

**ПРИШВИДШЕННЯ ПРОЦЕСУ ОБЧИСЛЕННЯ
ЗНАЧЕНЬ ХЕШ-ФУНКЦІЙ ПОБУДОВАНИХ НА
ЕЛІПТИЧНИХ КРИВИХ**

**В.А. Лужецький, д.т.н., професор,
В.В. Кичак, студент
Вінницький національний технічний університет
vvykach@gmail.com**

Еліптичні криві є найбільш перспективною структурою для побудови криптографічних алгоритмів, що обраховують в один бік, з перебірною складністю алгоритмів. У доповіді розглядається підхід до пришвидшення процесу обчислення значень хеш-функцій побудованих на еліптичних кривих.

Для еліптичної кривої $E(K)$ з циклічною групою $\langle Q \rangle$ великого простого порядку r функції $h:k \rightarrow x_{kP}$, що ставиться у відповідність невід'ємному цілому числу $k < r/2$ координату x_{kP} точки kP обраховують в один бік і немає колізій.

Повідомлення M розбивається на блоки даних розрядністю n :

$$M = \{m_1, m_2, \dots, m_L\}.$$

В процесі хешування обчислюється така послідовність хеш-значень h_0, h_1, \dots, h_{L+1} , де h_0 – початкове (задане) значення хеш-функції, h_{L+1} – остаточне значення хеш-функції для повідомлення M .

Проміжні значення хеш-функцій обчислюються за формулою:

$$h_i = (h_i'P) \bmod p, \quad i = 1, 2, \dots, L+1,$$

де P – точка групи точок еліптичної кривої $E_p(a,b)$;
 p – просте число.

$$h_i' = h_{i-1} \oplus m_i.$$

Для множення точки P на число h_i' останнє представляється у двійковому вигляді:

$$h_i' = \sum_{i=0}^{n-1} a_i \cdot 2^i,$$

тоді добуток $h_i' P \bmod p$ обчислюється за формулою:

$$h_i' \cdot P \bmod p = \left(\sum_{i=0}^{n-1} a_i \cdot (2^i \cdot P) \right) \bmod p.$$

Для пришвидшення обчислень пропонується попередньо розрахувати значення $2^i P$ шляхом подвоєння точки еліптичної кривої і зберігати ці значення в пам'яті. В процесі множення буде здійснюватись додавання тільки тих значень $2^i P$, для яких $a_i=1$. Порівняно з безпосереднім множенням кількість додавань зменшує в середньому в 3 рази.

Ще більший вигреш за кількістю операцій додавання досягається при використанні перетворення двійкового коду з цифрами 0 і 1 у двійковий код з цифрами -1, 0 і 1. В основі такого перетворення лежить властивість $1+2+2^2+\dots+2^m=2^{m+1}-1$, тобто послідовність з $m+1$ одиниць, що розташовані поруч замінюються тільки двома одиницями, одна з яких має знак мінус.

Відомо, що таке перетворення двійкового коду забезпечує в середньому $0,33n$ одиниць в коді (n – розрядного коду). З урахуванням цього вигреш за кількістю додавань складає 4,5 рази.

Точка еліптичної кривої – P отримується з точки P заміною координати y на координату $-y$, тому в пам'яті достатньо зберігати тільки значення $2^i P$, а значення $-2^i P$ обчислюються, шляхом інвертування.