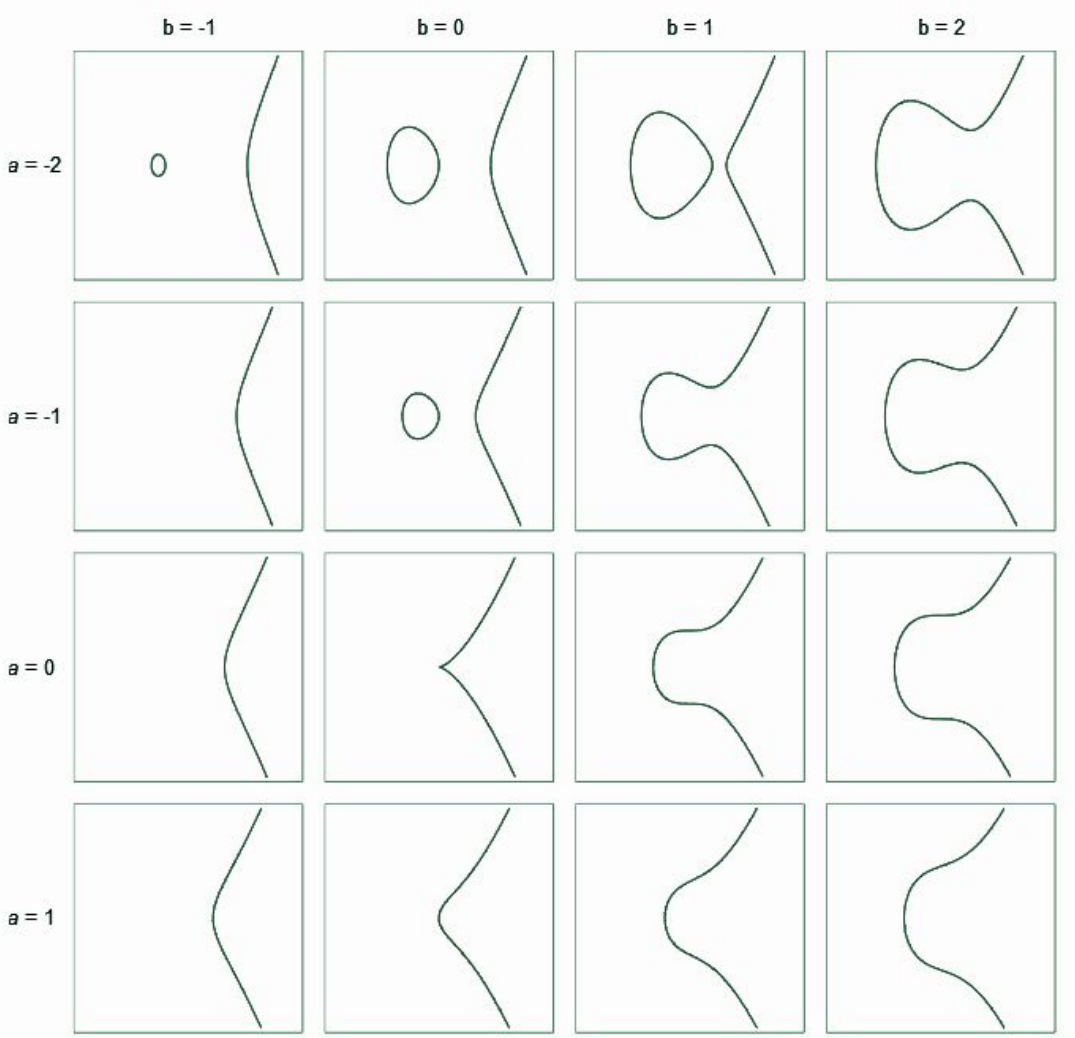
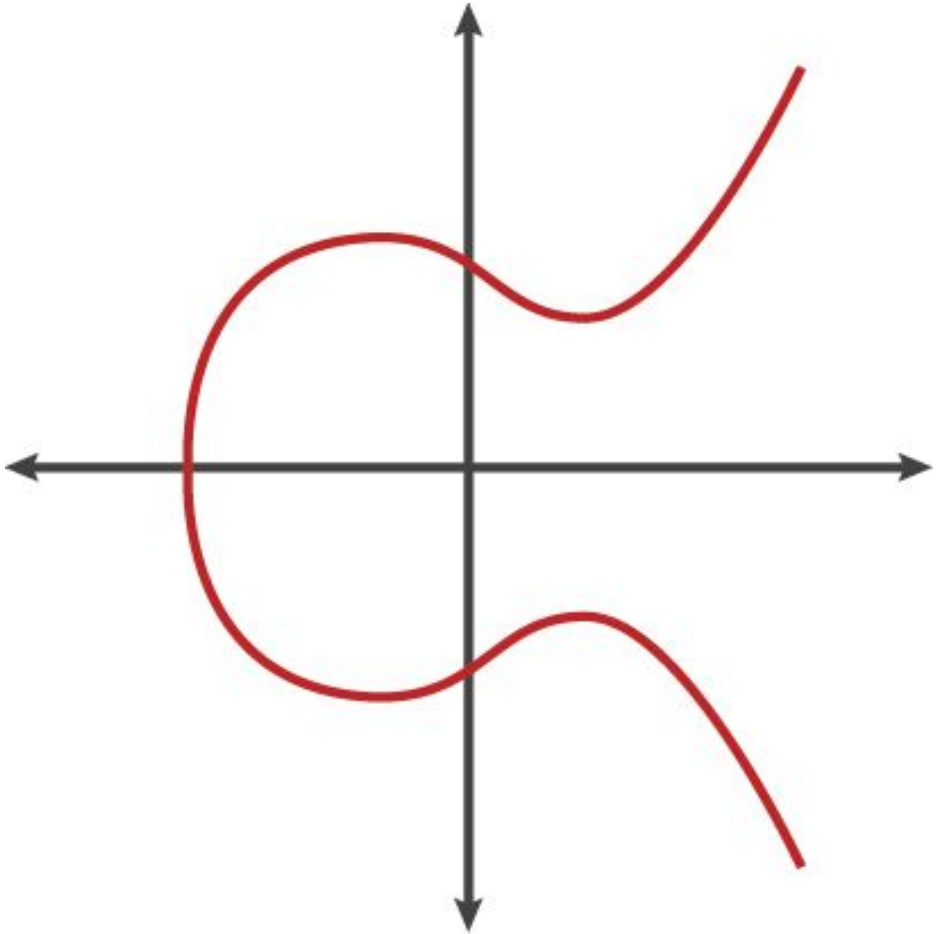
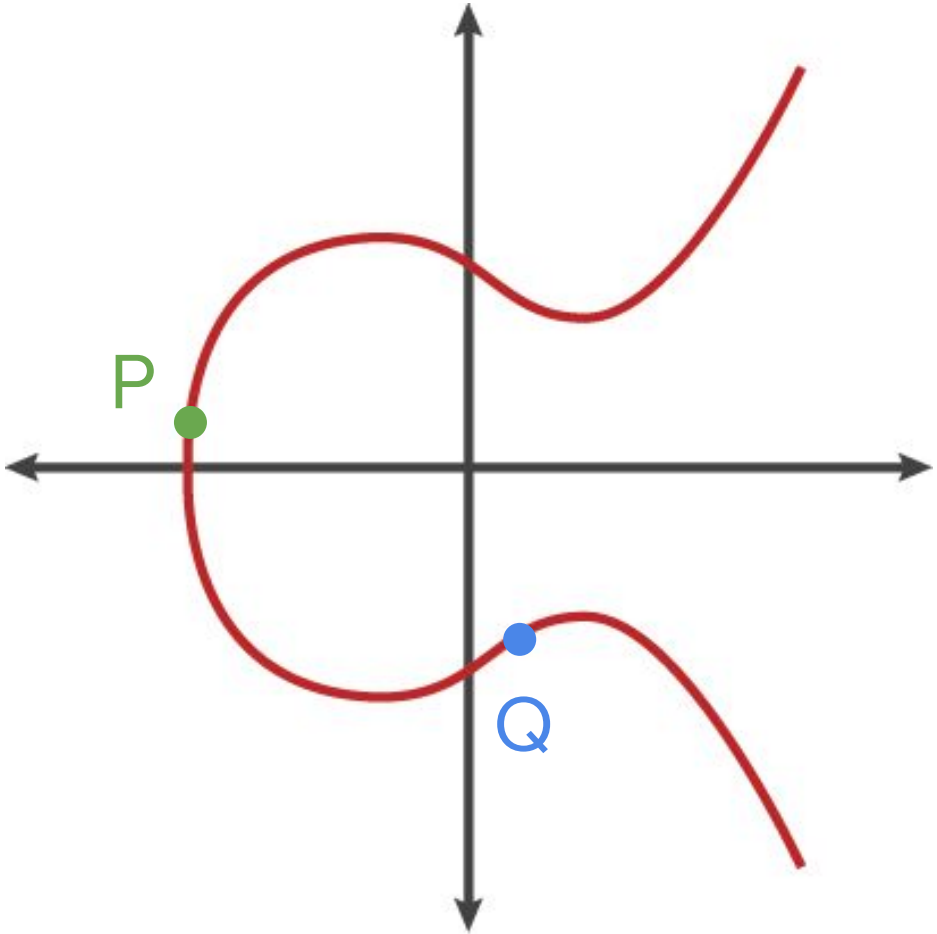
Elliptic curves and cryptography

Johanna Loyer

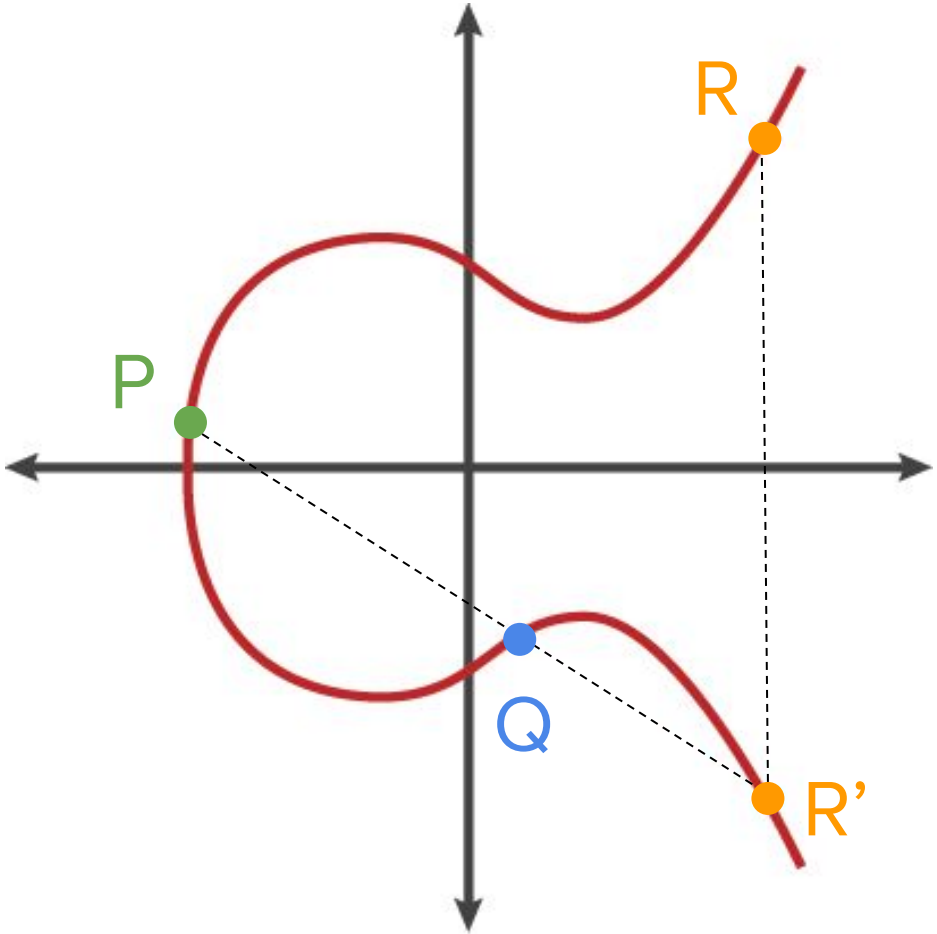
$$y^2 = x^3 + ax + b$$


b = -1
b = 0
b = 1
b = 2
a = -2
a = -1
a = 0
a = 1

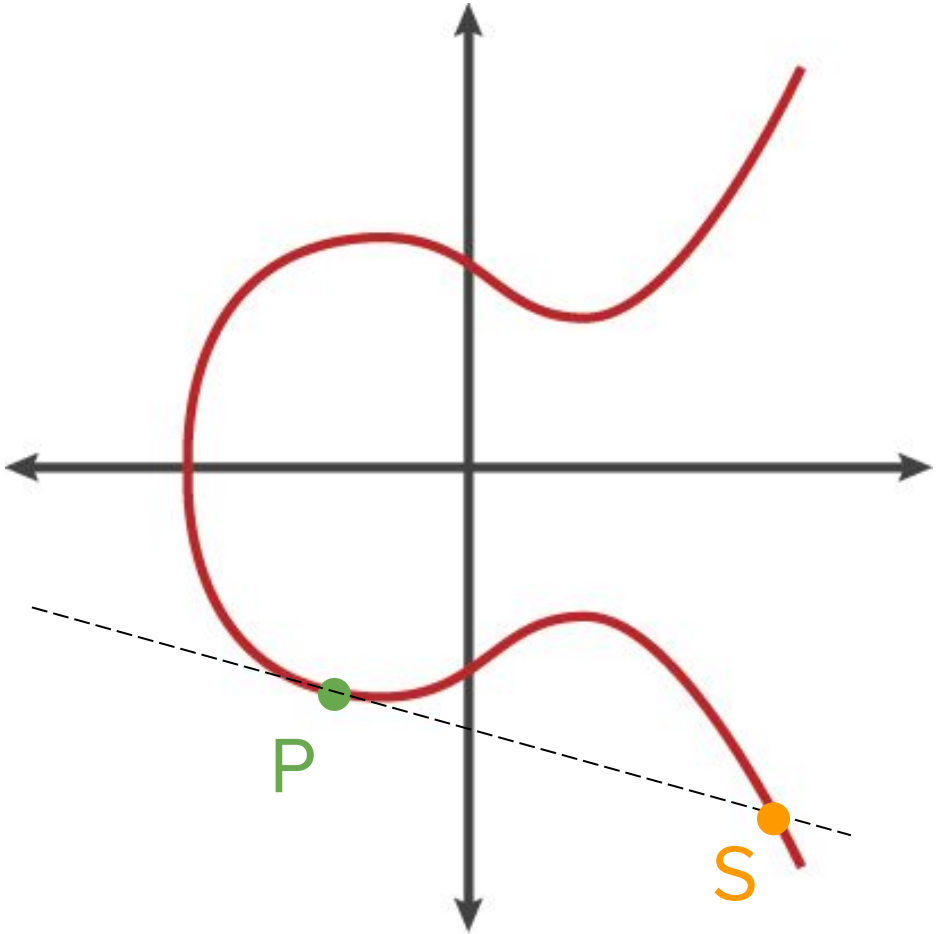




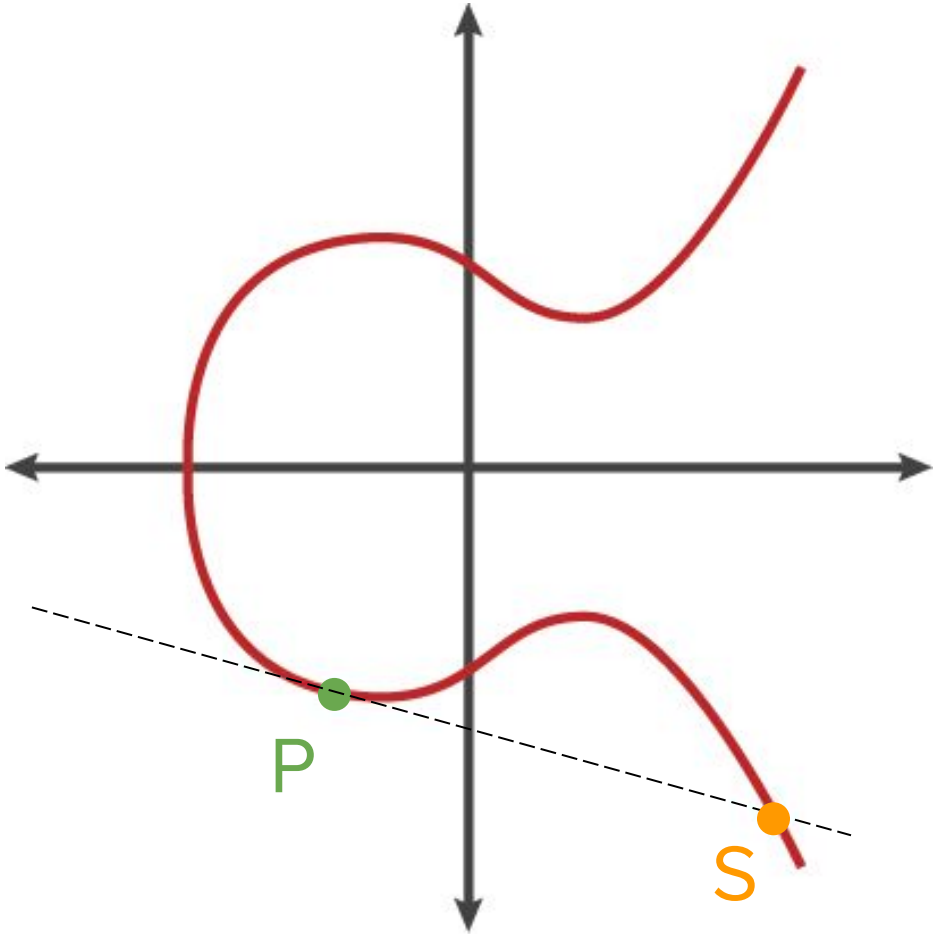
P + Q



$$P + Q = R$$

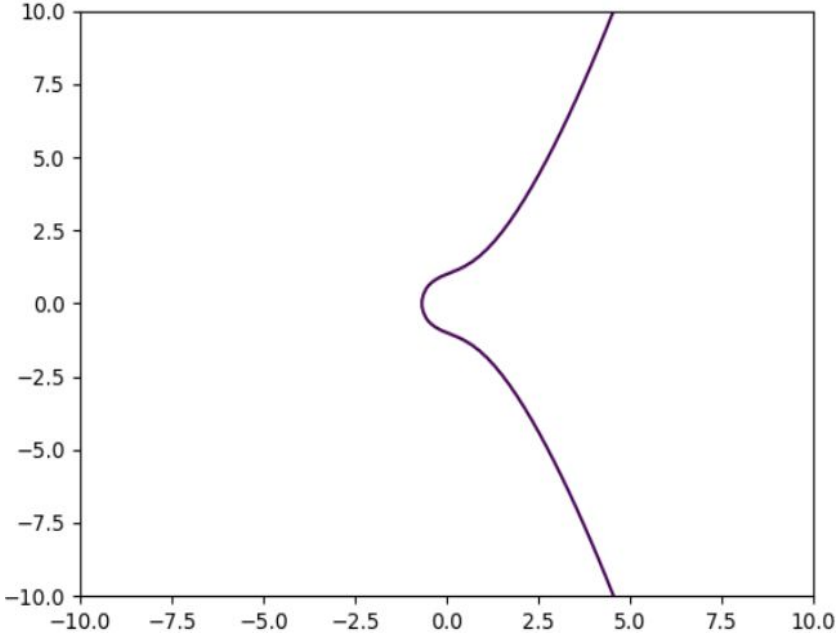


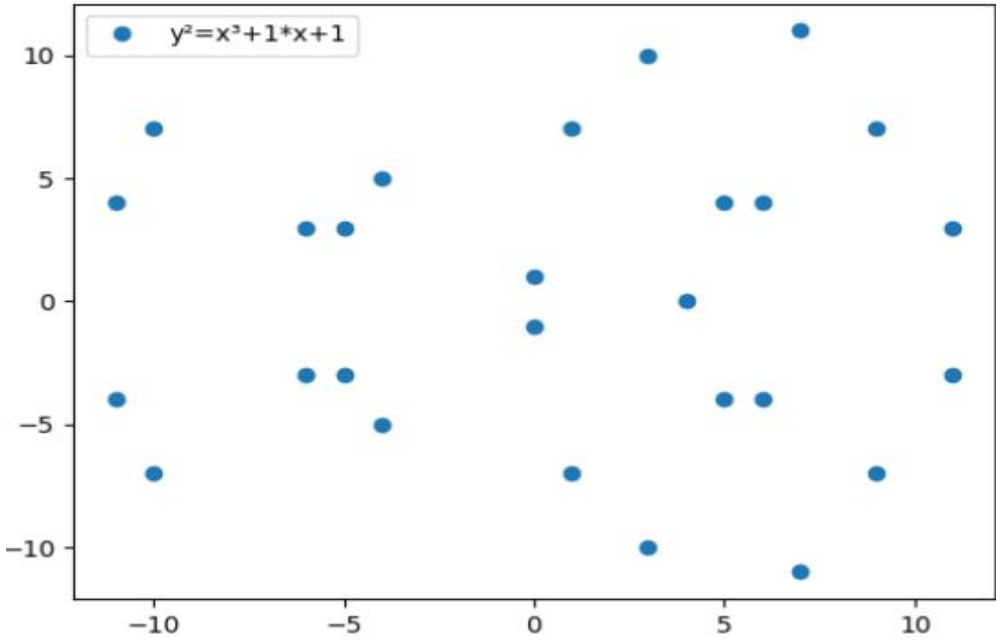
$2.P = S$

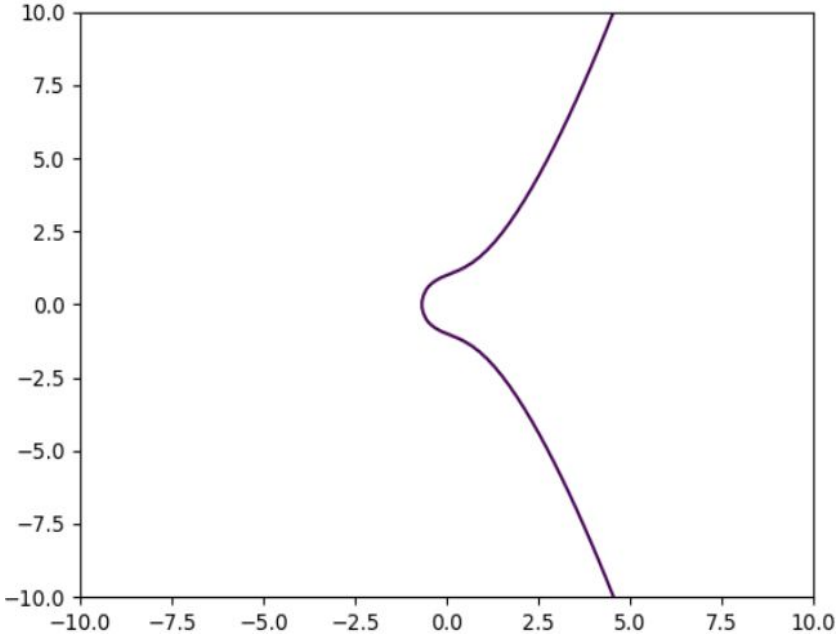


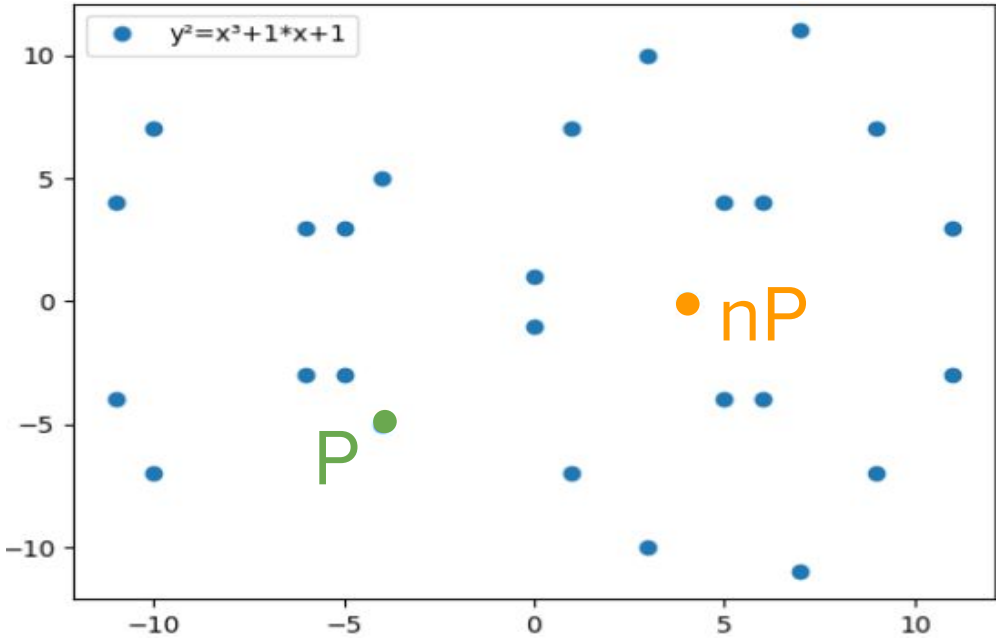
$$2.P = S$$

$$nP = \underbrace{P + P + \ldots + P}_{n \text{ times}}$$

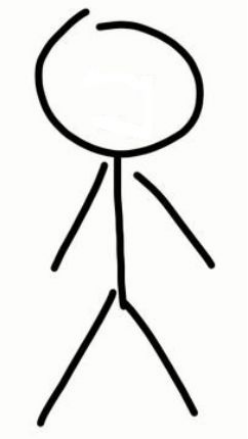

10.0
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−10.0
−10.0
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5
10.0


y²=x³+1*x+1
10
5
0
−5
−10
−10
−5
0
5
10


10.0
7.5
5.0
2.5
0.0
−2.5
−5.0
−7.5
−10.0
−10.0
−7.5
−5.0
−2.5
0.0
2.5
5.0
7.5
10.0

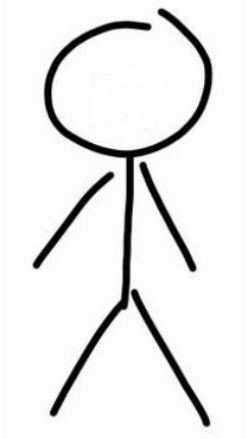

y²=x³+1*x+1
10
5
0
−5
−10
−10
−5
0
5
10
nP
P

n = ?



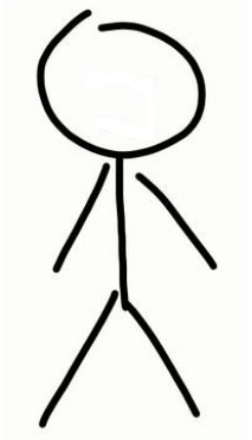
Alice

a, P

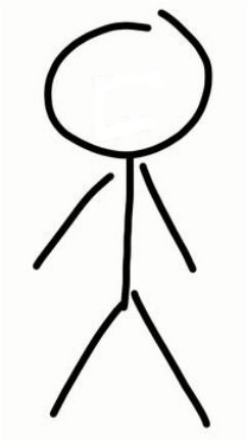


Bob

b



P

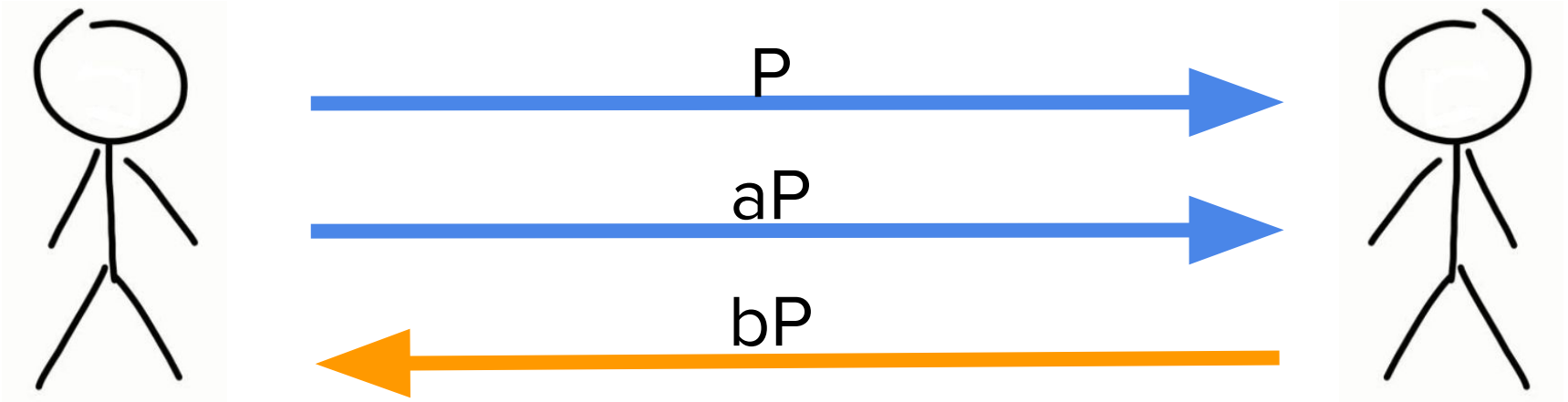


Alice

a, P, aP

Bob

b, P, bP



Alice

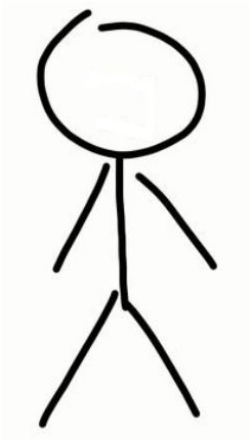
a, P, aP

bP

Bob

b, P, bP

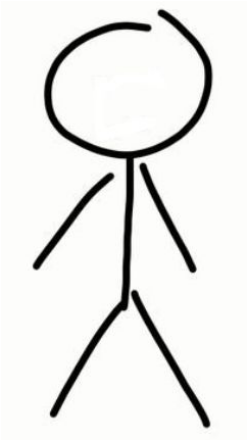
aP



P

aP

bP



Alice

a, P, aP

bP

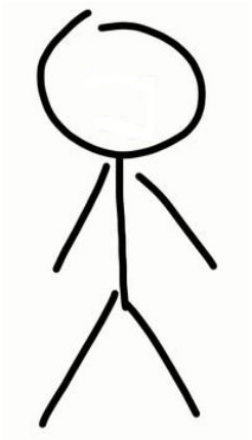
a.bP = K

Bob

b, P, bP

aP

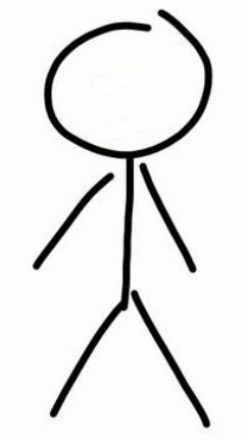
b.aP = K



P

aP

bP



Alice

a, P, aP

bP

a.bP = K

Eve

P, aP, bP

K = ???

Bob

b, P, bP

aP

b.aP = K