Nov12

Wednesday, November 11, 2020 9:57 PM

Recall

Cryptosystem $\mathcal{M}, \mathcal{C}, \mathcal{K}$.

$$\Omega = \mathcal{M} \times \mathcal{C} \times \mathcal{K}$$

Variables $M, C, K : (m,c,k) \longmapsto m, c, k$ resp.

Def$^{\underline{n}}$ System has perfect secrecy if

$$f_{M|C}(m|c) = f_M(m) \overset{\text{Bayes'}}{\leftrightsquigarrow} f_{C|M}(c|m) = f_C(c)$$

"No info about m leaks from c"

Saw f_M & f_K determine f_C.

$$\rightsquigarrow f_C(c) = \sum_{k \in \mathcal{K}} f_K(k) \cdot f_M(d_k(c))$$

Reminder For any $k \in \mathcal{K}$

$$e_k : \mathcal{M} \longrightarrow \mathcal{C}$$ must be injective.

Any cryptosystem, $\#\mathcal{C} \geq \#\mathcal{M}$.

Perfect secrecy enforces more relationships.

Def$^{\underline{n}}$ $\mathcal{M}^+ = \{ m \in \mathcal{M} \mid f_M(m) > 0 \}$

Prop If a cryptosystem has perfect secrecy then $\# \mathcal{K} \geq \# \mathcal{M}^+$

Proof Fix $c \in \mathcal{C}$ w/ $f_C(c) > 0$

$\Rightarrow f(c|m) = f(c) > 0 \quad \forall \; m \in \mathcal{M}^+$

Since prob positive, $\Rightarrow \exists \; k$ s.t.

$e_k(m) = c$.

Fix different m'. Same argument shows

$\exists \; k'$ w/ $e_{k'}(m') = c$

$k \neq k'$. Else $e_k(m) = e_k(m')$ ↯

$m \neq m'$.

$\rightsquigarrow$ Each $m \in \mathcal{M}^+$ produce a $k \in \mathcal{K}$.

new

$\longrightarrow \# \mathcal{K} \geq \# \mathcal{M}^+$.

For perfect secrecy.... (all messages have positive of appearing i.e. $\mathcal{M}^+ = \mathcal{M}$).

$$\rightsquigarrow \quad \#\mathcal{C} \geq \#\mathcal{M} \leq \#\mathcal{K}.$$

$\Longrightarrow$ Most efficient use of perfect secrecy is when $\#\mathcal{C} = \#\mathcal{M} = \#\mathcal{K}$.

Theorem

Assume $\#\mathcal{K} = \#\mathcal{C} = \#\mathcal{M}$. & $\mathcal{M}^+ = \mathcal{M}$.

Then we have perfect secrecy if & only if the following 2 conditions hold.

(1) All $k \in \mathcal{K}$ are used with equal probability.

(2) $\forall\, m \in \mathcal{M}$ & $c \in \mathcal{C}$ there exists a unique key k w/ $\boxed{\begin{array}{c} \underline{d_k(c) = m.} \\ e_k(m) = c \end{array}}$

Proof

$\Longrightarrow$ Assume have perf. sec. Show (1&2)

For $m \in \mathcal{M}$ & $c \in \mathcal{C}$ define

$$S_{m,c} = \{ k \in \mathcal{K} \mid e_k(m) = c \}.$$

Notice $(2) \Longleftrightarrow \#S_{m,c} = 1 \quad \forall\, m, c.$

Lemma 1 If $m \neq m'$

Then $S_{m,c} \cap S_{m',c} = \emptyset$.

Proof

Let $k \in S_{m,c} \cap S_{m',c}$.

Then $e_k(m) = e_k(m')$. But e_k injective.

$\lightning$.

$\emptyset$

Lemma 2 $S_{m,c} \neq \emptyset$.

Proof

By perfect secrecy

$$\underset{\sim\sim\sim}{f(m,c)} = f(m|c)\cdot f(c) = \underline{f(m)}\cdot f(c) > 0$$

>0 b/c $\mathcal{M}^+ = \mathcal{M}$

& $\#\mathcal{M} = \#\mathcal{C}$

$\Longrightarrow \exists\, k$ s.t. $e_k(m) = c$

So $k \in S_{m,c}$ $\emptyset$

Lemma 3 $\#S_{m,c} = 1$.

Proof Fix $c \in \mathcal{C}$

disjoint by Lemma 1

$$\#\mathcal{K} \geq \#\Big(\bigcup_{m\in\mathcal{M}} S_{m,c}\Big)$$

$$= \sum_{m\in\mathcal{M}} \#S_{m,c}$$

at least 1

$\geq \# \mathcal{M}$

$\uparrow = \# \mathcal{K}.$

$D_0 =$ so each $\# S_{m,c} = 1$

Proves statement (2)

Proof of (1). (each k appears w/ = prob).

Fix $(k, m, c) \in \mathcal{K} \times \mathcal{M} \times \mathcal{C}$ s.t. $e_k(m) = c$

Notice $k, m \overset{e_k}{\text{det}}\ c.$ By part ②

know $m, c \rightsquigarrow S_{m,c} \rightsquigarrow k.$ (2)

$c, k \underset{d_k}{\text{determine}}\ m.$

In particular $f(m,k) = f(m,c) = f(c,k)$ *

All same event

$$\cancel{f(m)} \overset{\text{P.S.}}{=} f(m|c) = \frac{f(m,c)}{f(c)}$$

$$= \frac{f(m,k)}{f(c)}$$

$$= \frac{\cancel{f(m)} \cdot f(k)}{f(c)}$$

$\Longrightarrow \forall\ k, c \quad f(k) = f(c).$

$\Rightarrow f(k) = \frac{1}{\#\mathcal{C}}$ indep of k

& equal for all k. $\varnothing$

Remark

This says we need to randomly use keys to acheive perfect secrecy.
We don't want to do this.

$\rightsquigarrow$ Pretty much never have perfect secrecy.
Study of measuring secrecy is called "entropy". We don't cover it.

Want to see it, read 5.6.

Elliptic Curves & Cryptography

Elliptic curves are remarkably versatile mathematical objects exist all over mathematics connecting many interesting branches.

Example of an application: Fermat's Last Thm

No integer solutions to $a^n + b^n = c^n$ $\quad n \geq 3$.

Idea

Have
$a^n+b^n=c^n$
$a,b,c\in\mathbb{Z}$

$\xrightarrow{\text{Ribet's Theorem}}$ Constructs an elliptic curve $E_{a,b,c}$ & observe it is not modular

Wiles showed all elliptic curves are modular.

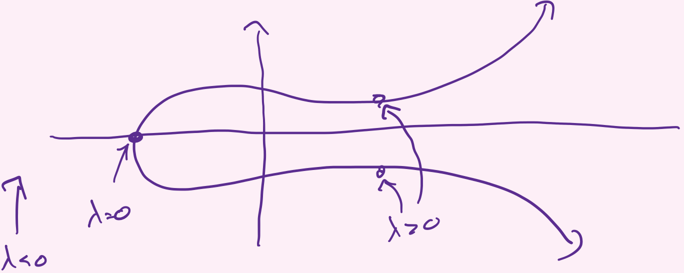
What is an elliptic curve?

The set of solutions to an equation of the form

$$y^2 = x^3 + ax + b$$

↑ weierstrass equation.

Examples $\boxed{1}$ $y^2 = x^3 - 3x + 3$

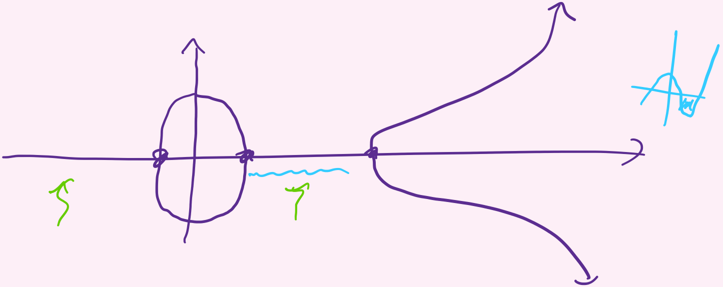


① Symmetry over x-axis.

Fix some x. $\lambda = x^3 - 3x + 3$ ⇐

$y = \pm\sqrt{\lambda}$ is y coord.

Example $\boxed{2}$ $y^2 = x^3 - 6x + 5$ ←



Still have symmetry over x-axis.

3 solns w/ $y=0$

Remark Call E - elliptic curve.

These pictures are of real value solutions.

$E(\mathbb{R})$

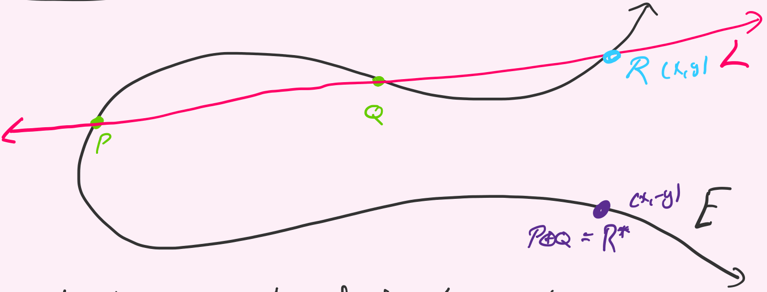
Also care about $\mathbb{C}$-solutions.

$E(\mathbb{C})$ ← Topologically a torus

Also care about $\mathbb{F}_p$-solutions } crypto

$E(\mathbb{F}_p)$ ← Geometry?

Elliptic Curves have an amazing features... you can add points together



Addition can be defined w/ geometry.

① $L = \overline{PQ}$

→ ② $L \cap E = \{P, Q, R\}$ ← {Bezout: a line & cubic interact @ 3 pts in general}

③ Reflect R over x-axis to get R*

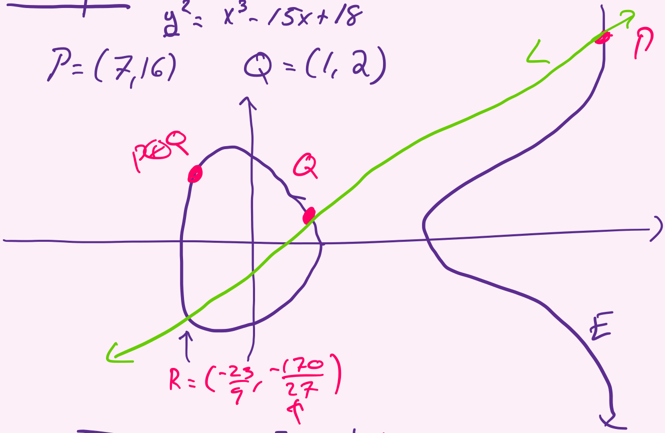
④ $P \oplus Q := R^*$

Described some process. Try it out.

Example

$$y^2 = x^3 - 15x + 18$$

$P = (7, 16)$ $Q = (1, 2)$



$R = \left(\frac{-23}{9}, \frac{-170}{27}\right)$

$L = \overline{PQ}$ $y = \frac{7}{3}x - \frac{1}{3}$ ←

$$\left(\frac{7}{3}x-\frac{1}{3}\right)^2 = x^3-15x+18$$

$$0 = x^3 - \underset{\nearrow\ \parallel}{\frac{49}{9}}x^2 - \frac{121}{9}x + \underset{\swarrow\ \nwarrow}{\frac{161}{9}}$$

$$(x-\underset{\uparrow}{1})(x-\underset{\uparrow}{7})(x-\underset{\uparrow}{\lambda})$$

$$(-1)(-7)(-\lambda) = \frac{161}{9}$$

$$\Longrightarrow \lambda = \frac{-23}{9}$$

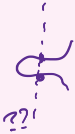
$$\rightsquigarrow P\oplus Q = \left(\frac{-23}{9}, \frac{170}{27}\right)$$

Questions

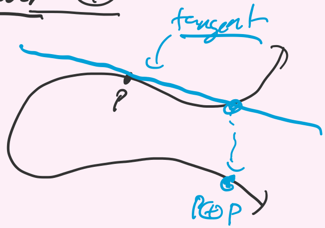
① What about $P\oplus P$?

② What abt $P\oplus P^*$? ←

③ What is identity?
What is inverse?



Answer ①

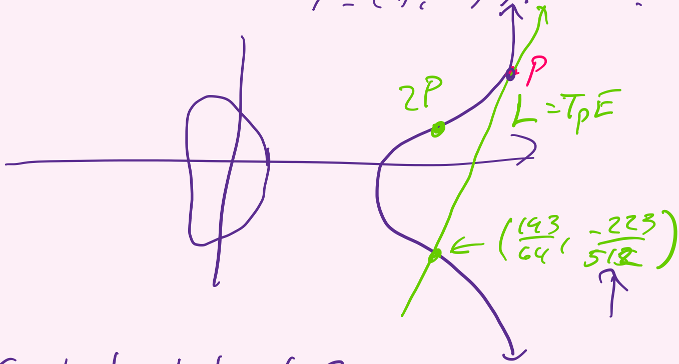


$P\oplus P$ to relate to $P\oplus Q$ for Q close to P!

Example

Same one → $y^2 = x^3 - 15x + 18$

$P = (7, 16)$, $P \oplus P = ?$



① Compute tangent line to P.

Implicit differentiation.

$$2y\frac{dy}{dx} = 3x^2 - 15$$

$$\frac{dy}{dx} = \frac{3x^2 - 15}{2y} \overset{\substack{x=7\\y=16}}{=} 33/8$$

② Intersect L & E

$$L: y = \frac{33}{8}x - \frac{103}{8} \qquad y^2 = x^3 - 15x + 18$$

$$0 = x^3 - \frac{1089}{\underset{\parallel}{64}}x^2 + \frac{2919}{32}x - \frac{9457}{64}$$

$$\underset{\sim}{(x-7)^2}\,(x-\underset{\sim}{\lambda})$$

↑ tangent @ $x=7$.

Rmk sum of roots =

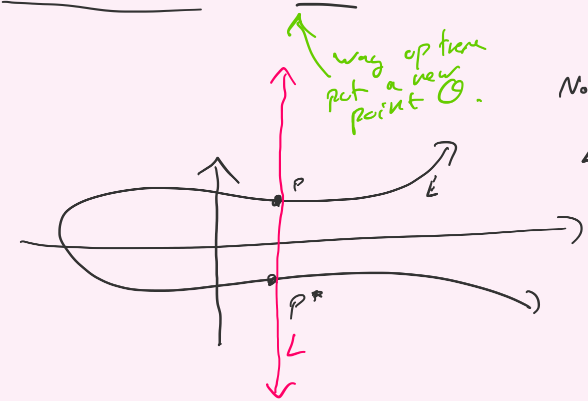
$$-49\lambda = -\frac{9457}{64}$$

$$\implies \lambda = {}^{193}/_{64}$$

$$\rightsquigarrow 2P = \left(\frac{193}{64}, \frac{223}{512}\right)$$ ✓

Question 2

$\underline{P \oplus P^*}$??



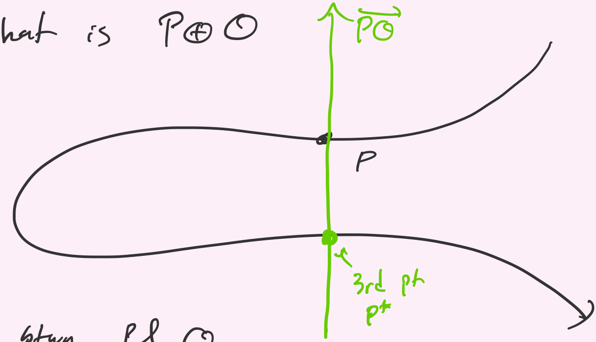
No third point on $E \cap L$

New point $\mathcal{O}$ "point at infinity" it is at the end of every vertical line.

Then $\underline{P \oplus P^* = \mathcal{O} \text{ for all } P \in E}$

This actually solves question 3:

What is $P \oplus \mathcal{O}$



Line btwn P & $\mathcal{O}$ is vertical

$$\Longrightarrow P \oplus \mathcal{O} = (P^*)^* = P$$

* So $\mathcal{O}$ is the identity!!!

* Inverse of P is P^*!!

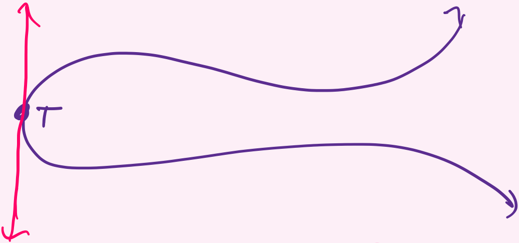
* Associativity is a bit more difficult to prove from this perspective.

Remark Elliptic curves are abelian b/c

$$\overline{PQ} = \overline{QP}$$

Example Elliptic curves have torsion

G a group. $G[n] = \{g \in G \mid g^n = 1_G\}$



$$\Longrightarrow T \oplus T = 2T = \mathcal{O}$$

So $T \in E[2]$.