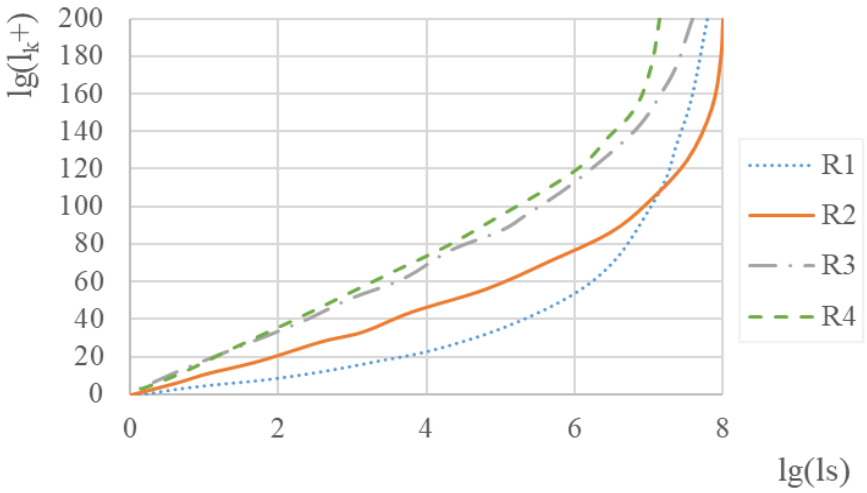

Рис. 4. Зведена діаграма складності злому і складності кодування

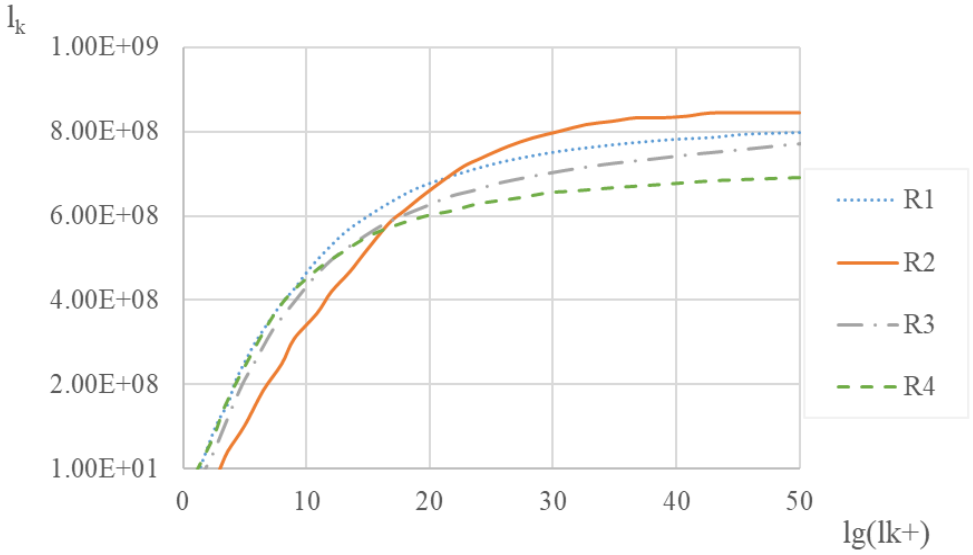

Рис. 5. Залежності обсягу відкритих ключових даних для різних показників стійкості

Аналіз наведених результатів рис. 4 та 5 ясно демонструє за рахунок чого отримано зростання відносної швидкості передачі даних: обсяг ключових даних в системах на укорочених кодах вдвічі менший за класичну НККС.

6. Висновки

1. Запропоновано формальний опис математичної моделі модифікованої крипто-кодової конструкції на основі описаної НККС Нідерайтера на МЕС.

2. Запропоновано практичні алгоритми реалізації описаної НККС Нідерайтера на МЕС (шифрування та розшифрування).

3. Досліджено описану НККС Нідерайтера на МЕС, основною відмінністю якої є зниження обсягу переданих даних шляхом укорочення вектору помилки перед формуванням синдрому на стороні відправника у класичній НККС Нідерайтера, що дозволяє знизити потужність поля і відповідно енергетичні витрати.

Таким, чином розглянута НККС Нідерайтера на МЕС формується над полем $GF(2^6)$ є конкурентоздатною системою забезпечення основних послуг безпеки та є перспективним напрямком досліджень по зниженню енерговитрат криптоперетворень в ККК на основі НККС Нідерайтера.

Література

1. Dinh, H., Moore, C., Russell, A. (2019). McEliece and Niederreiter Cryptosystems that Resist Quantum Fourier Sampling Attacks. Heidelberg: Springer-Verlag Berlin, 761–779. Available at: https://dl.acm.org/citation.cfm?id=2033093 Last accessed: 01.12.2019

2. Сидельников, В. М. (2008). Теория кодирования. Москва: ФИЗМАТЛИТ, 324.

3. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et. al. (2018). Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. doi: http://doi.org/10.15587/1729-4061.2018.150903

4. Cho, J. Y., Griesser, H., Rafique, D. (2017). A McEliece-Based Key Exchange Protocol for Optical Communication Systems. Lecture Notes in Electrical Engineering, 109–123. doi: http://doi.org/10.1007/978-3-319-59265-7_8

5. Yevseiev, S., Rzayev, K., Korol, O., Imanova, Z. (2016). Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (82)), 18–26. doi: http://doi.org/10.15587/1729-4061.2016.75250

6. Евсеев, С., Цыганенко, А. (2018). Розробка несиметричної крипто-кодової конструкції Нідеррайтера на модифікованих еліптичних кодах. Системи обробки інформації, 2 (153), 127–135. doi: http://doi.org/10.30748/soi.2018.153.16

7. Дудикевич, В. Б., Кузнецов, О. О., Томашевський, Б. П. (2010). Крипто-кодовий захист інформації з недвійковим рівноваговим кодуванням. Сучасний захист інформації, 2, 14–23.

8. Дудикевич, В. Б., Кузнєцов, О. О., Томашевський, Б. П. (2010). Метод недвійкового рівновагового кодування. Сучасний захист інформації, 3, 57–68.

9. De Vries, S. (2016). Achieving 128-bit Security againstQuantum Attacks in OpenVPN. Available at: https://internetscriptieprijs.nl/wp-content/uploads/2017/04/1-Simon-de-Vries-UT.pdf Last accessed: 01.12.2019

10. Baldi, M., Bianchi, M., Chiaraluce, F., Rosenthal, J., Schipani, D. (2014). Enhanced public key security for the McEliece cryptosystem. Available at: https://arxiv.org/abs/1108.2462 Last accessed: 01.12.2019

11. Yevseiev, S., Tsyhanenko, O., Gavrilova, A., Guzhva, V., Milov, O., Moskalenko, V. et. al. (2019). Development of Niederreiter hybrid crypto-code structure on flawed codes. Eastern-European Journal of Enterprise Technologies, 1 (9 (97)), 27–38. doi: http://doi.org/10.15587/1729-4061.2019.156620

12. Yevseiev, S., Shmatko, O., Tsyhanenko, O. (2019). Metodologicheskiye osnovy postroyeniya kriptostoykikh kriptosistem Mak-Elisa i Niderraytera na algebrogeometricheskikh kodakh v postkvantovoy kriptografii. 3rd International Symposium on Multidisciplinary Studies and Innovative Technologies. Ankara.

Received date 12.11.2019
Accepted date 04.12.2019
Published date 30.12.2019

Циганенко Олексій Сергійович, аспірант, кафедра кібербезпеки та інформаційних технологій, Харківський національний економічний університет ім. С. Кузнеця, пр. Науки, 9-А, м. Харків, Україна, 61166
E-mail: oleksii.tsyhanenko@hneu.net

УДК 669.054.82:669.714.82
DOI: 10.15587/2313-8416.2019.189686

АНАЛІЗ ТЕХНОЛОГІЙ ПЕРЕРОБКИ АЛЮМІНІЄВОГО СКРАПУ

Ф. М. Верховлюк, В. В. Довбенко, І. Ф. Червоний

Представлено аналіз технологій переробки алюмінієвого скрапу з урахуванням економічної та екологічної складових. Розглянуто кислотно-лужний способи, сульфатний і содовий способи, а також електродугової переплав алюмінієвого шлаку в однофазної електродугової печі змінного струму. Відзначається значна кількість проблем, що стосуються механічних і електрофізичних характеристик вироблених виробів. Вирішення цих питань, з урахуванням підвищення вимог споживача, можливо тільки при виконанні спеціальних досліджень в частині вдосконалення технології та розробки пристроїв і установок для проведення нових технологічних процесів

Ключові слова: *алюміній, вторинний алюміній, сировина, шлак, пінки, дроси, розплав, електротермічна установка, плавильна піч*

1. Вступ

Алюміній – легкий метал сріблясто-білого кольору, легко піддається формуванню, литтю та механічній обробці. Алюміній має високу тепло- та електропровідність, а також стійкість до корозії. Алюміній є елементом 13-й групи періодичної таблиці хімічних елементів з атомним номером 13. Алюміній належить до групи легких металів і є найбільш поширеним металом – третій метал за поширеністю хімічних елементів в земній корі (після кисню і кремнію).

Відповідно до довідкових даних [1, 2], вперше алюміній був отриманий датським фізиком Гансом Ерстед в 1825 році. Він відновив хлорид цього елемента амальгамою калію при нагріванні і виділив метал. Пізніше спосіб Ерстеда був поліпшений Фрідріхом Велером, який використовував для відновлення хлориду алюмінію до металу чистий металевий калій, і він же описав хімічні властивості алюмінію.

Напівпромисловим способом вперше алюміній отримав в 1854 р. Сент-Клер Девіль за методом Велера, замінивши калій на більш безпечний натрій. Рік