¿Qué difícil es el DECDLP en $E(\mathbb{F}_p)$? (12)

Resolver $nP = Q$ dado P y Q:

$j_1 P, j_2 P, j_3 P, \ldots, j_r P$ j_i al azar

$kP + Q, k_2 P + Q, \ldots, k_r P + Q$ k_i al azar módulo

Cuando hay una colisión $\Rightarrow$ $j_u P = k_v P + Q$

$\Rightarrow (j_u - k_v) P = Q.$

Un resultado probabilístico:

Thm (Colisión) contenedor con N pelotas n rojas, $N-n$ azules.

Bob elige una pelota al azar y la devuelve al contenedor. Bob elige otra pelota al azar y lo devuelve al contenedor. Bob sigue este procedimiento hasta que ha mirado m pelotas en total.

(a) $\Pr(\text{por lo menos una roja}) = 1 - \left(1 - \frac{n}{N}\right)^m$

(b) $\Pr(\text{por lo menos una roja}) \geq 1 - e^{-mn/N}$ (*)

$\Rightarrow$ $N \gg 0$ $m, n < 10\sqrt{N}$, entonces la $\geq$ en (*) para es más o menos una $=$.

Dem

(a) $Pr(\geq 1 \text{ roja}) = 1 - Pr(\text{todas azules})$

$= 1 - \prod_{i=1}^{n} Pr(i^{\text{a}} \text{ azul})$

$= 1 - \prod_{i=1}^{n} \frac{N-n}{N}$

$= 1 - \left(1 - \frac{n}{N}\right)^n$.

(b) $e^{-x} \geq 1-x$. □

Prop: G un grupo, $h \in G$ de orden N. Suponiendo que $\log_h(H)$ tiene solución, la solución se puede encontrar en $\Theta(\sqrt{N})$ pasos, donde cada paso es una operación de G.

Dem: $1P, 2P, \ldots, nP$ ← pelotas rojas

$k_1P+Q, k_2P+Q, \ldots, k_nP+Q$ ← elegir una pelota roja del grupo

$Pr(\text{alguno de los } k_iP+Q \text{ es roja}) \approx 1 - \left(1 - \frac{n}{N}\right)^n \approx 1 - e^{-n^2/N}$.

Entonces, p.ej., si $n \approx 3\sqrt{N} \Rightarrow Pr(\ ) \approx 1 - e^{-9} \approx 0.99987\ldots$

① Parámetros públicos:

primo p (grande)

una CE E sobre $\mathbb{F}_p$

$P \in E(\mathbb{F}_p)$.

② Computaciones privadas:

Alice:

genera $n_A \in \mathbb{Z}$

calcula $Q_A = n_A P$

Bob

genera $n_B \in \mathbb{Z}$

calcula $Q_B = n_B P$

③ Intercambio público

Q_A →

← Q_B

④ Computaciones privadas

Alice

calcula

$n_A Q_B = n_A n_B Q P$ ——— $n_B Q_A = n_B n_A Q$.

Bob

calcula

Def: El ECDHP es el problema de determinar $n_1 n_2 P$ solo sabiendo $n_1 P$ y $n_2 P$ (pero no n_1, n_2 en particular)

Obs: La práctica solamente se mancha la primera coordenada del punto. A lo peor, tendrían

$\pm n_B Q = \pm (n_A n_B) P$ si eligen la incorrecta raíz $Y^2 = \square$.

El Gamal

① Paramètres publics

p premier (grand) ; $E \setminus \mathbb{F}_p$, $P \in E(\mathbb{F}_p)$

② Création de clefs :

Alice

Elle choisit n_A

Calcule $Q_A = n_A P \in E(\mathbb{F}_p)$

Publie Q_A

③ Encryption

Bob

$M \in E(\mathbb{F}_p)$

k éphémère

Calcule

$C_1 = kP \in E(\mathbb{F}_p)$

$C_2 = M + kQ_A \in E(\mathbb{F}_p)$

Envoie (C_1, C_2) à Alice

④ Desencryption

Calcule

$$\begin{aligned} C_2 - n_A C_1 &= M + kQ_A - n_A kP \\ &= M + kQ_A - knP \\ &= M + kQ_A - kQ_A \\ &= M. \end{aligned}$$

Entonces si

$j_1 P, j_2 P, \ldots, j_r P$ y $k_1 P + Q, k_2 P + Q, \ldots, k_s P + Q$ hay $r \approx 3\sqrt{p}$ hay buen chance de encontrar una colisión.

Desventaja del método: requiere mucho espacio.

Otra opción el algoritmo Pollard-rho tiene la misma complejidad $\Theta(\sqrt{p})$ pero sin guardar nada. Proyecto!

El estado de la arte:

El algoritmo conocido más eficiente para resolver el ECDLP tiene complejidad $\Theta(\sqrt{p})$

Cálculo de índices DLP clásico tiempo subexponencial.

¿Entonces ECDLP más difícil que DLP?

Criptografía con curvas elípticas..

Consideremos:

1) Diffie-Hellman y

2) ElGamal.

Dos preguntas:

1) ¿Cómo se determina un mensaje en $M \in EC(F_p)$?

Una pregunta difícil en general:

para curvas de ciertas formas hay "encodings" inyectivos y eficientes.

Lo que se trata de evitar.

2) ~~El Gamal tiene una tasa de expansión 4:1 Se puede mejorar?~~ C

P.ej:

Menezes - Van Stone - ElGamal

Alice

n_A,

$Q_A = nP_A$

Bob

Textos planos m_1 y m_2

k al azar

$R = kP$

$S = kQ_A$, $S = (x_S, y_S)$

Sea $C_1 \equiv x_S m_1$ (cifrado)

$C_2 \equiv y_S m_2$

(R, C_1, C_2) a Alice

$T = n_A R$ $T = (x_T, y_T)$

~~$= n_A kP$~~

~~$= kQ_A$~~

$m_1' = x_T^{-1} C_1$

$m_2' = y_T^{-1} C_2$

$m_1 = m_1'$,

$m_2 = m_2'$