В чому сутність атаки повне розкриття для перетворення в групі точок еліптичної кривої та як оцінити складність такої атаки?

Згідно сучасних понять і поглядів, стійкість усіх наведених алгоритмів ЦП заснована на складності розв'язання дискретного логарифму в групі точок еліптичної кривої. Для знаходження секретного ключа необхідно розв'язати відносно *d*:

– у випадках ECDSA та ECSS – рівняння

$$Q = d \times G; \qquad (6.132)$$

– у випадках EC-GDSA та EC-KCDSA – рівняння

$$Q = d^{-1} \times G; \qquad (6.133)$$

– у випадку ДСТУ 4145-2002 – рівняння

$$Q = -d \times G. \qquad (6.134)$$

Розглянемо можливість знаходження d на основі атаки при відомих підписаних (перехоплених) підписаних повідомленнях. Нехай перехоплено і підписаних повідомлень. Розв'язуючи для ECDSA рівняння $s = k^{-1}(dr + e) \bmod n$ відносно d, одержимо $d = {(ks - e)}/{r} \pmod n$.

Для *i* повідомлень одержимо *i* рівнянь з *i* + 1 невідомими, тобто k1, k2, …,ki і d:

$$\begin{cases} d = {(k_1 s_1 - e_1)}/{r_1} \bmod n, \\ \vdots \\ d = {(k_i s_i - e_i)}/{r_i} \bmod n. \end{cases} \qquad (6.135)$$

$$\begin{cases} d = {(k_1 - s_1)}/{r_1} \bmod n, \\ \vdots \\ d = {(k_i - s_i)}/{r_i} \bmod n. \end{cases} \qquad (6.136)$$

Для алгоритму ДСТУ 4145-2002, використовуючи рівняння $s = (dr + k) \bmod n$, також одержуємо і рівнянь з $i+1$ невідомими:

$$\begin{cases} d = {(s_1 - k_1)}/{r_1} \bmod n, \\ \vdots \\ d = {(s_i - k_i)}/{r_i} \bmod n. \end{cases} \qquad (6.137)$$

Аналогічно, використовуючи алгоритми EC-GDSA і EC-KCDSA, можна одержати відповідно системи рівнянь порядку i з $i + 1$ невідомими.

Таким чином, для повного розкриття, тобто визначення секретного ключа d за i отриманим ЦП, необхідно розв'язувати систему i-го порядку з $i + 1$ невідомими.

У разі якщо повідомлення M є зашифрованим, невідомими є значення геш-функцій $e_1, e_2, ..., e_i$. Як результат одержимо систему рівнянь з $2i+1$ невідомими, тому шифрування підписаних повідомлень дозволяє істотно підвищити стійкість.

У цілому, зважаючи на наведені вище результати, можна зробити такі висновки.

1. Існує велика кількість методів криптоаналізу криптографічних перетворень у групах точок еліптичної кривої; у розділі наведено класифікацію методів криптоаналізу, їх систематизацію та огляд.

2. Відомо, що складність криптоаналізу в групі точок еліптичних кривих є експоненційно складною. У розділі розглянуто теореми та доведення формул, що аналітично доводять складність криптоаналізу. Показується, що ці формули припускають, що криптоаналітик може провести необмежену кількість обчислень, тобто його обчислювальні ресурси й кількість спроб нескінченні (обмеження можуть бути накладені тільки на обсяг пам'яті).

Однак результати оцінки складності розв'язання задачі дискретного логарифма, отримані вище, на цей час чисто теоретичні, оскільки не існує можливості задіяти необмежений обчислювальний ресурс для полів великої розмірності. Таким чином, актуальною є задача визначення ймовірності, з якою дії криптоаналітика при зламуванні системи досягнуть поставленої мети за обмеженого обчислювального ресурсу (обчислювальної потужності криптоаналітичної системи). Чи навпаки – складності криптоаналізу системи в тих випадках, коли задана ймовірність правильного результату. У розділі подається виведення формул, які дозволяють оцінити складність криптоаналізу криптографічних перетворень у групі точок еліптичних кривих

методами ρ- Полларда та λ-Полларда, коли задана ймовірність, з якою необхідно досягти успіху. Доведено, що в цілому зберігаються пропорції оцінки складності для цих методів.