

Glimpse of elliptic curves in cryptography, using GP/PARI

Recall

Discrete logarithm problem:

(p, g) , p prime, g generator of \mathbb{Z}_p^*

Hard

Given $g^a \bmod p$, find a . $[[a$ is encoded by pair $(g, g^a)]]$

Similar set-up for elliptic curves.

Note

\mathbb{F}_p^* can be thought of as a "degenerate elliptic curve"

$[[$ Degenerate means roots of multiplicity $> 1]$

Let E be an elliptic curve / \mathbb{F}_p (p prime)

Suppose $P \in E(\mathbb{F}_p)$ of large order exists.

Then, given $Q = [a]P$, it is hard in general to find $a \in \mathbb{Z}$ which satisfies this.

Can encode a as $(P, [a]P)$

Advantages (for use in cryptography)

Smaller primes needed (compared to \mathbb{Z}_p^*)

Less memory, less storage

More secure, more efficient

Analogue of Diffie-Helman key exchange

Public Key (p, E, B) , p prime, E elliptic curve, B point in E

M(ichael), N(ikita) choose $m, n \rightarrow$ publish mB, nB

ElGamal analogue

Encrypt message P_x

M chooses r (at random) and posts

$$(rB, (P_x, P_y) \oplus m(rB)) \text{ [a pair of points on } E]$$

To decrypt, N computes $n \times (\text{first coord})$ and subtracts this from 2nd coord (

$$= (P_x, P_y) \oplus r(nB))$$

$\rightarrow (P_x, P_y) + r(nB) - n(rB) = (P_x, P_y)$ then take first coordinate

\rightarrow original message.