УДК 004.02
Лехіцька Н. О. – ст. гр.. СНм-51
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ КРИПТОСТІЙКОСТІ ТА ШВИДКОДІЇ АЛГОРИТМУ ХЕШУВАННЯ KECCAK

Науковий керівник: кандидат технічних наук Козак Р.О.

Криза в галузі криптографії, пов'язана із стійкістю хеш-функцій, найбільш яскраво проявилася в середині 2000-х років. Дослідники з університету Шаньдуна (Китай) у 2005 році, опублікували алгоритм для пошуку колізій в хеш-функції MD5, а також представили атаку на алгоритм SHA-1, яка вимагає менше 269 операцій. Враховуючи це американський інститут стандартів і технологій (NIST) оголосив конкурс на створення нового стандарту хешування. Переможець конкурсу алгоритмів хешування Keccak отримав назву хеш-функції SHA-3.

В основі побудови хеш-функції лежить ітеративна послідовна схема. Ядром алгоритму є функція стиснення - перетворення k вхідних в n вихідних біт, де n - розрядність хеш-функції, а k - довільне число більше n. Повторюючи цю функцію під час декількох раундів з різними константами, досягають потрібного значення стійкості. Доповнюючи і зчіплюючи між собою блоки від різних фрагментів вихідного тексту, отримують можливість обчислити хеш повідомлення довільної довжини. При цьому виникає суттєва проблема – важко сконструювати функцію стиснення . Автори алгоритму Keccak стверджують, що сконструювати надійну функцію стиснення виду $k \rightarrow n$ $(k>n)$ як однораундовий блок криптопримітива, вкрай складно.

В ролі функції стиснення можна використовувати блочний шифр. Дійсно, на відміну від псевдовипадкових функцій, псевдовипадкові перестановки, створювати простіше. А блочний шифр – це перестановки залежні від ключа. Достатньо сконструювати шифр з розміром блоку і розміром ключа 512 біт і можна буде отримати функцію стиснення $k \rightarrow n$ $(k>n)$. Проблема однак у тому, що хоч блочні шифри і вважаються найстійкішими симетричними криптопримітивами, вони мають слабкий ключовий розклад (функцію розгортання підключів раунду з основного ключа). Це призводить до атак із зв'язними ключами, які ставлять під удар функцію стиснення на основі блочного шифру.

Автори хеш-функції Keccak прийняли ряд радикальних рішень. Вони вирішили не використовувати функцію стиснення у вигляді окремого блоку, а в ролі стійкого криптоперетворення вирішили сконструювати без ключову псевдовипадкову перестановку. Все це упаковано в дуже просту конструкцію Sponge ("Губка").

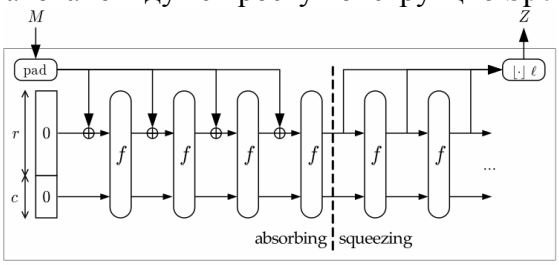

Рисунок 1 – Конструкція "Губка"

Метою магістерської роботи є власне дослідження криптостійкості та швидкодії нового алгоритму хешування Keccak.