ВИКОРИСТАННЯ ГІПЕР-ДЕРЕВ У КРИПТОГРАФІЇ

Марухненко О.С., Халімов Г.З.
Харківський національний університет радіоелектроніки, Харків, Україна

Криптосистеми на основі геш-функцій є перспективним напрямком постквантової криптографії. Перші ЕЦП цього класу були запропоновані достатньо давно, але не набули широкого використання через те, що пара ключів могла бути використана для створення лише одного підпису. Рішення було запропоновано Мерклі і базується на застосуванні так званих геш-дерев або дерев Мерклі [1]. Дерево об'єднує у собі певну кінцеву множини одноразових ключів і може бути використано для створення відповідної кількості підписів, однак побудова ключа для тисяч і більше використань потребує значних обчислювальних витрат. Альтернативним рішенням є використання структури гіпердерева, що представляє собою дерево з геш-дерев, листя дерев верхнього рівня використовуються для підпису коренів дерев, що лежать рівнем нижче [2]. Відкритим ключем користувача є корінь верхнього дерева. Така схема дозволяє поступово генерувати дерева нижчих рівнів, не змінюючи при цьому загального ключа. Одним з перспективних алгоритмів, що використовує цю структуру є SPHINCS+[3].

Метою доповіді є розгляд особливостей використання гіпер-дерев у криптосистемі SPHINCS+, аналіз впливу системних параметрів на властивості підпису.

В доповіді наводиться залежність стійкості, розмірів та швидкодії підпису SPHINCS+ від системних параметрів. Наведені дані показують, що однаковий рівень стійкості може бути забезпечений великою кількістю комбінацій параметрів, що дозволяє оптимізувати криптосистему в залежності від вимог до швидкості створення та перевірки підпису та його розмірів. Досягнення компромісу час-простір є важливою складової впровадження подібної системи.

Список літератури

1. Ralph Merkle. A certified digital signature. In Gilles Brassard, editor, Advances in Cryptology – CRYPTO '89, volume 435 of LNCS, pages 218–238. Springer, 1990.

2. Andreas Hülsing, Lea Rausch, and Johannes Buchmann. Optimal parameters for XMSSMT. Security Engineering and Intelligence Informatics, volume 8128 of Lecture Notes in Computer Science, pages 194–208. Springer Berlin Heidelberg, 2013.

3. Daniel J. Bernstein, Christoph Dobraunig, Maria Eichlseder and others. SPHINCS+ – Submission to the NIST's post-quantum cryptography standardization process, 2017.