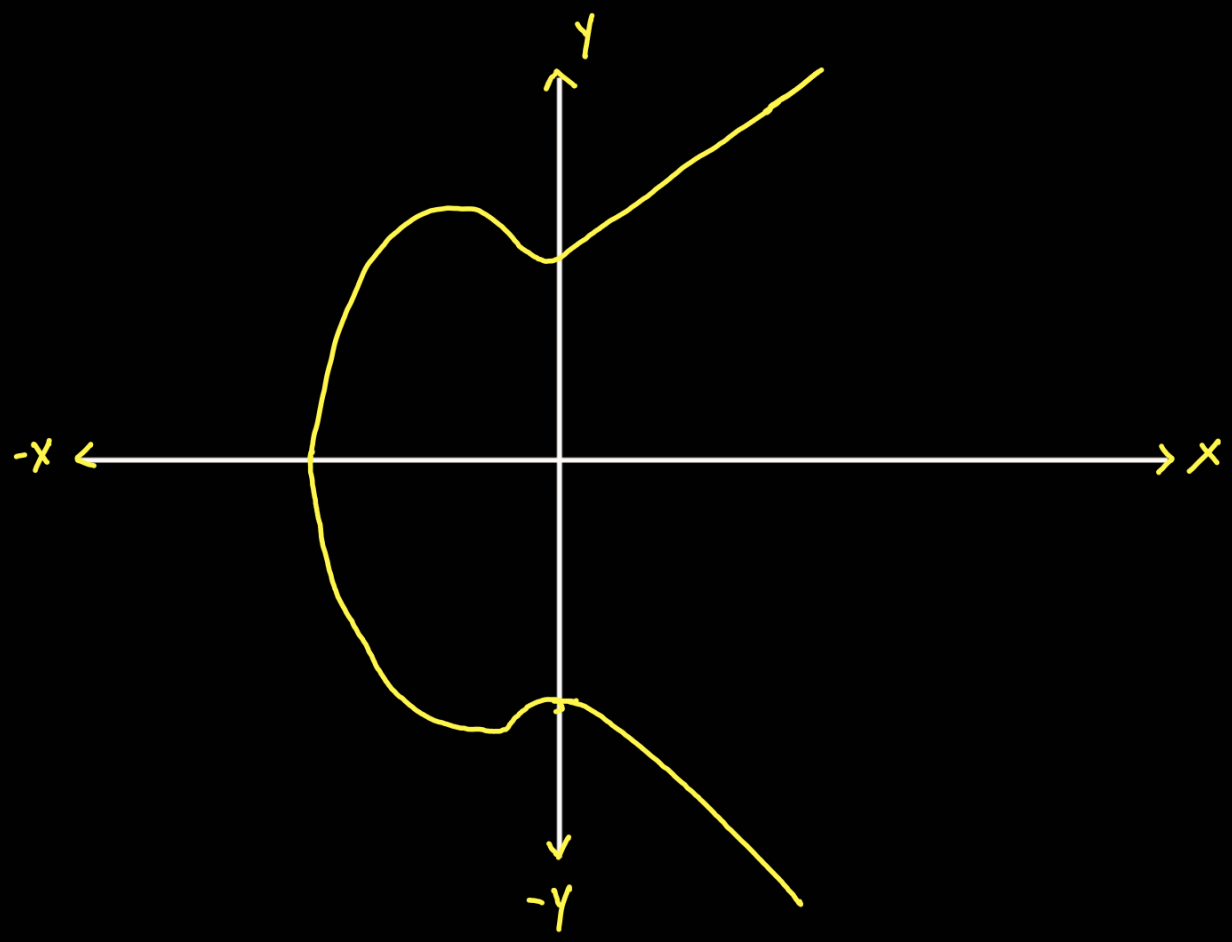
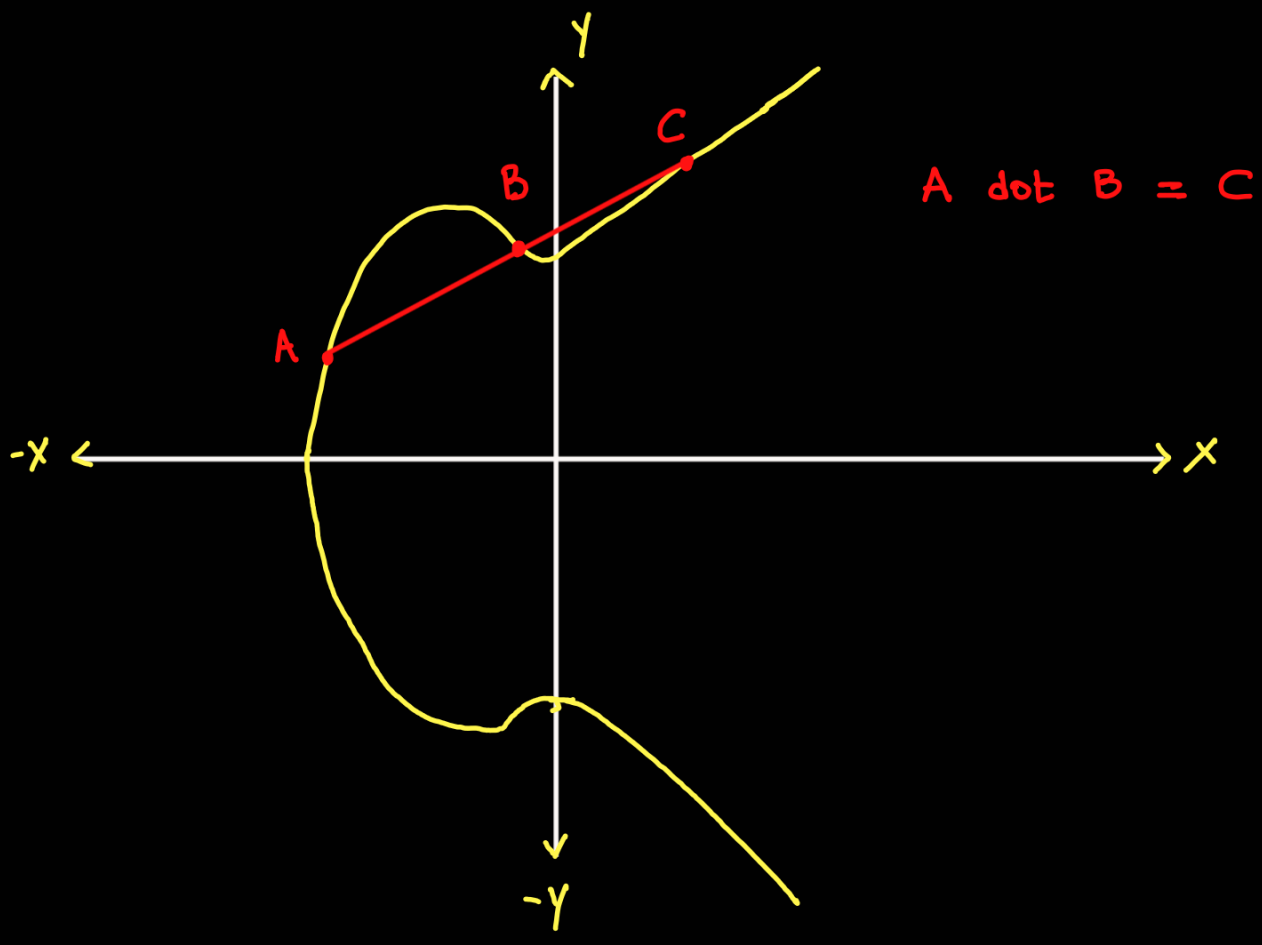
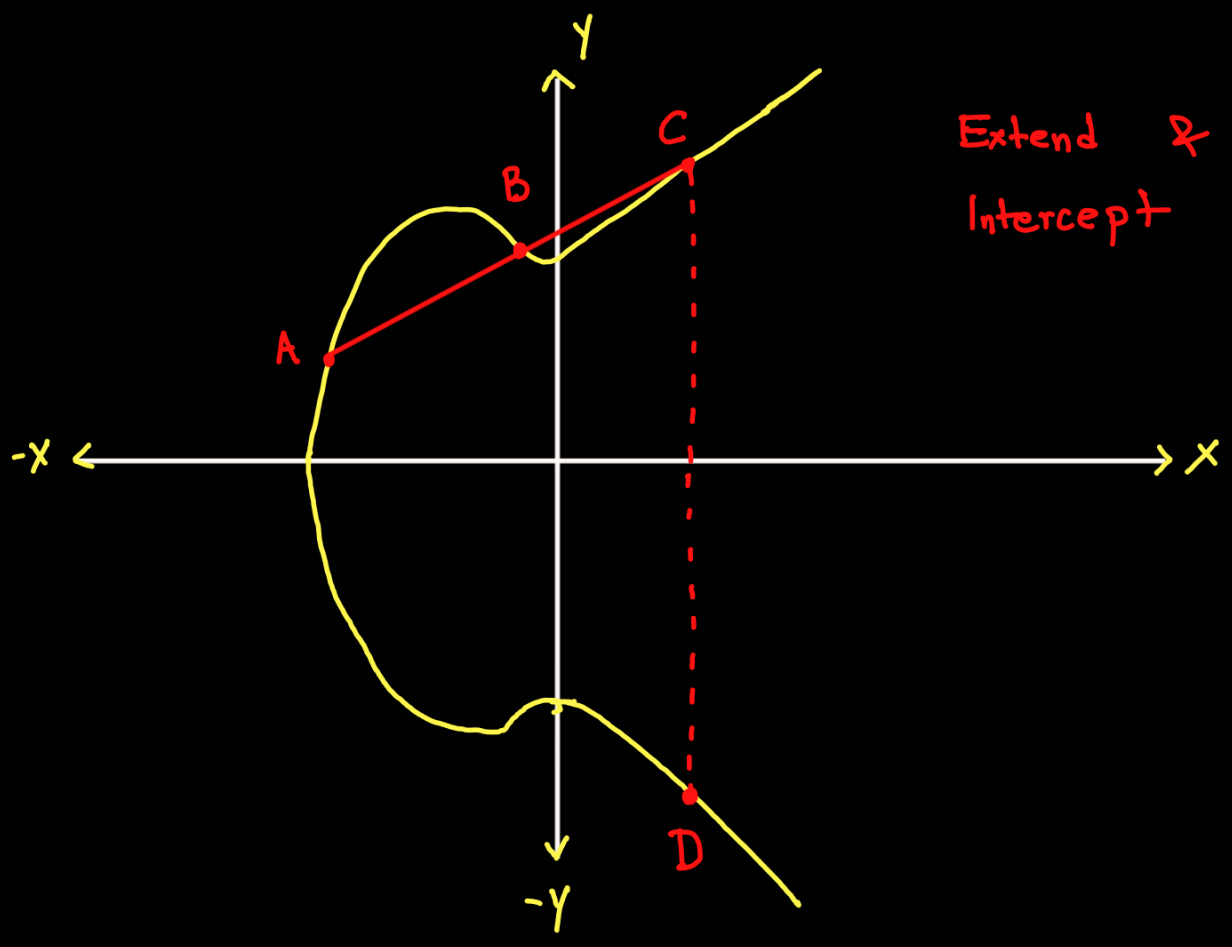
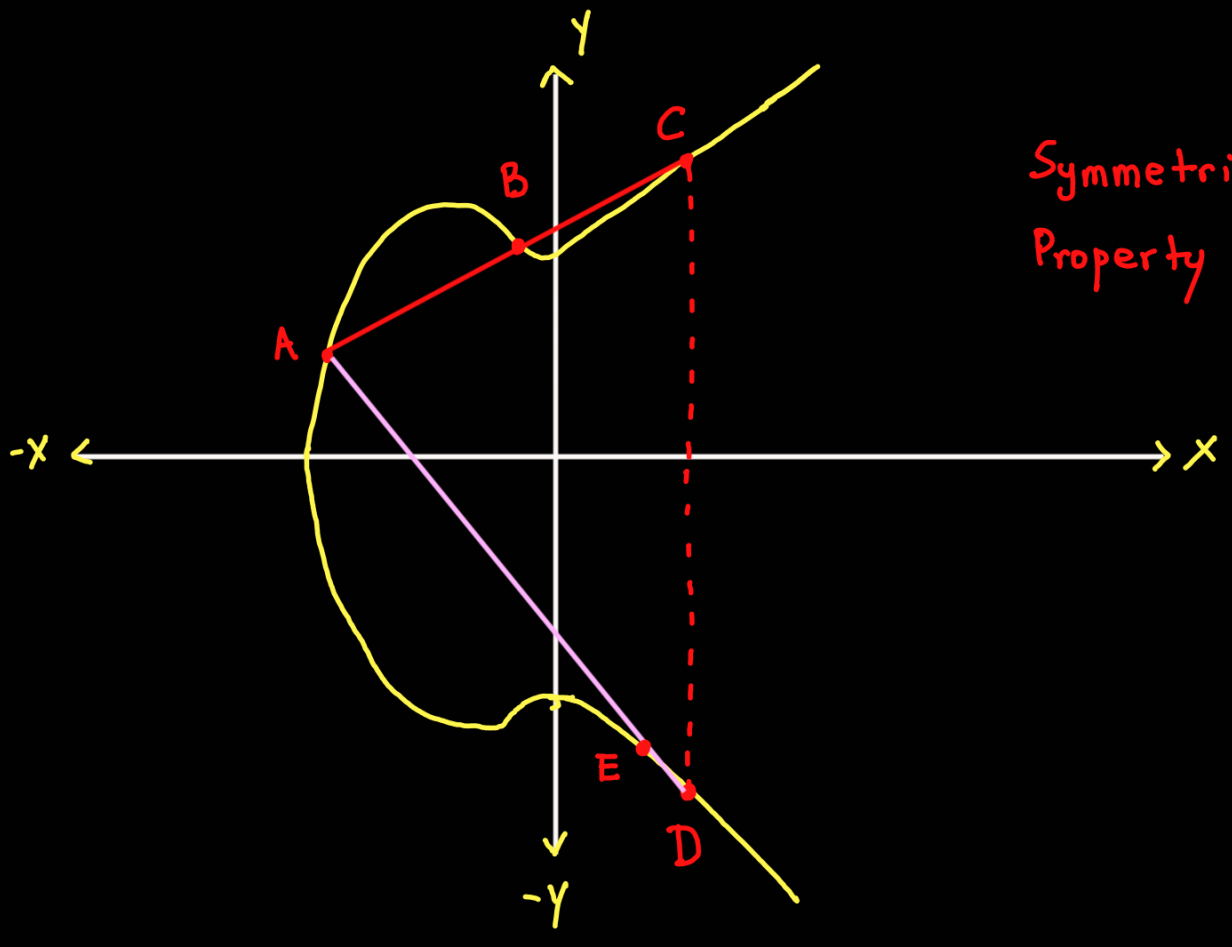

Y
-X
X
-Y

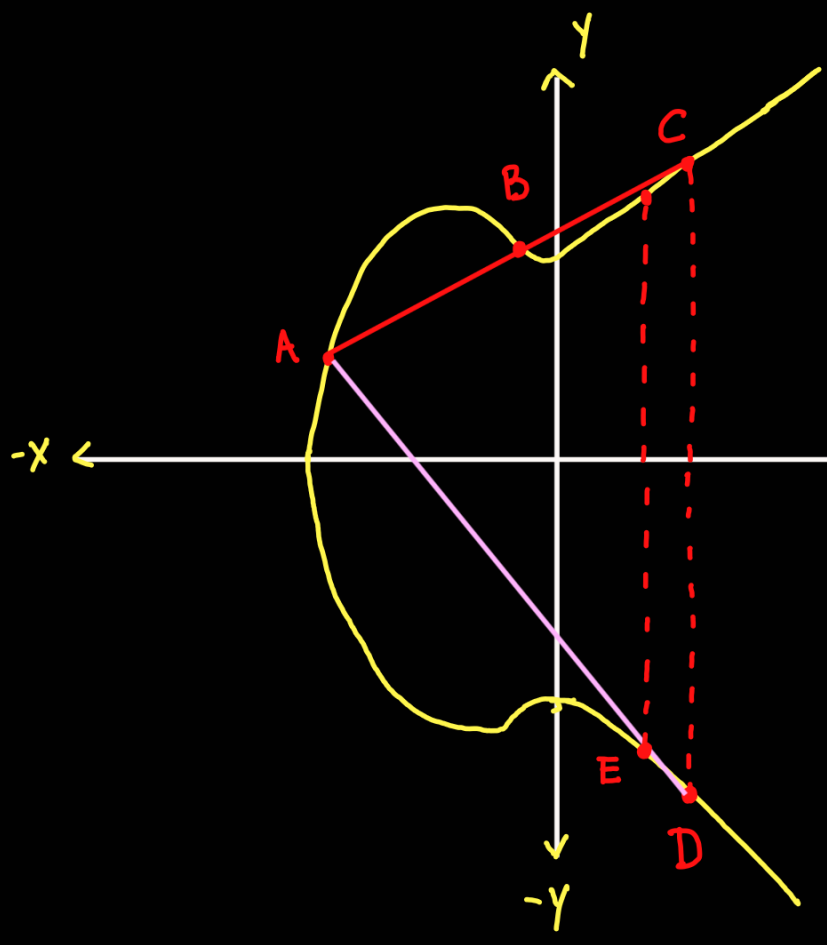

Y
C
B
A
-X
X
-Y
A dot B = C



Extend & Intercept



Symmetric Property



A dot A' → Z

↓

'n' no. of times

Trapdoor Function

A → B ✓

B → A X

ECC vs RSA

256 ≈ 3072

386 ≈ 7680

* We take a MAX value on the X-axis.
* This is your key size
* n is your private key (No. of times you "dot")
* x, y coordinates are the public key

Even if you have the value of A & Z with you, you won't be able to break into the implementation unless you have the private key component.

Why ?