

Elliptic Curves and Cryptography

USU Student Research Symposium April 2017
Shantel Spatig



The Need for Security Increases..

Cryptography

practice and study of techniques for secure communication

RSA

Most popular and understood cryptosystem



How does it work?

Step

1

2 Prime numbers 5, 7

Step

2

Multiply

$$5(7) = 35 \xleftarrow{\text{Maximum}}$$

HI

8

9

Step

3

Key

3

Step

4

Multiply

$$8(8)(8) = 512$$

2229

STEP

5

Divide

$$512 / 35 =$$

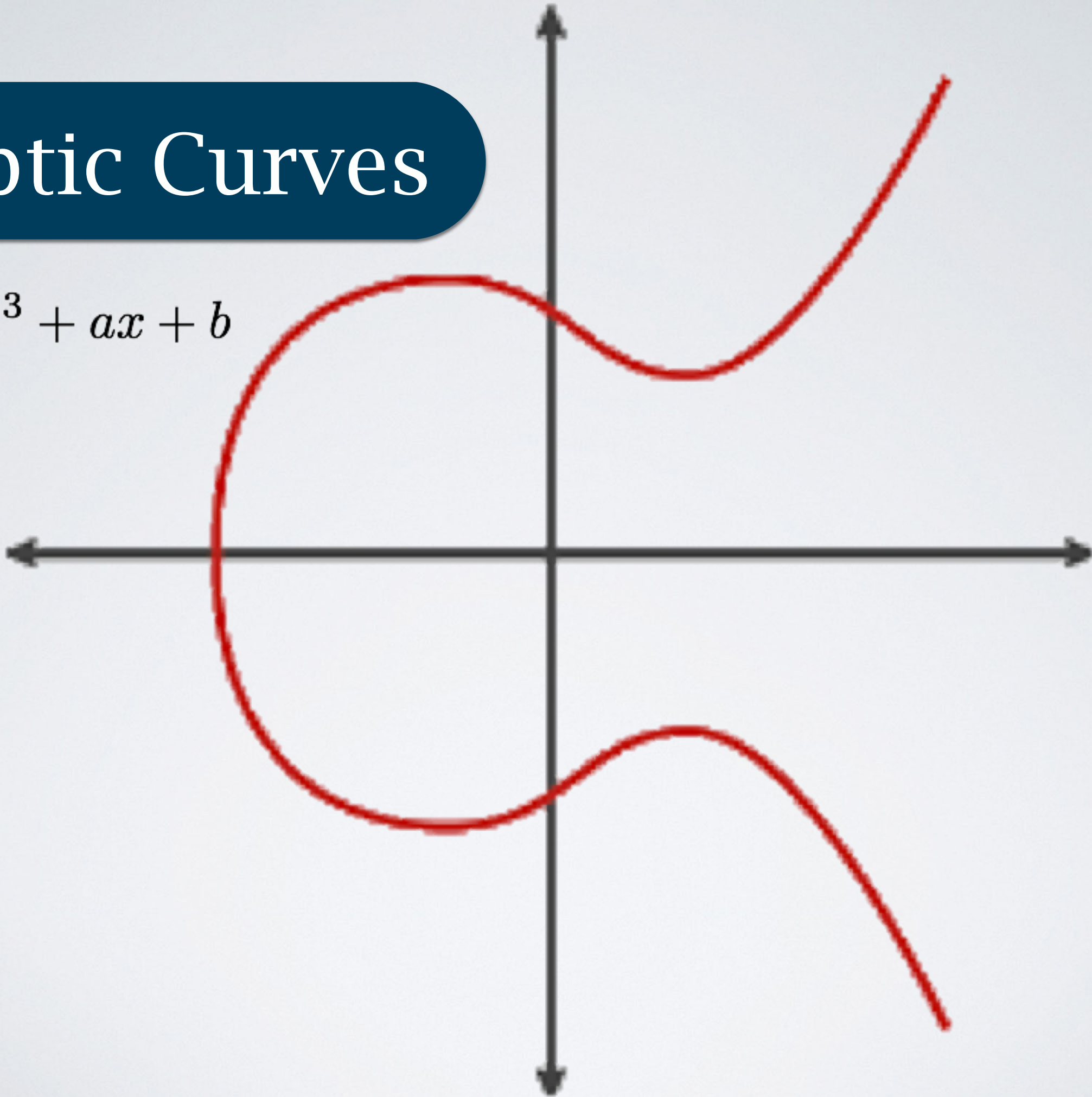
14 Remainder 22

VC

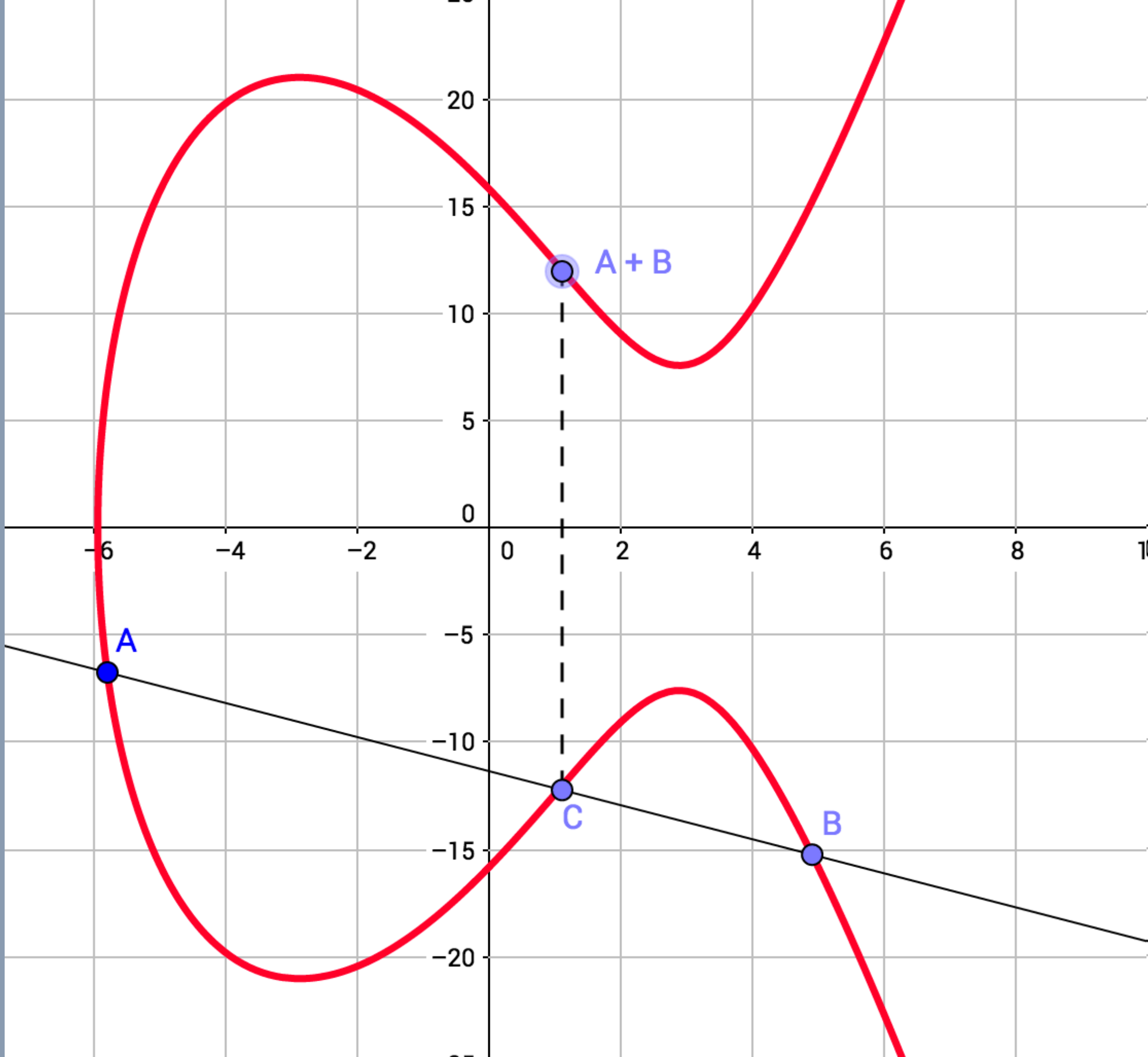
Is a new system really needed?

Elliptic Curves

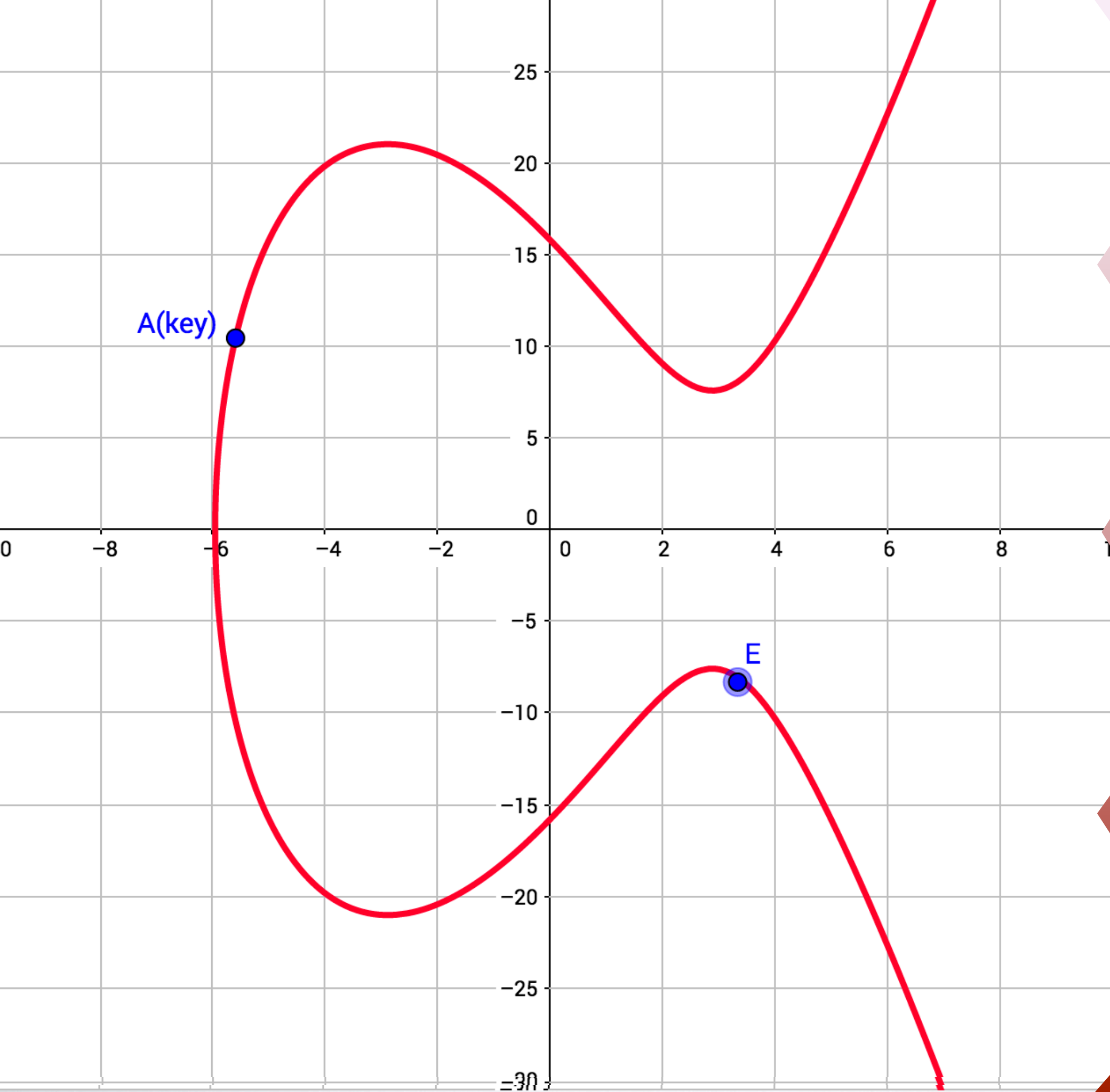
$$y^2 = x^3 + ax + b$$



ADDING POINTS



ELLIPTIC CURVE ENCRYPTION



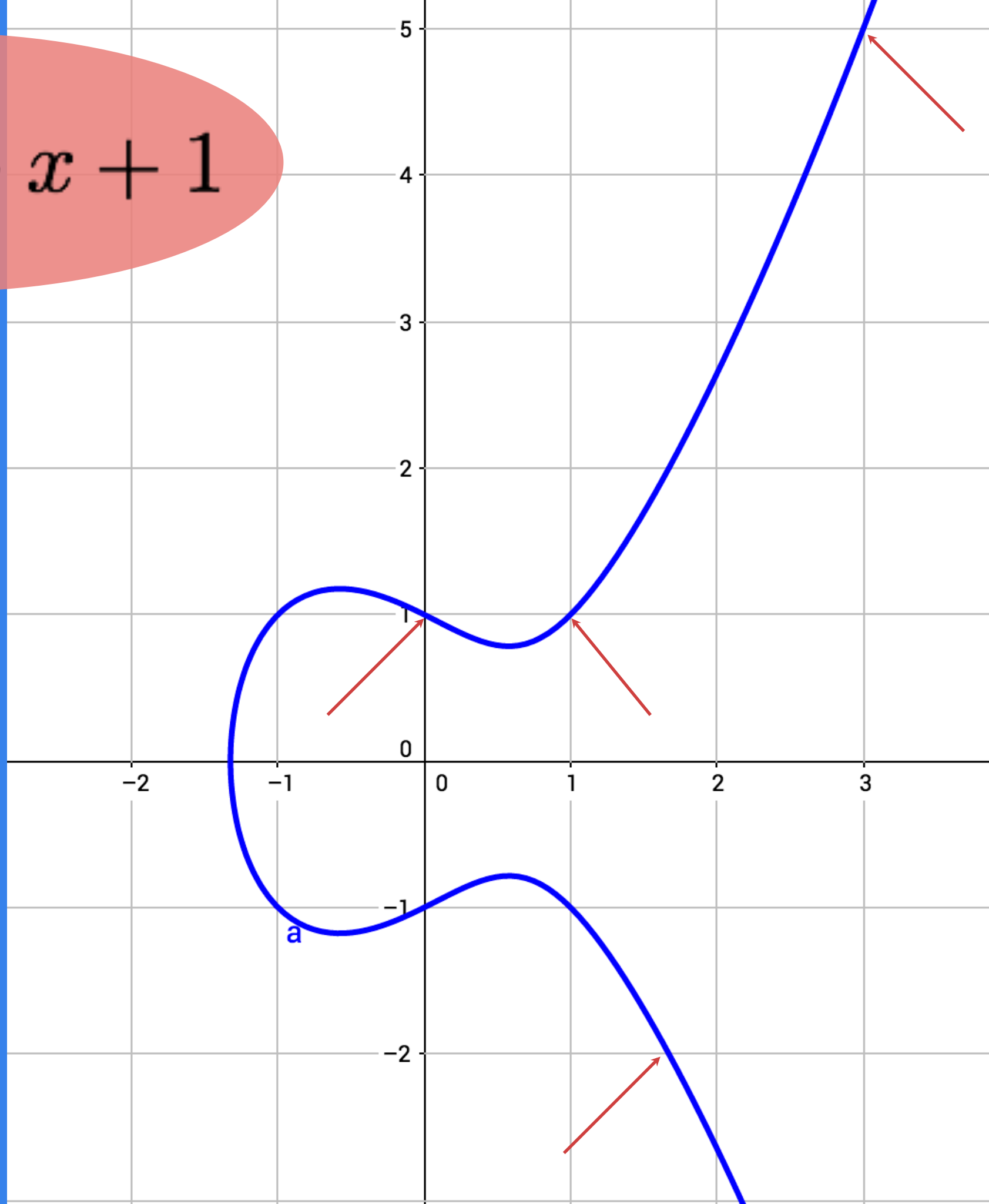
$$y^2 = x^3 - x + 1$$

$$x = 3,$$

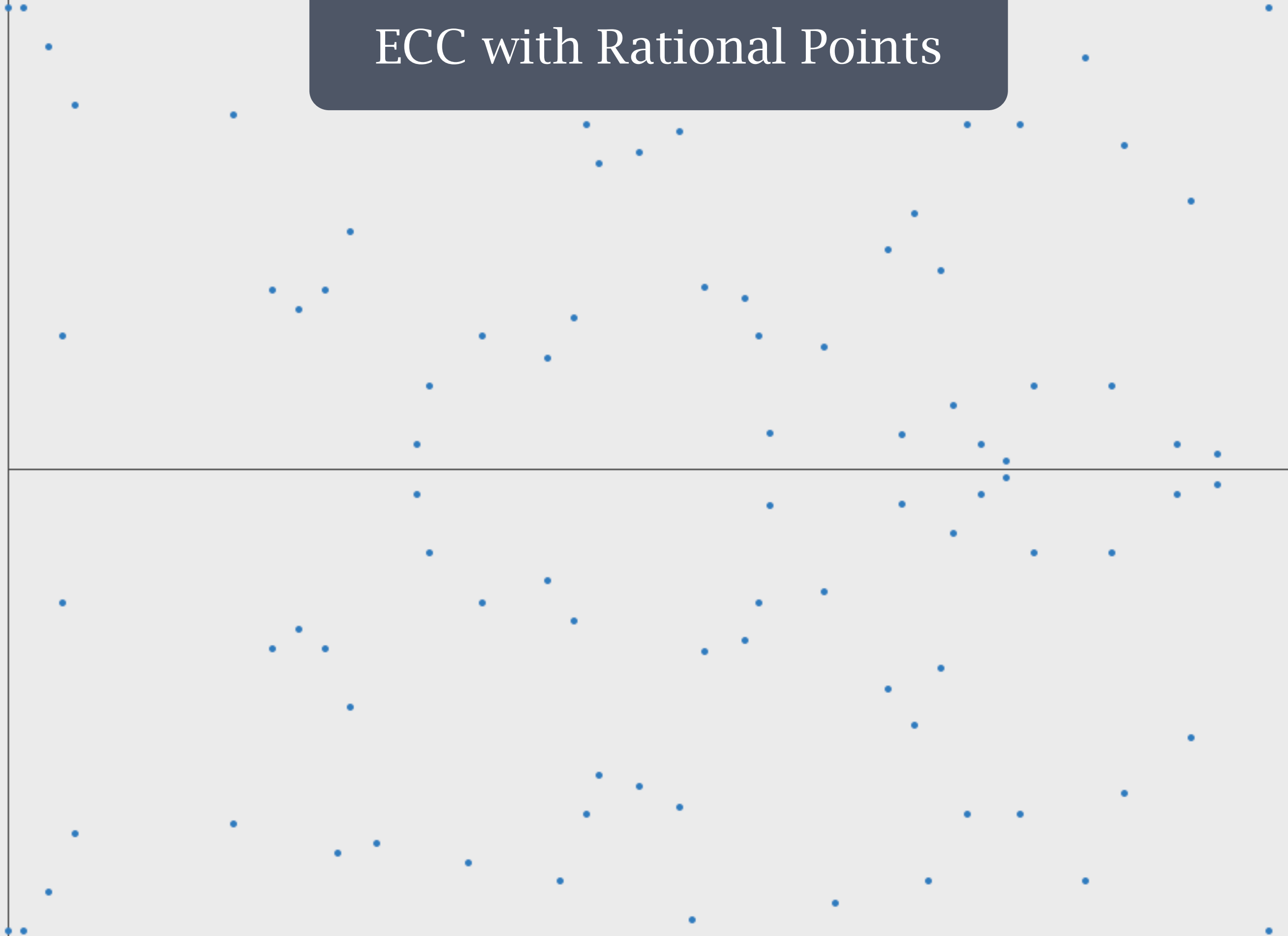
$$y^2 = 3^3 - 3 + 1$$

$$y^2 = 25$$

$$y = \pm 5$$



ECC with Rational Points



A high-speed photograph of a water droplet suspended in mid-air above a pool of water. The droplet is perfectly spherical and transparent, reflecting the surrounding blue light. Below it, the water surface is disturbed, creating concentric ripples that spread outwards. The background is a deep, uniform blue, giving the scene a serene and scientific feel.

What does this mean?

“Breaking a 228-bit RSA key requires less energy than it takes to boil a teaspoon of water...breaking a 228-bit elliptic curve key requires enough energy to boil all the water on the earth, this would require a 2,380-bit RSA key.”



Current Research

Understanding the structure and adding points on other algebraic curves