Nov23

Tuesday, November 23, 2021 11:16 AM

Elliptic Curve Curve Cryptography

Setup: $p > 2$ odd prime.

$$E: \quad y^2 \equiv x^3 + Ax + B \mod p$$

for $$\Delta_E = 4A^3 + 27B^2 \not\equiv 0 \mod p.$$

The ECDLP

Given $P, Q \in E(\mathbb{F}_p)$ s.t.

$$Q = \underline{nP} \qquad (n \in \mathbb{Z})$$

Find $\underline{n} = \log_P Q$

Rmk n is well defined up to $|P|$

$$(n + |P|)P = nP + |P| \cdot P$$
$$= nP + O = nP$$

Last time

① Given P, n, analog of fast powering to compute nP quickly.
(Double & add)
(Project 2 $\Longrightarrow$ implement this!)

② BabySteps - GiantSteps gives an attack on ECDLP.

(still exponential in the bits of $|P| \approx O(p)$)

③ Elliptic Curve Diffie-Hellman.

Setup: Alice & Bob agree on p & E & $P \in E(\mathbb{F}_p)$

Alice	Eve	Bob
1) Secret $n_A \in \mathbb{Z}$		1) Secret n_B
2) $Q_A = n_A \cdot P$		2) $Q_B = n_B \cdot P$ ← Double & Add
3) Q_A →		← 3) Q_B
4) $R = n_A \cdot Q_B$		4) $R = n_B \cdot Q_A$

Pf/ $n_A Q_B = n_A n_B P = n_B n_A P = n_B Q_A$

Def^n

The Elliptic Curve Diffie-Hellman Problem (ECDHP) is:

Knowing: E elliptic curve $/\mathbb{F}_p$
$P \in E(\mathbb{F}_p)$
$n_1 P$ & $n_2 P$ (not knowing n_1 & n_2)

Find: $n_1 n_2 P$

Prop

The ECDLP solves the ECDHP.

(The ECDLP is harder than the ECDHP)

Pf/ Have n_1P, & n_2P.

Consult ECDLP oracle,

feed oracle n_1P

oracle tells me $\log_P n_1P = n_1$

Double & add $\Longrightarrow$ $n_1(n_2P) = n_1n_2P$

Exercise:

Let G be a group.

1) State DLP for G.
2) State DHP for G.
3) Show DLP $\xrightarrow{\text{solves}}$ DHP for G.

Remarks

1) Shared secret is $R = (x_R, y_R)$ which is 2 elts of $\mathbb{F}_p$......

but they have a relationship:

$$y_R^2 = x_R^3 + Ax_R + B$$

Once I know x_R, I know y_R^2

& taking $\sqrt{\ }$ get $\pm y_R$.

a) Feels like we're sending too much info.

b) Eve only to find x_R.

Message Compression for ECDH

Let x_R be the shared secret.

Only share x-coordinates.

Alice

1) secrent n_A
2) $n_A \underline{P} = Q_A = (x_A, y_A)$
3) x_A
4) $y_B^2 = x_B^3 + Ax_B + B$
5) $\pm y_B$
6) $(x_B, \pm y_B) = \pm Q_B$
7) $n_A(\pm Q_B) = \pm n_A Q_B$ $= \pm R$

Eve

Bob

1) Secret n_B
2) $n_B \underline{P} = Q_B = (x_B, y_B)$
3) x_B

4--6) $\pm Q_A$

7) $n_B(\pm Q_A) = \pm R$

Pf/ $\pm R = (x_R, \pm y_R)$

So x_R is shared secret.

Remark: Resilience to attacks

- DLP (over $\mathbb{F}_p^*$) has a subexponential attack (index-calculus) (HW 8)

- ECDLP best attacks is exponential (e.g. Baby Giant).

  Better security = smaller primes
  = faster implementation.

- Index-Calculus for ECDLP is interesting to think about

Elliptic Curve Elgamal

First Approach: do exactly what we did for Elgamal over $\mathbb{F}_p^*$.

Setup: Alice & Bob choose E & $P \in E(\mathbb{F}_p)$

Alice

Eve

Bob

Public key Creation

1) Secret n_A.
2) $Q_A = n_A \cdot P_A$
3) Q_A = public key.

Message Encryption

1) $M \in E(\mathbb{F}_p)$ ← plaintext
2) $k \in \mathbb{Z}$ ← random int
3) Ciper $\begin{cases} C_1 = k \cdot P \\ C_2 = k \cdot Q_A + M \end{cases}$

Decryption

$$C_2 - n_A C_1 = M$$

Proof $C_2 - n_A C_1 = \underline{kQ_A} + M - \underline{n_A C_1}$

$$= \cancel{\underline{k n_A P}} + M - \cancel{\underline{n_A k P}}$$

$$= M$$

Exercise

G a group. Describe Elgamal for G.

Issues

① Plaintext $\xleftrightarrow{??}$ Points in $E(\mathbb{F}_p)$.

For $\mathbb{F}_p^*$, used ASCII (intToText & TextToInt)

For EC....

Start a message. $\xrightarrow{\text{intToText}}$ $m \in \mathbb{F}_p$

$\rightsquigarrow y^2 = m^3 + Am + B$

⚠ $m^3 + Am + B$ might not have a square root!
(50% chance!).

No EC w/ x-coord = m
(similarly for y-coord).

② 4-1 message expansion... (?)

best a message can be is $x \in \mathbb{F}_p$

need to send 2 points. (4 coords).

Solutions

Solution to ①

→ ElGamal is incorporating a shared secret & symmetric cipher as one thing.

Use ECDHP for shared secret.

Use $\mathbb{F}_p^*$ for symmetric cipher.

↑ $m \in \mathbb{F}_p^*$ know how to do

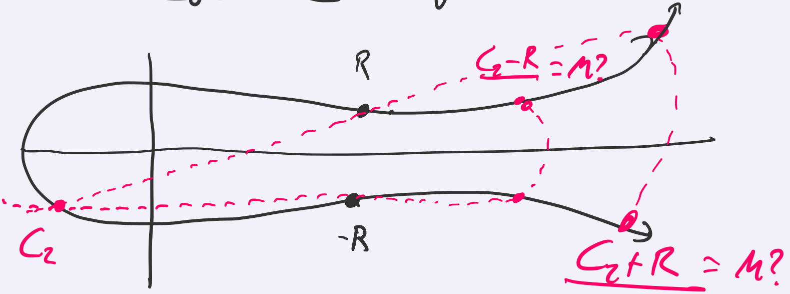
$$m \longmapsto x_R m \mod p$$

→ Also solve ②.

→ Project 2 will be implementing this mixed. Elgamal.

Solution for ②

⤳ Wrong Solution: only send x_1 coords.



Ambiguity in y-coord of shared secret.

Problem not ± of each other.

(Get around this by sending 1 extra bit)

Bob sends x coord. + one $b = 0, 1$

Alice computes $(x, \pm y) \rightsquigarrow$ w/ bit finds y

$$b = \begin{cases} 0 & 0 \le y < \frac{1}{2}p \\ 1 & \frac{1}{2}p < y \le p-1 \end{cases}$$

$$y < \tfrac{1}{2}p \rightsquigarrow p - y > p - \tfrac{1}{2}p = \tfrac{1}{2}p.$$

Elliptic Curve Digital Signatures

ECDSA which is directly analogous to DSA.

Recall

Document D

Sam signs $D \rightsquigarrow D^{Sig}$ ← only Sam can do

Victor checks (D, D^{Sig}) is valid. ← every can do.

Sam: Key Creation

- Public elliptic curve $E/\mathbb{F}_p$
- Public point $Q \in E(\mathbb{F}_p)$ w/ large prime order q.
- Secret signing key $1 < s < q-1$
- Compute $V = (sQ) \in E(\mathbb{F}_p)$.

Publishes (E, Q, V, q)

Document Signing

Document $d \in \mathbb{F}_q$.

Random $e \in \mathbb{F}_q^*$

different each time (c.f. HW 9)

Compute

$$\rightarrow s_1 = x(e\tilde{Q}) \mod q$$

$$s_2 = (\underline{d + ss_1})e^{-1} \mod q$$

$$D^{Sig} = (s_1, s_2).$$

Verification

$$v_1 = d \cdot s_2^{-1} \mod q$$

$$v_2 = s_1 s_2^{-1} \mod q$$

$$R = v_1 Q + v_2 V \in E(\mathbb{F}_p)$$

Check

$$x(R) \equiv s_1 \mod q \quad ?$$

If yes, sig correct!

Pf/ $R = v_1 Q + v_2 V$

$$= d s_2^{-1} \cdot Q + s_1 s_2^{-1} (sQ)$$

$$= s_2^{-1} (d + s s_1) Q$$

$$= s_2^{-1} (s_2 e) Q$$

$$= eQ$$

$$x(R) \equiv x(eQ) \equiv s_1 \mod Q$$

Lenstra's Elliptic Curve Factorization

Recall Pollard's (p-1)-algorithm

Factor $N = pq$ by finding L

s.t.
$$\left.\begin{aligned} A^L &\equiv 1 \mod p \\ A^L &\not\equiv 1 \mod q \end{aligned}\right\}$$

Then $\gcd(A^2-1, pq) = p$ ← we win.

Likely to work if $(p-1) \mid L$ & $\underline{\underline{(q-1) \nmid L}}$ (by Fermat's little theorem).

Then take $L = n!$ & hope $n!$ swallows up all prime facts of $(p-1)$

Idea GCD's witness arithmetic mod p & q that we know is going on under the hood.

Idea

Working
$$\begin{tikzcd} & \mathbb{F}_p \\ \mathbb{Z}/N\mathbb{Z} \arrow[ur] \arrow[dr] & \\ & \mathbb{F}_q \end{tikzcd}$$
$\Big\}$ Synthize

This is also going to work for an elliptic curve,

$E/(\mathbb{Z}/N\mathbb{Z})$ makes sense....

doing arithmetic $E/\mathbb{F}_p$ & $E/\mathbb{F}_q$ at the same time.

$nP = \mathcal{O}$ over $\mathbb{F}_p$ } see that

but $nP \neq \mathcal{O}$ over $\mathbb{F}_q$ } w/ GCDs & factor.

More Precisely

$N = pq$ trying to factor.

E given by $y^2 = x^3 + Ax + B$

$$\Delta_E = 4A^3 + 27B^2 \not\equiv 0 \bmod N.$$

Here $\underset{(a,b)}{\underset{\parallel}{P}} = E(\mathbb{Z}/N\mathbb{Z})$

$$b^2 \equiv a^3 + Aa + B \mod N.$$

Compute $P, 2P, 3P, \dots$ by rules in our EC addition alg...

Example $N = 187$

$E = y^2 + 3x + 7$

$P = (38, \underline{\underline{112}})$

① $2P$

$$\lambda = \frac{3x(P)^2 + A}{2y(P)} = \frac{34}{224} = 34 \cdot 91 \equiv 102 \mod 187$$

$$\left(\begin{array}{l} \text{Ext Euc Alg} \qquad \frac{1}{224} = 91 \\ \underline{224} \cdot 91 \equiv \underset{\text{w/ gcd}}{1} \mod \underline{187} \end{array} \right)$$

$$x(2P) = \lambda^2 - 2x(P) \equiv 43$$

$$y(2P) = \lambda(x(P) - x(2P)) - y(P)$$

$$= (102)(38-43) - 112 \equiv 126 \mod 187$$

$$2P = (43, 126). \quad \checkmark$$

② $3\underline{P} = 2\underline{P} + \underline{P}$

$$\frac{1}{x(2P) - x(P)} = \frac{1}{5} \equiv 75 \mod 187$$

$$\lambda = \frac{y(2P) - y(P)}{x(2P) - x(P)} = \frac{14}{5} = 14 \cdot 75 \equiv 115$$

$$\vdots$$

$$3\underline{P} = (54, 165)$$

③ $4P = 2P + 2P = 3P + P$

$$= \cdots = (93, 64) \qquad \text{(check).}$$

④ $5P = 3P + 2P$

$\lambda = \frac{\Delta y}{\Delta x}$ | $\Delta x = x(3P) - x(2P)$

$= \underline{54 - 43 = 11}$

Need $\frac{1}{\Delta x} \xrightarrow{EEA}$ But $\gcd(11, 187) = 11 \neq 1$

$\boxed{\underline{\text{can't compute } \lambda}}$

Couldn't add.... because we factored!!!

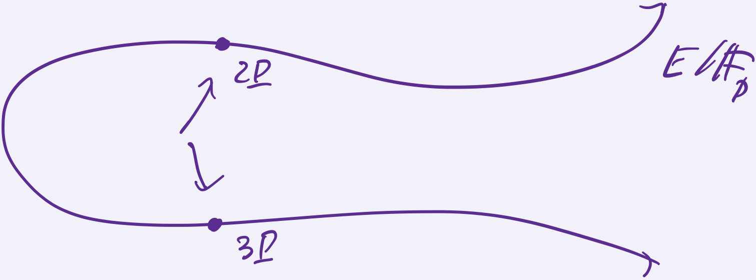
$11 \mid 187 \longrightarrow 11 \cdot 17 = 187.$

---

11 divided $\Delta x \equiv 0 \mod 11$

$\Delta y \neq 0$

"draw EC over $\mathbb{F}_p = \mathbb{F}_{11}$



$2P + 3P = \mathcal{O}$ in $\mathbb{F}_{11}$

But $\neq \mathcal{O}$ in $\mathbb{F}_{17}$ ←

we witness mod N that

$P + Q = \mathcal{O}$ mod p ⟸

$P + Q \neq \mathcal{O}$ mod q ⟸

That means $\gcd(\Delta x, N) \neq 1, N$

so we factored !!