

МЕТОДИ ГЕШУВАННЯ СТІЙКОГО ДО ЗАГАЛЬНИХ АТАК

Комаров А. О.

Науковий керівник - ст. викл, к.т.н. Баришев Ю. В.

Криптографічні геш-функції є важливим інструментом в криптографії для досягнення певних цілей безпеки, такі як справжність, цифрових підписів, цифровою міткою часу і автентифікації суб'єктів. Вони також тісно пов'язані з іншими важливими криптографічними інструментами, такими як блокові шифри і генератори псевдовипадкових чисел. Ця стаття спрямована на дослідження деяких відомих конструкцій гешування та підходу до зав'язування блоків даних.

Оскільки в основі загальних атак лежить ідея того що кожен блок даних обробляється окремо від інших блоків даних, пропонується використовувати конструкції, які передбачають використання декількох блоків даних на кожній з ітерацій гешування:

$$\begin{cases} h_i = f(h_{i-1}, m_i, m_{i-r_i}) \\ r_i = \text{rand}(m_i) \end{cases} \quad (1)$$

Функція $\text{rand}(\cdot)$ – деяка функція, значення якої, мають рівномірний закон

розподілу. Наприклад, це може бути генератор псевдовипадкових чисел, наприклад, на основі реєстрів зсуву зі зворотним зв'язком, для пришвидшення обчислень, початковим станом якого буде блок даних m_i . Для покращення стійкості можна використовувати генератор залежний від більшої кількості аргументів:

$$\begin{cases} h_i = f(h_{i-1}, m_i, m_{i-r_i}) \\ r_i = \text{rand}(m_i, m_{i+1}) \end{cases} \quad (2)$$

Конструкції (1) та (2) більш стійкі до мультиколізій, на відміну від інших, тому що для отримання мультиколізії злоумисник більше не зможе послідовно замінювати блоки даних, і вони будуть в більшій мірі залежати один від одного.

На основі проведеного дослідження можна сказати що найбільш вразливими є конструкції, вразливі до мультиколізії. Для покращення стійкості конструкцій гешування до атак, які базуються на мультиколізіях, пропонується підхід до зав'язування блоків даних, для того щоб пов'язати всі блоки повідомлення між собою, і ускладнити процес знаходження колізій, за рахунок того, що злоумисник уже не зможе послідовно замінювати блоки даних для отримання мультиколізії.