OTR and Signal

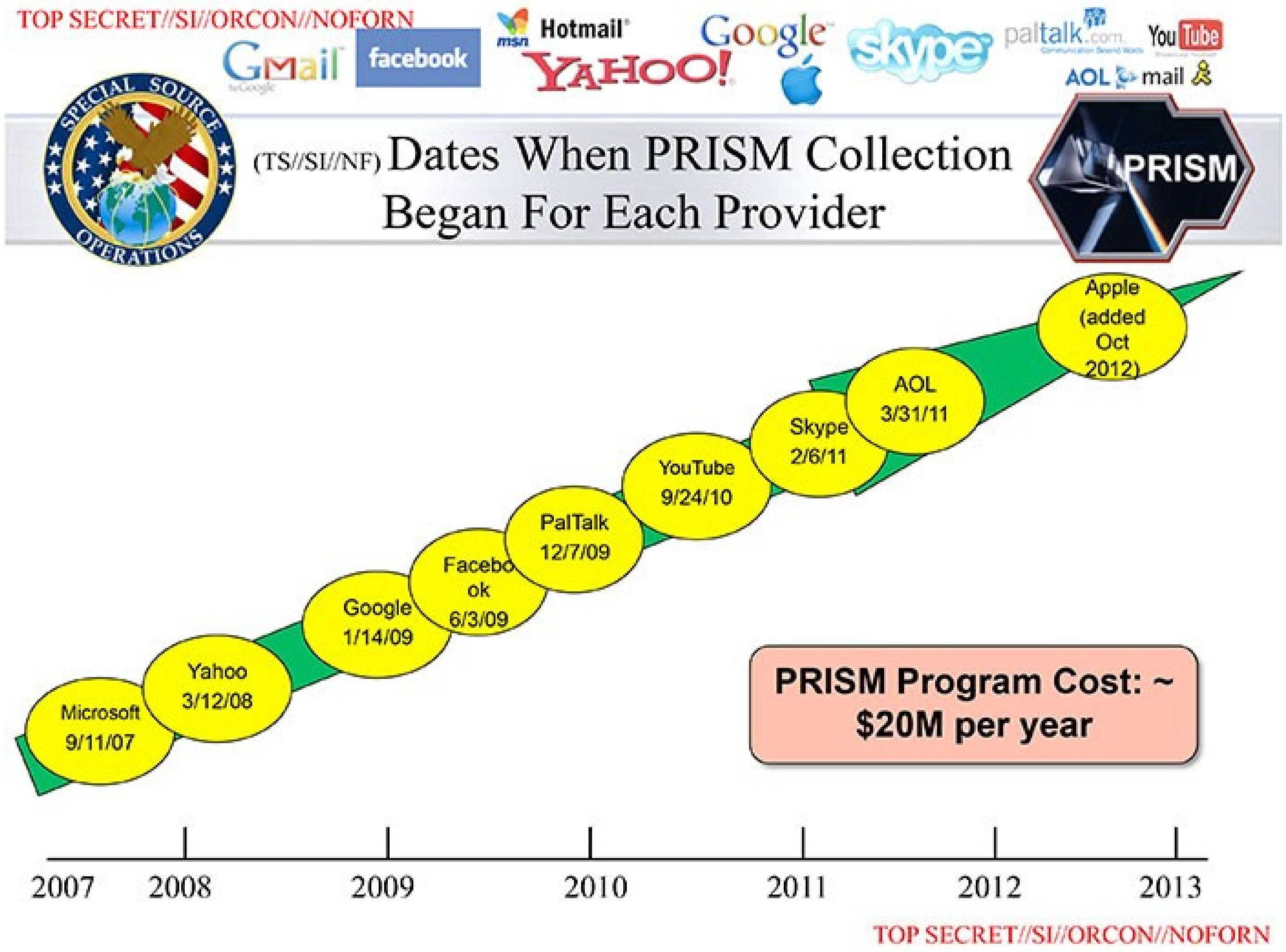
CSE 468 Fall 2025
jedimaestro@asu.edu

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- **"Off the record"**: the information is provided to inform a decision or provide a confidential explanation, not for publication.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

TOP SECRET//SI//ORCON//NOFORN



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

Microsoft 9/11/07

Yahoo 3/12/08

Google 1/14/09

Facebo ok 6/3/09

PalTalk 12/7/09

YouTube 9/24/10

Skype 2/6/11

AOL 3/31/11

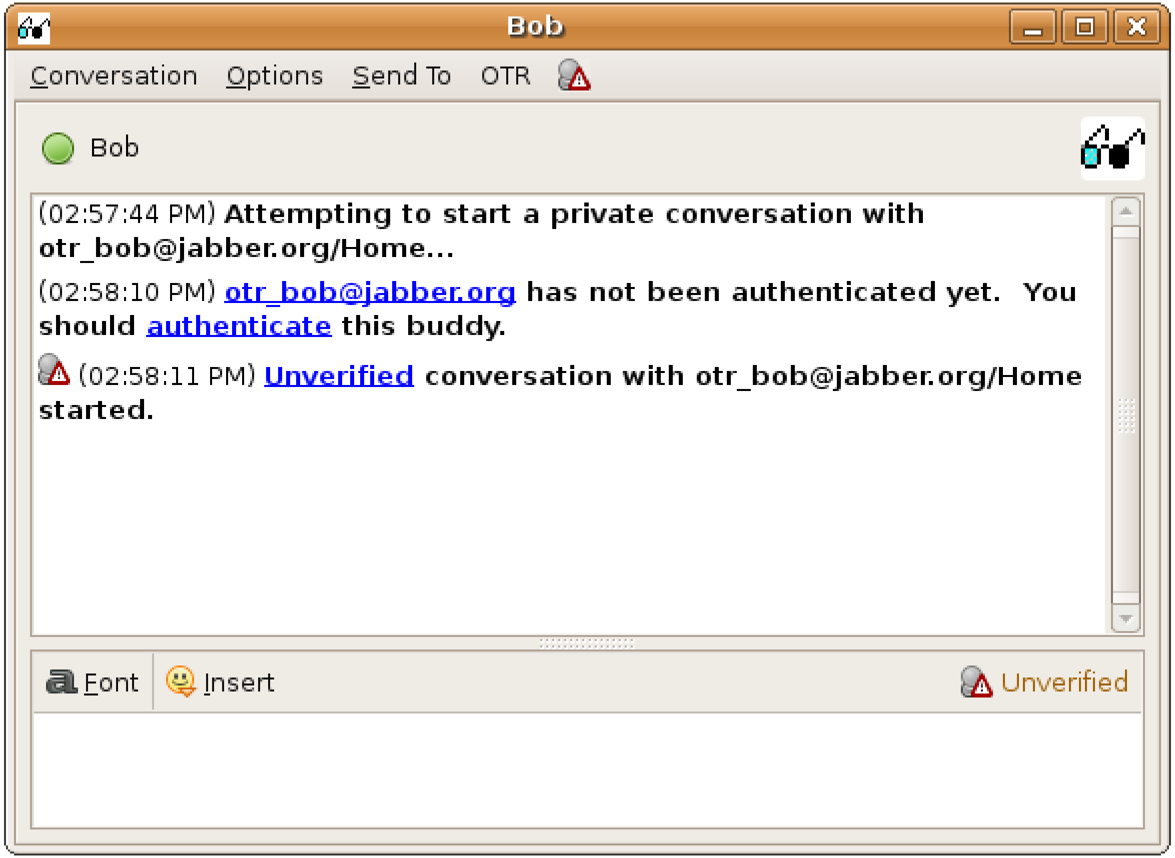
Apple (added Oct 2012)

PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN

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)



(02:57:44 PM) **Attempting to start a private conversation with otr_bob@jabber.org/Home...**

(02:58:10 PM) **otr_bob@jabber.org has not been authenticated yet. You should authenticate this buddy.**

(02:58:11 PM) **Unverified conversation with otr_bob@jabber.org/Home started.**

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)

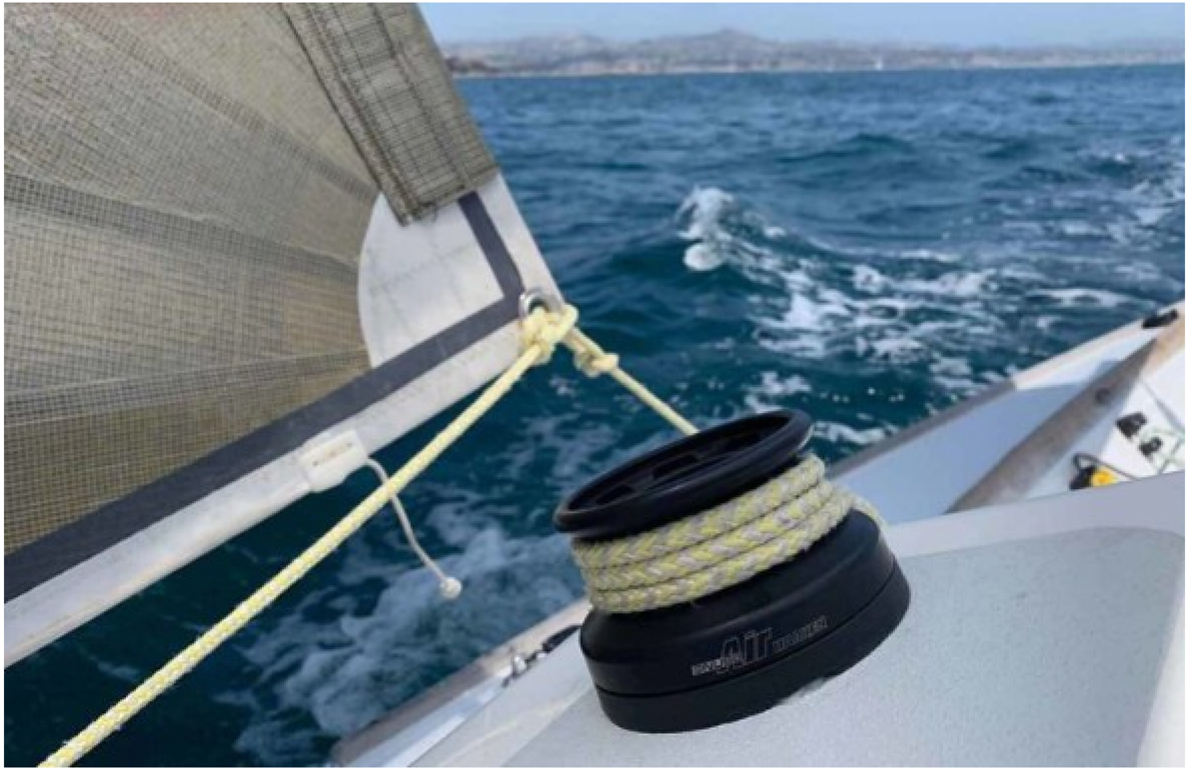
Deniable Authentication

- 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

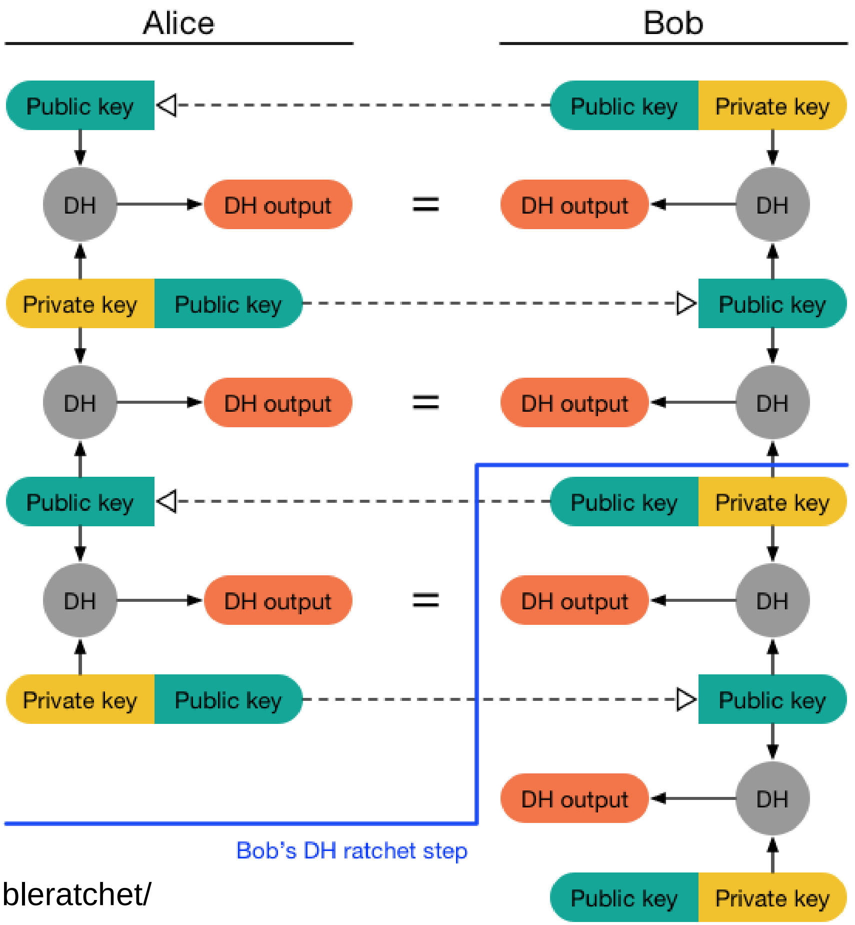
- If Alice or Bob’s key is compromised, past messages cannot be decrypted by the adversary

Ratchet in sailing...



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

Forward Secrecy (ratchet)



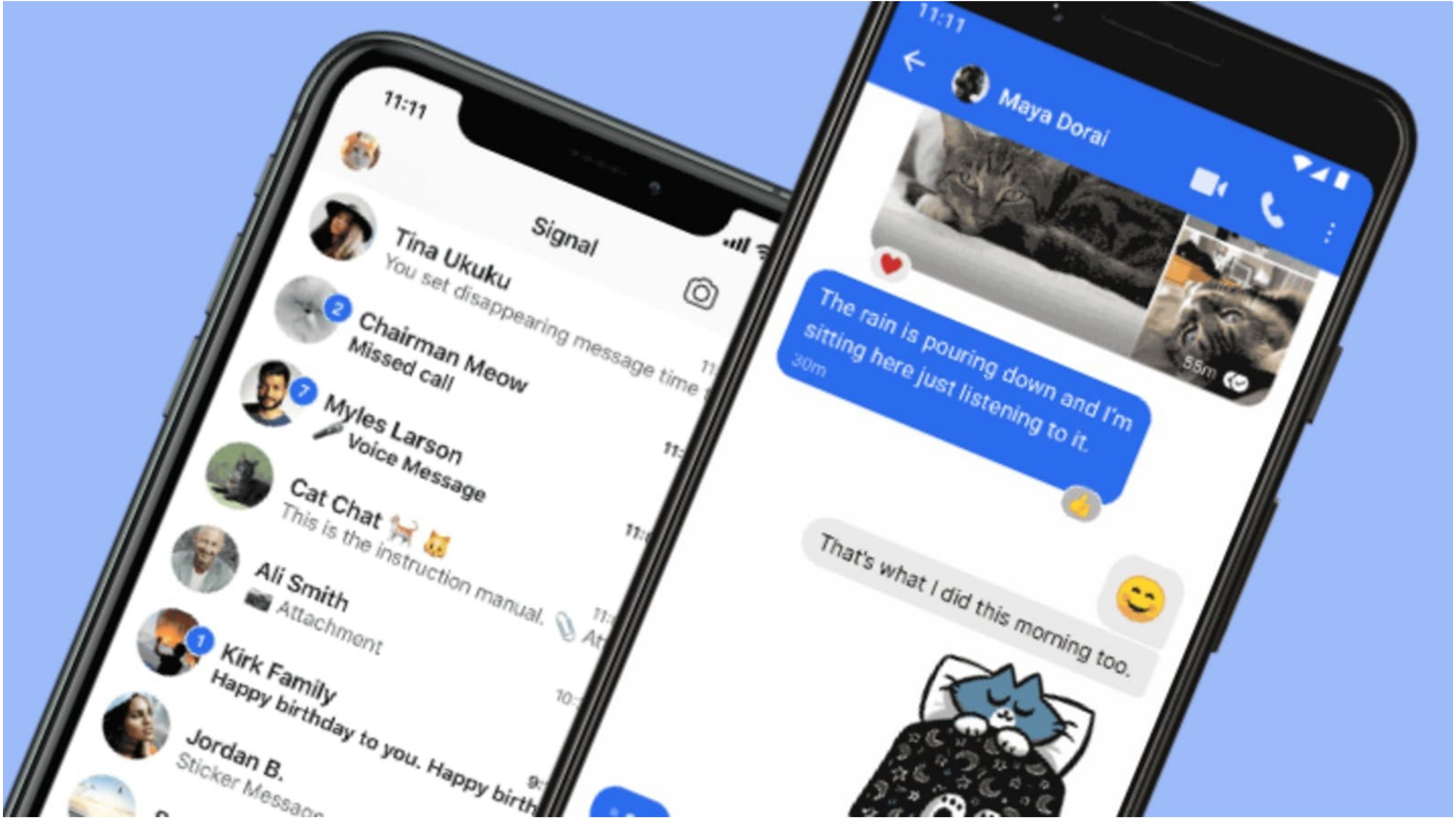
https://signal.org/docs/specifications/doubleratchet/

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



Tina Ukuku
You set disappearing message time

Chairman Meow
Missed call

Myles Larson
Voice Message

Cat Chat 🐈 🐱
This is the instruction manual.

Ali Smith
Attachment

Kirk Family
Happy birthday to you. Happy birth

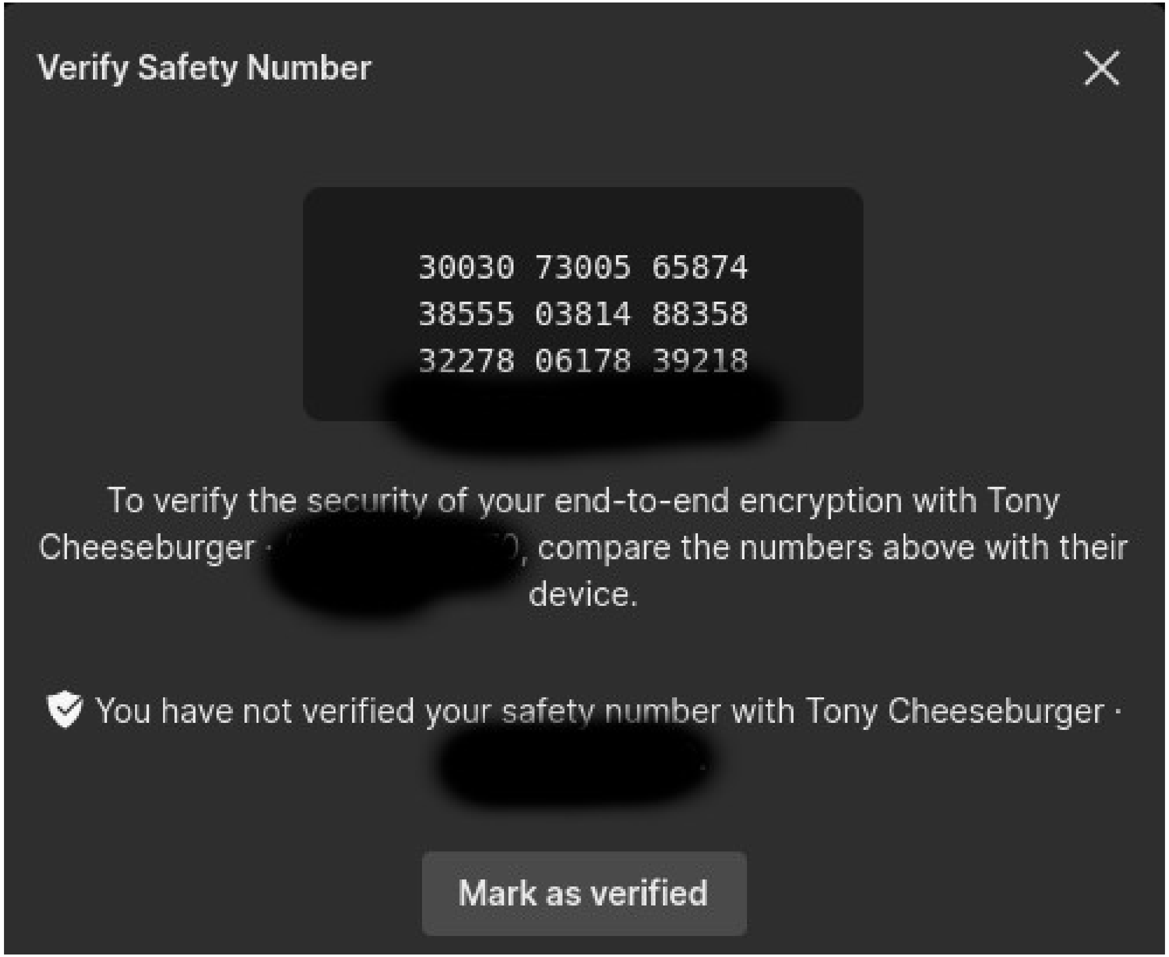
Jordan B.
Sticker Message

The rain is pouring down and I'm sitting here just listening to it.
30m

That's what I did this morning too.

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

Typical authentication



Verify Safety Number

```
30030 73005 65874
38555 03814 88358
32278 06178 39218
```

[redacted]

To verify the security of your end-to-end encryption with Tony Cheeseburger · [redacted], compare the numbers above with their device.

You have not verified your safety number with Tony Cheeseburger · [redacted]

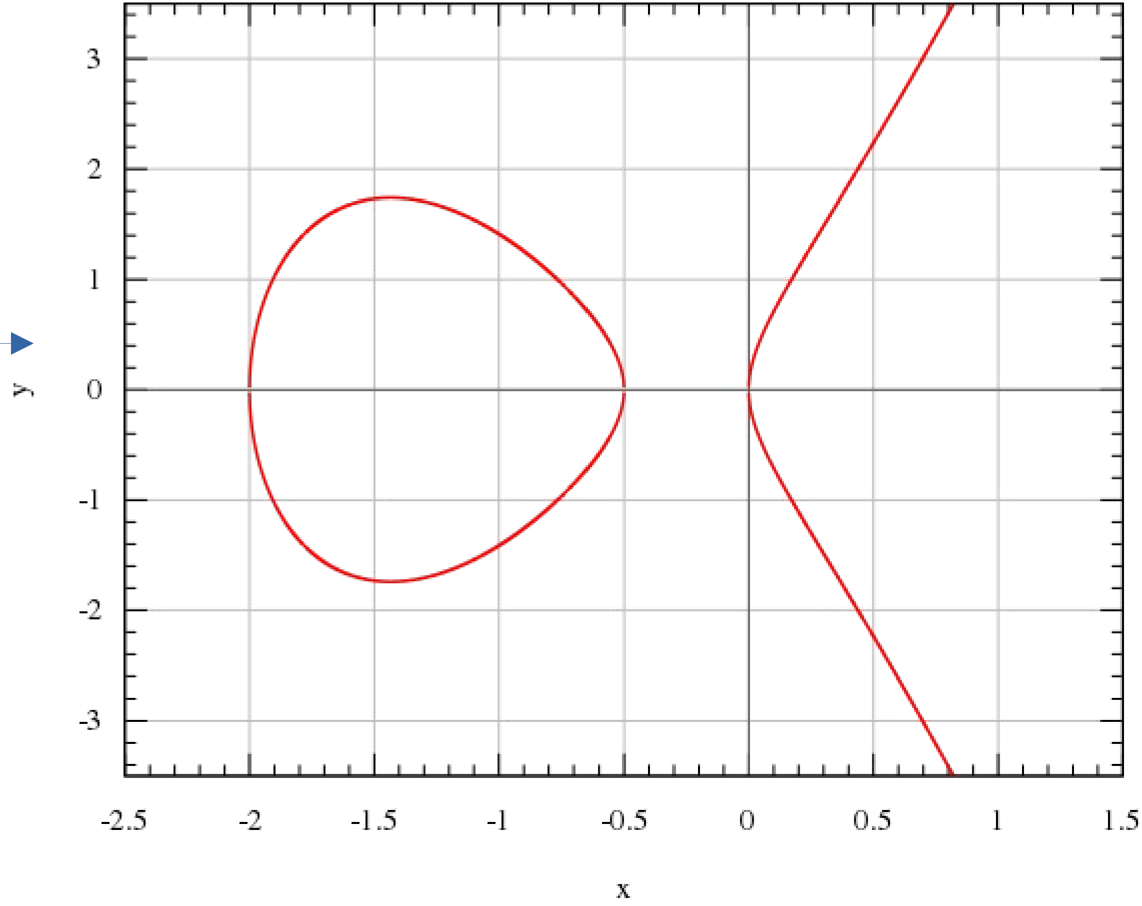
Signal encryption basics

- 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



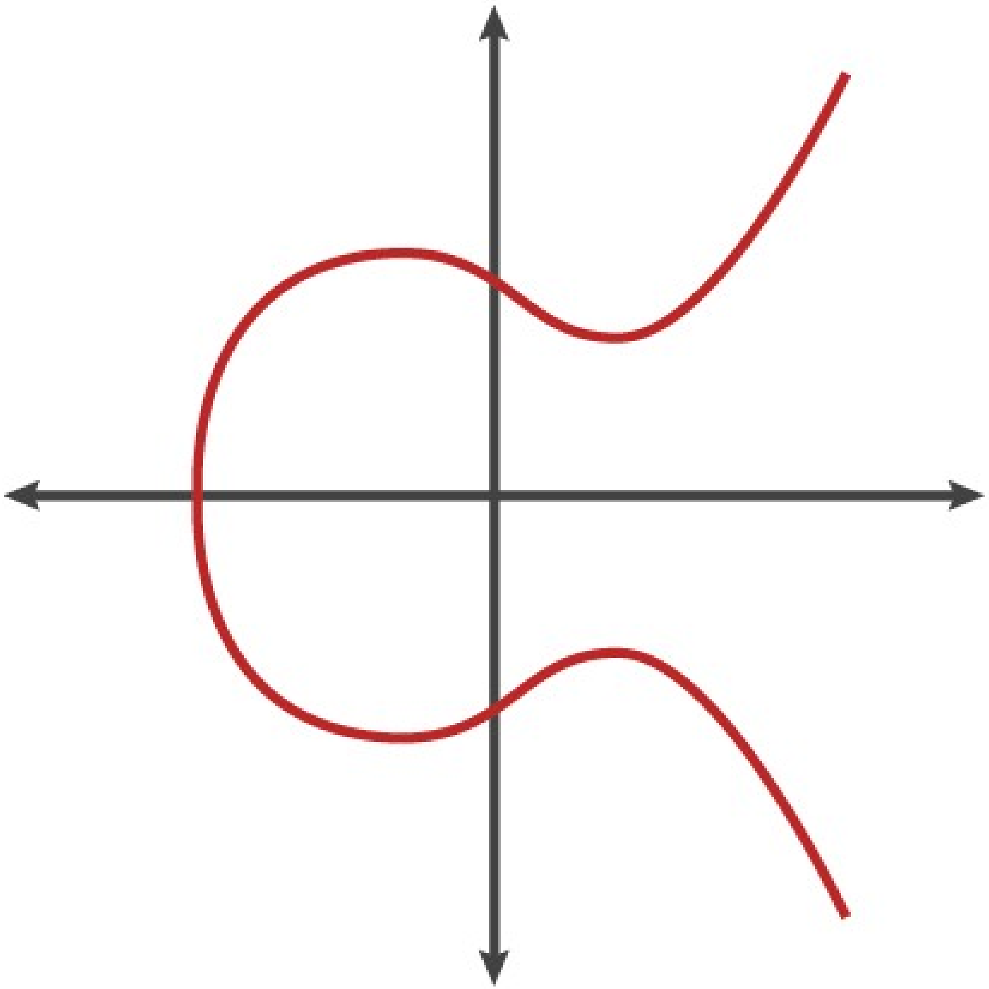
ECC background

- “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

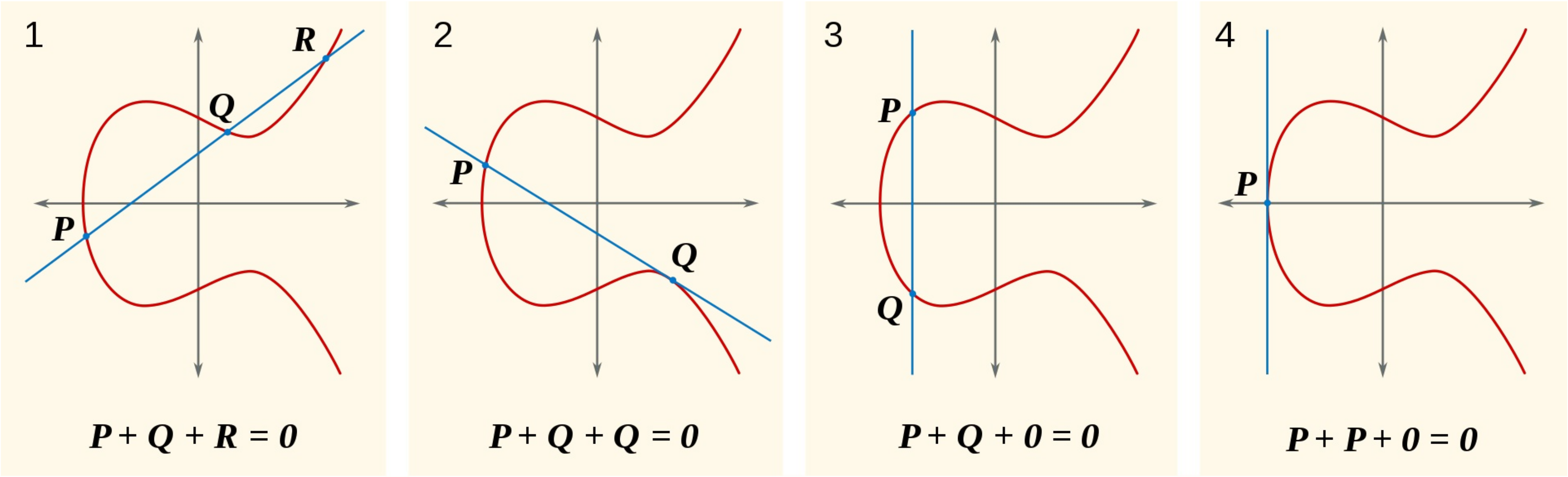
$$y^2 = x^3 + ax + b$$

Following figures are from…

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

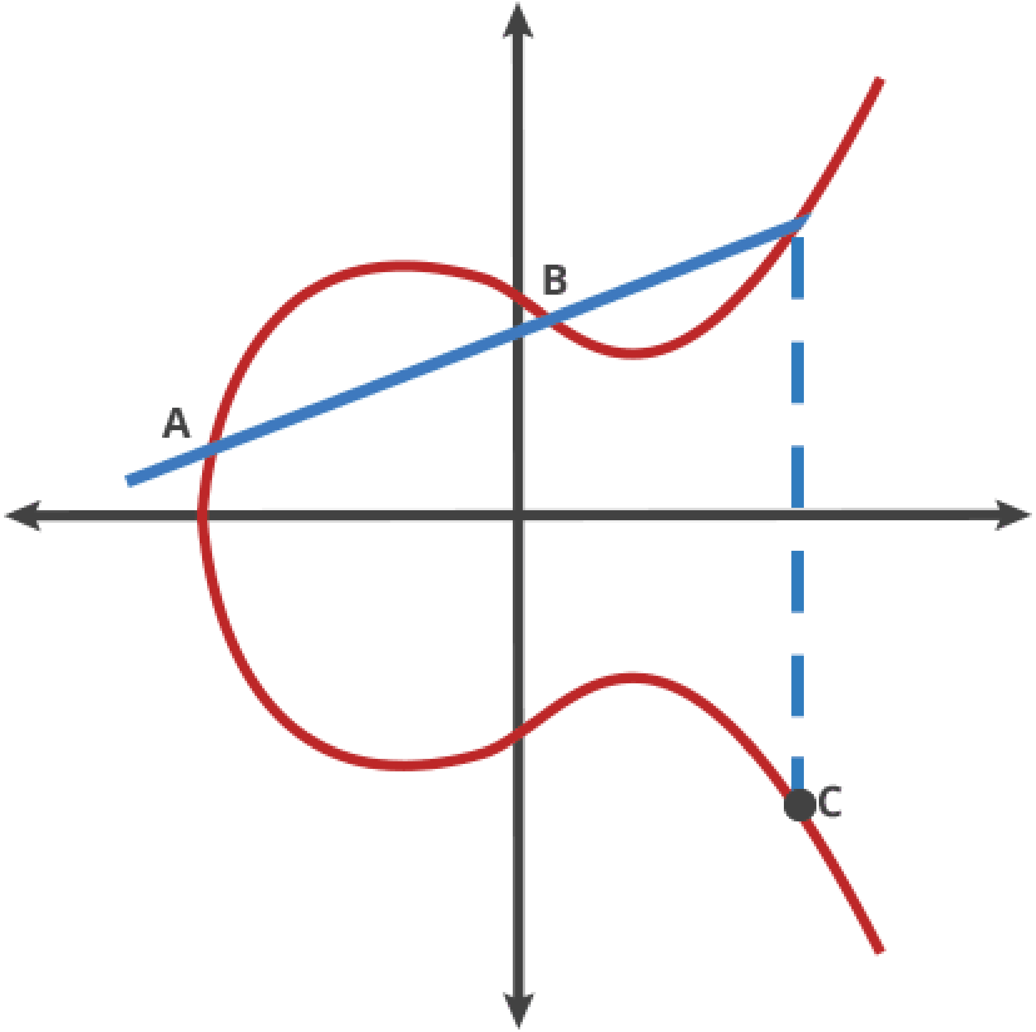


https://en.wikipedia.org/wiki/Elliptic_curve_point_multiplication#/media/File:ECClines.svg



O is point at infinity, serves as identity

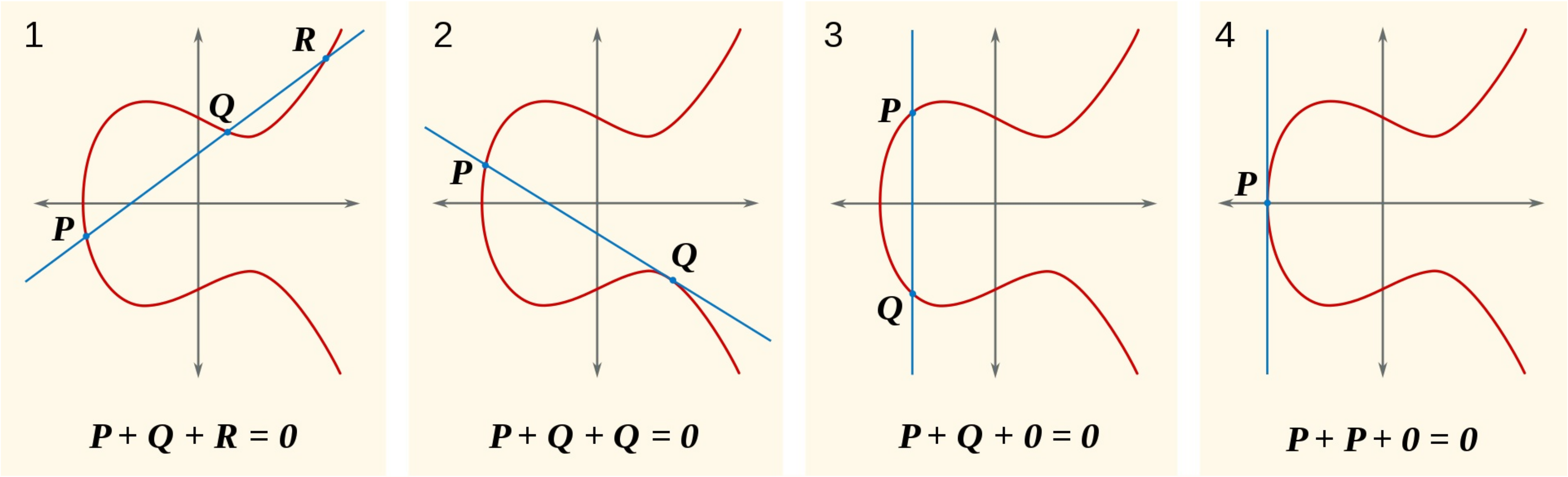
How to calculate “C = A + B”?


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

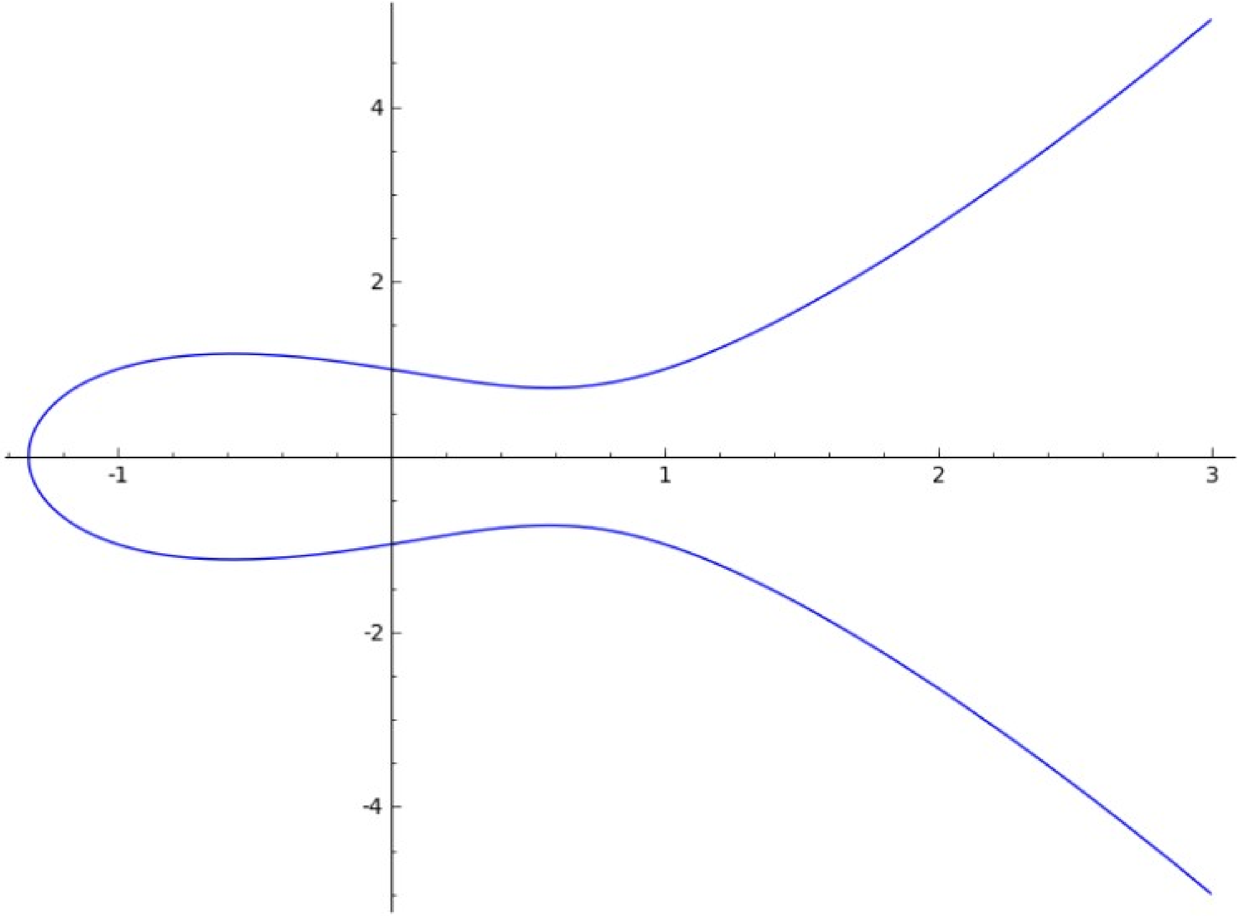
How to calculate?

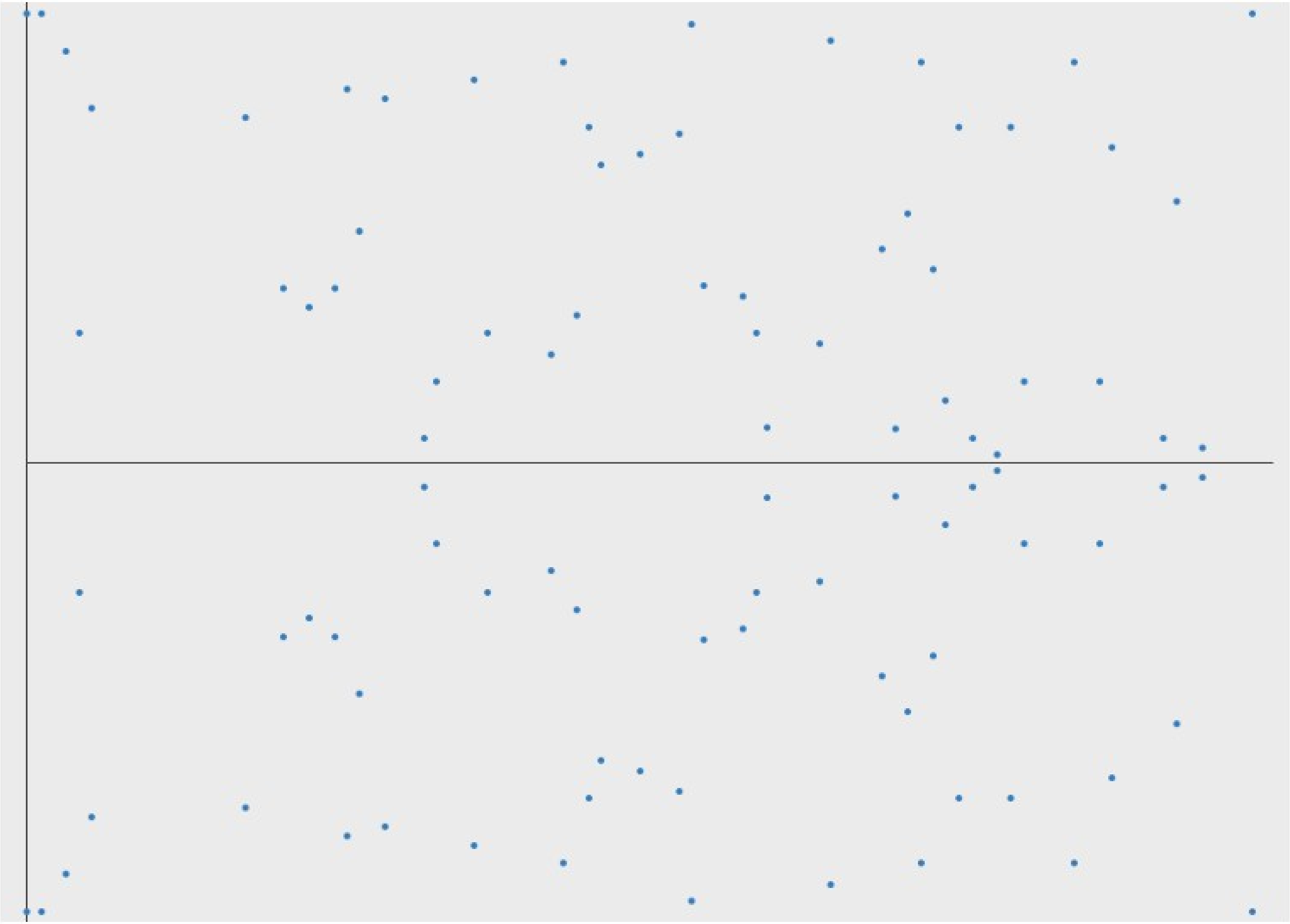
- C = -A (negation)
- C = 2A (doubling)
  - Or, C = A + A
- C = nA
  - What if n is some astronomically large number?
    - Double and add (like “square and multiply” for modular exponentiation) … Trap door function!

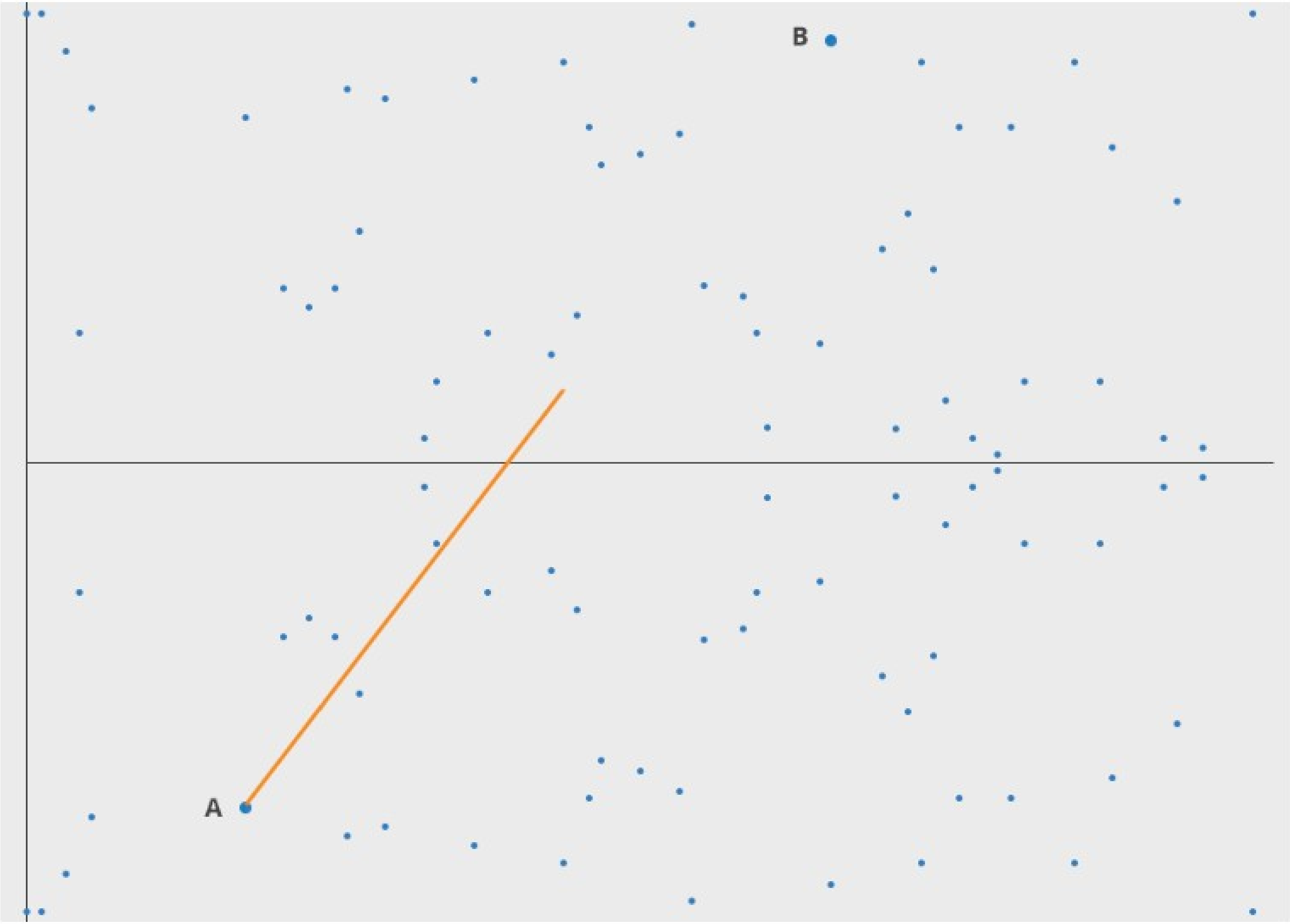
More figures stolen from…

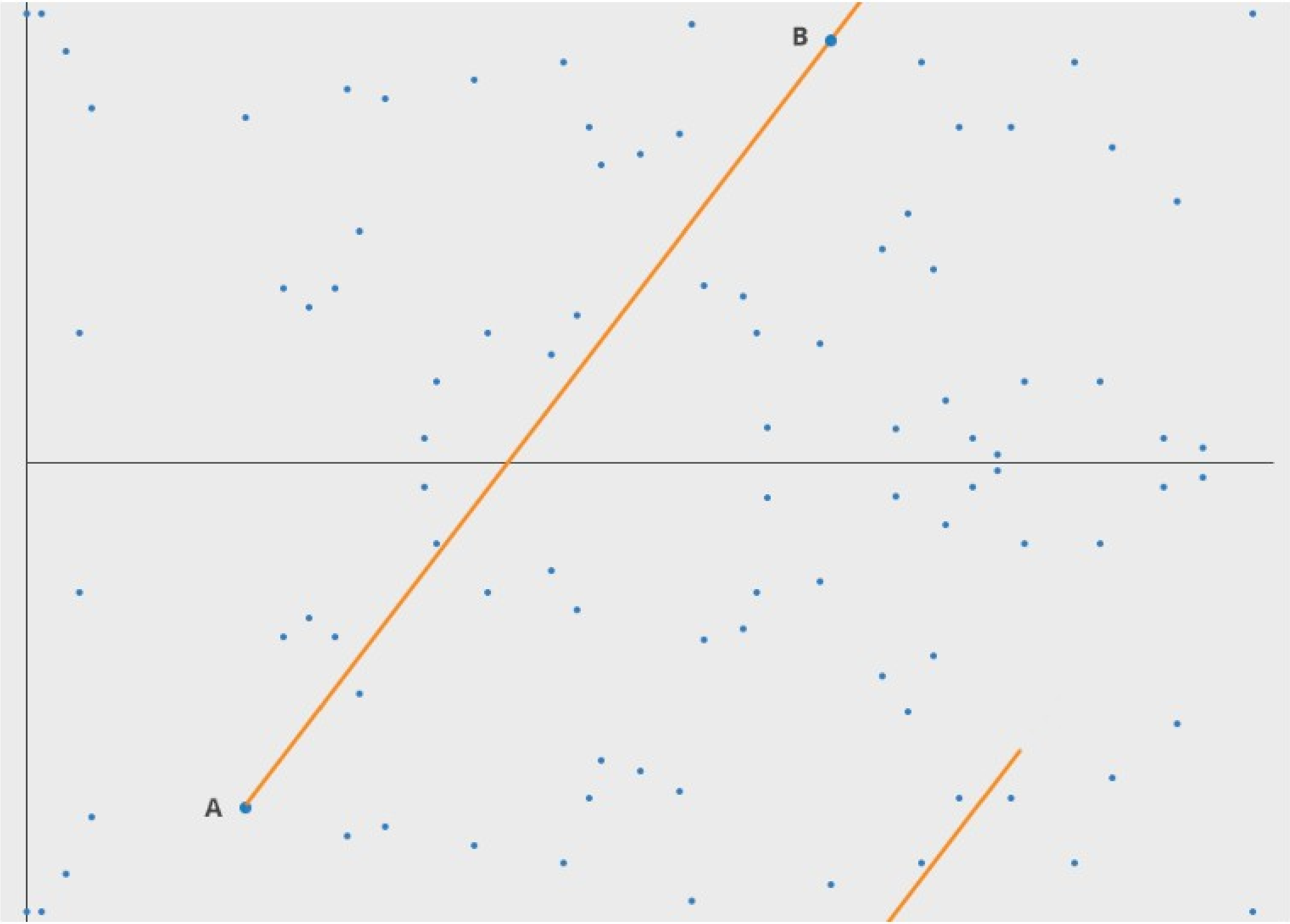
https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

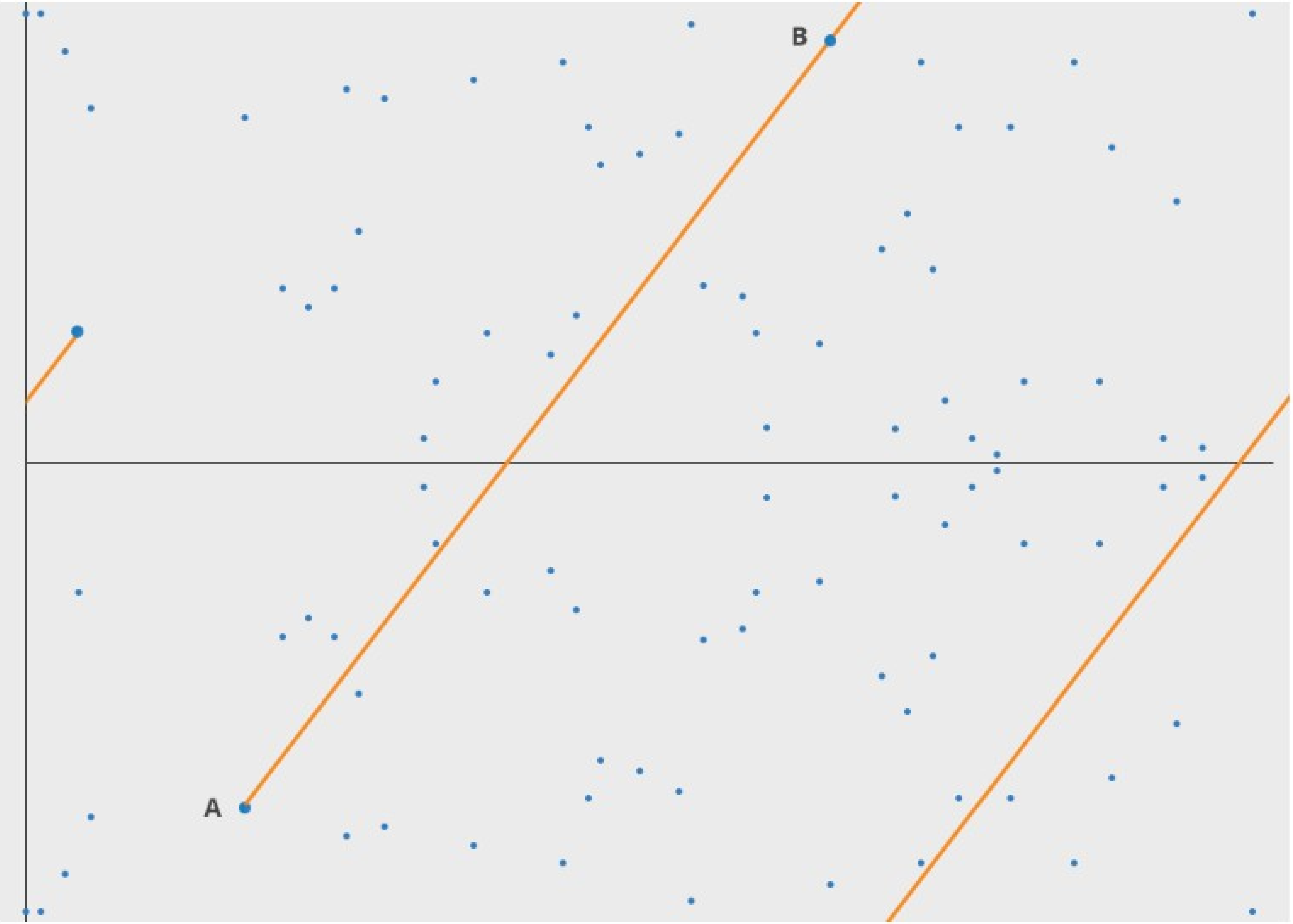
Here's an example of a curve ($y^2 = x^3 - x + 1$) plotted for all numbers:

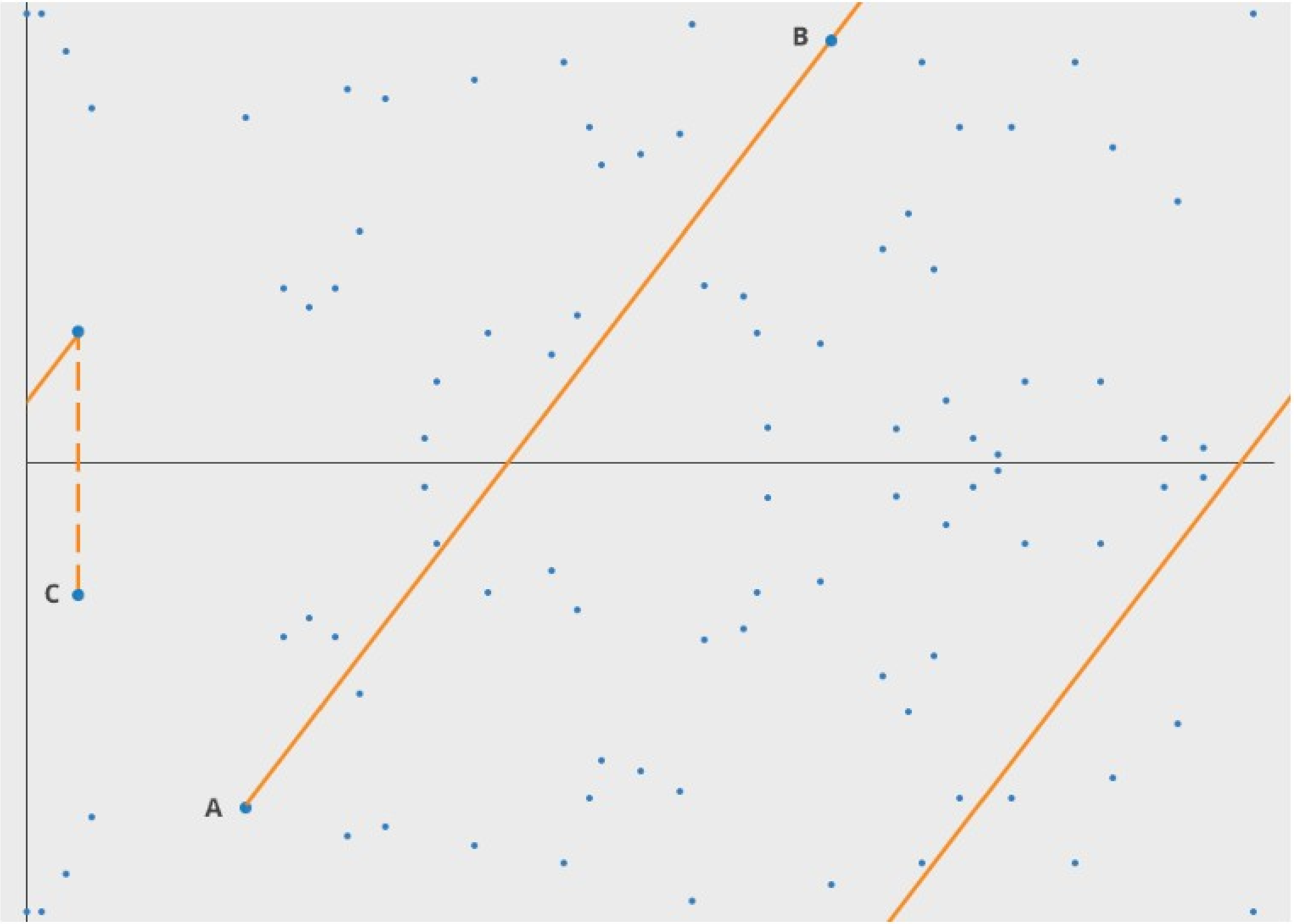





B
A

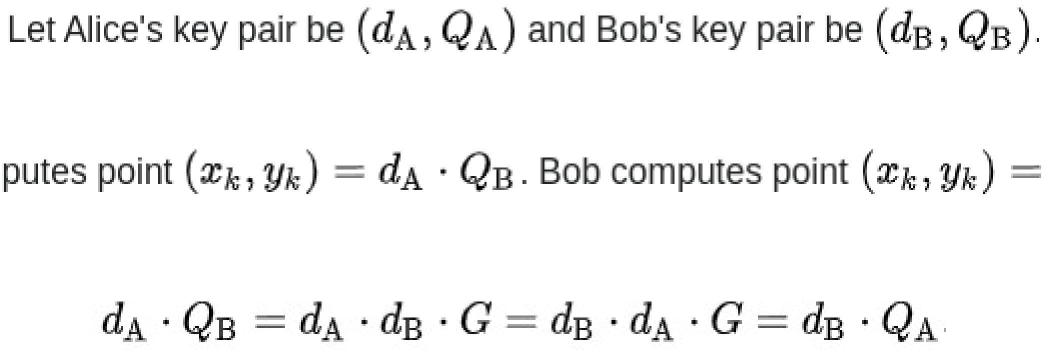

B
A


B
A


B
C
A

ECDH

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



Let Alice's key pair be $(d_{\text{A}}, Q_{\text{A}})$ and Bob's key pair be $(d_{\text{B}}, Q_{\text{B}})$.

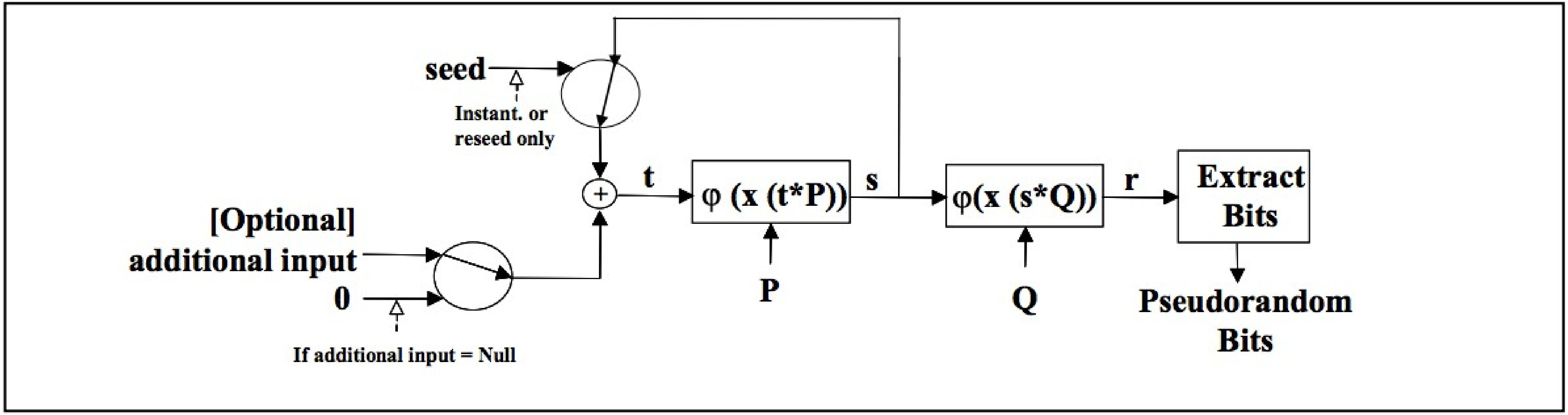
Alice computes point $(x_k, y_k) = d_{\text{A}} \cdot Q_{\text{B}}$. Bob computes point $(x_k, y_k) = d_{\text{B}} \cdot Q_{\text{A}}$.

$$d_{\text{A}} \cdot Q_{\text{B}} = d_{\text{A}} \cdot d_{\text{B}} \cdot G = d_{\text{B}} \cdot d_{\text{A}} \cdot G = d_{\text{B}} \cdot Q_{\text{A}}.$$

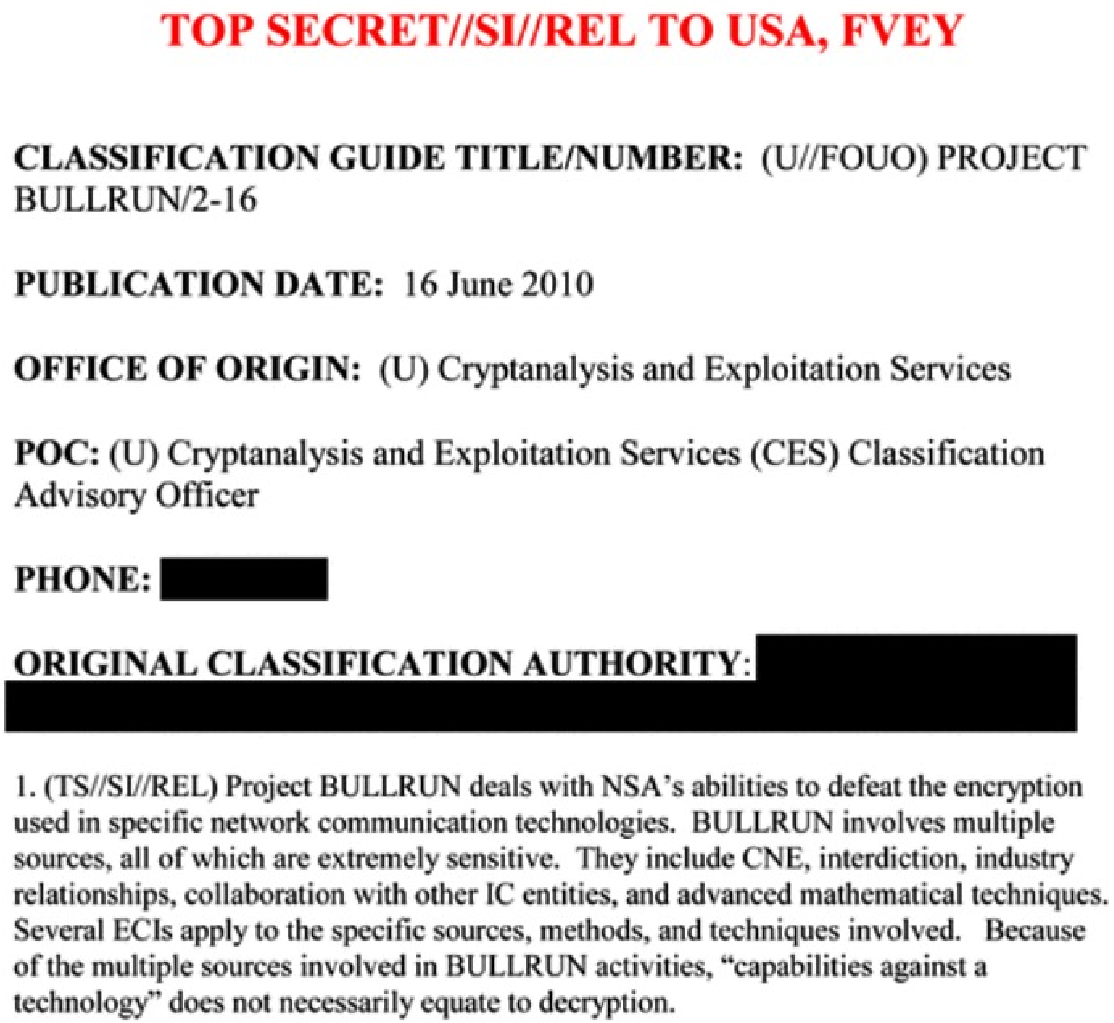
Can also do...

- 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

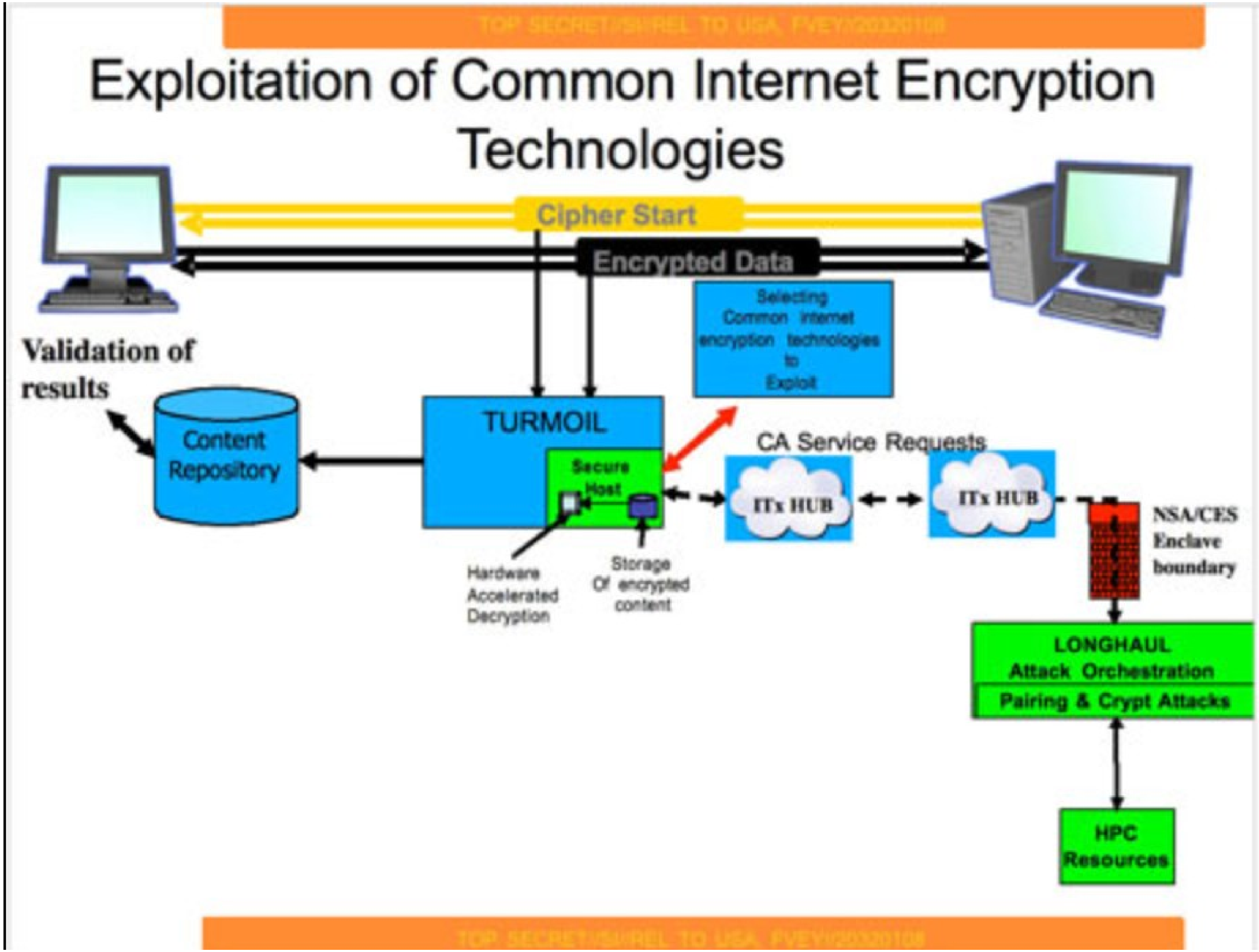
POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

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/f/fb/Classification_guide_for_Project_BULLRUN.pdf



TOP SECRET//SI//REL TO USA, FVEY//20320108

Exploitation of Common Internet Encryption Technologies

TOP SECRET//SI//REL TO USA, FVEY//20320108

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

Main takeaways about ECC

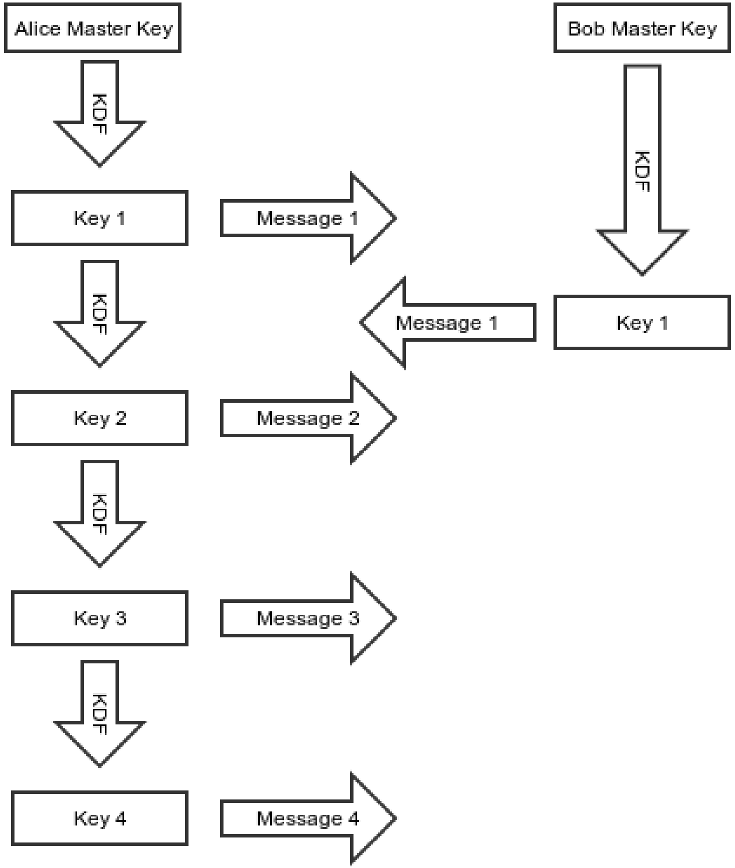
- Common choice because it’s more efficient, does key exchange and signatures
  - Not 100% immune to side channels or padding issues
  - Not quantum resistant

If you’re interested in more…

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

Back to Signal…

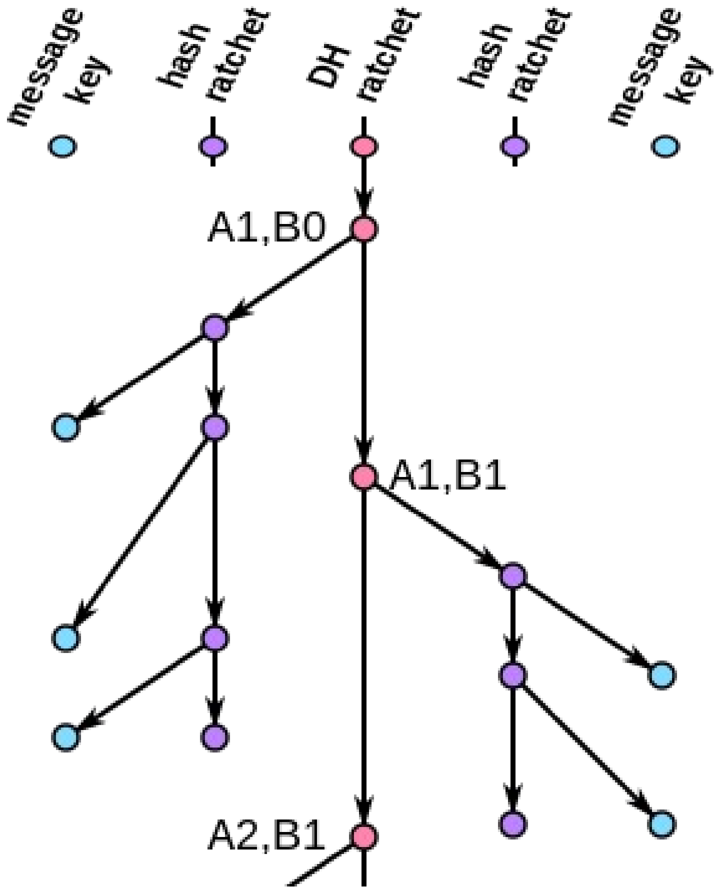
Silent Circle SCIMP ratchet



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

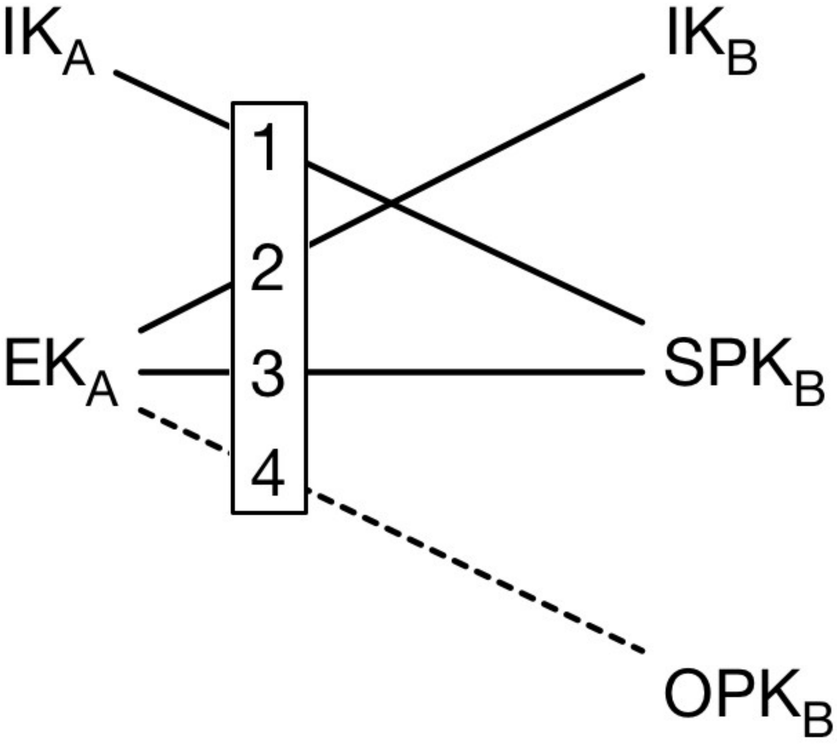
X3DH

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

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

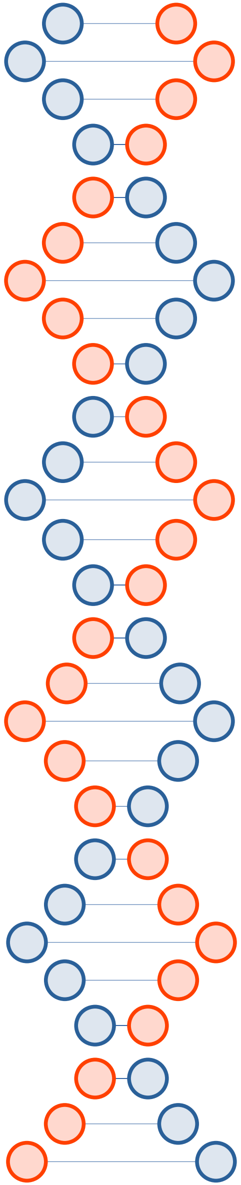
Alice’s first message encrypts the two on the left, authentication for Bob’s SPK comes from the signature.

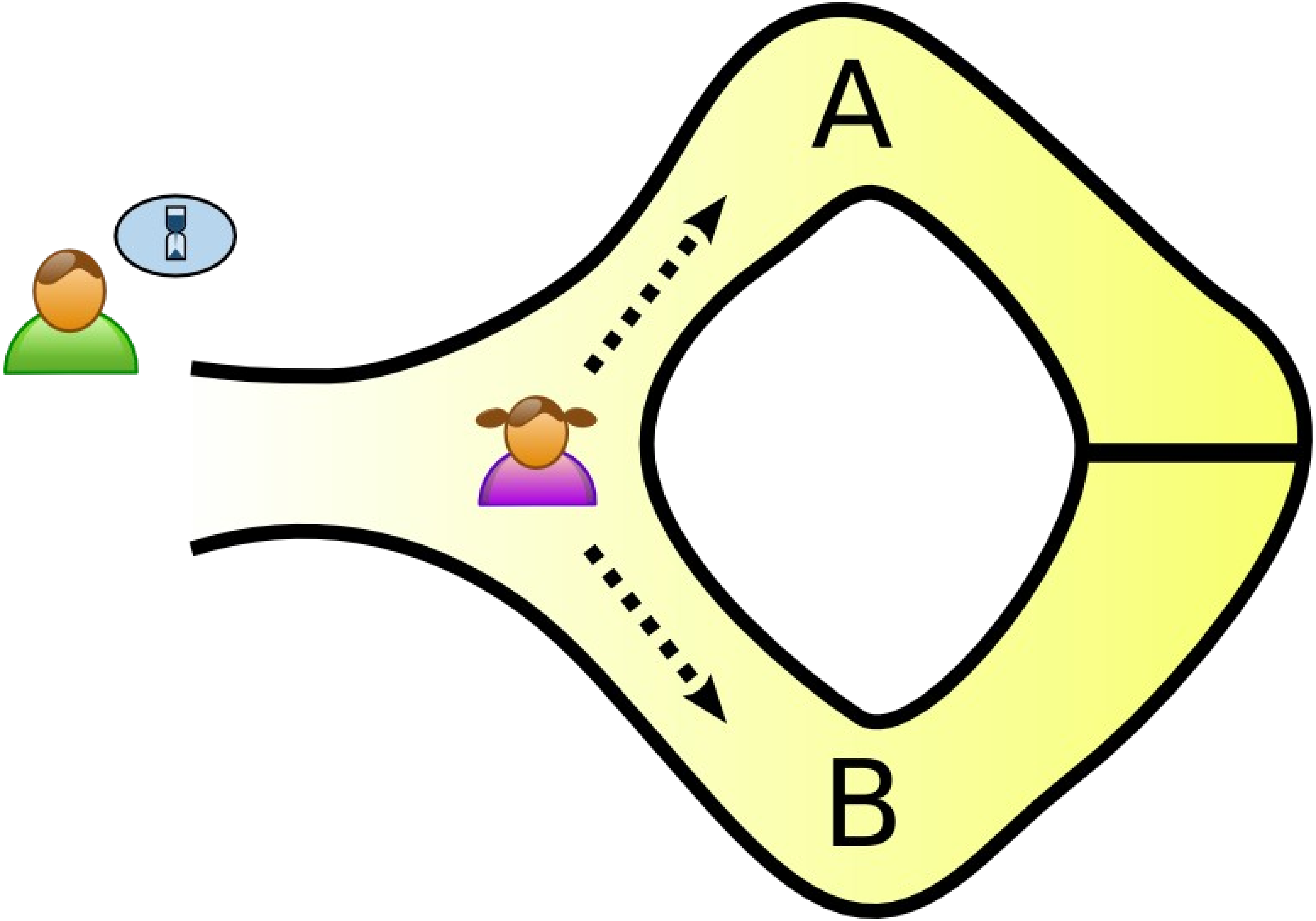
Deniability?

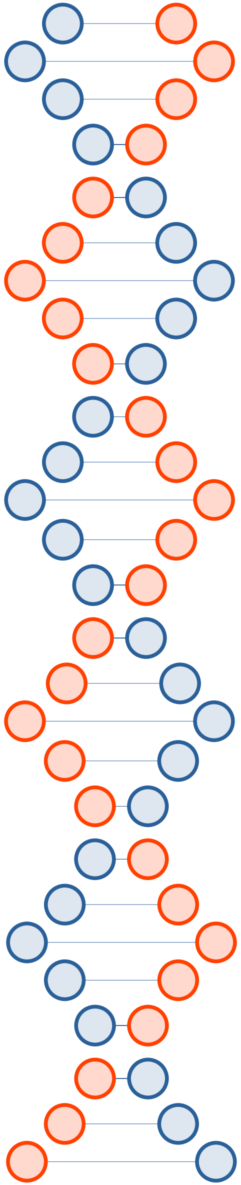


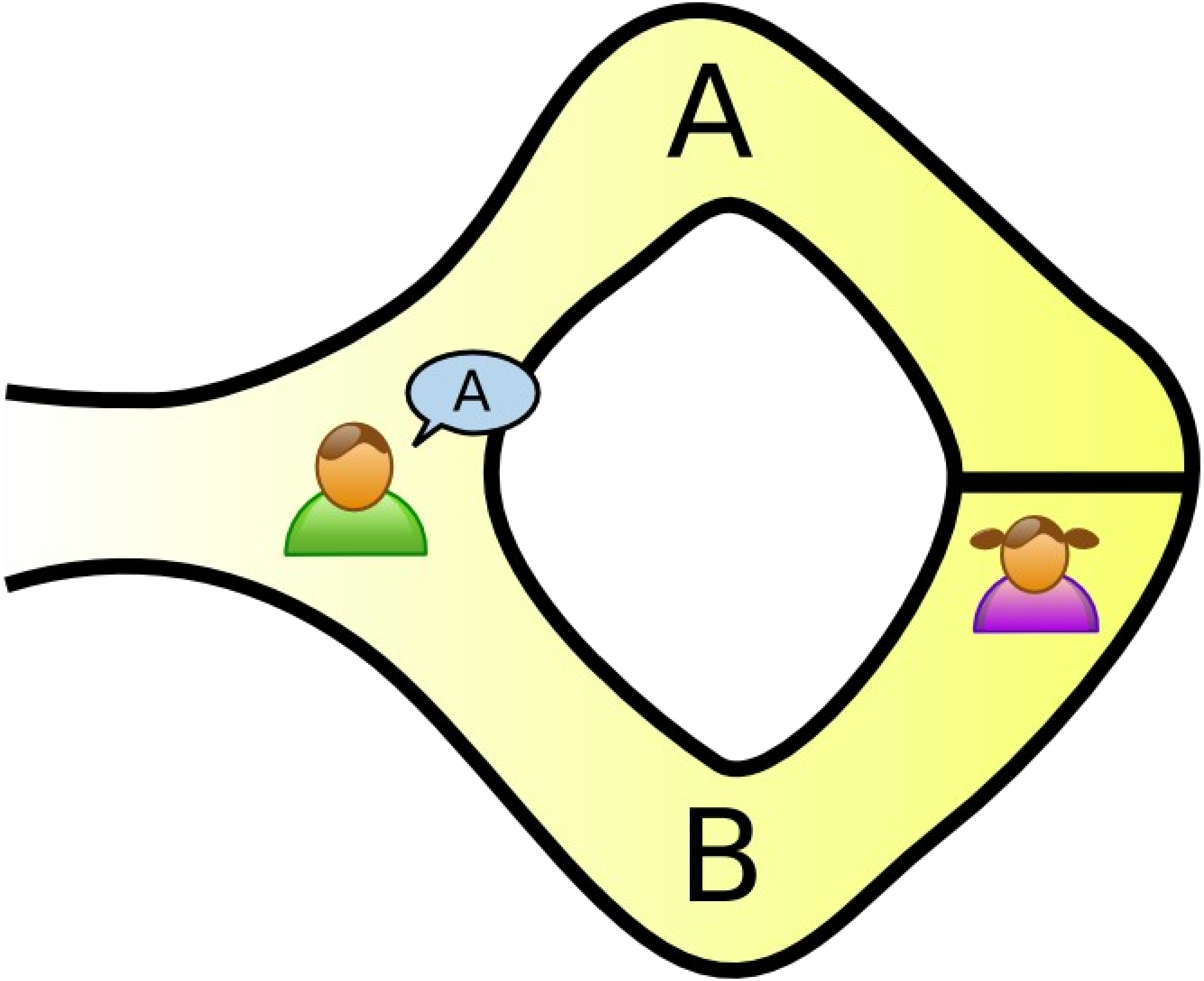
Zero Knowledge Proofs

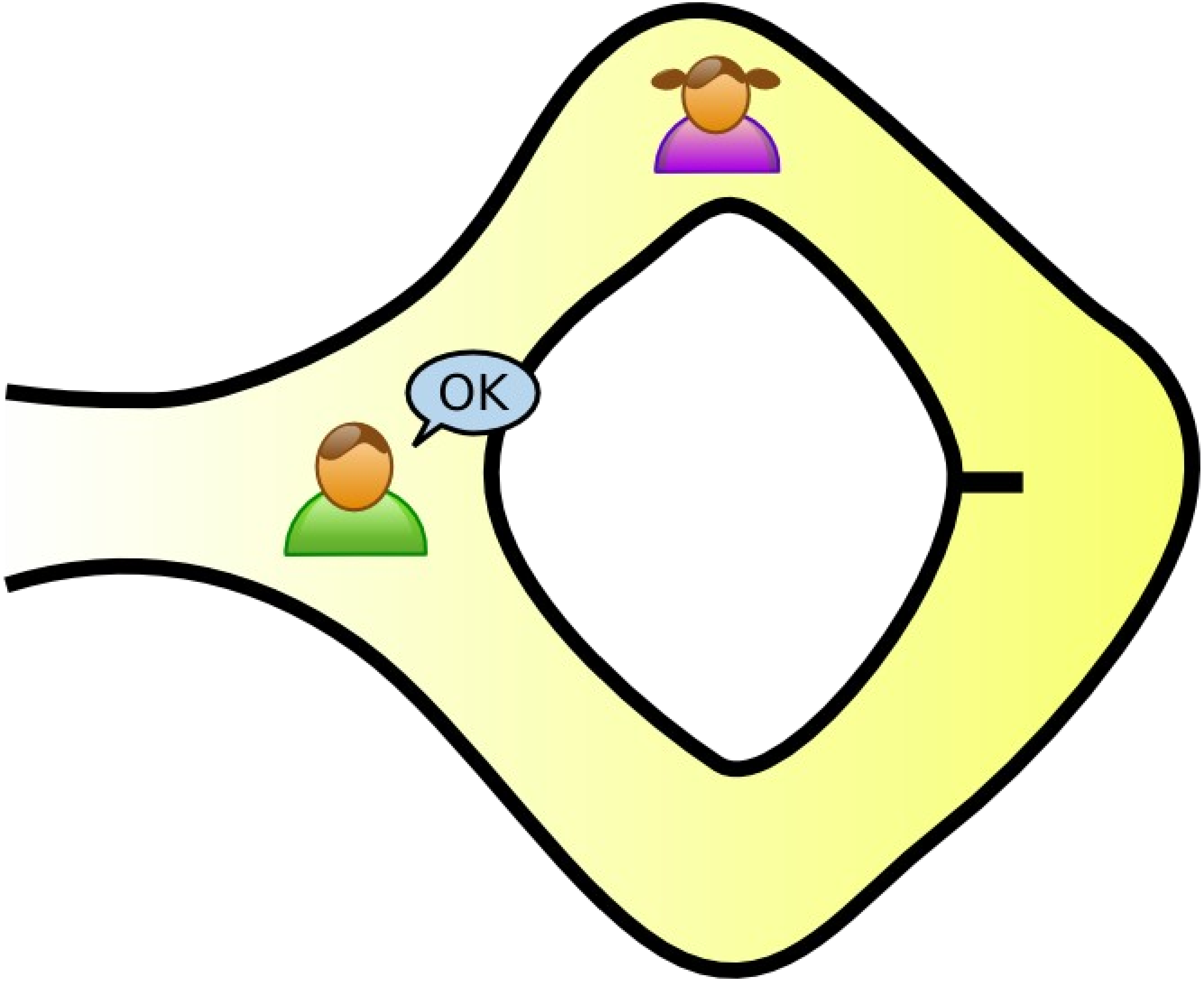
- Used for forming groups in Signal
- “a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true”
  - https://en.wikipedia.org/wiki/Zero-knowledge_proof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




A
B




A
A
B



OK

Example with discrete log

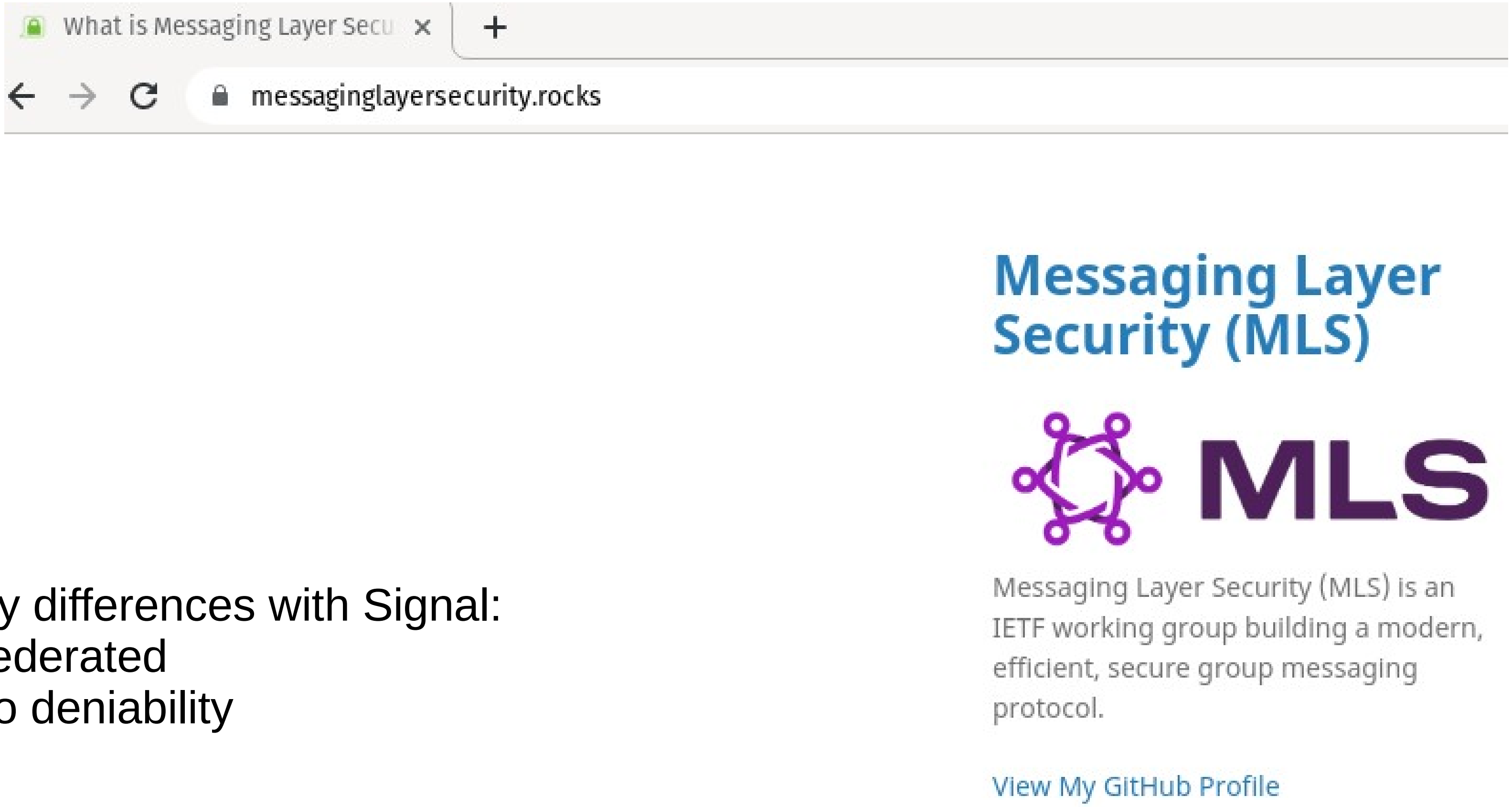
- $g^x \bmod p = y$
  - Peggy wants to prove she knows x
- Each round, Peggy computes $C = g^r \bmod p$
  - She generates r randomly
- In each round, Victor can ask for…
  - **r** --or--
  - **$(x + r) \bmod (p - 1)$**

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

The Hacker News

Signal Messenger Introduces PQXDH Quantum-Resistant Encryption

Sep 20, 2023 THN Encryption / Privacy



Messaging Layer Security (MLS)

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

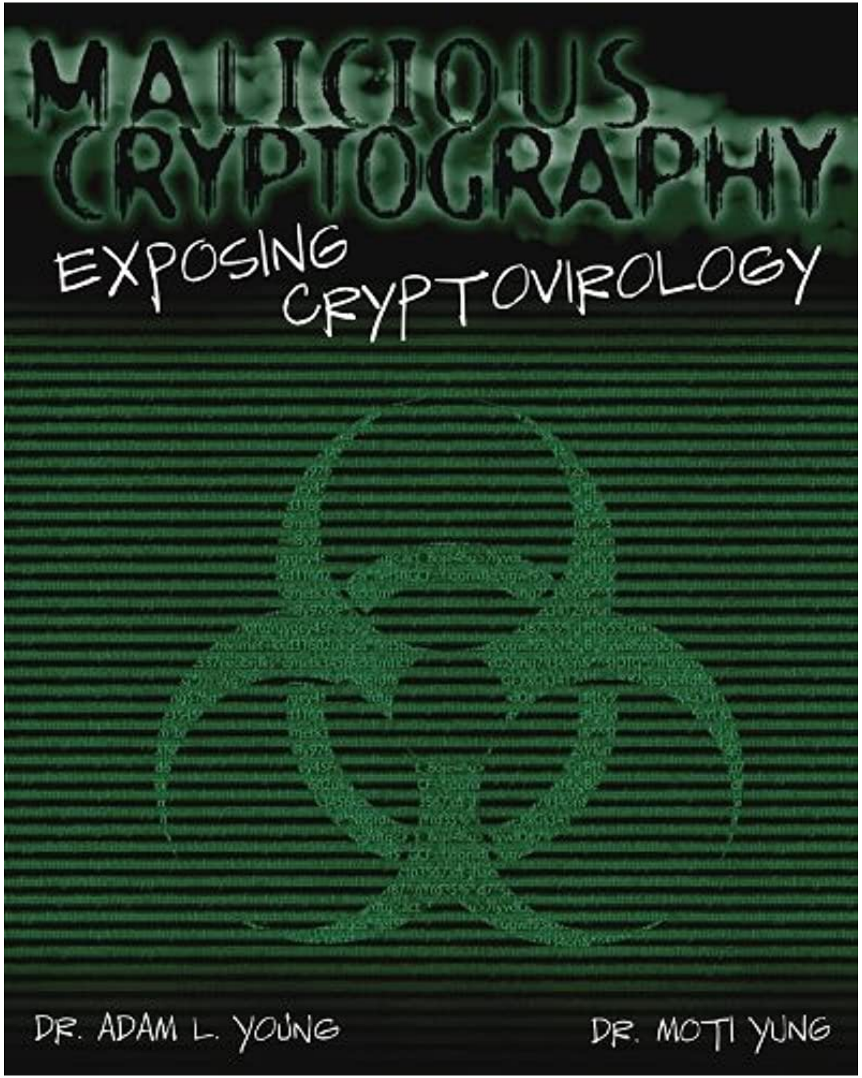
View My GitHub Profile

Two key differences with Signal:

- Federated
- No deniability

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

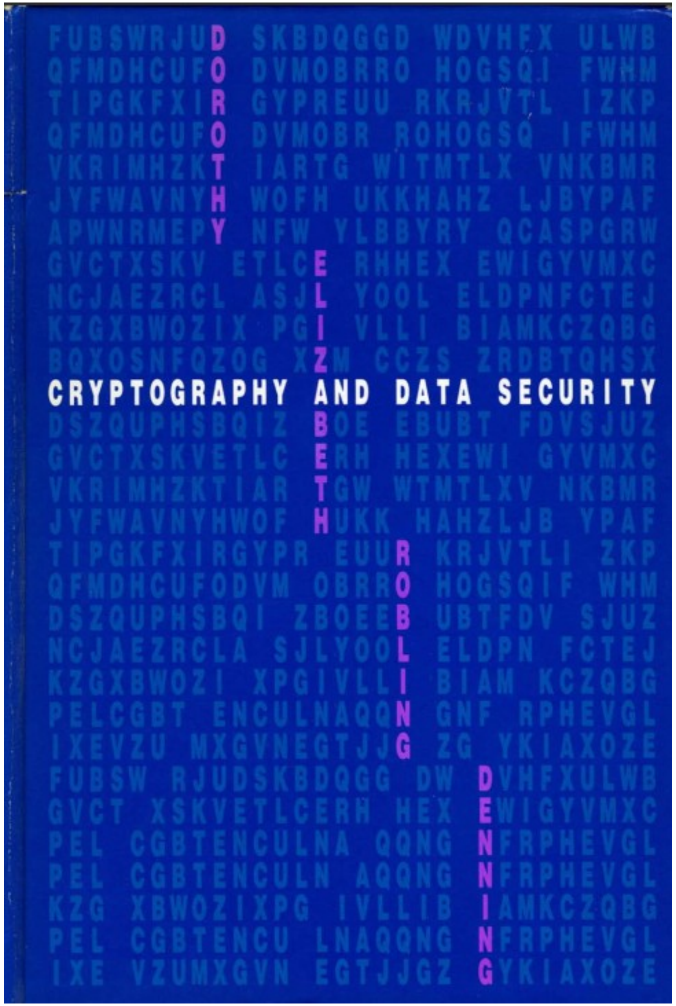


MALICIOUS CRYPTOGRAPHY

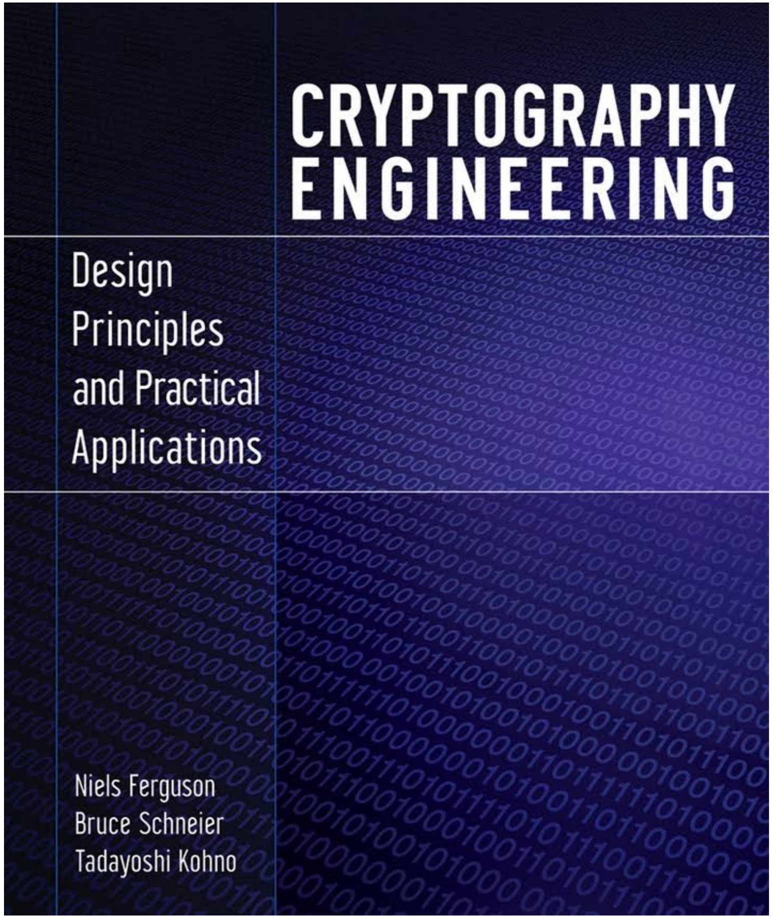
EXPOSING CRYPTOVIROLOGY

DR. ADAM L. YOUNG

DR. MOTI YUNG


FUBSWRJUD SKBDQGGD WDVHFX ULWB
QFMDHCUFO DVMOBRRO HOGSQI FWHM
TIPGKFXIR GYPREUU RKRJVTL IZKP
QFMDHCUFO DVMOBR ROHOGSQ IFWHM
VKRIMHZKT IARTG WITMTLX VNKBMR
JYFWAVNYH WOFH UKKHAHZ LJBYPAF
APWNRMEPY NFW YLBBYRY QCASPGRW
GVCTXSKV ETLCE RHHEX EWIGYVMXC
NCJAEZRCL ASJL YOOL ELDPNFCTEJ
KZGXBWOZIX PGI VLLI BIAMKCZQBG
BQXOSNFQZOG XZM CCZS ZRDBTQHSX
CRYPTOGRAPHY AND DATA SECURITY
DSZQUPHSBQIZ BOE EBUBT FDVSJUZ
GVCTXSKVETLC ERH HEXEWI GYVMXC
VKRIMHZKTIAR TGW WTMTLXV NKBMR
JYFWAVNYHWOF HUKK HAHZLJB YPAF
TIPGKFXIRGYPR EUUR KRJVTLI ZKP
QFMDHCUFODVM OBRRO HOGSQIF WHM
DSZQUPHSBQI ZBOEEB UBTFDV SJUZ
NCJAEZRCLA SJLYOOL ELDPN FCTEJ
KZGXBWOZI XPGIVLLI BIAM KCZQBG
PELCGBT ENCULNAQQN GNF RPHEVGL
IXEVZU MXGVNEGTJJG ZG YKIAXOZE
FUBSW RJUDSKBDQGG DW DVHFXULWB
GVCT XSKVETLCERH HEX EWIGYVMXC
PEL CGBTENCULNA QQNG NFRPHEVGL
PEL CGBTENCULN AQQNG NFRPHEVGL
KZG XBWOZIXPG IVLLIB IAMKCZQBG
PEL CGBTENCU LNAQQNG NFRPHEVGL
IXE VZUMXGVN EGTJJGZ GYKIAXOZE
DOROTHY
ELIZABETH
ROBLING
DENNING

Cryptography Engineering by Ferguson *et al.*



CRYPTOGRAPHY ENGINEERING

Design Principles and Practical Applications

Niels Ferguson
Bruce Schneier
Tadayoshi Kohno