

Elliptic Curve Cryptography

DR. ODELU VANGA

COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRI CITY



Generating our group

From the previous chart, and including the point at infinity O , we have a group with 13 points.

Since the $O(E)$ is prime, the group is cyclic.

We can generate the group by choosing any point other than the point at infinity.

Let our generator $P = (2, 7)$

The Group

We can generate this by using the rules of addition we defined earlier where $2P = P + P$

$$P = (2,7)$$

- Base point

$$2P = (5,2)$$

$$3P = (8,3)$$

$$4P = (10,2)$$

$$5P = (3,6)$$

$$6P = (7,9)$$

$$7P = (7,2)$$

$$8P = (3,5)$$

$$9P = (10,9)$$

$$10P = (8,8)$$

$$11P = (5,9)$$

$$12P = (2,4)$$

Encryption Rules

- Suppose we let $P = (2, 7)$ and
- choose the private key to be $k_{\text{priv}} = 7$
- Then public key $Q = 7P = (7, 2)$

Encryption:

choose random k

$$e_Q(M, k) = (\underbrace{kP}_{C_1}, \underbrace{M + kQ}_{C_2})$$

$$e_Q(M, k) = (k(2, 7), M + k(7, 2)),$$

where $M \in E$ and $0 \leq k \leq 12$

$\{ P, k_{\text{priv}} \text{ - scalar}$
 $Q = k_{\text{priv}} P$
 EC
 DHP
 Given P, Q
 finding k_{priv}

$$\begin{aligned} C_1 &= kP \\ C_2 &= m + kQ \end{aligned}$$

$$7P = P + 2P + 4P$$

$$2P = P + P$$

$$4P = 2P + 2P$$

Decryption Rule

Decryption:

$$d_K(C_1, C_2) = C_2 - k_{\text{priv}} C_1 = m$$

$$d_K(C_1, C_2) = C_2 - 7C_1$$

$$\text{where } K = k_{\text{priv}} = 7$$

This is based on the ElGamal scheme.

Security: Elliptic Curve Discrete Logarithm Problem (ECDLP)

$$C = \{C_1, C_2\}$$
$$C_1 = kP$$

$$\begin{array}{c} P, kP \\ \Rightarrow K \\ \text{ECDLP} \end{array}$$

$$Q, k_{\text{priv}}$$

$$C_1 = kP$$

$$C_2 = m + kQ$$

$$\begin{aligned} k_{\text{priv}} C_1 &= k_{\text{priv}} (kP) \\ &= (k_{\text{priv}} k) P \end{aligned}$$

$$\begin{aligned} C_2 &= m + k (k_{\text{priv}} P) \\ &= m + (k k_{\text{priv}}) P \end{aligned}$$

Alice Encrypts

$$\begin{aligned} 2P &= P + P - \text{double} \\ 3P &= 2P + P - \text{add.} \\ (K_{\text{priv}}, Q = K_{\text{priv}}P) & \text{ Bob} \end{aligned}$$

Suppose Alice wants to send a message to Bob.

Plaintext is $M = (10,9)$ which is a point in $E = \langle (2,7) \rangle$

- Choose a random value for k , $k = 3$
- So now calculate (C_1, C_2) :
- $C_1 = \underline{3(2,7)} = (8,3)$
- $C_2 = \underline{(10,9)} + 3\underline{(7,2)} = \underline{(10,9)} + \underline{(3,5)} = \underline{(10,2)}$
- Alice transmits $C = ((8,3), (10,2))$
 $\quad \quad \quad C_1 \quad \quad C_2$

Bob Decrypts

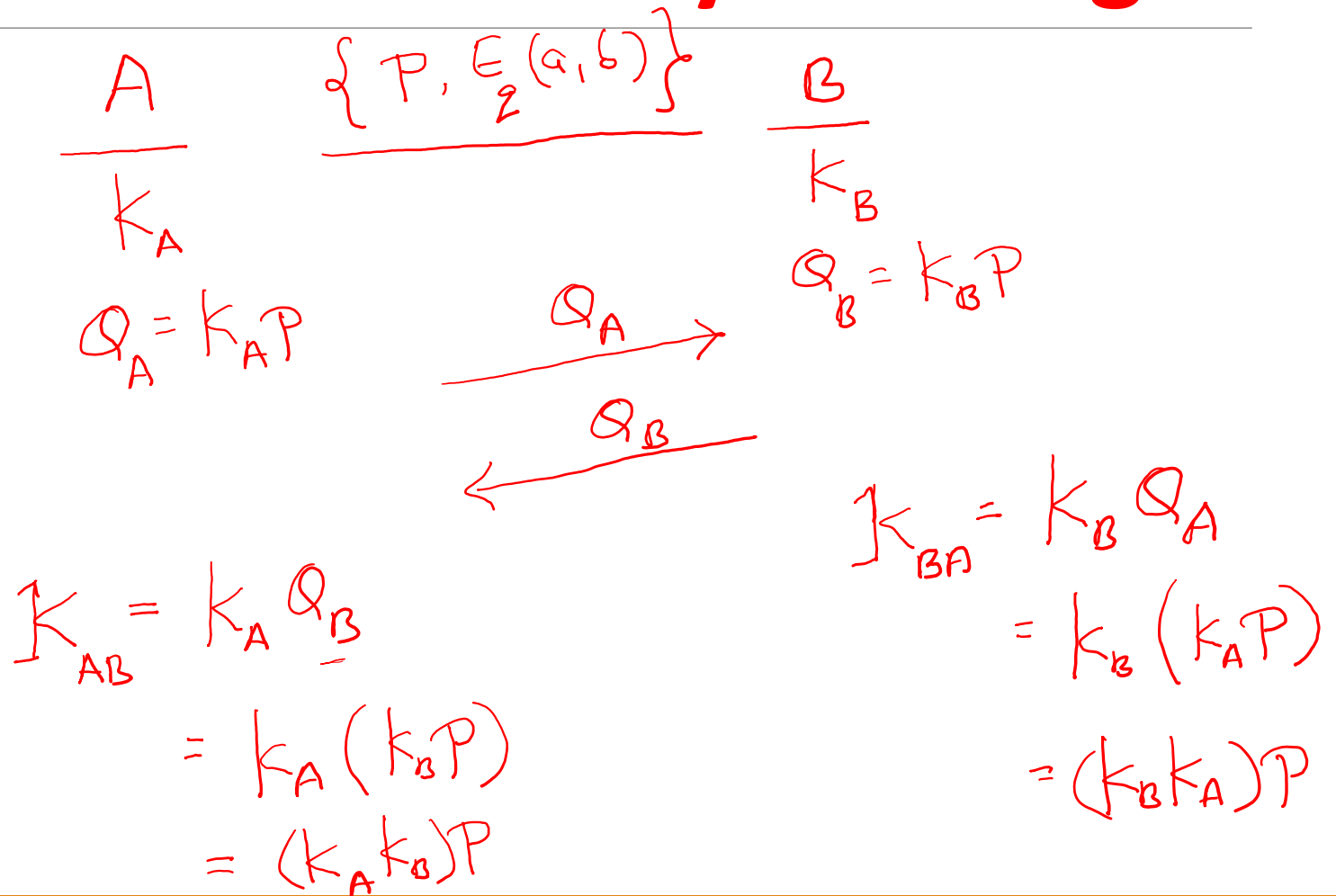
$$k_{\text{priv}}=7$$

Bob receives $C = ((\underbrace{8,3}_{C_1}), (\underbrace{10,2}_{C_2}))$

Calculates $M = (10,2) - 7(8,3) = (10,9)$

$$\underline{C_2} - k_{\text{priv}} C_1 = M$$

Diffie-Hellman Key Exchange

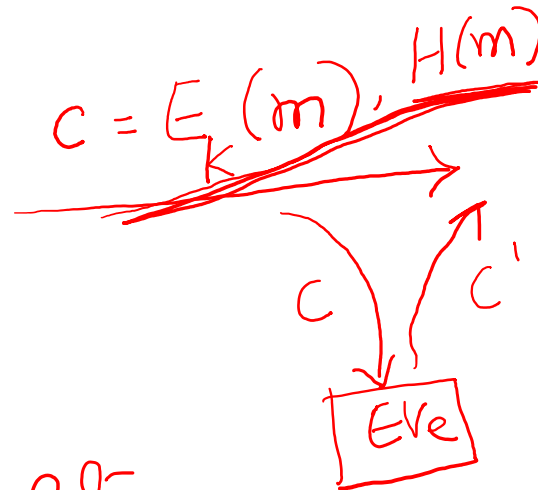


Two-Party Communication

$$x \Rightarrow H(x) \\ H(x) \not\Rightarrow x$$

$$\underline{x, y} \not\Rightarrow \underline{H(x)=H(y)}$$

$\langle k \rangle$ A



B $\langle k \rangle$

$$H(m') \neq H(m)$$

- * Confidentiality.
- * Integrity
- * Authentication
- * Non-repudiation.

$$C \rightarrow C' = E_K(m')$$

$$\boxed{H(m')}$$

Term Paper

The Java Pairing-Based Cryptography Library (JPBC)

(<http://gas.dia.unisa.it/projects/jpbc/#.YFLHN68zY2w>)

- **Title of the project:** Similar to your paper title
- **Group:** ____
- **Members:** Names and Roll Numbers
- **Abstract:** _____
- **Plan of Implementation:** Performance Analysis _____
- **Experimental Setup:** System configurations, Libraries used, _____
- **Summary of the results:** _____

Sources Used

“Recommended Elliptic Curves For Federal Government Use” July 1999

Cryptography Theory and Practice. Douglas Stinson, 3rd ed

A Friendly Introduction to Number Theory. Joseph Silverman, 3rd ed

Elements of Modern Algebra. Gilbert and Gilbert, 6th edition