КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.33.1217
УДК 004.056.53

**Опірський Іван Романович**
д.т.н., проф., завідувач кафедри захисту інформації
Національний університет «Львівська Політехніка», Львів, Україна
ORCID: 0000-0002-8461-8996
*ivan.r.opirskyi@lpnu.ua*

**Кучма Христина Юріївна**
Студентка кафедри «Захист інформації»
Національний університет «Львівська Політехніка», Львів, Україна
ORCID: 0009-0001-9093-6819
*khrystyna.kuchma.kb.2025@lpnu.ua*

# ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ СХЕМ СЛІПОГО ПІДПИСУ НА ОСНОВІ ECC

**Анотація**. У роботі досліджується ефективність схем сліпого цифрового підпису на основі еліптичної криптографії (ECC) у порівнянні з класичними реалізаціями на базі RSA. Актуальність дослідження зумовлена необхідністю забезпечення анонімності користувачів у системах електронного голосування, цифрових платежів та інших застосуваннях, де важливим є розмежування автентифікації та ідентифікації. У межах дослідження реалізовано схему сліпого підпису Фу-Гво Дженга мовою Python із використанням сучасних криптографічних бібліотек. Проведено експериментальне вимірювання продуктивності основних фаз протоколу (засліплення, підписування та зняття сліпоти) для еліптичних кривих P-256, P-384 та P-521. Для забезпечення об'єктивності результатів виконано порівняльний аналіз із реалізацією сліпого підпису на базі RSA при еквівалентних рівнях криптографічної стійкості. Отримані результати показують, що застосування ECC дозволяє суттєво підвищити ефективність генерації підпису: для кривої P-256 середній час виконання операції становить 7-8 мс, що приблизно у 10-12 разів швидше порівняно з RSA-3072. Встановлено, що зменшення розміру ключів та обчислювальної складності операцій забезпечує значну перевагу ECC у середовищах з обмеженими ресурсами. Наукова новизна роботи полягає у програмній реалізації схеми Дженга та експериментальному порівнянні її продуктивності з RSA-реалізацією для різних рівнів криптографічної стійкості. Практичне значення отриманих результатів полягає у можливості використання запропонованого підходу в системах з високими вимогами до швидкодії та енергоефективності.

**Ключові слова:** Еліптична криптографія, сліпий цифровий підпис, еліптичні криві, анонімність, проблема дискретного логарифмування (ECDLP), схема Фу-Гво Дженга (Jeng Scheme), ДСТУ 4145-2002, відстежувана анонімність.

## ВСТУП

Сучасний розвиток інформаційних технологій та цифровізація суспільства зумовлюють зростання вимог до забезпечення конфіденційності та цілісності даних. В умовах, коли значні обсяги персональних даних щоденно циркулюють відкритими каналами зв'язку, питання забезпечення конфіденційності та цілісності інформації набуває критичного значення. Особливої ваги проблема захисту приватності користувачів набуває у децентралізованих системах: під час проведення електронного голосування (e-voting), функціонування цифрових платіжних систем (e-cash), систем управління доступом та електронної комерції.

У таких архітектурах виникає фундаментальна суперечність: з одного боку, система повинна надійно автентифікувати користувача для надання йому відповідних прав (наприклад, переконатися, що виборець має право голосу), а з іншого – зберегти його повну анонімність, унеможлививши будь-яке відстеження його дій та розкриття особистості. Вирішення цієї дилеми вимагає чіткого розмежування процесів автентифікації та ідентифікації.

Ефективним криптографічним інструментом для досягнення такої мети є протоколи сліпого цифрового підпису. Концепцію сліпого підпису вперше запропонував Девід Чаум у 1983 році для

реалізації невідстежуваних (untraceable) електронних платежів [1]. Основна ідея полягає у специфічній взаємодії між користувачем (ініціатором) та підписувачем (наприклад, банком або виборчою комісією). Користувач застосовує математичне «засліплююче» перетворення до свого повідомлення перед тим, як відправити його на підпис. Підписувач формує цифровий підпис для цього образу, абсолютно не знаючи реального змісту документа. Після повернення підписаного повідомлення користувач «знімає сліпоту», отримуючи дійсний цифровий підпис під початковим текстом, справжність якого може перевірити будь-яка третя сторона.

Історично перші реалізації сліпих підписів базувалися на алгоритмі RSA. Криптографічна стійкість таких систем спирається на обчислювальну складність задачі факторизації великих цілих чисел. Однак із невпинним зростанням обчислювальних потужностей та вдосконаленням методів криптоаналізу, вимоги до довжини ключів RSA експоненціально зростають для збереження адекватного рівня безпеки. На сьогодні для забезпечення базового 128-бітного рівня безпеки за рекомендаціями NIST необхідні ключі довжиною щонайменше 3072 біти [16]. Оперування такими великими числами вимагає значних витрат ресурсів, що створює обмеження для використання RSA у смарт-картках, мобільних пристроях та мережах Інтернету речей (IoT).

Оптимальною альтернативою є використання еліптичної криптографії (ECC), незалежно запропонованої Нілом Кобліцом та Віктором Міллером у 1985 році [2, 3]. ECC використовує групу точок еліптичної кривої над скінченним полем. Криптостійкість таких систем ґрунтується на складності задачі дискретного логарифмування на еліптичній кривій (ECDLP). Це дозволяє досягати еквівалентного рівня безпеки при значно менших розмірах ключів. Наприклад, 256-бітний ключ ECC забезпечує такий же рівень захисту, як і 3072-бітний ключ RSA [16]. Мінімізація довжини операндів кардинально знижує накладні витрати на обчислення та передачу даних.

У цьому контексті особливий інтерес становить схема сліпого підпису Фу-Гво Дженга (2010 р.), яка забезпечує властивості сліпоти та непідроблюваності на базі еліптичних кривих [4]. Окрім того, для вітчизняних інформаційних систем актуальним є питання адаптації національного стандарту ДСТУ 4145-2002 для роботи в режимі анонімного підпису [5]. Тому порівняльне дослідження програмних реалізацій цих алгоритмів є необхідним етапом для їх практичного впровадження.

Постановка проблеми. Впровадження протоколів сліпого підпису в реальні програмно-апаратні комплекси стикається з проблемою вибору оптимального криптографічного базису. Незважаючи на доведені теоретичні переваги еліптичної криптографії, на практиці розробники потребують конкретних кількісних оцінок її продуктивності порівняно з RSA. Відсутність детальних експериментальних даних щодо часових витрат на фази засліплення, підписування та зняття сліпоти при еквівалентних цільових рівнях безпеки за стандартами NIST [16] ускладнює обґрунтований вибір архітектури для систем, що потребують одночасно високої швидкодії та гарантованого рівня анонімності.

Аналіз останніх досліджень і публікацій. Фундамент концепції сліпих підписів для невідстежуваних систем було закладено у працях Д. Чаума [1]. Теоретичні основи переходу до еліптичних кривих сформували Н. Кобліц та В. Міллер [2, 3], а їхнє практичне застосування детально розкрито у посібниках Д. Хенкерсона, А. Менезеса та С. Ванстоуна [6, 7]. Математичну стійкість та методи підрахунку точок на кривих ґрунтовно досліджував Р. Скуф [12].

Вагомий внесок у розвиток сліпих підписів на базі ECC зробила група дослідників під керівництвом Ф.-Г. Дженга, запропонувавши високоефективну схему підписання [4]. Питання математичного моделювання протоколів сліпого підпису в Україні досліджували М. В. Єсіна [8] та В. А. Пономар [9]. Практичні схеми реалізації алгоритмів на еліптичних кривих розглядали А. Чунарьова [10], а також О. Коссак та Я. Холявка [11]. Крім того, активно досліджувалася адаптація чинного стандарту ДСТУ 4145-2002 для режимів анонімності [5]. Сучасні можливості застосування ECC розглядаються у багатьох світових роботах: Р. Ма та Л. Ду використовують їх для атрибутивних підписів [13], М.-Т. Чен та Х.-Ц. Хуанг – для мереж IoT [14], а В. Рейес-Маседо з колегами – для блокчейн-систем [15].

Більшість існуючих праць (наприклад, [8, 9] ) зосереджені на теоретичному моделюванні алгоритмів або доведенні їхньої математичної стійкості. Водночас у науковій літературі спостерігається дефіцит робіт із прямим експериментальним порівнянням часу виконання фаз протоколів. Зокрема, бракує практичних досліджень схеми Дженга [4] з використанням сучасних кривих NIST (P-256, P-384, P-521) [16] у порівнянні з RSA на еквівалентних надвеликих ключах (3072, 7680, 15360 біт). Наукова новизна цієї роботи полягає саме у заповненні цієї прогалини через створення власної програмної імплементації схеми [17] та отримання об’єктивних результатів оцінювання ефективності алгоритмів.

Метою статті є програмна реалізація та експериментальне дослідження ефективності схем сліпого цифрового підпису на основі еліптичної криптографії (ECC) у порівнянні з класичними реалізаціями на базі RSA. Для досягнення поставленої мети сформульовано такі завдання дослідження:

- Здійснити аналіз математичних основ еліптичної криптографії та складності задачі дискретного логарифмування (ECDLP), що лежать в основі криптостійкості сучасних протоколів [6, 7].
- Дослідити алгоритмічну структуру схеми сліпого підпису Фу-Гво Дженга [4] та проаналізувати особливості адаптації національного стандарту ДСТУ 4145-2002 [5], зокрема у контексті застосування в схемах сліпого підпису [8].
- Виконати програмну реалізацію схеми Дженга (ECC) та базової схеми Чаума (RSA) мовою програмування Python із використанням сучасних криптографічних бібліотек [1, 17].
- Провести експериментальне вимірювання продуктивності основних фаз протоколів (засліплення, підписування та зняття сліпоти) для стандартизованих кривих P-256, P-384, P-521 та порівняти їх із RSA-реалізацією при еквівалентних цільових рівнях безпеки NIST [16].

## ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Еліптична криптографія (ECC), незалежно запропонована Нілом Кобліцом та Віктором Міллером у 1985 році [2, 3], базується на складній алгебраїчній структурі еліптичних кривих над скінченними полями. На відміну від класичних криптосистем (наприклад, RSA), які оперують у кільцях цілих чисел, ECC використовує групу точок кривої, що дозволяє досягти еквівалентного рівня безпеки при значно менших розмірах ключів. Це робить ECC особливо привабливою для використання в системах з обмеженими обчислювальними ресурсами, таких як смарт-картки та мобільні пристрої.

Математична модель та рівняння Вейєрштрасса. Еліптична крива в контексті криптографії розглядається як множина точок, що задовольняють певному кубічному рівнянню, заданому над скінченним полем, разом із спеціальним елементом – «точкою на нескінченності» $\mathcal{O}$. Згідно з дослідженнями Дженга (Jeng) [4], для побудови криптосистем найчастіше використовуються еліптичні криві над простим полем $Z_p$, де p – велике просте число.

Рівняння Вейєрштрасса та умови несингулярності. Еліптичною кривою E над скінченним полем $Z_p$(де характеристика поля більше 3) називається множина точок $(x, y) \in Z_p \times Z_p$, що задовольняють умову [6]:

$$y^2 = x^3 + ax + b \ (mod\ p) \tag{1}$$

де коефіцієнти $a, b \in Z_p$.

Для того, щоб крива була придатною для криптографічних застосувань, вона не повинна мати особливих точок (точок самоперетину або зламів). Умовою несингулярності (гладкості) кривої є відмінність від нуля її дискримінанта [6]:

$$\Delta = 4a^3 + 27b^2 \neq 0 \tag{2}$$

Правила додавання точок: геометрична та алгебраїчна. На множині точок еліптичної кривої $E(Z_p)$ вводиться операція додавання, яку позначають символом «+». Ця операція має чітку геометричну інтерпретацію (метод хорд і дотичних) та відповідний алгебраїчний опис [6, 11].

Геометрично операція додавання точок на еліптичній кривій інтерпретується методом хорд і дотичних: пряма, проведена через точки $P$ і $Q$, перетинає криву в третій точці, симетричній результату додавання відносно осі абсцис; у випадку $P = Q$ використовується дотична до кривої.

Алгебраїчні правила. Координати результуючої точки $R(x_3, y_3) = P + Q$ обчислюються через кутовий коефіцієнт січної або дотичної $\lambda$

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} (mod\ p), & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} (mod\ p), & P = Q \end{cases} \tag{3}$$

Відповідно, координати суми визначаються за формулами [6, 11]:

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \ (mod\ p) \\ y_3 &= \lambda(x_1 - x_3) - y_1 \ (mod\ p) \end{aligned} \tag{4}$$

Ці примітиви є базисом для скалярного множення точок (багаторазового додавання), на складності обернення якого (ECDLP) базується стійкість протоколу Дженга [4] та стандарту ДСТУ 4145-2002 [5].

Дискретне логарифмування на еліптичній кривій (ECDLP). Криптографічна стійкість схем сліпого

підпису на еліптичних кривих, таких як схема Дженга, базується на складності розв'язання задачі дискретного логарифмування в групі точок еліптичної кривої (Elliptic Curve Discrete Logarithm Problem – ECDLP). Задача формулюється наступним чином: для заданої точки $P \in E(\mathbb{Z}_p)$ порядку $n$та точки $Q$, що належить підгрупі $\langle P \rangle$, необхідно знайти скаляр $x$, який задовольняє рівняння:

$$Q = xP \tag{5}$$

Обчислення $Q$є ефективним, тоді як обернена задача знаходження $x$є обчислювально складною.

Найефективнішим відомим методом атаки на ECDLP для загальних еліптичних кривих є $\rho$-метод Полларда, очікувана складність якого оцінюється як:

$$T \approx \frac{\sqrt{\pi n}}{2r} \tag{6}$$

що асимптотично відповідає складності порядку $O(\sqrt{n})$ [6].

Залежність обчислювальної складності від розміру параметрів еліптичної кривої наведено в табл. 1 (адаптовано з [6, 7]).

*Таблиця 1*

**Залежність обчислювальної складності від розміру ключа в еліптичній криптографії**

| Розмір поля (біт) | Розмір $n$ (біт) | Кількість операцій | Складність у MIPS-роках |
|---|---|---|---|
| 163 | 160 | $2^{80}$ | $8{,}5 \times 10^{11}$ |
| 191 | 186 | $2^{93}$ | $7{,}0 \times 10^{15}$ |
| 239 | 234 | $2^{117}$ | $1{,}2 \times 10^{23}$ |
| 359 | 354 | $2^{177}$ | $1{,}3 \times 10^{41}$ |
| 431 | 426 | $2^{213}$ | $9{,}2 \times 10^{51}$ |

Згідно з табл. 1, навіть незначне збільшення розміру параметрів призводить до зростання складності розв’язання задачі ECDLP на декілька порядків, що робить практичні атаки обчислювально неможливими.

Дослідження та моделювання схем сліпого підпису на основі ECC. Сліпий підпис передбачає взаємодію користувача та підписувача, у межах якої підписувач формує підпис, не маючи доступу до змісту повідомлення. Це досягається шляхом застосування заслiплюючого перетворення перед передачею даних.

Протокол базується на двох основних властивостях [1]:

- Сліпота (blindness): гарантує, що підписувач не може визначити зміст повідомлення та встановити зв’язок між процесом підписання і фінальним підписом.
- Непідроблюваність (unforgeability): забезпечує можливість генерації коректного підпису виключно власником секретного ключа.

Перевагами використання еліптичної криптографії для реалізації сліпих підписів є компактність ключів та висока обчислювальна ефективність, що особливо важливо для ресурсно-обмежених систем.

Моделювання схеми сліпого підпису Дженга. Схема, запропонована групою тайванських дослідників під керівництвом Фу-Гво Дженга (Fuh-Gwo Jeng), Тцер-Лонг Чена (Tzer-Long Chen) та Тцер-Шйонг Чена (TzerShyong Chen) у 2010 році [4], представляє собою елегантне рішення для реалізації сліпого підпису на основі еліптичних кривих. Автори ставили за мету створити протокол, який би математично гарантував виконання обох умов Чаума [1] (сліпоти та непідроблюваності) і при цьому уникав недоліків попередніх схем, пов'язаних з великими накладними витратами.

Схема базується на еліптичній кривій $E_p(a,b)$: $y^2 = x^3 + ax + b$ над полем $Z_p$. Нехай $G$ – базова точка порядку $n$. Протокол складається з трьох чітко визначених фаз: засліплення, підпису та зняття сліпоти.

Фаза 1. Засліплення (Blinding Phase). Користувач формує засліплений образ повідомлення:

$$\alpha \equiv m \times (n_i \times p_i)(mod\, p) \tag{7}$$

Використання $n_i$ робить маскування унікальним для кожного користувача.

Фаза 2. Підпис (Signing Phase). Підписувач отримує значення $\alpha$. Він не може відновити оригінальне повідомлення $m$, але може накласти на нього свій цифровий підпис, використовуючи власний секретний ключ.

Підписувач має власний секретний ключ $n_s$ та відкритий ключ $P_s = n_s \times G$.

Для захисту від атак повтору він генерує унікальний сесійний ключ (nonce) $n_v$ та обчислює пару $(r, s)$:

$$r \equiv n_v \times \alpha \ (mod\ p) \quad (8)$$
$$s \equiv (n_v + n_s) \times \alpha \ (mod\ p)\#(9) \quad (9)$$

Отримані значення $\boldsymbol{r}$ та $\boldsymbol{s}$ є точками на еліптичній кривій.
Фаза 3. Зняття сліпоти (Unblinding Phase). Користувач отримує фінальний підпис:

$$s' \equiv s - m \times n_i \times P_s \ (mod\ p) \quad (10)$$
$$m' = n_i(n_i - 1)m \quad (11)$$

Фінальний підпис має вигляд трійки $(m',\ s',\ r)$.
На відміну від класичної схеми, у протоколі на основі еліптичних кривих, запропонованому Дженгом, перевірка підпису здійснюється за співвідношенням:

$$r \equiv s' - m' \times P_s \ (mod\ p) \quad (12)$$

Детальний доказ наведено у відповідних джерелах [4]. У межах даного дослідження ця схема використовується для програмної реалізації та експериментальної оцінки продуктивності її основних фаз.

Аналіз адаптації стандарту ДСТУ 4145-2002. Для практичного застосування технологій сліпого підпису в Україні важливим є використання національних криптографічних стандартів. У роботах [8, 9] запропоновано підхід до адаптації стандарту ДСТУ 4145-2002 для реалізації режиму сліпого підпису. Стандарт ДСТУ 4145-2002 базується на складності задачі дискретного логарифмування на еліптичній кривій (ECDLP) та визначає процедури генерації і перевірки цифрового підпису [5]. Основними параметрами є еліптична крива $E$, базова точка $G$, секретний ключ $d$ та відкритий ключ $Q = dG$. Адаптація стандарту передбачає введення етапу засліплення хеш-образу повідомлення та додаткову взаємодію між користувачем і підписувачем. Узагальнений алгоритм включає генерацію ефемерного ключа підписувачем, формування засліпленого хешу повідомлення користувачем, обчислення підпису та зняття сліпоти з отриманням фінального підпису $(r, s)$.

Оцінка безпеки адаптованої схеми дозволяє зробити наступні висновки. З точки зору криптографічної стійкості адаптована схема зберігає властивості безпеки базового стандарту, оскільки її захищеність ґрунтується на складності задачі ECDLP. Це унеможливлює відновлення секретного ключа або підробку підпису за поліноміальний час. Крім того, протокол забезпечує властивість незв'язності (unlinkability), що ускладнює встановлення відповідності між сеансом підписання та фінальним підписом.

Водночас важливою особливістю адаптації є феномен так званої «відстежуваної анонімності». На відміну від класичних схем сліпого підпису, де забезпечується повна незв'язність, у деяких варіантах реалізації ДСТУ 4145-2002 існують алгебраїчні залежності, які потенційно можуть дозволити підписувачу встановити зв'язок між підписом та сеансом взаємодії за наявності додаткових даних.

Таким чином, анонімність у цій схемі має умовний характер: пряма деанонімізація є обчислювально складною задачею, однак не виключається повністю. Це може розглядатися як недолік для систем із високими вимогами до приватності або як перевага для застосувань, де необхідна контрольована деанонімізація. Запропонована адаптація дозволяє інтегрувати механізм сліпого підпису в межах національного стандарту та використовується для теоретичного аналізу особливостей реалізації сліпих підписів на основі ECC.

## МЕТОДИКА ДОСЛІДЖЕННЯ

Методологія та програмне середовище дослідження. Для об'єктивної оцінки ефективності та підтвердження теоретичних переваг протоколів сліпого підпису на базі еліптичних кривих було проведено експериментальне моделювання базових криптографічних операцій. Реалізація схеми сліпого підпису на основі ECC базується на адаптованій версії схеми Дженга. Вихідний код розробленого програмного забезпечення розміщено у відкритому репозиторії на платформі GitHub [17].

Тестування продуктивності алгоритму RSA та алгоритмів на базі еліптичних кривих (ECC) проводилось на апаратній платформі з процесором AMD Ryzen 5 5600H (3.30 GHz) та 16 ГБ оперативної пам'яті під керуванням 64-розрядної ОС Windows. Для реалізації математичного апарату еліптичної криптографії та модульної арифметики використовувалися бібліотеки ecdsa та cryptography. Вимірювання часу виконання кожної фази (генерація ключів, формування підпису, верифікація)

здійснювалося за допомогою вбудованого модуля time (perf_counter) , що забезпечує високу точність вимірювань.

Для забезпечення статистичної достовірності кожна криптографічна операція алгоритмів ECC виконувалася 100 разів у циклі. Для ресурсоємних алгоритмів RSA на надвеликих ключах кількість ітерацій динамічно адаптувалася (від 2 до 50 разів) для оптимізації часу тестування На основі отриманих даних обчислювалося середнє арифметичне значення та середньоквадратичне відхилення у мілісекундах (мс).

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Експериментальні результати моделювання схем сліпого підпису. Під час практичного тестування було виміряно продуктивність схеми сліпого підпису Дженга для трьох стандартних еліптичних кривих NIST: P-256, P-384 та P-521. Результати програмного моделювання (табл. 2,3) демонструють високу ефективність алгоритму навіть при експоненціальному збільшенні криптографічної стійкості. Для проведення порівняльного аналізу в ідентичних апаратних умовах було також реалізовано базовий алгоритм сліпого підпису на основі RSA (схема Чаума) [1]. RSA-реалізація базується на класичній схемі Чаума та включає аналогічні фази протоколу: засліплення (blinding), підписування (signing) та зняття сліпоти (unblinding), що забезпечує коректність порівняння з ECC-реалізацією. З метою забезпечення еквівалентного рівня безпеки згідно з рекомендаціями NIST, тестування RSA-реалізації проводилось для ключів довжиною 3072, 7680 та 15360 біт.

*Таблиця 2*

**Середній час виконання фаз протоколу сліпого підпису на основі ECC (мс)**

| Еліптична крива (NIST) | Фаза 1: Засліплення (мс) | Фаза 2: Підпис (мс) | Фаза 3: Зняття сліпоти (мс) |
|---|---|---|---|
| P-256 | 3.57 ± 0.25 | 7.12 ± 0.46 | 3.69 ± 0.27 |
| P-384 | 8.11 ± 0.77 | 16.14 ± 0.86 | 8.29 ± 0.33 |
| P-521 | 17.10 ± 0.64 | 34.27 ± 1.18 | 17.63 ± 0.41 |

*Таблиця 3*

**Середній час виконання фаз протоколу сліпого підпису на основі RSA (мс)**

| Алгоритм | Фаза 1: Засліплення (мс) | Фаза 2: Підпис (мс) | Фаза 3: Зняття сліпоти (мс) |
|---|---|---|---|
| RSA-3072 | 0.42 ± 0.02 | 80.32 ± 1.87 | 0.80 ± 0.07 |
| RSA-7680 | 2.15 ± 0.01 | 1079.95 ± 1.95 | 4.70 ± 0.20 |
| RSA-15360 | 7.83 ± 0.01 | 7937.69 ± 14.35 | 16.98 ± 0.22 |

Значення наведено у вигляді середнього часу виконання та стандартного відхилення, обчислених за результатами багаторазових запусків. Низьке значення стандартного відхилення свідчить про стабільність отриманих результатів та відсутність суттєвого впливу випадкових факторів на процес вимірювання.

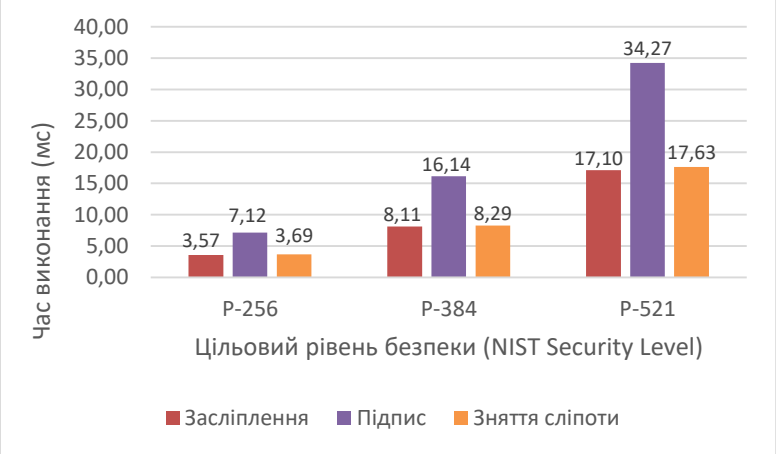


*Рис. 1 Порівняння часу виконання фаз сліпого підпису для алгоритмів на основі ECC.*

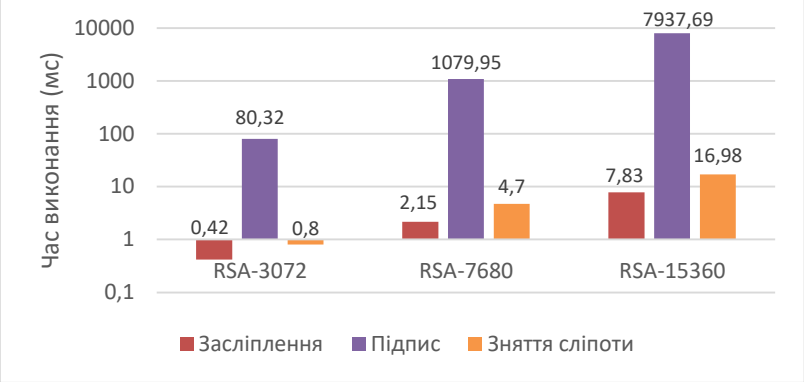


*Рис. 2 Порівняння часу виконання фаз сліпого підпису для алгоритмів RSA.*

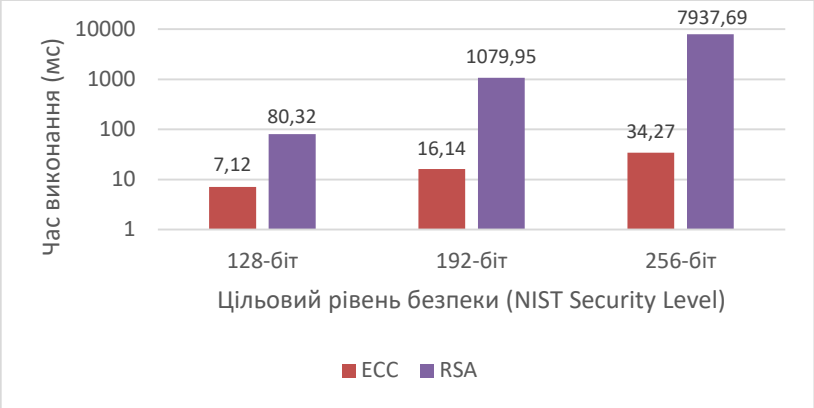


*Рис. 3 Порівняння часу генерації сліпого підпису для алгоритмів ECC та RSA при різних рівнях криптографічної стійкості.*

Еквівалентність криптографічної стійкості та розмір ключів. Фундаментальна різниця між класичним алгоритмом RSA та еліптичною криптографією полягає у математичних задачах, на яких вони базуються. Криптостійкість RSA спирається на задачу факторизації цілих чисел, для розв'язання якої існують субекспоненційні алгоритми. Натомість безпека ECC базується на складності задачі дискретного логарифмування на еліптичній кривій (ECDLP) [6, 7], для якої субекспоненційних методів розв'язання не знайдено. Це дозволяє ECC досягати аналогічного рівня безпеки при значно менших розмірах ключів. Згідно з офіційними рекомендаціями Національного інституту стандартів і технологій США (NIST SP 80057 Part 1 Rev. 5) [16], співвідношення довжини ключів для забезпечення еквівалентного цільового рівня безпеки наведено у табл. 4.

*Таблиця 4*

**Порівняння ефективності алгоритмів RSA та ECC для реалізації протоколів сліпого підпису**

| Цільовий рівень безпеки (NIST Security Level) | Довжина ключа RSA(біти) | Довжина ключа ECC(біти) | Співвідношення (RSA/ECC Size Factor) |
|---|---|---|---|
| 80 біт | 1024 | 160 | 1 : 6.4 |
| 112 біт | 2048 | 224 | 1 : 9.1 |
| 128 біт | 3072 | 256 | 1 : 12 |
| 192 біти | 7680 | 384 | 1 : 20 |
| 256 біт | 15360 | 512/521 | 1 : 30 / 1 : 29 |

Варто відзначити математичну специфіку вибору параметрів для максимального рівня безпеки (256 біт). Під час вибору параметрів кривої застосовується довжина ключа 521 біт, а не традиційні для інформатики 512 біт. Такий нетиповий розмір зумовлений використанням простих чисел Мерсенна, які мають вигляд $2^n - 1$ і дозволяють суттєво оптимізувати обчислення над скінченними полями. Оскільки число $2^{512} - 1$ не є простим, найближчим степенем, що генерує просте число Мерсенна для побудови безпечного криптографічного поля, є $n = 521$ [16].

Комплексна таблиця порівняння продуктивності: RSA проти ECC. Для всебічної оцінки

практичної імплементації протоколів сліпого підпису (наприклад, у системах e-cash або електронного голосування) необхідно проаналізувати комплекс параметрів: не лише математичний апарат, але й розміри ключів, обсяг фінального підпису та реальну швидкість криптографічних перетворень. У табл. 5 наведено зведене порівняння продуктивності класичної схеми Чаума (RSA-3072) та схеми Дженга (ECC-256), що базується на отриманих експериментальних даних для еквівалентного 128-бітного рівня безпеки.

*Таблиця 5*

**Порівняння продуктивності між RSA та ECC**

| Характеристика | Сліпий підпис RSA-3072 | Сліпий підпис на ECC-256 | Порівняльна перевага |
|---|---|---|---|
| Довжина ключа | 384 байт | 32 байти | ECC менший у 12 разів |
| Розмір фінального підпису | 384 байт | ~64-72 байти (дві координати $r, s$ ) | Розмір підпису ECC є істотно меншим |
| Математичний базис операцій | Модульна експоненціація (піднесення до величезного степеня $d$) | Скалярне множення точок еліптичної кривої | ECC забезпечує меншу обчислювальну складність при еквівалентному рівні безпеки |
| Швидкість генерації підпису | ≈ 80.32 мс | ≈ 7.12 мс | ECC демонструє значно менший час генерації підпису (приблизно у 10-12 разів швидше в експерименті) |
| Швидкість зняття сліпоти / верифікації | ≈ 0.80 мс | ≈ 3.69 мс | RSA демонструє вищу швидкість верифікації завдяки використанню малої відкритої експоненти (e = 65537) |

Дані з порівняльних таблиць ілюструють, що протоколи сліпого підпису на базі еліптичної криптографії є архітектурно та функціонально перевершуючими системами порівняно з алгоритмами на базі факторизації.

Аналіз результатів. Аналіз отриманих результатів свідчить про суттєві відмінності у продуктивності та ресурсних вимогах між алгоритмами сліпого підпису на основі RSA та еліптичних кривих. Згідно з табл. 5, застосування ECC дозволяє досягти значного зменшення розміру ключів і підписів при збереженні еквівалентного рівня криптографічної стійкості. Зокрема, довжина ключа для ECC-256 є у десятки разів меншою порівняно з RSA-3072, що позитивно впливає на ефективність зберігання та передачі даних [6, 16].

Експериментальні результати демонструють, що генерація сліпого підпису в схемах на основі ECC виконується значно швидше, ніж у випадку RSA, що зумовлено меншою обчислювальною складністю операцій скалярного множення точок еліптичної кривої порівняно з модульною експоненціацією великих чисел. Водночас встановлено, що операції зняття сліпоти та верифікації для RSA виконуються швидше, що пояснюється використанням малої відкритої експоненти, зокрема стандартного значення (e = 65537) [6].

Таким чином, результати дослідження підтверджують доцільність використання ECC у системах, де критичними є швидкість генерації підпису, компактність ключів та енергоефективність, тоді як RSA може залишатися доцільним вибором у сценаріях, де пріоритетом є швидка верифікація підписів. Важливо також відзначити характер зміни продуктивності алгоритмів залежно від рівня криптографічної стійкості. Зі збільшенням довжини ключа для ECC (від P-256 до P-521) спостерігається майже лінійне зростання часу виконання операцій. Натомість для алгоритмів на основі RSA зростання часу є значно швидшим і наближається до експоненційного характеру, що особливо помітно при переході від RSA-3072 до RSA-15360. Це свідчить про кращу масштабованість ECC при підвищенні рівня безпеки та підтверджує її доцільність для використання у довгострокових криптографічних системах. Зазначена тенденція також узгоджується з графічними результатами, наведеними на рис. 1-3 [7, 13].

Аналіз криптографічної стійкості. Криптографічна стійкість розглянутих схем базується на складності задачі дискретного логарифмування на еліптичній кривій (ECDLP), детально розглянутої у підрозділі, присвяченому задачі дискретного логарифмування на еліптичній кривій (ECDLP). З огляду на те, що найефективнішим відомим методом атаки є $\rho$-метод Полларда зі складністю порядку $O(\sqrt{n})$, використання параметрів, рекомендованих стандартами NIST, забезпечує практичну неможливість компрометації схеми [6, 16]. Водночас безпека практичної реалізації залежить від якості генерації випадкових параметрів (nonce), використання криптографічно стійких хеш-функцій та захисту від атак

побічними каналами. Недотримання цих вимог може призвести до компрометації секретного ключа незалежно від теоретичної стійкості алгоритму.

## ВИСНОВКИ

У результаті виконаного дослідження було проаналізовано теоретичні основи та практичні аспекти реалізації протоколів сліпого цифрового підпису на основі еліптичної криптографії. Особливу увагу приділено схемі Дженга, для якої здійснено програмну реалізацію та експериментальну оцінку продуктивності основних фаз протоколу.

Проведене експериментальне дослідження показало, що використання еліптичних кривих забезпечує суттєве підвищення ефективності генерації підпису порівняно з реалізаціями на основі RSA при еквівалентному рівні криптографічної стійкості. Зокрема, для кривої P-256 час виконання операції підпису є приблизно у 10-12 разів меншим, ніж для RSA-3072, що узгоджується з отриманими експериментальними даними. Водночас встановлено, що операції верифікації в RSA виконуються швидше, що пояснюється використанням малої відкритої експоненти.

Отримані результати також підтверджують, що застосування ECC дозволяє значно зменшити розмір ключів і підписів без втрати криптографічної стійкості, що є критично важливим для систем з обмеженими обчислювальними ресурсами. Це робить підходи на основі еліптичної криптографії доцільними для використання в таких прикладних областях, як електронне голосування, цифрові платіжні системи та IoT-середовища.

Окремо проаналізовано адаптацію стандарту ДСТУ 4145-2002 для реалізації сліпого підпису [5, 8], в межах якої виявлено особливість, пов’язану з феноменом відстежуваної анонімності. Це свідчить про необхідність врахування балансу між анонімністю та можливістю контрольованої деанонімізації при проєктуванні практичних систем.

Таким чином, результати роботи підтверджують доцільність використання схем сліпого підпису на основі ECC у сучасних інформаційних системах, де важливими є швидкодія, компактність криптографічних параметрів та забезпечення анонімності користувачів. Перспективою подальших досліджень є оптимізація реалізацій для апаратних платформ та дослідження стійкості схем у сучасних моделях криптографічної безпеки.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in cryptology (CRYPTO ’82)* (pp. 199-203).
2. Chen, M.-T., & Huang, H.-C. (2022). A practical and efficient node blind signcryption scheme for the IoT device network. *Applied Sciences, 12*(1), 278. https://doi.org/10.3390/app12010278.
3. Chunarova, A. (2013). Practical schemes for implementation of digital signature algorithms. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini*, 1(25), 81-87. (in Ukrainian).
4. DSTU 4145-2002. (2003). *Information technologies. Cryptographic information protection. Digital signature based on elliptic curves. Formation and verification*. Kyiv: Derzhstandart Ukrainy. (in Ukrainian).
5. Hankerson, D., Menezes, A. J., & Vanstone, S. (2004). *Guide to elliptic curve cryptography*. Springer.
6. Jeng, F.-G., Chen, T.-L., & Chen, T.-S. (2010). An ECC-based blind signature scheme. *Journal of Networks, 5*(8), 921–928. https://doi.org/10.4304/jnw.5.8.921-928.
7. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5.
8. Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptography. *Designs, Codes and Cryptography, 19*(2-3), 173-193. https://doi.org/10.1023/A:1008351012734.
9. Kossak, O., & Kholiavka, Y. (2014). Encryption using elliptic curves. *Visnyk Lvivskoho universytetu. Seriia mekhaniko-matematychna*, 79, 143-152. (in Ukrainian).
10. Kuchma, K. Y. (2026). Software implementation and experimental study of blind signature schemes (ECC vs RSA). *GitHub*. https://github.com/khrystyna-kuchma/ecc-vs-rsa-blind-signature.
11. Ma, R., & Du, L. (2022). Attribute-based blind signature scheme based on elliptic curve cryptography. *IEEE Access, 10*, 34221-34227. https://doi.org/10.1109/ACCESS.2022.3161237.
12. Miller, V. S. (1986). Use of elliptic curves in cryptography. In *Advances in cryptology – CRYPTO ’85* (pp. 417-426).

13. National Institute of Standards and Technology. (2020). *Recommendation for key management: Part 1 – General (Revision 5)* (NIST SP 800-57). https://doi.org/10.6028/NIST.SP.800-57pt1r5.
14. Ponomar, V. A. (2015). Mathematical model of the blind digital signature protocol. *Radiotekhnika*, 183, 163-168. (in Ukrainian).
15. Reyes-Macedo, V., Kawachi, A., Gallegos-García, G., & Salinas-Rosales, M. (2024). A threshold-blind signature scheme and its application in blockchain-based systems. *IEEE Access*.
16. Schoof, R. (1995). Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, *7*(1), 219-254.
17. Yesina, M. V. (2015). Mathematical model of blind signature protocol on elliptic curves. *Prykladna radioelektronika*, *14*(4), 300-305. (in Ukrainian).

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (33), 2026
ISSN 2663 – 4023

**Ivan Opirskyy**
Doctor of Technical Sciences, Professor, Head of the Information Protection Department
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-8461-8996
*ivan.r.opirskyi@lpnu.ua*

**Khrystyna Kuchma**
Student, Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0001-9093-6819
*khrystyna.kuchma.kb.2025@lpnu.ua*

## SOFTWARE IMPLEMENTATION AND EXPERIMENTAL RESEARCH OF BLIND SIGNATURE SCHEMES BASED ON ECC

**Abstract.** This paper investigates the efficiency of blind digital signature schemes based on Elliptic Curve Cryptography (ECC) compared to classical RSA-based implementations. The relevance of the study is driven by the increasing need for user anonymity in electronic voting systems, digital payments, and other applications requiring a clear distinction between authentication and identification. As part of the research, the Fuh-Gwo Jeng blind signature scheme was implemented using the Python programming language and modern cryptographic libraries. Experimental measurements of the performance of the main protocol phases – blinding, signing, and unblinding – were conducted for the NIST elliptic curves P-256, P-384, and P-521. To ensure objective results, a comparative analysis was performed against an RSA-based blind signature implementation at equivalent cryptographic strength levels. The obtained results demonstrate that the use of ECC significantly improves signature generation efficiency: for the P-256 curve, the average operation time is 7-8 ms, which is approximately 10-12 times faster than RSA-3072. It was established that the reduction in key sizes and computational complexity provides a substantial advantage for ECC in resource-constrained environments.
The scientific novelty lies in the software implementation of the Jeng scheme and the experimental comparison of its performance with RSA across various security levels. The practical significance of the results is the possibility of applying the proposed approach in systems with high requirements for speed and energy efficiency.

**Keywords:** Elliptic Curve Cryptography (ECC), blind digital signature, elliptic curves, anonymity, Elliptic Curve Discrete Logarithm Problem (ECDLP), Fuh-Gwo Jeng Scheme, DSTU 4145-2002, traceable anonymity.

### REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Chaum, D. (1983). Blind signatures for untraceable payments. In *Advances in cryptology (CRYPTO ’82)* (pp. 199-203).
2. Chen, M.-T., & Huang, H.-C. (2022). A practical and efficient node blind signcryption scheme for the IoT device network. *Applied Sciences, 12*(1), 278. https://doi.org/10.3390/app12010278.
3. Chunarova, A. (2013). Practical schemes for implementation of digital signature algorithms. *Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v Ukraini*, 1(25), 81-87. (in Ukrainian).
4. DSTU 4145-2002. (2003). *Information technologies. Cryptographic information protection. Digital signature based on elliptic curves. Formation and verification*. Kyiv: Derzhstandart Ukrainy. (in Ukrainian).
5. Hankerson, D., Menezes, A. J., & Vanstone, S. (2004). *Guide to elliptic curve cryptography*. Springer.
6. Jeng, F.-G., Chen, T.-L., & Chen, T.-S. (2010). An ECC-based blind signature scheme. *Journal of Networks, 5*(8), 921–928. https://doi.org/10.4304/jnw.5.8.921-928.
7. Koblitz, N. (1987). Elliptic curve cryptosystems. *Mathematics of Computation, 48*(177), 203-209. https://doi.org/10.1090/S0025-5718-1987-0866109-5.
8. Koblitz, N., Menezes, A., & Vanstone, S. (2000). The state of elliptic curve cryptography. *Designs, Codes and Cryptography, 19*(2-3), 173-193. https://doi.org/10.1023/A:1008351012734.

9. Kossak, O., & Kholiavka, Y. (2014). Encryption using elliptic curves. *Visnyk Lvivskoho universytetu. Seriia mekhaniko-matematychna*, 79, 143-152. (in Ukrainian).
10. Kuchma, K. Y. (2026). Software implementation and experimental study of blind signature schemes (ECC vs RSA). *GitHub*. https://github.com/khrystyna-kuchma/ecc-vs-rsa-blind-signature.
11. Ma, R., & Du, L. (2022). Attribute-based blind signature scheme based on elliptic curve cryptography. *IEEE Access*, *10*, 34221-34227. https://doi.org/10.1109/ACCESS.2022.3161237.
12. Miller, V. S. (1986). Use of elliptic curves in cryptography. In *Advances in cryptology – CRYPTO '85* (pp. 417-426).
13. National Institute of Standards and Technology. (2020). *Recommendation for key management: Part 1 – General (Revision 5)* (NIST SP 800-57). https://doi.org/10.6028/NIST.SP.800-57pt1r5.
14. Ponomar, V. A. (2015). Mathematical model of the blind digital signature protocol. *Radiotekhnika*, 183, 163-168. (in Ukrainian).
15. Reyes-Macedo, V., Kawachi, A., Gallegos-García, G., & Salinas-Rosales, M. (2024). A threshold-blind signature scheme and its application in blockchain-based systems. *IEEE Access*.
16. Schoof, R. (1995). Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, *7*(1), 219-254.
17. Yesina, M. V. (2015). Mathematical model of blind signature protocol on elliptic curves. *Prykladna radioelektronika*, *14*(4), 300-305. (in Ukrainian).

Отримано редакцією журналу / Received: 13.02.26
Прорецензовано / Revised: 27.02.26
Схвалено до друку / Accepted: 25.06.26