Lecture 21 Elliptic curve Cryptography §6.4

Elliptic Curve Cryptography

Fix p, $E(\mathbb{F}_p)$, $P \in E(\mathbb{F}_p)$.

Alice

$n_A \in \mathbb{Z}$

$Q_A = n_A P$

Q_A →

Bob

$n_B \in \mathbb{Z}$

$Q_B = n_B P$

← Q_B

$n_A Q_B$

$n_B Q_A$

$n_A n_B P$

shared secret

ECDHP ≤ ECDLP

Eve: given $n_A P$ & $n_B P$, find $n_A n_B P$.

Naive approach: transmit (x_{Q_A}, y_{Q_B})

requires twice as much data to be transmitted as classical DH.

But given x_P, only two choices for y_P. Can replace y_P by a bit $b_P = \begin{cases} 0 & \text{if } 0 \le y_P < \frac{1}{2}P \\ 1 & \text{if } \frac{1}{2}P < y_P \le P-1 \end{cases}$

Then it is as efficient as classical DHP.

Called "bit compression" ... patented!

Modified ECDH

Alice

Pick n_A

Compute $Q_A = n_A P$

Publish $x(Q_A)$ →

← Publish $x(Q_B)$

n_B

$Q_B = n_B P$

Compute $\pm Q_B$,

$n_A(\pm Q_B)$

$x(\pm n_A Q_B) = x(\pm n_A n_B P)$

Compute $\pm Q_A$,

$n_B(\pm Q_A)$

$x(\pm n_B Q_A) = x(\pm n_A n_B P)$

agree on $x(n_A n_B P) \in \mathbb{F}_p$.

This uses 2 fewer bits to agree on 1 fewer bit of info

Elliptic Curve Elgamal

Fix p, $E(\mathbb{F}_p)$, $P \in E(\mathbb{F}_p)$ w/ $\text{ord}(P) = q$ large prime

Alice

Private key $n_A \in \mathbb{Z}/q$

Public key $Q_A = n_A P \in E(\mathbb{F}_p)$

$\xrightarrow{\text{Publish } Q_A}$

Bob

Plaintext $M \in E(\mathbb{F}_p)$

Pick random k

$$\begin{cases} C_1 = kP \in E(\mathbb{F}_p) \\ C_2 = kQ_A + M \in E(\mathbb{F}_p) \end{cases}$$

$\xleftarrow{\text{Publish } (C_1, C_2)}$

Compute

$$\begin{aligned} C_2 - n_A C_1 &= C_2 - n_A kP \\ &= C_2 - kQ_A \\ &= M. \end{aligned}$$

Issues

(1) How to encode {messages} $\hookrightarrow E(\mathbb{F}_p)$?!

(2) Elgamal: Ciphertext = 2 · Plaintext

EC Elgamal: Ciphertext = $\frac{4}{2}$ · Plaintext

↳ Easily improved w/ bit compression

Improvement

Menezes-Vanstone variant of EC Elgamal

Alice

Private $n_A \in \mathbb{Z}/q$

Public $Q_A = n_A P \in E(\mathbb{F}_p)$

publish Q_A →

Bob

Plaintext $m = (m_1, m_2) \in \mathbb{F}_p^2$

$R = kP \in E(\mathbb{F}_p)$

$S = kQ_A \in E(\mathbb{F}_p)$

$c_1 = x_S m_1 \in \mathbb{F}_p$

$c_2 = y_S m_2 \in \mathbb{F}_p$

← (R, c_1, c_2)

$S = n_A R = (x_S, y_S)$

$m_1 = x_S^{-1} c_1$

$m_2 = y_S^{-1} c_2$.

Rmk Plaintext size $= 2p$

Ciphertext size $= 3p$

$3/2$ increase in size

Smaller than Elgamal!!

But $(m_1^{-1} c_1)^3 + A(m_1^{-1} c_1) + B = (m_2^{-1} c_2)^2$

$\Rightarrow$ If we know m_1 can compute m_2.