***Красиленко В.Г., к.т.н., с.н.с., доцент,***
***Нікітович Д.В.***
*Вінницький національний технічний університет*

## МОДЕЛЮВАННЯ ПОКРАЩЕНИХ СЛІПИХ ЕЛЕКТРОННИХ ЦИФРОВИХ ПІДПИСІВ 2D ТИПУ

**Вступ, аналіз останніх досліджень, публікацій.** Задача створення електронних цифрових підписів (ЕЦП) є актуальною та необхідною, особливо при використанні сучасних електронних комунікацій для передачі конфіденціальних текстографічних документів (ТГД), звітів та засвідчення їх підписами відповідальних осіб, нотаріусів. Суттєвий ріст числа публікацій, присвячених КП зображень, поява робіт [1-3], що зорієнтовані на моделі, алгоритми та засоби паралельної обробки, спричинили активізацію досліджень і у напрямку створення ЕЦП МТ [4-8]. Існує низка класичних ЕЦП, таких як ЕЦП на основі RSA та з хешуванням ТГД, Ель-Гамаля, Шнорра, DSA, незаперечні підписи, сліпі підписи та інші. Але більшість відомих алгоритмів та протоколів створення ЕЦП, протоколів формування ключів та систем верифікації ЕЦП орієнтовані на послідовну скалярну обробку блоків ТГД, перетворених у цифрові формати, блоки яких представляються числами великої розрядності, що спричинює до суттєвого зниження швидкодії криптографічних процедур. Матричні моделі (ММ) запропоновані в [1], а модифікації системи RSA до 2D типу в [2], які пізніше були використані і для створення ЕЦП. У роботі [4] були розроблені, досліджені і промодельовані цифрові сліпі підписи на основі матричних афінних шифрів, а в [5] - ЕЦП МТ (матричного типу) на базі модифікацій алгоритму RSA МТ і Ель-Гамаля до МТ. Але в [5] 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 (С_ЕЦП) та перевірка їх функціональних можливостей, переваг шляхом моделювання у середовищі Mathcad на конкретних ТГД з демонстрацією утворених С_ЕЦП, з їх гістограмно-ентропійним аналізом. Це дозволить оцінити якість, показники, особливості і сфери застосувань таких С_ЕЦП.

**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 [2, 5, 7] полягає у виборі в якості ключів не скалярів, а матричних ключів (МК), процес формування яких (випадкових та обернених до них) описано в [5] і тут через обмеження не надається. Кожен елемент МК вибирається з множини значень відповідних скалярних ключів e_i,j та d_i,j, що відповідали в наших експериментах вибраним значенням: k = 11, l = 23, kl = k · 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 застосування для С_ЕЦП багатокрокових процедур, як і в RSA МТ [7], коли процедуру поелементно-матричного піднесення у степінь за 2D-модулями сторони повторюють, використовуючи узгоджені публічні та приватні МК. Результати моделювання у Mathcad процесу створення С_ЕЦП 2D типу, на основі ММ RSA алгоритмів показані на рис. 1-5.

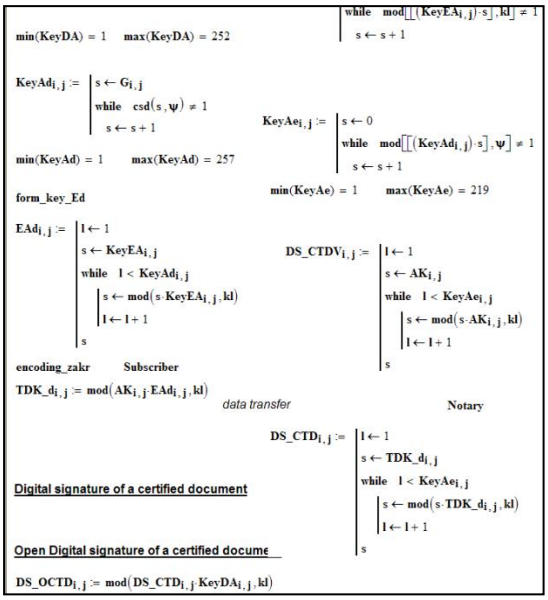


*Рис.1 Програмний модуль (вікно Mathcad), що використовувались для моделювання С_ЕЦП 2D типу на основі RSA алгоритму*

Якщо для зображення (З), рис. 2, результати допустимі, то, як видно з рис. 3-4, для деяких ТГД, є неприпустимим неякісне «закриття», тому нами запропоновано покращити С_ЕЦП введенням додаткового адитивного закриття публічним МК. Для цього був розроблений модуль, що показаний на рис. 4, а отримані з ним кращі результати показані на рис. 5. Узгодження МК розглядались у [6], а тому будуть висвітлені та продемонстровані лише у доповіді.

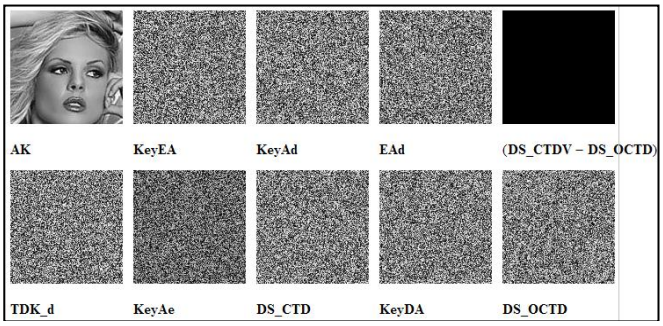


*Рис.2 Результати моделювання процесів створення та верифікації С_ЕЦП 2D типу RSA. У верхньому ряду зліва направо: З для підпису, МК KeyEA для закриття З, публічний МК KeyAd нотаріуса, створений ним МК EAd матричним піднесенням KeyEA у степінь за модулем, різницеве З для верифікації; у нижньому: закрите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

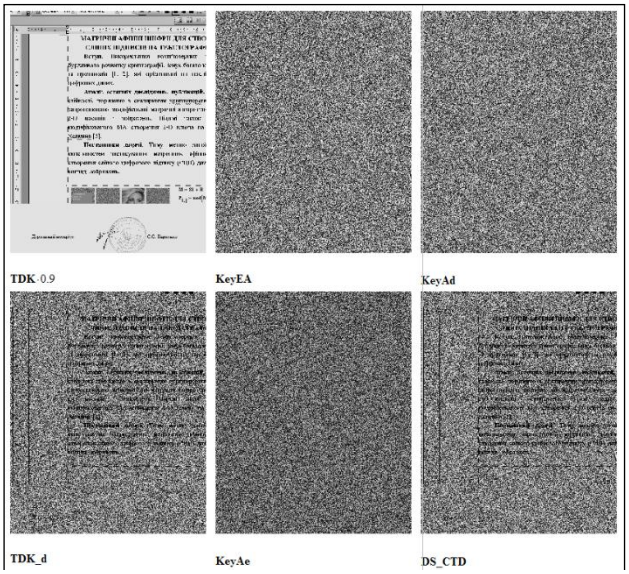


*Рис.3 Результати моделювання процесів створення та верифікації С_ЕЦП 2D типу RSA для ТГД, що підтверджують недостатність закриття. У верхньому ряду зліва направо: скоригований ТГД для підпису, МК KeyEA для закриття ТГД, публічний МК KeyAd нотаріуса; у нижньому: закритий ТГД у виді TDK_d, що підписує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

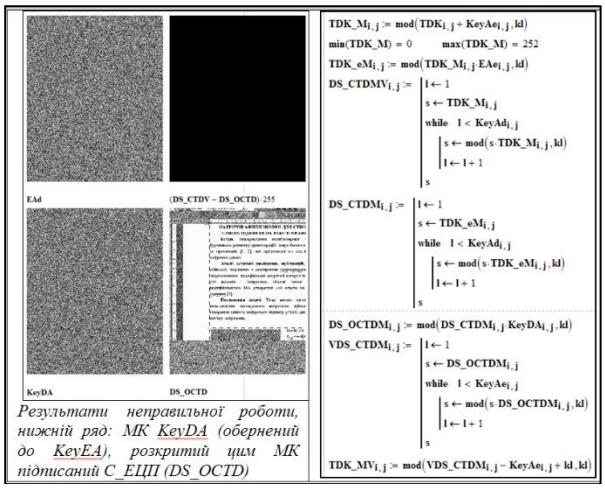


*Рис.4 Результати (ліворуч) моделювання С_ЕЦП для ТГД про недостатність закриття та додатково введений програмний модуль (вікно Mathcad, праворуч) для вдосконалення і моделювання покращеного С_ЕЦП 2D типу*

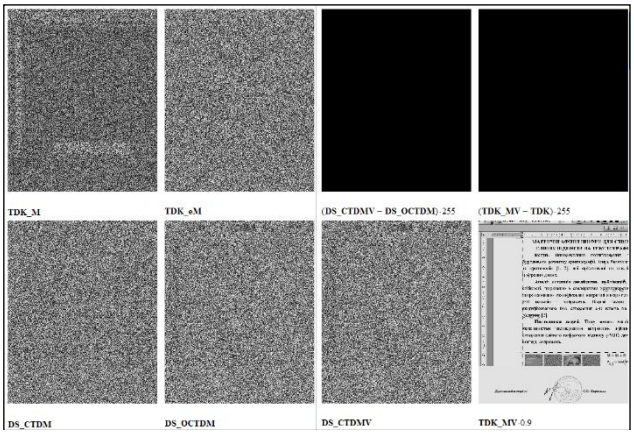


*Рис.5 Матриці-зображення, що формувалися в модельних експериментах та підтверджують правильну роботу процесів створення та верифікації* ***покращеного*** *С_ЕЦП 2D типу RSA. У верхньому ряду зліва направо: скоригований для підпису ТГД та зашифрований публічним МК KeyAe (TDK_M), закритий МК KeyEA (TDK_eM),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

**Висновки**: 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.).

**Список літератури**

1. *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.*

2. *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.*

3. *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*

4. *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.*

5. *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.*

6. *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.*

7. *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.*

8. *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.*