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 004.056.55

О. С. Циганенко[1], С. П. Євсеєв[1], Б. П. Томашевський[2]

oleksii.tsyhanenko@hneu.net, serhii.yevseiev@hneu.net, bogdan_tomashevsky@tntu.edu.ua

[1]*Харківський національний економічний університет імені Семена Кузнеця, м. Харків*
[2]*Тернопільський національний технічний університет ім. І. Пулюя, м. Тернопіль*

ГІБРИДНА КРИПТО-КОДОВА КОНСТРУКЦІЯ НІДЕРРАЙТЕРА НА ЗБИТКОВИХ КОДАХ

Вступ людства до ери високих технологій стимулює подальше розширення можливостей обчислювальних систем. Стрімке зростання і розширення функціональних можливостей корпоративних систем і соціальних мереж, дозволяє будувати інтегровані соціально-інформаційні мережі для вирішення різноманітного спектра завдань. Подальший розвиток технології передачі даних Ethernet формує глобальну ідеологію побудови телекомунікаційних мереж [1].

Використання модифікованої крипто-кодової конструкції (МККК) Нідеррайтера з додатковими векторами ініціалізації (з множиною неприпустимих позиційних векторів вектора помилок і множиною позицій укорочення вектора помилки) вимагає збільшення швидкодії криптоперетворень системи в цілому. Для цього пропонується використовувати збиткові коди. Збиткові коди дозволяють збільшити швидкість кодових перетворень за рахунок зменшення потужності поля при нанесенні збитку відкритого тексту і зменшити обсяг переданих даних за рахунок нанесення шкоди шифртексту. Такий підхід дозволяє будувати гібридні крипто-кодові конструкції на основі синтезу модифікованих криптокодових конструкцій Нідеррайтера на модифікованих (укорочених або подовжених) кодах на еліптичних кривих з процедурами нанесення збитку. Суттєвою відмінністю від класичних гібридних (комплексних) криптосистем є використання несиметричної криптосистеми для забезпечення безпеки даних з швидкими процедурами криптоперетворень (формування та розкодування кодограми). Використання механізму нанесення збитку MV2 в крипто-кодової конструкції Нідеррайтера на модифікованих еліптичних кодах в Інтернет-технологіях та мобільних мережах, забезпечення практичної реалізації на сучасних платформах та необхідної криптостійкості в умовах постквантової криптографії [2].

Розглянемо формальний опис гібридної математичної моделі несиметричної крипто-кодової конструкція Нідеррайтера на збиткових кодах.

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, $C_n^i = \frac{n!}{i! \cdot (n-1)!}$.

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

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

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

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: $S^*_{r-h_e} = (e_n - h_e) \times H_X^{EC^T}$.

Список літератури

1. Ethernet и промышленные сети [Электронный ресурс]. Доступно: https://www.osp.ru/lan/2013/09/13037411/. Дата обращения: Март 23, 2019.

2. S. Yevseiev, O. Tsyhanenko, A. Gavrilova, V. Guzhva, O. Milov, V. Moskalenko, and et. al, "Development of Niederreiter hybrid crypto-code structure on flawed codes", *Eastern-European Journal of Enterprise Technologies*, 1 (9 (97)), pp. 27–38, 2019.

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**