ISSN 2307-5732
DOI 10.31891/2307-5732

НАУКОВИЙ ЖУРНАЛ **1.2022**

ВІСНИК

Хмельницького національного університету

Технічні науки

Technical sciences

SCIENTIFIC JOURNAL
HERALD OF KHMELNYTSKYI NATIONAL UNIVERSITY

2022, Issue 1, Volume 305

Хмельницький

ВІСНИК
ХМЕЛЬНИЦЬКОГО НАЦІОНАЛЬНОГО УНІВЕРСИТЕТУ
серія: Технічні науки

Затверджений як фахове видання категорії «Б»,
РІШЕННЯ АТЕСТАЦІЙНОЇ КОЛЕГІЇ № 1643 ВІД 28.12.2019 та №409 від 17.03.2020

Засновано в липні 1997 р. ***Виходить 6 разів на рік***

Хмельницький, 2022, № 1(305)

Засновник і видавець: Хмельницький національний університет
(до 2005 р. – Технологічний університет Поділля, м. Хмельницький)

Наукова бібліотека України ім. В.І. Вернадського http://nbuv.gov.ua/j-tit/Vchnu_tekh

Включено до науково-метричних баз:

Google Scholar	http://scholar.google.com.ua/citations?hl=uk&user=aIUP9OYAAAAJ
Index Copernicus	http://jml2012.indexcopernicus.com/passport.php?id=4538&id_lang=3
Polish Scholarly Bibliography	https://pbn.nauka.gov.pl/journals/46221
CrossRef	http://doi.org/10.31891/2307-5732

Технічний редактор Горященко К. Л., к.т.н.
Редактор-коректор Броженко В. О.

Рекомендовано до друку рішенням вченої ради Хмельницького національного університету, протокол № 12 від 23.02.2022 р.

Адреса редакції: редакція журналу "Вісник Хмельницького національного університету"
Хмельницький національний університет
вул. Інститутська, 11, м. Хмельницький, Україна, 29016

☎ (038-2) 67-51-08 **web:** http://journals.khnu.km.ua/vestnik
http://lib.khnu.km.ua/visnyk_tup.htm

e-mail: visnyk.khnu@khmnu.edu.ua
visnyk.khnu@gmail.com

Зареєстровано Міністерством України у справах преси та інформації.
Свідоцтво про державну реєстрацію друкованого засобу масової інформації
Серія КВ № 24922-14862ПР від 12 липня 2021 року

ЗМІСТ

ЕКОЛОГІЯ

КОМП'ЮТЕРНІ НАУКИ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, СИСТЕМНИЙ АНАЛІЗ ТА КІБЕРБЕЗПЕКА

DOI 10.31891/2307-5732-2022-305-1-72-77
УДК 681.3.05

КРАСИЛЕНКО В. Г.
ORCID ID: 0000-0001-6528-3150
e-mail: krasvg@i.ua
Вінницький національний аграрний університет
НІКІТОВИЧ Д. В.
ORCID ID: 0000-0002-8907-1221
e-mail: diananikitovych@gmail.com
Вінницький національний технічний університет

МОДЕЛЮВАННЯ ПОКРАЩЕНИХ СЛІПИХ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ 2D ТИПУ ДЛЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Анотація - У статті розглядаються аспекти застосування матричних модифікацій криптосистеми RSA для створення на основі матричних моделей та алгоритмів криптоперетворень зображень сліпих електронних цифрових підписів (СЕЦП). Перевагою запропонованих матричних моделей RSA є враховування специфіки зображень та простота адаптації до різних типів та форматів зображень. Наведені формули та алгоритмічні кроки процедур створення СЕЦП та проміжних кроків закриття, зашифрування та розшифрування зображень. Модельними експериментами у програмному середовищі Mathcad Professional, скрінами зі створених програмних модулів продемонстровані функціональні можливості та переваги процедур та алгоритмів створення покращених сліпих ЕЦП матричного типу на текстографічні документи (ТГД) конфіденційного характеру. Наведені результати моделювання процесів створення таких підписів для великоформатних документів у програмному середовищі Mathcad підтвердили адекватність запропонованих моделей перетворень та правильність функціонування та верифікації СЕЦП та дозволили визначити час та обмеження відповідних криптоперетворень.

Ключові слова: криптографія, матричні моделі, сліпі електронні цифрові підписи, Mathcad Professional, моделювання, текстографічний документ, зашифрування-розшифрування зображень, криптографічні перетворення інтенсивності зображення, нелінійна обробка.

VLADIMIR KRASILENKO
Vinnytsia National Agrarian University
DIANA NIKITOVICH
Vinnytsia National Technical University

SIMULATIONS OF IMPROVED BLIND ELECTRONIC DIGITAL SIGNATURES 2D TYPE FOR INFORMATION PROTECTION SYSTEMS

Abstract - The article considers aspects of application of matrix modifications of RSA cryptosystem for creation on the basis of matrix models and algorithms of cryptoconversions of images of blind electronic digital signatures (BEDS). The advantage of the proposed matrix models of RSA is to take into account the specifics of images and ease of adaptation to different types and formats of images. Formulas and algorithmic steps of BEDS creation procedures and intermediate steps of closing, encrypting and decrypting images are given. Model experiments in the Mathcad Professional software environment, screens from the created software modules demonstrate the functionality and advantages of procedures and algorithms for creating improved blind EDS of matrix type for textual documents (TGD) of a confidential nature. The results of modeling the processes of creating such signatures for large-format documents in the Mathcad software environment confirmed the adequacy of the proposed transformation models and the correct operation and verification of BEDS and allowed to determine the processing time and limitations of relevant cryptographic transformations. Improved BEDS take into account the specifics of TGD, adapt to different formats, have better temporal, histogram-entropy characteristics (shown an increase in the entropy of BEDS to 7.98 bits/el.).

Keywords: cryptography, matrix models, blind electronic digital signatures, Mathcad Professional, modeling, text document, encryption-decryption of images, cryptographic transformations of image intensity, nonlinear processing.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Одним з ключових питань практичного застосування криптографії є завдання створення електронних цифрових підписів (ЕЦП), їх верифікації, які є електронними відповідниками традиційних підписів і можуть при задоволенні відповідних вимог і властивостей гарантувати набагато вищий рівень безпеки, ніж традиційні. Це завдання стає ще більш актуальним та гострим в останнє десятиріччя ще прискоренішого, розширенішого використання сучасних електронних комунікацій для передачі конфіденційних тєекстографічних документів (ТГД), звітів та засвідчення їх підписами відповідальних осіб, нотаріусів. Документи з конфіденційною економічною інформацією часто представлені у вигляді цифрових масивів, таблиць, малюнків, графіків, діаграм, резолюцій та підписів осіб, що приймають рішення. А тому з урахуванням структури такі документи є суто ТГД. Серед низки відомих різновидів ЕЦП, таких як ЕЦП на основі RSA та з хешуванням ТГД, Ель-Гамаля, Шнорра, DSA, тощо, та таких, що вже широко застосовуються, можна відмітити незаперечні, сліпі та інші. Проте зі списку існуючих та описаних класичних шифрів та процедур створення цифрових підписів, в тому числі тих, що базуються на відповідних державних стандартах, одним з найпопулярніших методів генерування цифрових підписів, включаючи сліпі, на сьогодні є підписування за допомогою алгоритму RSA [1-4]. Оскільки для генерування відомих сліпих ЕЦП добре підходить алгоритм RSA, але тут ми зауважуємо,

що він був раніше використаний лише як скалярний, а серед швидко зростаючої великої кількості публікацій, що присвячені новим удосконаленим моделям та алгоритмам криптографічних перетворень (КП) даних, у тому числі зображень [2-4], появились роботи [5–11] стосовно КП, що зорієнтовані на матричні моделі, алгоритми та засоби паралельної обробки та спричинили активізацію досліджень і у напрямку створення ЕЦП нового матричного типу (МТ) [12-14], то саме таким ЕЦП і присвячується наша робота. При генеруванні сліпих ЕЦП документ не оприлюднюється, а сам процес відповідає ситуації, коли особа чи сторона А хоче отримати сліпий пілпис нотаріуса під повідомленням чи ТГД, зміст якого нотаріус (сторона В) не повинен бачити. Недоліком більшості відомих алгоритмів і протоколів створення ЕЦП, протоколів формування ключів, систем верифікації ЕЦП, що зорієнтовані на послідовну скалярну обробку блоків ТГД, перетворених у цифрові формати, блоки яких представляються числами великої розрядності, є суттєве зниження швидкодії криптографічних процедур. Матричні моделі (ММ) КП запропоновані вперше в [5] і потім розвинені у [6-10], а модифікації системи RSA були узагальнені до 2D типу в [11], які пізніше були використані і для створення ЕЦП [12-14]. У роботі [6] були розроблені, досліджені і промодельовані цифрові сліпі підписи на основі матричних афінних шифрів, а в [7] - ЕЦП МТ (матричного типу) на базі модифікацій алгоритму RSA МТ і Ель-Гамаля до МТ. Але в [7] наводилися результати моделювання таких ЕЦП МТ лише для деяких специфічних невеликих чорно-білих зображень, що обмежувало узагальнення та висновки.

Постановка задачі

Тому **метою** даної роботи є подальше **вдосконалення**, дослідження ММ при створенні **сліпих** ЕЦП (СЕЦП) та перевірка їх функціональних можливостей, переваг шляхом моделювання у середовищі Mathcad на конкретних ТГД з демонстрацією утворених СЕЦП, з їх гістограмно-ентропійним аналізом. Це дозволить оцінити якість, показники, особливості і сфери застосувань таких СЕЦП.

Виклад основного матеріалу, результатів дослідження

Для моделювання ми використовували різні зображення (З), ТГД, в тому числі як матриці розмірністю 704 × 572 елементи та ТГД формату А4. Ідея узагальнення на 2D випадок скалярного RSA та похідних від нього алгоритмів [11, 13, 14] полягає у виборі в якості ключів не скалярів, а матричних ключів (МК), процес формування яких (випадкових та обернених до них) описано в [13] і тут через обмеження детально не розглядається. Кожен елемент МК вибирається з множини значень відповідних скалярних ключів $e_{i,j}$ та $d_{i,j}$, що відповідали в деяких з наших експериментів вибраним значенням: $k = 11$, $l = 23$, $kl = k \cdot l$, $kl = 253$, а функція Ейлера дорівнювала 220. Першим фактором ускладнення розв’язування задачі обчислення дискретного логарифма за модулем є розширення задачі на 2D випадок за рахунок збільшення потужностей множин МК при їх значних розмірах, а другим фактором стало застосування для СЕЦП багатокрокових процедур, як і в RSA МТ [14], коли процедуру поелементно-матричного піднесення у степінь за 2D-модулями сторони повторюють, використовуючи узгоджені публічні та приватні МК. Скріни з вікон, формули, програмні модулі та результати моделювання у Mathcad процесу створення СЕЦП 2D типу на основі ММ RSA алгоритмів, показані на рис. 1-5.

Як видно з отриманих результатів моделювання, що показані на рис. 2, то для такого виду вибраного зображення (З), результати повністю допустимі, що пдтверджується не лише візуально, але і відповідним гістограмним та ентропійним аналізом. Проте, як видно з рис. 3-4, для деяких ТГД, є неприпустимим неякісне «закриття», дивись TDK_d та DS_CTD (закритий ТГД) на рис.3 та DS_OCTD (підписаний ТГД) на рис.4. А тому нами запропоновано покращити СЕЦП введенням додаткового адитивного закриття TDK наявним публічним матричним ключем KeyAd нотаріуса. Для цього був розроблений модуль, що показаний праворуч на рис. 4, а отримані з ним кращі результати показані на рис. 5. Аналіз отриманих цим покращеним алгоритмом створення СЕЦП результатів показав, що видно також і візуально, достатнє та більш якісне формування усіх проміжних масивів (зображень). Таким чином, отримані результати моделювання підтверджують, що мета роботи досягнута і що за допомогою таких покращених сліпих ЕЦП МТ легко та криптостійко виконуються всі необхідні криптографічні перетворення ТГД формату А4 та близького до нього чи навіть значно більших масивів. Важливим аспектом для правильного функціонування таких СЕЦП є формування необхідних випадкових МК. Узгодження секретних МК різного типу розглядались у [15-18], а тому тут не висвітлюються.

Запропонований алгоритм створення сліпого ЕЦП МТ дозволяє зробити верифікацію підпису лише при спільних діях обох сторін що створювали підпис. Крім того, запропонований алгоритм може бути покращений ще більше за рахунок подвійного, так званого нами двостороннього, закриття як TDK так і реквізитів нотаріуса, сутність якого полягає в закритті не лише повідомлення TDK, що після піднесення у степінь та подвійного по суті адитивно-мультиплікативного закриття відсилається нотаріусу, але і у аналогічному закритті реквізитів (особистих ідентифікаторів) нотаріуса при створенні таких підписів. Це ще більше підсилює надійність таких двосторонніх процедур формування покращесліпих ЕЦП МТ та їх криптостійкість.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

Виконана демонстрація функціональних можливостей, переваг запропонованих покращених алгоритмів створення сліпих ЕЦП на конфіденційні документи, наведені результати моделювання у

середовищі Mathcad процесів створення таких підписів для великоформатних документів, що підтвердили адекватність ММ, правильність їх функціонування, верифікації, досягнення покращень. Покращені С_ЕЦП враховують специфіку ТГД, адаптуються до різних форматів, мають кращі часові, гістограмно-ентропійні характеристики (показано збільшення ентропії С_ЕЦП до 7,98 біт/ел.).

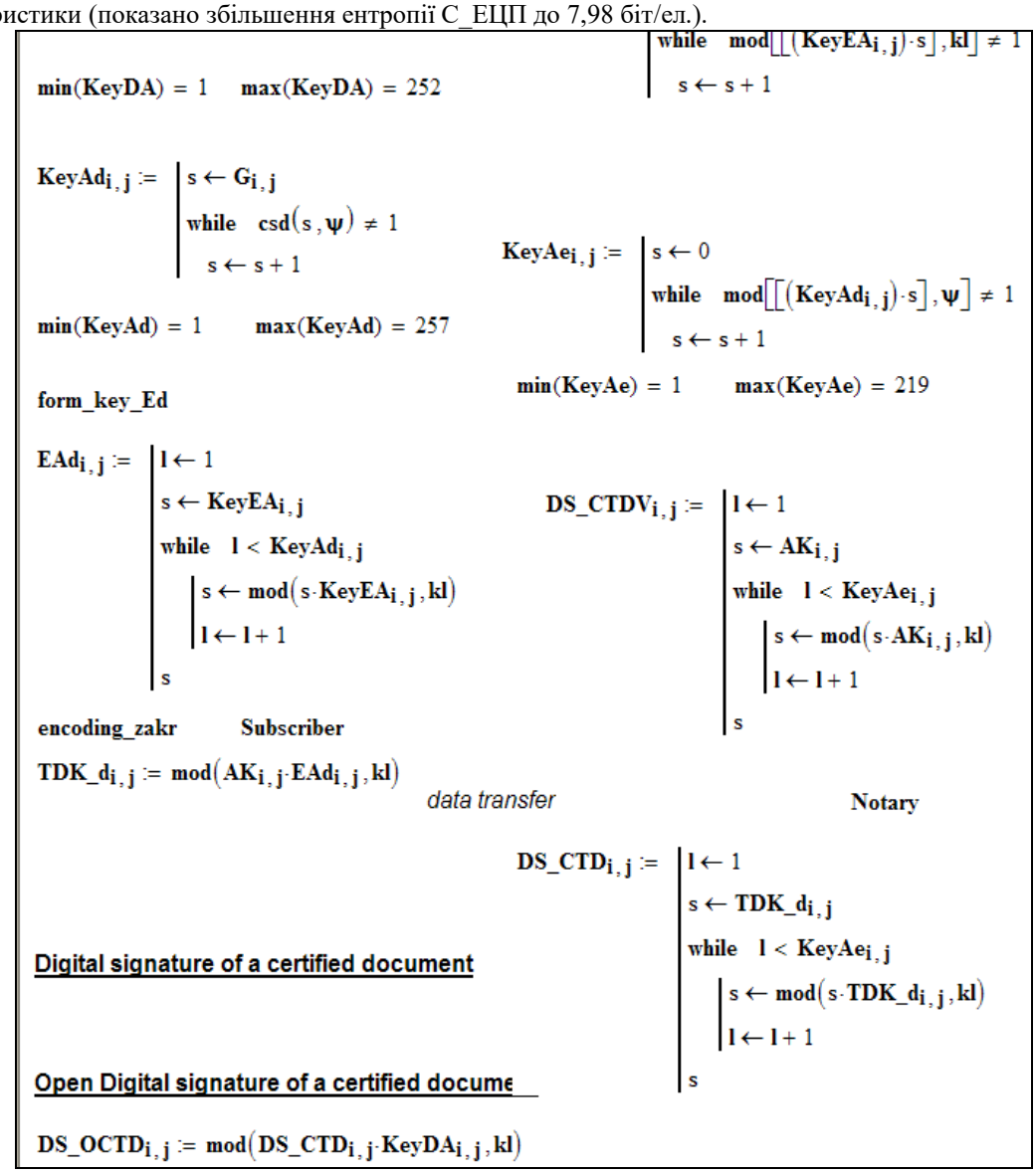

Рис.1. Формули, коментарі та програмні модулі (вікно Mathcad), що використовувались для моделювання СЕЦП 2D типу на основі RSA алгоритму

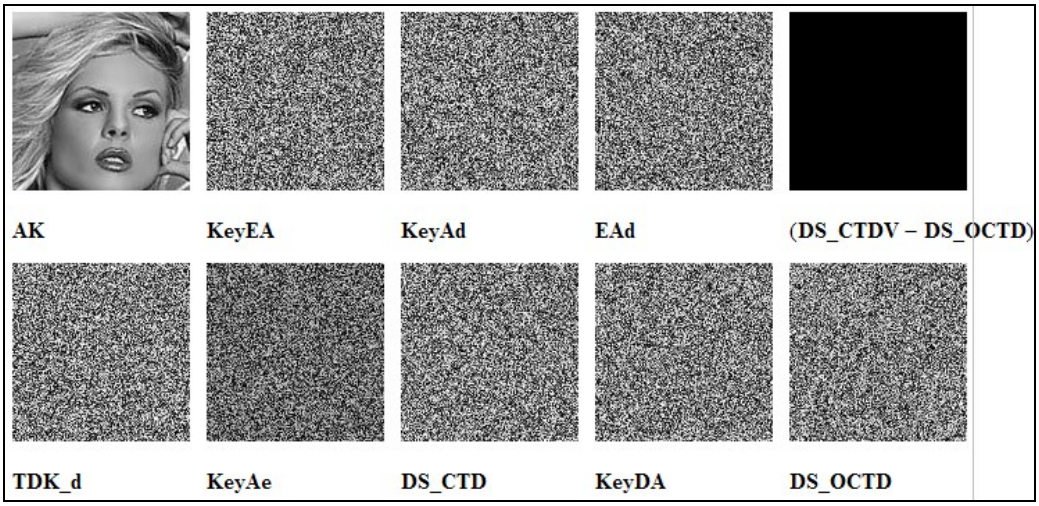

Рис.2 Результати моделювання процесів створення та верифікації СЕЦП 2D типу RSA. У верхньому ряду зліва направо: З для підпису, МК KeyEA для закриття З, публічний МК KeyAd нотаріуса, створений ним МК EAd матричним піднесенням KeyEA у степінь за модулем, різницеве З для верифікації; у нижньому: закрите МК EAd З у виді TDK_d, що підписує нотаріус, його приватний МК KeyAe, закритий СЕЦП (DS_CTD), МК KeyDA (обернений до KeyEA), розкритий цим МК підписаний СЕЦП

(DS_OCTD)

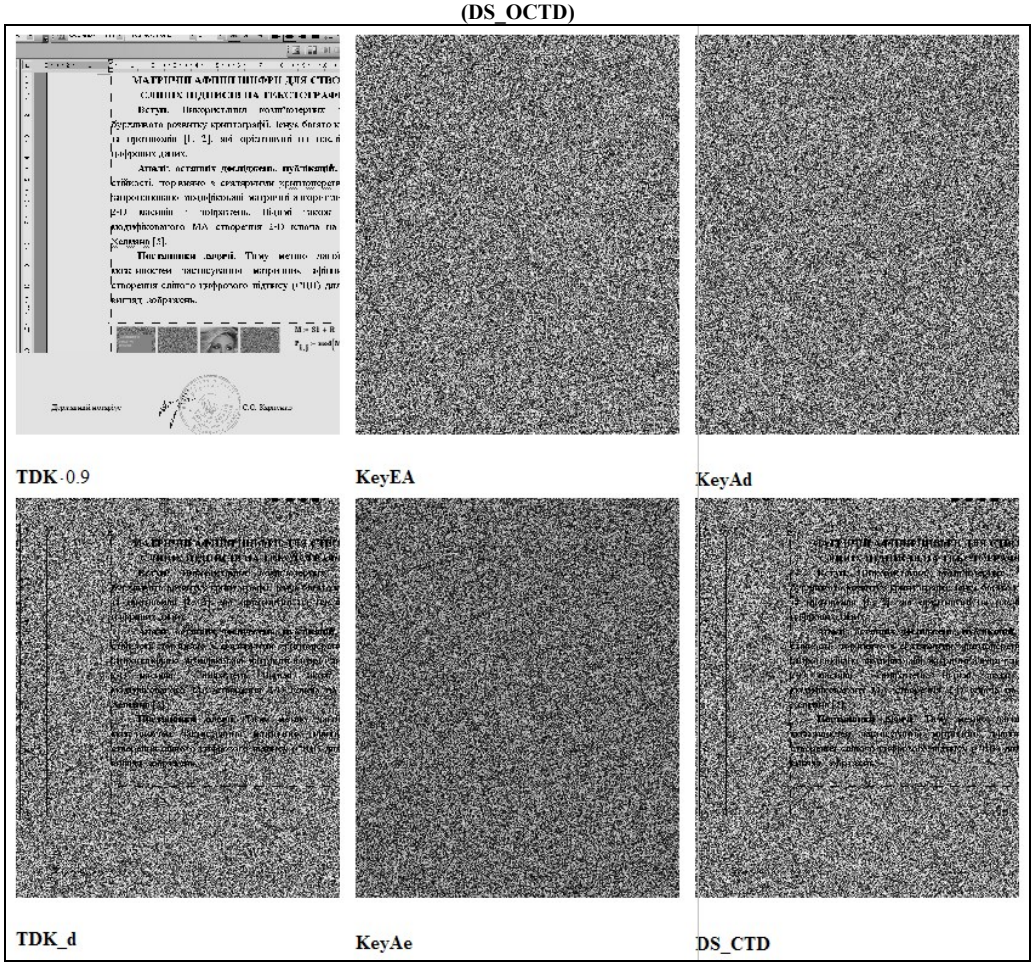

Рис.3 Результати моделювання процесів створення та верифікації СЕЦП 2D типу RSA для ТГД, що підтверджують недостатність закриття. У верхньому ряду зліва направо: скоригований ТГД для підпису, МК KeyEA для закриття ТГД, публічний МК KeyAd нотаріуса; у нижньому: закритий ТГД у виді TDK_d, що підписує нотаріус, його приватний МК KeyAe, закритий СЕЦП (DS_CTD)

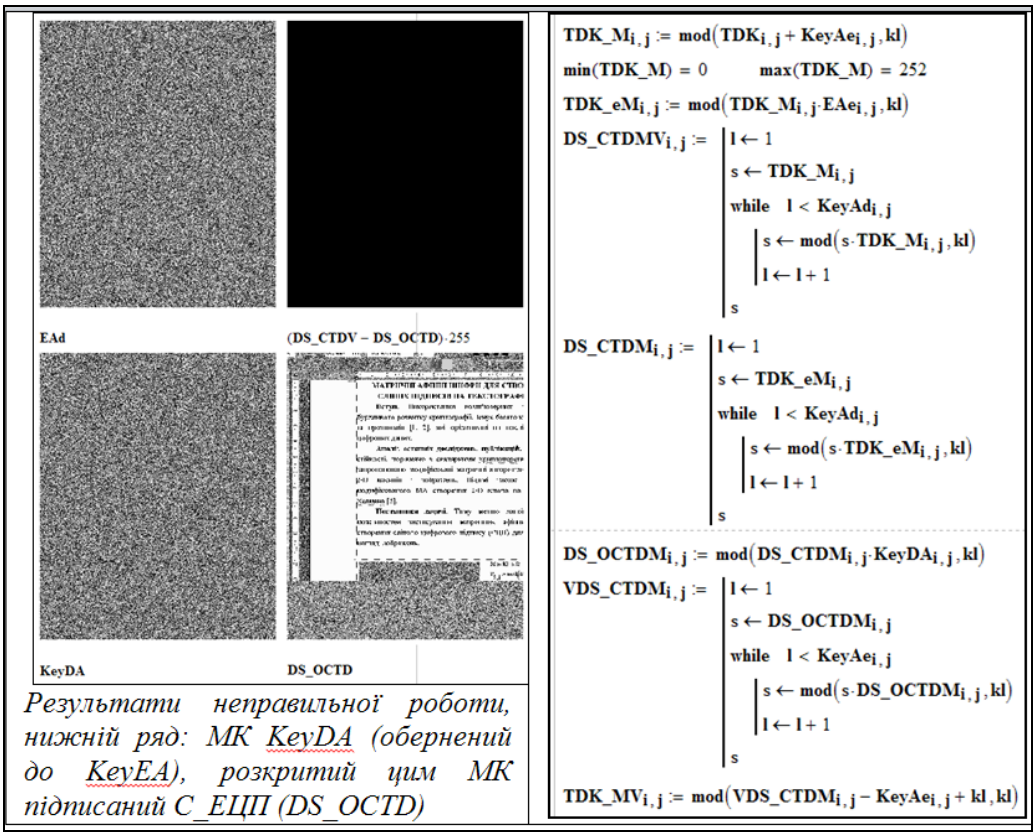

Рис.4 Результати (ліворуч) моделювання СЕЦП для ТГД про недостатність закриття та додатково введений програмний

модуль (вікно Mathcad, праворуч) для вдосконалення і моделювання покращеного СЕЦП 2D типу

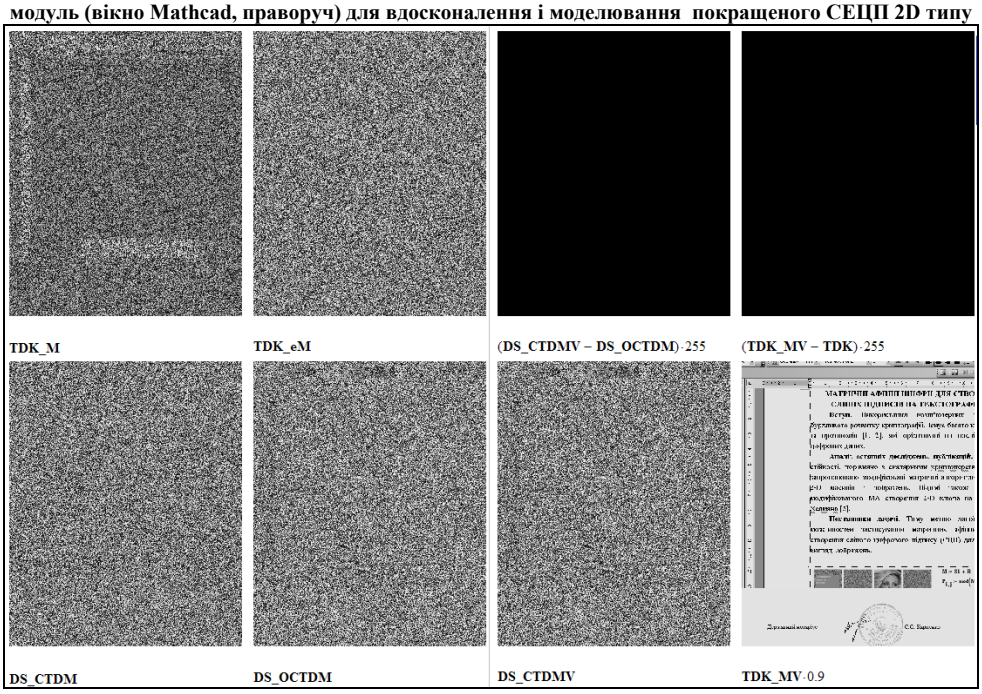

Рис.5 Матриці-зображення, що формувалися в модельних експериментах та підтверджують правильну роботу процесів створення та верифікації покращеного СЕЦП 2D типу RSA. У верхньому ряду зліва направо: скоригований для підпису ТГД та зашифрований публічним МК KeyAe (TDK_M), закритий МК KeyEA (TDK_eM), верифікаційні різниці; у нижньому: закритий СЕЦП (DS_CTDM), розкритий підписаний СЕЦП (DS_OCTDM), перевірені підписи

Література

1. Хорошко В.О. Методи та засоби захисту інформації: навч. Посібник / В.О. Хорошко, А.О. Четков. – К.: Юніор, 2003. – 502 с.

2. Ємець В. Сучасна криптографія: Основні поняття / В. Ємець, А. Мельник, Р. Попович. – Львів: БаК, 2003. – 144 с.: іл.

3. M.A. Dabbah, W.L. Woo, S.S. Dlay, "Secure Authentication for Face Recognition, "presented at Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on, 2007.

4. Коркішко Т. Алгоритми та процесори симетричного блокового шифрування / Т. Коркішко, А. Мельник, В. Мельник. – Львів: БаК, 2003. – 168 с.

5. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісн. нац. ун-ту "Львів. політехнік". - 2009. - № 658. - С. 59-63.

6. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97). – С. 60 – 63.

7. Красиленко В. Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. - 2012. - Вип. 3(2). - С. 53-61. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15

8. Красиленко В.Г. Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрізовою декомпозицією та їх моделювання / В.Г. Красиленко, В.М. Дубчак // Вісник Хмельницького національного університету. Технічні науки. – 2014. – № 1. – С. 74-79.

9. Красиленко В.Г. Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-бітовозрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології: збірник наукових праць. – Львів: Львівський національний університет імені Івана Франка, 2015. – Вип. 6. – С 111-127.

10. Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрізовою декомпозиціями / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво: наук. журн. – Луцьк: Видавництво Луц. нац. техн. ун-т., 2016. – № 23. – С. 31-36. – [Електронний ресурс]. – Режим доступу: http://ki.lutsktu.com.ua/node/132/section/9 .

11. Красиленко В.Г. Модифікації системи RSA для створення на її основі матричних моделей та алгоритмів для зашифрування та розшифрування зображень / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – 2012. – №8(106). – С.102-106.

12. Красиленко В.Г. Моделювання сліпих електронних цифрових підписів матричного типу на конфіденційну текстографічну документацію / В.Г. Красиленко, Р. О. Яцковська, С. К. Грабовляк, // І Міжнародна науково-методична конференція, Вінниця: ВНАУ, 2012. – С.103-107.

13. Красиленко В.Г. Демонстрація процесів створення сліпих електронних цифрових підписів на

текстографічну документацію на основі моделей матричного типу / В.Г. Красиленко, Р.О. Яцковська, Ю.М. Тріфонова, // Системи обробки інформації. – 2013. – Вип. 3(110). – Т. 2. – С. 18 – 22.

14. Красиленко В.Г. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів / В.Г. Красиленко, Д.В. Нікітович // Матеріали VI МПК «Інформаційні управляючі системи та технології» (ІУСТ-Одеса-2017), Одеський національний морський університет, – Одеса: 2017. - С. 312 -318.

15. Красиленко В.Г. Алгоритми формування двовимірних ключів для матричних алгоритмів криптографічних перетворень зображень та їх моделювання / В.Г. Красиленко, В.І., Яцковський, Р.О. Яцковська // Системи обробки інформації. – Х.: ХУПС, 2012. – Вип. 8(106). – С. 107-110.

16. Красиленко В.Г. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу / В.Г. Красиленко, Д.В. Нікітович // Системи обробки інформації. – 2017. – Вип. 3 (149). – С 151-157.

17. Красиленко В. Г., Юрчук Н. П, Нікітович Д. В. Застосування ізоморфних матричних представлень для моделювання протоколу узгодження секретних ключів-перестановок значної розмірності. Вісник Хмельницького національного університету. Технічні науки. Хмельницький, 2021, Вип. № 2. С. 78-88. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/32827/83207.pdf?sequence=2&isAllowed=y

18. Красиленко В. Г., Нікітович Д. В. Криптографічний кооперативний протокол узгодження ізоморфно представленого спільного секретного матричного ключа-перестановки великої розмірності: матеріали IX Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» (ІУСТ), 24– 26 вересня 2020 р. Одеса, 2020. С. 45-50. URL: http://ir.lib.vntu.edu.ua//handle/123456789/30698

References

1. Khoroshko V.O. Metody ta zasoby zakhystu informatsii: navch. Posibnyk / V.O. Khoroshko, A.O. Chetkov. – K.: Yunior, 2003. – 502 s.

2. Yemets V. Suchasna kryptohrafiia: Osnovni poniattia / V. Yemets, A. Melnyk, R. Popovych. – Lviv: BaK, 2003. – 144 s.: il.

3. M.A. Dabbah, W.L. Woo, S.S. Dlay, "Secure Authentication for Face Recognition, "presented at Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on, 2007.

4. Korkishko T. Alhorytmy ta protsesory symetrychnoho blokovoho shyfruvannia / T. Korkishko, A. Melnyk, V. Melnyk. – Lviv: BaK, 2003. – 168 s.

5. Krasilenko V.G. Modeliuvannia matrychnykh alhorytmiv kryptohrafichnoho zakhystu / V.G. Krasilenko, Yu.A. Flavytska // Visn. nats. un-tu "Lviv. politekhnik".- 2009. - № 658. - S. 59-63.

6. Krasilenko V.G. Matrychni afinni shyfry dlia stvorennia tsyfrovykh slipykh pidpysiv na tekstohrafichni dokumenty / V.G. Krasilenko, S.K. Hrabovliak // Systemy obrobky informatsii. – Kh.: KhUPS, 2011. – Vyp. 7(97). – S. 60 – 63.

7. Krasilenko V.G. Matrychni afinno-perestanovochni alhorytmy dlia shyfruvannia ta deshyfruvannia zobrazhen / V.G. Krasilenko, S.K. Hrabovliak // Systemy obrobky informatsii. - 2012. - Vyp. 3(2). - S. 53-61. - Rezhym dostupu: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15

8. Krasilenko V.G. Kryptohrafichni peretvorennia zobrazhen na osnovi matrychnykh modelei perestanovok z matrychno-bitovozrizovoiu dekompozytsiieiu ta yikh modeliuvannia / V.G. Krasilenko, V.M. Dubchak // Herald of Khmelnytskyi National University. Technical sciences. – 2014. – № 1. – S. 74-79.

9. Krasilenko V.G. Modeliuvannia ta doslidzhennia kryptohrafichnykh peretvoren zobrazhen na osnovi yikhnoi matrychno-bitovozrizovoi dekompozytsii ta matrychnykh modelei perestanovok z veryfikatsiieiu tsilisnosti / V.G. Krasilenko, D.V. Nikitovich // Elektronika ta informatsiini tekhnolohii: zbirnyk naukovykh prats. – Lviv: Lvivskyi natsionalnyi universytet imeni Ivana Franka, 2015. – Vyp. 6. – S 111-127.

10. Krasilenko V.G. Modeliuvannia kryptohrafichnykh peretvoren kolorovykh zobrazhen na osnovi matrychnykh modelei perestanovok zi spektralnoiu ta bitovo-zrizovoiu dekompozytsiiamy / V.G. Krasilenko, D.V. Nikitovich // Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo: nauk. zhurn. – Lutsk: Vydavnytstvo Luts. nats. tekhn. un-t., 2016. – № 23. – S. 31-36. – [Elektronnyi resurs]. – Rezhym dostupu: http://ki.lutskntu.com.ua/node/132/section/9 .

11. Krasilenko V.G. Modyfikatsii systemy RSA dlia stvorennia na yii osnovi matrychnykh modelei ta alhorytmiv dlia zashyfruvannia ta rozshyfruvannia zobrazhen / V.G. Krasilenko, S.K. Hrabovliak // Systemy obrobky informatsii. – 2012 . – №8(106).–S.102-106.

12. Krasilenko V.G. Modeliuvannia slipykh elektronnykh tsyfrovykh pidpysiv matrychnoho typu na konfidentsiinu tekstohrafichnu dokumentatsiiu / V.G. Krasilenko, R.O. Yatskovska, S.K. Hrabovliak, // I Mizhnarodna naukovo-metodychna konferentsiia, Vinnytsia: VNAU, 2012. – S.103-107.

13. Krasilenko V.G. Demonstratsiia protsesiv stvorennia slipykh elektronnykh tsyfrovykh pidpysiv na tekstohrafichnu dokumentatsiiu na osnovi modelei matrychnoho typu / V.G. Krasilenko, R.O. Yatskovska, Yu.M. Trifonova, // Systemy obrobky informatsii. – 2013. – Vyp. 3(110). – T. 2. – S. 18 – 22.

14. Krasilenko V.G. Vdoskonalennia ta modeliuvannia elektronnykh tsyfrovykh pidpysiv matrychnoho typu dlia tekstohrafichnykh dokumentiv / V.G. Krasilenko, D.V. Nikitovich // Materialy VI MPK «Informatsiini upravliaiuchi systemy ta tekhnolohii» (IUST-Odesa-2017), Odeskyi natsionalnyi morskyi universytet, – Odesa: 2017. - S. 312 -318.

15. Krasilenko V.G. Alhorytmy formuvannia dvovymirnykh kliuchiv dlia matrychnykh alhorytmiv kryptohrafichnykh peretvoren zobrazhen ta yikh modeliuvannia / V.G. Krasilenko, V.I., Yatskovskyi, R.O. Yatskovska // Systemy obrobky informatsii. – Kh.: KhUPS, 2012. – Vyp. 8(106). – S. 107-110.

16. Krasilenko V.G. Modeliuvannia protokoliv uzghodzhennia sekretnoho matrychnoho kliucha dlia kryptohrafichnykh peretvoren ta system matrychnoho typu / V.G. Krasilenko, D.V. Nikitovich // Systemy obrobky informatsii. – 2017. – Vyp. 3 (149). – S 151-157.

17. Krasilenko V.G., Yurchuk N.P, Nikitovich D.V. Zastosuvannia izomorfnykh matrychnykh predstavlen dlia modeliuvannia protokolu uzghodzhennia sekretnykh kliuchiv-perestanovok znachnoi rozmirnosti. Herald of Khmelnytskyi National University. Technical sciences. Khmelnytskyi, 2021, Vyp. № 2. S. 78-88. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/32827/83207.pdf?sequence=2&isAllowed=y

18. Krasilenko V.G, Nikitovych D.V. Kryptohrafichnyi kooperatyvnyi protokol uzghodzhennia izomorfno predstavlenoho spilnoho sekretnoho matrychnoho kliucha-perestanovky velykoi rozmirnosti: materialy IX Mizhnarodnoi naukovo-praktychnoi konferentsii «Informatsiini upravliaiuchi systemy ta tekhnolohii» (IUST), 24– 26 veresnia 2020 r. Odesa, 2020. S. 45-50. URL: http://ir.lib.vntu.edu.ua//handle/123456789/30698

Рецензія/Peer review : 09.01.2022 р. Надрукована/Printed :27.02.2022 р.