УДК 004.056:004.424.47

МЕТОД ШВИДКОГО ХЕШУВАННЯ НА ОСНОВІ ЕЛІПТИЧНИХ КРИВИХ

В. А. Лужецький, д.т.н.. професор,
А. О. Олексюк, студентка
Вінницький національний технічний університет

У зв'язку зі швидким розвитком інформаційних технологій, захисту інформації приділяється підвищена увага. Хеш-функції відіграють значну роль в автентифікації повідомлень та цифровому підписуванні. З появою успішних атак на традиційні хеш-функції, постала задача створення нових більш захищених методів хешування. Математичний апарат еліптичних кривих представляє собою потужний механізм для створення захищених хеш-функцій, адже криптосистеми та системи цифрового підписування на основі еліптичних кривих мають зменшений розмір ключа та підвищену стійкість у порівнянні з традиційними, за рахунок того, що базується на проблемі дискретного логарифмування в групі точок еліптичної кривої.

Оскільки процес хешування є ітеративним багатокроковим процесом, при якому на кожному кроці виконуються однотипні обчислення, то в даному методі перед початком хешування пропонується виконати передобчислення значень точок еліптичної кривої, для того щоб спростити обчислення на кожній ітерації.

Суть методу, що пропонується, полягає в такому.

Дані M подають у вигляді послідовності

$$M=\{m_1, m_2, \ldots, m_N\}.$$

На кожній ітерації обчислюється проміжне хеш-значення

$$h_i = (h_{i-1} \oplus m_i) \cdot P = K_i P, \quad (1)$$

де

i =1,2, …, N;

$K_i = (h_{i-1} \oplus m_i) = a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + \cdots + a_0$,

h_i - хеш-значення отримане на i-му кроці;

m_i - i-й блок даних;

P - значення точки еліптичної кривої.

У випадку, коли h_0 є секретним значенням, то воно вважається секретним ключем і мова йде про ключове хешування.

Підставивши у формулу (1) значення K_i, отримаємо такий вираз:

$$h_i = (a_{n-1}2^{n-1} + a_{n-2}2^{n-2} + \cdots + a_0) \cdot P = a_{n-1}(2^{n-1}P) + a_{n-2}(2^{n-2}P) + \cdots + a_0 P.$$

З цього виразу випливає, що обчислення проміжного хеш-значення полягає у нагромадженні добутків $2^j P$ ($j \in [0; n-1]$), яким керують цифри коду K_i. Тобто, маючи наперед обчислені значення точок P, $2P$, $4P$, …, $2^{n-1}P$, можна позбавитися однотипних операцій щодо обчислення таких значень на кожному кроці хешування, це дозволить пришвидшити процедуру хешування. Попередні обчислення полягають у формуванні значень $2^j P$ тільки шляхом подвоєння точок еліптичної кривої.

Після N-ї ітерації отримується остаточне значення хеш-функції.Оскільки значна частка механізмів автентифікації користувачів та даних використовує методи хешування, запропонований метод дозволяє пришвидшити процедуру хешування даних в 3 рази, а отже і покращити процедуру автентифікації.