УДК 004.056.55

**А. В. Василина**

# ГРУПОВІ ПІДПИСИ ЯК МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ ТА ПІДЗВІТНОСТІ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Вінницький національний технічний університет

**Анотація**

*У роботі розглянуто криптографічні схеми групових підписів як механізм забезпечення анонімної участі суб'єктів із можливістю контрольованого розкриття їхньої ідентичності. Проаналізовано формальну модель групового підпису, базові властивості безпеки та сучасні ефективні реалізації на основі білінійних відображень. Розглянуто підходи до селективної та конвертованої зв'язуваності підписів як розширення класичних схем групових підписів. Показано перспективи застосування групових підписів в інформаційних системах із підвищеними вимогами до приватності та підзвітності, зокрема в електронних закупівлях та інших електронних сервісах.*

**Ключові слова:** груповий підпис, криптографія, анонімність, невідслідковуваність, нульове розголошення, кібербезпека.

**Abstract**

*The article considers cryptographic group signature schemes as a mechanism for ensuring anonymous participation of entities with the possibility of controlled identity disclosure. The formal model of group signatures, basic security properties, and modern efficient constructions based on bilinear pairings are analyzed. Approaches to selective and convertible linkability are briefly discussed as extensions of classical group signature schemes. The applicability of group signatures in information systems with increased privacy and accountability requirements is outlined, in particular in electronic procurement systems and other electronic services.*

**Keywords:** group signature, cryptography, anonymity, unlinkability, zero-knowledge, cybersecurity.

## Вступ

Забезпечення балансу між прозорістю функціонування інформаційних систем та захистом учасників є актуальною проблемою сучасної кібербезпеки. У низці прикладних сценаріїв необхідно підтвердити належність суб'єкта до певної групи без розкриття його конкретної ідентичності, водночас зберігаючи можливість подальшої ідентифікації у разі порушення правил або виникнення суперечок. Групові підписи є криптографічним примітивом, що дозволяє реалізувати такий підхід. Вони забезпечують анонімність підписувача для зовнішніх спостерігачів і водночас підтримують механізм контрольованого розкриття особи спеціально уповноваженим суб'єктом. Зростання ролі електронних закупівель, електронного голосування та інших електронних сервісів зумовлює актуальність дослідження формальних моделей і практичних реалізацій групових підписів.

Метою роботи є покращення захисту неув'язності користувачів за рахунок застосування криптографічних схем групових підписів в інформаційних системах. Завданнями роботи є розгляд формальної моделі групового підпису, аналіз базових криптографічних властивостей, дослідження сучасних реалізацій та обґрунтування доцільності їх практичного використання.

## Результати дослідження

У межах дослідження проаналізовано формальні моделі криптографічних схем групових підписів та їхні базові властивості безпеки. Показано, що групові підписи дозволяють реалізувати механізм підтвердження належності суб'єкта до визначеної групи без розкриття його ідентичності, зберігаючи можливість контрольованого розкриття особи спеціально уповноваженим суб'єктом.

Криптографічні схеми групових підписів (group signatures), формалізують зазначений підхід шляхом введення спеціальної ролі менеджера групи та набору алгоритмів, що визначають життєвий цикл підпису.

Актуальність дослідження групових підписів зростає у зв'язку з розвитком електронних сервісів, зокрема систем електронних закупівель, де необхідно мінімізувати ризики тиску, дискримінації або змови між учасниками без зниження рівня підзвітності та контролю.

У межах інфраструктури групового підпису виокремлюється спеціальна привілейована роль менеджера групи, який відповідає за ініціалізацію криптографічних параметрів системи, приєднання нових учасників до групи та, за наявності визначених підстав, ідентифікацію підписувачів. Така модель передбачає централізований контроль операцій розкриття при збереженні анонімності учасників у штатному режимі функціонування системи.

Формально схема групового підпису визначається як сукупність алгоритмів: $GS = (Setup, Join, Sign, Verify, Open)$, які реалізують повний життєвий цикл системи — від генерації криптографічних параметрів до створення, перевірки та контрольованого розкриття підписів. Окремі алгоритми використовують випадковість для досягнення криптографічних властивостей, зокрема анонімності та невідслідковуваності, тоді як алгоритми перевірки та розкриття є детермінованими [2].

Setup — алгоритм ініціалізації, який виконується менеджером групи. У результаті генеруються публічні параметри системи та публічний ключ групи gpk, а також секретні ключі керування, зокрема ключ розкриття особи підписувача.

Join — протокол приєднання нового члена до групи, у ході якого учасник після автентифікації отримує секретний ключ підпису. Менеджер групи зберігає інформацію, необхідну для подальшого розкриття особи підписувача.

Sign — алгоритм створення підпису, за допомогою якого член групи формує груповий підпис на повідомленні. Підпис підтверджує, що повідомлення підписане легітимним членом групи, але не розкриває його ідентичність.

Verify — алгоритм перевірки, який дозволяє будь-якому верифікатору перевірити дійсність підпису, використовуючи лише gpk, повідомлення та підпис.

Open — алгоритм розкриття, який виконується менеджером групи з метою ідентифікації конкретного члена групи, що створив підпис.

До базових властивостей групових підписів належать:

- Анонімність — обчислювальна нерозрізненність підписів різних членів групи без доступу до ключа розкриття.
- Невідслідковуваність — неможливість встановити, чи були два різні підписи створені одним і тим самим членом групи.
- Непідробність — лише легітимні члени групи здатні створювати дійсні підписи.
- Нефреймовність (non-frameability) — навіть менеджер групи не може підробити підпис так, щоб звинуватити чесного члена.

Формальні визначення та ігрові моделі безпеки цих властивостей наведені у фундаментальній роботі Mihir Bellare, Daniele Micciancio та Bogdan Warinschi [2].

Однією з найбільш впливових практичних реалізацій є схема коротких групових підписів, запропонована Dan Boneh, Xavier Boyen та Hovav Shacham [3]. Її ключовою перевагою є константний розмір підпису, який не залежить від кількості членів групи.

Схема базується на білінійних групах простого порядку та припущенні складності задачі q-Strong Diffie–Hellman. Підпис формується як доказ знання з нульовим розголошенням володіння коректним сертифікатом членства, а перевірка здійснюється шляхом відновлення проміжних значень та перевірки геш-челенджу у стилі перетворення Fiat–Shamir [3]. Ефективність цієї схеми робить її придатною для практичних систем з великою кількістю учасників та високими вимогами до масштабованості.

Класичні групові підписи забезпечують повну невідслідковуваність, однак у деяких прикладних сценаріях виникає потреба у контрольованому зв’язуванні підписів одного й того ж учасника. Сучасні дослідження пропонують підходи до так званої селективної або конвертованої зв’язуваності.

Зокрема, у роботі Lukas Garms та Anja Lehmann [4] запропоновано модель, у якій підписи за замовчуванням залишаються незв’язуваними, але можуть бути перетворені у зв’язуваний вигляд спеціальним уповноваженим суб’єктом за наявності правових підстав. Такий підхід дозволяє поєднати сильну анонімність з можливістю обмеженого аналізу поведінки учасників без повного розкриття їхньої ідентичності.

Системи електронних державних закупівель, як і низка інших інформаційних систем із підвищеними вимогами до приватності, характеризуються необхідністю одночасного забезпечення відкритості процедур і захисту економічних інтересів учасників. Аналогічна суперечність між прозорістю та анонімністю виникає у системах електронного голосування, анонімної автентифікації, захисту інформаторів та експертного рецензування. У всіх зазначених випадках

після завершення окремих етапів взаємодії або прийняття рішень інформація про суб'єктів може ставати доступною широкому колу осіб, що потенційно створює ризики небажаного впливу, кореляційного аналізу або координації дій.

У цьому контексті групові підписи можуть використовуватися як універсальний криптографічний механізм анонімної участі суб'єктів на початкових етапах процедур з подальшим контрольованим розкриттям інформації у разі виникнення визначених умов. Зокрема, в електронних закупівлях це відповідає анонімній подачі тендерних пропозицій, у системах голосування — таємному поданню бюлетенів, у системах контролю доступу — підтвердженню членства в групі без ідентифікації користувача, а в системах захисту інформаторів — доведенню належності джерела до організації без розкриття його особи.

Можлива архітектура впровадження групових підписів у таких системах передбачає наявність чітко розмежованих ролей:

- менеджер групи, який здійснює первинну автентифікацію суб'єктів та видає їм криптографічні ключі групового підпису;
- прикладна платформа, що приймає та автоматично перевіряє групові підписи без доступу до інформації про конкретного підписувача;
- орган розкриття та аудиту, уповноважений ініціювати процедуру ідентифікації підписувача за наявності правових або регламентних підстав.

У такій моделі участь у процедурі — подання пропозицій, голосів, повідомлень або автентифікаційних запитів — здійснюється анонімно, тоді як ідентифікація конкретного суб'єкта можлива лише після завершення об'єктивної перевірки результатів або у разі виявлення порушень. Це дозволяє формалізувати баланс між анонімністю та підзвітністю на криптографічному рівні.

Впровадження групових підписів у національні інформаційні системи, зокрема у сфері електронних закупівель, електронного голосування та державних сервісів доступу, потребує нормативного врегулювання, включно з визначенням їх правового статусу та процедур контрольованого розкриття особи підписувача. Доцільним видається гібридний підхід, за якого групові підписи застосовуються на етапах, де критичною є анонімність і невідслідковуваність дій учасників, тоді як завершальні юридично значущі дії виконуються із застосуванням персоналізованих кваліфікованих електронних підписів.

## Висновки

Таким чином, групові підписи є перспективним криптографічним механізмом забезпечення анонімної участі суб'єктів із можливістю контрольованого розкриття ідентичності. Разом із тим залишаються відкритими питання практичної інтеграції таких схем у національні інформаційні системи, зниження рівня довіри до менеджера групи та формалізації правових процедур розкриття, що визначає напрями подальших досліджень у цій галузі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. D. Chaum, E. van Heyst. Group Signatures. Advances in Cryptology - EUROCRYPT '91, LNCS 547, 1991, pp. 257-265. URL: https://link.springer.com/content/pdf/10.1007/3-540-46416-6_22.pdf (accessed: 24.01.2026).
2. Bellare M., Micciancio D., Warinschi B. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. Advances in Cryptology — EUROCRYPT 2003. Lecture Notes in Computer Science, vol 2656. Springer, 2003. P. 614-629.
3. D. Boneh, X. Boyen, H. Shacham. Short Group Signatures. URL: https://crypto.stanford.edu/~dabo/papers/groupsigs.pdf (accessed: 25.01.2026).
4. L. Garms, A. Lehmann. Group Signatures with Selective Linkability. URL: https://eprint.iacr.org/2019/027.pdf (accessed: 25.01.2026).



***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, e-mail: nstvsln@gmail.com.

Supervisor: ***Yurii Baryshev*** —PhD (eng), associated professor of information protection department, Vinnytsia National Technical University, Vinnytsia, email: yuriy.baryshev@vntu.edu.ua.