Recap: Point addition on elliptic curve

[Washington Chapter 2.6]

Suppose that $P=(x_1,y_1)$ $Q=(x_2,y_2)$

$m=(y_2 \oplus \neg y_1) \otimes \boxed{1/(x_2 \oplus \neg x_1)}$ → computation time for field inversion $O(\lg^3 p)$

Bottleneck of point addition

$c = y_1 \oplus \neg m \otimes x_1$

$x_3 = m \otimes m \oplus \neg x_1 \oplus x_2$

$y_3 = \neg m \otimes x_3 \oplus \neg c$

$P \oplus Q = (x_3, y_3)$

Jacobian Coordinate

$M = y_2 \oplus \neg y_1 \qquad Z_3 = x_2 \oplus \neg x_1$

$m = M \otimes 1/Z_3$

$c = y_1 \oplus \neg m \otimes x_1 = y_1 \oplus \neg M \otimes 1/Z_3 \otimes x_1$

$= 1/Z_3 \otimes [\underbrace{y_1 \otimes Z_3 \oplus \neg M \otimes x_1}_{\hat{c}}]$

$c = 1/Z_3 \otimes \hat{c}$

$x_3 = m \otimes m \oplus \neg x_1 \oplus \neg x_2$

$= \underbrace{M \otimes M \otimes 1/Z_3 \otimes 1/Z_3}_{M^2 \otimes 1/Z_3^2} \oplus \neg x_1 \oplus \neg x_2$

$= 1/Z_3^2 \otimes [\underbrace{M^2 \oplus \neg x_1 \otimes Z_3^2 \oplus \neg x_2 \otimes Z_3^2}_{X_3}]$

$= X \otimes 1/Z_3^2$

$y_3 = \neg m \otimes x_3 \oplus \neg c$

$= \neg M \otimes 1/Z_3 \otimes X \otimes 1/Z_3^2 \oplus 1/Z_3 \otimes \hat{c}$

$= 1/Z_3^3 \otimes [\underbrace{\neg M \otimes X \oplus \hat{c} \otimes Z_3^2}_{\hat{Y}_3}] = \hat{Y} \otimes 1/Z_3$

$M = y_2 \oplus \neg y_1, \; Z_3 = x_2 \oplus \neg x_1$

$c = y_1 \otimes Z_3 \oplus \neg M \otimes x_1$

$X_3 = M^2 \oplus \neg x_1 \otimes Z_3^2 \oplus \neg x_2 \otimes Z_3^2$

$\hat{Y}_3 = \neg M \otimes X \oplus \hat{c} \otimes Z_3^2$

The bottleneck operation is $\otimes$ which takes $O(\log p \log\log p)$.

$(x_1,y_1) \oplus (x_2,y_2) = (X_3, Y_3, Z_3) = (x_3, y_3)$

When $x_3 = X_3 \otimes 1/Z_3^2$

$y_3 = \hat{Y}_3 \otimes 1/Z_3^3$

still need inversion which takes $O(\log^3 p)$ anyway ☹

Scalar Multiplication Calculate 16P

$P \oplus P = 2P$

$2P \oplus 2P = 4P$

$4P \oplus 4P = 8P$

$8P \oplus 8P = 16P$

$(x_1, y_1) \oplus (x_1, y_1) = (X_2, Y_2, Z_2)$

$(X_2, Y_2, Z_2) \oplus (X_2, Y_2, Z_2) = (X_4, Y_4, Z_4)$

$(X_4, Y_4, Z_4) \oplus (X_4, Y_4, Z_4) = (X_8, Y_8, Z_8)$

$(X_8, Y_8, Z_8) \oplus (X_8, Y_8, Z_8) = (X_{16}, Y_{16}, Z_{16})$

$4 \times O(\log p \log\log p)$

$(X_{16}/Z_{16}^2, Y_{16} \otimes 1/Z_{16}^3)$ ← $O(\log^3 p)$ lazy division.

If we need m point additions,

computation time $= m \times O(\log p \log\log p) + O(\log^3 p)$

In the previous algorithm, $m = O(\log^2 p)$

computation time $= O(\log^2 p)\, O(\log p \log\log p) + O(\log^3 p)$

$= O(\log^3 p \log\log p)$

Double-based Number Representation (DBNS)

$57 = \underbrace{2^5 + 2^4 + 2^3 + 2^0}_{O(\lg p) \text{ terms}}$ (binary representation)

$57 = \underbrace{2 \cdot 3^0 + 3^1 + 3^0}_{O(\lg p) \text{ terms}}$ (ternary representation)

merge

$57 = 2^3 \cdot 3^1 + 3^2 = 48 + 9$ [Double-based Number representation]

Situation: P is fixed for many scalar multiplications, but a changed. (↳ scalar)

Pre-computation

$2^0 3^0 P \quad 2^1 3^0 P \quad 2^2 3^0 P \quad \cdots \quad 2^n 3^0 P$

$2^0 3^1 P \quad 2^1 3^1 P \quad \circ\circ \; 2^3 3^1 P \; \circ\circ \quad 2^n 3^1 P$

$2^0 3^2 P$ ⋮

$2^0 3^m P \quad \circ\circ\circ \quad 2^n 3^m P$

$[n = \lceil \log_2 p \rceil]$

$[m = \lceil \log_3 p \rceil]$

add together to have $57P$

How to find #DBNS?

- We want to find a representation with smallest # terms → smallest # additions.

Greedy algorithm Suppose that we want to calculate $aP = Q$

1: $Q \leftarrow \infty$

2: Find the largest $2^i 3^j$ ~~smaller~~ no larger than a [i and j are integers]

3: $Q \leftarrow Q \oplus 2^i 3^j P$

4: $a \leftarrow a - 2^i 3^j$

5: If $a = 0$, then terminate.

Otherwise, go to Step 2

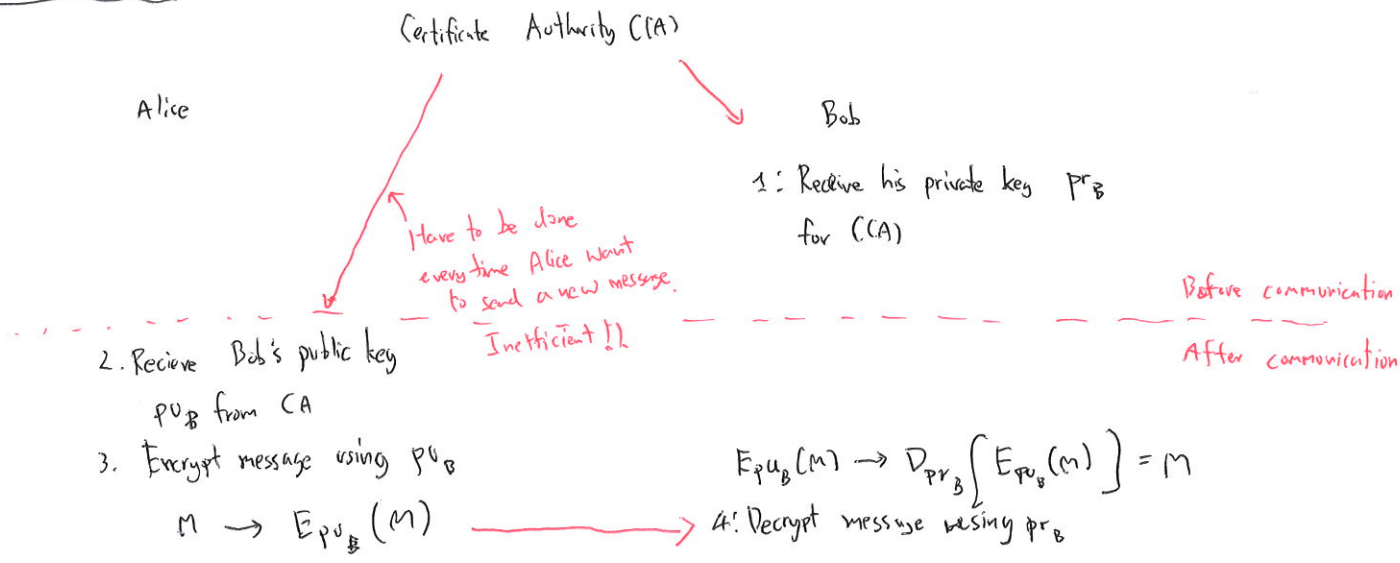
Theorem # terms = # point additions $= O(\log p / \log\log p)$

Computation time $= O(\log p / \log\log p) \cdot O(\log p \cdot \log\log p) + O(\log^2 p)$

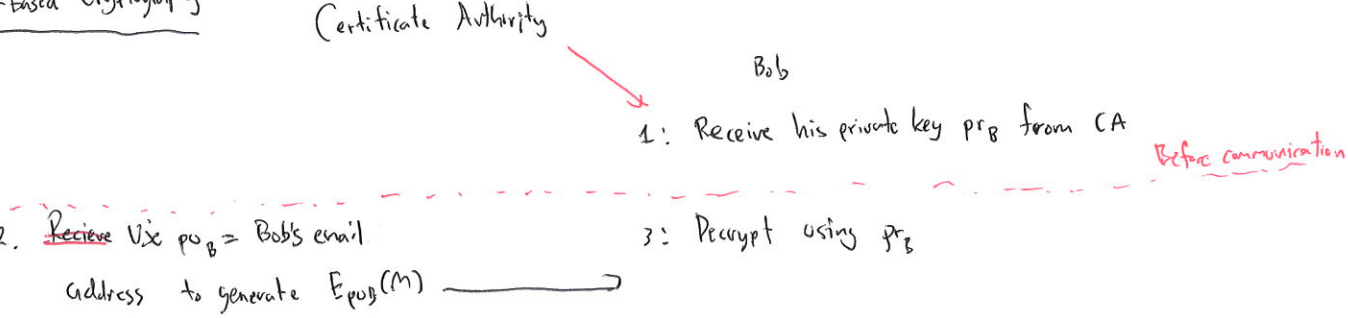
$= O(\log^2 p)$

Theorem # terms $= \Omega(\log p / \log\log p)$ for any algorithm for DBNS.

Public Key Cryptography [Washington, Chapter 6.9]



Identity-based Cryptography



Cryptographic Hash Function : H : (some set) $\to$ random bits length n.

1. It should be hard to find a and b such that $H(a) = H(b)$.

Given b, It is hard to find a such that $H(a) = b$.

Most common : MD5, SHA-1

Recommended : SHA-3

Field Extension Prime field on $\mathbb{F}_7 = \{0, 1, \dots, 6\}$

Irreducible polynomial : $x \otimes x \oplus 2 = 0$

There is no solution to this equation. ☹

x	$x \otimes x \oplus 2$
0	
2	
2	
3	
4	
5	
6	

Bonus Question

Fill this table.

Include α ($\sqrt{5}$) to $\mathbb{F}_7$!

$\mathbb{F}_{7^2} = \{ a_0 + b\alpha : a, b \in \mathbb{F}_7 \}$

Operation : $(3+6\alpha) \otimes (6+5\alpha)$

$= (3 \otimes 6) + (5 \otimes 6)\alpha = 2 + 4\alpha$

$(3+6\alpha) \otimes (6+5\alpha) = (6 \otimes 5)\alpha^2 + (3 \otimes 6 \oplus 5 \otimes 3)\alpha + (3 \otimes 3) = 2\alpha^2 \oplus 2\alpha \oplus 4 = 2\alpha$

($\alpha^2 \oplus \alpha \oplus 4 = 0$)

Theorem $\mathbb{F}_{7^2}$ with the operation defined above is a field.

Weil Pairing A function e with following properties: [output of e is $\mathbb{F}_{p^2}$]

1. $e(S_1 \oplus S_2, T) = e(S_1, T) \otimes e(S_2, T)$ [$e(nS, T) = e(S, T)^n$]

   $e(S, T_1 \oplus T_2) = e(S, T_1) \otimes e(S, T_2)$ [$e(S, nT) = e(S, T)^n$]

2. $e(S, T) = 1$ for all T only if $S = \infty$

   $e(S, T) = 1$ for all S only if $T = \infty$

3. ~~$e(T, T) = 1$ for all T~~ 3. $e(T, T) \neq 1$ for all T.

4. $e(S, T)$ can be computed efficiently.

5. We cannot calculate $e(P, T)^{abc}$ from T, aT, bT, cT

Pairing Friendly Curve : $y^2 = x^3 \oplus 1$ when $p = 6l - 1$ for some prime l

Warning : This curve is not suitable for Diffie-Hellman Key Exchange Protocol.