УДК 004.56:004.424.47

МАТЕМАТИЧНА МОДЕЛЬ ПСЕВДОНЕДЕТЕРМІНОВАНОГО ХЕШУВАННЯ ТА КРИПТОГРАФІЧНІ ПРИМІТИВИ ДЛЯ ЇЇ РЕАЛІЗАЦІЇ

Ю.В. Баришев, аспірант
Вінницький національний технічний університет
yuriy.baryshev@gmail.com

Відкритість алгоритмів хешування породжує низку проблем, що пов'язані зі сталою послідовністю операцій, що виконуються на кожній ітерації хешування. Однак засекречення цих алгоритмів не може стати адекватним рішенням цих проблем. Це обумовлено низкою факторів, найбільш значущими з яких є такі три: наявність людського фактору в розробці алгоритмів хешування, можливість декомпіляції виконуваних файлів зловмисниками, потреба в доведенні стійкості алгоритмів підприємцям, які їх будуть використовувати. Виходом із ситуації є реалізація концепції псевдонедетермінованого хешування. Дана концепція випливає з автоматного опису процесу хешування.

Відомо, що недетермінований автомат описується п'ятіркою $\{S, A \cup \{\varepsilon\}, s_0, \delta', D\}$, де S – множина станів автомата; A – вхідний алфавіт; ε – вхідне повідомлення нульової довжини; s_0 – початковий стан, $s_0 \in S$; δ' – відображення виду $S \times A \to S$; D – множина кінцевих станів, $D \subseteq S$. Частковим випадком недетермінованого автомата є детермінований, який описується такою п'ятіркою $\{S, A, s_0, \delta, D\}$, де δ – функція, що реалізує

відображення $S \times A \to S$. Очевидно, що хешування може бути реалізовано лише за допомогою детермінованого автомата, оскільки, за визначенням, в результаті виконання процесу хешування над одним й тим самим повідомленням необхідно отримувати одне й те саме хеш-значення. Тому вживається термін псевдонедетерміноване хешування, тобто таке, яке є детермінованим, але описується з точки зору зловмисника недетермінованим автоматом. Для реалізації даної концепції пропонується така математична модель, або, як її ще прийнято називати, конструкція:

$$h_i = f_{v_i}(h_{i-1}, m_i),$$

де h_i – проміжне хеш-значення, отримане після обробки блока даних, що хешуються, m_i $\left(i = \overline{1,l}\right)$; h_0 – вектор ініціалізації; $f_{v_i}(\cdot)$ – функція ущільнення, що належить певній скінченній множині функцій F; v_i – вектор керування, що належить певній множині векторів V.

Отже, таке хешування описується шісткою $\{S, A, h_0, F, h_l, V\}$, однак, якщо вектори керування будуть закриті від зловмисника, то для нього хешування буде описуватись п'ятіркою $\{S, A, h_0, F, h_l\}$, що представляє собою недетермінований автомат.

Впровадження псевдоенедетермінованої концепції спричинює перегляд вимог до криптографічних примітивів в напрямку їх послаблення, оскільки очікується збільшення нелінійності всього процесу хешування за рахунок того, що операції, які виконуватимуться на кожному раунді будуть закриті від зловмисника. Пропонується використання низки криптографічних примітивів, які базуються на операціях додавання, виключного або, логічного додавання, логічного множення, циклічного зсуву та інвертування.