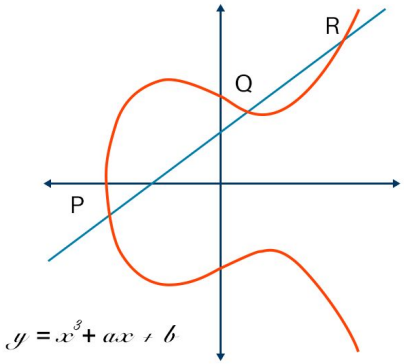
Elliptic Curve Cryptography

Python Presentation Night @ Virtual (PPN #85)



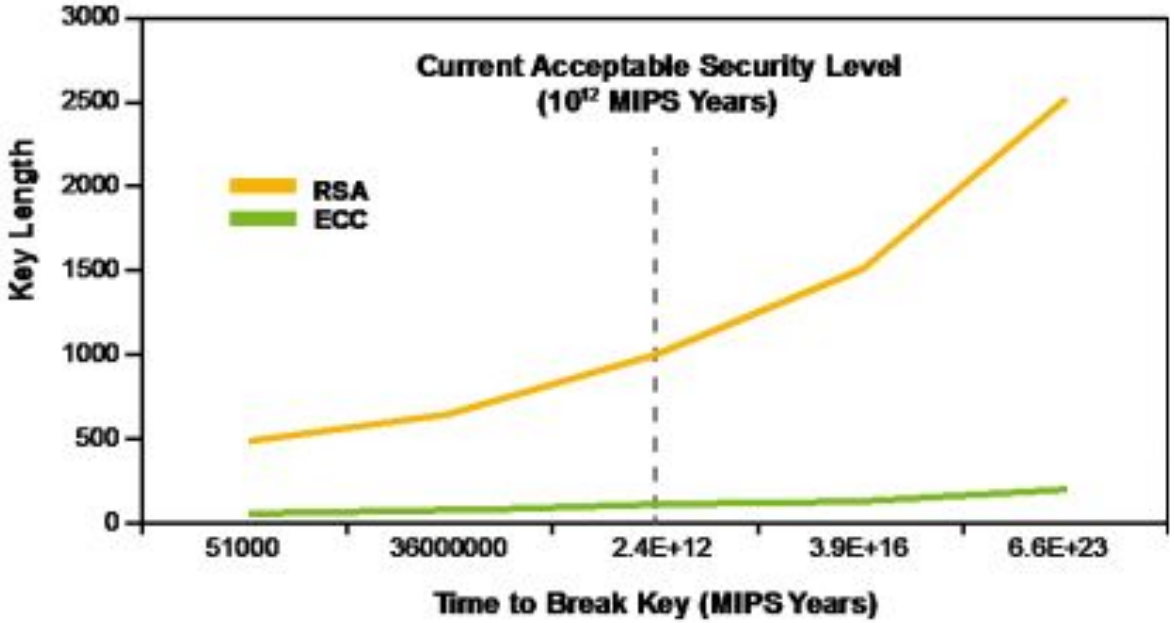
Sebastian Troncoso

What is Elliptic Curve Cryptography?

- ECC is a key-based technique for encrypting data. ECC focus on pairs of public and private keys for decryption and encryption of web traffic.
- ECC is an alternative technique to RSA.
- It is a powerful cryptography approach that required much smaller key sides in compare to RSA keys.

Security Comparison for Various Algorithm-key Size Combinations (Source: NSA) [7]

Security Bits	Symmetric Encryption Algorithm	Minimum Size (bits) of Public Keys	
		RSA	ECC
80	Skipjack	1024	160
112	3DES	2048	224
128	AES-128	3072	256
192	AES-192	7680	384
256	AES-256	15360	512



Security Comparison for Various Algorithm-key Size Combinations (Source: NSA) [7]

Security Bits	Symmetric Encryption Algorithm	Minimum Size (bits) of Public Keys	
		RSA	ECC
80	Skipjack	1024	160
112	3DES	2048	224
128	AES-128	3072	256
192	AES-192	7680	384
256	AES-256	15360	512

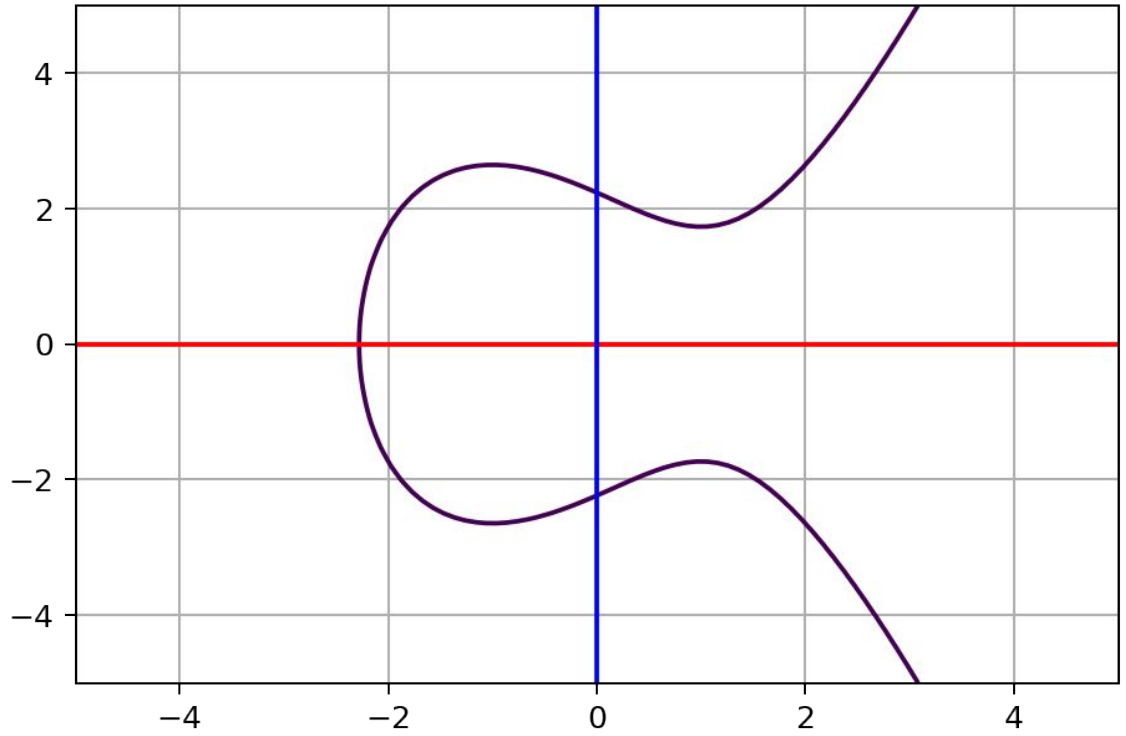
Who uses Elliptic Curve Cryptography?

- Google
- NSA
- Bitcoins
- Wikipedia
- Facebook

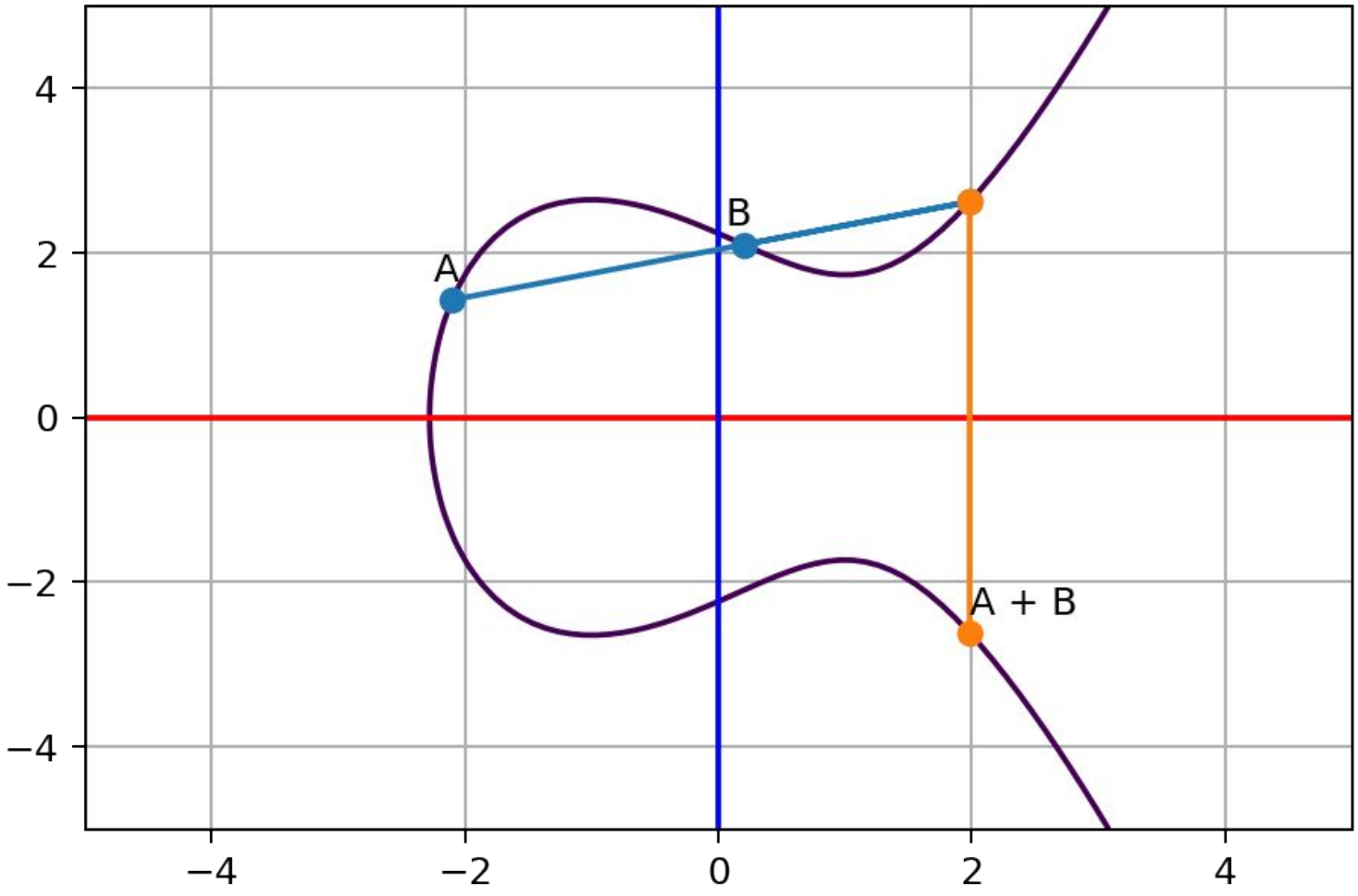
		Parameters:			ECDLP security:				ECC security:			
Curve	Safe?	field	equation	base	rho	transfer	disc	rigid	ladder	twist	complete	ind
Anomalous	False	True✓	True✓	True✓	True✓	False	False	True✓	False	False	False	False
M-221	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
E-222	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
NIST P-224	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	False	False	False
Curve1174	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
Curve25519	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
BN(2,254)	False	True✓	True✓	True✓	True✓	False	False	True✓	False	False	False	False
brainpoolP256t1	False	True✓	True✓	True✓	True✓	True✓	True✓	True✓	False	False	False	False
ANSSI FRP256v1	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	False	False	False
NIST P-256	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	True✓	False	False
secp256k1	False	True✓	True✓	True✓	True✓	True✓	False	True✓	False	True✓	False	False
E-382	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
M-383	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
Curve383187	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
brainpoolP384t1	False	True✓	True✓	True✓	True✓	True✓	True✓	True✓	False	True✓	False	False
NIST P-384	False	True✓	True✓	True✓	True✓	True✓	True✓	False	False	True✓	False	False
Curve41417	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
Ed448-Goldilocks	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
M-511	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓
E-521	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓	True✓

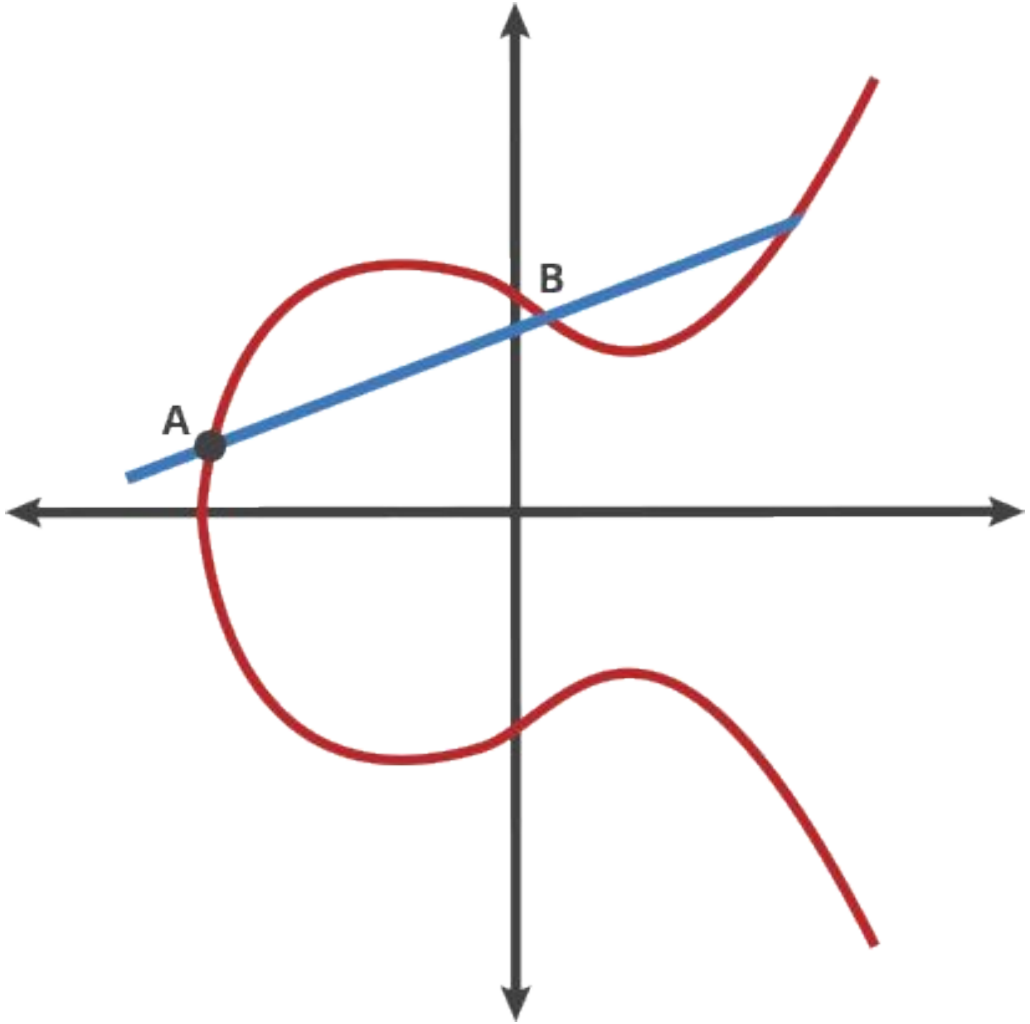
Elliptic curves are the solution of the equation

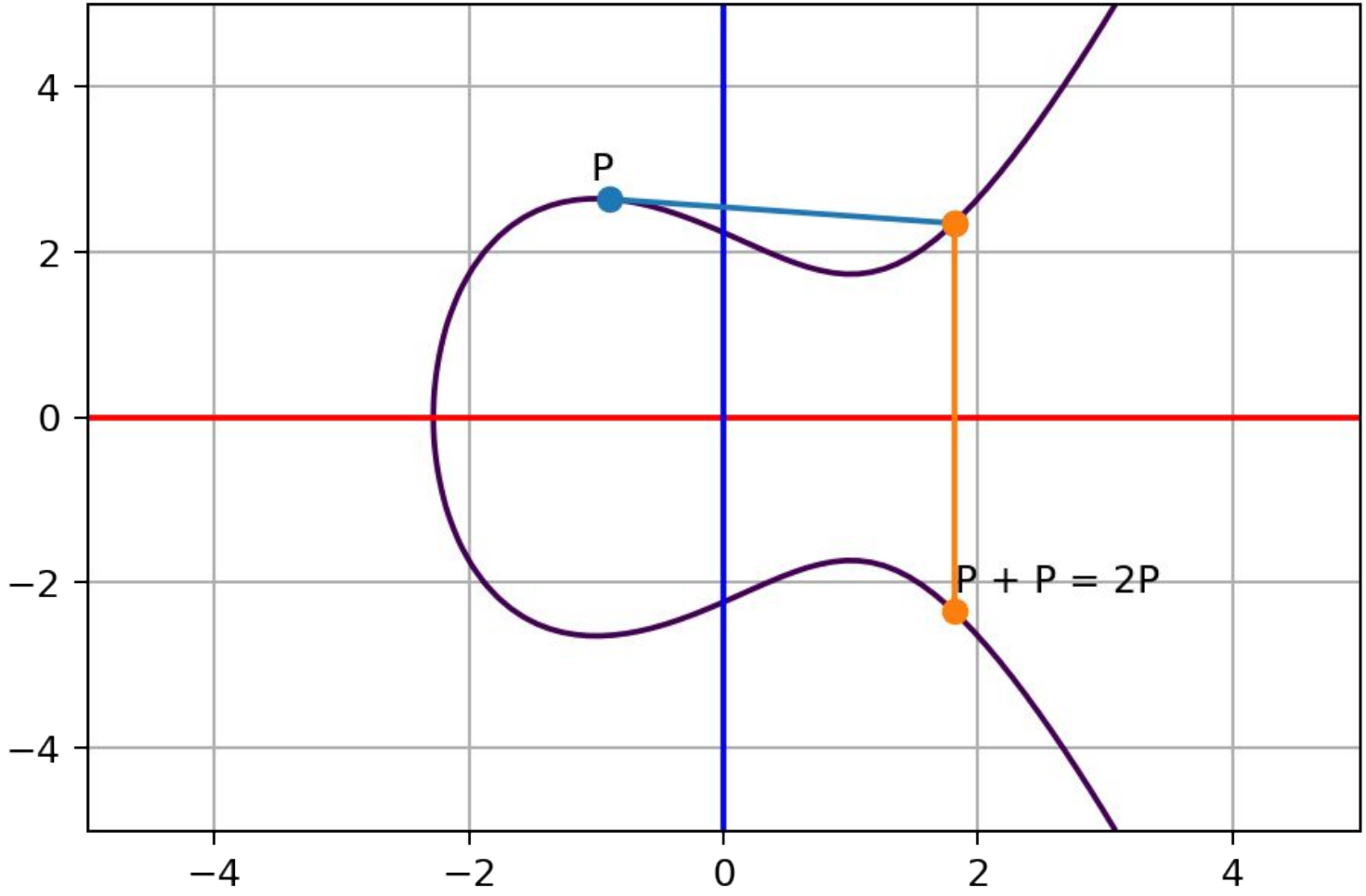
$$y^2 = x^3 + ax + b$$

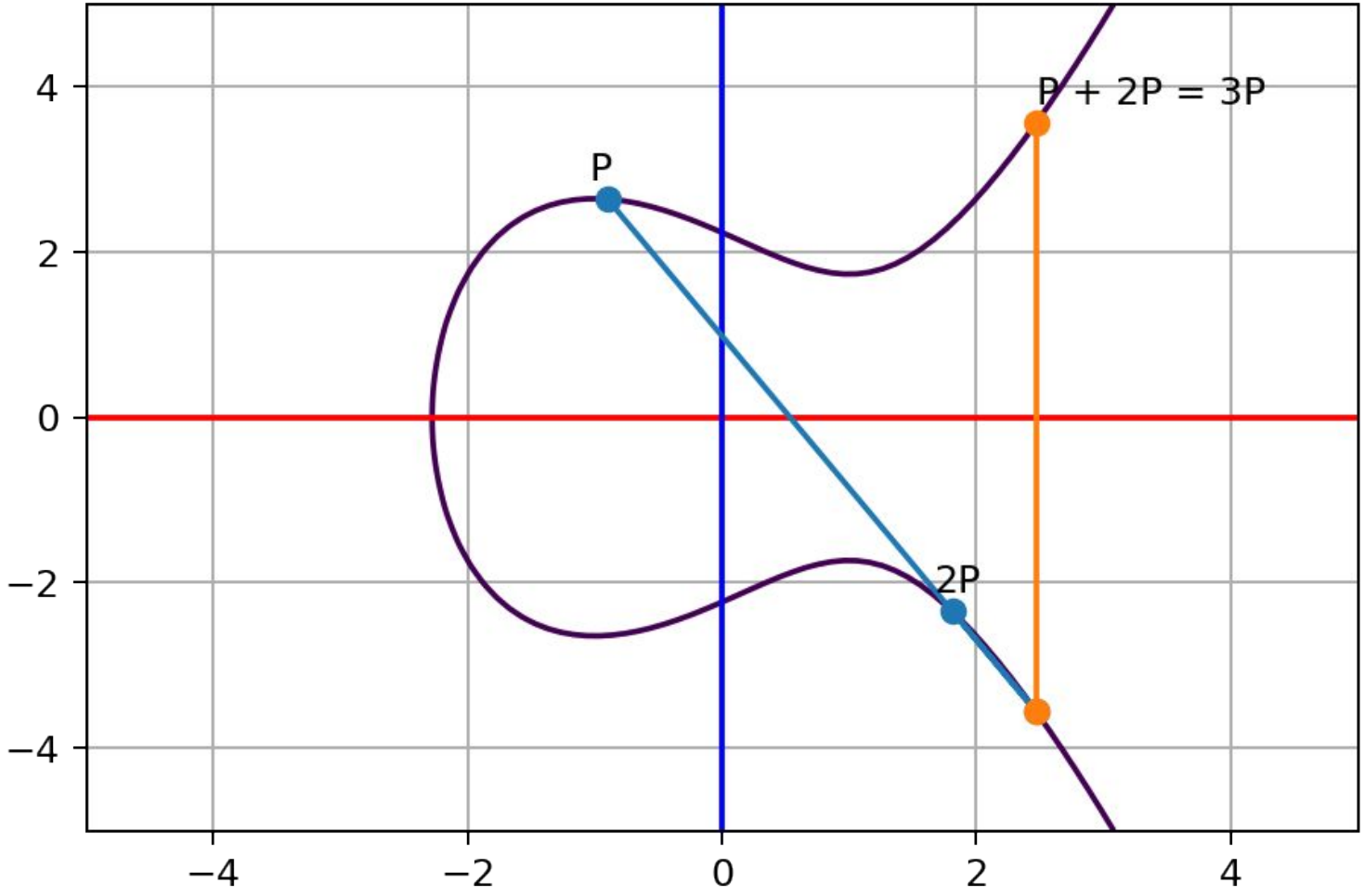


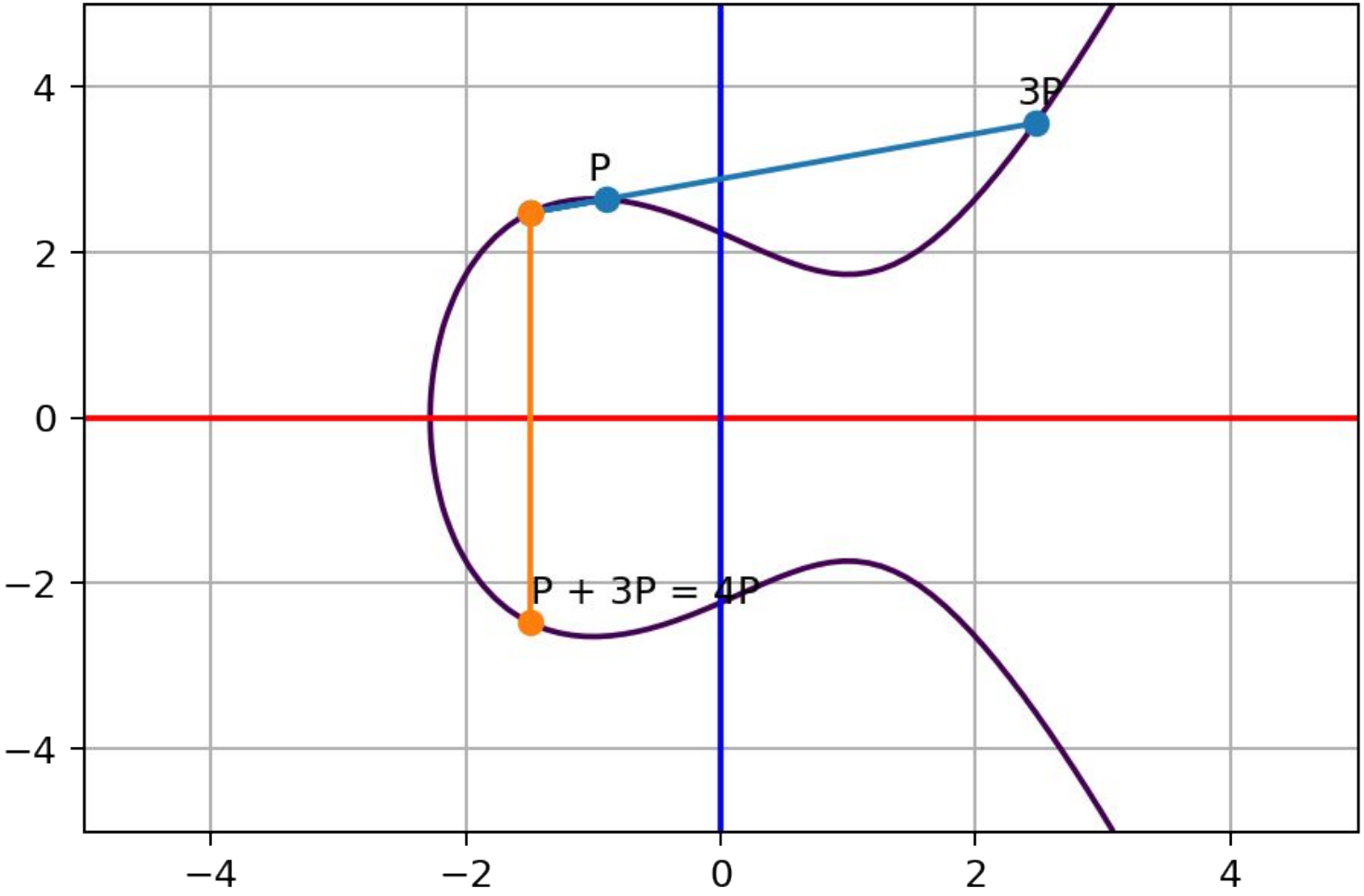
$$y^2 = x^3 - 3x + 5$$

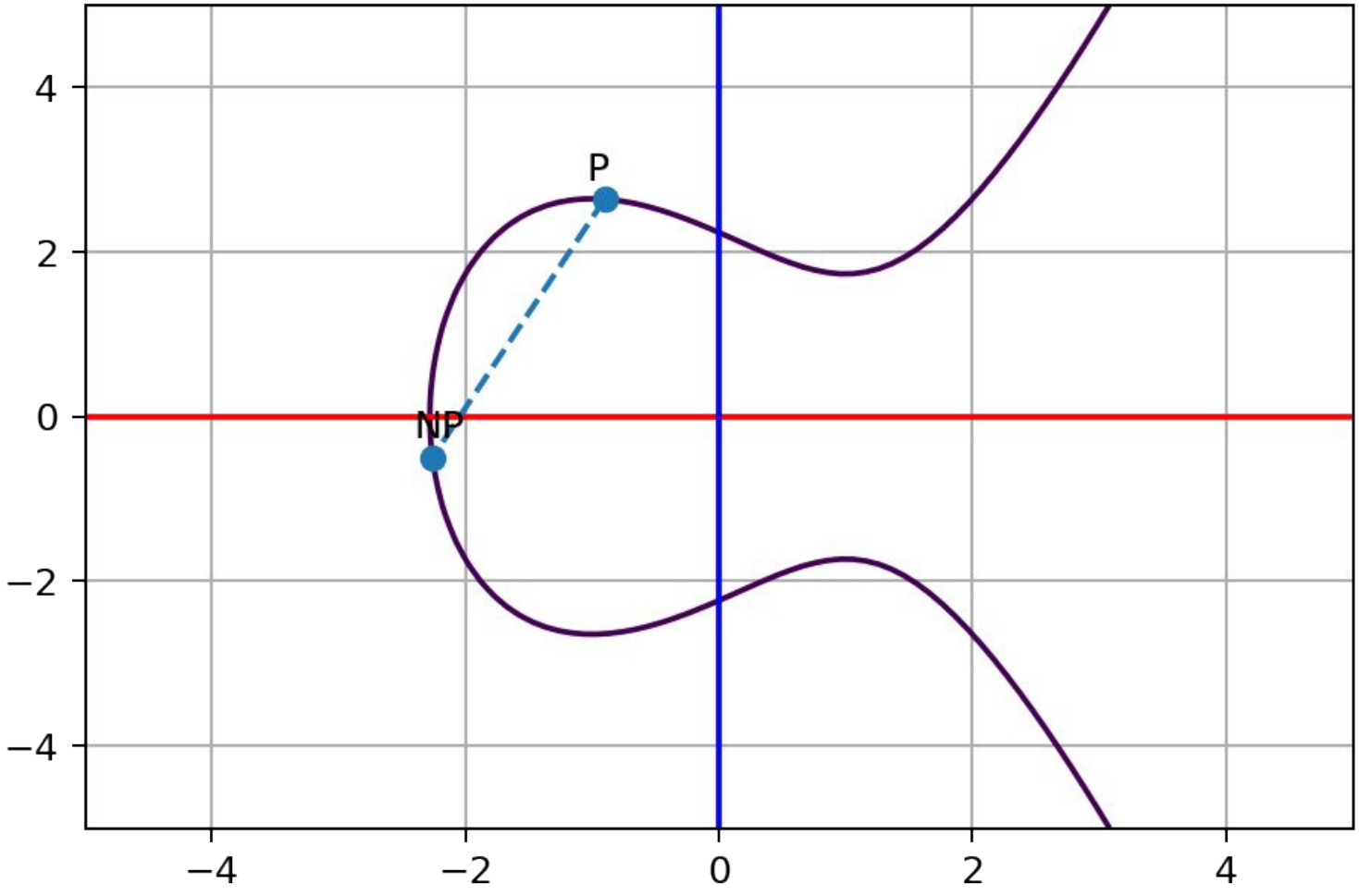

4
2
0
−2
−4
−4
−2
0
2
4
A
B
A + B


A
B


P
P + P = 2P
4
2
0
−2
−4
−4
−2
0
2
4


P + 2P = 3P
P
2P
4
2
0
−2
−4
−4
−2
0
2
4


3P
P
P + 3P = 4P
4
2
0
−2
−4
−4
−2
0
2
4


P
NP
4
2
0
−2
−4
−4
−2
0
2
4

- Given an integer ***n*** then it is **“easy”** to find ***nP***

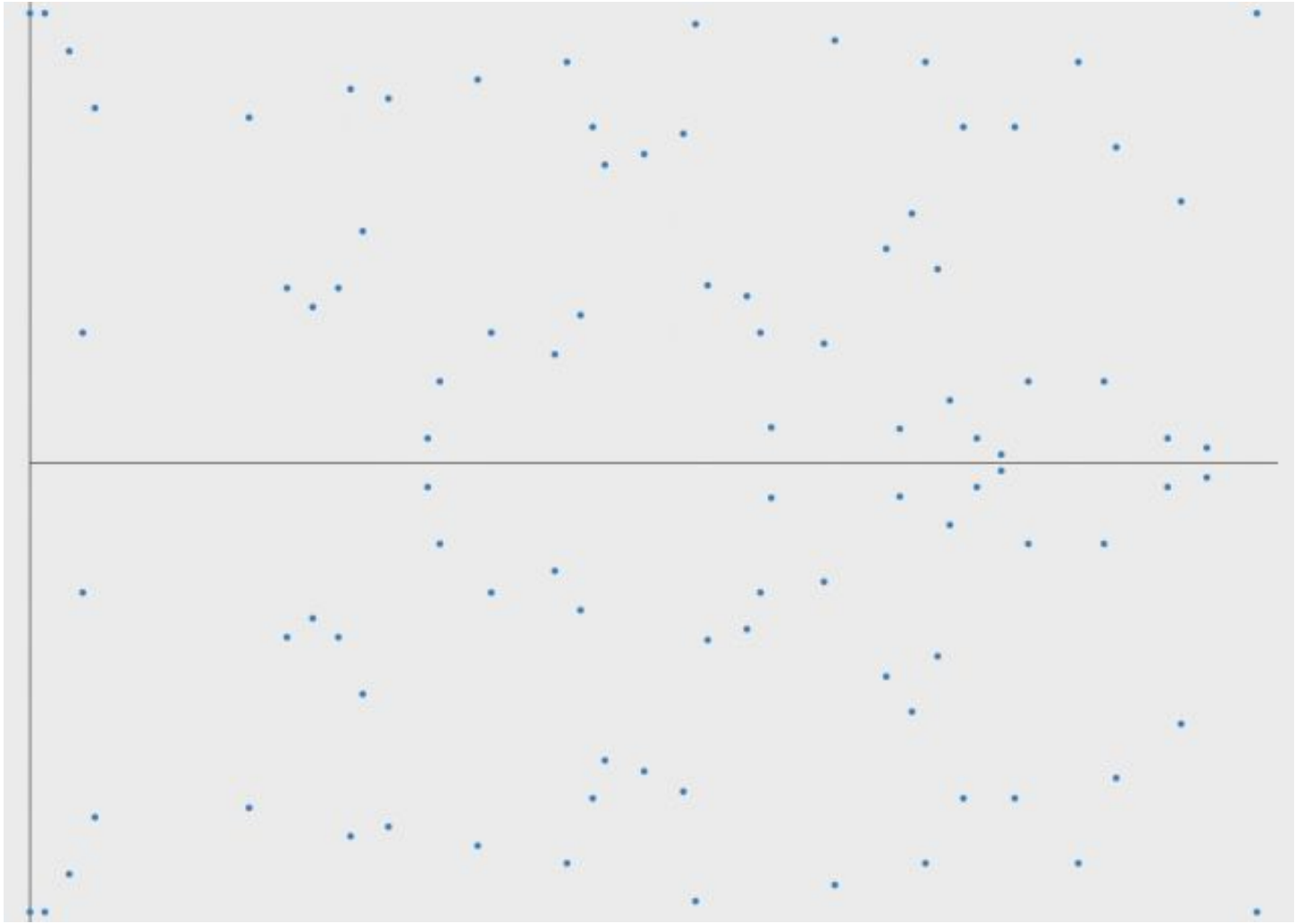
- Given ***nP*** then it is **extremely hard** to find ***n***

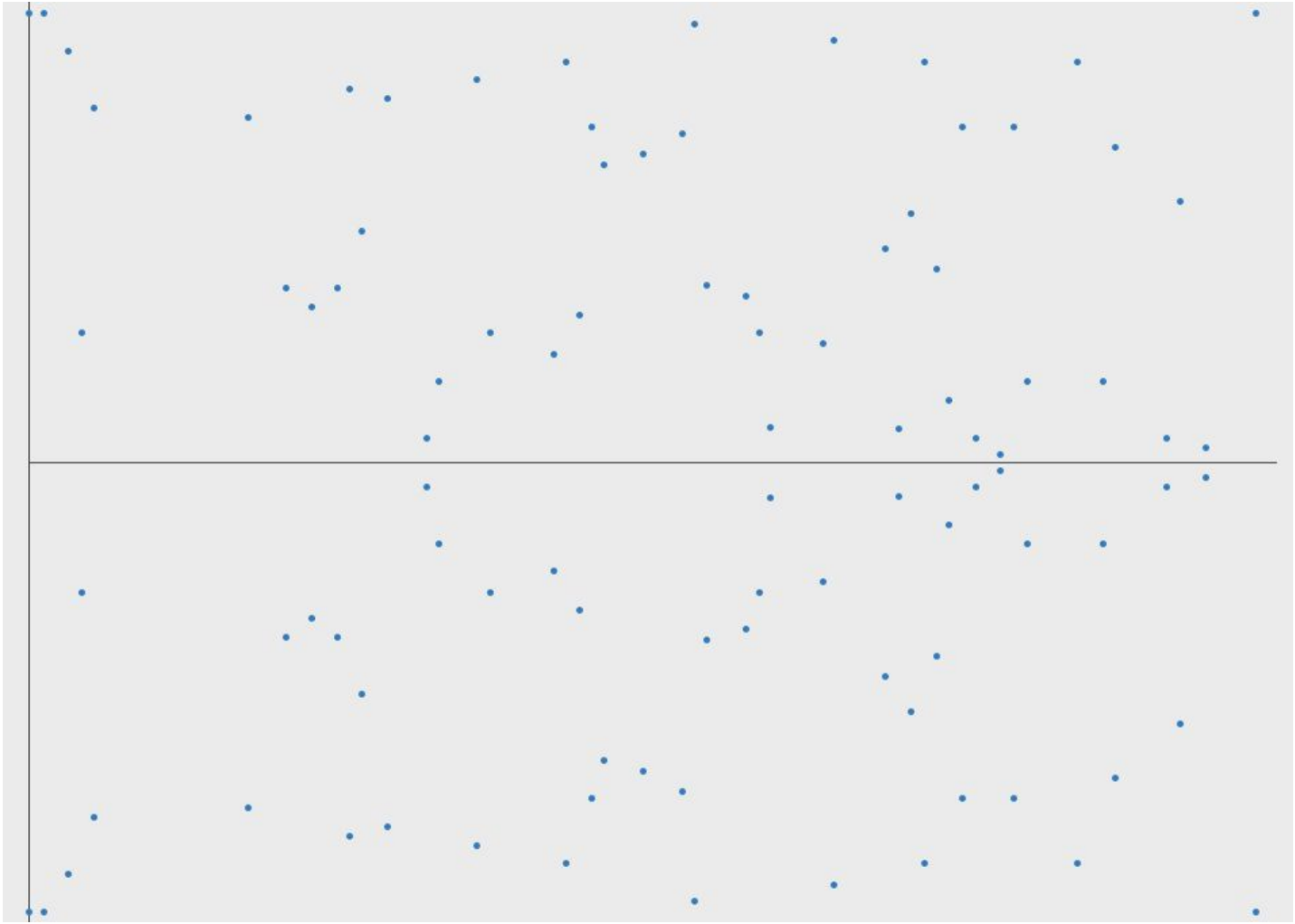
  Elliptic Curve Discrete Logarithm Problem

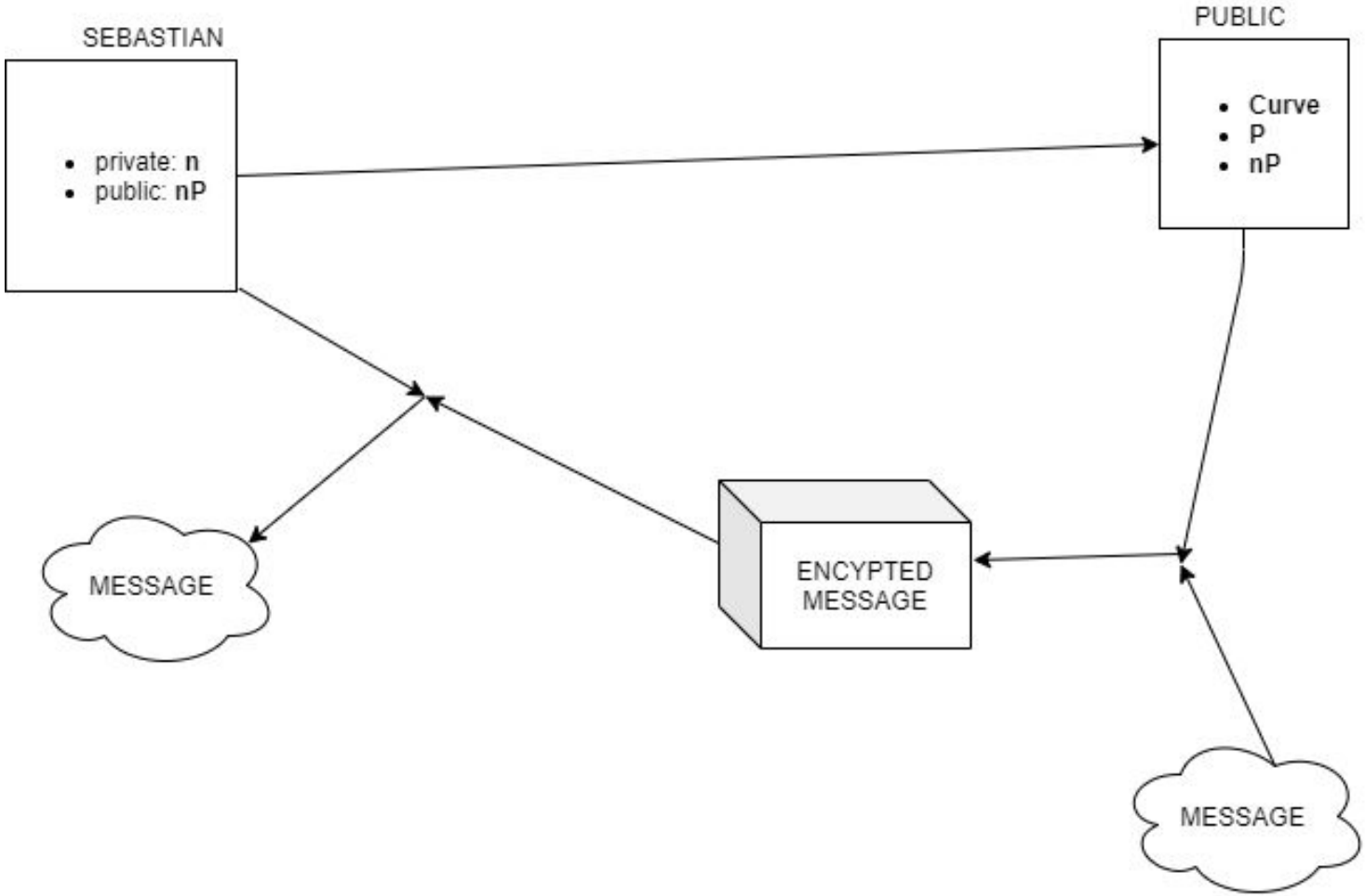
- Given a elliptic curve and a point P.

Pick a random an integer n

- **n** is the PRIVATE KEY
- **nP** is the PUBLIC KEY






SEBASTIAN
private: n
public: nP
PUBLIC
Curve
P
nP
MESSAGE
ENCYPTED MESSAGE
MESSAGE