Elliptic Curve Summary

$E_p(a,b)$ is eqn $y^2 = (x^3 + ax + b) \pmod{p}$

$4a^3 + 27b^2 \neq 0 \pmod{p}$

Rules for adding points
Multiplication is Repeated Addition

$kQ$ represents $Q + Q + \ldots + Q$, $k$ times

Efficient Calculation

Point add(point Q, int ktimes) {
    if (ktimes = 0) return Origin;
    if (ktimes = 1) return Q;
    if (ktimes = 0/2) {
        Point tmp = add(Q, ktimes/2);
        return double(tmpB, tmp);
    }
    Point R = add(Q, ktimes - 1);
    return reg add(R, Q);
}

Runtime is $O(\log ktimes \times\text{cost of add})$

If I know $Q$ and $kQ$ it's hard to
\textbf{EC C - ONE METHOD}

\underline{Public Keys}

1. \(E_p(a, b)\) (cycle length)
2. \(G\) is a point with a large order value \(n\).

\underline{User A}

Select private key \(n_A\) \((n_A < n)\)

Calculate public key \(P_A = n_A \times G\).

Encrypt message to send to \(A\):

\[C_m = \begin{cases} k \times G, & P_m + k \times P_A \\ C_1, & C_2 \end{cases}\]

\(C_1\) and \(C_2\) are randomly selected (like El-Gamal)

Alice receives this \(P_m + k(n_A \times G)\)

\[C_2 = P_m + n_A(kG)\]

Alice takes \(C_1\) and multiplies it by \(n_A\). This gives her \(k \times n_A \times G\).

Calculates \(C_2 = k \times n_A \times G\).
Diffie–Hellman Key Exchange

\[ E_p(a, b) \]

\[ G \]

Alice \( n_A \quad P_A = n_A G \)

Bob \( n_B \quad P_B = n_B G \)

Alice \( \xrightarrow{P_A} \quad Bob \quad n_B \times P_A = n_B \times n_A \times G \)

Alice \( \xleftarrow{P_B} \quad Bob \quad n_A \times P_B = n_A \times n_B \times G \)