АНАЛІЗ АЛГОРИТМІВ ПОБУДОВИ ЭЦП SPHINCS ТА SPHINCS+

Нечволод К.В.
Науковий керівник –доцент кафедри БІТ, к.т.н. Петренко О.Є.
Харківський національний університет радіоелектроніки
(61166, Харків, просп. Науки,14, каф.БІТ, тел +38 (057) 702-14-25)
e-mail: kostiantyn.nechvolod@nure.ua

As e-commerce has become more important in society, the need to certify the origin of exchanged information has arisen. Modern digital signatures enhance security based on the difficulty of solving a mathematical problem, such as finding the factors of large numbers. Unfortunately, the task of solving these problems becomes feasible when a quantum computer is available. To face this new problem, new quantum digital signature schemes are in development to provide protection against tampering, even from parties in possession of quantum computers and using powerful quantum cheating strategies. Object of a research is the two post-quantum algorithms of the digital signature SPHINCS and SPHINCS+, which were submitted to the NIST post-quantum crypto project.

Квантова криптографія – єдина, яка може реалізувати беззастережну безпеку в пост квантовий період. Наукове співтовариство по-різному оцінює перспективи побудови повноцінного квантового комп'ютера. Деякі вважають, що на це піде не менше десятка років, інші – що повноцінний квантовий комп'ютер не буде побудований ніколи. Проте, співтовариство, не покладаючись на велику кількість фізичних проблем по розробці квантових обчислювальних систем, заздалегідь потурбувалося завданням боротьби з майбутніми квантовими комп'ютерами і створило напрямок – пост-квантова криптографія. Цей напрямок розробляє криптографічні системи, які є криптостійкими для майбутніх квантових комп'ютерів. Зокрема, пост-квантова криптографія пропонує захищені системи передачі інформації на основі хеш-функцій.

Мета роботи: на основі порівняльного аналізу алгоритмів SPHINCS+ та SPHINCS визначити найкращій алгоритм для застосування в пост квантовий період.

Алгоритм SPHINCS [1] є надійною системою електронного цифрового підпису, що заснована на на хеш-функціях [2]. Ця система дозволяє забезпечити достатній рівень стійкості в пост квантовий період, застосовуючи довжину, що дорівнює 128 біт та може бути реалізована на базі звичайних комп'ютерів.

Система SPHINCS+ [1] будується на SPHINCS, вносячи кілька покращень, а саме:

1. Здібність захисту від багатоцільової атаки, застосовуючи методи зм'якшення за допомогою функцій хешування ключа. Кожен виклик функцій хешування набирається з іншим ключем і застосовується інша

бітова маска. Ключі та бітові маски генеруються псевдовипадково з адреси, що визначає контекст виклика та публічного seed [1].

2. Здійснено стиснення відкритого ключа WOTS+ на відміну від алгоритму, що застосовано в SPHINCS без L-дерева: останні вузли ланцюгів WOTS+ не стискуються за допомогою L-дерева, але використовують виклик однієї хеш-функції, що настроюється. Цей виклик знову отримує адресу та публічний seed для запуску цього виклика та генерації бітової маски такої ж довжини, як і вхід.

3. Пара ключів FORS, на відміну від алгоритму SPHINCS, не складається більше з одного монолітного дерева. Замість цього вона складається з дерев висоти *a*. Листя цих дерев являють собою хеші секретних ключових елементів 2^a. Публічний ключ - це хеш конкатенації всіх кореневих вузлів, як для відкритого ключа WOTS+, може використовуватися для підписування $k2^a$ бітових повідомлень.

4. Алгоритм SPHINCS+, на відміну від SPHINCS спроможний здійснювати вибір індексу верифікації наступним чином:

- детерміновано генерується випадкове *R = PRF (SK.prf, OptRand, M)*. Де *OptRand* має значення 256 біт, за замовчуванням 0, але може бути заповнений випадковими бітами, наприклад. взятих з *TRNG*, що дозволяє уникнути детерміністичного підписання та протидіяти атакам бічних каналів;
- обчислюється дайджест повідомлення та індекс як *(md || idx) = Hmsg (R, PK, M)*, де *PK = (PK.seed, PK.root)* містить верхній кореневий вузол та публічний seed.

Отже, алгоритм SPHINCS+ є покращеною версією SPHINCS, яка дозволяє генерувати та веріфікувати стійкі до криптоаналітичних атак електронні цифрові підписи в пост квантовий період. Використання впроваджених змін дозволяє швидше генерувати менші за розміром підписи ніж в алгоритмі SPHINCS.

Список джерел:

1. Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder, Scott Fluhrer, Stefan-Lukas Gazdag, Andreas Hülsing, Panos Kampanakis, Stefan Kölbl, Tanja Lange, Martin M. Lauridsen, Florian Mendel, Ruben Niederhagen, Christian Rechberger, Joost Rijneveld, Peter Schwabe. SPHINCS+, 2017

2. 2. Merkle R. C. A Digital Signature Based on a Conventional Encryption Function [Електронний ресурс] / Ralph C. Merkle // Advances in Cryptology – CRYPTO '87, Lecture Notes in Computer Science. – Вид. 293. – с. 369–378.