УДК 004.056.55

А. В. Василина

АНАЛІЗ СУЧАСНИХ КРИПТОГРАФІЧНИХ СХЕМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Вінницький національний технічний університет

Анотація

У роботі проведено аналіз класичних та сучасних схем електронного цифрового підпису, включно з індивідуальними, пороговими, кільцевими, груповими та делегованими підписами. Визначено їхні функціональні властивості та принципи побудови. Виконано порівняльний аналіз та формалізовано сильні та слабкі сторони, а також визначено рекомендації щодо застосування в інформаційних системах з урахуванням вимог безпеки та обмежень практичного застосування. Визначено напрямки подальшого розвитку електронних підписів і проблеми, що залишаються відкритими для майбутніх досліджень.

Ключові слова: електронний цифровий підпис, пороговий підпис, кільцевий підпис, груповий підпис, делегований підпис, кібербезпека.

Abstract

The article analyzes classic and modern electronic digital signature schemes, including individual, threshold, ring, group and delegated signatures. Their functional properties and construction principles are determined. A comparative analysis was performed and strengths and weaknesses were formalized, as well as recommendations for use in information systems were determined, taking into account security requirements and limitations of practical application. Directions for the further development of electronic signatures and problems that remain open for future research have been determined.

Keywords*: electronic digital signature, threshold signature, ring signature, group signature, delegated signature, cybersecurity.*

Вступ

Електронний цифровий підпис є ключовим механізмом забезпечення автентичності та цілісності даних у сучасних інформаційних системах. Його широке застосування зумовлене тим, що більшість країн світу впровадили законодавчі норми, які регулюють використання електронних підписів як повноцінної заміни фізичних. Зокрема такий закон є чинним в Україні [1], який визначає поняття кваліфікованого електронного підпису. Завдяки цьому електронний цифровий підпис став базовим інструментом у сфері електронного документообігу, банківських операцій, державних послуг та багатьох інших галузях.

Розвиток криптографії сприяв появі нових класів алгоритмів підпису – групових, порогових, кільцевих та делегованих, які забезпечують додаткові властивості, недосяжні для класичних алгоритмів. Ці методи дозволяють здійснювати підписання групою учасників, зберігати анонімність підписувача, реалізовувати колективні рішення чи делегування повноважень. Хоча такі алгоритми не підпадають під пряме законодавче регулювання, вони мають перспективу застосування у спеціалізованих системах безпеки, зокрема у корпоративних, технічних та розподілених середовищах.

Метою роботи є розширення функціональних можливостей електронних цифрових підписів за рахунок визначення перспектив застосування новітніх підходів до їх побудови. Завданнями є порівняння різних типів підписів, визначення їхніх сильних і слабких сторін та формування рекомендацій щодо можливого застосування у реальних системах.

Результати дослідження

Електронний цифровий підпис є одним із ключових механізмів криптографічного захисту інформації. Згідно із Законом України «Про електронний цифровий підпис» [2], електронний цифровий підпис – це вид електронного підпису, отриманого в результаті криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого (секретного) ключа та перевіряється за допомогою відкритого ключа.

Формальна модель цифрового підпису включає три базові алгоритми:

– генерування ключів (KeyGen) – створення пари ключів: секретного *sk* та відкритого *pk*;
– підписування (Sign) – обчислення підпису $\sigma = Sign(sk, m)$ для повідомлення *m*;
– верифікування (Verify) – перевірку правильності підпису $Verify(pk, m, \sigma) \rightarrow \{True, False\}$.

Коректність схеми вимагає виконання властивості:

$$Verify(pk, m, Sign(sk, m)) = True$$

для будь-якої коректно згенерованої пари ключів і будь-якого повідомлення [3]. Електронний цифровий підпис має забезпечувати три ключові властивості: автентичність підписувача, цілісність підписаних даних та невідмовність від факту підписання. Ці характеристики досягаються завдяки використанню криптографічних алгоритмів, які унеможливлюють підробку підпису без знання секретного ключа.

Класичні криптографічні алгоритми сформували основу сучасних систем автентифікації та захисту даних. Вони базуються на складності фундаментальних математичних задач, що забезпечують неможливість підробки підпису без знання секретного ключа. До найпоширеніших алгоритмів належать RSA, DSA, ECDSA та EdDSA [4], які використовуються у стандартах електронного документообігу, інфраструктурі відкритих ключів та протоколах безпеки.

Алгоритм RSA [4] є одним із найдавніших і найпоширеніших криптографічних алгоритмів, заснованих на факторизації великого числа $n = p \cdot q$, де p і q – великі прості числа. Підписування здійснюється шляхом піднесення загешованого повідомлення до степеня секретного ключа, а перевірка – до степеня відкритого ключа модулем *n*.

DSA [4] ґрунтується на складності задачі дискретного логарифмування у мультиплікативній групі простого модуля. Алгоритм використовує випадкове значення *k* (nonce – одноразове випадкове число) для формування пари підпису *(r, s)*, що робить кожне підписування унікальним. Однак повторне використання або передбачуваність *k* призводить до розкриття секретного ключа, що є критичною вразливістю DSA.

ECDSA [4] є аналогом DSA, побудованим на групах точок еліптичних кривих. Завдяки використанню задачі дискретного логарифмування на еліптичних кривих, алгоритм забезпечує рівень безпеки еквівалентний RSA, з використанням значно менших ключів (256 біт проти 4096 в RSA). Процес створення та перевірки підпису аналогічний DSA, але всі операції виконуються в групі точок еліптичної кривої.

EdDSA [4] – сучасний алгоритм цифрового підпису, який використовує криві Едвардса й детермінований механізм формування nonce, що усуває проблему слабкої генерації випадкових чисел, притаманну DSA та ECDSA.

Індивідуальний електронний цифровий підпис є базовою формою цифрового підписування, у якій один підписувач використовує власну пару криптографічних ключів – секретний для створення підпису та відкритий для його перевірки [5]. Такі підписи реалізуються за допомогою розглянутих класичних алгоритмів асиметричної криптографії [4], що забезпечують автентичність підписувача, цілісність даних і невідмовність від факту підписання. Серед сильних сторін індивідуального ЕЦП — простота моделі, стандартизованість, висока сумісність з відомими інфраструктурами та передбачувані властивості безпеки (автентичність, цілісність, невідмовність, стійкість до підроблення, односторонність та коректність). Основним недоліком є повна залежність від захищеності одного секретного ключа: його компрометація робить можливим створення підроблених підписів і ставить під загрозу всі попередні транзакції. У реальних системах індивідуальні підписи доцільно застосовувати у середовищах із чітким персональним контролем доступу, у системах електронного документообігу, банківських сервісах та державних реєстрах, доповнюючи їх апаратними засобами захисту (HSM, смарт-карти) та політиками регулярної ротації ключів.

Подальший розвиток криптографії сприяв появі схем цифрового підпису з можливостями, недосяжними для класичних алгоритмів, зокрема колективним підписанням, забезпеченням анонімності або делегуванням повноважень. Такі підходи застосовуються там, де звичайний підпис не забезпечує потрібної гнучкості чи рівня безпеки.

Порогові підписи [6] — це схема, у якій для створення цифрового підпису необхідна участь щонайменше *t* учасників із *n* можливих. Ключовою технічною основою таких схем є метод секретного розподілу Шаміра, у якому секрет (у тому числі секретний ключ) розподіляється між учасниками у вигляді часток, і його можна відновити лише за наявності достатньої кількості цих часток [7].

До сильних сторін порогових підписів належать колективний контроль, відмовостійкість та можливість безпечного управління критичними операціями. Водночас такі схеми мають і слабкі місця — складність протоколів, інтерактивність процесу підписання та потребу у надійному керуванні частками секрету. Щодо

застосування, порогові підписи доцільно використовувати там, де рішення приймається колегіально або де високий ризик компрометації ключа однієї особи: у керуванні доступом до критичних ресурсів, банківських і корпоративних системах високої вартості, багаторівневих інфраструктурах безпеки та сервісах, де важлива відмовостійкість. У малих організаціях або середовищах без налагодженого управління ключами такі схеми можуть бути надмірно складними.

Кільцеві підписи [8] дозволяють одному учаснику сформувати підпис від імені групи так, що сторона, яка верифікує, може впевнитися, що підпис був створений одним із членів групи, але не може встановити, ким саме. Для цього підписувач використовує свій секретний ключ та відкриті ключі інших учасників, формуючи анонімний підпис без їхнього залучення.

Однією з ключових властивостей таких схем є повна децентралізованість: для створення підпису не потрібно організовувати групу чи звертатися до центру керування — підписувач самостійно вибирає набір відкритих ключів, у колі яких він хоче залишатися анонімним. Сильні сторони кільцевих підписів полягають у здатності забезпечувати високий рівень анонімності та відсутності довірених третіх сторін, що робить їх привабливими для сценаріїв, де джерело інформації потребує захисту. Водночас такі схеми мають і значні обмеження: неможливість встановлення автора у разі зловживання, збільшення розміру підпису зі збільшенням групи, а також залежність рівня анонімності від правильного вибору ключів у кільці. У практичних системах кільцеві підписи доцільно використовувати в анонімних каналах інформування, у середовищах, де важливо зберегти конфіденційність автора повідомлення, або в умовах, коли неможливо забезпечити централізовану інфраструктуру керування учасниками. Однак вони не підходять для регульованих сфер або критичних систем, де необхідна підзвітність та можливість розслідування інцидентів.

Групові підписи [9] також забезпечують анонімність підписувача, але на відміну від кільцевих схем, передбачають наявність централізованого керування групою. У системі визначаються дві ключові ролі: менеджер групи, який відповідає за додавання та відкликання учасників, та менеджер відкриття, який має можливість розкрити особу підписувача у разі необхідності.

Сильні сторони групових підписів полягають у поєднанні анонімності з контрольованою підзвітністю, можливості централізованого управління групою та відносній ефективності перевірки підписів незалежно від кількості учасників. Слабкими сторонами є залежність від довірених органів керування, складність побудови безпечної інфраструктури, необхідність захисту ключа відкриття та підвищені обчислювальні витрати порівняно з індивідуальними схемами. Рекомендовано застосовувати групові підписи у корпоративних або міжорганізаційних системах, де необхідно забезпечити анонімність користувачів, але зберегти можливість встановлення відповідальності — наприклад, у системах звітування, голосування, аудиту або внутрішнього контролю. Їх недоцільно використовувати там, де неможливо гарантувати захист ролей менеджера групи або відсутня інфраструктура довіри.

Делеговані підписи [10] дозволяють власнику секретного ключа надати іншому користувачеві право підписувати повідомлення від його імені без передачі самого секретного ключа. Делегування реалізується шляхом створення спеціального проксі-ключа, який має обмежені повноваження, наприклад обмеження за часом, типом документів або контекстом використання.

Сильні сторони таких схем полягають у можливості точного контролю повноважень, збереженні недоторканості основного секретного ключа та забезпеченні гнучкості в багаторівневих організаційних структурах. Недоліками є складність правильного формування політик делегування, потреба у надійному механізмі відкликання делегованих ключів і можливі ризики зловживання у разі неправильної конфігурації. У реальних системах делеговані підписи доцільно застосовувати для організації керованих робочих процесів, у сервісах автоматизації, у корпоративних і фінансових структурах, де окремі дії можуть виконуватися довіреними агентами. Такі схеми не рекомендується використовувати у середовищах, де неможливо забезпечити оперативне відкликання делегованих ключів або де рішення мають критичну юридичну вагу.

Таблиця 1 - Порівняльна таблиця схем цифрового підпису

Критерій	Індивідуальний підпис	Пороговий підпис	Кільцевий підпис	Груповий підпис	Делегований підпис
Кількість підписувачів	1 підписувач	t із n	1 із групи, не визначається	1 із групи з можливістю відкриття	Підписувач діє від імені власника
Анонімність	Відсутня	Відсутня	Висока	Середня, керована	Відсутня

Критерій	Індивідуальний підпис	Пороговий підпис	Кільцевий підпис	Груповий підпис	Делегований підпис
Розмір підпису	Малого розміру	Малого розміру	Зростає лінійно	Середній	Малого розміру
Потреба в координації	Немає	Висока (керування збором t частин)	Немає	Висока (керування групою)	Середня (делегування/відкликання)
Типові сфери застосування	Е-документообіг, банківські сервіси	Критичні системи, управління доступом	Анонімні повідомлення, захист викривачів	Корпоративні системи зі звітністю	Корпоративне управління, автоматизація
Основний ризик	Компрометація єдиного ключа	Недоступність учасників / складність протоколу	Неможливість деанонімізації при зловживанні	Надмірна централізація довіри	Неправильне управління делегуванням

Розглянуті алгоритми цифрових підписів демонструють різні способи забезпечення автентичності та цілісності даних. Класичні індивідуальні підписи залишаються універсальними, тоді як порогові, кільцеві, групові та делеговані підписи розширюють можливості систем за рахунок колективності, анонімності чи делегування повноважень. Вибір схеми визначається конкретними вимогами до надійності, продуктивності, конфіденційності та підзвітності.

Висновки

Таким чином, розглянуті схеми цифрового підпису демонструють різноманітність криптографічних підходів до забезпечення автентичності даних та управління повноваженнями, однак попри значний прогрес залишаються відкриті питання щодо їх масштабованості, стійкості до нових типів атак і практичного впровадження в складних системах. Подальший розвиток технологій вимагає удосконалення механізмів безпечного керування ключами, протоколів колективної взаємодії та підвищення стійкості до квантових обчислень. Комплексне дослідження цих аспектів є необхідним для створення більш надійних, гнучких і довготривалих систем електронного підпису.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про електронну ідентифікацію та електронні довірчі послуги : Закон України від 01.12.2022 № 2801-IX. URL: https://zakon.rada.gov.ua/laws/show/2155-19#n534 (дата звернення: 20.11.2025).
2. Про електронний цифровий підпис : Закон України від 22.05.2003 № 852-IV. URL: https://zakon.rada.gov.ua/laws/show/852-15#Text (дата звернення: 20.11.2025).
3. Patrick Struck and Maximiliane Weishäupl. A Framework for Advanced Signature Notions. *IACR Cryptol. ePrint Arch.*, paper 960, 2025. URL: https://eprint.iacr.org/2025/960 (Last accessed: 20.11.2025).
4. FIPS PUB 186-5. Digital Signature Standard (DSS) : Federal Information Processing Standards Publication. – Gaithersburg, MD : National Institute of Standards and Technology, 2023. URL: https://doi.org/10.6028/NIST.FIPS.186-5 (Last accessed: 22.11.2025).
5. R. Rivest, A. Shamir and L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978. URL: https://doi.org/10.1145/359340.359342 (Last accessed: 23.11.2025).
6. Chelsea Komlo and Ian Goldberg. FROST: Flexible Round-Optimized Schnorr Threshold Signatures. *IACR Cryptol. ePrint Arch.*, paper 852, 2020. URL: https://eprint.iacr.org/2020/852 (Last accessed: 23.11.2025).
7. Shamir, Adi. "How to Share a Secret." *Communications of the ACM*, vol. 22, no. 11, 1979, pp. 612–613. URL: https://doi.org/10.1145/359340.359342 (Last accessed: 23.11.2025).
8. Bender, A., Katz, J., Morselli, R. Ring signatures: stronger definitions, and constructions without random oracles. *Proceedings of the 3rd Theory of Cryptography Conference (TCC 2006)*. URL: https://ia.cr/2005/304 (Last accessed: 24.11.2025).
9. Manulis, M., Fleischhacker, N., Günther, F., Kiefer, F., Poettering, B. *Group Signatures: Authentication with Privacy*. Bonn : BSI, 2012. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/GruPA/GruPA.html (Last accessed: 25.11.2025).
10. Michael Backes, Sebastian Meiser and Dominique Schröder. Delegatable Functional Signatures. *IACR Cryptol. ePrint Arch.*, paper 408, 2013. URL: https://eprint.iacr.org/2013/408 (Last accessed: 27.11.2025).

Василина Анастасія Василівна – студентка групи 2БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: nstvsln@gmail.com.

Науковий керівник: ***Баришев Юрій Володимирович*** — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: yuriy.baryshev@vntu.edu.ua.

Anastasiia Vasylyna - student of group 2BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Yurii Baryshev*** —PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia.