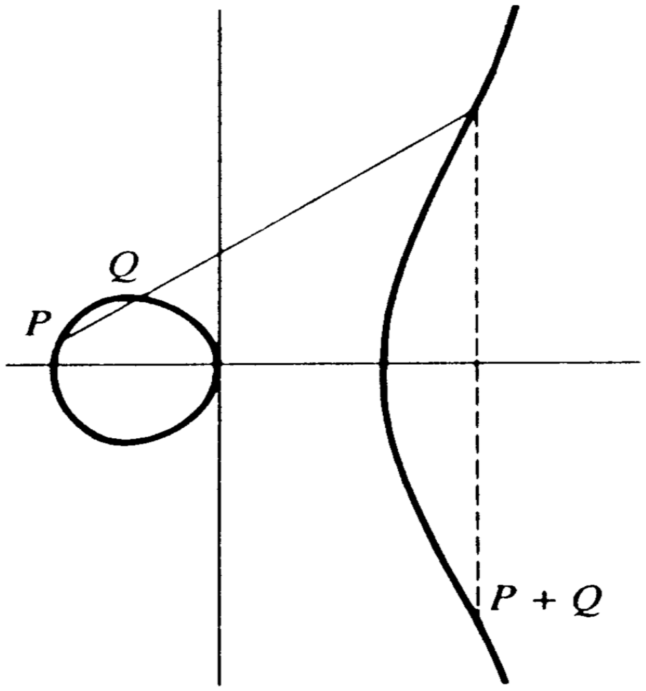
Cryptosystems

ElGamal on Elliptic Curves

G. Esther Guan

Mentor: Yao-rui Yeo

Background



- Elliptic Curves – non-singular cubic curves

  $y^2 = x^3 + ax + b$ (no multiple roots), O point at infinity

- Addition on elliptic curves (P+Q)

  $x_{P+Q} = m^2 - x_p - x_Q, y_{P+Q} = -y_P + m(x_p - x_{\mathrm{Q}})$

- Legendre symbol* - for n prime:

  $$\left(\frac{a}{n}\right) = a^{(n-1)/2}\ mod\ n = \begin{cases} 0, if\ n|a \\ 1, if\ a\ is\ a\ square\ mod\ n \\ -1, if\ a\ is\ a\ not\ a\ square\ mod\ n \end{cases}$$

  *Computation can be simplified using quadratic reciprocity

ElGamal on Elliptic Curves

- ElGamal on Finite Fields

  Encrypted Message: $\left(g^k, Pg^{ak}\right)$ - g^a public key, a private key, P message

- Discrete log → Multiples of points (over F_q)

  For some b, y: $b^x = y, x = ?$ → for some Q: $kQ \in E, k = ?$

- ElGamal on Elliptic Curves

  Private: key a, message P_m, some random k

  Public: key aQ, encrypted message $(kQ, P_m + k(aQ))$

  To decrypt: $P_m = P_m + k(aQ) - a(kQ)$

Example – Encoding the Letter "S"

"1" = 0, … , "0" = 9, "A" = 10, … , "Z" = 35
Number of chances to look for valid $(y^*)^2$: $\kappa = 20$
E = $y^2 + y = x^3 - x$ over the field of $p = 751$ elements

- $y^* = y + 376$: $E \rightarrow (y^*)^2 = x^3 - x + 188$
- "S" = 28, cycle through $x = \kappa\text{"}S\text{"} + j,\ \ j \in [1, \kappa]$
  - $j = 1 \rightarrow x = 561 \rightarrow (y^*)^2 = 261 \rightarrow \left(\frac{261}{751}\right) = -1$
  - $j = 2 \rightarrow \underline{x = 562} \rightarrow (y^*)^2 = 598 \rightarrow \left(\frac{598}{751}\right) = 1$
- $y^* = \sqrt{598} = \underline{201}$

$$\boxed{\mathrm{S} \rightarrow (562, 201)}$$

Example – Encrypting "S" w/ Elliptic ElGamal

E = $y^2 + y = x^3 - x$ over the field of $p = 751$ elements
Q = (0, 0), public key = aQ = (201, 380), $k = 386$

- $y^* = y + 376$: $(0,0) \rightarrow (0,376)$; $(201,380) \rightarrow (201,5)$
- "Clue": $kQ^* = 386Q = 2\left(B + 2\left(2\left(2\left(2\left(2(2(B+2B))\right)\right)\right)\right)\right)$

  $= (676,558) \rightarrow \underline{(676,182)}$
- Secret Message: $P_m + k(key) = (562,201) + 386(201,5)$

  $= (385,328) \rightarrow \underline{(385,703)}$