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 then 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 $\mathbf{k_{priv}=7}$
- 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 $0 \le k \le 12$

P, K_{priv} - scalar

$Q = K_{priv} P$

EC DLP: Given P, Q finding K_{priv}

$\boxed{\begin{array}{l} c_1 = kP \\ c_2 = m + kQ \end{array}}$

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

$2P = P + P$

$4P = 2P + 2P$

Decryption Rule

$C = \{C_1, C_2\}$

$C_1 = kP$

Q, k_{priv}

$P, kP \Rightarrow k$

ECDLP.

$\boxed{C_1 = kP}$

$C_2 = m + kQ$

Decryption:

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

$$= m$$

$$k_{priv}C_1 = k_{priv}(kP)$$

$$= (k_{priv} \cdot k)P$$

$$C_2 = m + k(k_{priv}P)$$

$$= m + (k\, k_{priv})P$$

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

where $K = k_{priv} = 7$

This is based on the ElGamal scheme.

Security: Elliptic Curve Discrete Logarithm Problem (ECDLP)

Alice Encrypts

$2P = P + P$ - double
$3P = 2P + P$ - add.
$(K_{prv}, Q = K_{prv}P)$
Bob

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 = 3(2,7) = (8,3)
- C_2 = (10,9) + 3(7,2) = (10,9) + (3,5) = (10,2)
- Alice transmits C = ((8,3),(10,2))

C_1 C_2

Bob Decrypts

$k_{priv}=7$

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

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

$C_2 - k_{priv} C_1 = M$

Diffie–Hellman Key Exchange

$$\{P, E_2(a,b)\}$$

A		B
k_A		k_B
$Q_A = k_A P$	$\xrightarrow{Q_A}$	$Q_B = k_B P$
	$\xleftarrow{Q_B}$	

$$K_{AB} = k_A Q_B = k_A(k_B P) = (k_A k_B)P$$

$$K_{BA} = k_B Q_A = k_B(k_A P) = (k_B k_A)P$$

$x \Rightarrow H(x)$

$H(x) \not\Rightarrow x$

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

Two-Party Communication

$\langle K \rangle$ A

B $\langle K \rangle$

$c = E_K(m), \; H(m)$

$c \quad c'$

Eve

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

$c \to c' = E_K(\underline{m'})$

$\boxed{H(m')}$

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

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