УДК 004.056.5

АНАЛІЗ БЕЗПЕКИ ЦП НА ОСНОВІ ГЕШ ФУНКЦІЇ KECCAK

Івашов В.А,
Науковий керівник – ст., викл. В'юхін Д.О.
Харківський Національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: vladyslav.ivashov@nure.ua

An analysis of the security of digital signatures using the Keccak hash function was carried out in order to determine their resistance to modern cryptanalytic attacks and justify their suitability for protecting digital information. Analysis of the security of a digital signature includes an assessment of the resistance of such a signature to various attacks, including cryptanalysis, collisions, and other types of attacks on the hashing algorithm and the signature scheme itself.

В сучасному цифровому світі захист інформації від несанкціонованого доступу є однією з найважливіших проблем. Останнім часом кількість загроз та атак на інформаційні системи постійно зростає. Аналіз сучасних методів атак на інформаційні системи показав на необхідність забезпечення цілісності та автентичності на високому рівні [1, 2]. Одним з методів вирішення цієї задачі є використання стійких цифрових підписів, що використовуються для забезпечення цілісності та автентичності електронних документів. Дослідження безпеки ЦП на основі геш-функції Keccak є актуальним у контексті постійного розвитку кіберзлочинності та криптографічних атак.

Метою цього дослідження є проведення аналізу безпеки цифрових підписів, які використовують геш-функцію Keccak, з метою визначення їхньої стійкості до сучасних криптоаналітичних атак та обґрунтування їхньої придатності для захисту цифрової інформації.

Аналіз безпеки цифрового підпису (ЦП) на основі геш-функції Keccak включає в себе оцінку стійкості такого підпису до різних атак, зокрема криптоаналізу, колізій та інших видів атак на алгоритм гешування та саму схему підпису.

Геш-функція Keccak, яка є основою стандарту SHA-3, має відмінності від попередніх алгоритмів, таких як SHA-1 та SHA-2. Ці відмінності можуть включати розмір вихідного геша, стійкість до певних видів атак, швидкодію та інші
фактори [3].

При аналізі безпеки ЦП на основі Keccak слід розглядати такі аспекти:

– стійкість геш-функції Keccak. Це забезпечується реалізацією криптографічної губки на 24 раунди;

– використання Keccak в протоколах ЦП. Оцінка, як саме використовується Keccak в протоколі ЦП, включаючи методи гешування, конкатенації та інші операції [4]. Також ця схема більш швидка бо в процесі відбору на конкурс SHA-3 розробники змінили спосіб заповнення блоків губки. Що дало більш високу ефективність;

– стійкість самої схеми ЦП. Оцінка того, наскільки безпечно використання Keccak у протоколі ЕЦП, враховуючи усі можливі атаки на схему підпису;

– відповідність стандартам безпеки. Перевірка відповідності протоколу ЦП на основі Keccak сучасним стандартам безпеки та рекомендаціям криптографічної спільноти [4]. За результатами різноманітних спроб криптоатак на Keccak, було прийнятий висновок що пошук прообразів його геш-функцій повинен мати потужність мінімум квантового рівня.

На основі проведеного аналізу можна зробити висновок, що цифрові підписи, побудовані на базі геш-функції Keccak, виявляють високий рівень стійкості до сучасних криптоаналітичних атак [5]. Але якщо рівень технічного обладнання дозволяє провести атаку постквантового рівня то це шифрування буде вже не ефективним. Це приводить нас до того, що хоч алгоритм і є на наш час досить безпечним, але майже 10 років його існування потребує нових конкурсів на генерування геш-функцій.

Список використаних джерел

1. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі // Системи обробки інформації 9 (2015): 101-104.

2. Голубничий Д.Ю., Сєвєрінов О.В., Коломійцев О.В., Місюра О.М., Третяк В.Ф., Власов А.В., Крук Б.М. Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації. (2021).

3. Bertoni, Guido, Joan Daemen, Michael Peeters, and Gilles Van Assche. Keccak sponge function family main document. NIST. 2010.

4. Aumasson, Jean-Philippe. The hash function Keccak. In Fast Software Encryption. Springer. 2013 р.. 313 с.

5. Качко Е. Г. Дослідження застосування SMT/SAT доказів у криптоаналізі хеш-функцій сімейства Keccak / Е. Г. Качко, Д. К. Телевний // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. - 2017. - Вип. 189. - С. 75 – 80.