УДК 004.056

Вадим ШУХМАНН, Дмитро СМИРНОВ, Владислав КОНДРАТЮК

Західноукраїнський національний університет

ПОРОГОВА СХЕМА ЦИФРОВОГО ПІДПИСУ ДЛЯ ЗАХИСТУ АНОНІМНОСТІ В БЛОКЧЕЙНІ

Вступ. Технологія блокчейн революціонізує багато галузей, від фінансів до логістики та Інтернет речей. Одним із ключових аспектів безпеки блокчейну є цифровий підпис, який гарантує автентичність та цілісність даних. У контексті децентралізованих систем важливим є поняття порогових схем, які дозволяють розподіляти контроль над приватним ключем між кількома учасниками [1].

Актуальність дослідження обумовлена постійним зростанням інтересу до технології блокчейн та необхідністю забезпечення високого рівня безпеки децентралізованих систем. Вибір оптимального алгоритму цифрового підпису для порогової схеми є критичним рішенням, яке впливає на ефективність і надійність всієї системи [2].

Порогові схеми дозволяють розподіляти повноваження підписанта між кількома учасниками, що забезпечує додатковий рівень захисту та надійності системи. Такі схеми широко застосовуються у фінансових транзакціях, управлінні розподіленими базами даних, блокчейнах та інших системах з високими вимогами до безпеки. Вибір оптимального алгоритму цифрового підпису є важливим завданням при розробці та впровадженні порогових схем, оскільки він впливає на ефективність та швидкодію системи, а також на стійкість до атак.

Мета: аналіз ефективності алгоритмів цифрового підпису для побудови порогових схем.

1. Порогова схема цифрового підпису

Порогові схеми (threshold schemes) - це криптографічні протоколи, які дозволяють розподілити секретний ключ (наприклад, приватний ключ для цифрового підпису) між кількома учасниками. Для відновлення секретного ключа або створення підпису необхідна участь лише певної кількості учасників (поріг).

Алгоритми цифрового підпису в порогових схемах відіграють ключову роль у забезпеченні безпеки та ефективності таких систем.

В порогових схемах використовуються наступні алгоритми цифрового підпису:

1. ECDSA (Elliptic Curve Digital Signature Algorithm):

- широко використовується в блокчейні завдяки своїй ефективності та високому рівню безпеки;
- в порогових схемах ECDSA може бути використаний з різними протоколами розподілу секретного ключа.

До переваг необхідно віднести: висока швидкість, невеликий розмір підпису.

До недоліків необхідно віднести: може бути вразливий до певних типів атак при неправильній реалізації.

2. Schnorr signatures:

- модернізований варіант алгоритму DSA, який пропонує більш ефективну перевірку підпису;
- забезпечує високий рівень безпеки та добре масштабується для великих кількостей учасників.

До переваг необхідно віднести: швидка перевірка підпису, компактні підписи.

До недоліків необхідно віднести: може бути менш поширеним у порівнянні з ECDSA.

3. BLS signatures (Boneh–Lynn–Shacham):

- базуються на парних спарюваннях на еліптичних кривих.
- дозволяють агрегувати кілька підписів в один, що значно зменшує розмір транзакцій.

До переваг необхідно віднести: компактні агреговані підписи, висока пропускна здатність.

До недоліків необхідно віднести: більш складні в реалізації порівняно з ECDSA та Schnorr signatures.

В таблиці 1 наведено якісне порівняння основних алгоритмів цифрового підпису, які використовуються для побудови порогових схем.

Таблиця 1 - Якісне порівняння алгоритмів цифрового підпису

Характеристика	**ECDSA**	**Schnorr signatures**	**BLS signatures**
Швидкість	Середня	Висока	Висока
Розмір підпису	Середній	Середній	Дуже малий (при агрегації)
Безпека	Висока	Висока	Висока
Складність реалізації	Середня	Середня	Висока
Агрегація підписів	Можлива, але менш ефективна	Можлива	Легко

Порогова схеми є специфічним типом мультипідпису. Вона не покладається на те, що користувачі підписуватимуть повідомлення своїми унікальними ключами; натомість для цього потрібен лише один відкритий ключ і один закритий ключ, що призводить до лише одного цифрового підпису. У режимі мультипідпису кінцеве повідомлення містить цифрові підписи всіх підписувачів і потребує індивідуальної перевірки стороною, що перевіряє, але в порогових підписах перевіряльник перевіряє лише один цифровий підпис. Основна ідея схеми полягає в тому, щоб розділити закритий ключ на кілька частин, і кожен підписувач зберігає свою власну частину закритого ключа. Процес підписання вимагає від кожного користувача використання відповідної частини закритого ключа для підпису повідомлення. У даній схемі лише підмножина підписувачів може створити підпис зі своєю часткою, і немає необхідності, щоб усі учасники співпрацювали для створення підпису.

Порогові підписи також можна використовувати для надання послуг анонімності в мережі блокчейн. Це відбувається тому, що схеми порогового підпису не розкривають членів порогової групи, які підписалися для створення

підпису. Це відрізняється від схем мультипідпису, які розкривають особи всіх підписантів. Крім того, у дозволених мережах порогові підписи можна використовувати в сценаріях, де для узгодження операції потрібен поріг користувачів.

2. Алгоритм цифрового підпису на основі кривої Едвардса

Алгоритм цифрового підпису на основі кривої Едвардса (EdDSA) використовується для створення цифрового підпису з використанням покращення підпису Шнорра за допомогою скручених кривих Едвардса. Загалом він швидший, ніж багато інших методів цифрового підпису, і надійний з точки зору безпеки.

Одним із прикладів EdDSA є Ed25519, який базується на кривій 25519. Він генерує 64-байтове значення підпису (R, s) і має 32-байтові значення відкритого та закритого ключів. Розділимо закритий ключ на секретну політику спільного доступу 2 із 3 і розподілимо його між кількома сторонами. Далі кожна зі сторін може створити частину підпису, а потім вони об'єднуються разом для створення загального підпису. Таким чином закритий ключ ніколи не потрібно перебудовувати, щоб створити підпис для об'єкта даних.

Перевагою використання Ed25519 над ECDSA є те, що можна об'єднувати підписи та відкриті ключі [3].

Спочатку кожна сторона створює секрет (s_i) і передає відкритий ключ

$$A_i = s_i \cdot B,$$

де B - базова точка на кривій.

Сторона також генерує випадкове значення r_i та зобов'язується:

$$R_i = r_i \cdot B.$$

Нарешті кожна сторона генерує:

$$S_i = r_i + h \cdot s_i (mod\ l),$$

де q - порядок кривої. Потім кожна сторона зобов'язується (A_i, R_i, S_i) і надсилає іншим сторонам та чекає на відповідь про зобов'язання. З усіма отриманими зобов'язаннями можемо відновити:

$$R = R_1 + R_2 + \cdots R_2,$$

$$S = S_1 + S_2 + \ldots S_n.$$

Тоді відкритий ключ (A):

$$A = A_1 + A_2 + \ldots A_n,$$

який дорівнює:

$$A = s_1 \cdot B + s_2 \cdot B + \ldots s_n \cdot B.$$

Потім перевіряємо за допомогою:

$$S \cdot B = R + k \cdot A.$$

Тоді підпис (R, S).

За допомогою розділення секрету Шаміра змінюємо секретний ключ так, щоб кожна сторона мала значення секретного ключа (s_i) помножене на коефіцієнт Лагранжа l_i, який відповідає певній частці.

Потім відновлюємо за допомогою:

$$A_i = s_i \cdot l_i \cdot B,$$

$$R_i = r_i \cdot B,$$

$$S_i = r_i + k \cdot l_i \cdot s_i (mod\ p).$$

Розглянемо приклад. Нехай повідомлення: Vadym Shukhman

Відкритий ключ:
e0c205f73ed6826a948f97330595c70708e4eecd316e4ea593a0c7cd0b7e99b9

Порогове значення Sig1:
e6d7797b689f38a3a7cc24e9624cd2876caf92fbed5dbc04e785c1cd83daca0233cc8fe1cb960b8cb3ff317a889c6888060e233f29cdff80f13cffb711d02a0b.

Порогове значення Sig2:
e6d7797b689f38a3a7cc24e9624cd2876caf92fbed5dbc04e785c1cd83daca02a1c95e2d24a83abea0b4c9fb1030ad63d21d8f05be493fc0ec5aedf2bbac330d.

Порогове значення Sig3:
e6d7797b689f38a3a7cc24e9624cd2876caf92fbed5dbc04e785c1cd83daca020fc72d797cb969f08d69617d99c3f13e9e2dfbcb52c67effe778db2d66893c0f.

Зміна підпису із спільний доступ 1 і 3:
e6d7797b689f38a3a7cc24e9624cd2876caf92fbed5dbc04e785c1cd83daca02c5cec0957385dc59c64a9af8ff0824ad3afeb6789450c041f61e117d67f32109.

Зміна підпису із спільний доступ 2 і 3:
e6d7797b689f38a3a7cc24e9624cd2876caf92fbed5dbc04e785c1cd83daca02c5cec0957385dc59c64a9af8ff0824ad3afeb6789450c041f61e117d67f32109.

Підпис перевірено.

Довжина підпису становить 64 байти, які складаються з 32 байтів для значення R і 32 байтів для значення s. Довжина відкритого ключа також становить 32 байти, а закритого –32 байти. Загалом Ed25519 створює один із найменших розмірів підпису та має невеликий розмір відкритого та закритого ключів.

Висновок. В роботі проведемо аналіз ефективності різних алгоритмів цифрового підпису, таких як ECDSA, Schnorr signatures та BLS signatures, у контексті їх використання для побудови порогових схем у технології блокчейні. Розглянуто переваги та недоліки кожного з алгоритмів, їх продуктивність, безпеку та відповідність вимогам сучасних блокчейн-систем. Крім того, наведено приклад обчислення цифрового підпису на основі еліптичної кривої 25519. Загалом Ed25519 створює один із найменших розмірів підпису та має невеликий розмір відкритого та закритого ключів.

Перелік використаних джерел.

1. Блокчейн і децентралізовані системи: навч. посібник для студ. закладів вищ. освіти: в 3 частинах. Ч. 2 / П. Кравченко, Б. Скрябін, О. Курбатов, О. Дубініна. - Харків, 2019. - 412 с.

2. Digital Signature. [Електронний ресурс].- Режим доступу: https://academy.binance.com/en/glossary/digital-signature.

3. Buchanan, William J (2024). Ed25519 - Edwards-curve Digital Signature Algorithm (EdDSA) using RFC 8032. [Електронний ресурс]. - Режим доступу: Asecuritysite.com. https://asecuritysite.com/encryption/eddsa2