АЛГОРИТМ LUFFA У ОДНОРАЗОВИХ ПОВІДОМЛЕННЯХ

Федяєв Д.В., В'юхін Д.А.
Харківський національний університет радіоелектроніки, Харків, Україна

На даний час функції гешування використовуються у багатьох застосуваннях систем захисту інформації. При цьому не всі геш-функції є криптографічно безпечними та можуть використовуватись у різних напрямках безпеки.

Метою доповіді є аналіз можливостей алгоритму Luffa для використання у одноразових повідомленнях.

Алгоритм Luffa - це сімейство криптографічних геш-функцій, який є варіантом функції губки, але на відміну від оригіналу, використовує множину паралельних перестановок та функції інжекції повідомлень [1].

У ході другого туру конкурсу SHA-3 Luffa-224 та Luffa-256 у початковому варіанті показали низьку криптостійкість, для успішної атаки знадобилося 2^{216} повідомлень. Барт Пренель (Bart Preneel) представив успішну атаку з пошуку колізій для 4 раундів крокової функції Luffa за операцій гешування та для 5-раундової, показавши тим самим межу стійкості дизайну до диференційного пошуку колізій. Після чого алгоритм був вдосконалений Даї Ватанабе і отримав назву Luffa v.2 [2, 3].

Зміни Luffa v.2:

– доданий порожній раунд функції завершення для всіх розмірів гешу;
– змінено S-блок;
– збільшено кількість повторень крокової функції з 7 до 8.

Проведений аналіз показав, що на даний час статус безпеки Luffa:

– немає доказів безпеки для з'єднання;
– відомо кілька загальних атак, але жодна з них нереалізована;
– можлива диференціальна атака, яка показала межу стійкості алгоритму;
– алгоритм здається достатньо безпечним

Таким чином проведений аналіз показав, що алгоритм Luffa не може використовуватися як довгостроковий цифровий підпис, але його особливості достатні для систем з одноразовим повідомленням.

Список літератури

1. Hisayoshi Sato, Dai Watanabe: Hash Function Luffa Supporting Document, 31 October 2008, https://ehash.iaik.tugraz.at/uploads/f/fe/Luffa_SupportingDocument.pdf

2. Shugo Mikami1 , Nagamasa Mizushima1 , Setsuko Nakamura1 , and Dai Watanabe1 https://www.hitachi.com/rd/yrl/crypto/luffa/ACompactHardwareImplementationOfSHA-3CandidateLuffa_20100810.pdf

3. Dai Watanabe Christophe De Cannière Hisayoshi Sato, 25th February 2009, https://csrc.nist.rip/groups/ST/hash/sha-3/Round1/Feb2009/documents/luffa_sha3ws1_2pp.pdf