УДК 003.26:004.424.47

Ю.В. Баришев

Вінницький національний технічний університет, Вінниця

ПІДХІД ДО ХЕШУВАННЯ, ЩО СТІЙКЕ ДО АНАЛІЗУ ЗЛОВМИСНИКА

Для забезпечення електронної комерції використовується хешування, тобто процес обчислення хеш-значення. Це суттєво вплинуло на математичні моделі хешування – вони повинні бути відкритими для дослідження, оскільки підприємці, що користуються даним здобутком криптографії, бажають мати гарантії того, що їх підпис не буде підроблений протягом певного вельми довгого проміжку часу [1]. Відповідно й відомі хеш-функції є відкритими для дослідження криптоаналітиками. Такий підхід до розробки алгоритмів хешування став причиною того, що на сьогоднішній день більшість хеш-функцій, що широко використовуються можуть бути зламані за проміжок часу, суттєво менший за той, що передбачався при проектуванні. В той же час, у тих хеш-функцій, що розробляються їм на заміну, часто також швидко знаходять вразливі місця, оскільки вони є також відкритими для дослідження з боку криптоаналітиків. Тому сьогодні методи хешування, що використовуються в електронній комерції, не виконують функції, покладені на них. Вилучення умови щодо відкритості алгоритму хешування для дослідження могло б виправити ситуацію для криптологів.

З іншого боку, процес засекречення алгоритмів сам по собі – вельми складна задача. Останнє пояснюється людським фактором, що присутній в процесі розробки та засекреченні алгоритмів хешування. Відповідно бізнесмени, що користуватимуться алгоритмом хешування, не матимуть жодних гарантій того, що їх конкуренти не "домовились" з розробниками. Крім того, розв'язок задачі впровадження закритих алгоритмів в глобальних розподілених комп'ютерних мережах є утопічним.

Отже, задача розробки нового підходу до хешування полягає в тому, щоб він одночасно задовольняв умови відкритості для дослідження стійкості криптоаналітиками хеш-функції та її закритості для дослідження з метою зламу зловмисниками. Вирішення цієї задачі було поставлено метою даного дослідження.

Для розв'язку даної задачі пропонується використовувати керовані операції, значний внесок в розвиток яких внесла робота [2]. Під керованими операціями в [2] розуміють такі, що результат виконання яких залежить від заданого вектора керування v_i:

$$h_i = f\left(h_{i-1}, m_i, v_i\right),$$

де h_i – проміжне хеш-значення, отримане після і-тої ітерації; m_i – блок повідомлення, що хешується, $M = \{m_1, m_2, ..., m_l\}$; $f(\cdot)$ – функція хешування.

Не зважаючи на значні результати, отримані в

[2], використовуючи результати цієї робота не можливо досягти поставленої в даній доповіді мети, оскільки в самій же роботі [2] представлені формули для опису залежності вихідного біта хеш-значення від вхідних. Це пов'язано з тим, що керованість операцій в [2] фактично передбачає використання вектора керування v_i як додаткового операнда при обчисленні хеш-значення. Для усунення цього недоліку пропонується використовувати множину функцій хешування F, а замість однієї функції хешування. Таким чином, вектор керування v_i буде визначати номер функції $f_{v_i}(\cdot) \in F$, що буде виконуватись на і-ій ітерації. Тобто від зловмисника будуть закриті операції, що будуть виконуватись над певним блоком вхідних даних, а в той же час стійкість функцій з множини F можуть бути перевірені суспільством.

Список літератури

1. Бернет С., Пейн С. Криптография. Официальное руководство RSA Security. – М.: Бином-Пресс, 2002. – 384 с.

2. Молдовян Н.А., Молдовян А.А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. – СПб.: БХВ-Петербург, 2004. – 448 с.