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

ХЕШ-ФУНКЦІЯ KECCAK І КОНСТРУКЦІЯ SPONGE ЯК УНІВЕРСАЛЬНИЙ КРИПТОПРИМІТИВ

Науковий керівник: асистент Шимчук Г.В.

Криза в галузі криптографії, пов'язаний зі стійкістю хеш-функцій, найбільш яскраво проявилася в середині 2000-х років, американський інститут стандартів і технологій змусив оголосити конкурс на створення нового стандарту хешування – SHS (Secure Hash Standart). Переможець конкурсу алгоритмів хешування отримав ім'я хеш-функції SHA-3.

Традиційний дизайн хеш-функцій заснований на використанні функції стиснення. Ця функція відображає значення m → n (m> n) псевдовипадковим чином. При цьому значення n повинне бути до 512 біт, а m порядку 2n. Повторюючи цю функцію під час декількох раундів з різними константами, досягають потрібного значення стійкості. Доповнюючи і зчеплені між собою блоки від різних фрагментів вихідного тексту, отримують можливість обчислити хеш від повідомлення довільної довжини. При цьому виникає істотна проблема: сконструювати функцію стиснення важко. Багатораундові повторення згладять її дефектність, але наперед відома наявність швидкої можливості знайти часткову колізію в вихідної функції стиснення ставить під питання стійкість всієї конструкції. Автори алгоритму Keccak (Guido Bertoni, Joan Daemen, Michael Peeters і Gilles Van Assche) стверджують, що сконструювати надійну функцію стиснення виду m → n (m> n) як одноразундовий блок криптопримітива, вкрай складно (або неможливо взагалі).

Автори алгоритму Skein і Whirlpool вважають, що в якості функції стиснення можна використовувати блоковий шифр. Дійсно, на відміну від псевдовипадкових функцій (Pseudo Random Function – PRF), псевдовипадкові перестановки (Pseudo Random Permutation – PRP), створювати простіше. А блоковий шифр є такою перестановкою, залежною від ключа. Досить сконструювати шифр із розміром блоку і розміром ключа 512 біт і можна буде отримати функцію стиснення m → n (m> n), подаючи на вхід такого шифру ці значення. Проблема однак у тому, що хоча блокові шифри і вважаються самими довіряємими в плані стійкості симетричних криптопримітивів, вони часто мають полегшене або слабкий ключовий розклад (функцію розгортання підключів раунду з основного ключа). Це призводить до атак зі зв'язаними ключами, які хоча і не представляють практичної загрози в більшості протоколів, але ставлять під удар функцію стиснення на основі блокового шифру. Більш того – ідеальнмй ключовий розклад для ідеального блочного шифру саме по собі повинен мати властивості ідеальної псевдовипадкової функції. Тобто для створення ідеальної хеш-функції потрібно використовувати ... ідеальну хеш-функцію. Виходить замкнуте коло, яке лише частично можна перемогти деякими специфічними рішенями.

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