ПОРІВНЯЛЬНИЙ АНАЛІЗ ХЕШ-ОРІЄНТОВАНИХ СХЕМ ЦИФРОВОГО ПІДПИСУ XMSS ТА SPHINCS+

Мельникова О.А., Грасмік С.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Розвиток квантових комп'ютерів робить необхідним перегляд підходів до забезпечення криптографічної стійкості цифрових підписів. Адже складність факторизації та дискретного логарифмування, на яких базується стійкість багатьох асиметричних алгоритмів, є вразливою до квантових обчислень. Через це сучасна постквантова криптографія звертається до цифрових підписів, безпека яких базується на інших математичних задачах, наприклад на властивостях криптографічних хеш-функцій [1, 2]. Особливе місце серед них посідають XMSS і SPHINCS+. Перший належить до схем зі станом (stateful), а другий не потребує зовнішнього керування станом (stateless) [3, 4].

Метою доповіді є порівняння хеш-орієнтованих схем цифрового підпису XMSS і SPHINCS+ з урахуванням їх криптографічних властивостей, зазначених в документах NIST (National Institute of Standards and Technology) та особливостей рекомендацій Федерального управління інформаційної безпеки Німеччини (BSI — Bundesamt für Sicherheit in der Informationstechnik) щодо їх застосування [1, 3, 4].

У рекомендаціях BSI зазначається, що для хеш-орієнтованих схем критичне значення має стійкість до знаходження їх прообразу, тоді як колізійна стійкість не виступає основною визначальною вимогою [1].

Ключова особливість XMSS полягає в тому, що алгоритм безпечний лише за умови ретельного керування станом, тобто для кожного нового підпису має використовуватися новий внутрішній елемент структури (дерева), а повторне використання вже задіяного стану може поставити безпеку під загрозу. Відтак XMSS не подається як універсальне рішення загального призначення, а рекомендується для тих систем, де можна гарантувати відповідальне використання особистого конфіденційного ключа та безпечне ведення стану. Додатково в документі зазначається, що генерація ключів і створення підписів мають виконуватися в апаратних криптомодулях. Тобто NIST пов'язує XMSS не лише з математичною задачею, а й із наявністю контрольованої апаратної інфраструктури [3].

У рекомендаціях BSI вказується, що однією з проблем є необхідність безпомилкового керування станом, зокрема монотонного збільшення лічильника при кожному новому підписі. Через це схеми зі станом рекомендуються для спеціальних сценаріїв, наприклад підписування програмного забезпечення та оновлень прошивки [1, 3].

SPHINCS+ у нормативному полі NIST представлений через стандарт FIPS 205, у якому стандартизовано алгоритм SLH-DSA [4]. У документі прямо зазначено, що SLH-DSA базується на SPHINCS+, тобто є його стандартизованою формою. Головною його відмінністю від XMSS є відсутність потреби у зовнішньому керуванні станом. Такий підхід значно

знижує організаційні ризики, пов'язані з неправильним веденням лічильника або повторним використанням стану, що робить цю схему більш придатною для широкого використання [1, 4].

BSI у своїх технічних документах зазначає, що для SLH-DSA рекомендується hedged-варіант. Це означає, що під час створення підпису використовується не лише сам конфіденційний особистий ключ і повідомлення, а й додатково рандомізація.

Також зазначається, що перевага надається Pure-version SLH-DSA, у якому схема підписує вихідне повідомлення без попереднього зовнішнього хешування цього повідомлення. Тоді як Pre-hash-version допускається лише для спеціальних випадків [1].

BSI чітко формулює свої вимоги до параметрів SLH-DSA. У документі зазначено, що рекомендуються усі набори параметрів, які відповідають NIST Security Strength Category 3 та NIST Security Strength Category 5, але саме в hedged-варіанті.

Таким чином, порівняння XMSS і SPHINCS+ виявляє насамперед різницю між різними схемами зі станом та без стану. XMSS розглядається як схема, придатна для контрольованих сценаріїв, де гарантується надійне ведення стану, апаратний захист ключового матеріалу та обмежена кількість підписів. SPHINCS+ позиціонується як цифровий підпис без стану, що є більш зручним для широкого використання, хоча BSI і додає окремі уточнення щодо параметрів.

У німецькому контексті це добре узгоджується з дослідженнями, які присвячені розвитку квантово-стійких криптографічних технологій Німеччини, де хеш-орієнтовані цифрові підписи розглядаються як довгостроковий захист [2].

У такому випадку XMSS і SPHINCS+ є двома різними підходами до реалізації хеш-орієнтованих цифрових підписів.

У результаті проведеного аналізу визначено, що XMSS і SPHINCS+ належать до одного класу хеш-орієнтованих схем цифрового підпису, але істотно відрізняються в технічній будові схем і моделі їх безпечного застосування.

Список літератури

1. Bundesamt für Sicherheit in der Informationstechnik. *Kryptographische Verfahren: Empfehlungen und Schlüssellängen*. BSI TR-02102-1. Bonn : BSI, 2025.

2. Мельникова О. А., Грасмік С. В. Становлення та розвиток квантово-стійких криптографічних технологій у Німеччині. *Вісник Херсонського національного технічного університету*. 2025. № 4 (95). Т. 2. С. 119–124. DOI: https://doi.org/10.35546/kntu2078-4481.2025.4.2.15

3. *Recommendation for Stateful Hash-Based Signature Schemes: NIST Special Publication 800-208* / National Institute of Standards and Technology. Gaithersburg, MD : NIST, 2020.

4. *Stateless Hash-Based Digital Signature Standard: FIPS PUB 205* / National Institute of Standards and Technology. Gaithersburg, MD : NIST, 2024.