Diffie-Hellman, Elliptic Curve Diffie Hellman (ECDH) and asymmetric crypto primitives

CSE 539

jedimaestro@asu.edu

To prepare for this lecture...

- https://www.youtube.com/watch?v=YEBfamv-_do
- https://www.youtube.com/watch?v=wXB-V_Keiu8

Outline

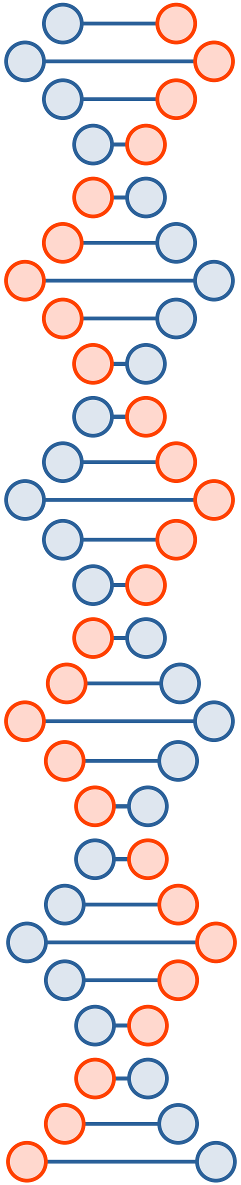
- Historical context
- Diffie Hellman
- ECDH
- Asymmetric crypto primitives and possibilities

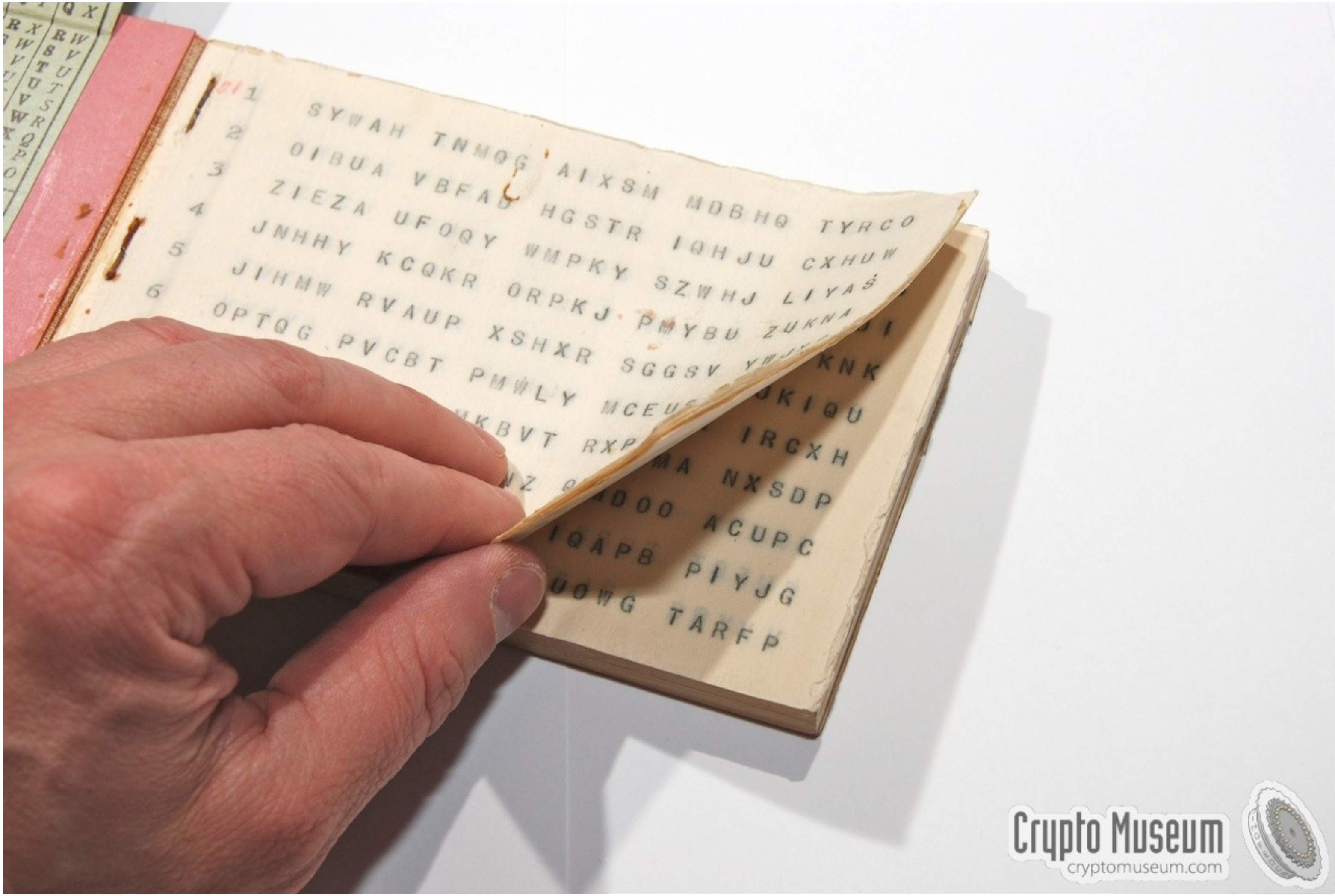
Darknet Diaries, Episode 83

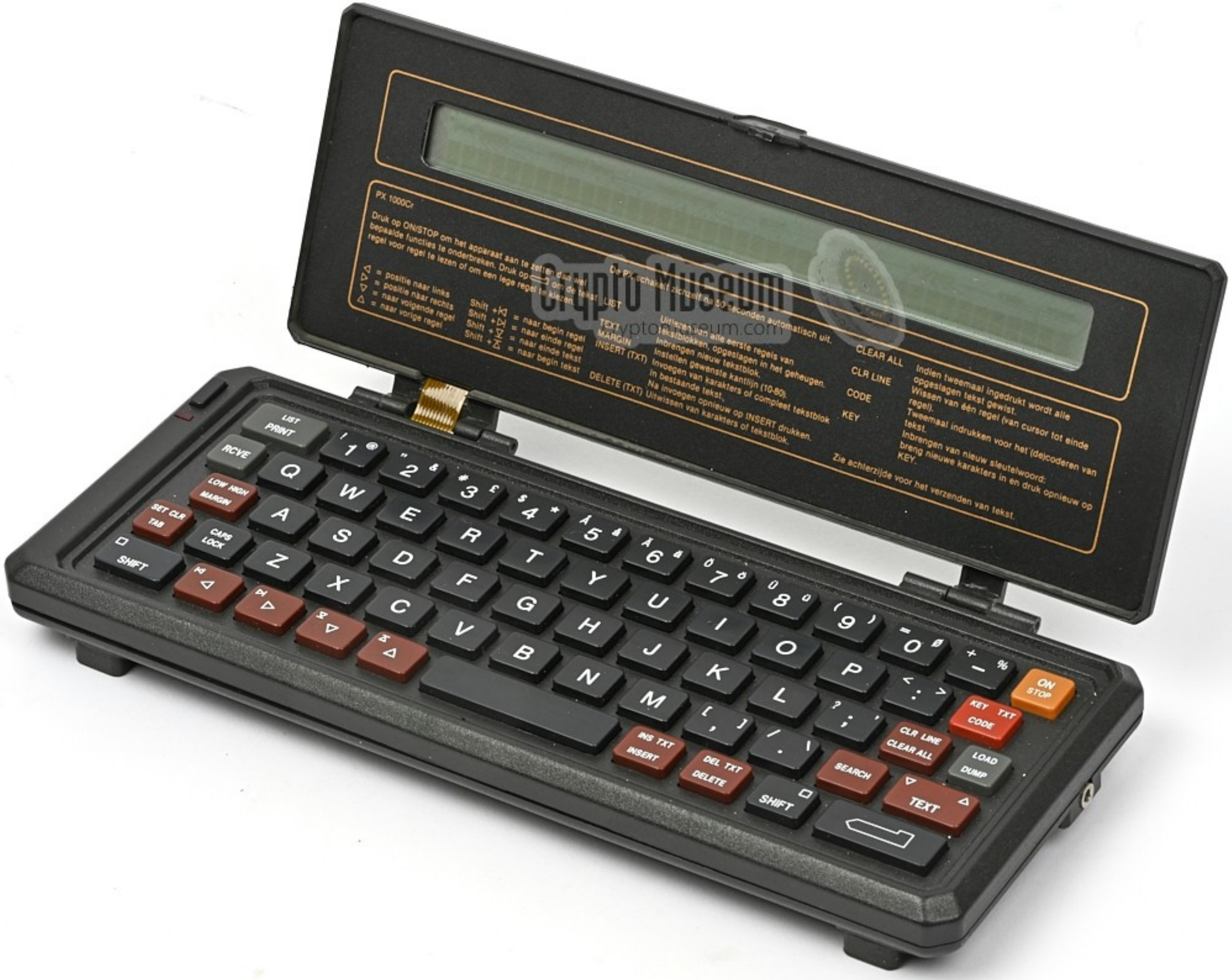
https://darknetdiaries.com/transcript/83/

- “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 LIYAS
4 JNHHY KCQKR ORPKJ PMYBU ZUKNA
5 JIHMW RVAUP XSHXR SGGSV
6 OPTQG PVCBT PMWLY MCEU
KNK
KIQU
IRCXH
NXSDP
DOO
ACUPC
IQAPB
PIYJG
UOWG
TARFP
Crypto Museum
cryptomuseum.com



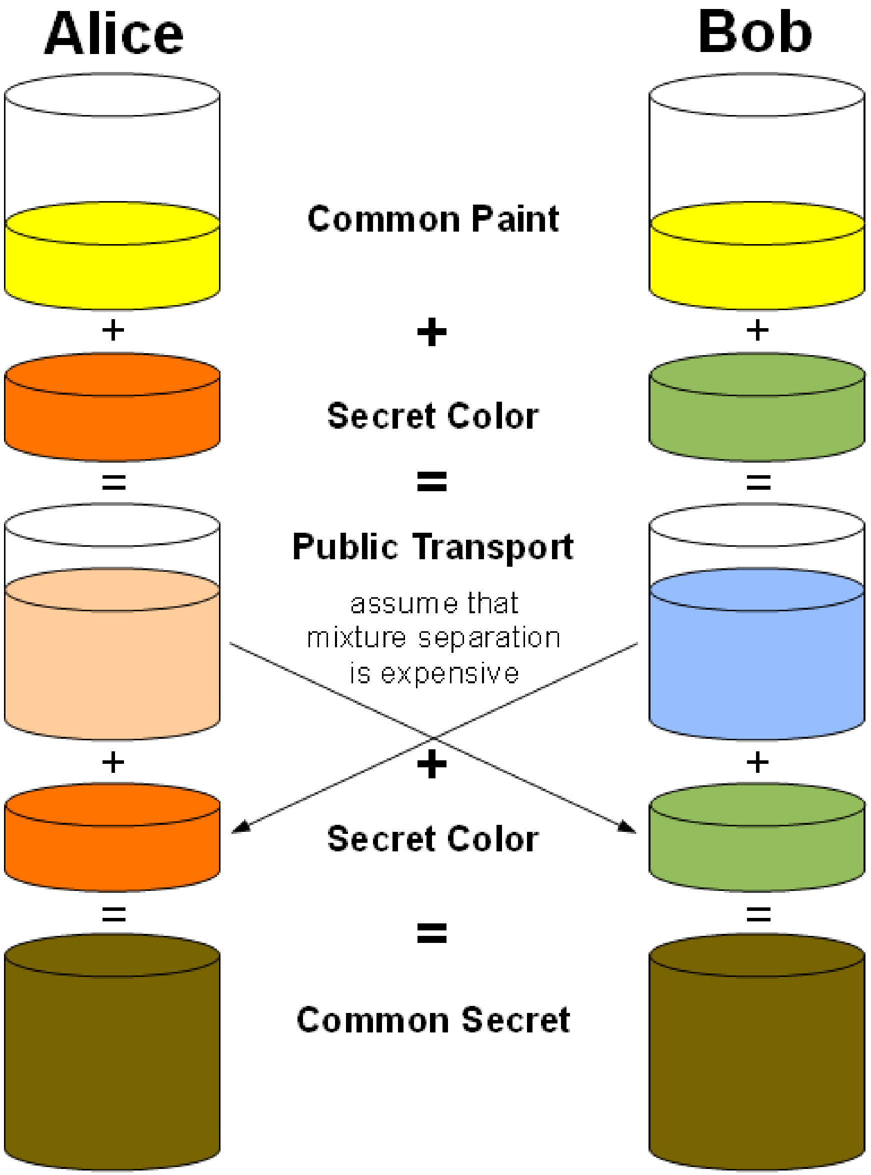
PX 1000Cr
Druk op ON/STOP om het apparaat aan te zetten dan wel bepaalde functies te onderbreken. Druk op ⟸ om de tekst regel voor regel te lezen of om een lege regel te kiezen.
◁ = positie naar links
▷ = positie naar rechts
▽ = naar volgende regel
△ = naar vorige regel
Shift + ◁ = naar begin regel
Shift + ▷ = naar einde regel
Shift + ▽ = naar einde tekst
Shift + △ = naar begin tekst
De PX schakelt zichzelf na 50 seconden automatisch uit.
LIST
TEXT Uitlezen van alle eerste regels van tekstblokken, opgeslagen in het geheugen.
Inbrengen nieuw tekstblok.
MARGIN Instellen gewenste kantlijn (10-80).
INSERT (TXT) Invoegen van karakters of compleet tekstblok in bestaande tekst.
Na invoegen opnieuw op INSERT drukken.
DELETE (TXT) Uitwissen van karakters of tekstblok.
CLEAR ALL Indien tweemaal ingedrukt wordt alle opgeslagen tekst gewist.
CLR LINE Wissen van één regel (van cursor tot einde regel).
CODE Tweemaal indrukken voor het (de)coderen van tekst.
KEY Inbrengen van nieuw sleutelwoord: breng nieuwe karakters in en druk opnieuw op KEY.
Zie achterzijde voor het verzenden van tekst.
LIST PRINT
RCVE
LOW HIGH MARGIN
SET CLR TAB
CAPS LOCK
SHIFT
INS TXT INSERT
DEL TXT DELETE
SEARCH
SHIFT
TEXT
CLR LINE CLEAR ALL
LOAD DUMP
KEY TXT CODE
ON STOP

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

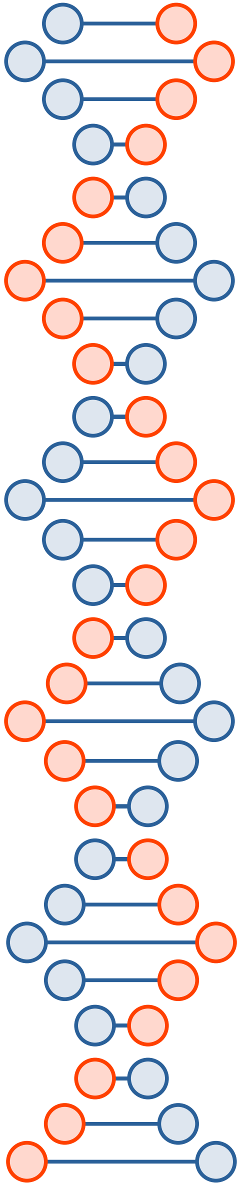
assume that
mixture separation
is expensive

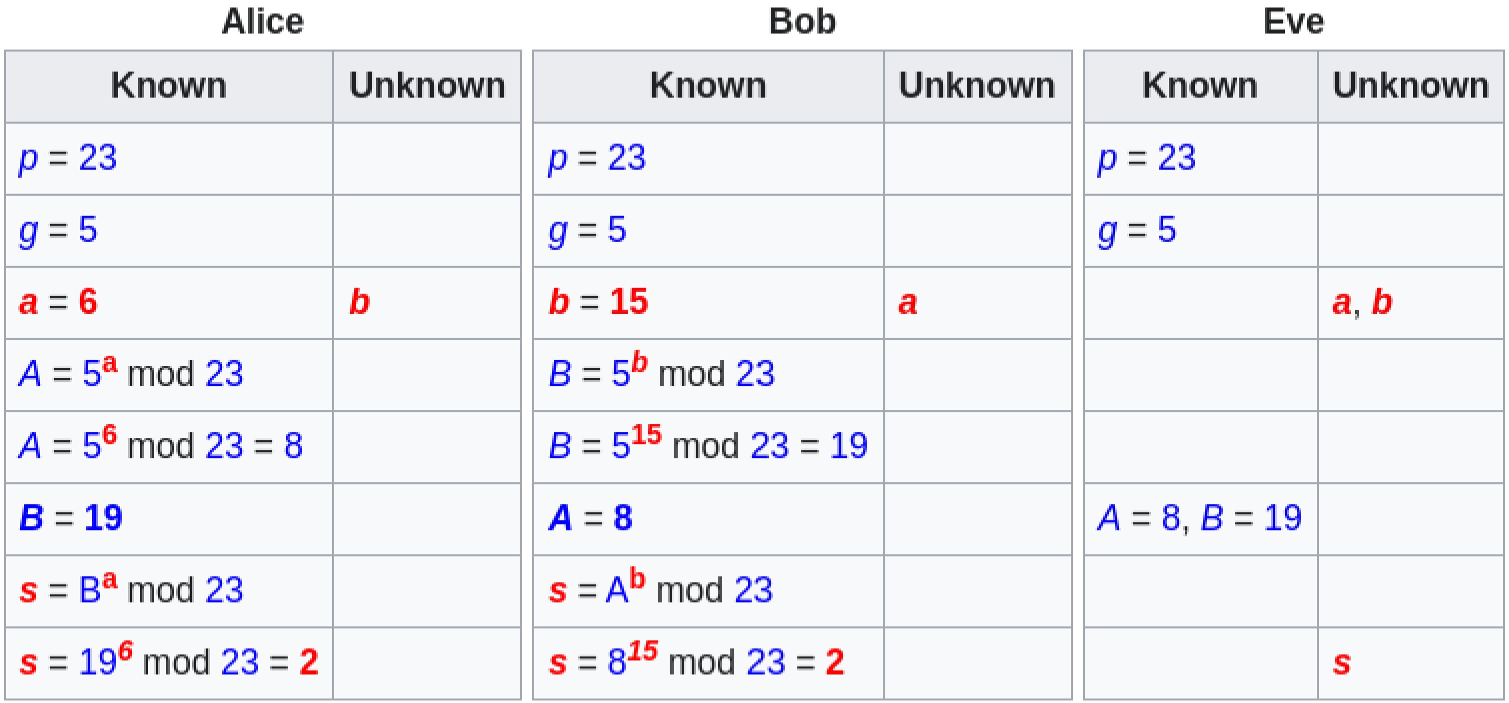
+

Secret Color

=

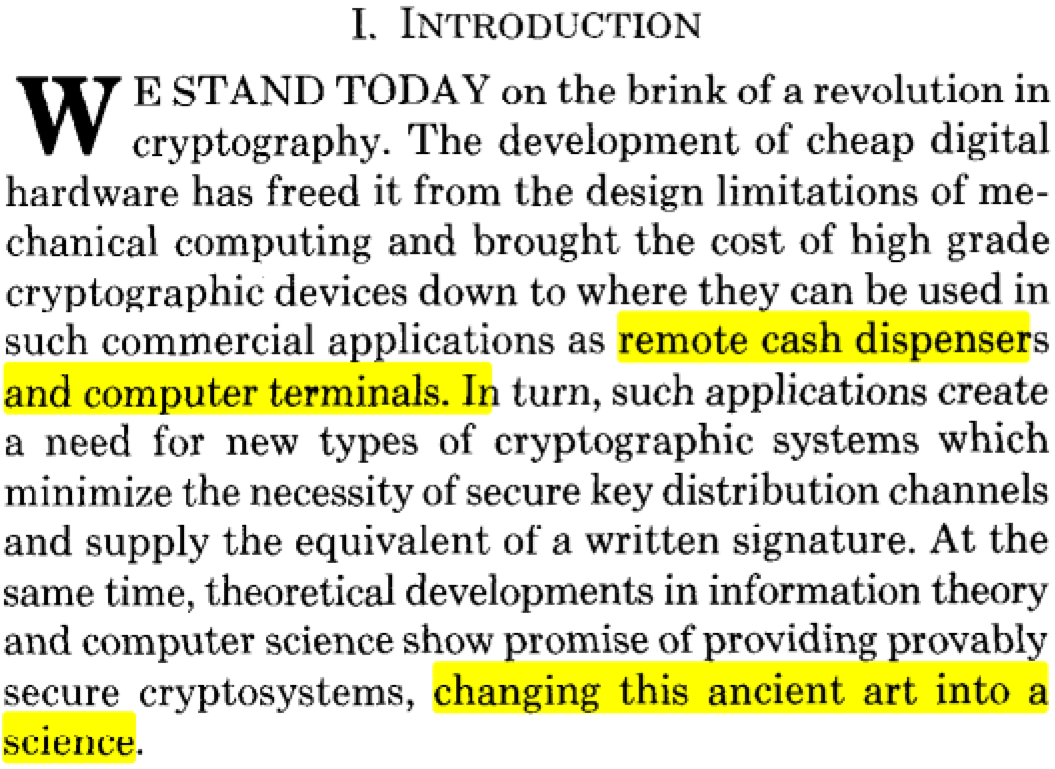
Common Secret





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

The paper...

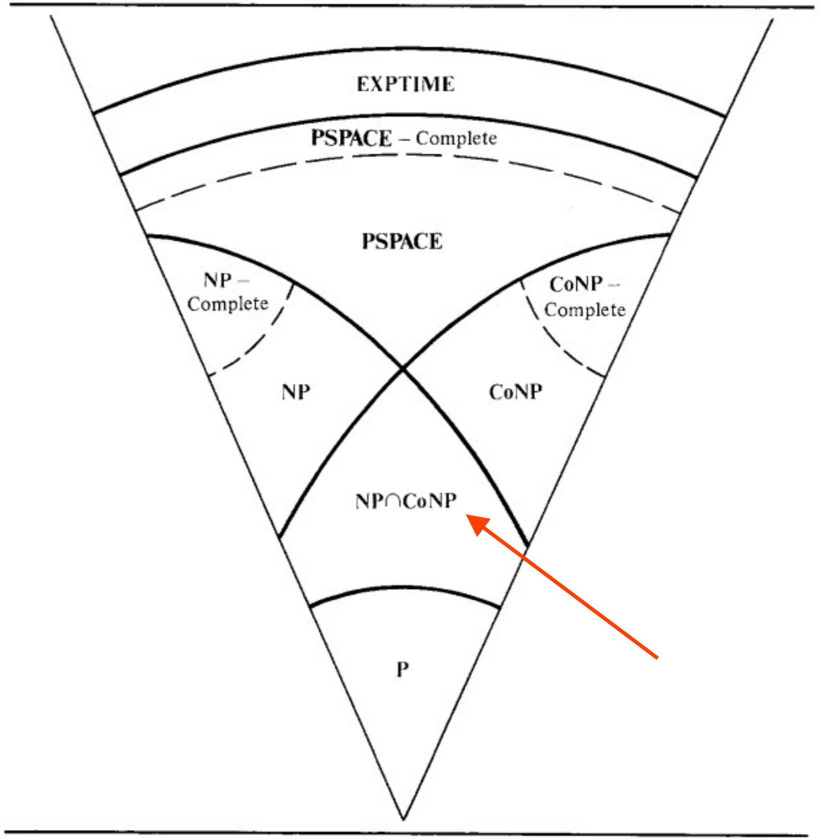


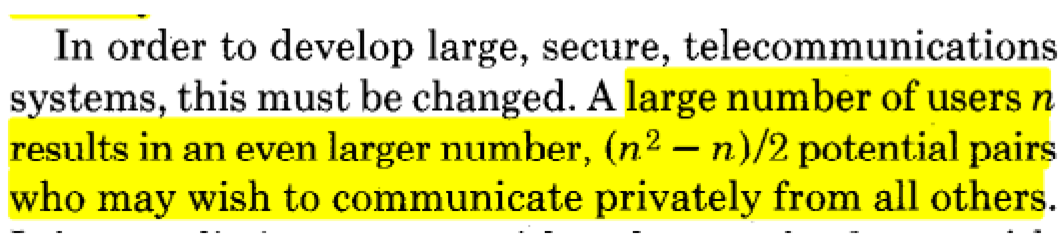
I. INTRODUCTION

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.

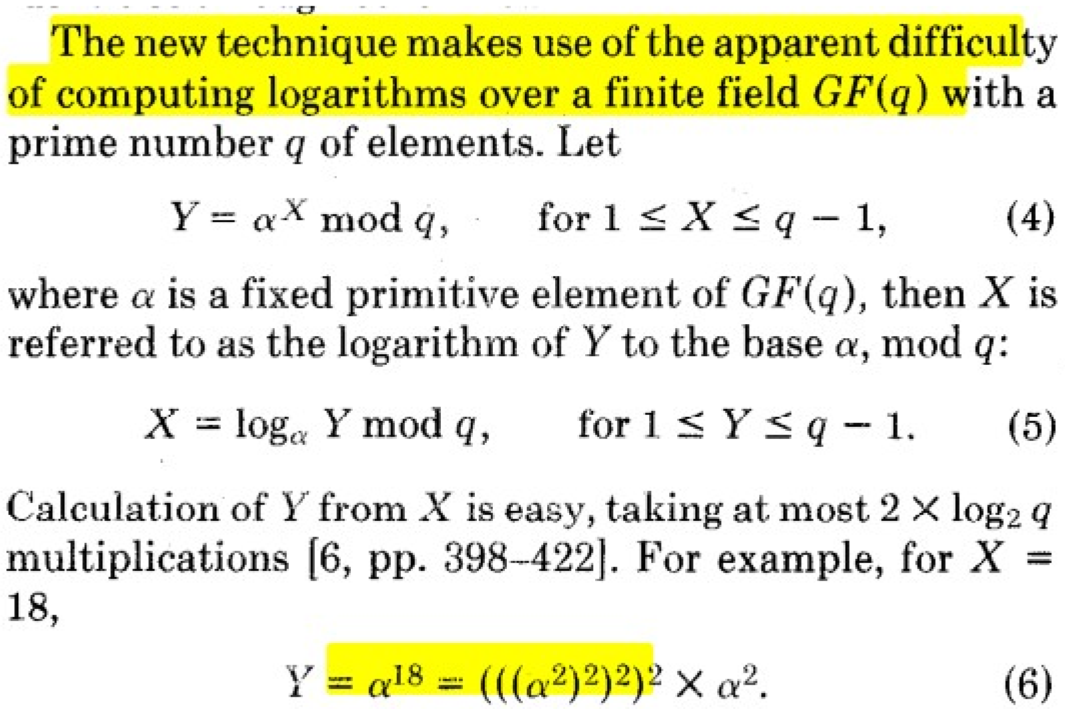
https://faculty.nps.edu/dedennin/publications/Denning-CryptographyDataSecurity.pdf

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

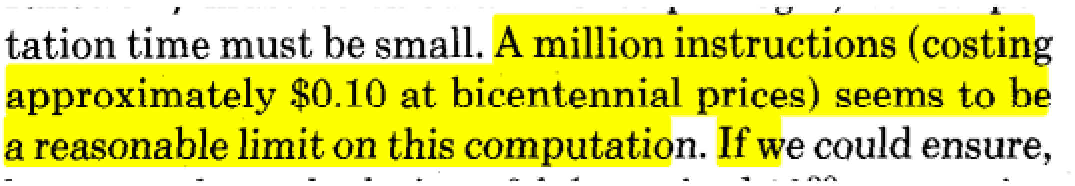
$$Y = \alpha^X \bmod q, \qquad \text{for } 1 \leq X \leq q - 1, \qquad (4)$$

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:

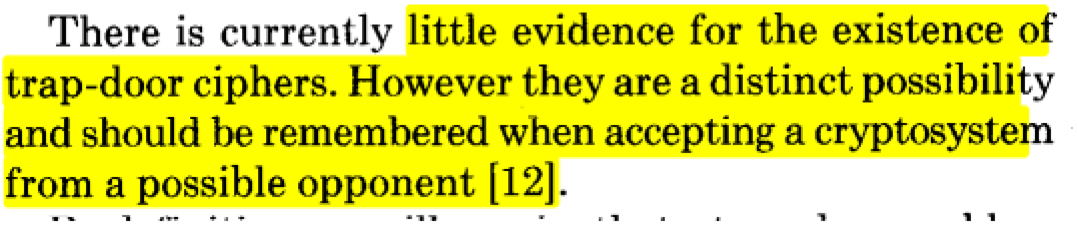
$$X = \log_\alpha Y \bmod q, \qquad \text{for } 1 \leq Y \leq q - 1. \qquad (5)$$

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

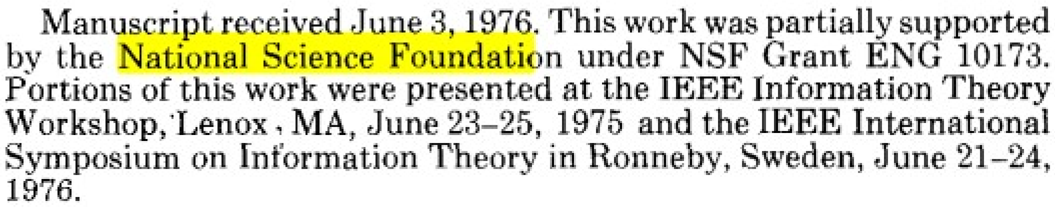
$$Y = \alpha^{18} = (((\alpha^2)^2)^2)^2 \times \alpha^2. \qquad (6)$$



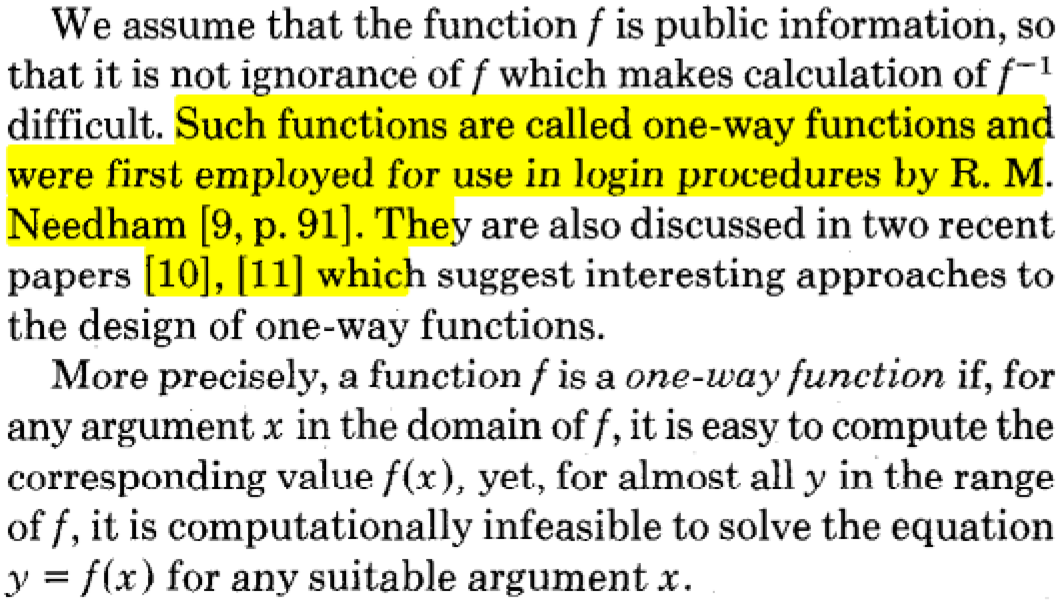
tation time must be small. A million instructions (costing approximately $0.10 at bicentennial prices) seems to be a reasonable limit on this computation. If we could ensure,



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].

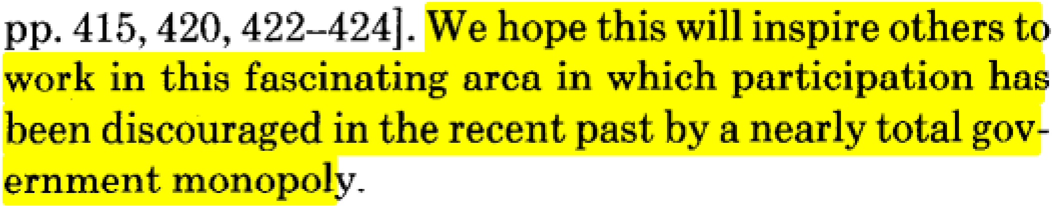


Manuscript received June 3, 1976. This work was partially supported by the National Science Foundation under NSF Grant ENG 10173. Portions of this work were presented at the IEEE Information Theory Workshop, Lenox, MA, June 23–25, 1975 and the IEEE International Symposium on Information Theory in Ronneby,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

Asymmetric crypto

- Some people use “public key crypto” to generally refer to all of asymmetric crypto
- Goes beyond Diffie-Hellman and RSA
  - *E.g.*, elliptic curve crypto
  - Quantum resistant
- Goes well beyond encryption, authentication, non-repudiation (signatures), and key exchange
  - Oblivious transfer, secure multiparty computation, cryptocurrencies, identity-based encryption, secret sharing, zero-knowledge proof, private information retrieval, cryptocounters, subliminal channels, ransomware, deniable encryption, off-the-record, forward secrecy, future secrecy, ...

Elliptic Curve Cryptography (ECC)

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

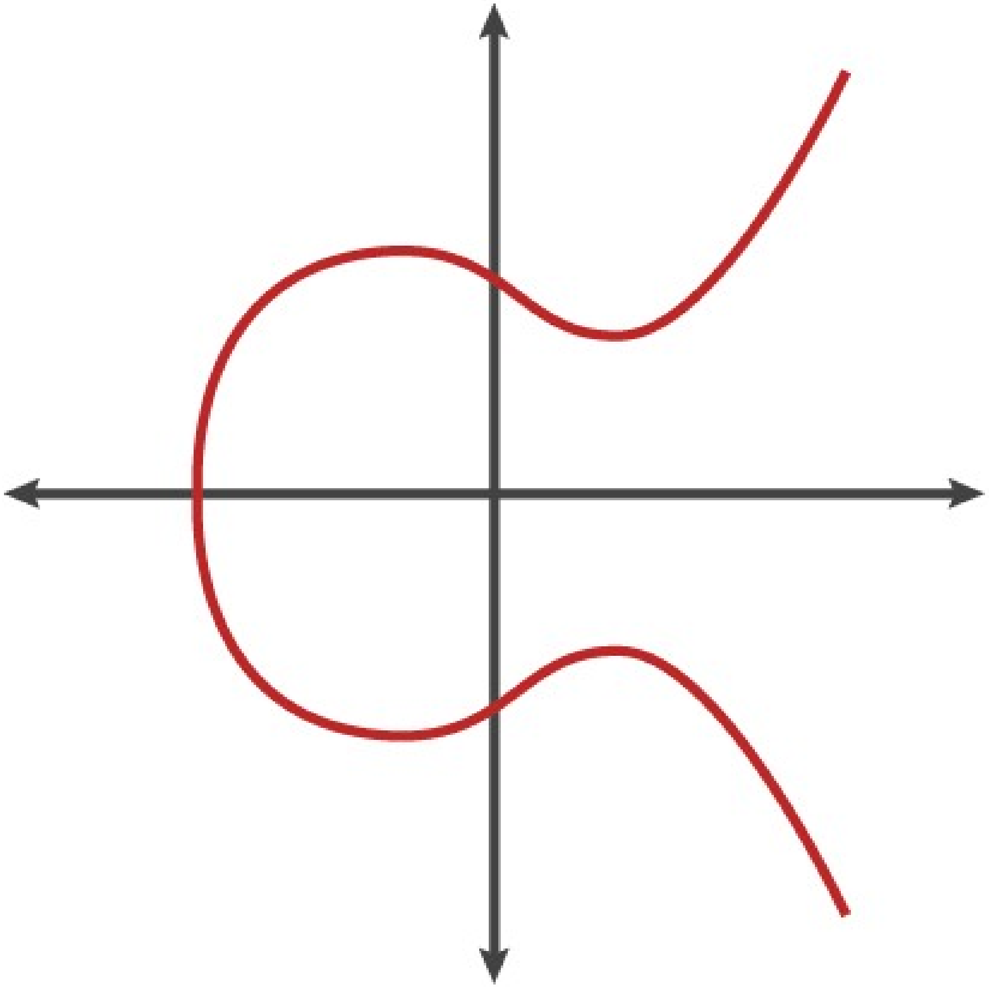
ECC background

- “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

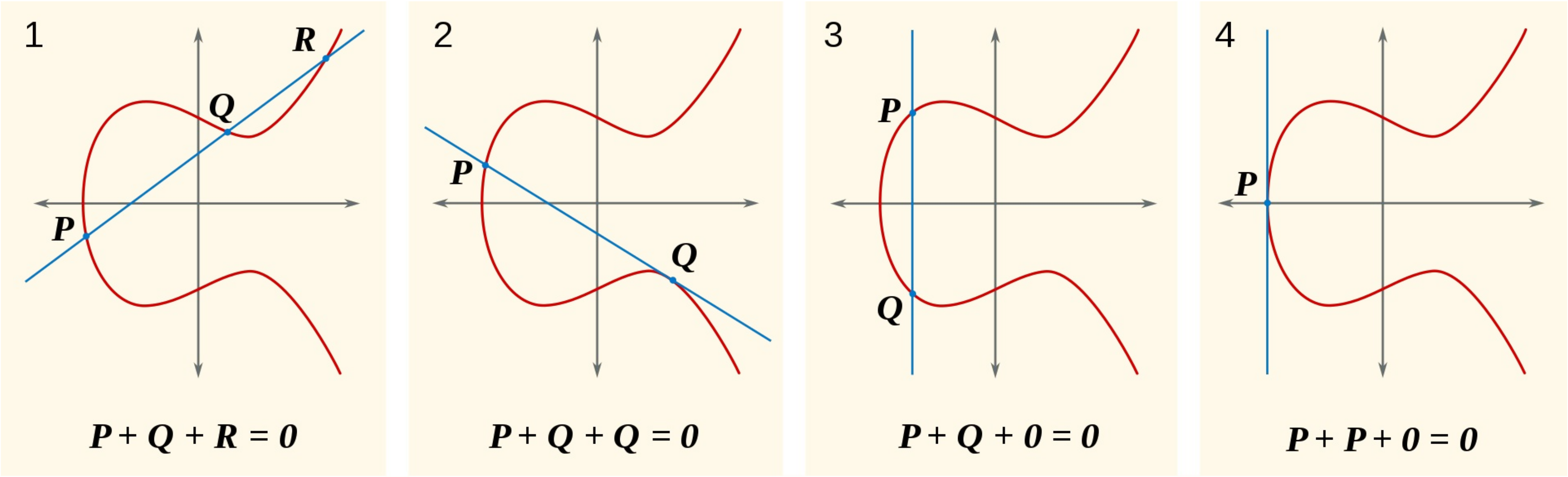
$$y^2 = x^3 + ax + b$$

Following figures are from…

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

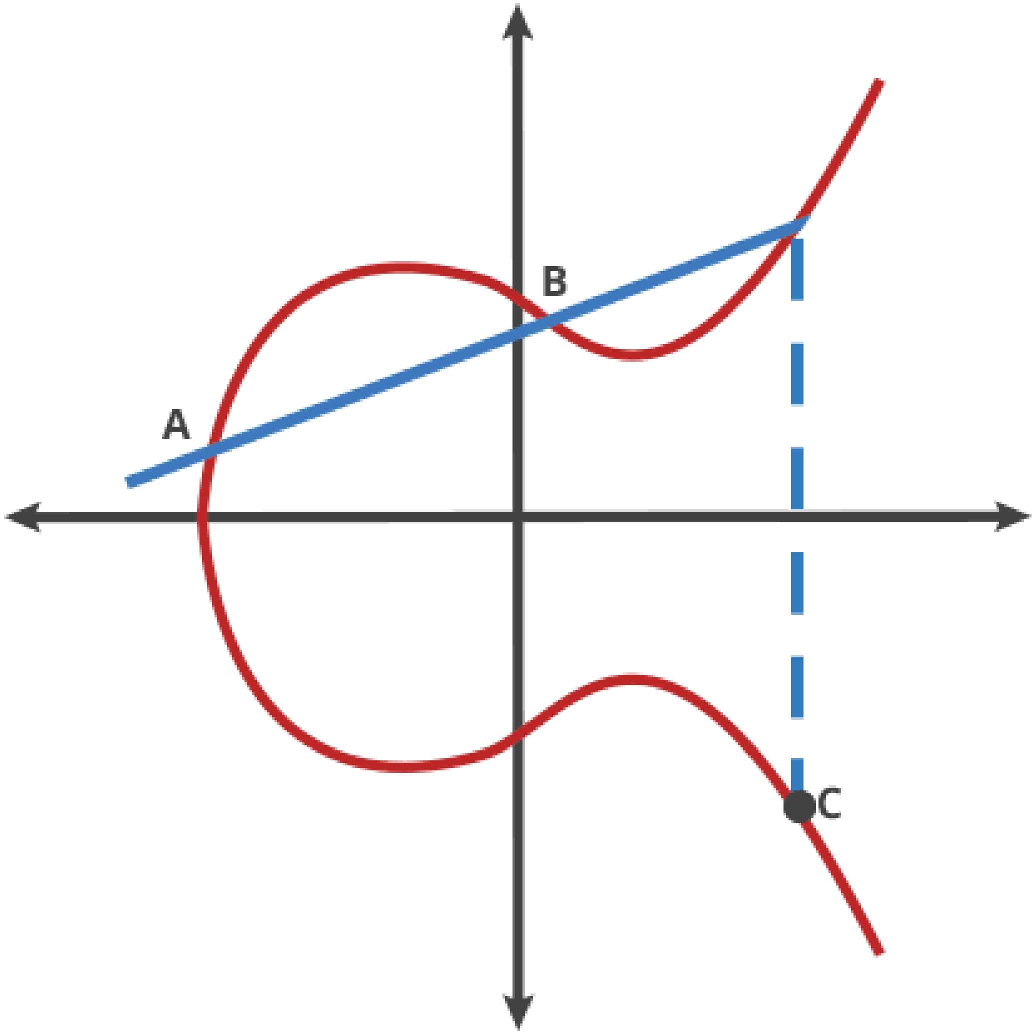


https://en.wikipedia.org/wiki/Elliptic_curve_point_multiplication#/media/File:ECClines.svg



O is point at infinity, serves as identity

How to calculate “C = A + B”?

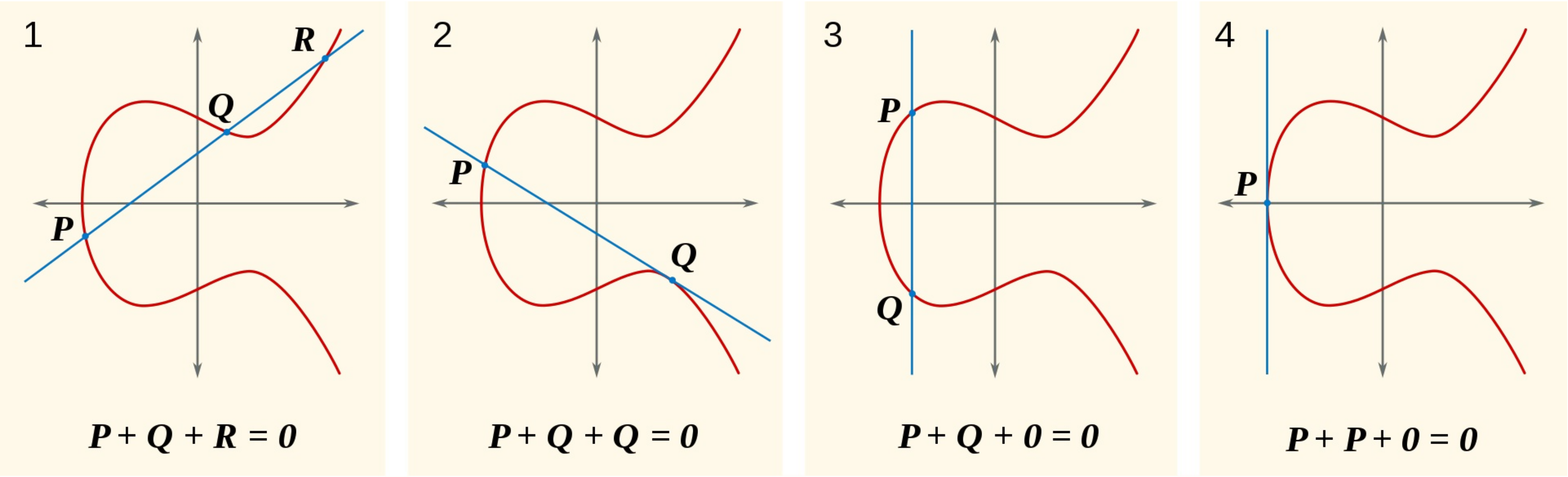


A
B
C

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

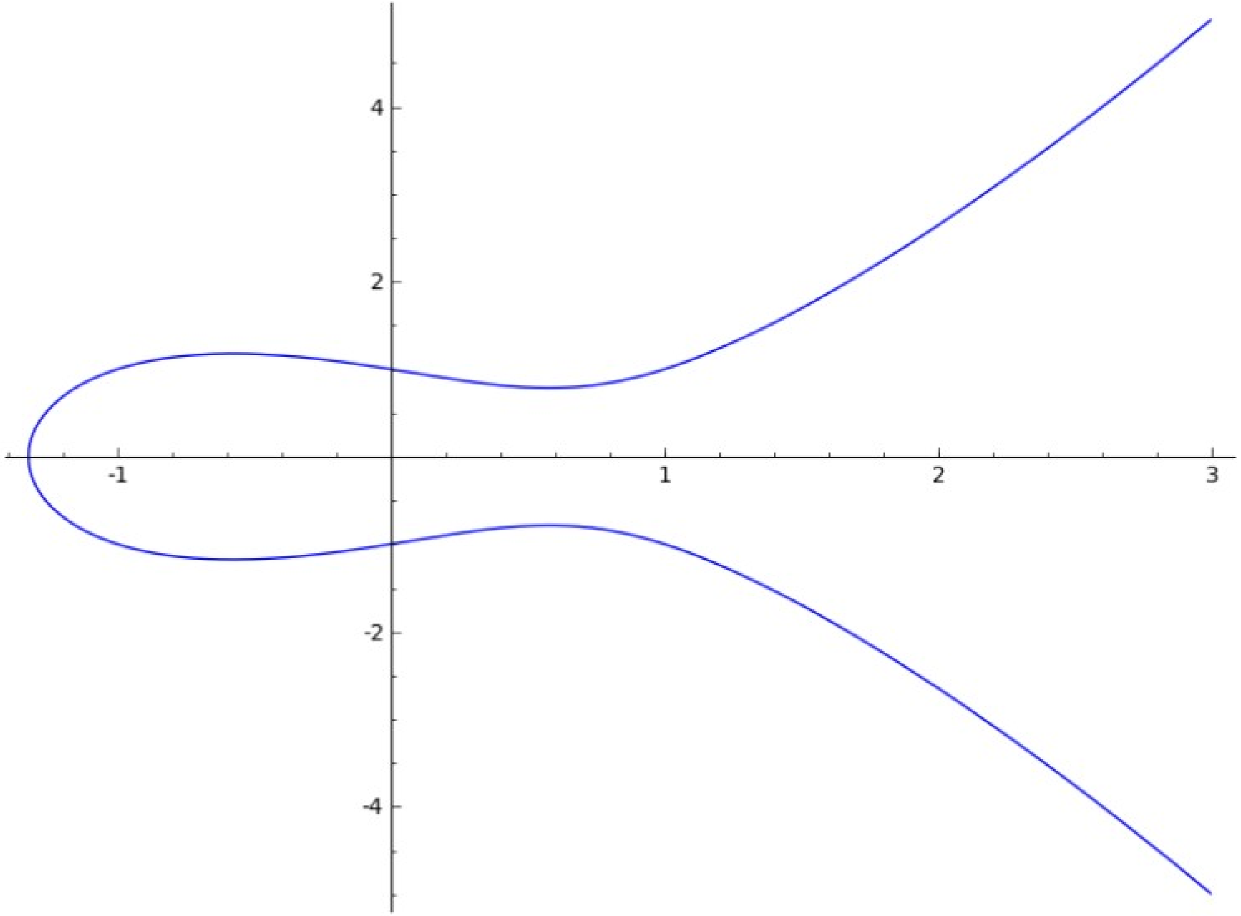
How to calculate?

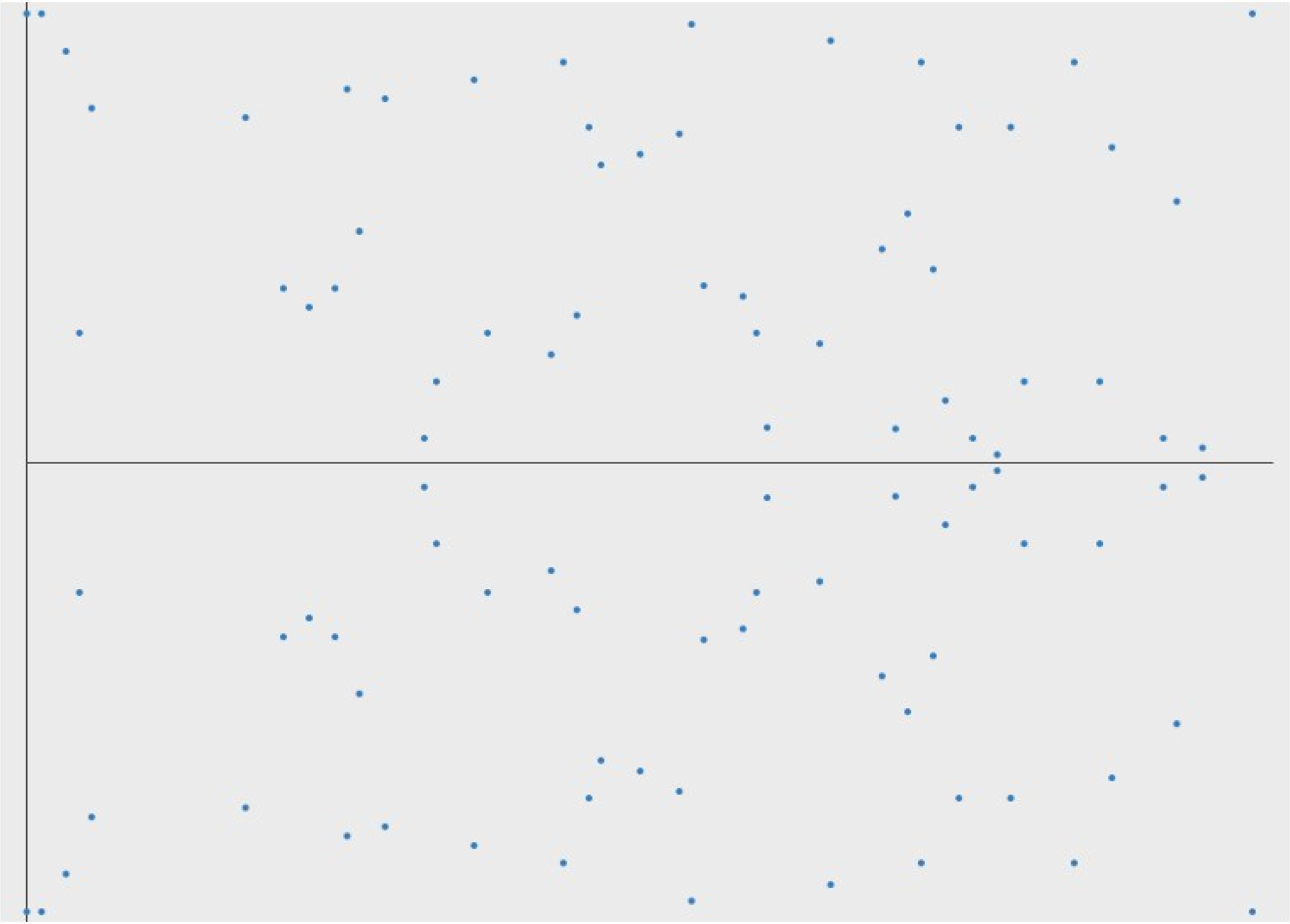
- C = -A (negation)
- C = 2A (doubling)
  - Or, C = A + A
- C = nA
  - What if n is some astronomically large number?
    - Double and add (like “square and multiply” for modular exponentiation) … Trap door function!

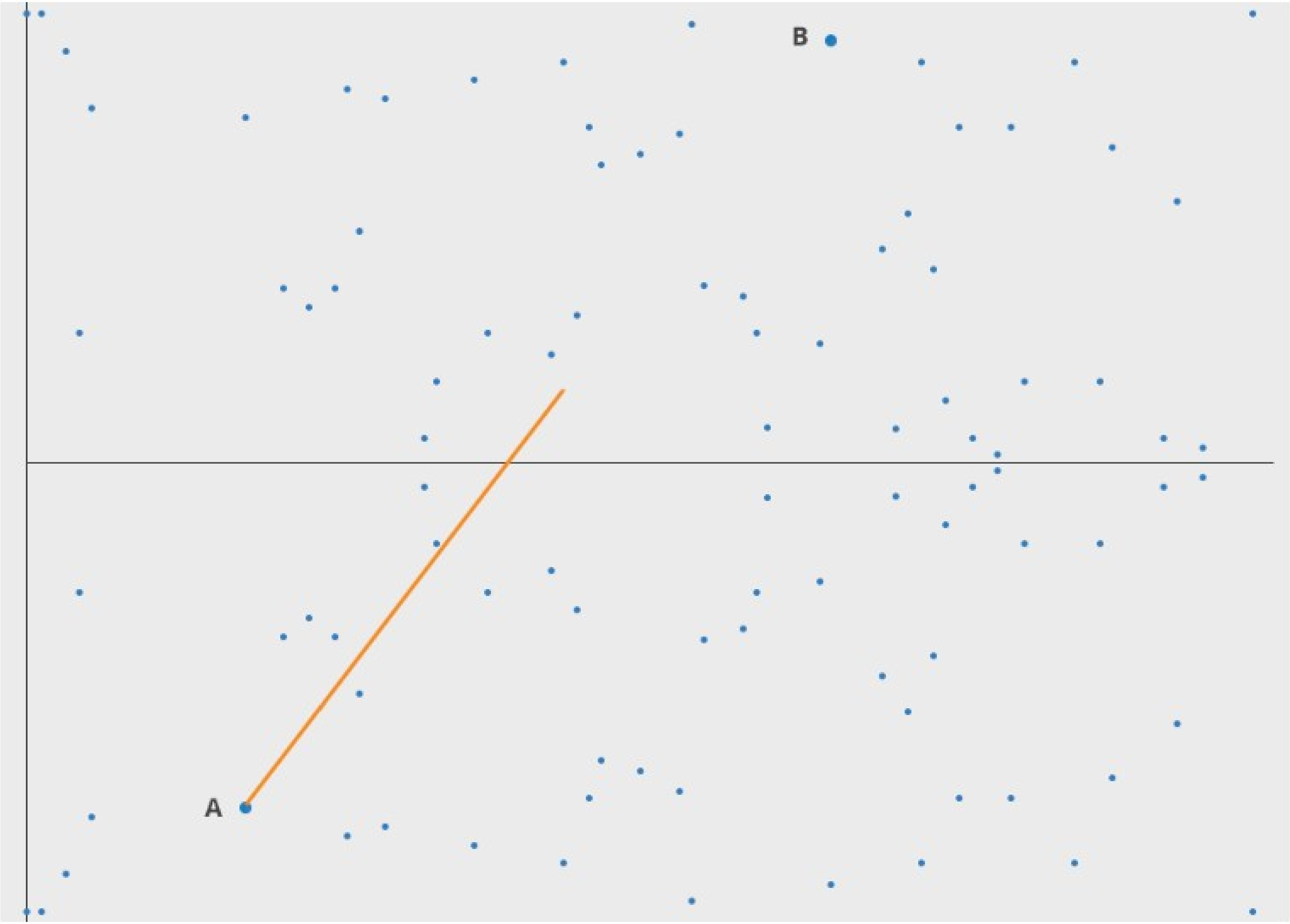
More figures stolen from…

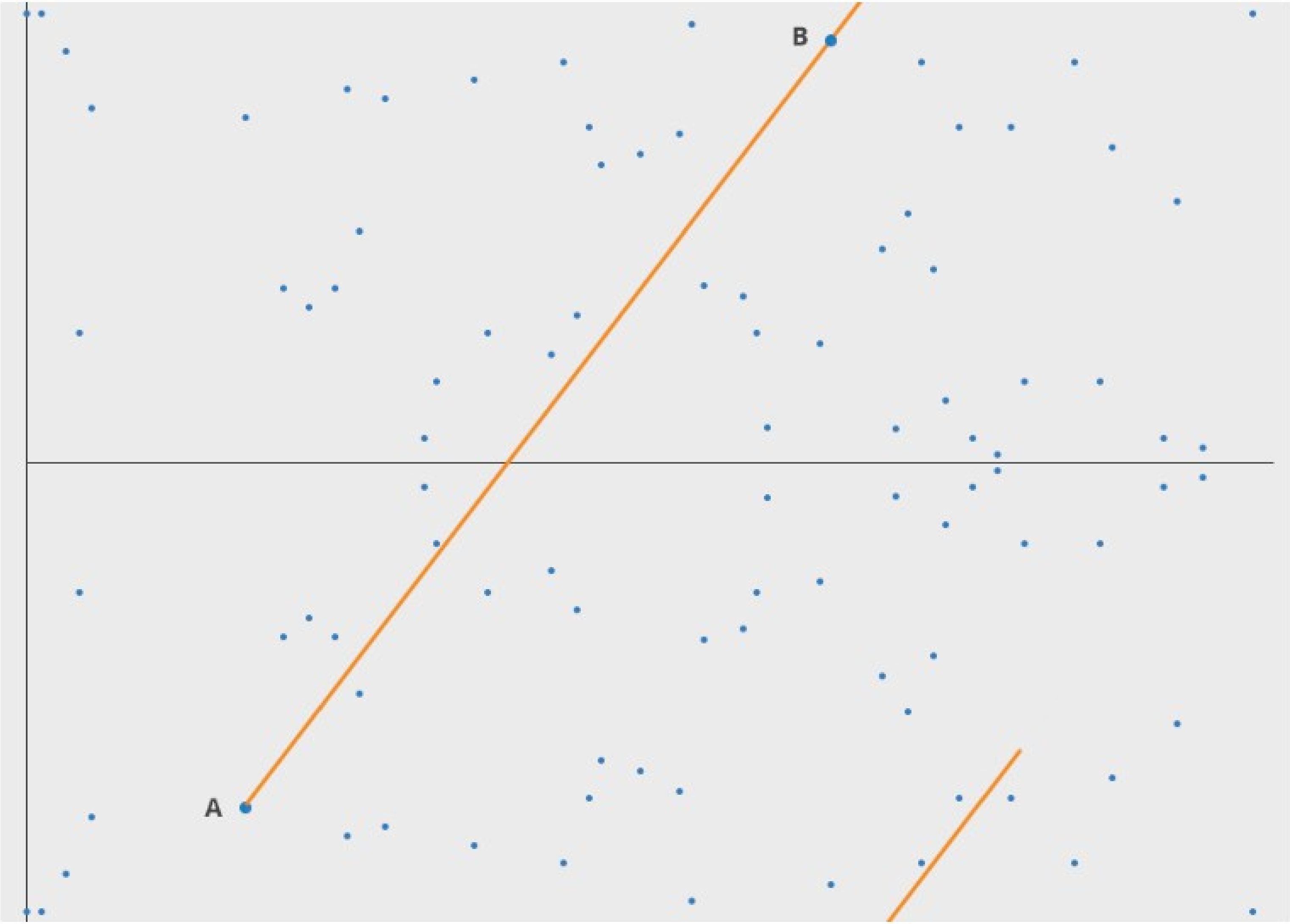
https://blog.cloudflare.com/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography/

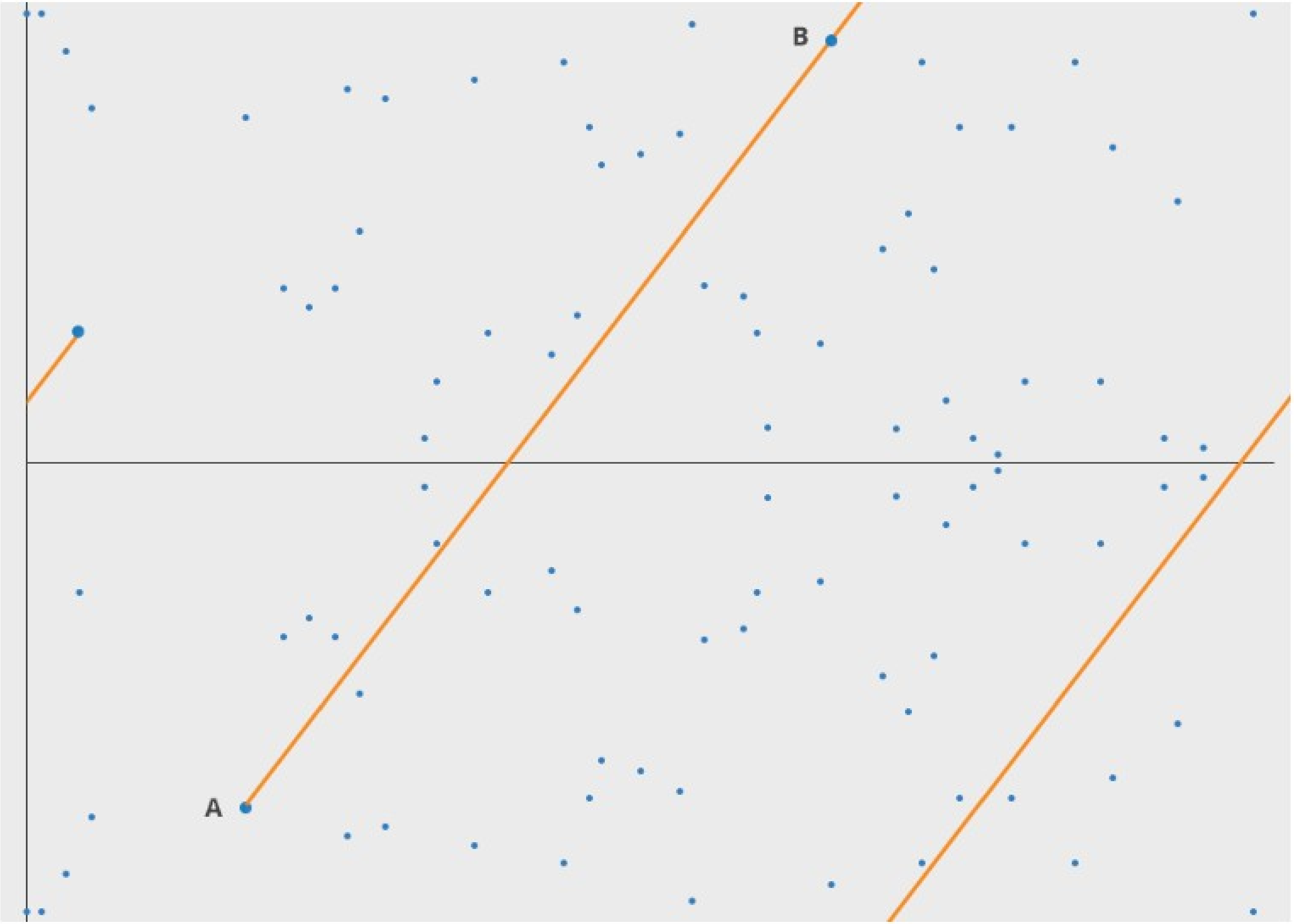
Here's an example of a curve ($y^2 = x^3 - x + 1$) plotted for all numbers:

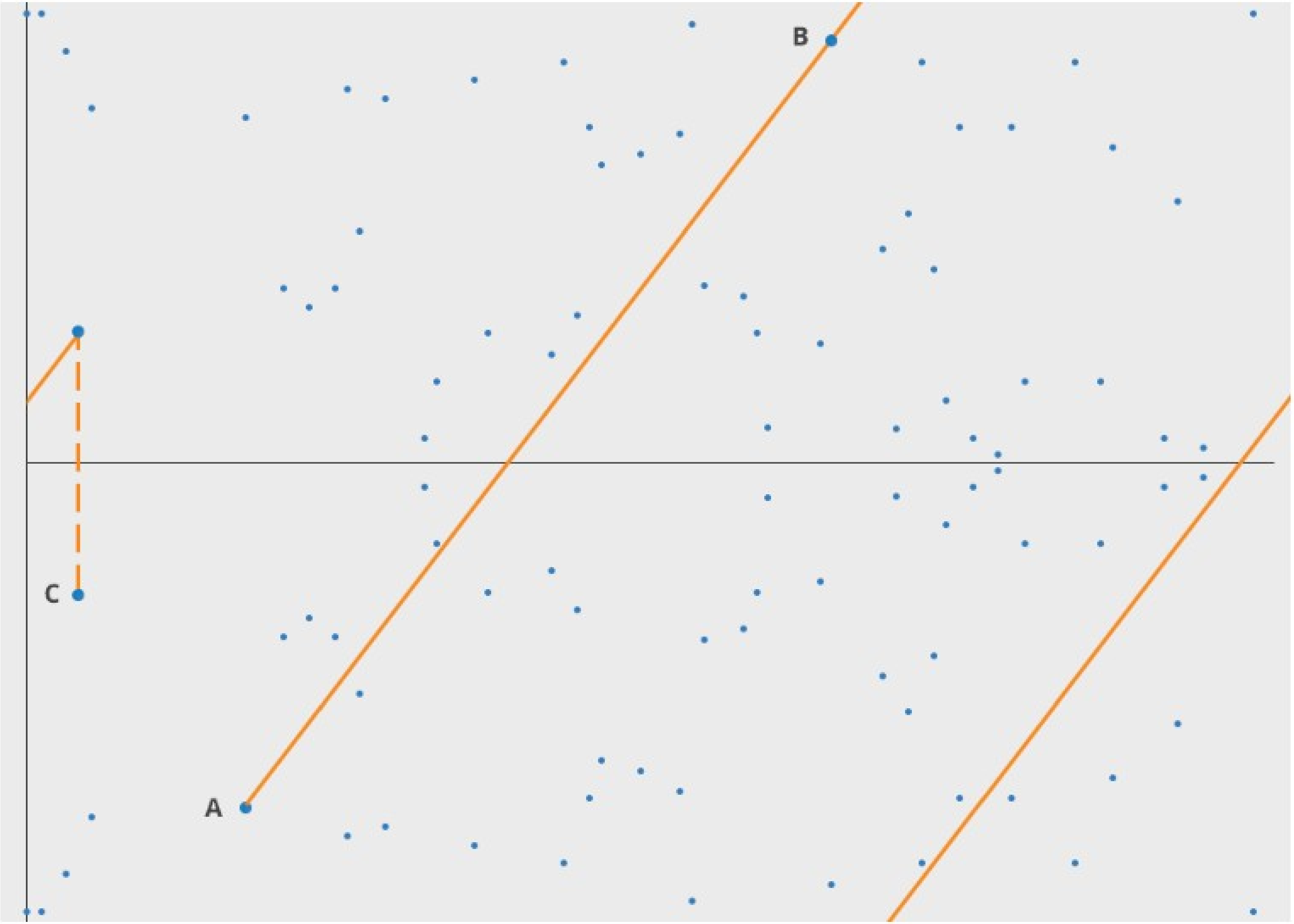





B
A

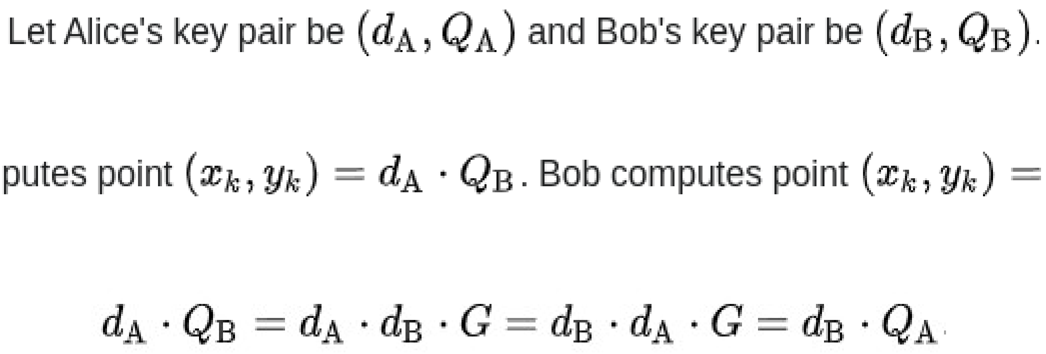

B
A


B
A


B
C
A

ECDH

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



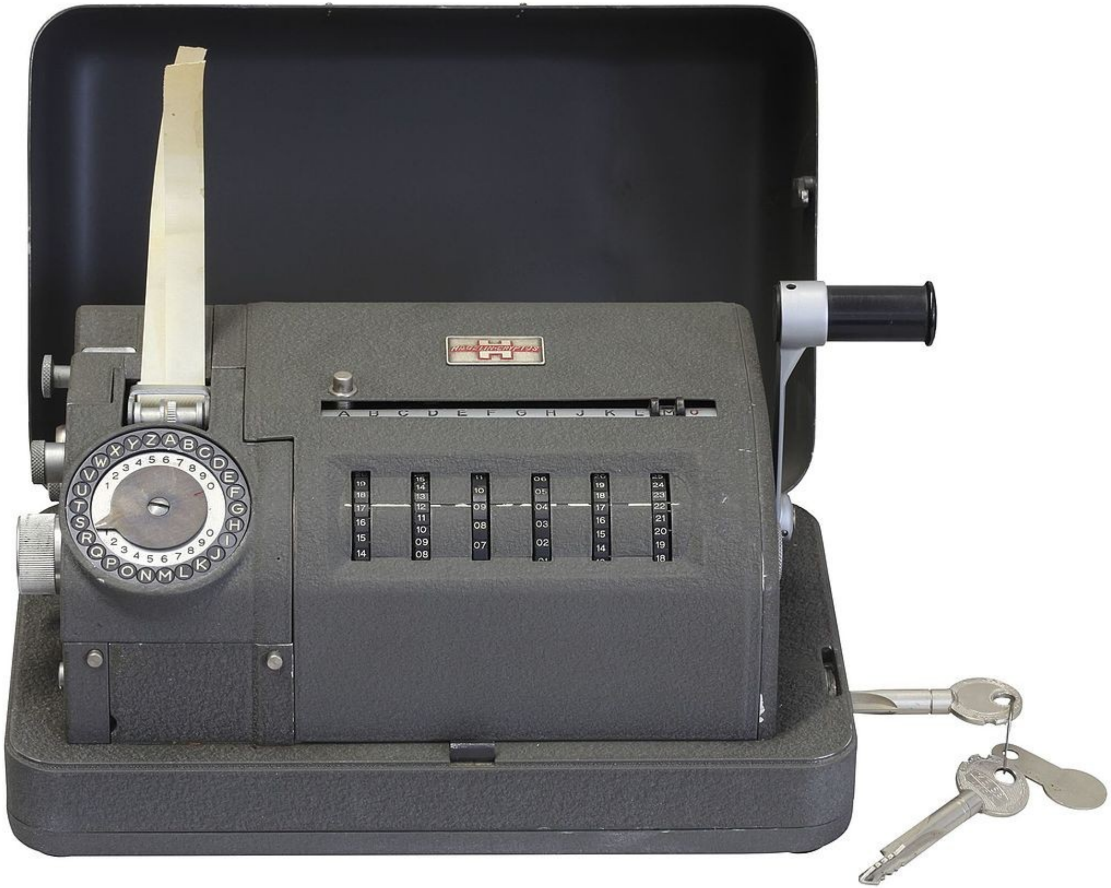
Let Alice's key pair be $(d_{\text{A}}, Q_{\text{A}})$ and Bob's key pair be $(d_{\text{B}}, Q_{\text{B}})$.

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

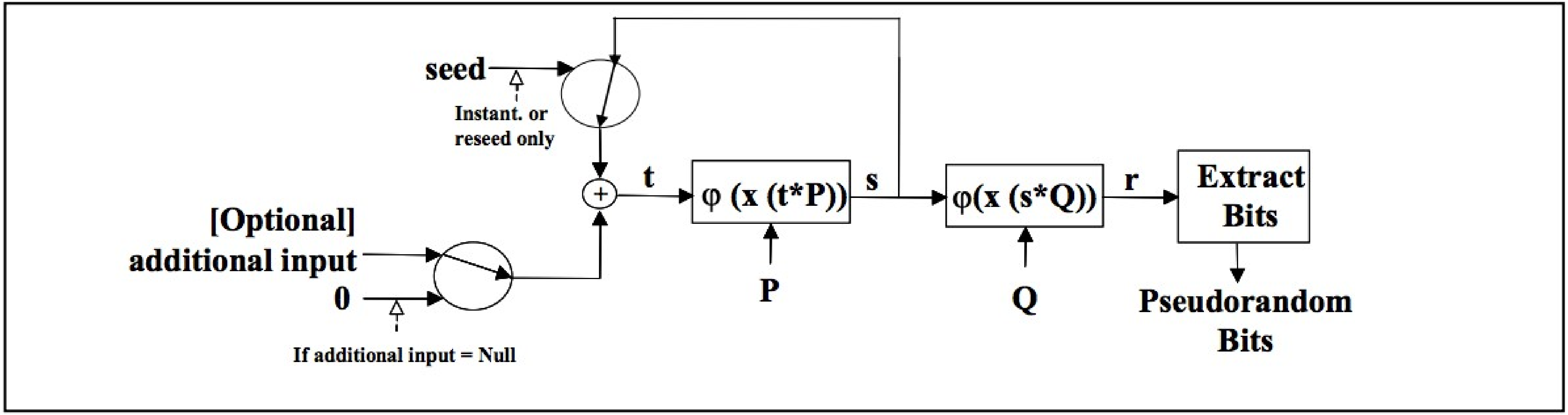
$$d_{\text{A}} \cdot Q_{\text{B}} = d_{\text{A}} \cdot d_{\text{B}} \cdot G = d_{\text{B}} \cdot d_{\text{A}} \cdot G = d_{\text{B}} \cdot Q_{\text{A}}.$$

Can also do...

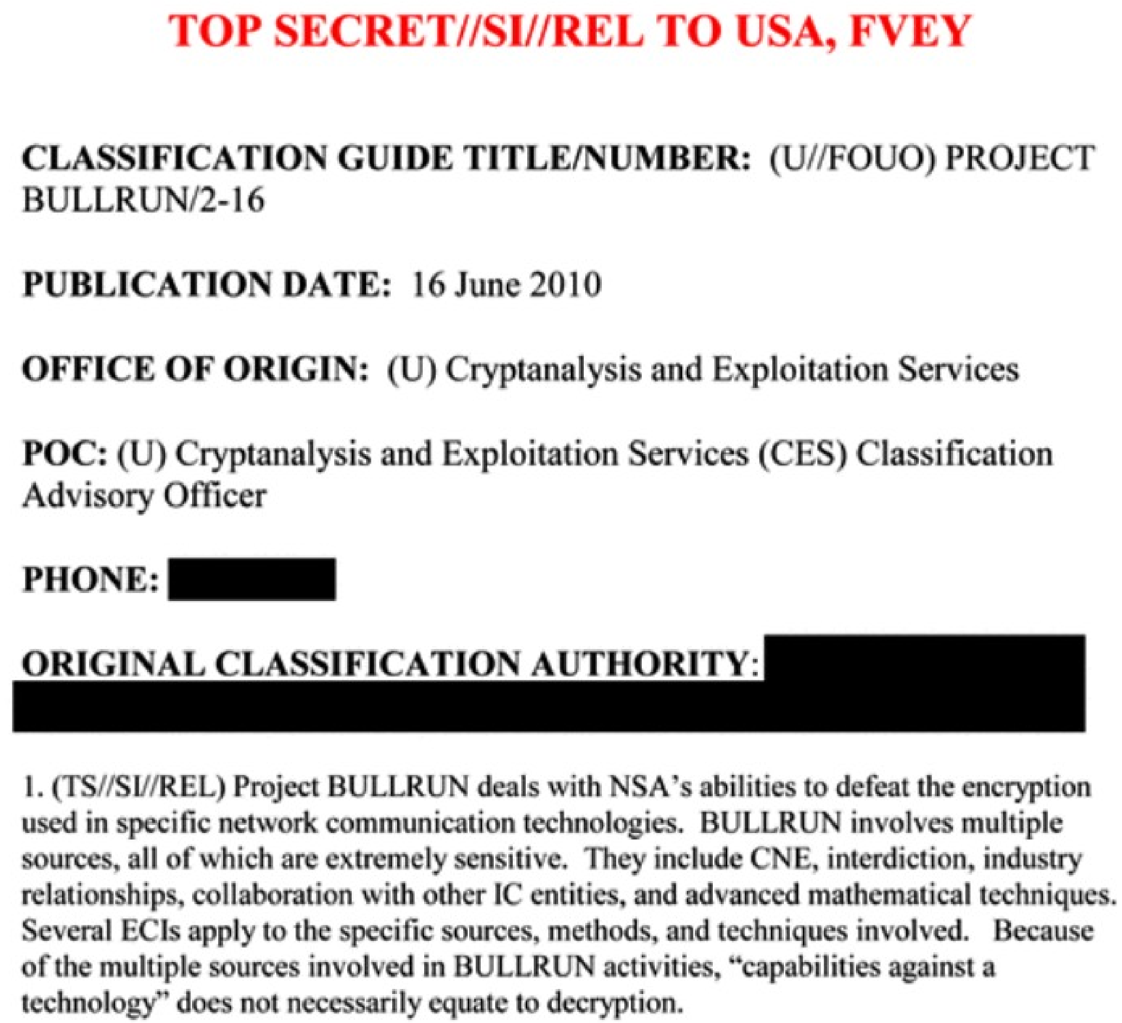
- Elliptic Curve Digital Signature Algorithm (ECDSA)
  - PlayStation 3 signing key leak
- Elliptic Curve Integrated Encryption Scheme (ECIES)



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

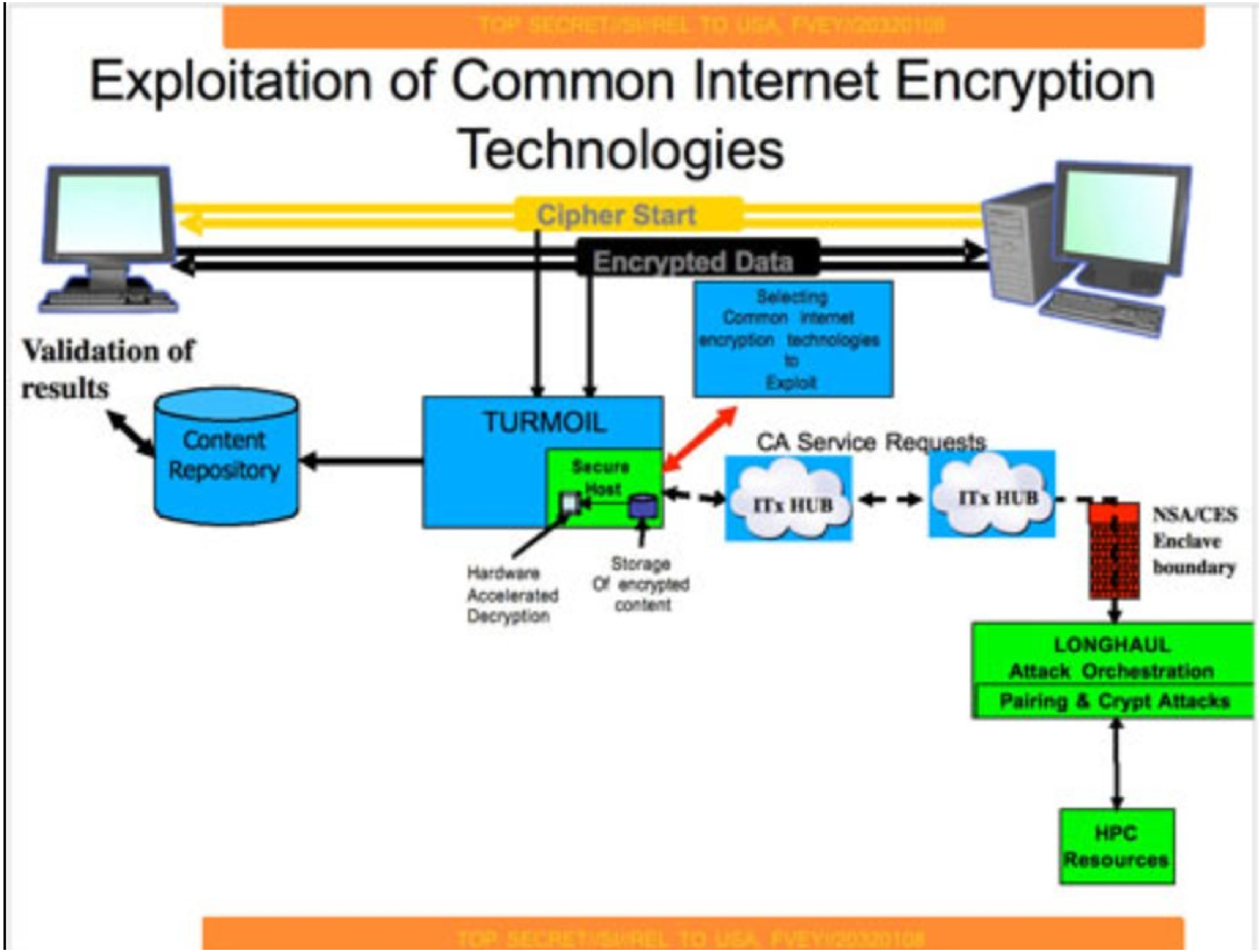
POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

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

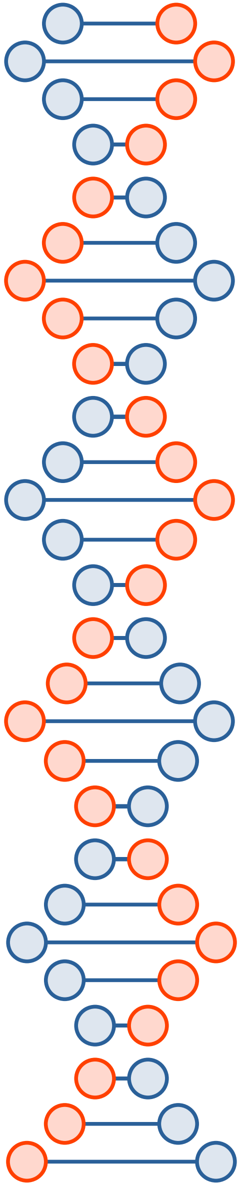
https://upload.wikimedia.org/wikipedia/commons/e/e1/NSA-diagram-001.jpg

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

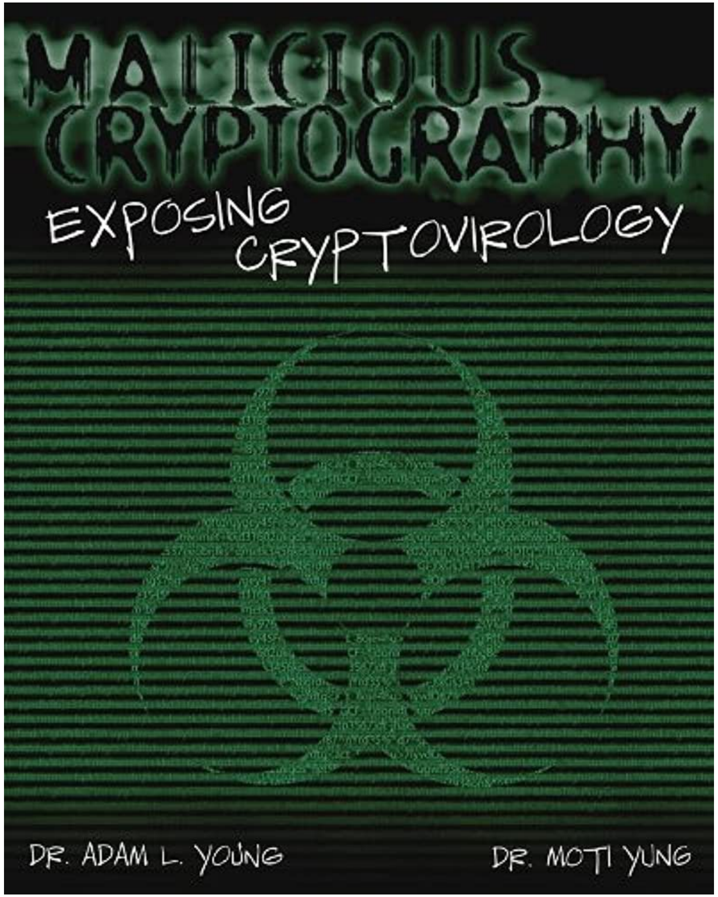
If you’re interested in more…

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



Other examples of asymmetric crypto...

Crypto is more than just sending messages

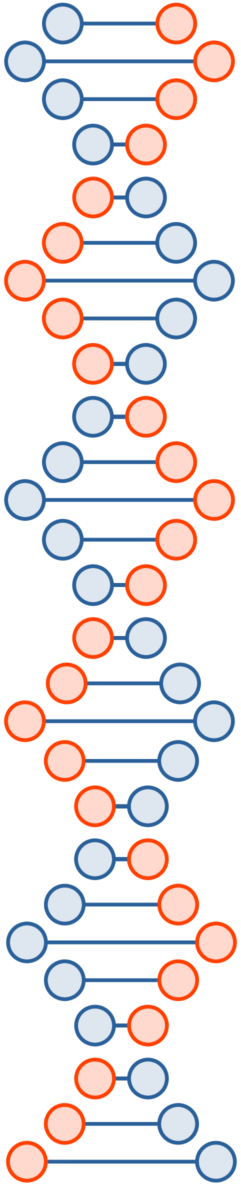


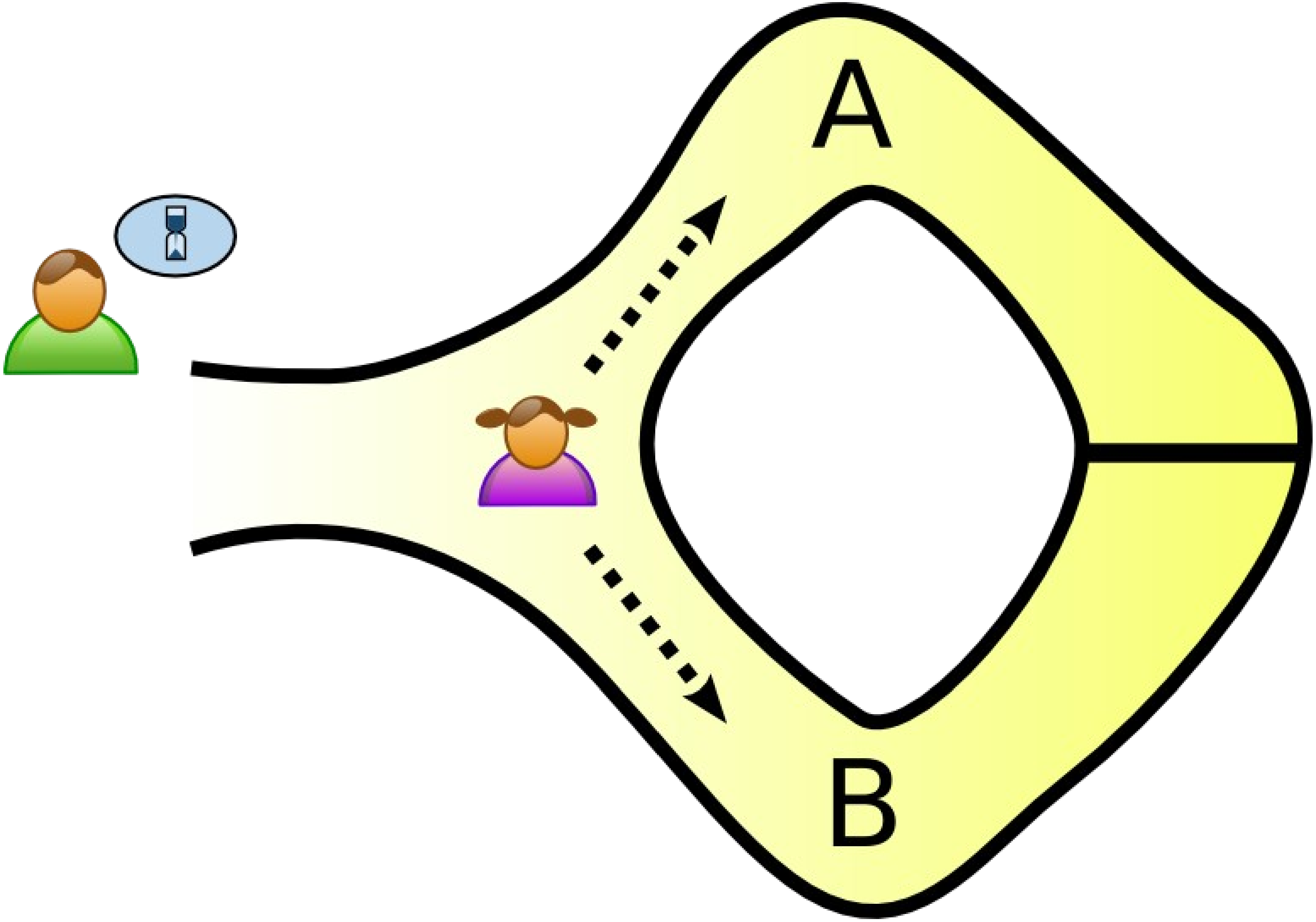
A sampling of topics

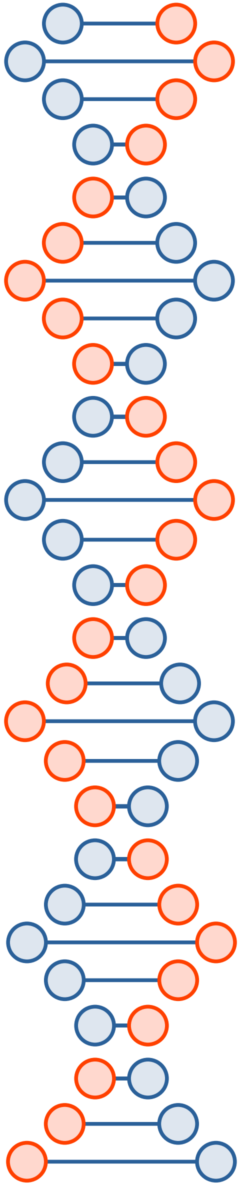
- Zero Knowledge Proofs
- Commitment scheme
- Secret sharing
- ThreeBallot

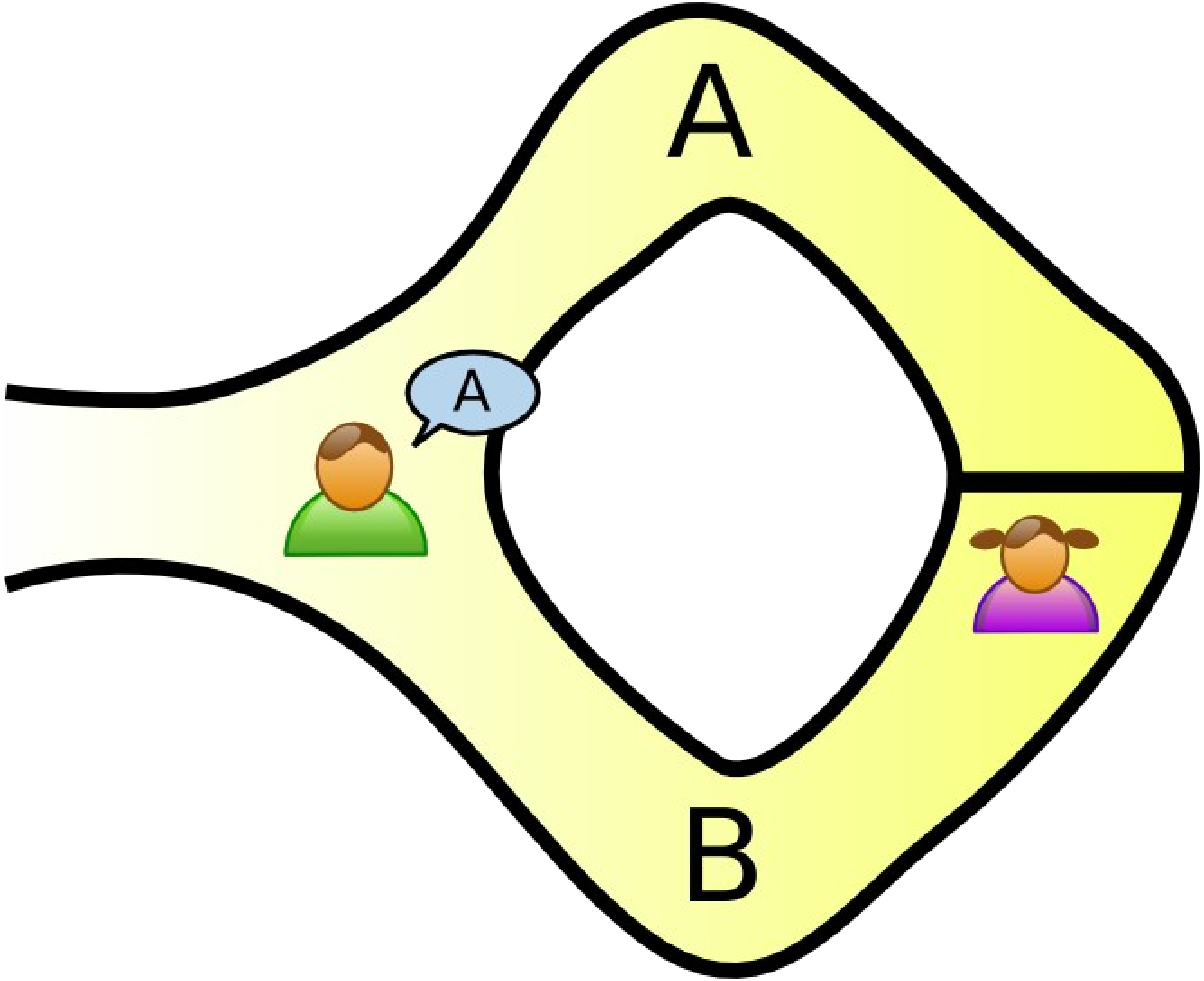
Zero Knowledge Proofs

- “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)

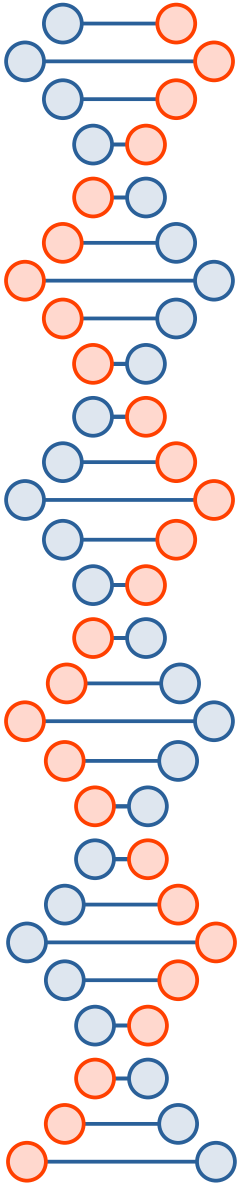


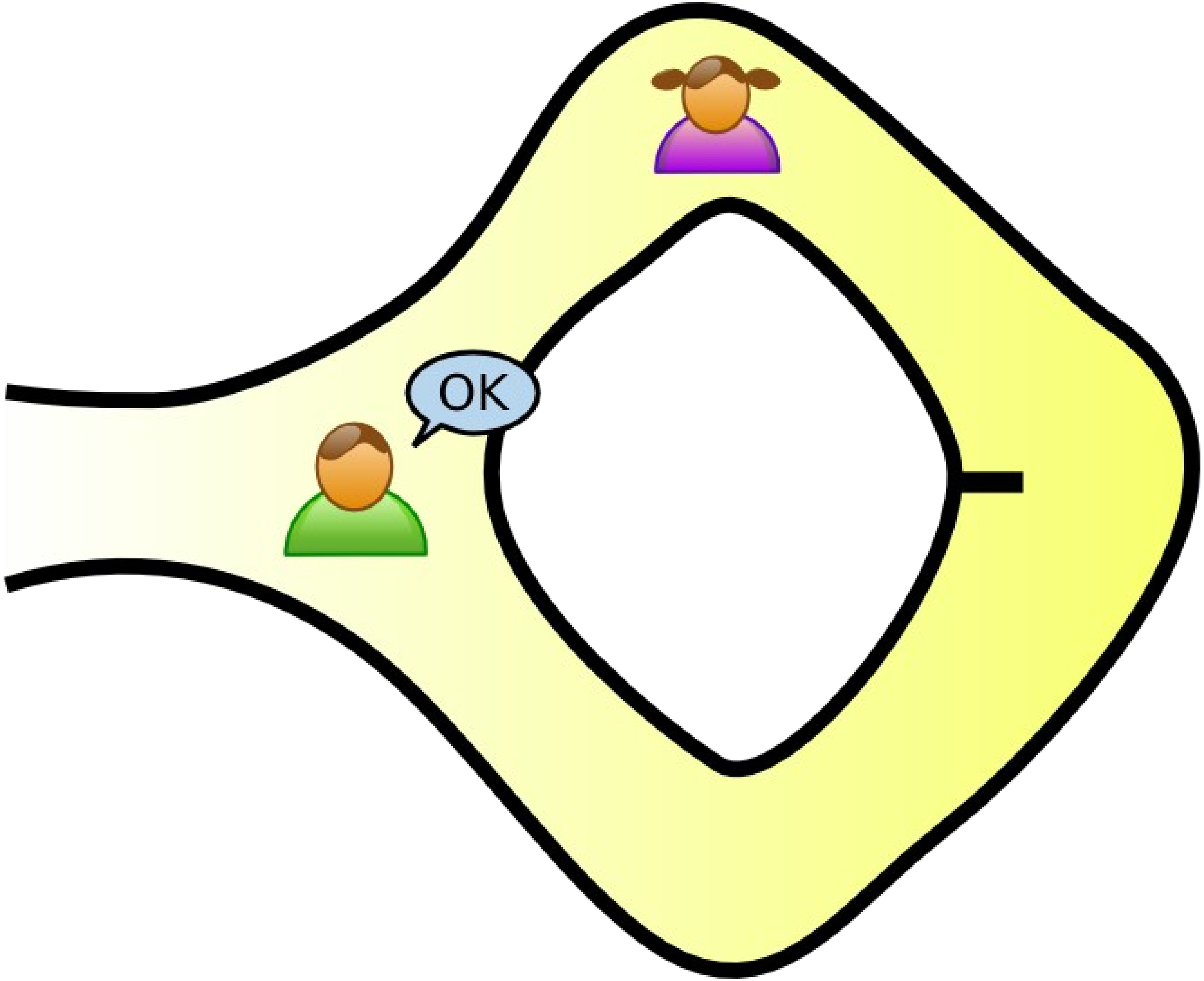

A
B

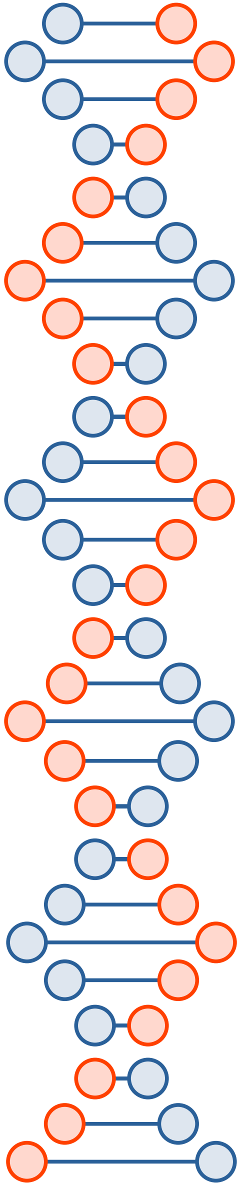


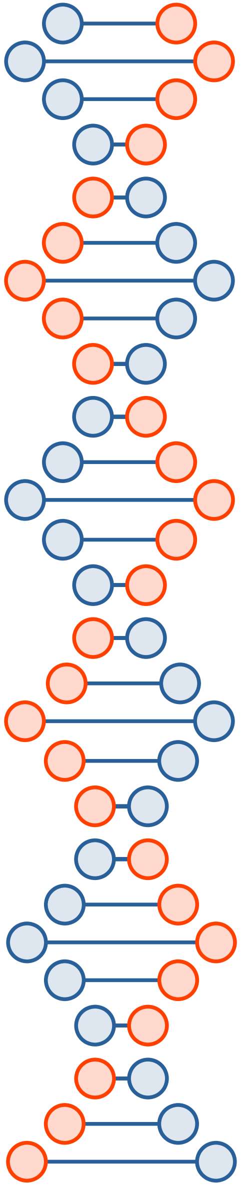


A
A
B



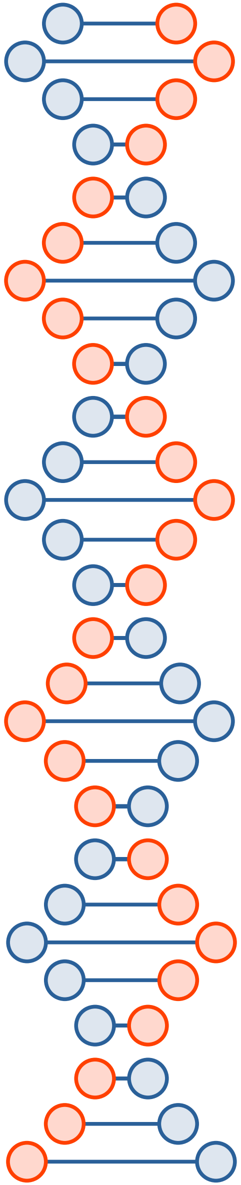

OK





Some definitions

- “Completeness: if the statement is true, an honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.
- Soundness: if the statement is false, no cheating prover can convince an honest verifier that it is true, except with some small probability.
- Zero-knowledge: if the statement is true, no verifier learns anything other than the fact that the statement is true.”



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) mod (p – 1)**

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

Applications

- Signal’s anonymous credentials
- Blockchain
- Voting: verify your vote without revealing who you voted for
- Finance: verify your income is in a certain range
- Many more...

Commitment scheme

- Bob and Alice are getting a divorce (Coin Flipping by Telephone, *Manual Blum*)…
  - Hash(randomnumber, “heads”)
  - Can enforce randomness of bits
- Mental poker

$$D(E(M)) \equiv (E(M))^{d} \equiv (M^{e})^{d} \equiv M^{e*d} \pmod{n}$$

$$E(D(M)) \equiv (D(M))^{e} \equiv (M^{d})^{e} \equiv M^{e*d} \pmod{n}$$

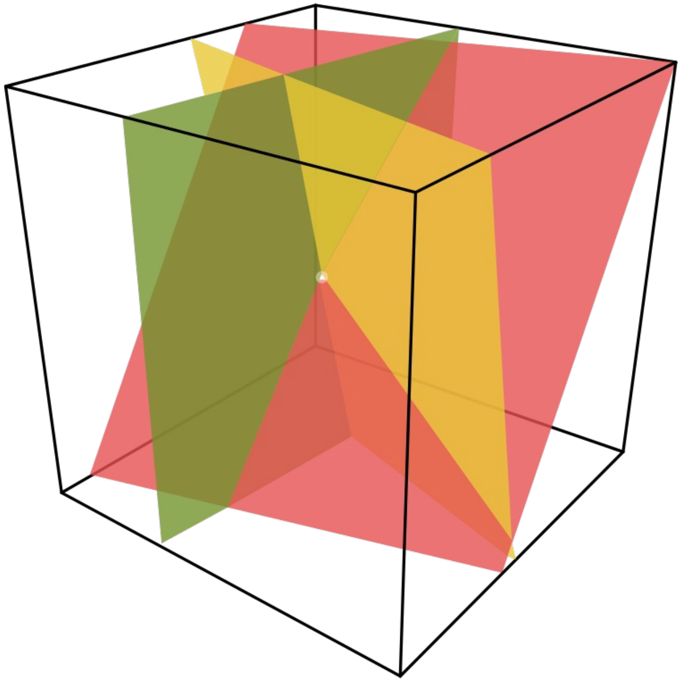
Moving in the direction of oblivious transfer and secure multiparty computation…

Oblivious Transfer

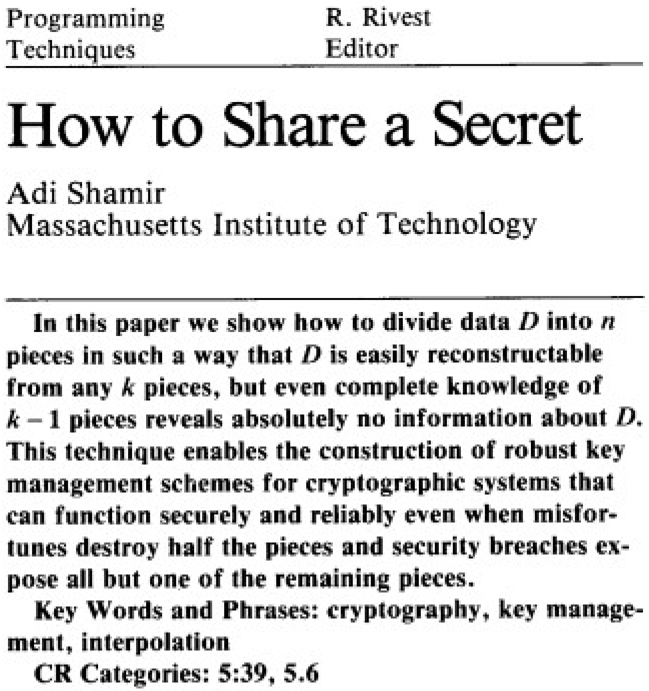
- *How to exchange secrets with oblivious transfer*, Rabin 1981
- Wikipedia: “an oblivious transfer (OT) protocol is a type of protocol in which a sender transfers one of potentially many pieces of information to a receiver, but remains oblivious as to what piece (if any) has been transferred.”
- “given an implementation of oblivious transfer it is possible to securely evaluate any polynomial time computable function without any additional primitive”

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

Secret sharing



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



Programming Techniques

R. Rivest
Editor

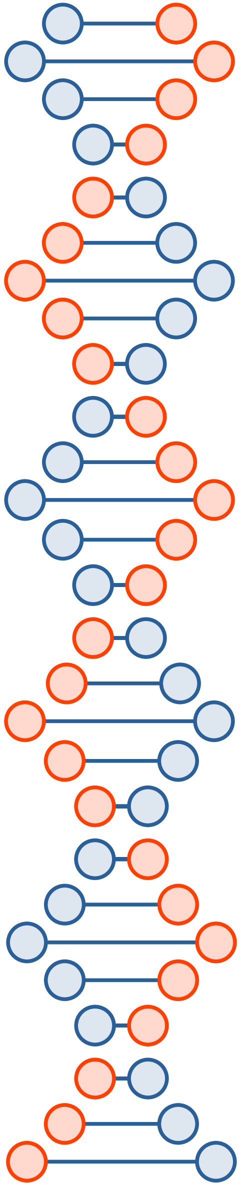
How to Share a Secret

Adi Shamir
Massachusetts Institute of Technology

In this paper we show how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of $k-1$ pieces reveals absolutely no information about D. This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces.

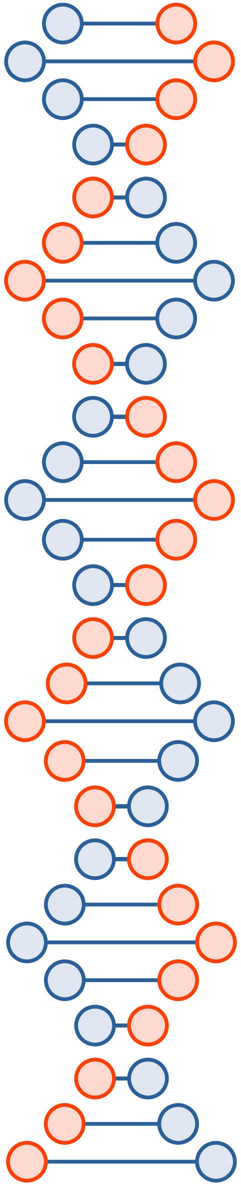
Key Words and Phrases: cryptography, key management, interpolation

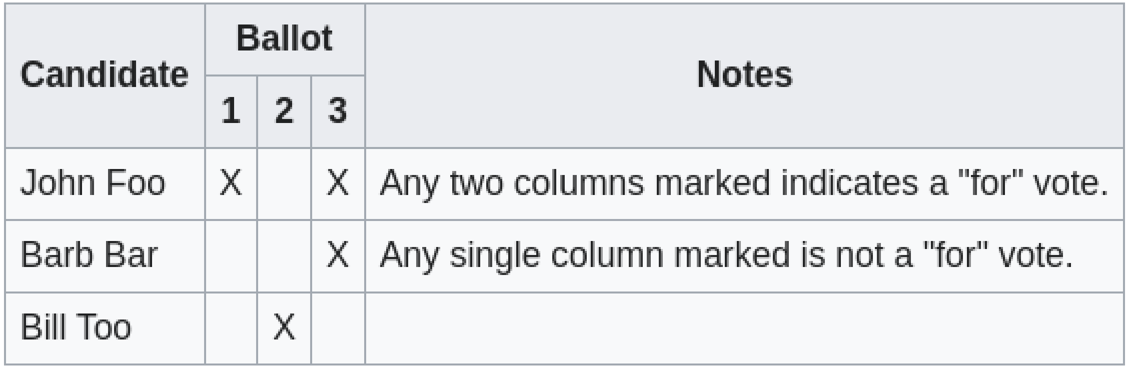
CR Categories: 5:39, 5.6



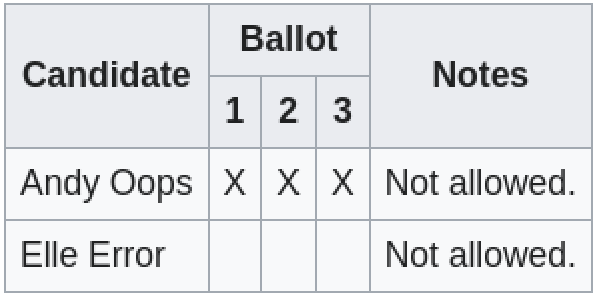
ThreeBallot (https://en.wikipedia.org/wiki/ThreeBallot)

- Proposed by Ron Rivest in 2006
- Voting principles in the U.S.
  - You should be able to verify your vote was counted correctly
  - You should not be able to prove to anybody who you voted for





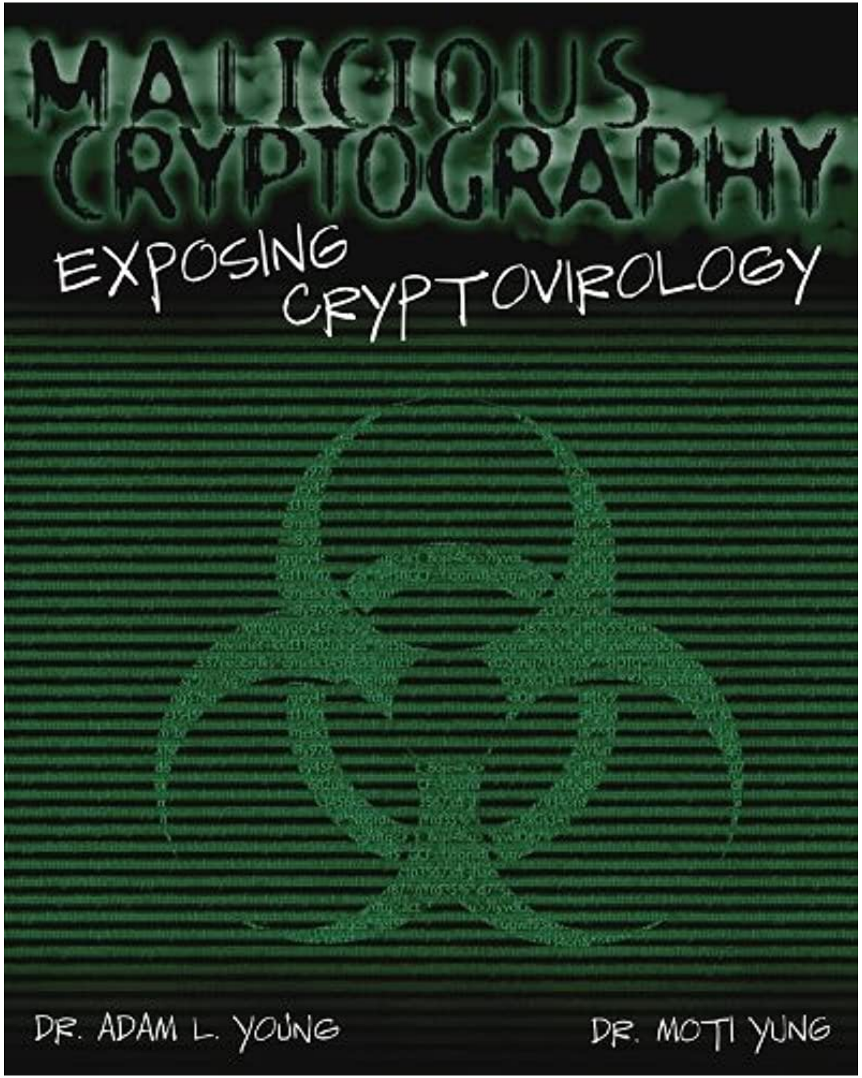
Candidate	Ballot			Notes
	1	2	3	
John Foo	X		X	Any two columns marked indicates a "for" vote.
Barb Bar			X	Any single column marked is not a "for" vote.
Bill Too		X		

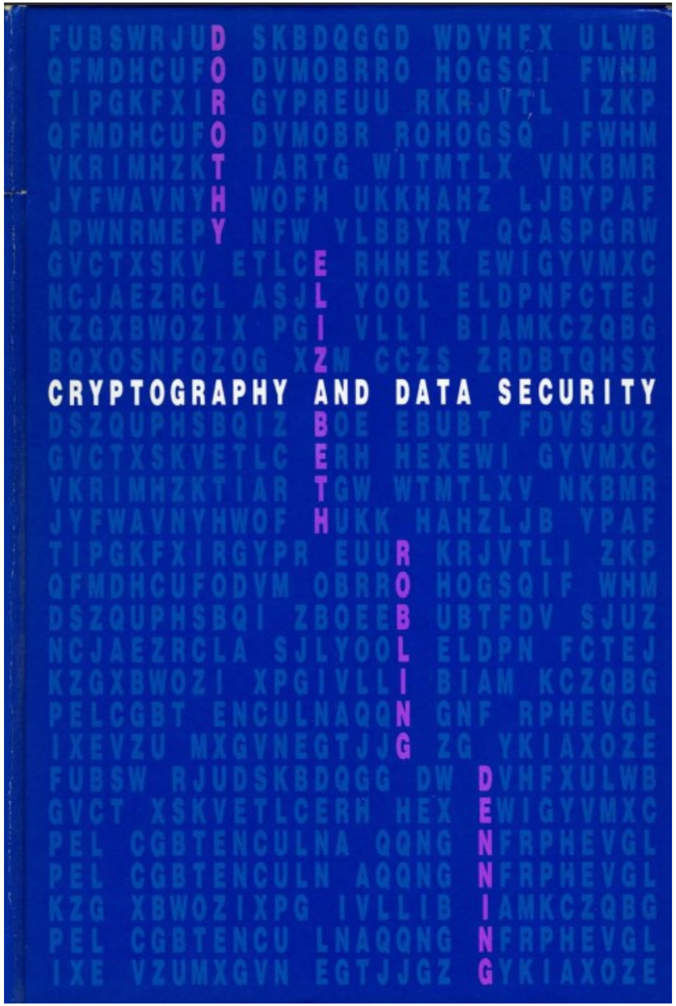


Candidate	Ballot			Notes
	1	2	3	
Andy Oops	X	X	X	Not allowed.
Elle Error				Not allowed.

ThreeBallot

- All three ballots must be checked for compliance
  - Should vote twice for candidate you like, once for candidates you don’t
  - After this check, the entire stack of ballots should be shuffled
- The voter gets to track one ballot
  - 1/3 chance tampering with votes is detected by each voter
  - Number of votes that cancel out should be equal to the number of voters
- The voter can’t prove to anybody how they actually voted


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



CRYPTOGRAPHY AND DATA SECURITY

DOROTHY ELIZABETH ROBLING DENNING

To prepare for the next lecture...

- https://jedcrandall.github.io/courses/cse539spring2023/Rsapaper.pdf