УДК 004.894:004.023
DOI https://doi.org/10.32782/IT/2025-3-24

Ірина УДОВИК
кандидат технічних наук, доцент, декан факультету інформаційних технологій, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0002-5190-841X*
***Scopus Author ID:** 55998874400*

Володимир ГНАТУШЕНКО
доктор технічних наук, професор, завідувач кафедри інформаційних технологій та комп'ютерної інженерії, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0003-3140-3788*
***Scopus Author ID:** 6505609275*

Іван ЛАКТІОНОВ
доктор технічних наук, професор, професор кафедри програмного забезпечення комп'ютерних систем, Національний технічний університет «Дніпровська політехніка», просп. Дмитра Яворницького, 19, м. Дніпро, Україна, 49005
***ORCID:** 0000-0001-7857-6382*
***Scopus Author ID:** 57194557735*

Сергій ДУНАЄВ
аспірант кафедри кібербезпеки, Національний технічний університет «Харківський політехнічний інститут», вул. Кірпичова, 2, м. Харків, Україна, 61002, serg.dynaev@gmail.com
***ORCID:** 0000-0001-8736-3602*

Бібліографічний опис статті: Удовик, І., Гнатушенко, В., Лактіонов, І., Дунаєв, С. (2025). Розробка методу автентифікації на основі крипто-кодових систем. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 201–212, doi: https://doi.org/10.32782/IT/2025-3-24

РОЗРОБКА МЕТОДУ АВТЕНТИФІКАЦІЇ НА ОСНОВІ КРИПТО-КОДОВИХ СИСТЕМ

Запропоновано метод автентифікації на основі модифікованого алгоритму UMAC на основі крипто-кодових конструкцій Рао-Нама, який забезпечує можливість використання відповідного вектору помилки в крипто-кодовій конструкції та забезпечує швидкість криптоперетворення на рівні симетричних блокових шифрів та криптостійкість на основі NP-повної задачі – декодування випадкового коду.

Метою роботи є розробка методу автентичності у бездротових засобах зв'язку на основі модифікованого алгоритму UMAC на основі крипто-кодових конструкцій Рао-Нама. Такий підхід забезпечує сучасні вимоги щодо швидкості, стійкості та ємності крипто-перетворень під час формування MAC-коду.

***Методологія** забезпечення рішення полягає у використанні теорій захисту інформації, завадостійкого кодування та автентичності. Такий синтез забезпечує формування постквантових алгоритмів автентифікації з мінімальними обчислювальними та ємними потребами.*

***Наукова новизна** отриманих у роботі результатів полягає в побудові принципово нового методу автентичності на основі модифікованого алгоритму UMAC на основі крипто-кодових конструкцій Рао-Нама, що дозволяє його використання в постквантовий період, забезпечує відповідні вимоги щодо стійкості, оперативності та обчислювальних ресурсів.*

***Висновки.** Застосування запропонованого еволюційного методу пошукової оптимізації до мінімізації тестових функцій у неперервному просторі розмірністю до 20 показало його ефективність у порівнянні з відомими раніше. В подальшому актуальним бачиться застосування викладеного алгоритму для розв'язання задач оптимізації технологічних процесів.*

***Ключові слова:** постквантовий алгоритм, автентичність, крипто-кодова конструкція, модифікований алгоритм UMAC.*

Iryna UDOVYK
Candidate of Technical Science, Associate Professor, Dean of Information Technologies Department, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, udovyk.i.m@nmu.one
***ORCID:** 0000-0002-5190-841X*
***Scopus Author ID:** 55998874400*

Volodymyr HNATUSHENKO
Doctor of Technical Science, Professor, Head of the Information Technology and Computer Engineering Department, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, hnatushenko.v.v@nmu.one
***ORCID:** 0000-0003-3140-3788*
***Scopus Author ID:** 6505609275*

Ivan LAKTIONOV
Doctor of Technical Sciences, Professor, Professor at the Department of Software of Computer Systems, Dnipro University of Technology, 19, Dmytra Yavornytskoho Ave., Dnipro, Ukraine, 49005, laktionov.i.s@nmu.one
***ORCID:** 0000-0001-7857-6382*
***Scopus Author ID:** 57194557735*

Sergii DUNAIEV
Postgraduate Student at the Department of Cybersecurity, National Technical University «Kharkiv Polytechnic Institute», 2, Kyrpychova Str., Kharkiv, Ukraine, 61002, serg.dynaev@gmail.com
***ORCID:** 0000-0001-8736-3602*

To cite this article: Udovyk, I., Hnatushenko, V., Laktionov, I., Dunaiev, S. (2025). Rozrobka metodu avtentyfikatsii na osnovi krypto-kodovykh system [Development of an authentication method based on cryptographic code systems]. *Information Technology: Computer Science, Software Engineering and Cyber Security*, 201–212, doi: https://doi.org/10.32782/IT/2025-3-24

DEVELOPMENT OF AN AUTHENTICATION METHOD BASED ON CRYPTOGRAPHIC CODE SYSTEMS

A method of authentication based on a modified UMAC algorithm based on Rao-Nam cryptographic code constructions has been proposed, which provides the possibility of using a corresponding error vector in the cryptographic code construction and ensures the speed of cryptographic transformation at the level of symmetric block ciphers and cryptographic resistance based on an NP-complete problem – decoding of random code.

***The aim of this work** is to develop a method of authenticity in wireless communication based on a modified UMAC algorithm, utilizing Rao-Nam cryptographic code constructions. This approach meets modern requirements for speed, stability, and capacity of cryptographic transformations during MAC code formation.*

***The methodology** for ensuring the solution involves the application of theories related to information protection, noise-resistant coding, and authenticity. Such a synthesis ensures the formation of post-quantum authentication algorithms with minimal computational and capacity requirements.*

***The scientific novelty** of the results obtained in this work lies in the development of a fundamentally new method for authenticity based on a modified UMAC algorithm, utilizing Rao-Nam crypto-code constructions, which enables its application in the post-quantum era and meets the relevant requirements for stability, efficiency, and computational resources.*

***Conclusions.** The application of the proposed evolutionary search optimization method to minimize test functions in a continuous space with dimensions of up to 20 has demonstrated its effectiveness compared to previously known methods. In the future, it seems relevant to apply the presented algorithm to solve optimization problems in technological processes.*

***Key words:** post-quantum algorithm, authenticity, cryptographic code structure, modified UMAC algorithm.*

Актуальність проблеми. Сучасний розвиток смарт-технологій та mesh-мереж, IoT-мереж, та мобільних технологій в умовах постквантового періоду висуває жорсткі вимоги до протоколів, які забезпечують основні послуги безпеки: конфіденційність, цілісність, автентичність. Основою смарт-технологій є інтеграція стандартів бездротових комунікацій з мобільними та комп'ютерними протоколами. Окрім того, технології 4G/5G взаємодіють з різноманітними веб-платформами з урахуванням цифровізації послуг у кіберпросторі, як правило (наприклад,

понад 80 % трафіку в Chrome), використовується мережевий протокол SSL/TLS. Цей протокол ґрунтується на комбінації симетричних алгоритмів шифрування та алгоритмів хешування (в режимі AEAD), що гарантує високий рівень секретності. Проте, цей протокол може бути вразливим до атак типу «Зустріч на середині», POODLE, BEAST, CRIME, BREACH, а також, з розвитком квантових комп'ютерів, існує ймовірність його зламування. Актуальною науково-технічною задачею є вдосконалення цього протоколу та/або побудова додаткових процедур для забезпечення вимог до оперативності, криптостійкості та енергоємності.

Аналіз останніх досліджень і публікацій. Проведений аналіз (Saribas та ін., 2022; Ramraj та ін., 2023; Nie та ін., 2023; Berbecaru та ін., 2023; Wang та ін., 2022; Kottur та ін., 2022; Aayush та ін., 2022; Guo та ін., 2022; Arunkumar та ін., 2022) показав, що попри широке застосування протоколу SSL/TLS v.1.3 у сучасних інфокомунікаційних системах, він залишається вразливим до низки атак, що створює ризики для конфіденційності та цілісності переданих даних.

У роботах (Aayush та ін., 2022; Guo та ін., 2022) зазначається, що навіть із використанням сучасних засобів шифрування протокол піддається атакам типу «людина посередині» та «злий двійник», що зумовлено недосконалістю реалізації модулів WPA у бездротових мережах. Запропоновані системи моніторингу трафіку (TLS-Monitor) дозволяють виявляти відомі вразливості, однак не усувають першопричини їх виникнення.

Автори робіт (Guo та ін., 2022; Arunkumar та ін., 2022) підкреслюють, що попри ключову роль SSL-сертифікатів у забезпеченні безпеки вебресурсів, етап рукостискання залишається найуразливішим – через можливість перехоплення керуючих пакетів, використання бекдорів і експлуатацію особливостей алгоритму 0-RTT. Пропозиції з контролю часових характеристик та структури даних дають змогу виявляти загрози, але не запобігають їм.

З метою підвищення стійкості протоколу в постквантовий період у роботі (Saribas та ін., 2022) запропоновано використання постквантових алгоритмів шифрування. Проте результати експериментів засвідчили значні накладні витрати на обробку повідомлень, що обмежує їх застосування у смарт-пристроях з обмеженими ресурсами.

У дослідженнях (Ramraj та ін., 2023; Nie та ін., 2023; Kottur та ін., 2022) розглядаються практичні аспекти застосування SSL/TLS у соціальних мережах, месенджерах та мережах 4G/5G. Виявлено, що, попри впровадження наскрізного шифрування, аналіз трафіку все ще може розкривати частину службової інформації. Запропоновані рішення на основі смарт-мережевих адаптерів або динамічної генерації сертифікатів не забезпечують достатнього рівня стійкості у постквантовий період.

Альтернативні підходи, як-от безсертифікатний протокол сліпої реєстрації (CLS-BPR) (Bertók та ін., 2022), базуються на криптографії з ідентифікаторами та ускладнюють офлайн-атаки, але їхня надійність обмежена невизначеною стійкістю білінійних карт. У роботі (Arunkumar та ін., 2022) рекомендовано використовувати еліптичні криві для підвищення рівня захисту в електронній комерції, проте не враховано енергоефективність та швидкодію таких алгоритмів у мобільних середовищах.

Таким чином, узагальнений аналіз показує, що для мінімізації загроз протоколу SSL/TLS на сьогодні пропонуються два основні напрями: моніторинг мережевого трафіку або впровадження постквантових і еліптичних криптографічних алгоритмів. Проте перший підхід не усуває причин виникнення атак, а другий не забезпечує необхідного рівня швидкодії та непридатний для використання у смарт-технологіях із обмеженими обчислювальними ресурсами.

Мета дослідження: розробка методу автентифікації на основі вдосконаленого протоколу SSL/TLS із використанням постквантових алгоритмів Рао-Нама. Такий підхід спрощує етап рукостискання, не вимагає значних обчислювальних ресурсів і забезпечує необхідний рівень безпеки.

Для досягнення мети роботи необхідно вирішити такі завдання:

– розробка крипто-кодових конструкцій Рао-Нама на основі еліптичних (EC), модифікованих (MEC), збиткових та LDPC-кодів;

– розробка інтегрованих алгоритмів забезпечення конфіденційності, цілісності та автентичності на основі постквантових алгоритмів для протоколу SSL/TLS на основі алгеброгеометричних та збиткових кодах.

Виклад основного матеріалу. Крипто-кодові конструкції забезпечують побудову симетричних та несиметричних криптосистем на основі синтезу теорії завадостійкого кодування та теорії захисту інформації. Такий підхід гарантує їх використання в умовах появи повномасштабного квантового комп'ютера та використання алгоритмів Гровера та Шора. При цьому в якості закритого ключа у кожного користувача несиметричних криптосистем (Мак-Еліса та Нідеррайтера) використовуються

матриці маскування, а в симетричній криптосистемі Рао-Нама – породжувальна матриця та/або переставна матриця. Несиметричні крипто-кодові конструкції за швидкістю криптоперетворень порівнянні зі швидкістю криптоперетворень симетричних блокових шифрів, при цьому забезпечується доказова криптостійкість на основі NP-повної задачі – декодування випадкового коду. Симетрична крипто-кодова конструкція Рао-Нама забезпечує у 4–5 разів швидше криптоперетворення ніж у несиметричних криптосистем.

Основним недоліком криптосхем Рао-Нама є недостатня стійкість до зламу в період появи повномасштабного квантового комп'ютера та велика кількість об'єму ключових даних, а також злам «атакою із використання структурних особливостей секретного ключа криптосистеми» – знаходження елементів породжувальної матриці. За рахунок ортогональності породжувальної та перевірочної матриць ця атака дозволяє злам як ККК Мак-Еліса, так й ККК Нідеррайтера на збиткових кодах (Çalkavur, 2022; Minder та ін., 2007).

Поєднання геометричних параметрів еліптичних кривих (EC) (точки кривої) з математичним апаратом завадостійкого кодування (матриця Вейєрштрасса) забезпечують формування алгеброгеометричних кодів. Крім цього, в якості додаткового вектора ініціалізації крім точок еліптичної кривої, використовуються незвідні коефіцієнти рівняння кривої. Цей вектор ініціалізації дозволяє визначати рівняння за яким формується породжувальна та/або перевіркова матриця, та може бути використаний у якості ключової послідовності (Yevseiev та ін., 2018; Yevseiev та ін., 2016; Couvreur та ін., 2014; Yevseiev та ін., 2017a; Yevseiev та ін., 2017b).

Для побудови використовується породжувальна матриця, елементами якої є проєктивні точки Pi(Xi, Yi, Zi). Значення генераторних функцій від визначених точок забезпечує формування породжувальної матриці еліптичного коду (Yevseiev та ін., 2018; Yevseiev та ін., 2016; Couvreur та ін., 2014; Yevseiev та ін., 2017a; Yevseiev та ін., 2017b), яка визначена виразом:

$$G = \begin{pmatrix} F_0(P_0) & F_0(P_1) & \dots & F_0(P_{n-1}) \\ F_1(P_0) & F_1(P_1) & \dots & F_1(P_{n-1}) \\ \dots & \dots & \dots & \dots \\ F_{k-1}(P_0) & F_{k-1}(P_1) & \dots & F_{k-1}(P_{n-1}) \end{pmatrix} = \left\| F_j(P_i) \right\|_{n,k}, \quad (1)$$

При цьому в афінному просторі A^2 над полем *GF(q)* еліптична крива задається виразом (Yevseiev та ін., 2018; Yevseiev та ін., 2016; Couvreur та ін., 2014; Yevseiev та ін., 2017a; Yevseiev та ін., 2017b):

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (2)$$

або у проєкційному просторі P^2 (Yevseiev та ін., 2018; Yevseiev та ін., 2016; Couvreur та ін., 2014; Yevseiev та ін., 2017a; Yevseiev та ін., 2017b):

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz + a_6z^3, \quad (3)$$

$a_i \in GF(q)$, род кривої $g = 1$.

Загальна кількість точок кривої визначається теоремою Хасе-Веля (Yevseiev та ін., 2018; Yevseiev та ін., 2016; Couvreur та ін., 2014; Yevseiev та ін., 2017a; Yevseiev та ін., 2017b):

$$N \le 2\sqrt{q} \cdot g + q + 1, \quad (4)$$

де g – род кривої, $q = p^m$ поля Галуа.

Таким чином, теорема (межа) Хасе-Веля визначає максимальну кількість точок, які можуть бути визначені у якості елементів еліптичного коду. Алгеброгеометричний (*n, k, d*)-код задає наступні параметри завадостійкого коду: $k + d \ge n$, $n \le 2\sqrt{q} + q + 1$, $k \ge \alpha$, $d \ge n - \alpha$, $\alpha = 3 \times degF$ (Yevseiev та ін., 2018; Yevseiev та ін., 2016; Couvreur та ін., 2014; Yevseiev та ін., 2017a; Yevseiev та ін., 2017b). Для забезпечення криптостійкості спеціалісти НІСТ (Національний інститут стандартів та технологій) США рекомендують будувати ККК із використанням завадостійких кодів з елементами на *GF* (210–213), що дуже складно практично реалізувати в смартфонах та мобільних технологіях (Ramraj та ін., 2023; Nie та ін., 2023). Таким чином, необхідний підхід щодо скорочення множини поля Галуа зі збереженням рівня криптостійкості системи у цілому.

Для побудови симетричної криптосистеми на основі крипто-кодової конструкції Рао-Нама на *EC* визначимо:

G^{EC} – породжувальна матриця еліптичного коду розмірністю $k \times n$ над $GF(q)$ – секретний ключ криптосистеми;

Криптограма (кодограма) є вектором довжини n та обчислюється за формулою:

$$c^* = i \times G^{EC} + e, \quad (5)$$

де вектор $c^* = i \times G^{EC}$ належить (*n, k, d*)-коду, i – k-розрядний інформаційний вектор, вектор e – секретний вектор помилок вагою $\le t$ (виправна здатність коду). Схему передачі секретного повідомлення від абонента А до абонента В у симетричній криптосистемі на основі схеми Рао-Нама із використанням еліптичних кодів наведено (рис. 1).

Для побудови симетричної криптосистеми на основі модифікованої крипто-кодової конструкції Рао-Нама на EC визначимо:

G^{EC} – породжувальна матриця *EC* розмірністю $k \times n$ над $GF(q)$, Z – переставна матриця (у кожному стовбці та строки одна одиниця)

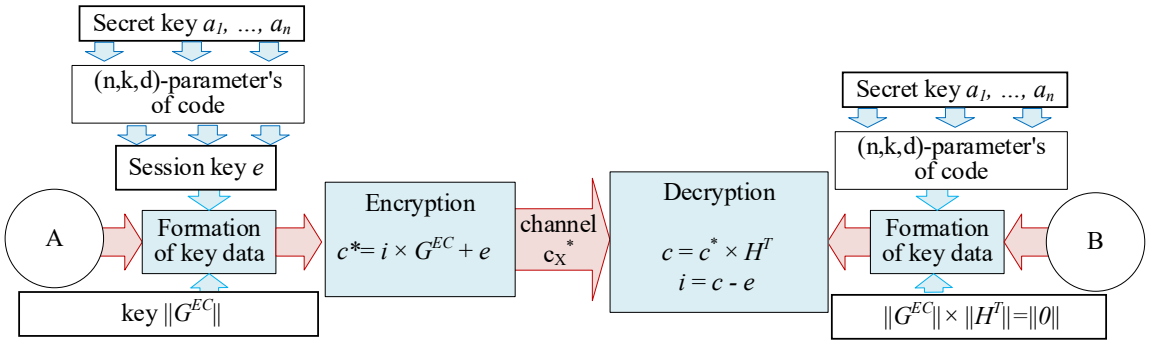

Рис. 1. Структурна схема крипто-кодової конструкції Рао-Нама з використанням еліптичних кодів

розмірністю $n \times n$ – матриця маскування. Матриці G^{EC} та Z – секретний ключ криптосистеми. Криптограма (кодограма) є вектором довжини n та визначена та наведена на рис. 2.

$$c^* = (i \times G^{EC} + e) \times Z \qquad (6)$$

Запропонований підхід забезпечує необхідний рівень стійкості та вірогідності за рахунок використання завадостійкого алгеброгеометричного коду. *EC* (n, k, d)-код над $GF(q)$ задає наступні параметри: $k + d \geq n$, $n\ 2\sqrt{g} + q + 1$, $k \geq \alpha$, $d \geq n - \alpha$, $\alpha = 3 \times degF$. Складність алгоритму несистематичного кодування формально складає $O(3 \times degF \times n)$ або $O((n–d) \times n)$ (рис. 2).

Для скорочення розміру ключових даних та потужності поля (при заданому рівні стійкості) в (Yevseiev та ін., 2018; Yevseiev та ін., 2016; Couvreur та ін., 2014; Yevseiev та ін., 2017a; Yevseiev та ін., 2017b) пропонується використовувати модифіковані еліптичні коди (*MEC*).

Способи модифікації завадостійкого кодування забезпечують параметри (n, k, d) лінійного блокового коду зі змінами (Yevseiev та ін., 2017a; Yevseiev та ін., 2017b). На рис. 3 наведені найбільш поширені способи модифікації.

При цьому для забезпечення необхідного рівня стійкості серед параметрів завадостійкого коду необхідно зафіксувати параметр d – конструктивна відстань, яка визначає кількість визначення та виправлення помилок у кодовому слові (Yevseiev та ін., 2017a; Yevseiev та ін., 2017b; Tsyhanenko та ін., 2018; Massey, 1985).

Таким чином, для забезпечення необхідного рівня стійкості ККК Рао-Нама необхідно використовувати способи модифікації, що не допускають зниження мінімальної кодової відстані (Yevseiev та ін., 2017a; Yevseiev та ін., 2017b; Tsyhanenko та ін., 2018; Massey, 1985). Проведений аналіз, результати якого наведено на (рис. 3), показав, що d (конструктивна відстань) не змінюється при використанні параметрів завадостійкого коду при їх скорочені (скорочується кількість символів у кодовому слові).

Для подальшого скорочення обчислювальної ємності та об'єму ключових даних пропонується використовувати модифіковані *EC* (*MEC*) – скорочені та подовжені. Такий підхід забезпечує зменшення потужності поля для побудови ККК Рао-Нама до *GF* (26–28). На (рис. 4 і 5) наведено протоколи обміну на основі симетричної криптосистеми Рао-Нама на *MEC* (скорочених, подовжених), (на рис. 6 і 7) – на основі модифікованої схеми Рао-Нама на MEC (скорочених, подовжених).

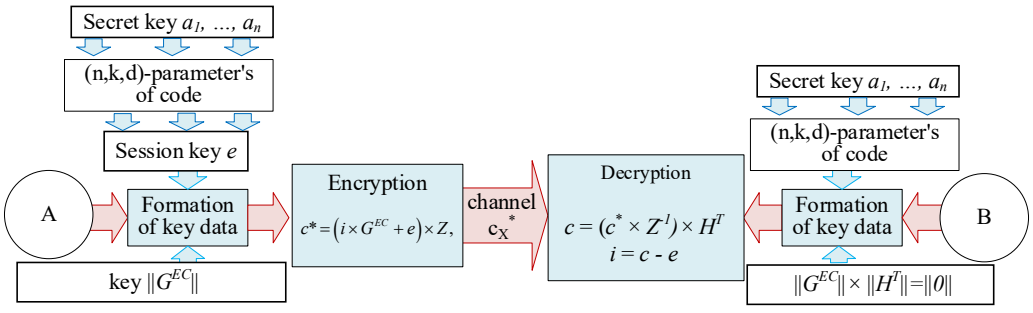

Рис. 2. Структурна схема модифікованої крипто-кодової конструкції Рао-Нама з використанням еліптичних кодів

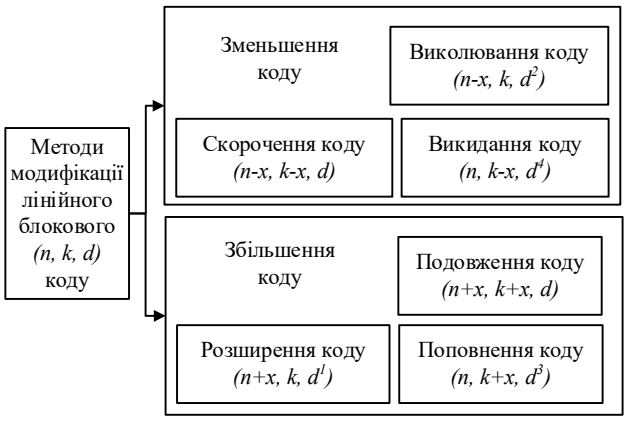

Рис. 3. Способи модифікації блокових кодів

Для подальшого зменшення енергоємності та збереження рівня криптостійкості пропонується використання збиткових кодів, які забезпечують багатоканальні методи криптографічного перетворення (Evseev, 2017). Для використання запропонованих крипто-кодових конструкцій над полями Галуа (2^4–2^6), що забезпечує зменшення об'єму ключових даних пропонується використовувати збиткові коди, які будують гібридні (комплексні) криптосистеми. Збиткова криптографія – багатоканальна криптографія, яка забезпечує в такому випадку додаткову ентропію та криптостійкість системи у цілому. Криптографічними збитковими текстами називаються тексти, отримані такими способами (Evseev, 2017):

– підхід 1: нанесення збитку початковому тексту з подальшим шифруванням збиткового тексту і / або його збитків;

– підхід 2: нанесення збитку шифртексту;

– підхід 3: нанесення збитку вихідному тексту і шифртексту збиткового тексту. Проведений аналіз використання алгоритму MV2 (алгоритму нанесення збитку) показав, що кращий результат забезпечується при виконанні наступних послідовностей – з початку шифрування у ККК Рао-Нама, потім нанесення збитку до шифртексту (підхід 3). На рис. 8, 9 наведені протоколи обміну інформацією у гібридної симетричної криптосистемі на основі ККК, (модифікованої ККК) Рао-Нама на МЕС (скорочені коди).

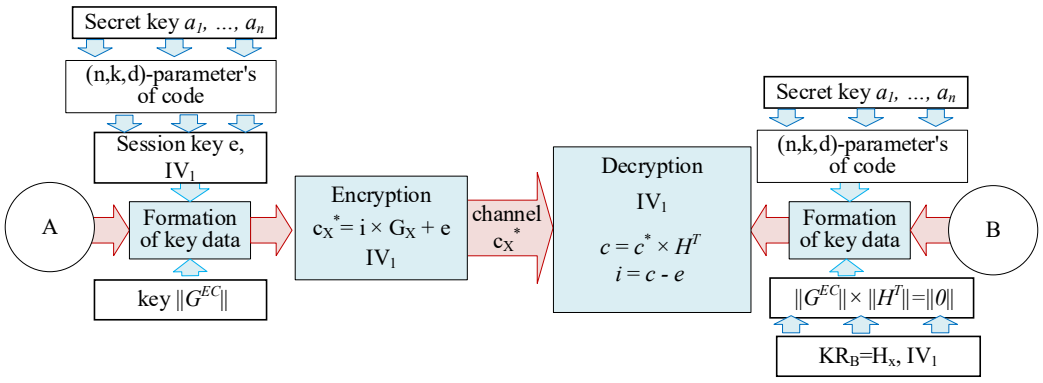

Рис. 4. Структурна схема крипто-кодової конструкції Рао-Нама з використанням модифікованих (скорочених) еліптичних кодів

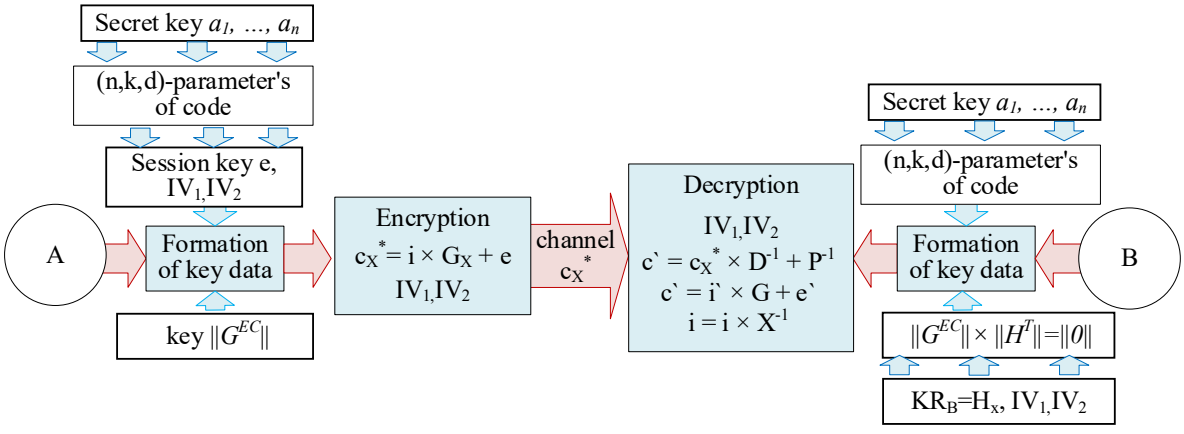

Рис. 5. Структурна схема крипто-кодової конструкції Рао-Нама з використанням модифікованих (подовжених) еліптичних кодів

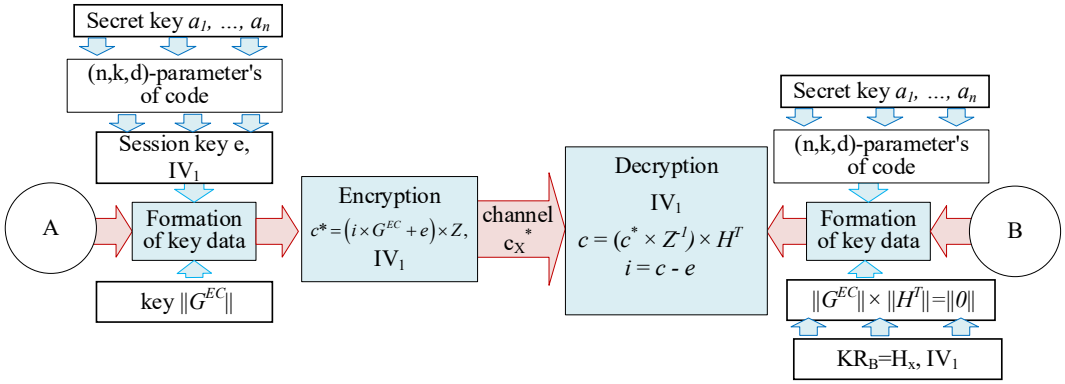

Рис. 6. Структурна схема модифікованої крипто-кодової конструкції Рао-Нама з використанням модифікованих (скорочених) еліптичних кодів

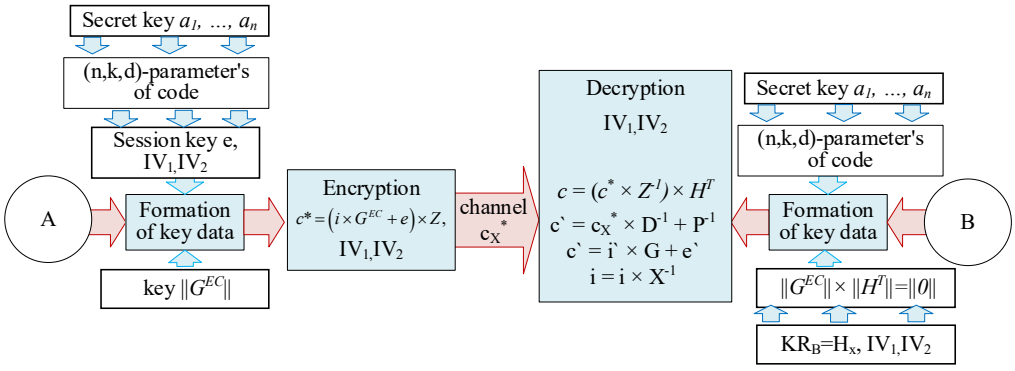

Рис. 7. Структурна схема модифікованої крипто-кодової конструкції Рао-Нама з використанням модифікованих (подовжених) еліптичних кодів

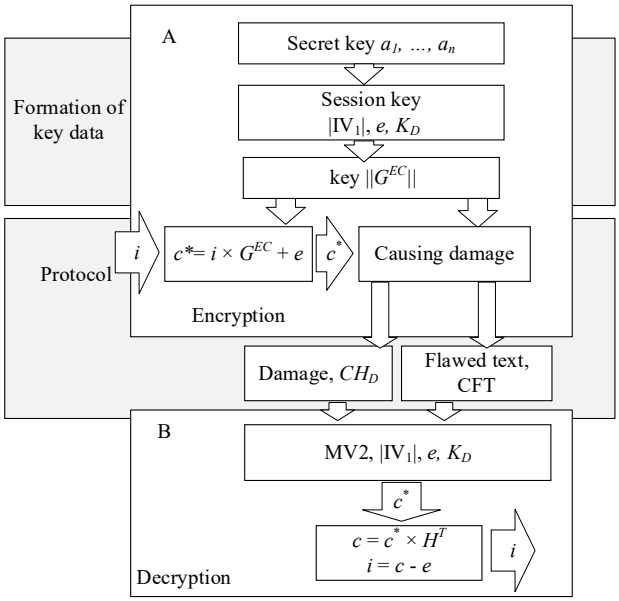

Рис. 8. Протокол обміну інформацією у гібридній симетричній криптосистемі на основі крипто-кодової конструкції Рао-Нама на модифікованих еліптичних кодах *(скорочені коди)*

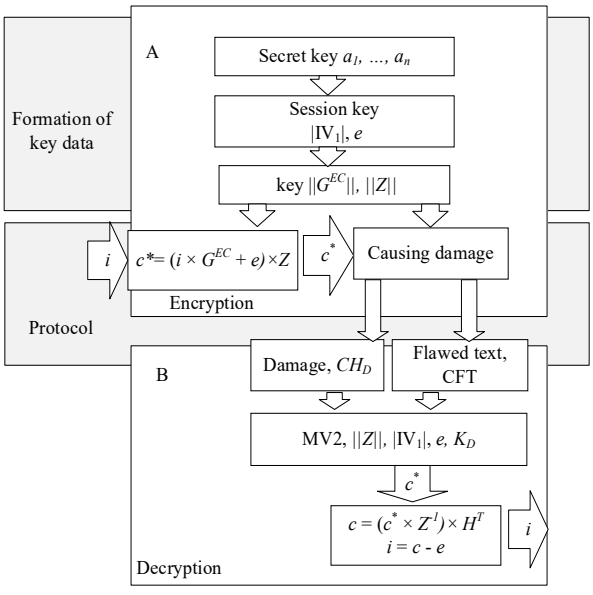

Рис. 9. Протокол обміну інформацією у гібридній симетричній криптосистемі на основі модифікованої крипто-кодової конструкції Рао-Нама на модифікованих еліптичних кодах *(скорочені коди)*

Запропонований підхід забезпечує необхідний рівень криптографічної стійкості завдяки використанню багатоканальної криптографії на основі збиткових кодів. Така архітектура дозволяє підвищити вірогідність функціонування системи та суттєво зменшити обсяг ключових даних, необхідних для встановлення безпечного з'єднання.

Додатково, для оптимізації процесу обміну ключовими параметрами та підвищення рівня їх захищеності, передбачається передача між учасниками протоколу лише коефіцієнтів рівняння еліптичної кривої без усього кортежу векторів ключових даних. Такий механізм дозволяє мінімізувати обсяг переданої службової інформації, зменшити навантаження на канали зв'язку та підвищити стійкість системи до криптоаналітичних атак.

У результаті запропонований підхід поєднує ефективність використання ресурсів із високим рівнем інформаційної безпеки, що робить його перспективним для застосування у смарт-технологіях та кіберзахисних системах нового покоління.

В основу формування компенсованого алгоритму надання послуг безпеки в протоколі SSL/

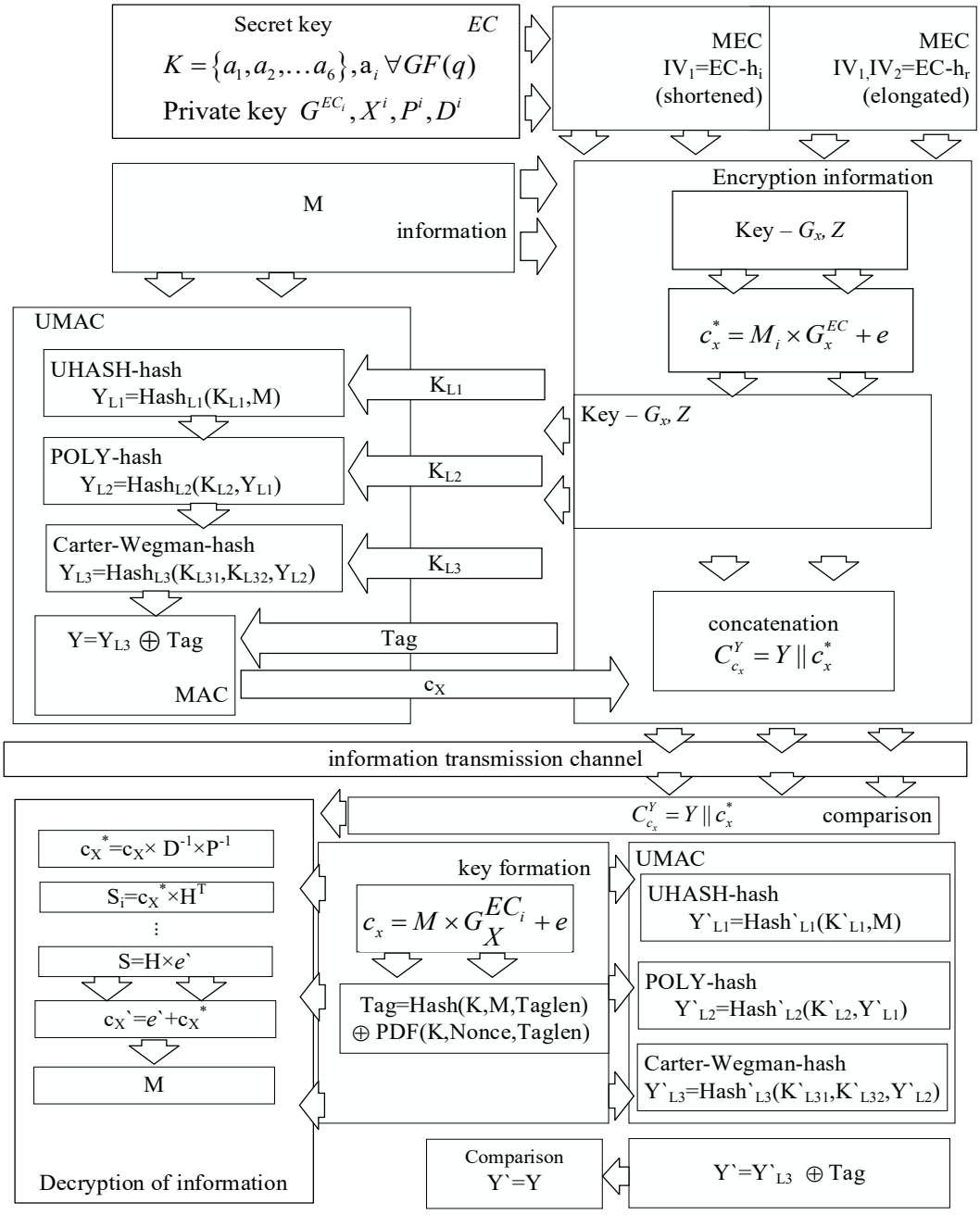

Рис. 10. Структурна схема формування автентифікованого повідомлення

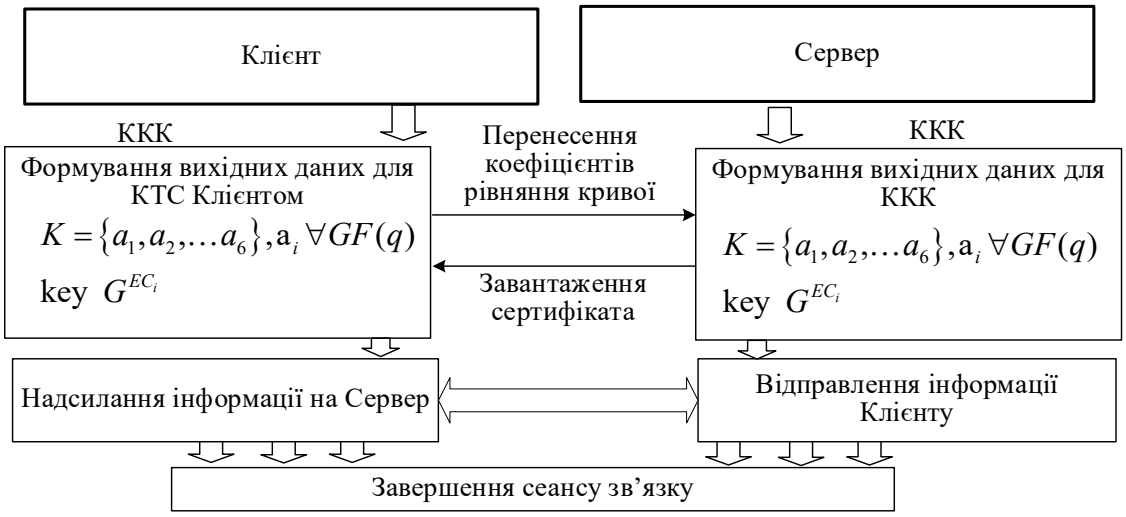

Рис. 11. Структурна схема протоколу SSL/TLS на основі ККК Рао-Нама

TLS запропоновано використовувати синтез алгоритмів постквантової криптографії з удосконаленим алгоритмом UMAC, що забезпечить необхідний рівень міцності, ефективності та надійності в постквантовий криптоперіод. При цьому відмінною рисою запропонованого підходу є зміна принципу формування автентифікованого повідомлення. На початку дані подаються в алгоритм каскадного хешування, а паралельно генеруються параметри для структур криптокоду та векторів ініціалізації модифікованих еліптичних кодів. Такий підхід забезпечує максимальну швидкість конвертації та дозволяє розпаралелювати завдання шифрування та генерації МАС-коду. На приймальній стороні перетворення також виконуються в паралельному режимі, що забезпечує необхідний рівень ефективності. На рис. 10 представлена блок-схема формування автентифікованого повідомлення та у вигляді алгоритму:

Крок 1. Генерація закритого ключа сесії: вибір параметрів еліптичної кривої:

$$K = \{a_1, a_2, \ldots a_6\}, a_i \forall GF(q)$$
$$\text{Private key } G^{EC_i}, X^i, P^i, D^i, e. \quad (7)$$

За необхідності формуються вектори ініціалізації – IV1, IV2 (для параметризації та генерації скорочених та/або розширених модифікованих еліптичних кодів. Введення інформації до першого рівня алгоритма UMAC:

$$\begin{aligned} Hash_{L1_i} &= Hash_{L1_i} +_{64} ((M_{i_{j+0}} +_{32} K_{L1_{j+0}}) \times_{64} (M_{i_{j+4}} +_{32} K_{L1_{j+4}})), \\ Hash_{L1_i} &= Hash_{L1_i} +_{64} ((M_{i_{j+1}} +_{32} K_{L1_{j+1}}) \times_{64} (M_{i_{j+5}} +_{32} K_{L1_{j+5}})), \\ Hash_{L1_i} &= Hash_{L1_i} +_{64} ((M_{i_{j+2}} +_{32} K_{L1_{j+2}}) \times_{64} (M_{i_{j+6}} +_{32} K_{L1_{j+6}})), \\ Hash_{L1_i} &= Hash_{L1_i} +_{64} ((M_{i_{j+3}} +_{32} K_{L1_{j+3}}) \times_{64} (M_{i_{j+7}} +_{32} K_{L1_{j+7}})). \end{aligned} \quad (8)$$

Крок 2. Генерація хеш-коду на другому рівні алгоритму каскадного хешування $Y_{L2} = \left(M_{P_n} + kM_{P_{n-1}} + \ldots + k^{n-1}M_{P_1} + k^n\right) \bmod(p)$, який обчислюється за допомогою ітераційної процедури (для всіх i = 1, 2, ..., n): $Poly_i = \left(kPoly_{i-1} + M_{P_i}\right) \bmod(p), Poly_0 = 1, p = prime(Wordbits)$, за схемою Горнера:

$$M_{P_n} + kM_{P_{n-1}} + \ldots + k^{n-1}M_{P_1} + k^n = (((k + M_{P_1})k + M_{P_2})k + \ldots + M_{P_{n-1}})k + M_{P_n} \quad (9)$$

Крок 3. Шифрування відкритого тексту M на основі МЕС у дизайні криптокоду Рао-Нама:

$$c_x^* = M_i \times G_X^{EC_i} + e, \quad (10)$$

Генерація МАС-коду за допомогою Pad на основі QKK на МЕС:

$$Y_{L3} = \left(\left(\left(\sum_{i=1}^{m} Y_{L2_i} K_{L3_{1i}}\right) \bmod(prime(36))\right) \bmod(2^{32})\right) xor(K_{L3_2}),$$
$$Y = Y_{L3} \oplus Pad. \quad (11)$$

Крок 4. Створення автентифікованого повідомлення на основі алгоритму конкатенації:

$$C_{c_x}^Y = Y \,||\, c_x^*. \quad (12)$$

Структурна схема протоколу SSL/TLS на основі ККК Рао-Нама наведена на (рис. 11).

Висновки і перспективи подальших досліджень. У цій статті запропоновано метод автентифікації, який гарантує необхідний рівень криптографічної стійкості завдяки застосуванню багатоканальної криптографії, побудованої на основі збиткових кодів. Такий підхід підвищує надійність функціонування системи та водночас зменшує обсяг ключових даних, що використовуються під час встановлення захищеного з'єднання.

Для додаткового підвищення рівня безпеки та оптимізації процесу обміну ключовими параметрами пропонується передавати між сторонами протоколу лише коефіцієнти рівняння еліптичної кривої, без усього набору векторів ключових даних. Це дозволяє істотно скоротити обсяг службової інформації, знизити навантаження на канали зв'язку та підвищити стійкість системи до криптоаналітичних впливів.

Таким чином, запропоноване рішення поєднує високу ефективність використання обчислювальних ресурсів із посиленим рівнем інформаційної безпеки, що робить його доцільним для впровадження у смарт-системах і технологіях кіберзахисту нового покоління.

Запропонований удосконалений протокол транспортного рівня SSL/TLS базується на комплексних алгоритмах – крипто-кодових конструкціях Рао-Нама на основі МЕС (збиткових кодів) у поєднанні з удосконаленим каскадним алгоритмом хешування. Такий підхід суттєво знижує вплив відомих вразливостей протоколу SSL/TLS за рахунок використання лише несиметричних криптосистем та спрощення фази «рукостискання».

Запропоноване удосконалення усуває необхідність попереднього обміну окремим ключем перед передачею даних, а також використання несиметричних алгоритмів шифрування для обміну ключовими даними (сертифікатами). При цьому забезпечується необхідний рівень криптостійкості в постквантовий криптографічний період, а також оптимізуються обчислювальні та енергетичні витрати, що робить протокол придатним для застосування в кіберфізичних системах на основі смарт-технологій.

Статтю підготовлено в рамках проєкту 2025.06/0047 «Інформаційні технології криптографічного захисту й автентифікації даних для систем мобільного та супутникового зв'язку» (№ держреєстрації 0125U003538), що фінансується Національним фондом досліджень України.

ЛІТЕРАТУРА:

1. Saribas S., Tonyali S. Performance Evaluation of TLS 1.3 Handshake on Resource-Constrained Devices Using NIST's Third Round Post-Quantum Key Encapsulation Mechanisms and Digital Signatures. In: *Proceedings – 7th International Conference on Computer Science and Engineering*, 2022. P. 294–299. https://doi.org/10.1109/UBMK55850.2022.9919545.

2. Ramraj S., Usha G. Signature identification and user activity analysis on WhatsApp Web through network data. *Microprocessors and Microsystems*, 2023. Vol. 97. P. 1–12. https://doi.org/10.1016/j.micpro.2023.104756.

3. Nie P., Wan C., Zhu J., Lin Z., Chen Y., Su Z. Coverage-directed Differential Testing of X.509 Certificate Validation in SSL/TLS Implementation. *ACM Transactions on Software Engineering and Methodology*, 2023. Vol. 32 (1). P. 1–32. https://doi.org/10.1145/3510416.

4. Berbecaru D. G., Petraglia G. TLS-Monitor: A Monitor for TLS Attacks. In: *Proceedings – IEEE Consumer Communications and Networking Conference*, 2023. P. 1–6. https://doi.org/10.1109/CCNC51644.2023.10059989.

5. Wang K., Zheng Y., Zhang Q., Bai G., Qin M., Zhang D., Dong J. S. Assessing certificate validation user interfaces of WPA supplicants. In: *Proceedings of the Annual International Conference on Mobile Computing and Networking*, 2022. P. 501–513. https://doi.org/10.1145/3495243.3517026.

6. Kottur S. Z., Kadiyala K., Tammana P., Shah R. Implementing ChaCha based crypto primitives on programmable SmartNICs. In: *FFSPIN 2022 – Proceedings of the ACM SIGCOMM 2022 Workshop on Formal Foundations and Security of Programmable Network Infrastructures*, 2022. P. 15–23. https://doi.org/10.1145/3528082.3544833.

7. Aayush A., Aryan Y., Muniyal B. Understanding SSL Protocol and Its Cryptographic Weaknesses. In: *Proceedings of 3rd International Conference on Intelligent Engineering and Management*, 2022. P. 825–832. https://doi.org/10.1109/ICIEM54221.2022.9853153.

8. Guo S., Zhang F., Song Z., Zhao Z., Zhao X., Wang X., Luo X. Detection of SSL/TLS protocol attacks based on flow spectrum theory. *Chinese Journal of Network and Information Security*, 2022. Vol. 8 (1). P. 30–40. https://doi.org/10.11959/j.issn.2096-109x.2022004.

9. Arunkumar B., Kousalya G. Secure and light weight elliptic curve cipher suites in SSL/TLS. *Computer Systems Science and Engineering*, 2022. Vol. 40 (1). P. 179–190. https://doi.org/10.32604/CSSE.2022.018166.

10. Bertók C., Huszti A., Kovács S., Oláh N. Provably secure identity-based remote password registration. *Publicationes Mathematicae*, 2022. Vol. 100. P. 533–565. https://doi.org/10.5486/PMD.2022.Suppl.1.

11. Çalkavur S. Public-Key Cryptosystems and Bounded Distance Decoding of Linear Codes. *Entropy*, 2022. Vol. 24 (4). P. 1–9. https://doi.org/10.3390/e24040498.

12. Minder L., Shokrollahi A. Cryptanalysis of the Sidelnikov Cryptosystem. *Advances in Cryptology – EUROCRYPT* 2007. *Lecture Notes in Computer Science*, 2007. Vol. 4515. P. 347–360. https://doi.org/10.1007/978-3-540-72540-4_20.

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

14. Yevseiev S., Hryhorii K., Liekariev Y. Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system. *Eastern-European Journal of Enterprise Technologies*, 2016. Vol. 6 (4 (84)). P. 11–23. https://doi.org/10.15587/1729-4061.2016.86175.

15. Couvreur A., Otmani A., Tillich J. Polynomial Time Attack on Wild McEliece over Quadratic Extensions. *Advances in Cryptology – EUROCRYPT 2014. Lecture Notes in Computer Science*, 2014. Vol. 8441. P. 17–39. https://doi.org/10.1007/978-3-642-55220-5_2.

16. Yevseiev S., Korol O., Kots H. Construction of hybrid security systems based on the crypto-code structures and flawed codes. *Eastern-European Journal of Enterprise Technologies*, 2017a. Vol. 4 (9 (88)). P. 4–21. https://doi.org/10.15587/1729-4061.2017.108461.

17. Yevseiev S., Tsyhanenko O., Gavrilova A., Guzhva V., Milov O., Moskalenko V. et al. Development of Niederreiter hybrid crypto-code structure on flawed codes. *Eastern-European Journal of Enterprise Technologies*, 2017b. Vol. 1 (9 (97)). P. 27–38. https://doi.org/10.15587/1729-4061.2019.156620.

18. Tsyhanenko O., Rzayev K., Mammadova T. Mathematical model of the modified niederreiter crypto-code structures. *Advanced Information Systems*, 2018. Vol. 2 (4). P. 37–44. https://doi.org/10.20998/2522-9052.2018.4.06.

19. Massey J. Review of 'Theory and Practice of Error Control Codes' (Blahut, R.E.; 1983). *IEEE Transactions on Information Theory*, 1985. Vol. 31 (4). P. 553–554. https://doi.org/10.1109/TIT.1985.1057072.

20. Evseev S. P. The use of defective codes in cryptographic code systems. *Sistemi obrobki informacii*, 2017. Vol. 5. P. 109–121. https://doi.org/10.30748/soi.2017.151.15.

REFERENCES:

1. Saribas, S., Tonyali, S. (2022). Performance Evaluation of TLS 1.3 Handshake on Resource-Constrained Devices Using NIST's Third Round Post-Quantum Key Encapsulation Mechanisms and Digital Signatures. In: *Proceedings – 7th International Conference on Computer Science and Engineering*. P. 294–299.

2. Ramraj, S., Usha, G. (2023). Signature identification and user activity analysis on WhatsApp Web through network data. *Microprocessors and Microsystems*, 97. P. 1–12.

3. Nie, P., Wan, C., Zhu, J., Lin, Z., Chen, Y., Su, Z. (2023). Coverage-directed Differential Testing of X.509 Certificate Validation in SSL/TLS Implementation. *ACM Transactions on Software Engineering and Methodology*, 32 (1). P. 1–32.

4. Berbecaru, D. G., Petraglia, G. (2023). TLS-Monitor: A Monitor for TLS Attacks. In: *Proceedings – IEEE Consumer Communications and Networking Conference*. P. 1–6.

5. Wang, K., Zheng, Y., Zhang, Q., Bai, G., Qin, M., Zhang, D., Dong, J. S. (2022). Assessing certificate validation user interfaces of WPA supplicants. In: *Proceedings of the Annual International Conference on Mobile Computing and Networking*. P. 501–513.

6. Kottur, S. Z., Kadiyala, K., Tammana, P., Shah, R. (2022). Implementing ChaCha based crypto primitives on programmable SmartNICs. In: *FFSPIN 2022 – Proceedings of the ACM SIGCOMM 2022 Workshop on Formal Foundations and Security of Programmable Network Infrastructures*. P. 15–23.

7. Aayush, A., Aryan, Y., Muniyal, B. (2022). Understanding SSL Protocol and Its Cryptographic Weaknesses. In: *Proceedings of 3rd International Conference on Intelligent Engineering and Management*. P. 825–832.

8. Guo, S., Zhang, F., Song, Z., Zhao, Z., Zhao, X., Wang, X., Luo, X. (2022). Detection of SSL/TLS protocol attacks based on flow spectrum theory. *Chinese Journal of Network and Information Security*, 8 (1). P. 30–40.

9. Arunkumar, B., Kousalya, G. (2022). Secure and light weight elliptic curve cipher suites in SSL/TLS. *Computer Systems Science and Engineering*, 40 (1). P. 179–190.

10. Bertók, C., Huszti, A., Kovács, S., Oláh, N. (2022). Provably secure identity-based remote password registration. *Publicationes Mathematicae*, 100. P. 533–565.

11. Çalkavur, S. (2022). Public-Key Cryptosystems and Bounded Distance Decoding of Linear Codes. *Entropy*, 24 (4). P. 1–9.

12. Minder, L., Shokrollahi, A. (2007). Cryptanalysis of the Sidelnikov Cryptosystem. *Advances in Cryptology – EUROCRYPT* 2007. *Lecture Notes in Computer Science*, 4515. P. 347–360.

13. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et al. (2018). Practical implementation of the Niederreiter modified cryptocode system on truncated elliptic codes. *Eastern-European Journal of Enterprise Technologies*, 6 (4 (96)). P. 24–31.

14. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system. *Eastern-European Journal of Enterprise Technologies*, 6 (4 (84)). P. 11–23.

15. Couvreur, A., Otmani, A., Tillich, J. (2014). Polynomial Time Attack on Wild McEliece over Quadratic Extensions. *Advances in Cryptology – EUROCRYPT 2014. Lecture Notes in Computer Science*, 8441. P. 17–39.

16. Yevseiev, S., Korol, O., Kots, H. (2017a). Construction of hybrid security systems based on the crypto-code structures and flawed codes. *Eastern-European Journal of Enterprise Technologies*, 4 (9 (88)). P. 4–21.

17. Yevseiev, S., Tsyhanenko, O., Gavrilova, A., Guzhva, V., Milov, O., Moskalenko, V. et al. (2017b). Development of Niederreiter hybrid crypto-code structure on flawed codes. *Eastern-European Journal of Enterprise Technologies*, 1 (9 (97)). P. 27–38.

18. Tsyhanenko, O., Rzayev, K., Mammadova, T. (2018). Mathematical model of the modified Niederreiter crypto-code structures. *Advanced Information Systems*, 2 (4). P. 37–44.

19. Massey, J. (1985). Review of 'Theory and Practice of Error Control Codes' (Blahut, R.E.; 1983). *IEEE Transactions on Information Theory*, 31 (4). P. 553–554.

20. Evseev, S.P. (2017). The use of defective codes in cryptographic code systems. *Sistemi obrobki informacii*, 5. P. 109–121.

Дата надходження статті: 25.09.2025
Дата прийняття статті: 22.10.2025
Опубліковано: 28.11.2025