МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

УДК 681.518.54

Тези доповідей

Міжнародної науково-практичної конференції

“Інформаційна безпека та інформаційні технології”
“Information Security and Information Technologies”

24–25 квітня 2019 р.

Харків 2019

УДК 681.518.54

Матеріали Міжнародної науково-практичної конференції “Інформаційна безпека та інформаційні технології”: тези доповідей, 24 – 25 квітня 2019 р. – Х.: ХНЕУ імені Семена Кузнеця, 2019. – 68 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несе автор.

УДК 621.391

С.П. Євсеєв[1], О. Г. Король[1], А.А. Гаврилова[1], Керім Четінкайя[2]

serhii.yevseiev@hneu.net, korol.olha2016@gmail.com, sharaya1972@gmail.com

[1]*Харківський національний економічний університет імені Семена Кузнеця, м. Харків*
[2]*Університет Карабюк, Турція*

ПОБУДОВА ГІБРИДНОЇ КРИПТО-КОДОВОЇ КОНСТРУКЦІЇ МАК-ЕЛІСА

Криптографічні системи на алгоритмах несиметричної криптографії (RSA, ECC, DSA) вразливі до атак “грубої сили” з використанням повномасштабного квантового комп’ютера. Тому основні дослідження і розробки криптографічних засобів захисту інформації (КЗЗІ) 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.

Аналіз практичної реалізації алгоритмів шифрування / розшифрування в гібридній крипто-кодовій конструкції (ГККК) Мак-Еліса показує, що досягається зменшення поля до *GF* (*2*[4]) зі збереженням гарантованої стійеості за рахунок використання збиткових кодів та медоів багатоканальної криптографії. Алгоритм формування кодограми (криптограми) що реалізовується за допомогою відповідних пристроїв кодування, та полягає у виконанні наступних кроків:

1. Фіксування кінцевого поля *GF(q)*. Фіксування еліптичної кривої $y^2z+a_1xyz+a_3yz^2=x^3+a_2x^2z+a_4xz+a_6z^3$ і набір її точок $EC(GF(q)):(P_1, P_2, ..., P_N)$ над *GF(q)*. Фіксування підмножини точок $h(GF(q)): (P_{x1}, P_{x2}, ..., P_{xx}),\ h \subseteq EC(GF(q)),\ /h/=x$ і зберігаємо його в секреті.

2. Фіксування вектору ініціалізації $IV=EC–h_j$, h_j – інформаційні символи рівні нулю, $/h/ = \frac{1}{2}k$, т. то. $I_i = 0,\ \forall I_i \in h$;

3. За введеним інформаційним вектором *I* формування кодового слову *c.* Якщо *(n, k, d)* код над *GF(q)* заданий породжувальною матрицею, то $c=I\cdot G$.

4. Формування випадкового вектору помилки *e* такий, що $w(e)\le t,\ \ t = \lfloor (d-1)/2 \rfloor$. Отримання кодового слову шляхом додавання сформованого вектору до кодового слову: $c^*=c+e$.

5. Формування кодограми, шляхом видалення (укорочення) символів вектора ініціалізації, яка поступає на алгоритм *MV2* [3]: $c_X{}^*=c^*–IV$.

6. Формування прапору $CH_D{}^i\ \left\| f(x)_i \right\|$ і залишку $CFT^i\ \left\| C(x)_i \right\|$ на основі алгоритму *MV2*:

$$C_j^* = C_j - C_{k-h_j},\ E_{K_{MV2}} : C_j^* \to \left\| f(x)_i \right\| + \left\| C(x)_i \right\|.$$

Алгоритм розкодування кодограми (криптограми), що реалізовується за допомогою відповідних пристроїв кодування, та полягає у виконанні наступних кроків:

1. Введення кодограми, що підлягає розкодуванню. Осмислення кодограми за алгоритмом *MV2*:

$$E_{K_{MV2}}^{-1} : \left\| f(x)_i \right\| + \left\| C(x)_i \right\| \to C_j.$$

2. Додавання нульових інформаційних символів до отриманої кодограми: $C_j^* = C_j + C_{k-h_j}$;

3. Розкодування отриманого вектору у відповідних пристроях за алгоритмом Берлекемпа-Мессі: $C = M_i \cdot \left(X^u\right)^T \cdot \left(G^{EC}\right)^T + e \cdot \left(D^u\right)^{-1} \cdot \left(P^u\right)^{-1}$, кодограма – суть кодове слово з помилками еліптичного коду. Вага вектора помилок $w(e) \le t$.

4. Формування інформаційного вектору. Для цього у відповідних пристроях отриманий результат розкодування $M_i \cdot \left(X^u\right)^T$ слід помножити на $\left(X^u\right)^{-1}$:

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

Таким чином використовуючи вектор ініціалізації при формуванні кодограми і універсальний механізм заподіяння збитку на основі алгоритму MV2 забезпечується суттєве зменшення довжини кодового слова який поступає в канал зв’язку, тим самим складність формування криптограми зменшується ≈ в 12 разів і розкодування криптограми ≈ в 20 разів зі збереженням стійкості несиметричної крипто-кодової конструкції.

Список літератури

1. С. П. Євсеєв, “Використання кодів пошкоджень у крипто-кодових системах”, *Інформаційні системи,* № 5 (151), с. 109–121, 2017.

2. С. П. Євсеєв, Г. П. Коц, С. В. Мінухін, О. Г. Король, та А В. Холодкова, “Розробка методу багатофакторної аутентифікації на основі гібридних криптокодових конструкцій на дефектних кодах”, *Східноєвропейський журнал передових технологій*, 5/9(89), с. 19 – 35, 2017.

3. С. .П. Євсеєв, Г. П. Коц, та Є. С. Лєкарєв, “Розробка багатофакторного методу аутентифікації на основі модифікованої криптокодової системи Нідеррайтера-Мак\еліса”, *Східноєвропейський журнал передових технологій*, 6/4(84), с. 1, 2010.

ЗМІСТ

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, СУСПІЛЬСТВА ТА ОСОБИСТОСТІ

СЕКЦІЯ 2 ПРОГРАМУВАННЯ ТА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

СЕКЦІЯ 3 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ, МЕДИЦИНІ ТА ОСВІТІ

ТЕЗИ ДОПОВІДЕЙ
Міжнародної науково-практичної конференції
“Інформаційна безпека та інформаційні технології”

“Information Security and Information Technologies”

24–25 квітня 2019 р.

Відповідальний за випуск: *С.П. Євсеєв*

Комп`ютерна верстка: *А.А. Гаврилова*

Підписано до друку 30.03.2017. Формат 60×84/8. Папір офсетний.
Гарнітура «TimesNewRoman». Друк ризографічний. Ум.-друк. арк. – 8,6. Ціна договірна.
Наклад 250 прим.Зам. 0330/9-18

Видавництво «Цифрова друкарня №1»
Свідоцтво суб’єкта видавничої справи: серія ДК № 4354 від 06.07.2012 р.
61001, м. Харків, пл. Повстання, 7/8
e-mail: zebra-zakaz@mail.ru

Віддруковано з готових оригінал-макетів у друкарні ФОП Петров В.В.
Єдиний державний реєстр юридичних осіб та фізичних осіб-підприємців.
Запис № 24800000000106167 від 08.01.2009.
61144, м. Харків, вул. Гв. Широнінців, 79в, к. 137, тел. **(057)778-60-34**e-mail: **bookfabric@rambler.ru**