Elliptic Curve Cryptography (ECC)

CSE 539

jedimaestro@asu.edu

Why ECC?

- We already know how to do encryption (AES, RSA), signatures (RSA), and key exchange (DH), but...
  - ECC can do all three
- More efficient
  - Lower number of bits in key
    - 224 bits for ECC *vs.* 2048 bits for RSA
  - Less power, computation, and time
- Less susceptible to side channels, chosen ciphertext attacks?
  - **Is** susceptible to quantum computers

Resources

- https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
- https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/
- https://en.wikipedia.org/wiki/Elliptic_curve_point_multiplication
- https://cseweb.ucsd.edu/classes/fa22/cse207B-a/lectures/13-ecc.pdf

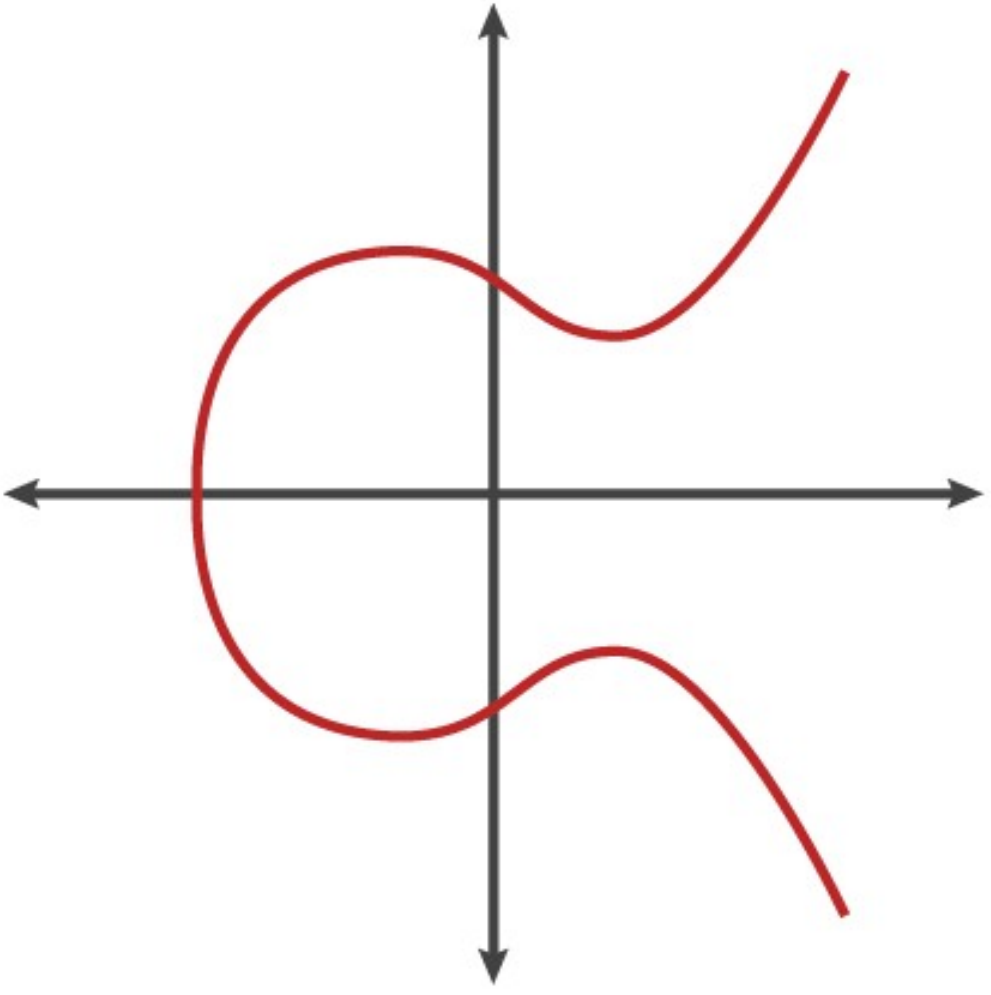
ECC background

- “The use of elliptic curves in cryptography was suggested independently by Neal Koblitz[7] and Victor S. Miller[8] in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005.” -- Wikipedia
- SSL/TLS, Signal, LINE, WhatsApp, Viber, SSH, Matrix, WireGuard, Tor, I2P, ProtonMail, … use it

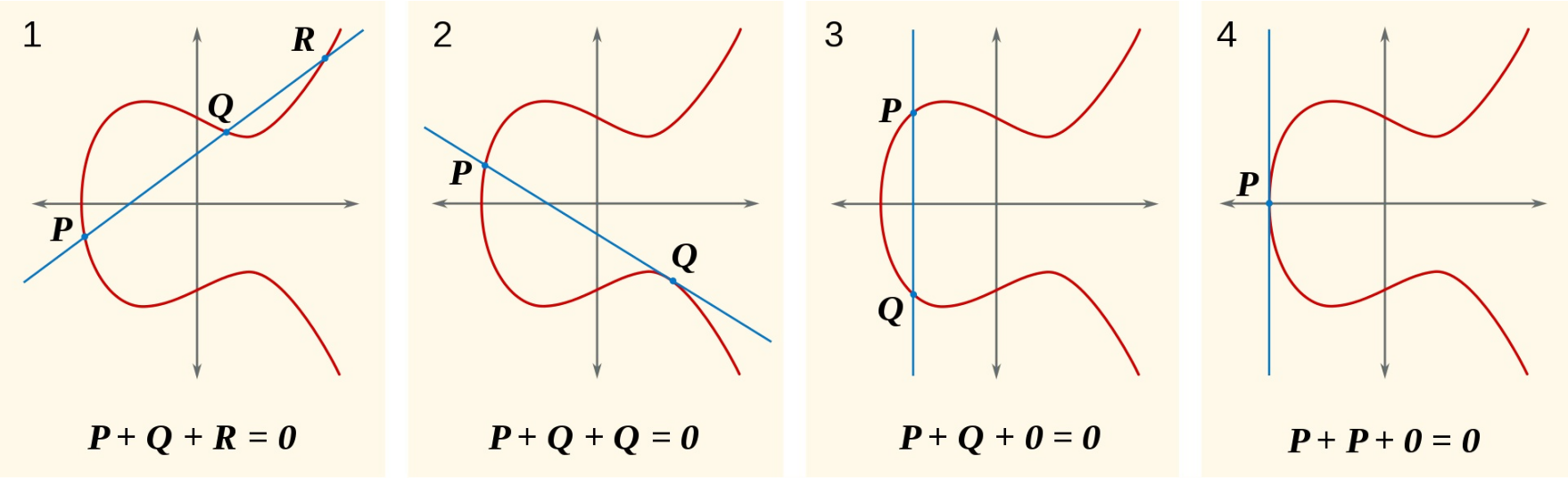
$$y^2 = x^3 + ax + b$$

Following figures are from…

https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

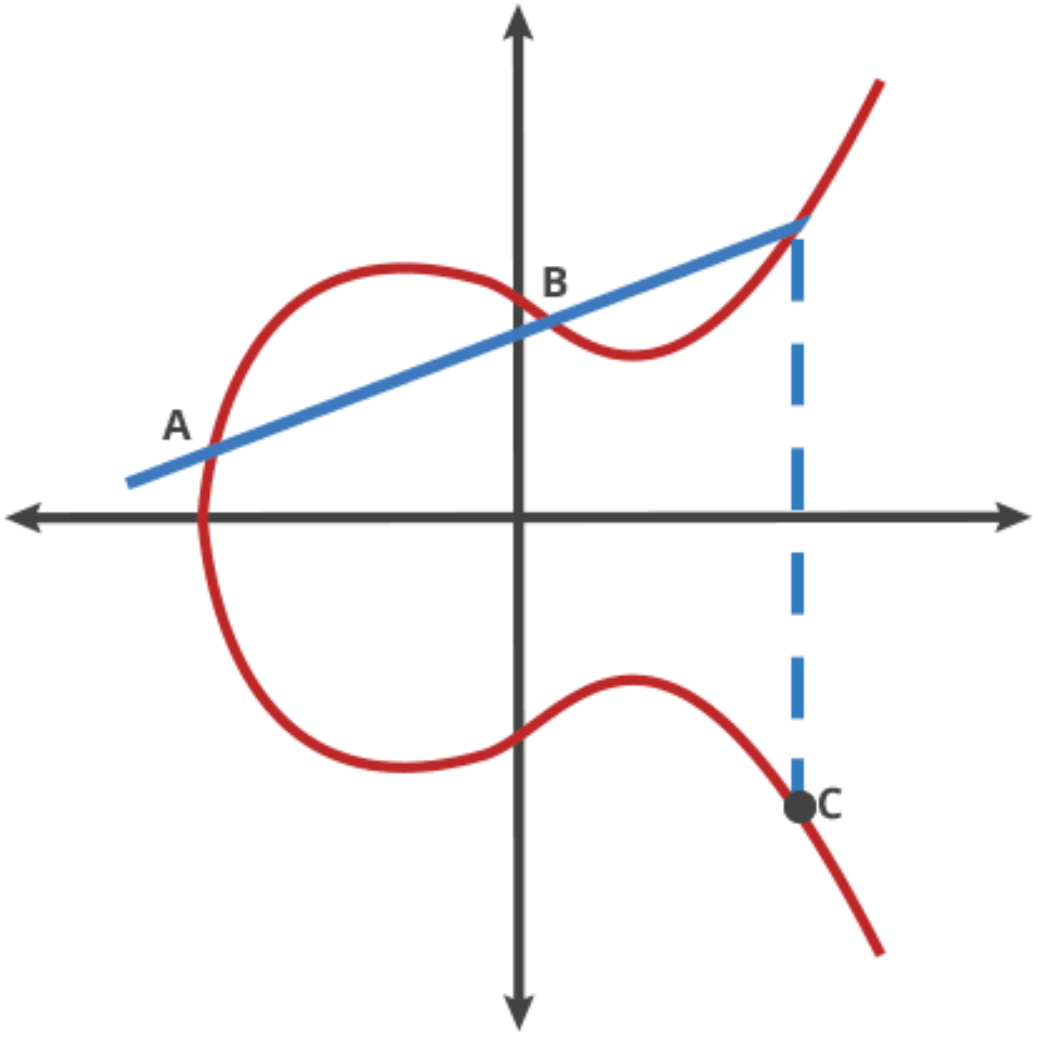


https://en.wikipedia.org/wiki/Elliptic_curve_point_multiplication#/media/File:ECClines.svg



O is point at infinity, serves as identity

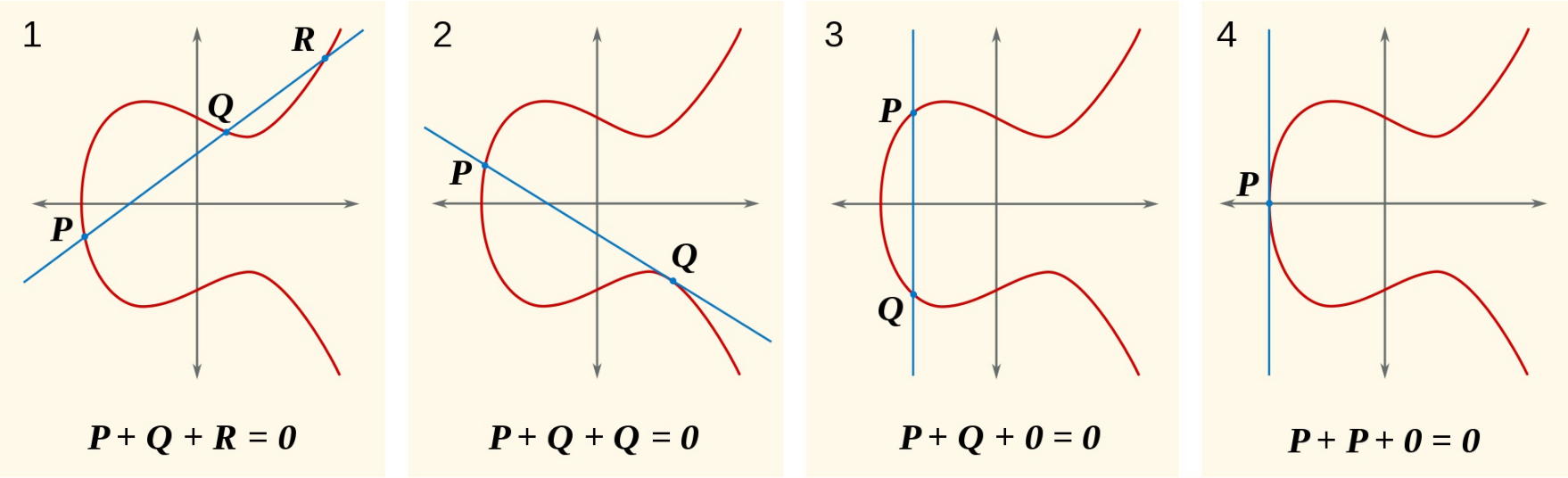
How to calculate “C = A + B”?


A
B
C

How to calculate?

- C = -A (negation)
- C = 2A (doubling)
  - Or, C = A + A
- C = nA
  - What if n is some astronomically large number?

https://en.wikipedia.org/wiki/Elliptic_curve_point_multiplication#/media/File:ECClines.svg



O is point at infinity, serves as identity

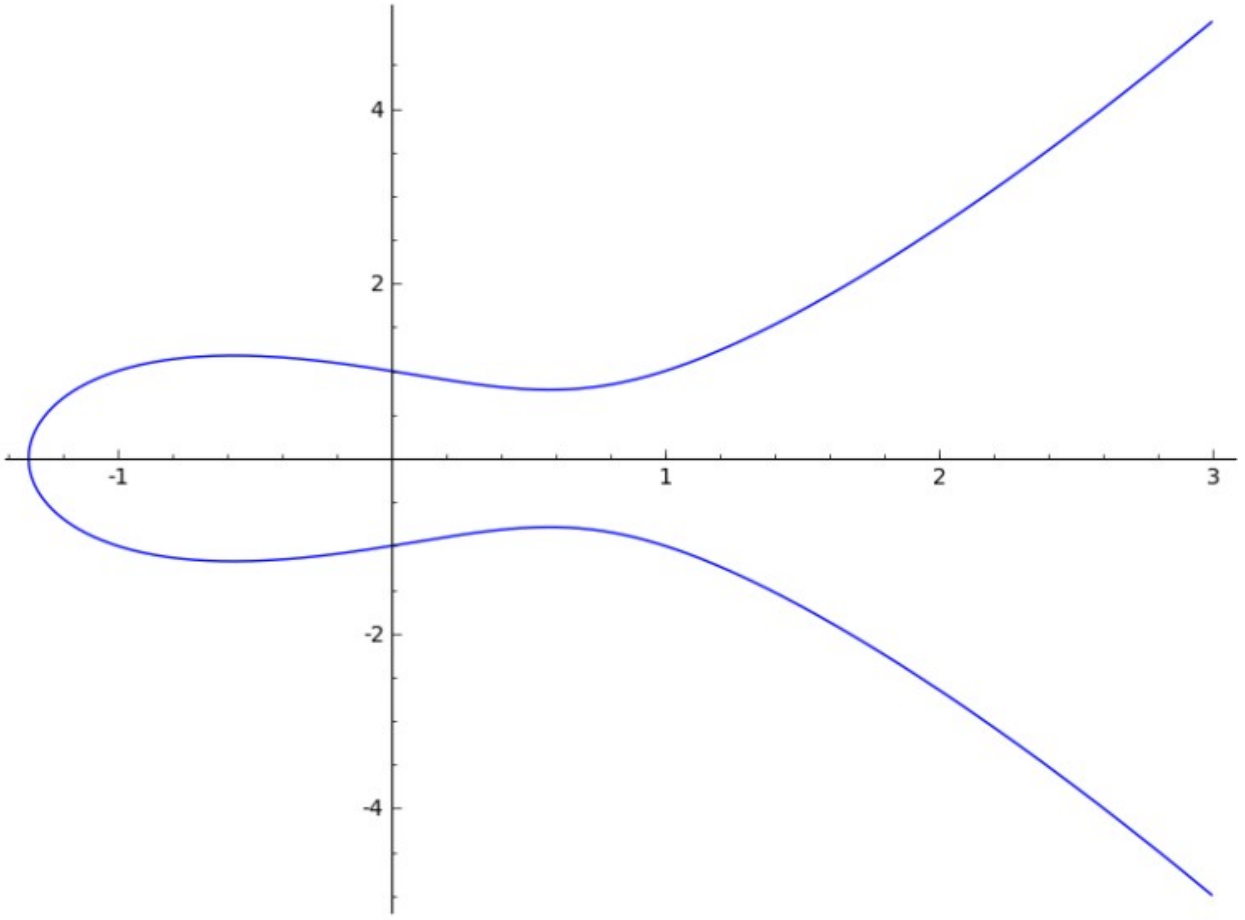
How to calculate?

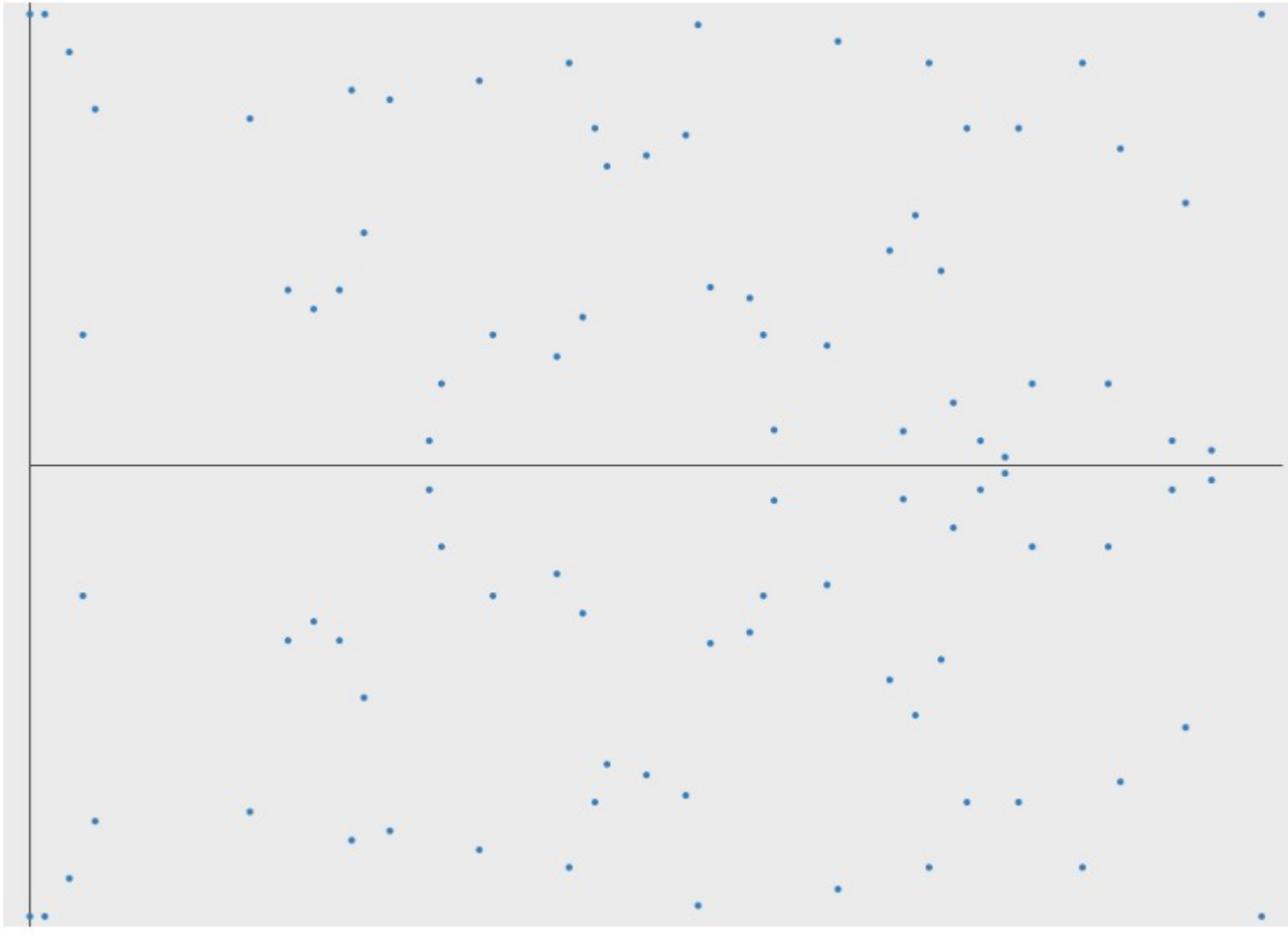
- C = -A (negation)
- C = 2A (doubling)
  - Or, C = A + A
- C = nA
  - What if n is some astronomically large number?
    - Double and add (like “square and multiply” for modular exponentiation) … Trap door function!

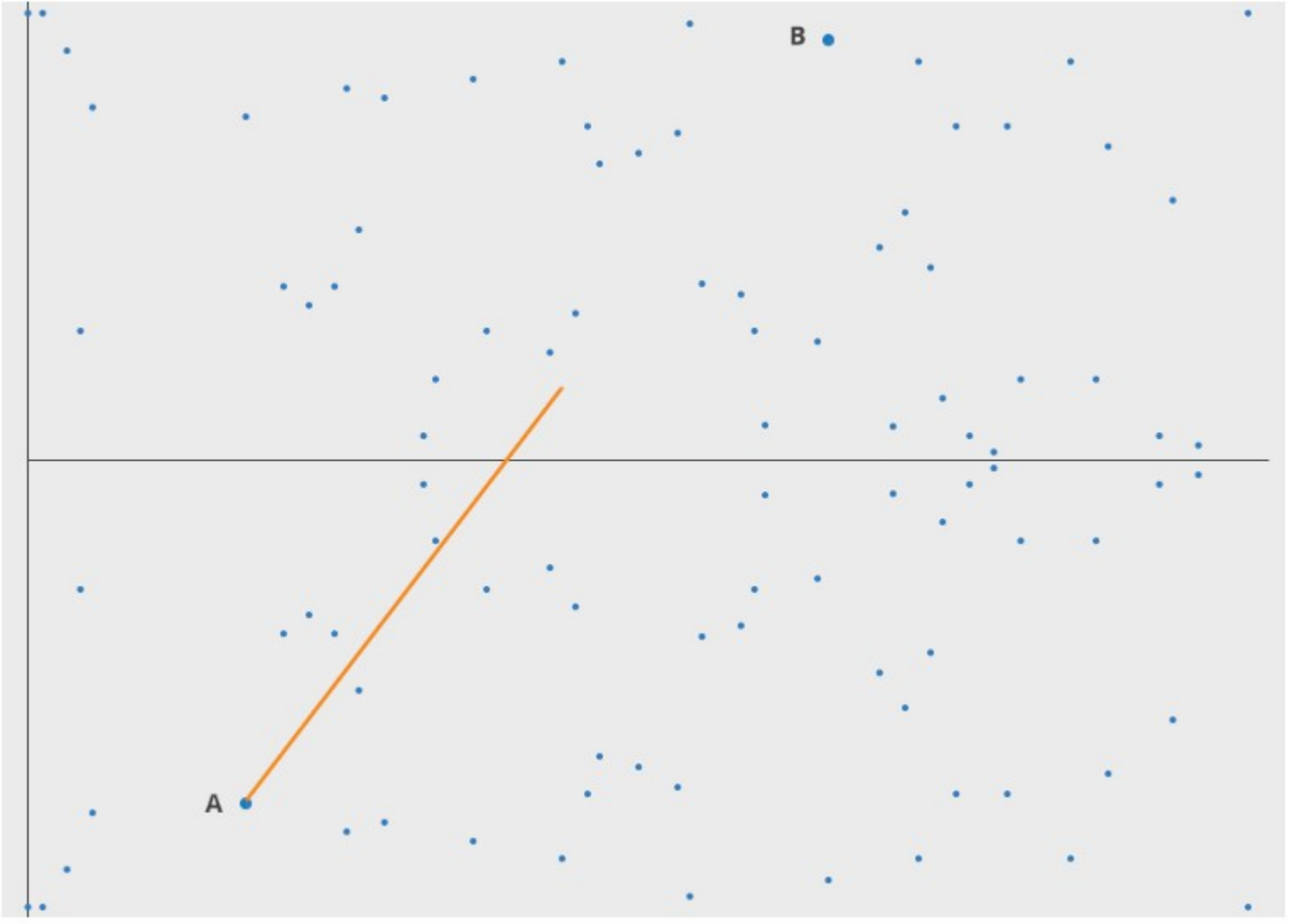
More figures stolen from…

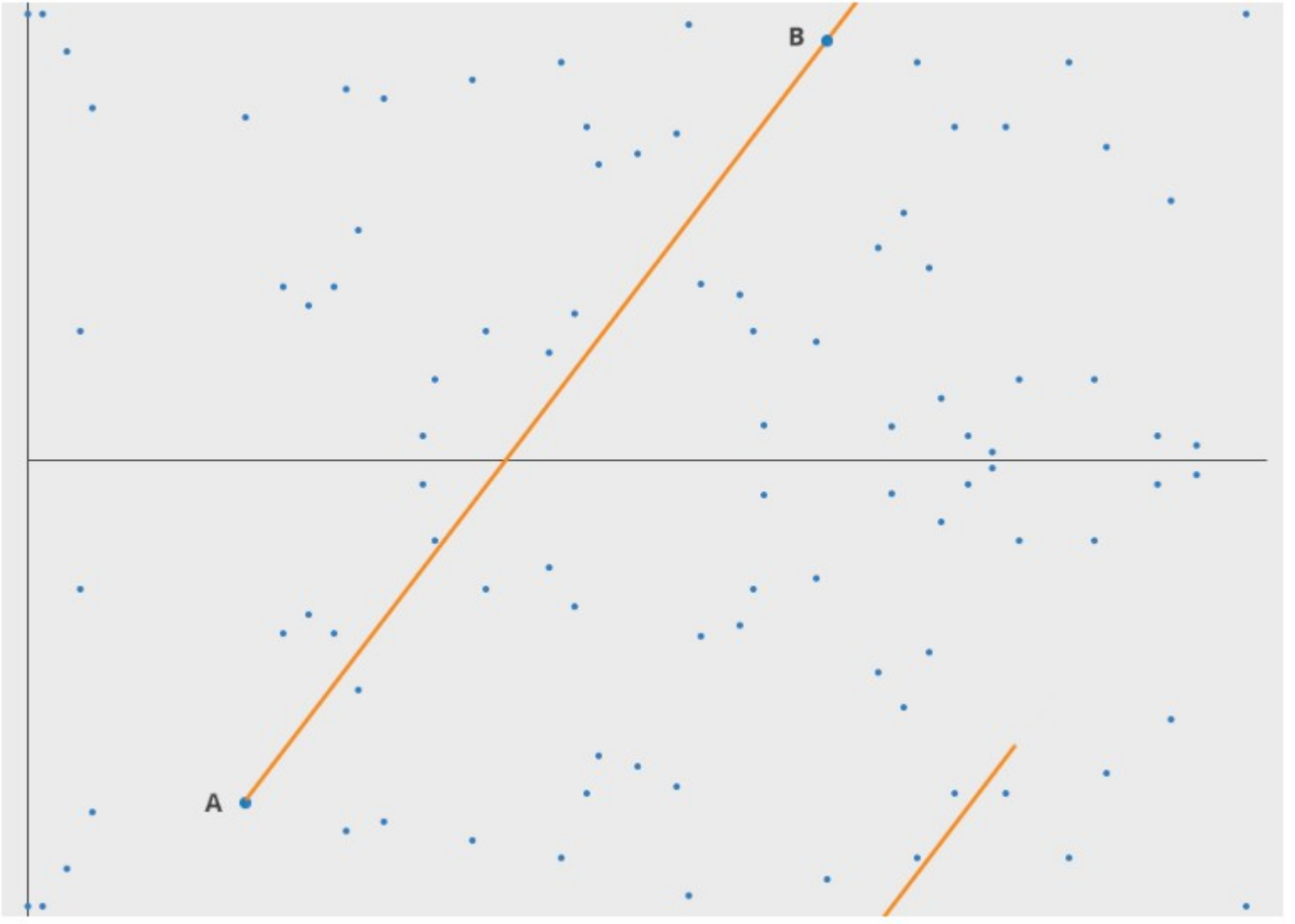
https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

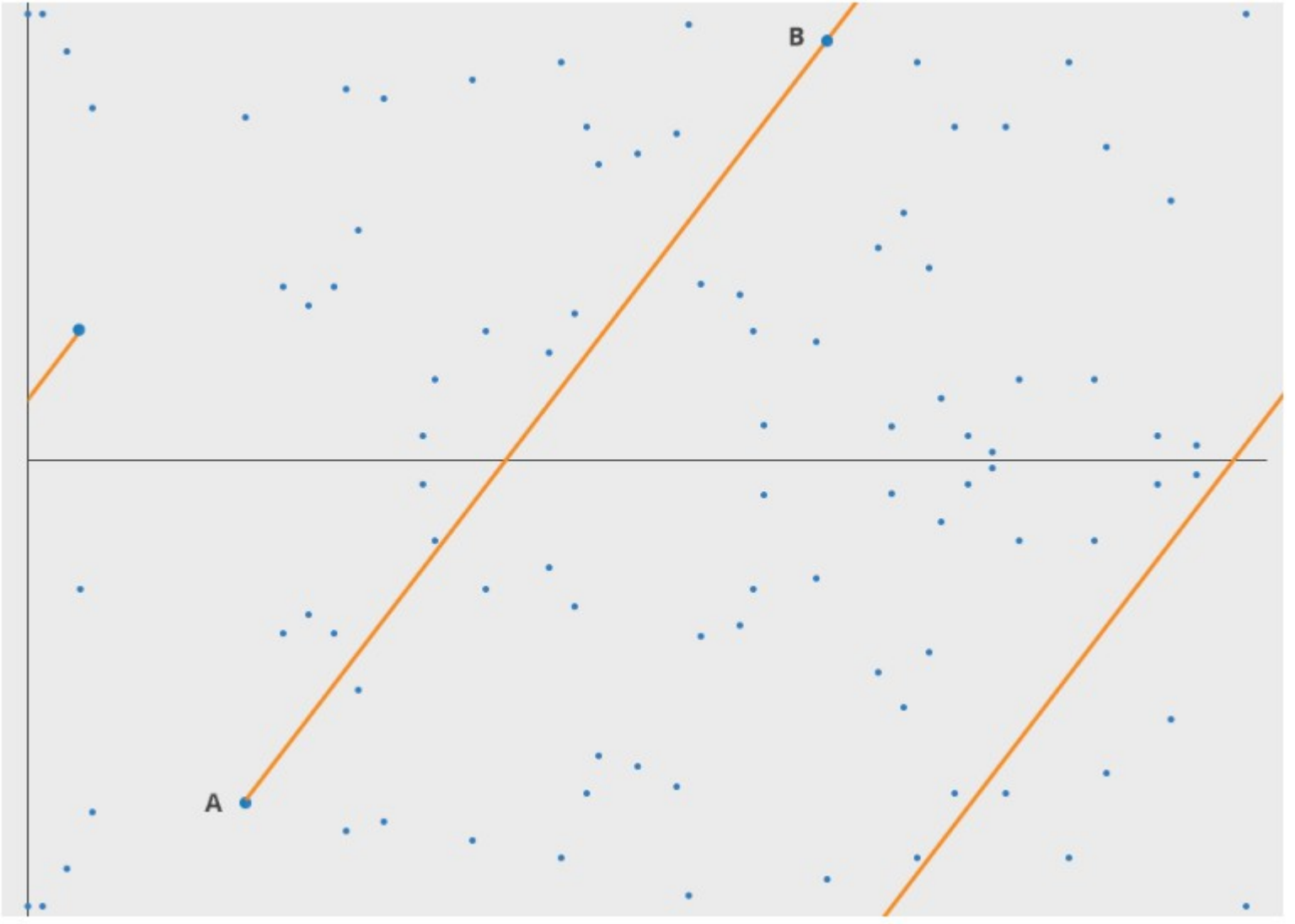
Here's an example of a curve ($y^2 = x^3 - x + 1$) plotted for all numbers:

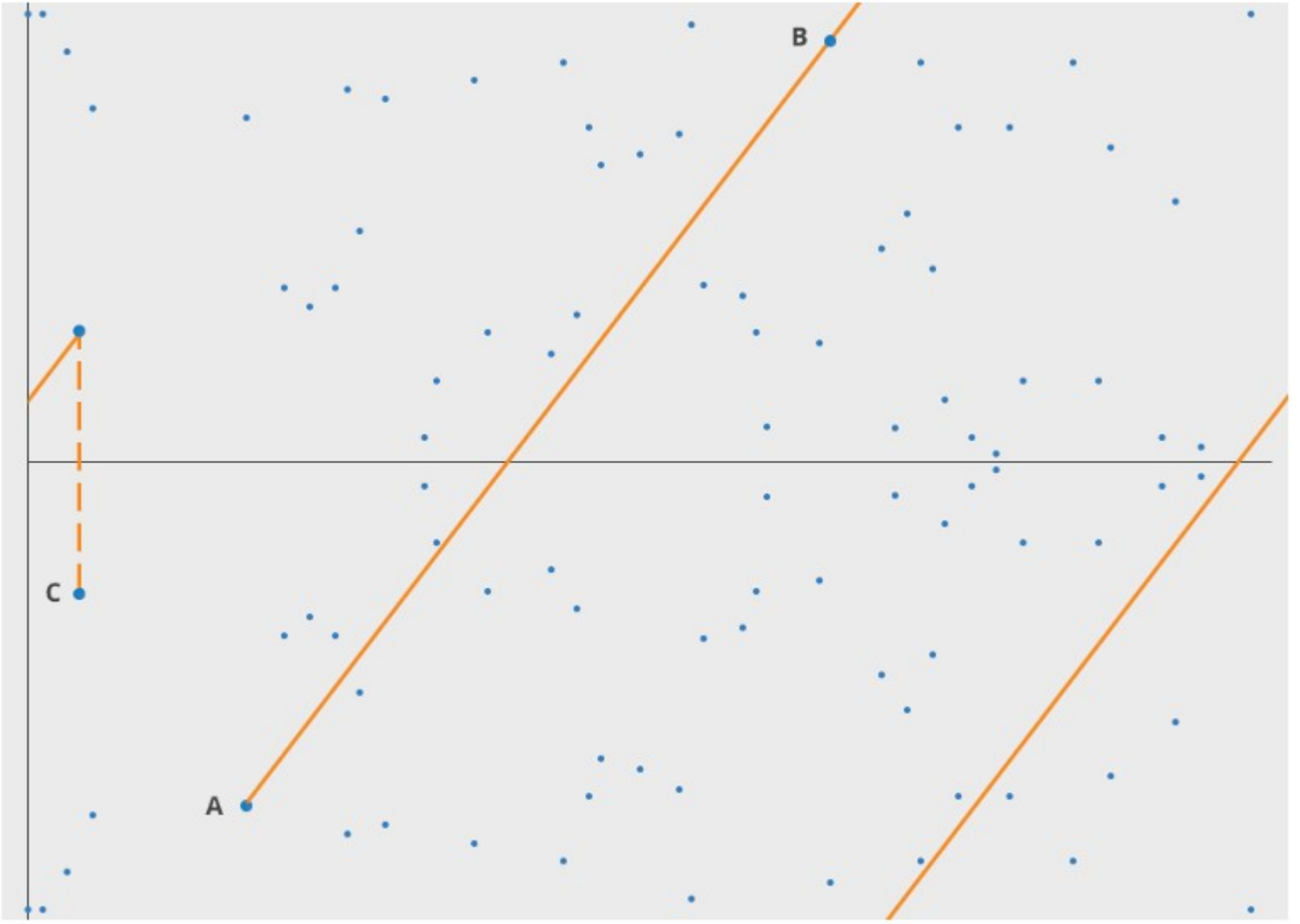





B
A


B
A


B
A


B
C
A

ECDH

- https://en.wikipedia.org/wiki/Elliptic-curve_Diffie%E2%80%93Hellman

Let Alice's key pair be (d_A, Q_A) and Bob's key pair be (d_B, Q_B).

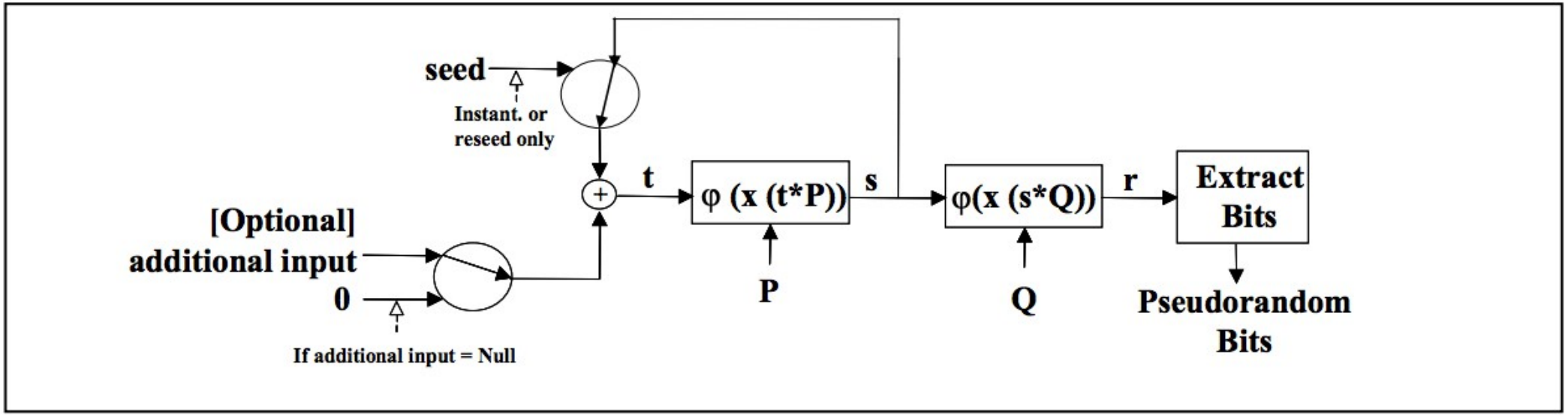
Alice computes point $(x_k, y_k) = d_A \cdot Q_B$. Bob computes point $(x_k, y_k) = d_B \cdot Q_A$.

$$d_A \cdot Q_B = d_A \cdot d_B \cdot G = d_B \cdot d_A \cdot G = d_B \cdot Q_A$$

Can also do...

- Elliptic Curve Digital Signature Algorithm (ECDSA)
  - PlayStation 3 signing key leak
- Elliptic Curve Integrated Encryption Scheme (ECIES)

https://en.wikipedia.org/wiki/Crypto_AG#/media/File:Hagelin_CX-52-IMG_0568-white.jpg



https://matthewdgreen.files.wordpress.com/2013/09/b9dec-dual_ec_diagram.png

TOP SECRET//SI//REL TO USA, FVEY

CLASSIFICATION GUIDE TITLE/NUMBER: (U//FOUO) PROJECT BULLRUN/2-16

PUBLICATION DATE: 16 June 2010

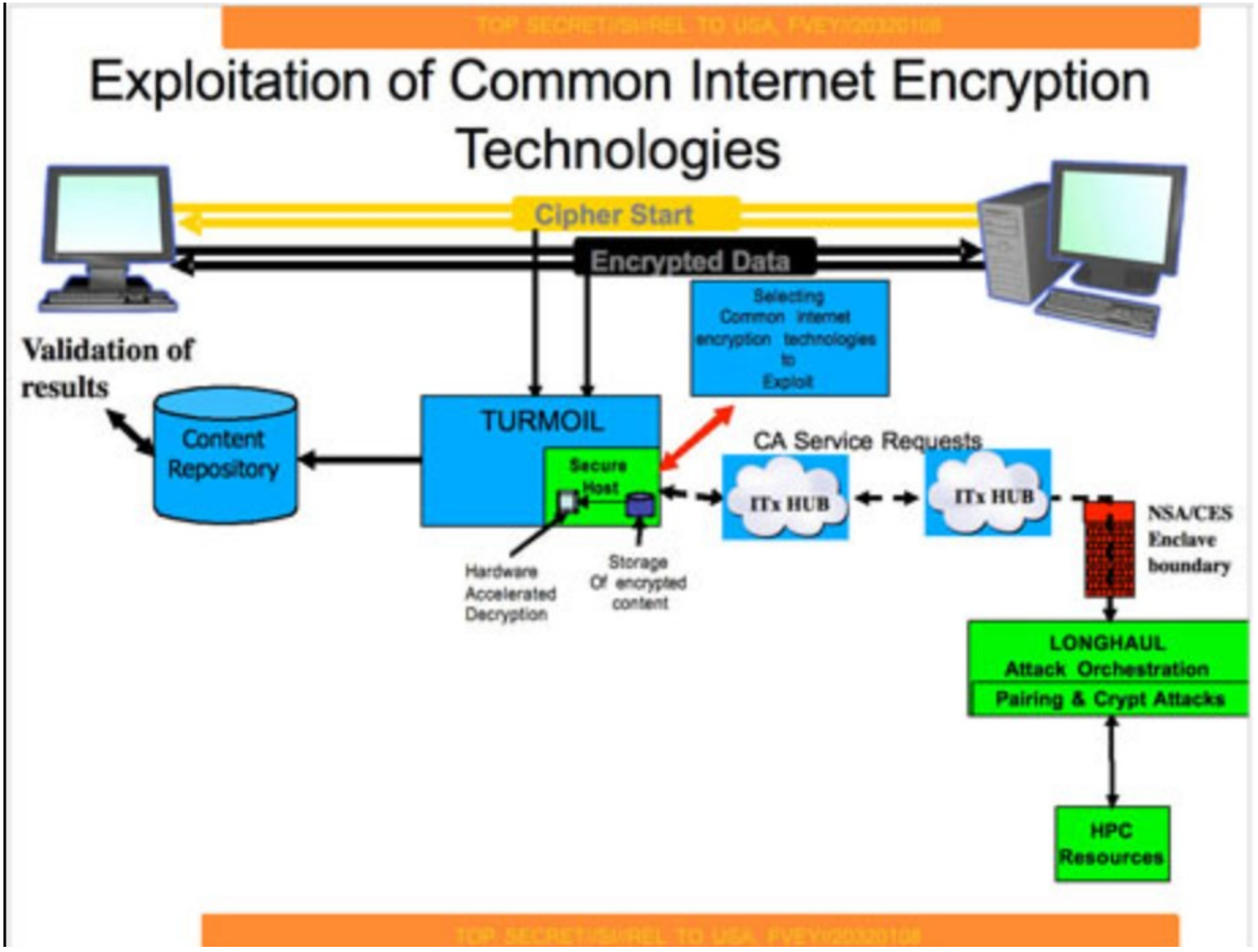
OFFICE OF ORIGIN: (U) Cryptanalysis and Exploitation Services

POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

PHONE: [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple sources, all of which are extremely sensitive. They include CNE, interdiction, industry relationships, collaboration with other IC entities, and advanced mathematical techniques. Several ECIs apply to the specific sources, methods, and techniques involved. Because of the multiple sources involved in BULLRUN activities, "capabilities against a technology" does not necessarily equate to decryption.



https://upload.wikimedia.org/wikipedia/commons/e/e1/NSA-diagram-001.jpg

Main takeaways about ECC

- Common choice because it’s more efficient, does key exchange and signatures
  - Not 100% immune to side channels or padding issues
  - Not quantum resistant

If you’re interested in more…

https://www.youtube.com/watch?v=CPHLvx6jbOc