полное раскрытие. Противник находит секретный ключ пользователя.

Сутність атаки типу повне розкриття міститься в розв'язку дискретних логарифмічних рівнянь

$$X_A = \log_a Y_A (\mathrm{mod}\, P) \tag{15.32}$$

та

$$X_B = \log_a Y_B (\mathrm{mod}\, P)$$

При розв'язку (2.74) вважається, що загальносистемні параметри (*P*, *a*) та відкриті ключі $Y_A$ та $Y_B$ є відомими.

Якщо криптоаналітик визначить особистий ключ $X_A(X_B)$, то в подальшому він зможе нав'язувати хибні загальні секрети та відповідно хибні повідомлення. Для суттєвого ускладнення можливості нав'язування хибних загальних секретів використовують як довгострокові, так і сеансові загальні секрети.

Підтверджено, що складність криптоаналізу в групі точок еліптичних кривих є експоненційно складною задачею. Необхідно відмітити, що результати оцінки складності розв'язання задачі дискретного логарифма на цей час є чисто теоретичними, оскільки не існує можливості задіяти необмежений обчислювальний ресурс для полів великої розмірності.

Показано, що скоріше найшвидшим (найменш складним) алгоритмом атаки типу «повне розкриття» випадкових «неслабих» кривих над полями $F(p)$, $F(2^m)$ і $F(p^m)$ на цей час є паралельний метод ρ-Полларда. Його складність оцінюється як залежність вигляду

$$\mathrm{O}(\sqrt{\pi n/4}/r) \tag{9.59}$$

від порядку базової точки *n* та кількості працюючих паралельно процесорів $r$. Тому для обчислення складності розв'язання дискретного логарифмічного рівняння (9.58) може бути застосована наближена формула:

$$I = \sqrt{\frac{\pi n}{4}} \Big/ r \; . \tag{9.60}$$

Також було показано, що особистий ключ можливо одержати, розв'язавши рівняння вигляду:

(9.61)

$$d = \frac{\alpha_j - \alpha_i}{\beta_i - \beta_j} \pmod n, \ \beta_i \neq \beta_j .$$

Використання функції вигляду (6.99) розділу 6 цієї монографії дозволяє обчислення виконувати паралельно, тобто для різних областей значень процес пошуку коефіцієнтів $\alpha_k$ і $\beta_k$.

У п.6.8.2 наведена теорема щодо оцінки математичного сподівання складності дискретного логарифмування, коли очікуване число елементів, обраних до виникнення колізії, складає:

$$E(X) \approx \sum_{k=0}^{\infty} e^{-x^2/(2n)} = \int_0^{\infty} e^{-x^2/(2n)} dx = \sqrt{\pi n/2} \, . \qquad (9.62)$$

Тут же (п.6.8.2) зроблено оцінку складності дискретного логарифмування на основі методу ρ-Полларда з урахуванням імовірності колізії. Отримано формулу для оцінки ймовірності відбуття колізії за відомих порядку базової точки $n$ та складності $k$:

$$\begin{aligned} P(n,k) &= 1 - \frac{n}{n} \cdot \left(\frac{n-1}{n}\right)\left(\frac{n-2}{n}\right) \ldots \left(\frac{n-(k-1)}{n}\right) = \\ &= 1 - \left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) \ldots \left(1 - \frac{k-1}{n}\right). \end{aligned} \qquad (9.63)$$

Обґрунтованою є оцінка

$$P(n,k)=1-e^{-\left(\frac{1}{n}+\frac{k-1}{n}\right)\frac{k-1}{2}}=1-e^{-\frac{k(k-1)}{2n}}, \qquad (9.64)$$

яку можна подати у вигляді параметричного рівняння:

$$I^2-I+2n\ln(1-P_k)=0\,. \qquad (9.65)$$

З урахуванням того, що $I^2 >> I$, можна отримати для оцінки наближення:

$$I^2 \approx -2n\ln(1-P_k)$$

або

$$I_\rho \approx \sqrt{-2n\ln(1-P_k)}\,. \qquad (9.66)$$

У п.6.8.5 отримані оцінки складності криптоаналізу на основі λ-методу.

Імовірність того, що хоча б одне значення $\rho_1(Z_i)$ збігається з $\rho_2(Z_j)$ для всіх значень $k$, буде становити:

$$R(\rho_1(Z_i)=\rho_2(Z_j))=1-\left(1-\frac{1}{n_G}\right)^{k^2}, \qquad (9.67)$$

тобто (9.67) у загальному вигляді визначає ймовірність колізії за λ-методом Полларда.

Отримано також наближену формулу, аналогічну (9.64):

$$P_k = 1 - e^{-\frac{1}{n_G}\left(k^2-1\right)} = 1 - e^{-\frac{k^2-1}{n_G}},$$

або після ряду перетворень одержано формулу наближеної оцінки аналогічно (9.65):

$$I^2 - 1 + n\ln\left(1 - P_k\right) = 0\,. \qquad (9.68)$$

Таким чином, параметричні рівняння (9.65) і (9.68) можуть бути використані для оцінки складності дискретного логарифмування в групах точок еліптичних кривих при їх застосуванні для існуючих криптографічних перетворень – направленого шифрування, цифрового підпису, криптографічних протоколів і взагалі для різноманітних криптографічних механізмів.

У п.6.9 розглянуті задачі оцінки криптографічної стійкості для всіх стандартизованих алгоритмів ЕЦП, що також засновані на складності розв’язання дискретного логарифму в групі точок еліптичної кривої. Так, для знаходження секретного ключа ЕЦП EC-DSA і ECSS необхідно розв’язати рівняння:

$$Q = d \times G\,. \qquad (9.69)$$

У випадках УЦП ЕС GDSA і ЕС KCDSA необхідно розв'язати рівняння

$$Q = d^{-1} \times G, \tag{9.70}$$

а в разі УЦП ДСТУ 4145-2002 – порівняння

$$Q = -d \times G. \tag{9.71}$$