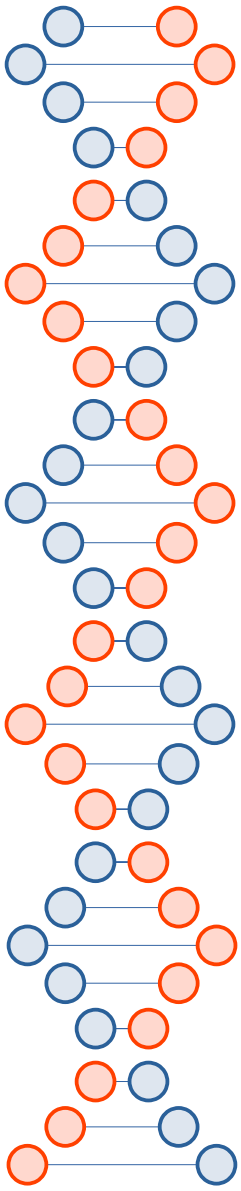
Diffie-Hellman, OTR, and Signal

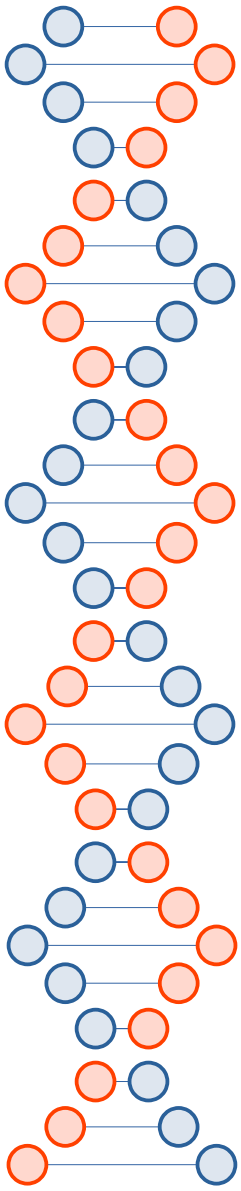
CSE 548 Spring 2026

jedimaestro@asu.edu



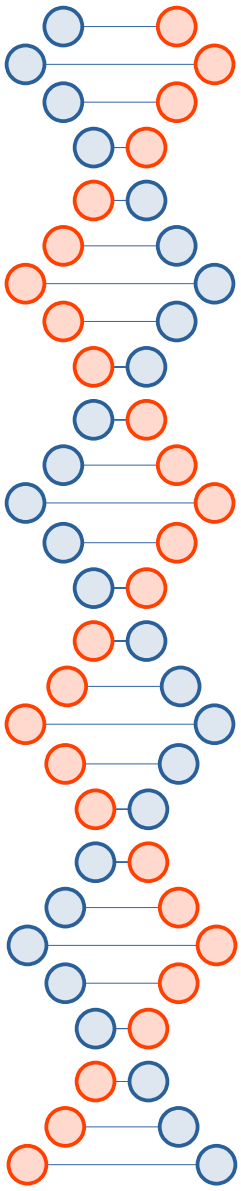
Basic types of crypto...

- Symmetric encryption
  - Assumes two parties wishing to communicate already have a shared secret
- Asymmetric encryption
  - Makes different assumptions (*e.g.*, that everybody knows the public key or that the eavesdropper is passive)
  - Quantum computers break current algorithms that are used in practice
- Secure hash functions and message authentication



Symmetric Crypto

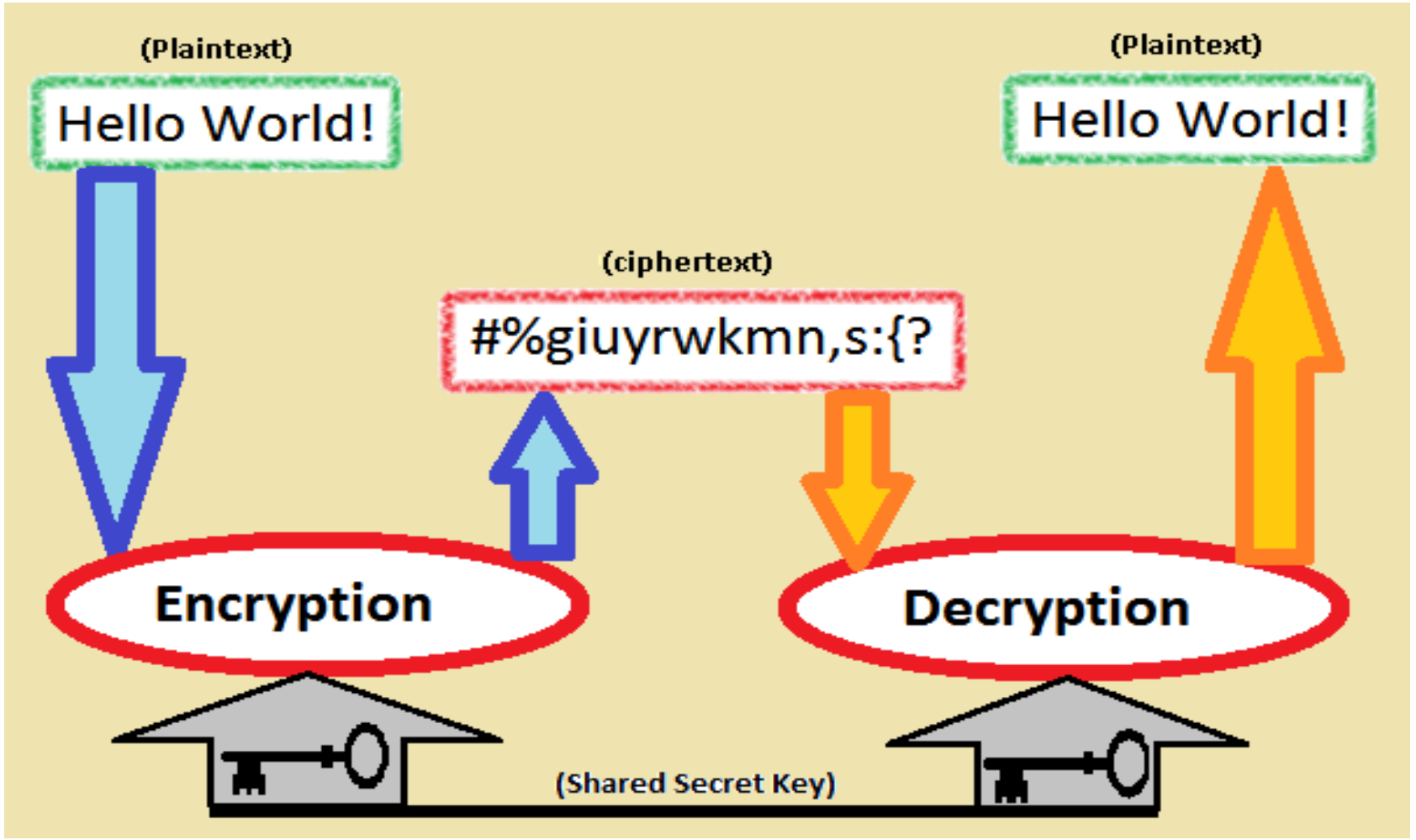
- Confidentiality
- Integrity
- ~~Availability~~
- Authentication
- ~~Non-repudiation~~
- ~~A way to distribute the shared secret keys~~



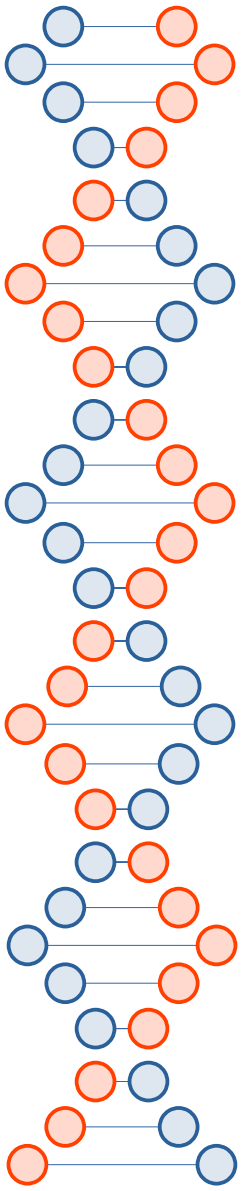
Symmetric Crypto

- Confidentiality
- Integrity
- ~~Availability~~
- Authentication
- ~~Non-repudiation~~
- ~~A way to distribute the shared secret keys~~

Diffie-Hellman will give us this one

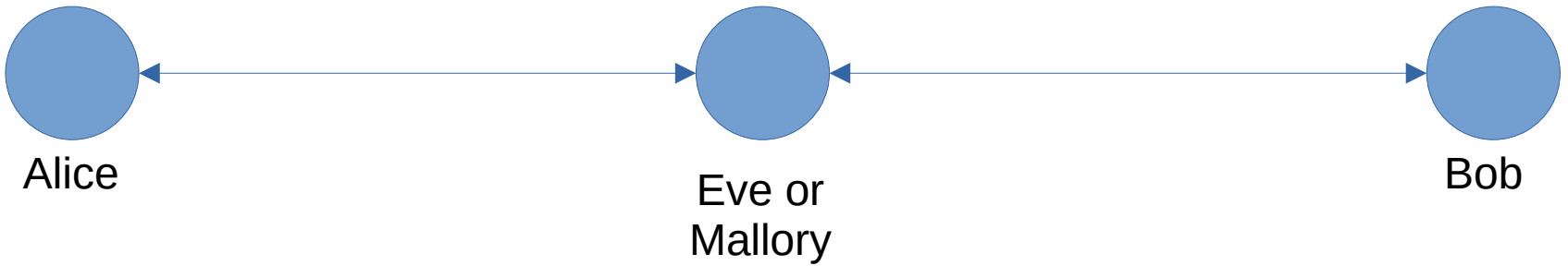


Source: Wikipedia

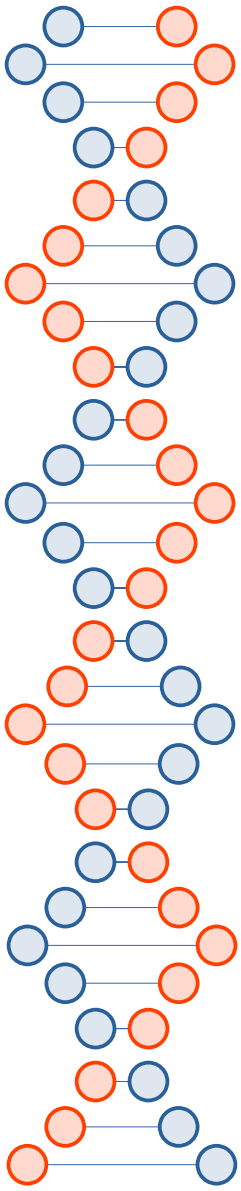


Terminology

- Plaintext – before encryption, easy to read
- Ciphertext – after encryption, hopefully indecipherable without the key
- Key – the shared secret, typically just bits that were generated with a high entropy process



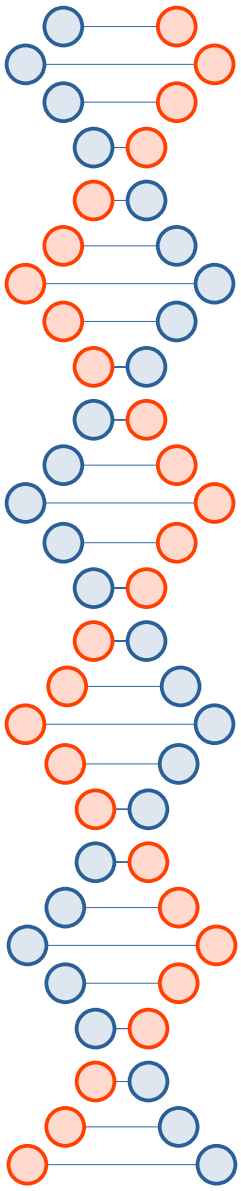
WiFi, electric path, or optical… Eve or Mallory get their own copy!
So how to Alice and Bob exchange a key?



A nice video about Diffie-Hellman

- https://www.youtube.com/watch?v=YEBfamv-_do

Diffie-Hellman is *asymmetric* crypto

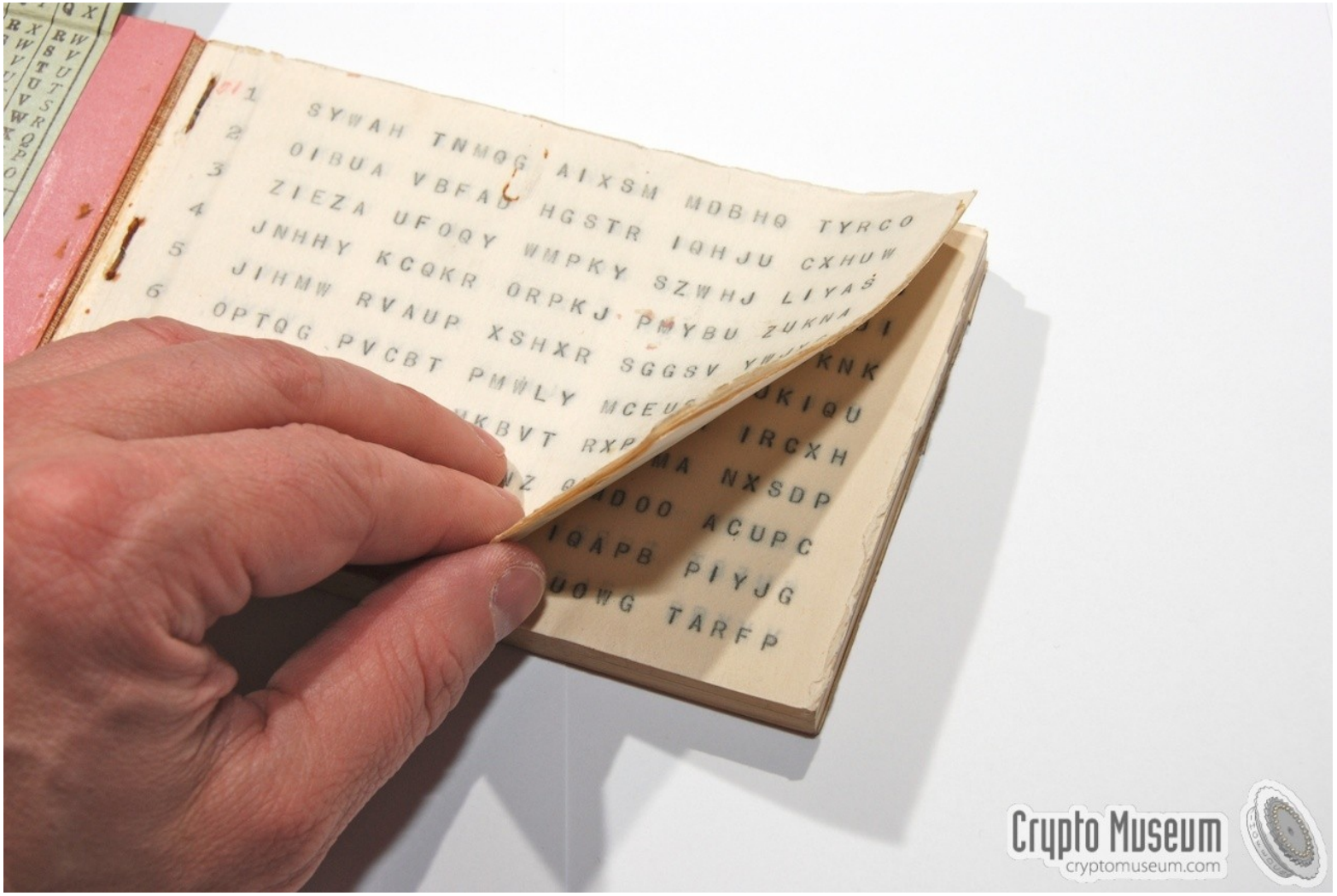


Darknet Diaries, Episode 83

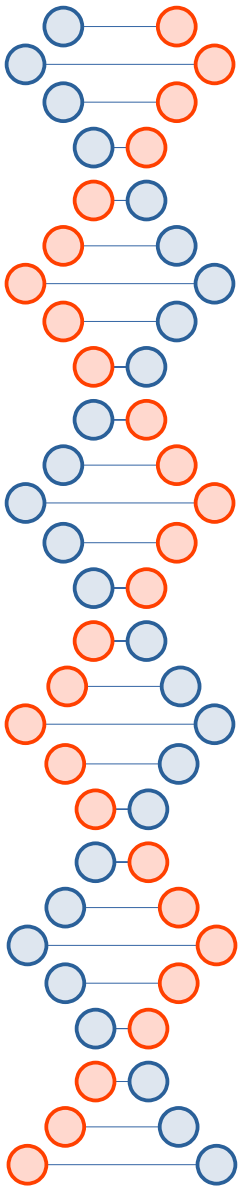
https://darknetdiaries.com/transcript/83/

- “There was no concept of doing anything cryptographic in terms of software back in the late 80s. I say this, I’m in contact with a fellow alumni from the InfoSec organization and people that were there years before I was, and I’ve asked. To the best that I have been able to figure out, what we ended up producing which was half paper pad, half key on a floppy, and a computer program that would do the encryption and decryption. That was the first foray into software-based cryptography that NSA produced.”

  --Jeff Man

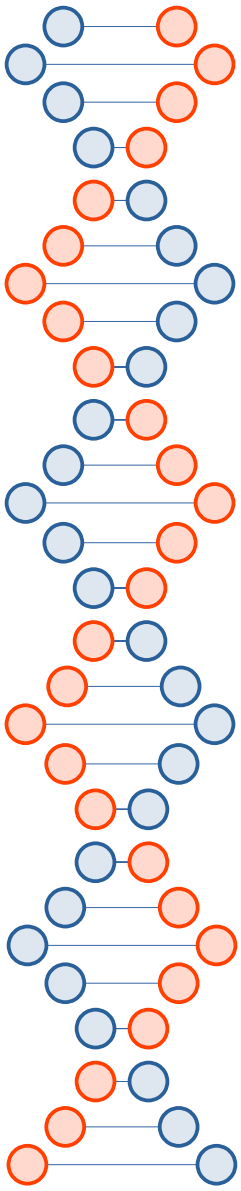

1 SYWAH TNMQG AIXSM MDBHQ TYRCO
2 OIBUA VBFAD HGSTR IQHJU CXHUW
3 ZIEZA UFOQY WMPKY SZWHJ LIYAŚ
4 JNHHY KCQKR ORPKJ PMYBU ZUKNA
5 JIHMW RVAUP XSHXR SGGSV
6 OPTQG PVCBT PMWLY MCEU
KBVT RXP
IRCXH
NXSDP
ACUPC
PIYJG
TARFP
Crypto Museum
cryptomuseum.com


PX 1000Cr
CLEAR ALL
CLR LINE
CODE
KEY
ON STOP
KEY TXT
CODE
CLR LINE
CLEAR ALL
LOAD
DUMP
SEARCH
TEXT
INS TXT
INSERT
DEL TXT
DELETE
SHIFT
LIST
PRINT
RCVE
LOW HIGH
MARGIN
SET CLR
TAB
CAPS
LOCK
SHIFT



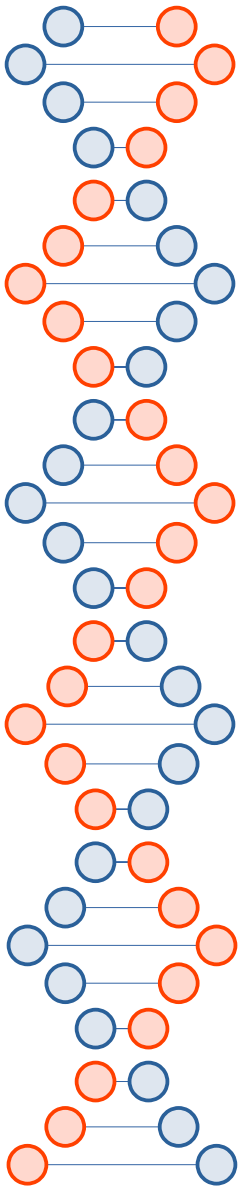
Couple of footnotes

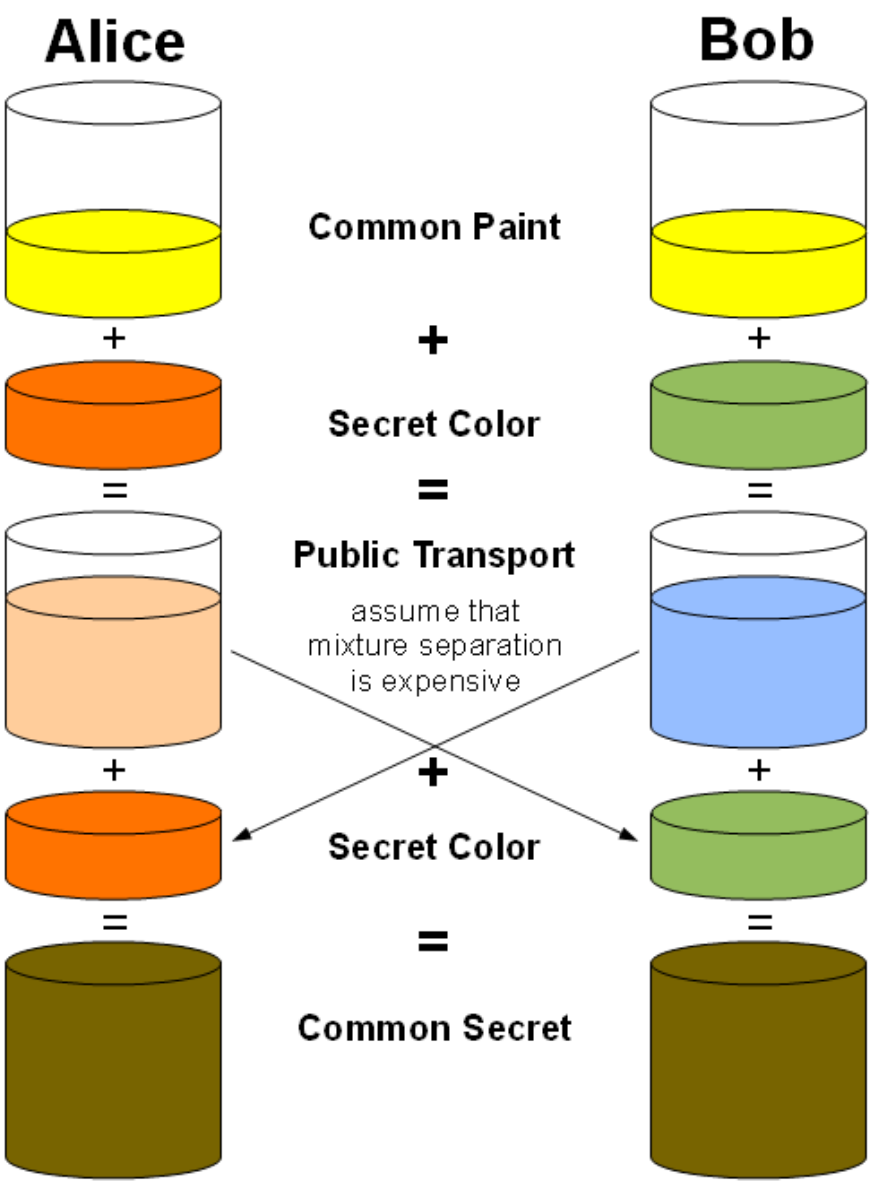
- Diffie-Hellman-Merkle?
- Who was first?
  - Diffie-Hellman conceived and then published 1976
  - GCHQ version conceived 1969, published 1997



Basics...

- https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange



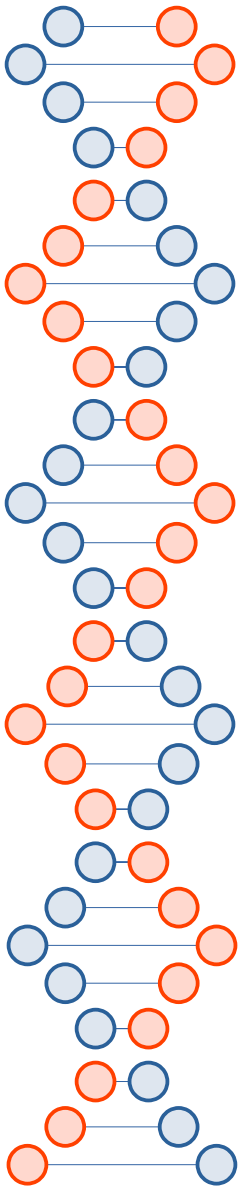

Alice
Bob
Common Paint
+
Secret Color
=
Public Transport
assume that
mixture separation
is expensive
+
Secret Color
=
Common Secret

Alice		Bob		Eve	
Known	Unknown	Known	Unknown	Known	Unknown
$p = 23$		$p = 23$		$p = 23$	
$g = 5$		$g = 5$		$g = 5$	
$\mathbf{a = 6}$	$\mathbf{b}$	$\mathbf{b = 15}$	$\mathbf{a}$		$\mathbf{a}$, $\mathbf{b}$
$A = 5^{a} \bmod 23$		$B = 5^{b} \bmod 23$			
$A = 5^{6} \bmod 23 = 8$		$B = 5^{15} \bmod 23 = 19$			
$\mathbf{B = 19}$		$\mathbf{A = 8}$		$A = 8, B = 19$	
$\mathbf{s} = B^{a} \bmod 23$		$\mathbf{s} = A^{b} \bmod 23$			
$\mathbf{s} = 19^{6} \bmod 23 = \mathbf{2}$		$\mathbf{s} = 8^{15} \bmod 23 = \mathbf{2}$			$\mathbf{s}$

The paper...

I. Introduction

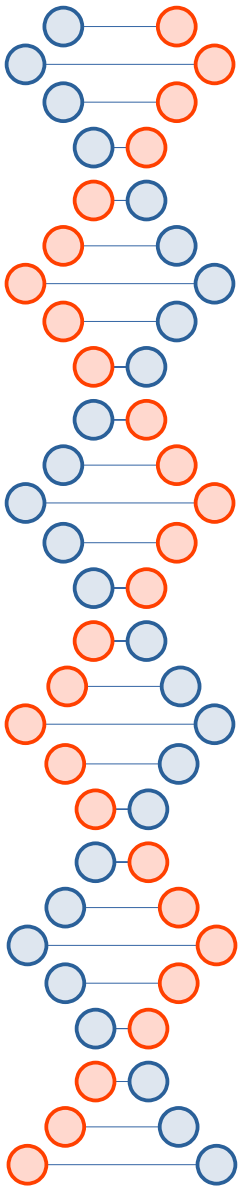
WE STAND TODAY on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.



tation time must be small. A million instructions (costing approximately $0.10 at bicentennial prices) seems to be a reasonable limit on this computation. If we could ensure,

There is currently little evidence for the existence of trap-door ciphers. However they are a distinct possibility and should be remembered when accepting a cryptosystem from a possible opponent [12].

Manuscript received June 3, 1976. This work was partially supported by the National Science Foundation under NSF Grant ENG 10173. Portions of this work were presented at the IEEE Information Theory Workshop, Lenox, MA, June 23–25, 1975 and the IEEE International Symposium on Information Theory in Ronneby, Sweden, June 21–24, 1976.



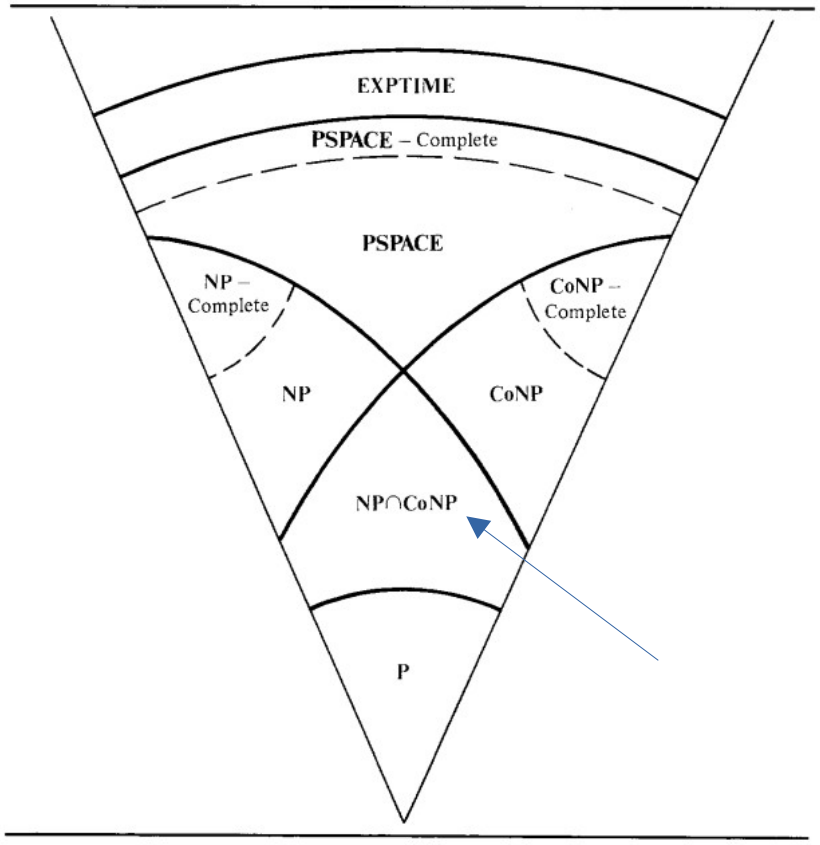
We assume that the function f is public information, so that it is not ignorance of f which makes calculation of f^{-1} difficult. Such functions are called one-way functions and were first employed for use in login procedures by R. M. Needham [9, p. 91]. They are also discussed in two recent papers [10], [11] which suggest interesting approaches to the design of one-way functions.

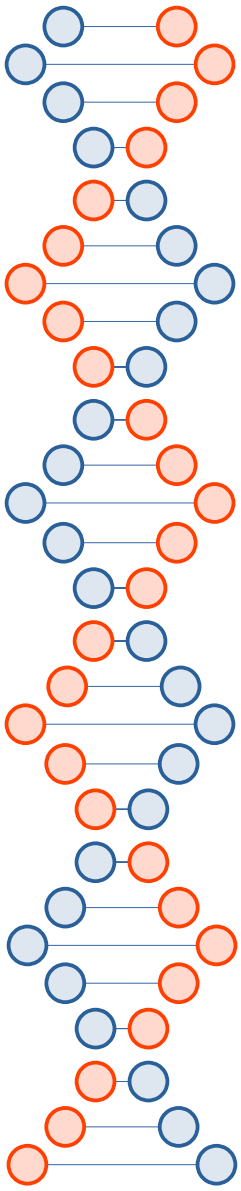
More precisely, a function f is a *one-way function* if, for any argument x in the domain of f, it is easy to compute the corresponding value $f(x)$, yet, for almost all y in the range of f, it is computationally infeasible to solve the equation $y = f(x)$ for any suitable argument x.

pp. 415, 420, 422–424]. We hope this will inspire others to work in this fascinating area in which participation has been discouraged in the recent past by a nearly total government monopoly.

https://faculty.nps.edu/dedennin/publications/Denning-CryptographyDataSecurity.pdf

FIGURE 1.18 Complexity classes.





In order to develop large, secure, telecommunications systems, this must be changed. A large number of users n results in an even larger number, $(n^2 - n)/2$ potential pairs who may wish to communicate privately from all others.

The new technique makes use of the apparent difficulty of computing logarithms over a finite field $GF(q)$ with a prime number q of elements. Let

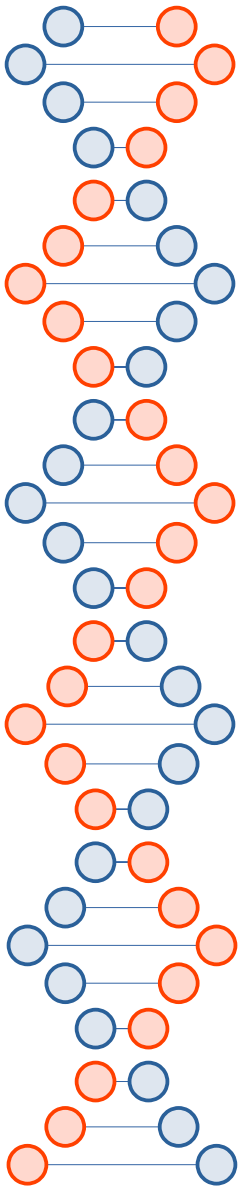
$$Y = \alpha^X \bmod q, \qquad \text{for } 1 \leq X \leq q - 1, \tag{4}$$

where α is a fixed primitive element of $GF(q)$, then X is referred to as the logarithm of Y to the base α, mod q:

$$X = \log_\alpha Y \bmod q, \qquad \text{for } 1 \leq Y \leq q - 1. \tag{5}$$

Calculation of Y from X is easy, taking at most $2 \times \log_2 q$ multiplications [6, pp. 398–422]. For example, for $X = 18$,

$$Y = \alpha^{18} = (((\alpha^2)^2)^2)^2 \times \alpha^2. \tag{6}$$



RSA *vs.* DH

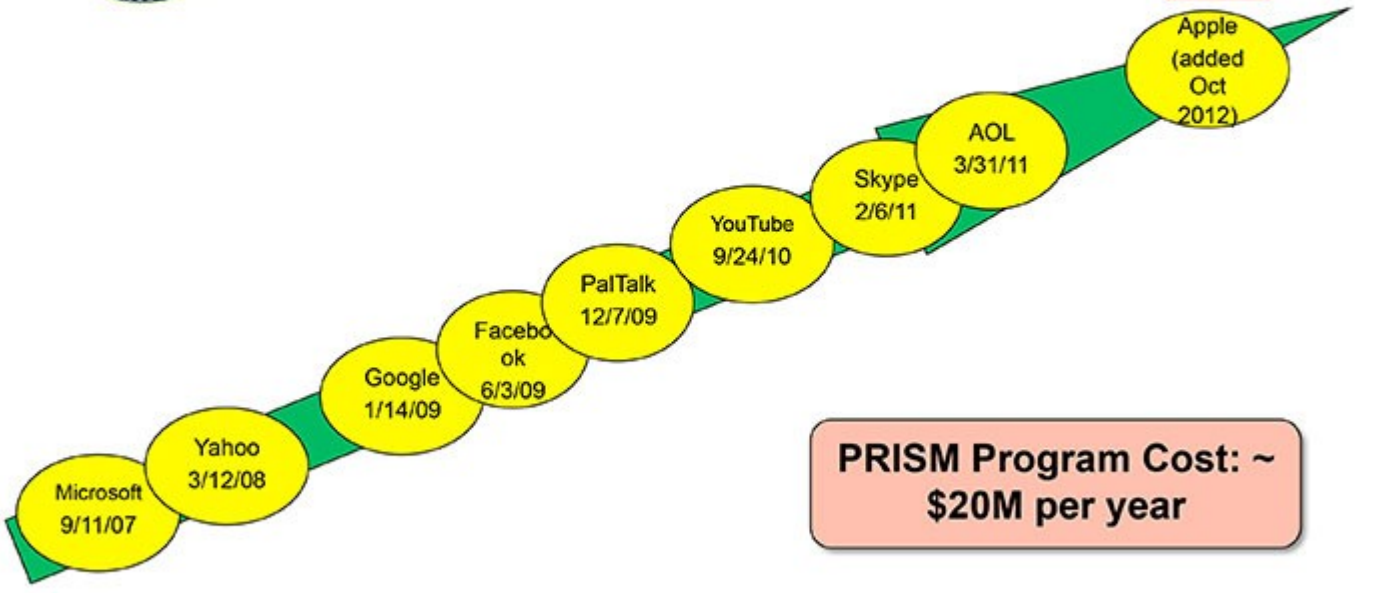
- Diffie-Hellman (1976)
  - Key exchange
  - *Both sides get to choose something random*
- RSA (1977)
  - Encryption
  - Signatures

https://en.wikipedia.org/wiki/Source_(journalism)

- **"On the record"**: all that is said can be quoted and attributed.
- **"Unattributable"**: what is said can be reported but not attributed.
- **"Off the record"**: the information is provided to inform a decision or provide a confidential explanation, not for publication.

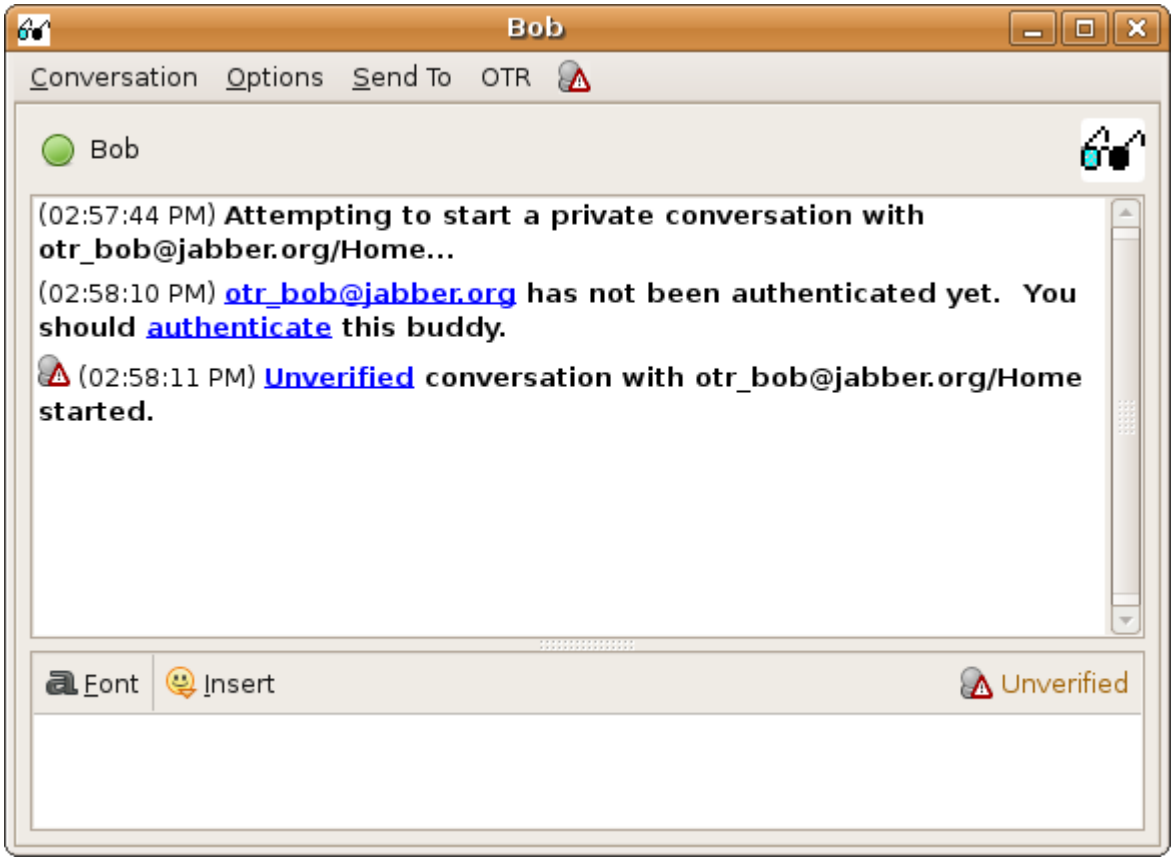
https://www.theguardian.com/film/2014/oct/11/citizenfour-review-snowden-vindicated-poitras-nsa-journalism

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



OTR

- Off-The-Record messaging
- 2004, Nikita Borisov, Ian Goldberg, Eric Brewer. "Off-the-Record Communication, or, Why Not To Use PGP"
- (PGP is from 1991, basically RSA for email)



https://otr.cypherpunks.ca/help/3.2.0/authenticate.php?lang=en

Requirements, OTR *vs.* TLS...

- Forward secrecy
  - Both OTR and TLS care, for different reasons
- Deniable authentication *a.k.a.* off-the-record
  - TLS doesn’t care about this, OTR does
- Future secrecy
  - TLS doesn’t care about this, OTR does it by accident
- Out-of-order messages, parties offline for long periods of time, groups…
  - TLS doesn’t need to worry about any of these, nor does OTR (Signal does)

Off-The-Record (OTR) Messaging

- Based on Diffie-Hellman and AES, and originally SHA-1
  - There are new versions
- Deniable Authentication
  - “Off the record” in journalism
- Forward secrecy
  - Ephemeral key exchange
- Future secrecy (not a design goal, but has it)

Deniable Authentication

- Concept of “malleability”
- Basic idea has two parts:
  - Hash the decryption key for a message, use the hash digest as an authentication key
  - Reveal the authentication key in the next message

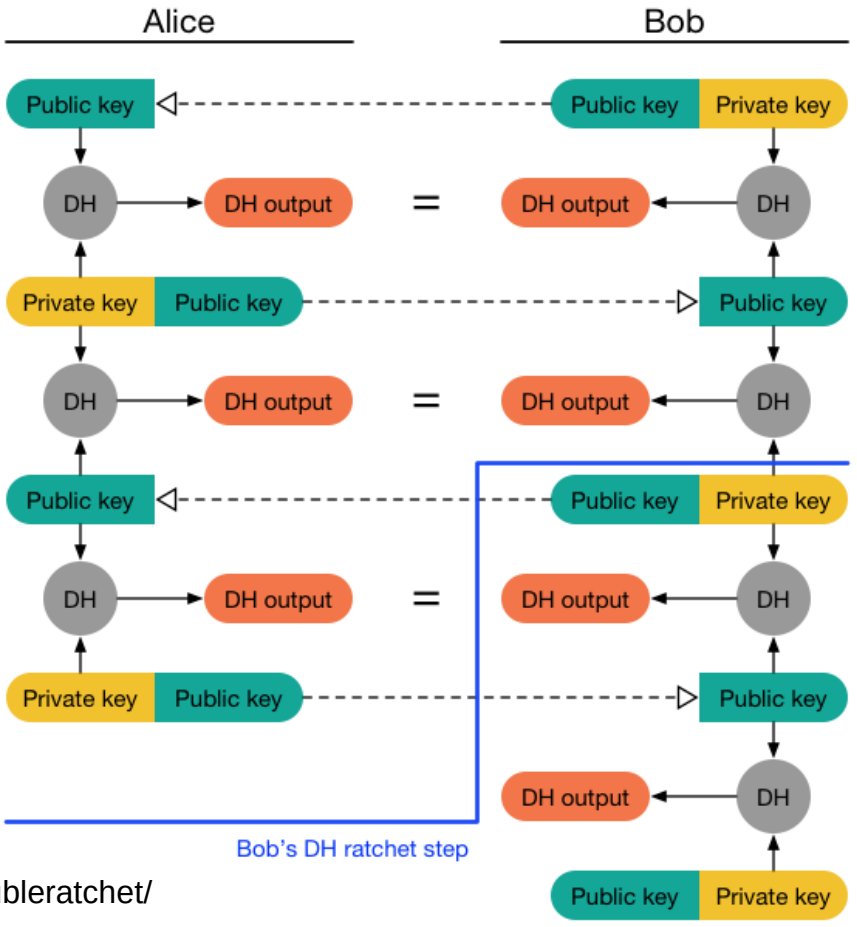
Forward secrecy

- If Alice or Bob’s key is compromised, past messages cannot be decrypted by the adversary

Ratchet in sailing...

https://www.westmarine.com/harken-snubbair-ratcheting-drum-19471861.html

Forward Secrecy (ratchet)



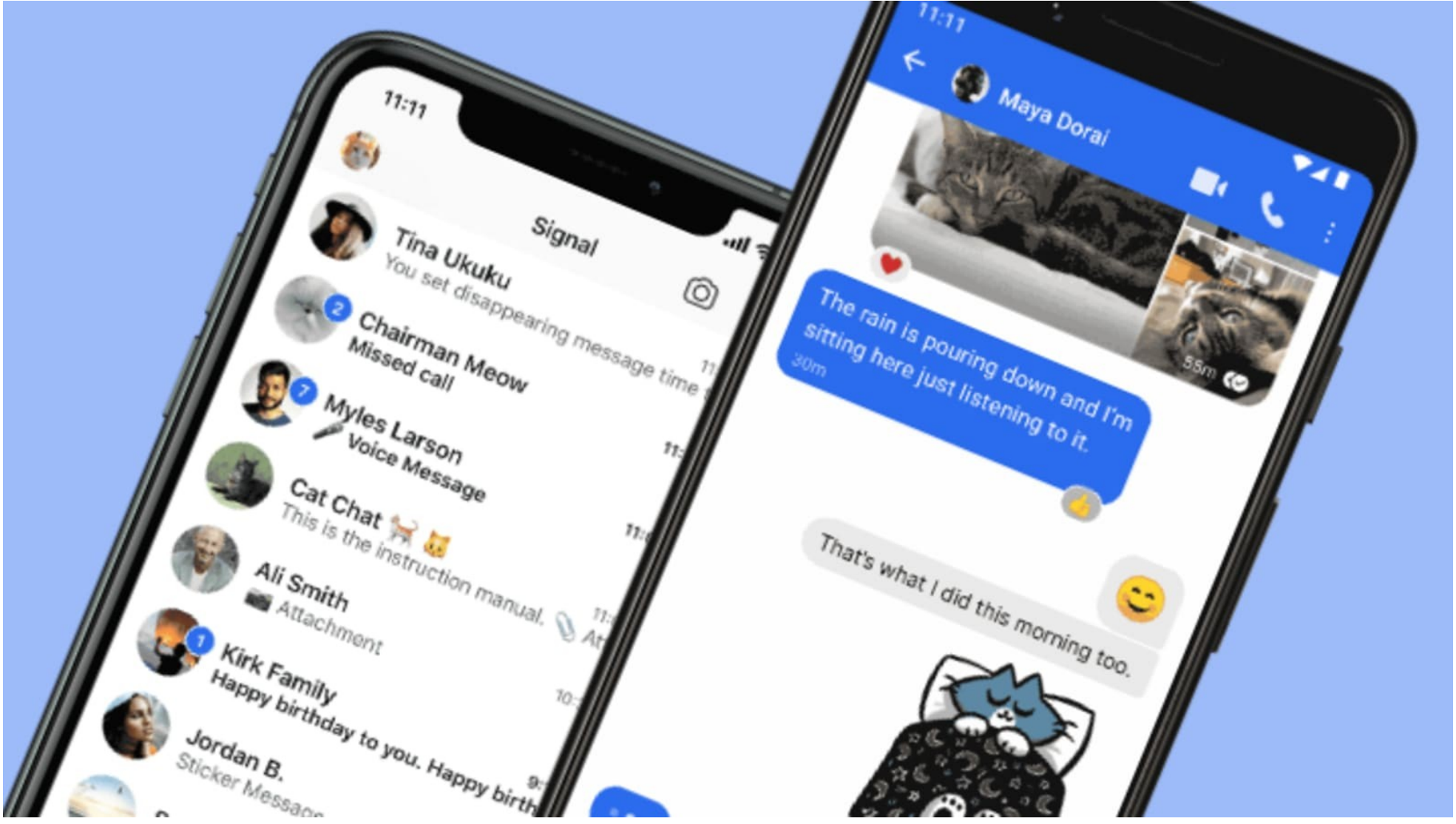
https://signal.org/docs/specifications/doubleratchet/

Future Secrecy

- *Future* secrecy is not the same as *forward* secrecy, and is in fact sometimes called *backward* secrecy
- If a private key is compromised, the attacker needs to intercept every message thereafter or else the crypto will “self heal”
- We get this for free because of the Diffie-Hellman key exchange every time we ratchet in OTR

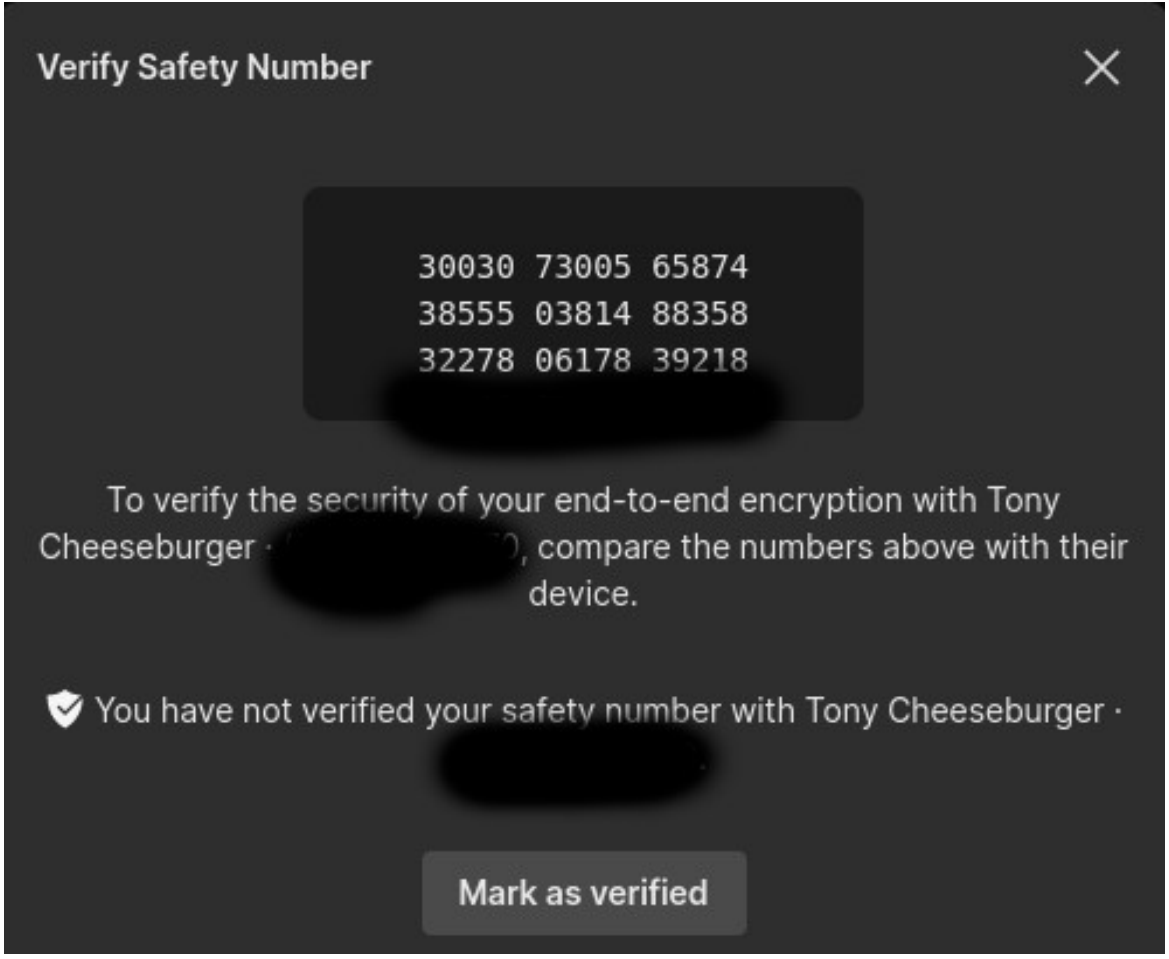
Signal

- Multiple devices, some or all can be offline for long periods of time
- Group messages



https://www.cnbc.com/2021/01/12/how-to-use-signal-instead-of-whatsapp.html

Typical authentication



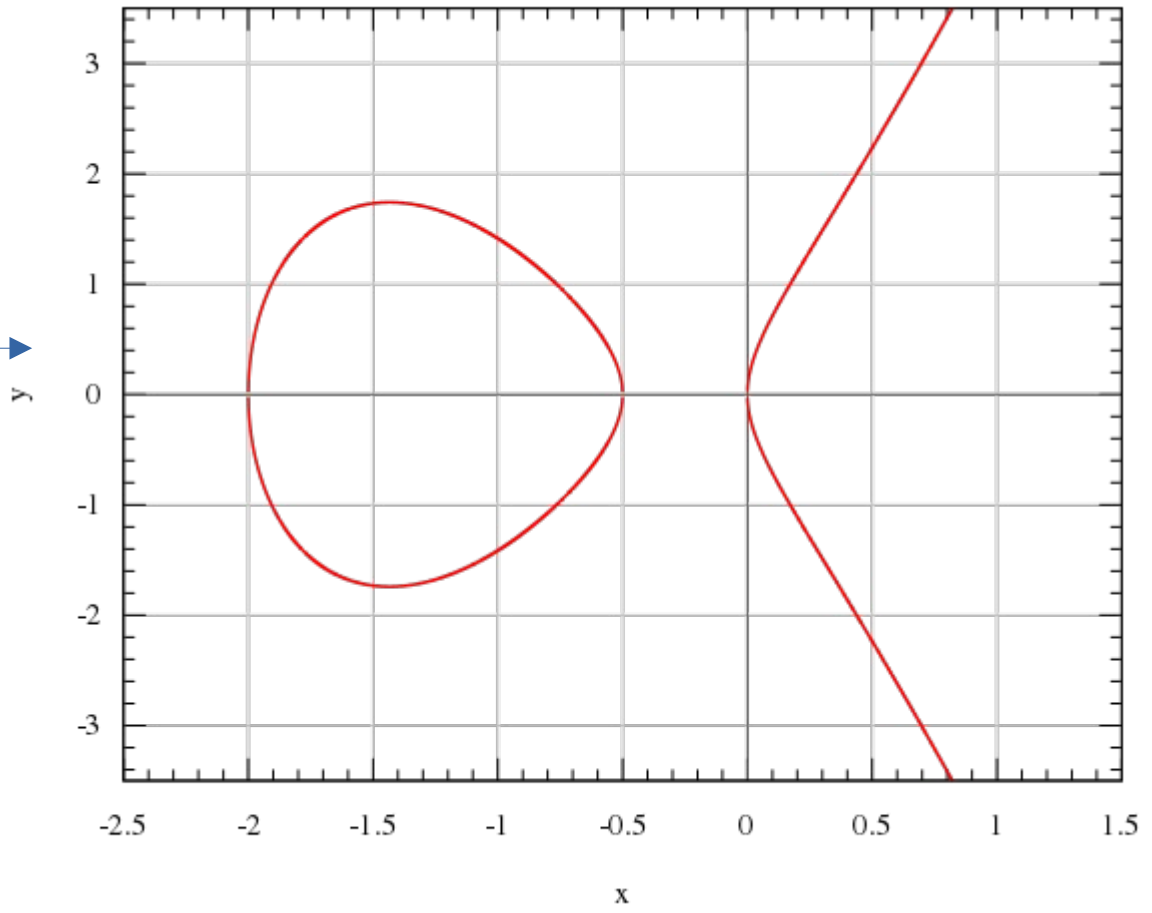
Signal encryption basics

- AES-256 in CBC mode
  - Why not a stream cipher?
- HMAC-256 with SHA-256 (SHA-2)
- Curve25519 for key exchange and signatures

The following about ECC is just FYI, you will not use it for an assignment or be tested on it this semester…

Elliptic Curve

https://commons.wikimedia.org/wiki/File:Montgomery_curve2.svg



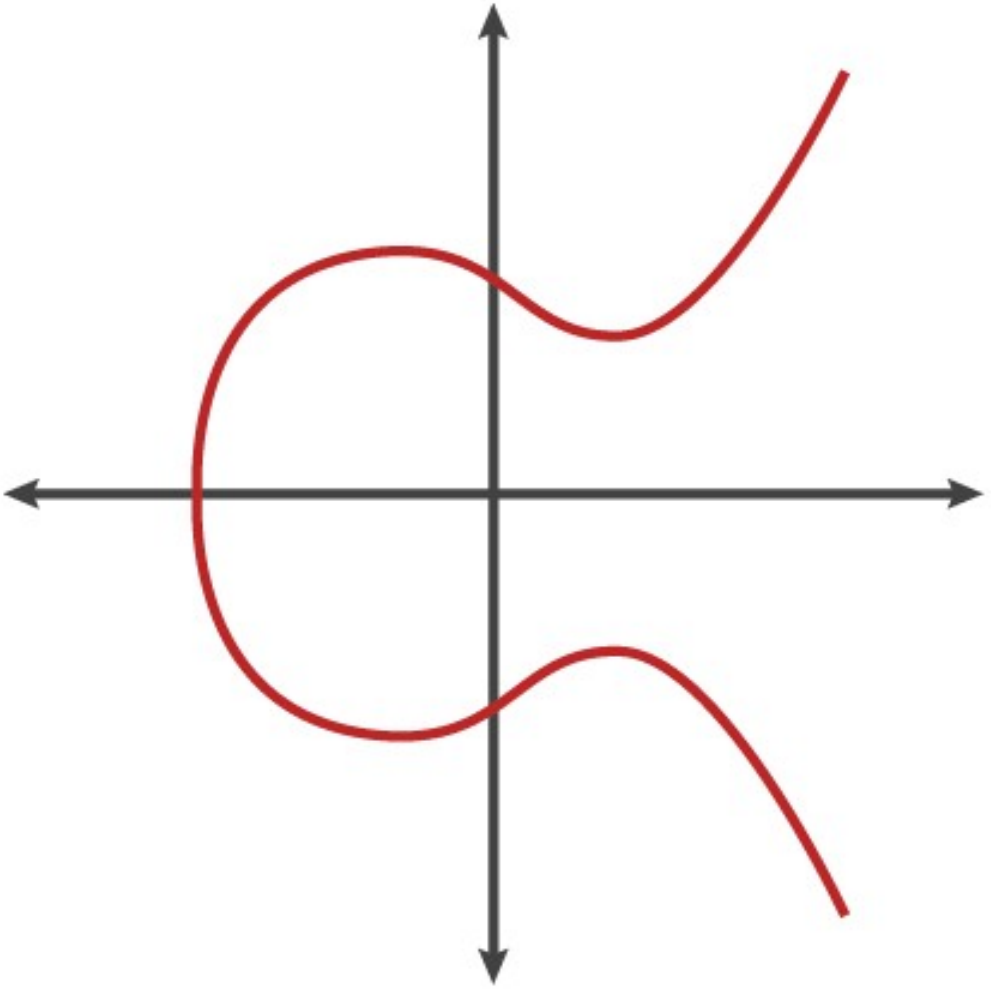
ECC background

- “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

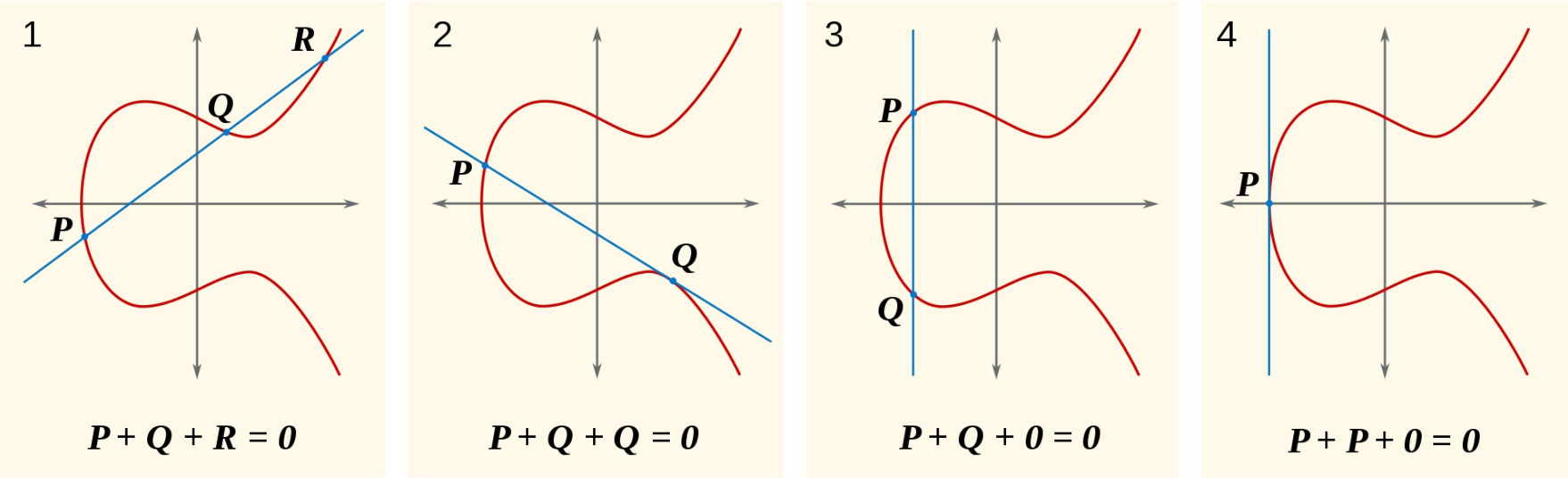
$$y^2 = x^3 + ax + b$$

Following figures are from…

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

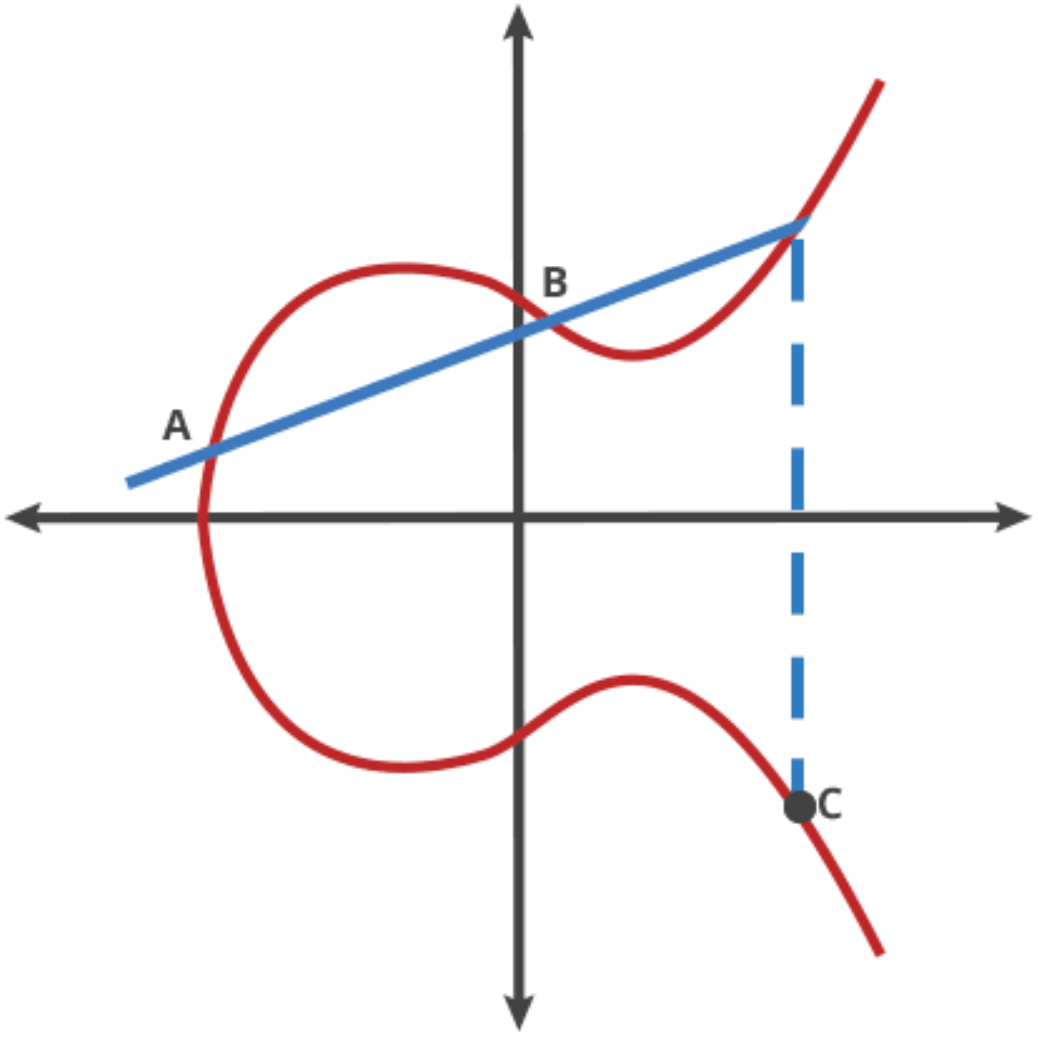


https://en.wikipedia.org/wiki/Elliptic_curve_point_multiplication#/media/File:ECClines.svg



O is point at infinity, serves as identity

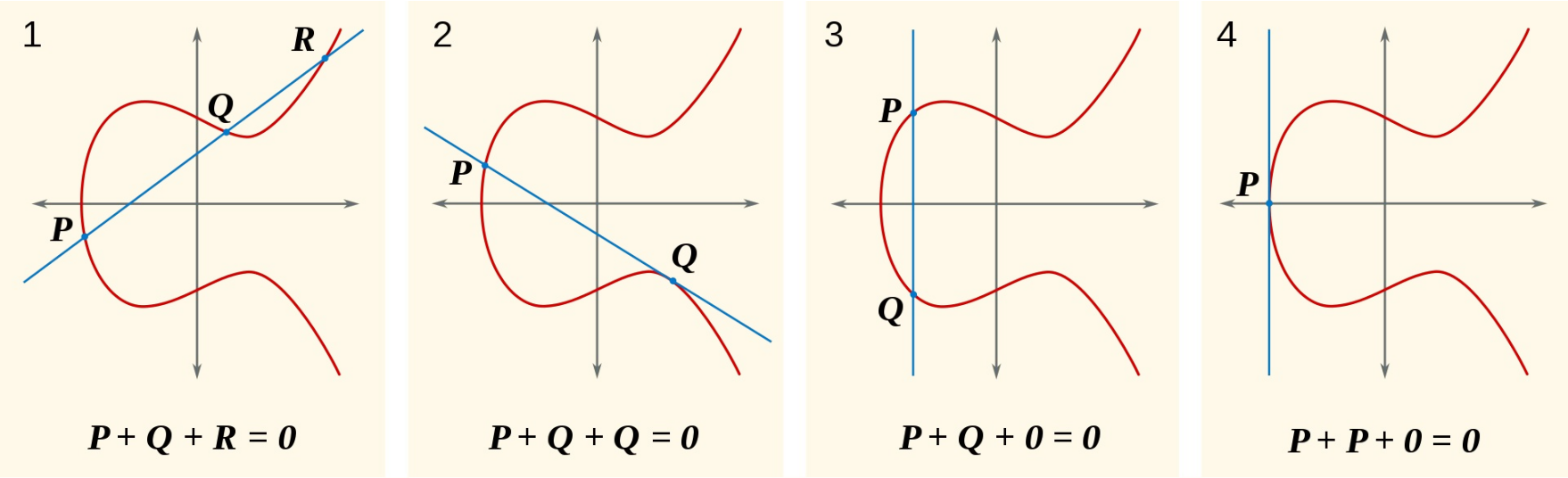
How to calculate “C = A + B”?


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

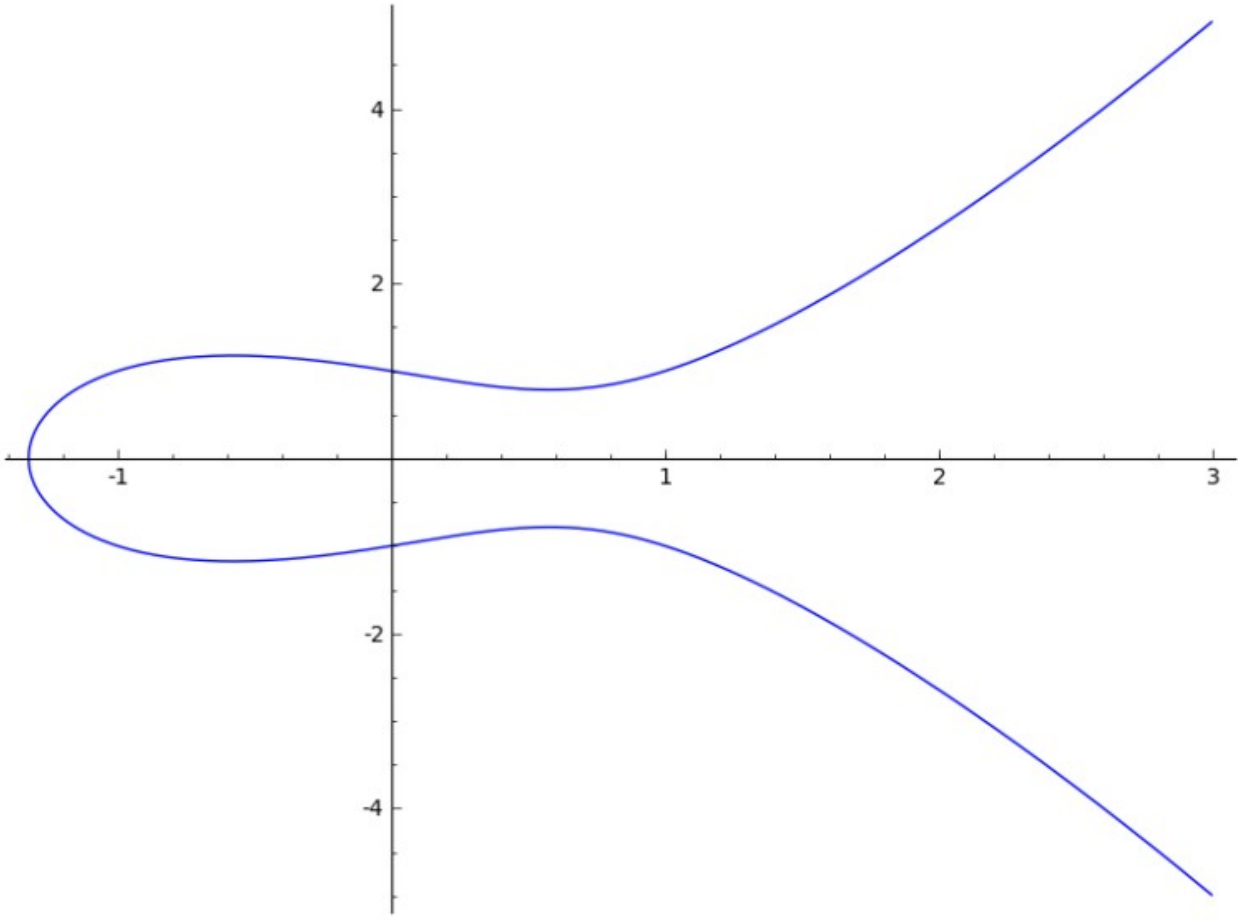
How to calculate?

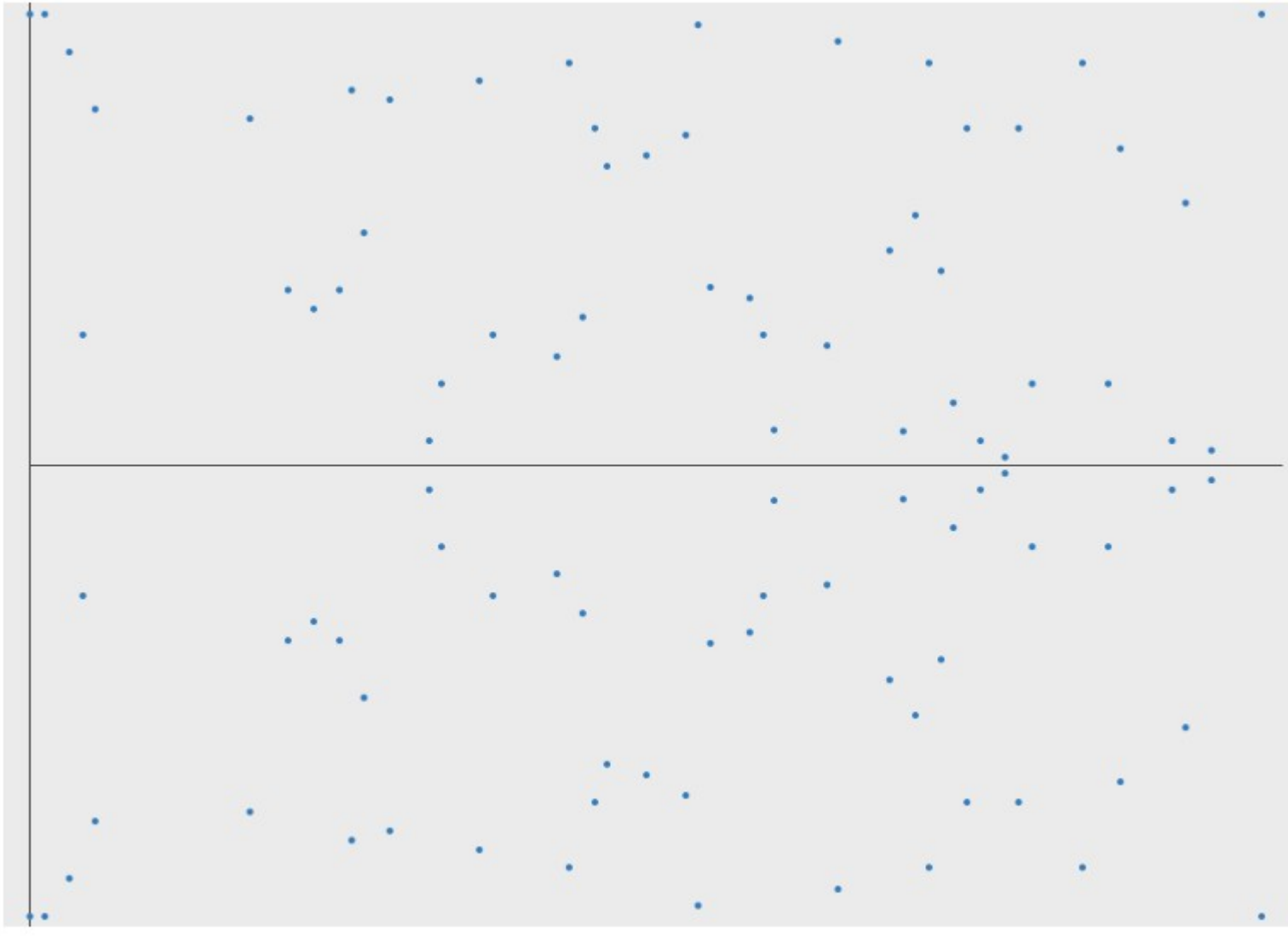
- C = -A (negation)
- C = 2A (doubling)
  - Or, C = A + A
- C = nA
  - What if n is some astronomically large number?
    - Double and add (like “square and multiply” for modular exponentiation) … Trap door function!

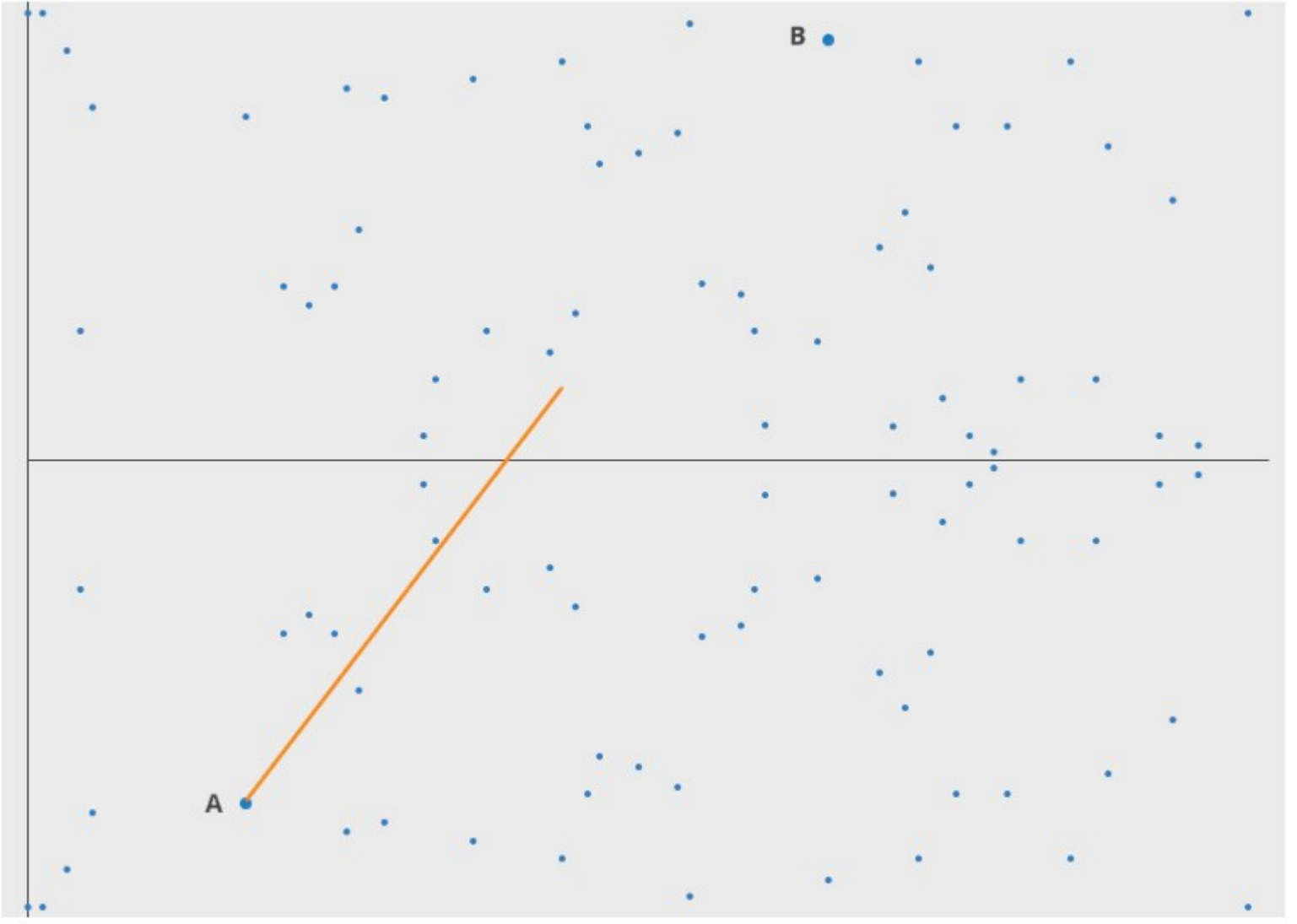
More figures stolen from…

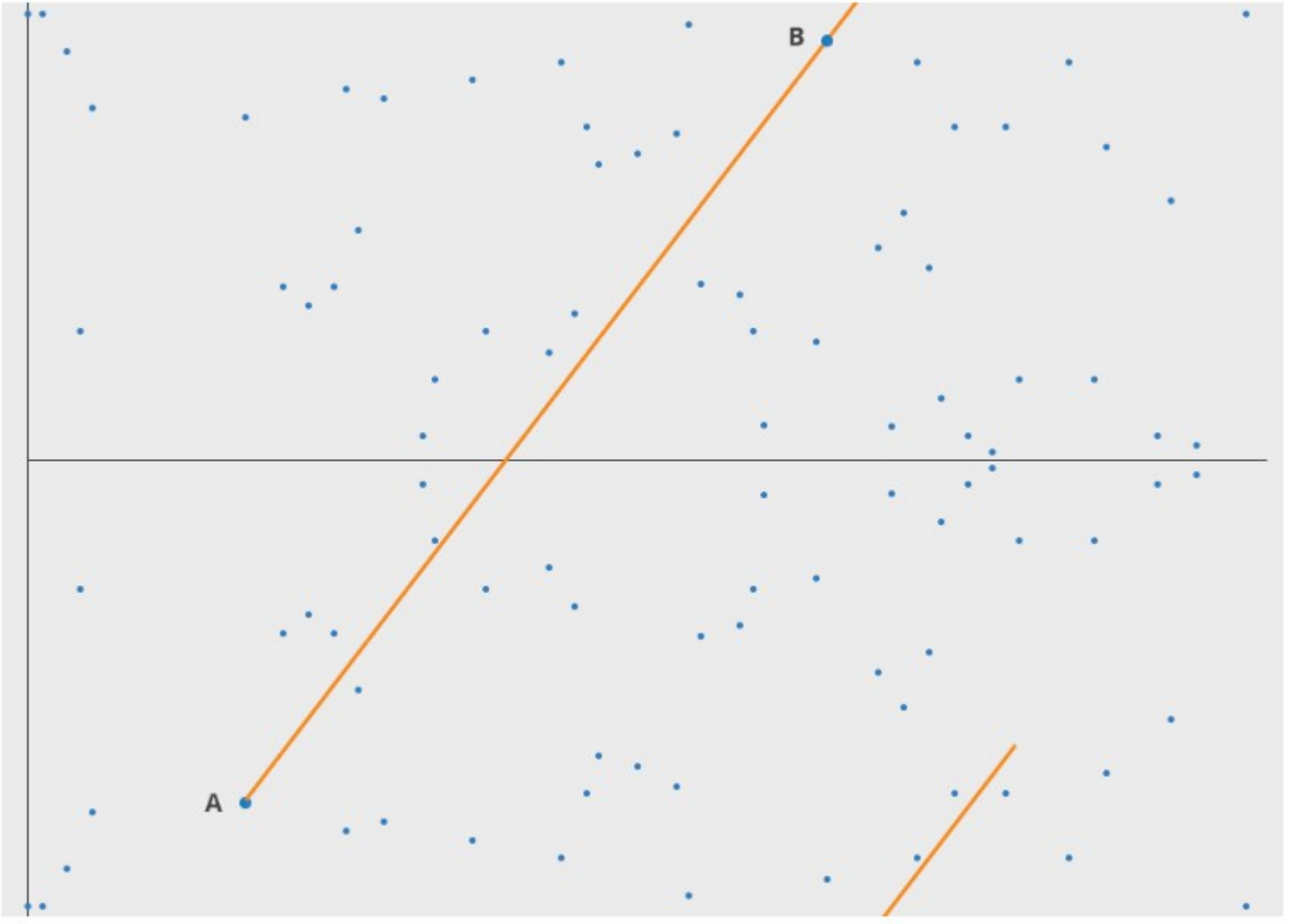
https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

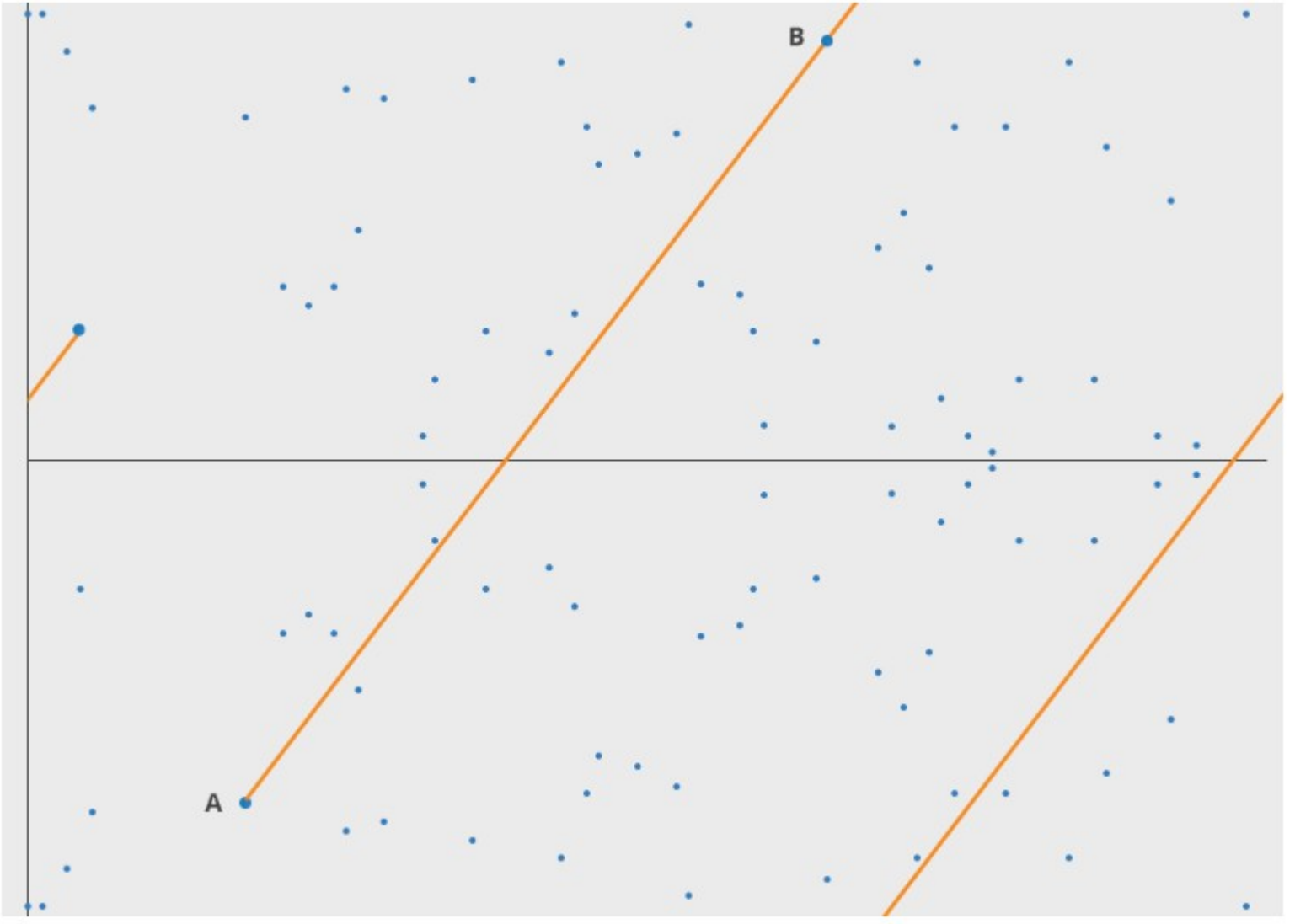
Here's an example of a curve ($y^2 = x^3 - x + 1$) plotted for all numbers:

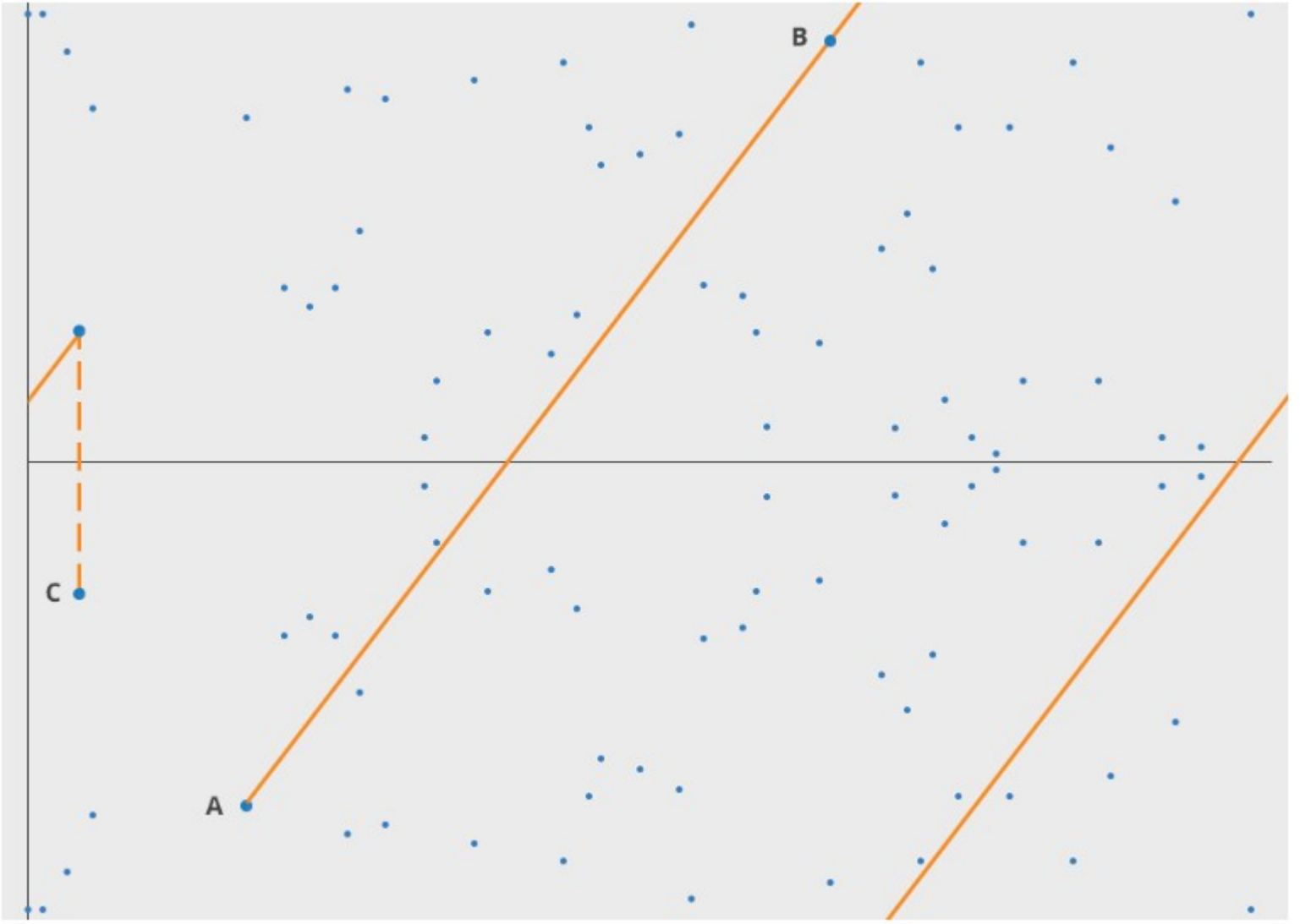





B
A


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).

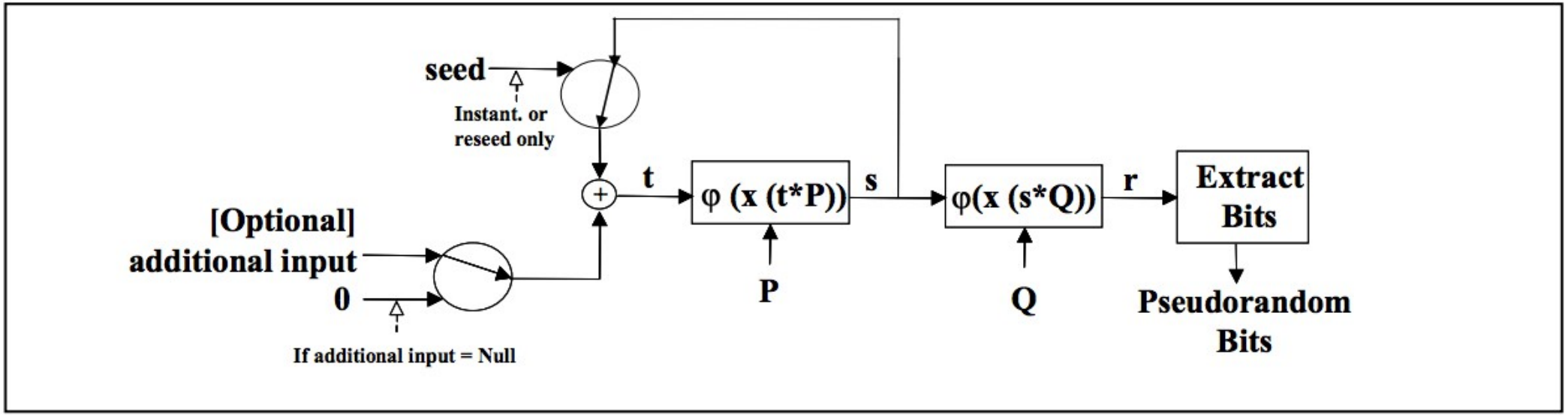
Alice computes point $(x_k, y_k) = d_A \cdot Q_B$. Bob computes point $(x_k, y_k) = d_B \cdot Q_A$.

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

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://malicious.life/crypto-ag-the-greatest-espionage-operation-ever-part-1/



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

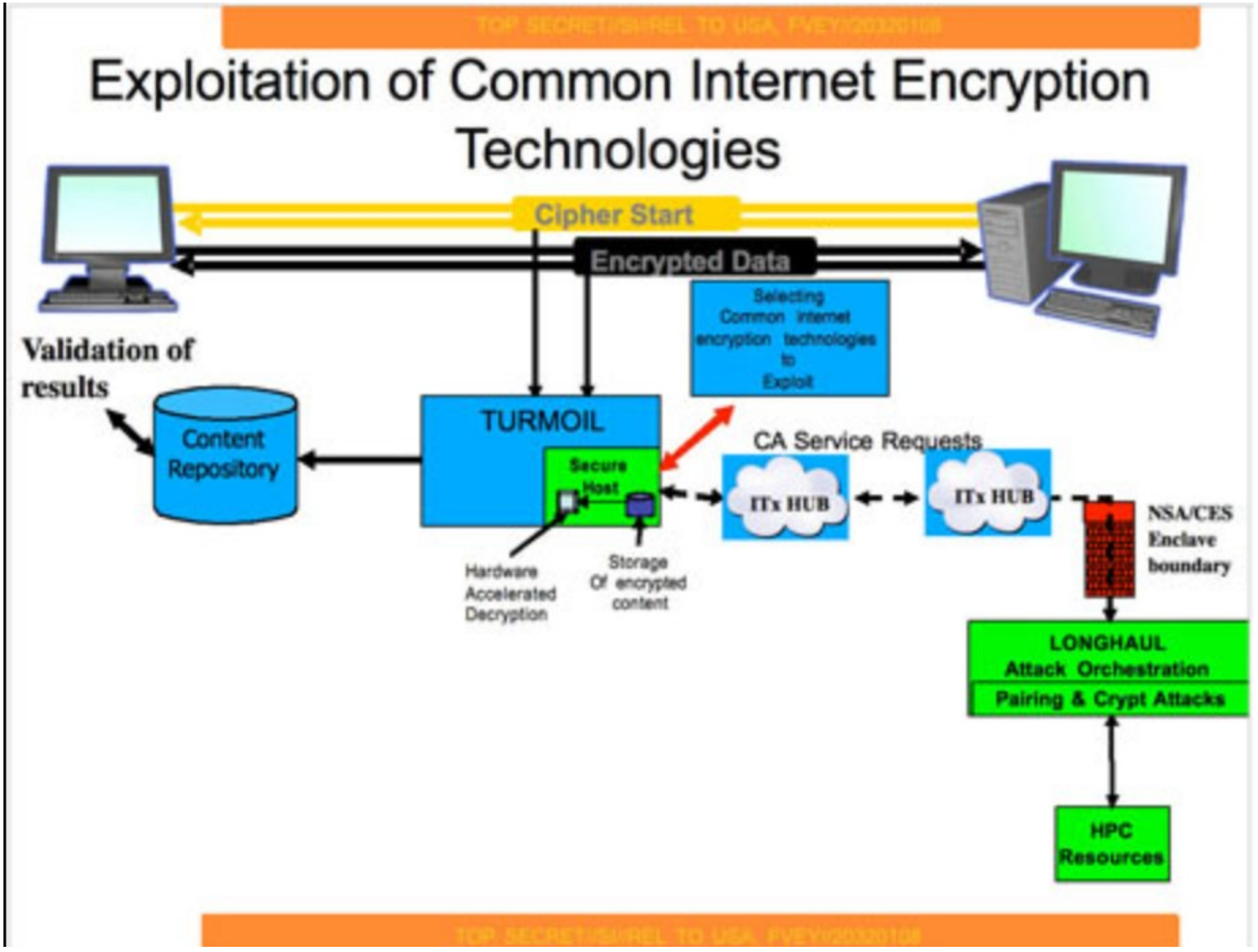
OFFICE OF ORIGIN: (U) Cryptanalysis and Exploitation Services

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

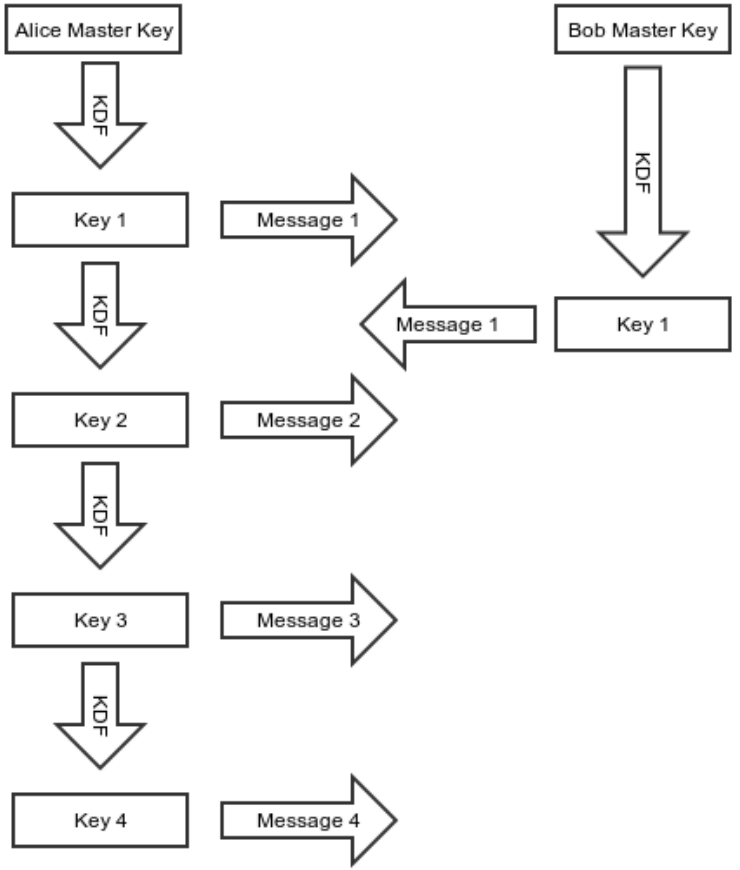
- Common choice because it’s more efficient, does key exchange and signatures
  - Not 100% immune to side channels or padding issues
  - Not quantum resistant

If you’re interested in more…

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

Back to Signal…

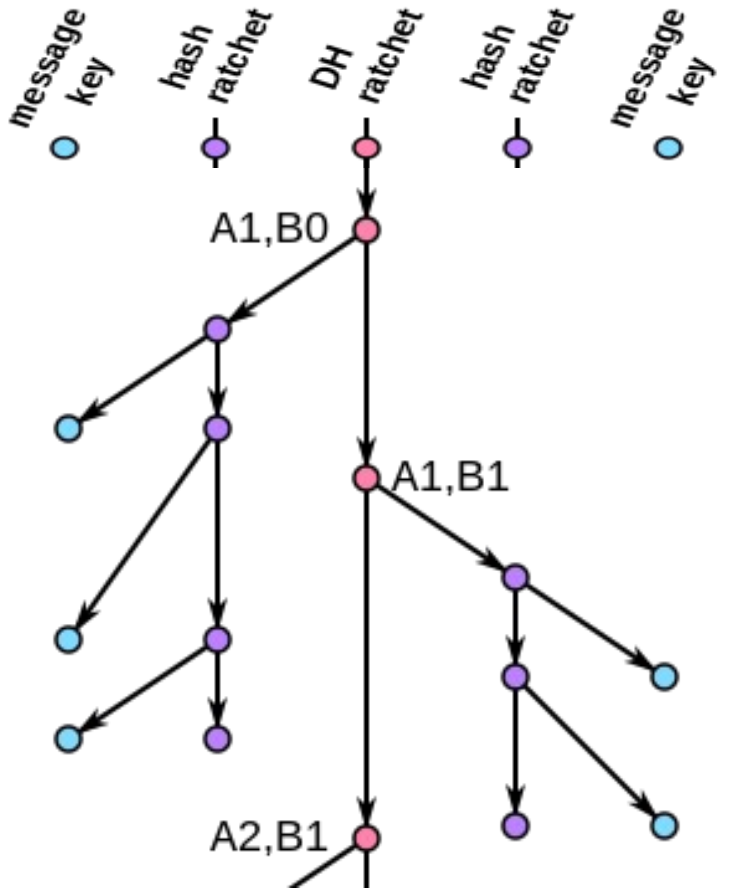
Silent Circle SCIMP ratchet



Tradeoffs

- Both have forward secrecy, but SCIMP's is better
  - In synchronous case, can ratchet and delete old key right away if Bob acknowledges it and ratchets, too
- OTR ratchet not great for multiple devices, devices that go offline
- SCIMP ratchet leaves key material around for a long time if messages are lost or out of order
- OTR ratchet "self heals", *i.e.*, future/backward sececy

Double Ratchet



https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm

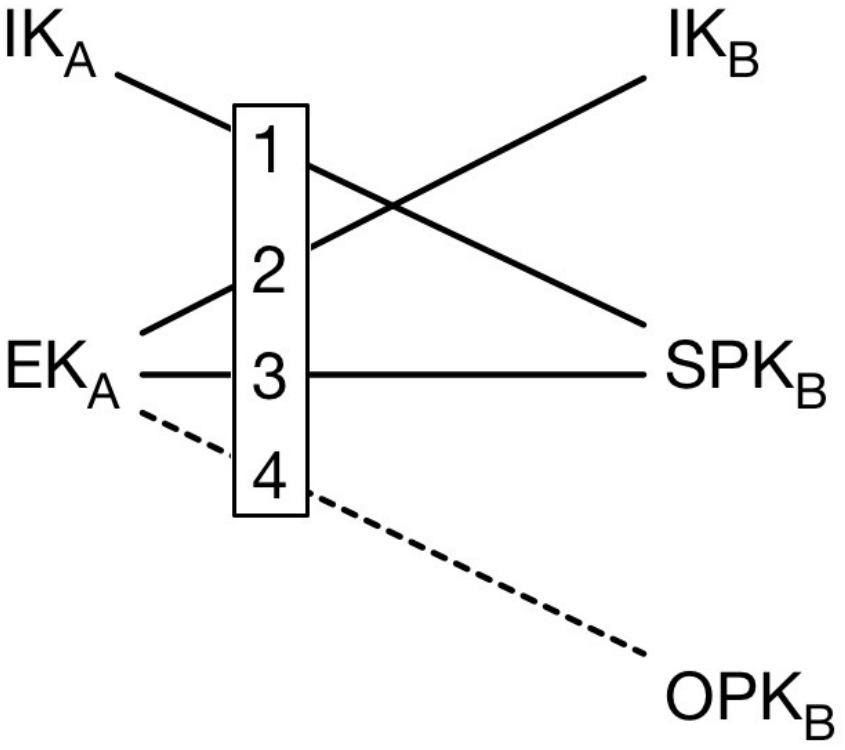
X3DH

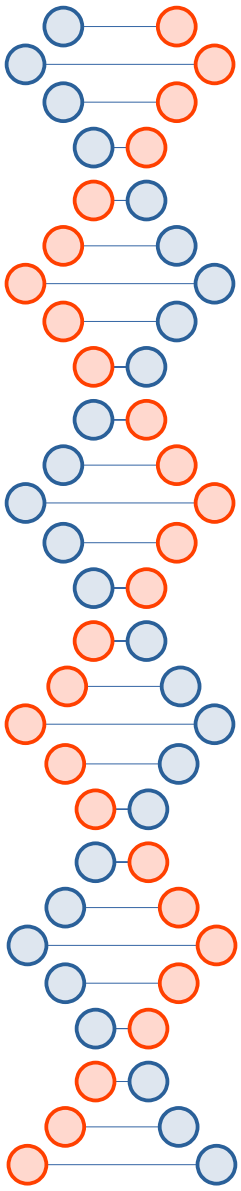
IK = Identity Key
EK = Ephemeral Key
SPK = Signed Pre-Key
OPK = One-Time Pre-Key

SK = KDF(DH1 || DH2 || DH3 || DH4)

Alice's first message encrypts the two on the left, authentication for Bob's SPK comes from the signature.

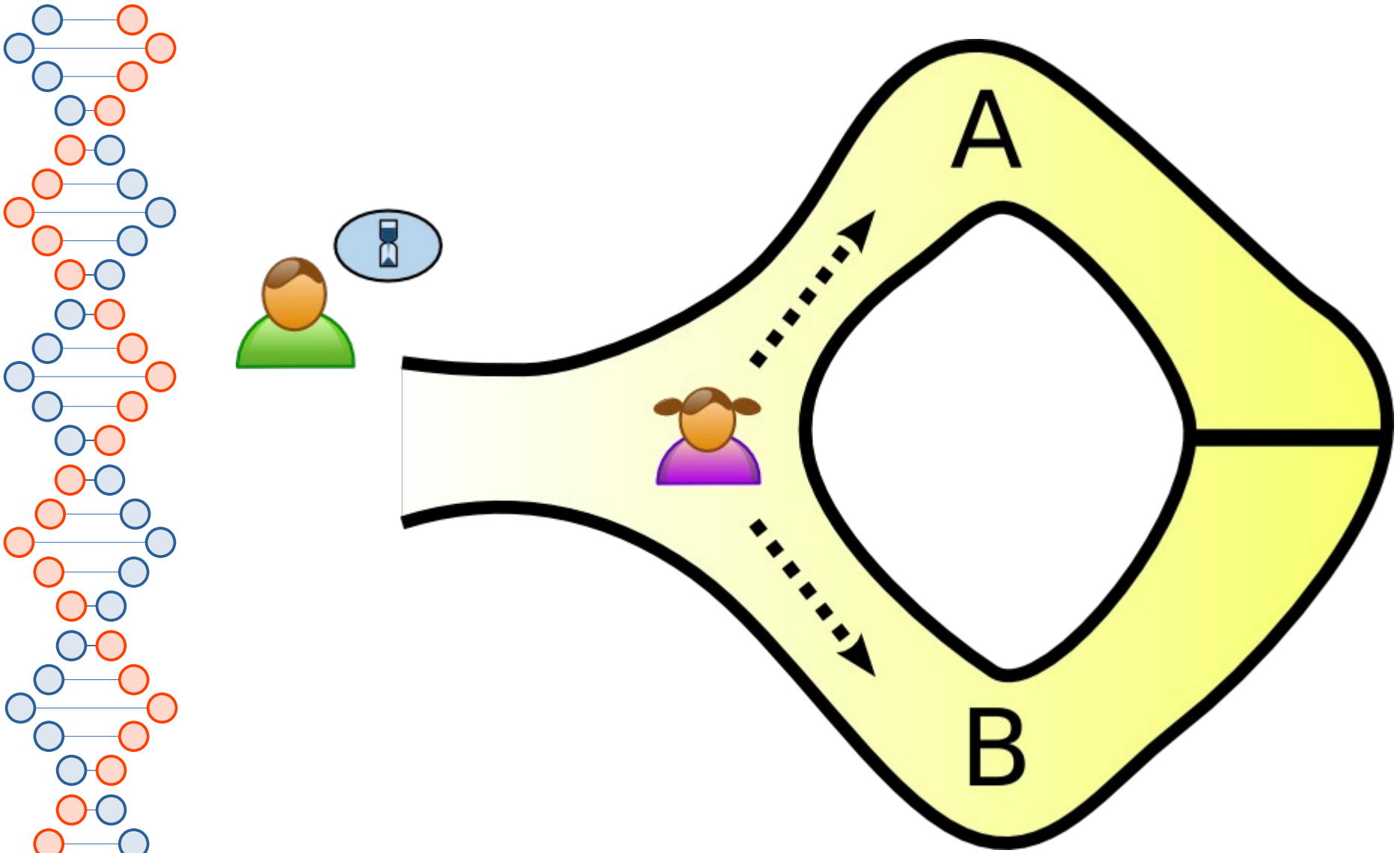
Deniability?

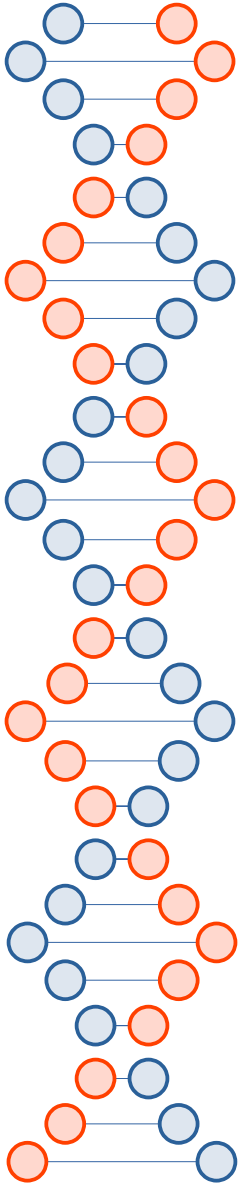


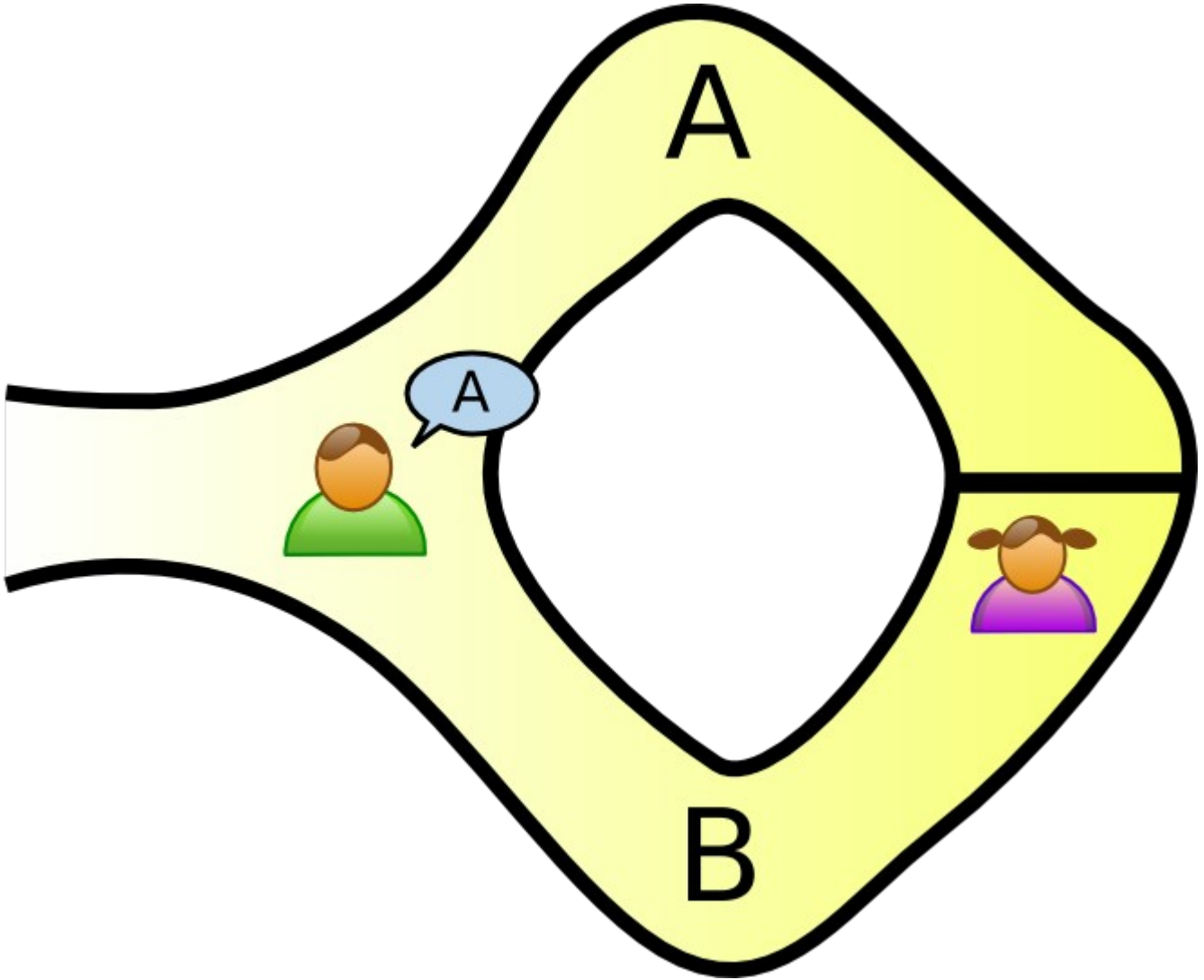


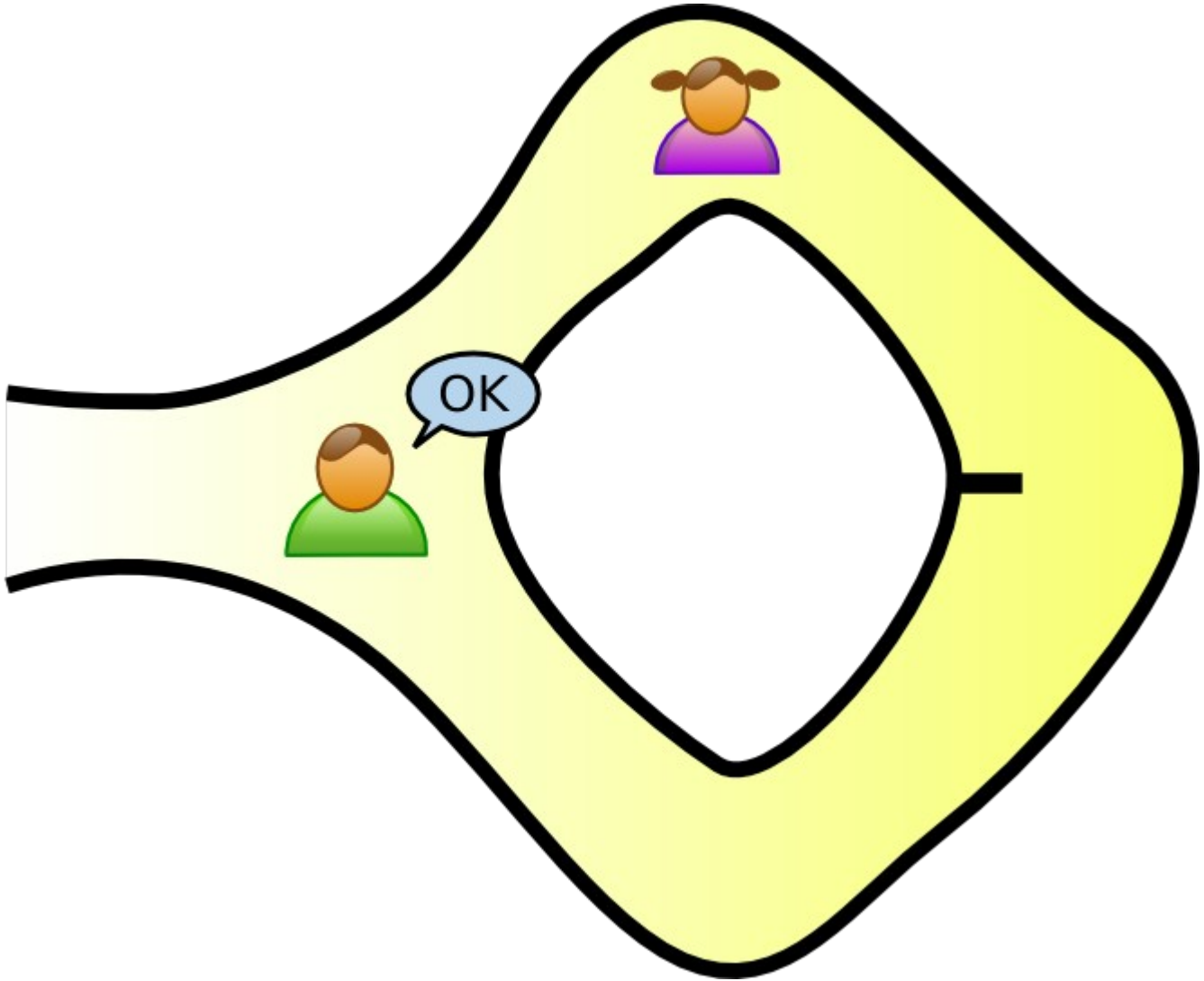
Zero Knowledge Proofs

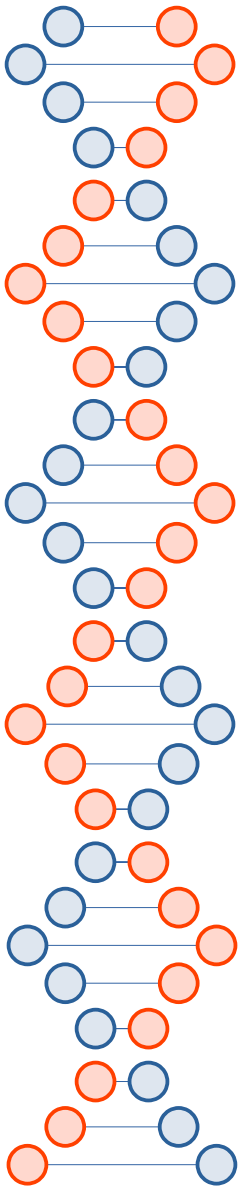
- Used for forming groups in Signal
- “a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true”
  - https://en.wikipedia.org/wiki/Zero-knowledge_proof (also the source of the following images and examples)


A
B




A
A
B


OK



Example with discrete log

- $g^x \bmod p = y$
  - Peggy wants to prove she knows x
- Each round, Peggy computes $C = g^r \bmod p$
  - She generates r randomly
- In each round, Victor can ask for…
  - **r** --or--
  - **$(x + r) \bmod (p - 1)$**

$g^{(x + r) \bmod (p - 1)} \bmod p = g^x g^r \bmod p = Cy \bmod p$

Signal Messenger Introduces PQXDH Quantum-Resistant Encryption

Sep 20, 2023 THN Encryption / Privacy

Two key differences with Signal:

- -Federated
- -No deniability

Messaging Layer Security (MLS)

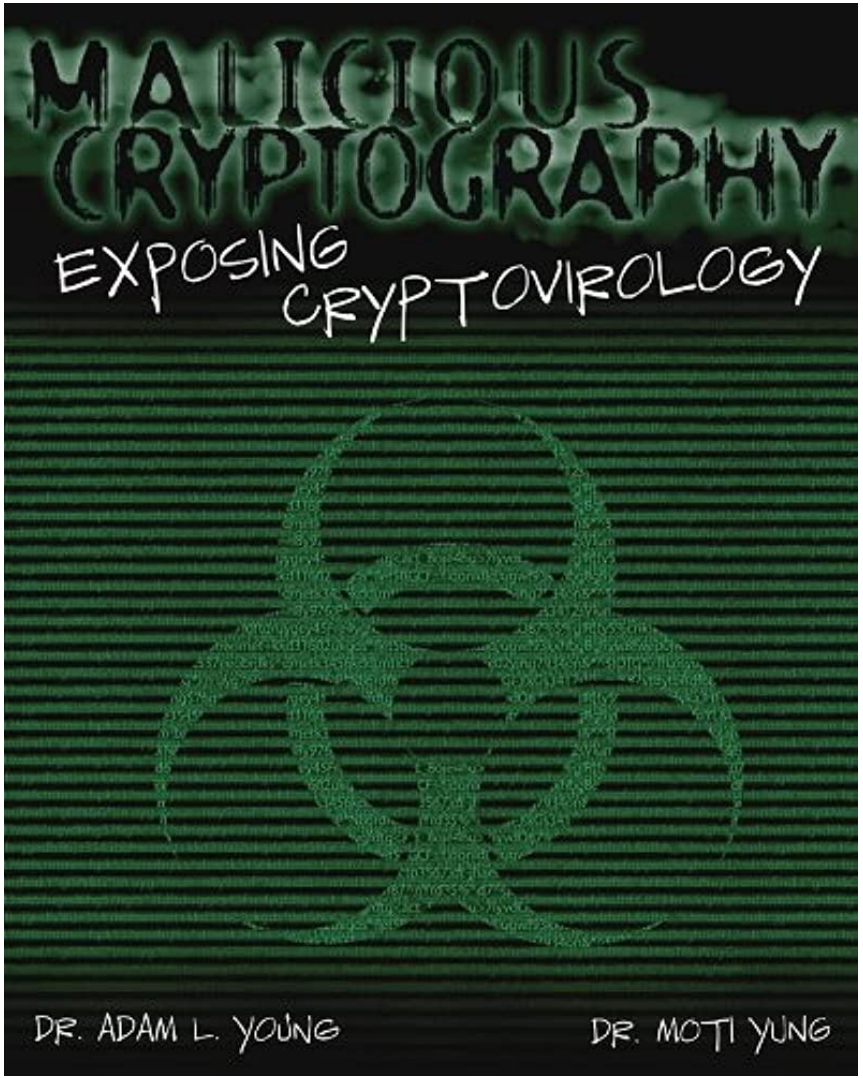
MLS

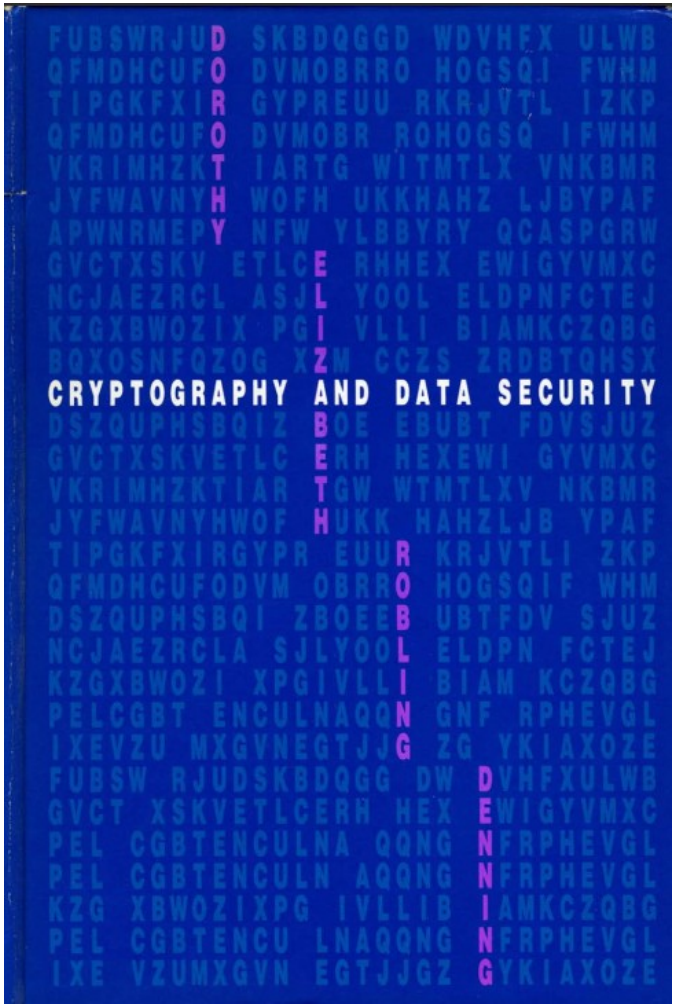
Messaging Layer Security (MLS) is an IETF working group building a modern, efficient, secure group messaging protocol.

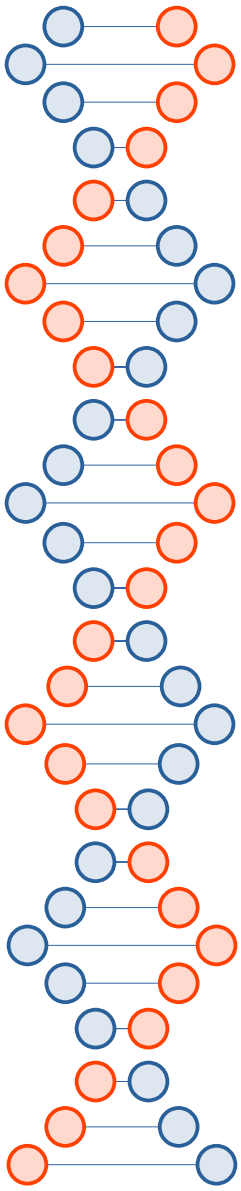
View My GitHub Profile

Resources

- https://signal.org/blog/advanced-ratcheting/
- https://en.wikipedia.org/wiki/Off-the-Record_Messaging
- https://en.wikipedia.org/wiki/Double_Ratchet_Algorithm
- https://signal.org/docs/specifications/doubleratchet/
- https://signal.org/docs/specifications/x3dh/
- https://www.youtube.com/watch?v=7WnwSovjYMs
- https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)
- https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013%E2%80%93present)
- https://thehackernews.com/2023/09/signal-messenger-introduces-pqxdh.html


MALICIOUS CRYPTOGRAPHY
EXPOSING CRYPTOVIROLOGY
DR. ADAM L. YOUNG
DR. MOTI YUNG


CRYPTOGRAPHY AND DATA SECURITY
DOROTHY
ELIZ
BETH
ROBLING
DENNING



Cryptography Engineering by Ferguson *et al.*