Modern Applications of Cryptography

Youssef El Housni | yelhousni.eth

Consensys
New York City | United States

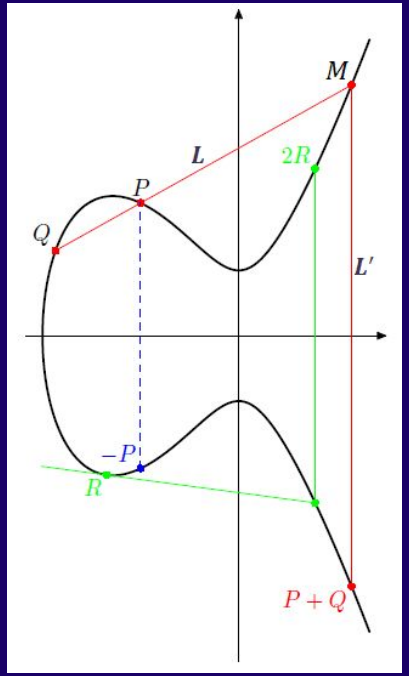
Linea


Linea
VISA
MasterCard

Linea

$$f(x) = a_0 + a_1 x + \cdots + x_n x^n, a_i \in \mathbb{Z}/p\mathbb{Z}$$

$$x^{p-1} \equiv 1 \pmod{p}$$



$$A_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

$$\mathbb{P}(X) \quad \mathbb{P}(X) \quad \mathbb{P}\left(\frac{X}{2}\right)$$

$$\mathbb{P}(X \mid Y) \quad \mathbb{P}(X \mid Y) \quad \mathbb{P}\left(\frac{X}{2} \,\middle|\, Y\right)$$

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$$

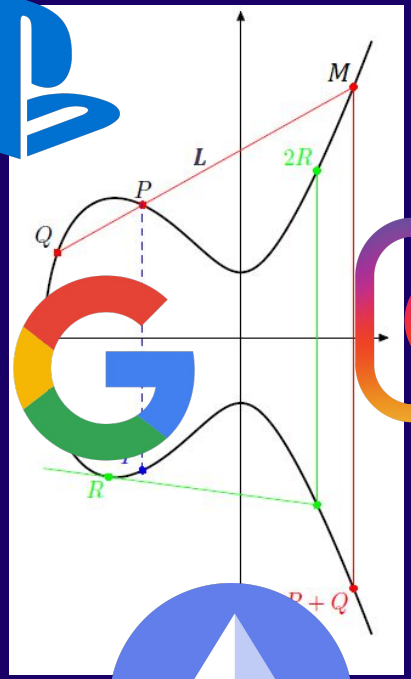
Linea

$$f(x) = a_0 + a_1 x + \cdots + x_n x^n, a_i \in \mathbb{Z}/p\mathbb{Z}$$

$$x^{p-1} \equiv 1 \pmod{p}$$

$$\mathbb{P}(X) \quad \mathbb{P}(X) \quad \mathbb{P}\left(\frac{X}{2}\right)$$

$$\mathbb{P}(X \mid Y) \quad \mathbb{P}(X \mid Y$$



$$A_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ & 22 & \cdots & a_{2n} \\ & & \ddots & \vdots \\ & 2 & \cdots & a_{mn} \end{bmatrix}$$

$$n \quad p_2^{n_2} \cdots \quad = \prod_{i=1}$$

VISA

MasterCard

Linea

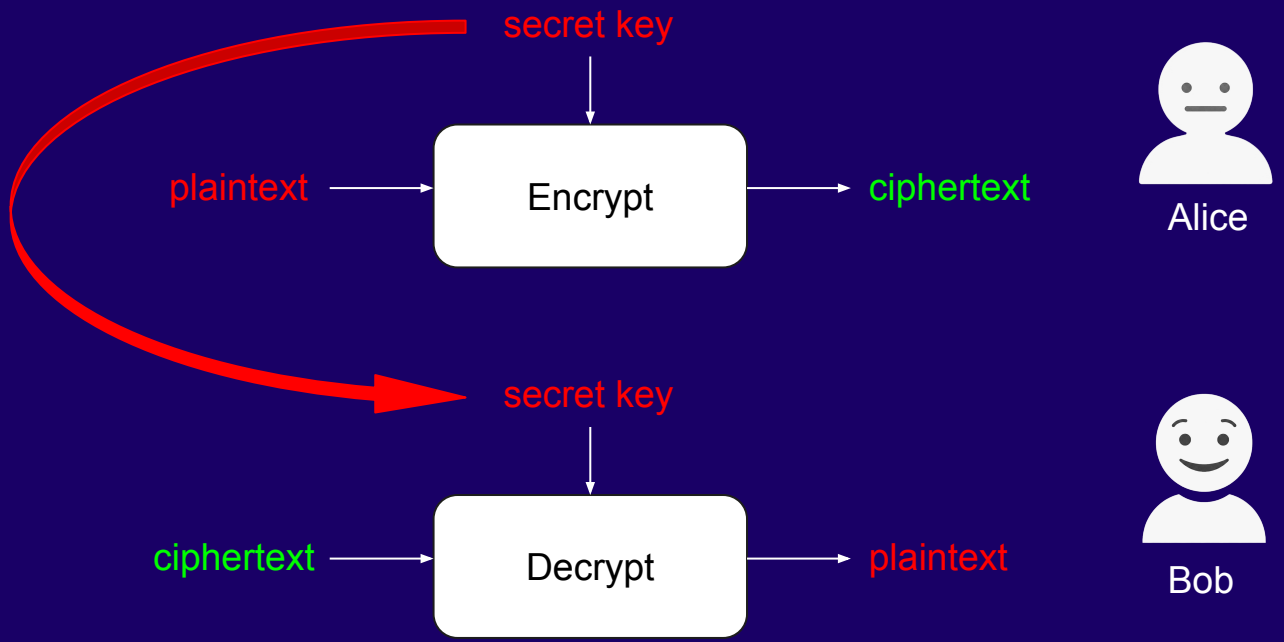
Crypt-o-graphy

- The prefix “crypt-” means hidden
- The suffix “-graphy” means writing

So, all together it says **“hidden writing”**

Linea

Encryption



Linea

Encryption

Hieroglyphs

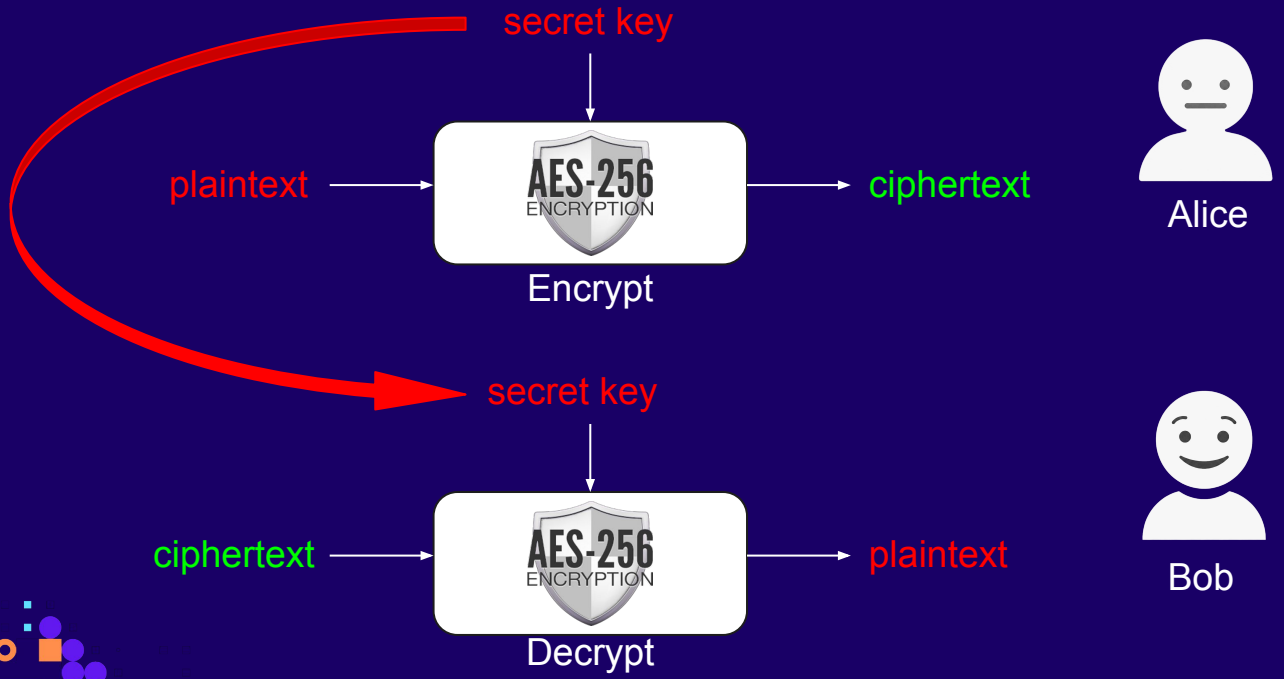
Caesar Cipher

Current standard

Enigma WWII

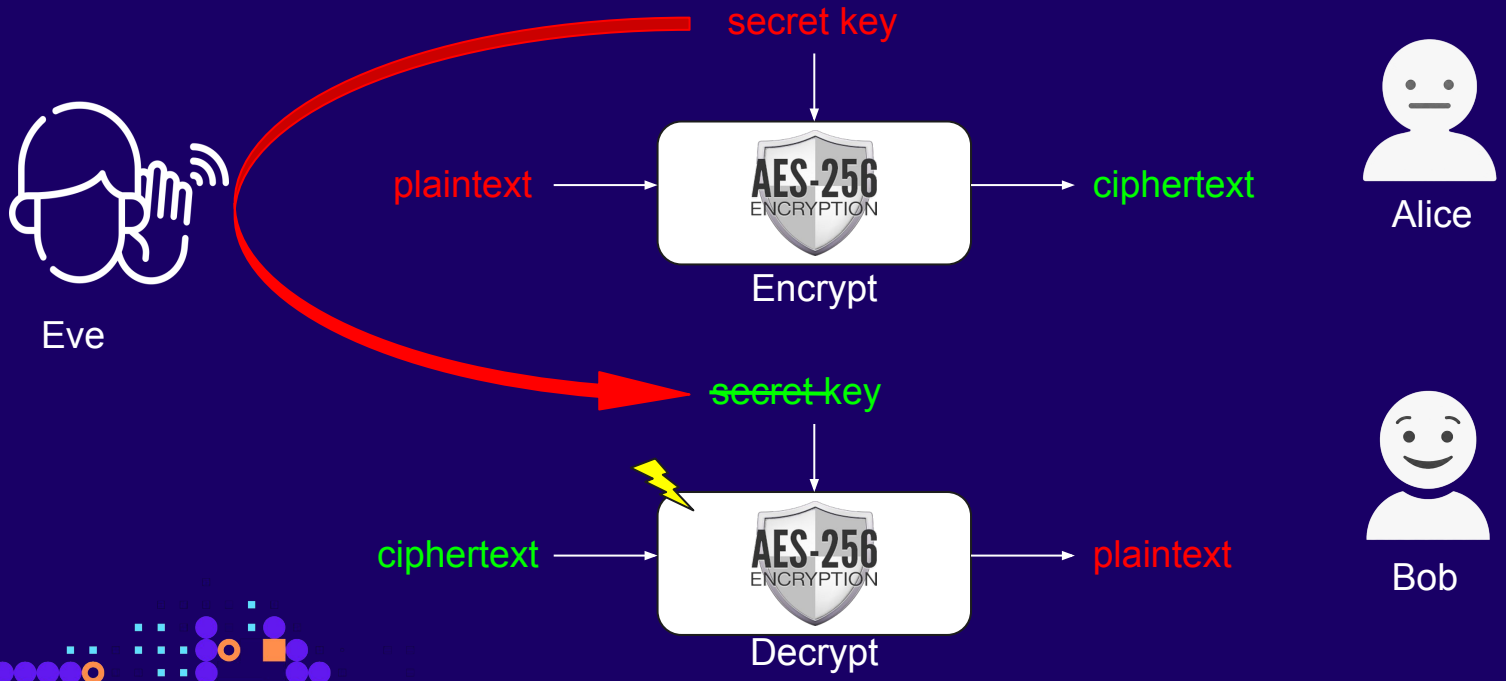
Linea

Encryption



Linea

Encryption



Linea

Public key encryption

(secret) key → (public) key

public key

plaintext → AES-256 ENCRYPTION → ciphertext

Encrypt

public key

Alice

secret key

ciphertext → AES-256 ENCRYPTION → plaintext

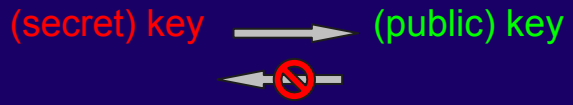
Decrypt

public key

secret key

Bob

Linea



Trapdoor function

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k} = \prod_{i=1}^{k} p_i^{n_i}$$

p_1, p_2 → $n = p_1 \cdot p_2$

$n = p_1 \cdot p_2$ ⊘→ p_1, p_2

6895601 = 1931 x 3571

LINEA

Computational complexity

n	2^n	Examples
32	$2^{32} = 10^{9.6}$	number of humans on Earth
47	$2^{47} = 10^{14.2}$	distance Earth - Sun in millimeters ($149.6 \cdot 10^{12}$) number of operations in one day on a processor at 2 GHz
56	$2^{55.8} = 10^{16.8}$	number of operations in one year on a processor at 2 GHz
79	$2^{79} = 10^{23.8}$	Avogadro number: atoms of Carbon 12 in 1 mol
82	$2^{82.3} = 10^{24.8}$	mass of Earth in kilogrammes
100	$2^{100} = 10^{30}$	number of operations in $13.77 \cdot 10^9$ years (age of the universe) on a processor at 2 GHz
155	$2^{155} = 10^{46.7}$	number of molecules of water on Earth
256	$2^{256} = 10^{77.1}$	number of electrons in universe

Linea

RSA Encryption

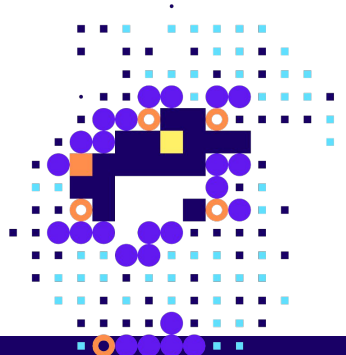
1977, Rivest, Shamir, Adleman

- modulus $N = p \times q$, p, q two distinct large primes
- arithmetic modulo N, in $\mathbb{Z}/N\mathbb{Z} = \{0, 1, \ldots, N-1\}$

The **multiplicative group** is the set of **invertible** integers in $\{1, 2, \ldots, N-1\}$.
invertible x means $gcd(x, N) = 1$, x coprime to N.
There are $\varphi(N) = (p-1)(q-1)$ invertible integers in $\{1, \ldots, N-1\}$

Hard tasks without knowing p, q if N is large enough:

- computing $(p-1)(q-1)$,
- computing a square root $\sqrt{x} = x^{1/2} \bmod N$,
- computing an e-th root $x^{1/e} \bmod N$.



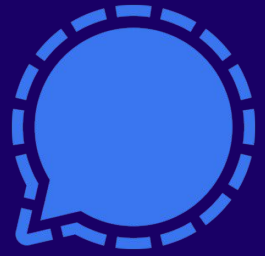
LINEA

End-to-end encryption

- By default
- Closed-source

- By default
- Closed-source

- By default
- Open-source client
- closed-source server



- By default
- Open-source client
- Open-source server

Linea

(secret) key → (public) key

Signature

$$s \cdot G \to_{\text{easy}} P$$

$$P(= s \cdot G) \to_{\text{hard}} s$$

- Only Bob can sign with s
- Alice (or anyone) can verify with P

Alice

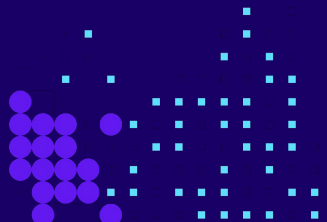
public key P

Bob

public key P

secret key s

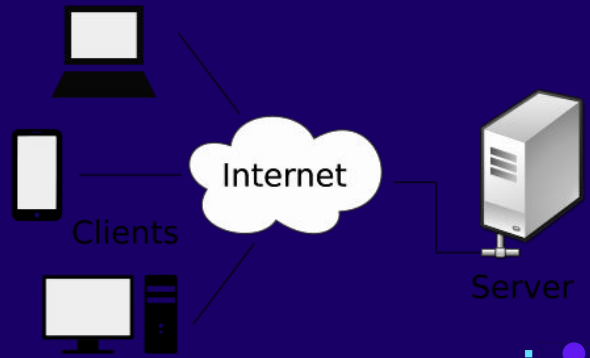
$$x^{p-1} \equiv 1 \pmod{p}$$



Traditional cryptography

https://cipherchallenge.github.io

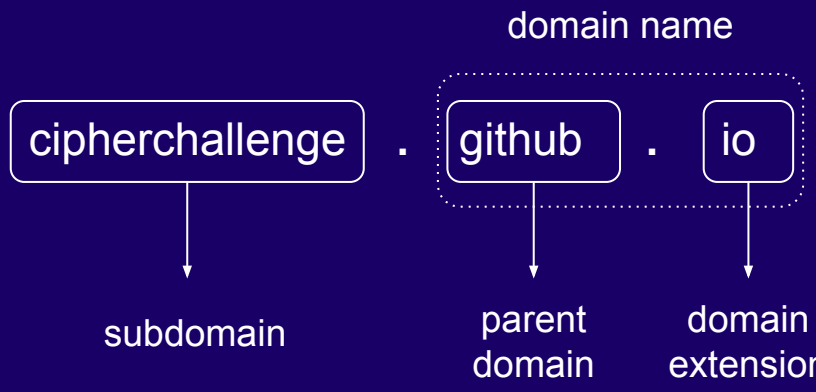
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bits, TLS 1.2



Linea

Websites

- Hosting (server)
- Domain name resolution (DNS)



IP addresses for **cipherchallenge.github.io**

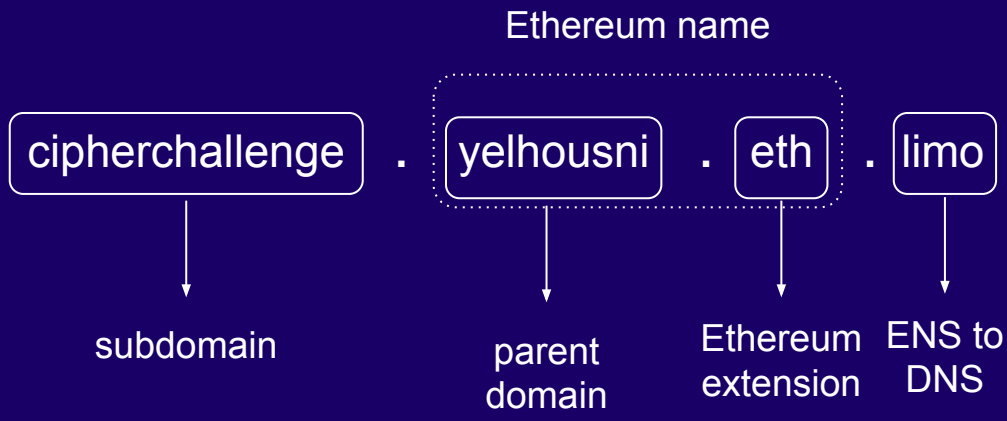
Our DNS servers responded with these IP addresses when we queried it for the domain cipherchallenge.github.io. Some DNS servers may return different IP addresses based on your location.

IP address	Type	Hosted by	Location
185.199.108.153	IPv4	Fastly, Inc.	United States of America

Linea

Decentralized Websites

- Decentralized Hosting (p2p IPFS)
- Ethereum name resolution (ENS)



bafybeiclwibybzcxnmbudh5xekmvwhgkhfiod7q4arfimhszru6vhcpjhi.ipfs.dweb.link

Linea

Modern cryptography

$$f(x) = a_0 + a_1 x + \cdots + x_n x^n, a_i \in \mathbb{Z}/p\mathbb{Z}$$

Secret sharing:

Secret key s:
s = s1, s2, s3, …, sn

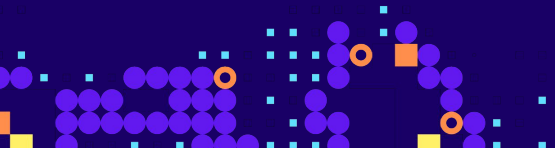
$$s = a_0$$

$$s_i = f(i)$$

E.g. DNSSEC
root key s
s = s1, …, s7
5/7 keys to restart the internet

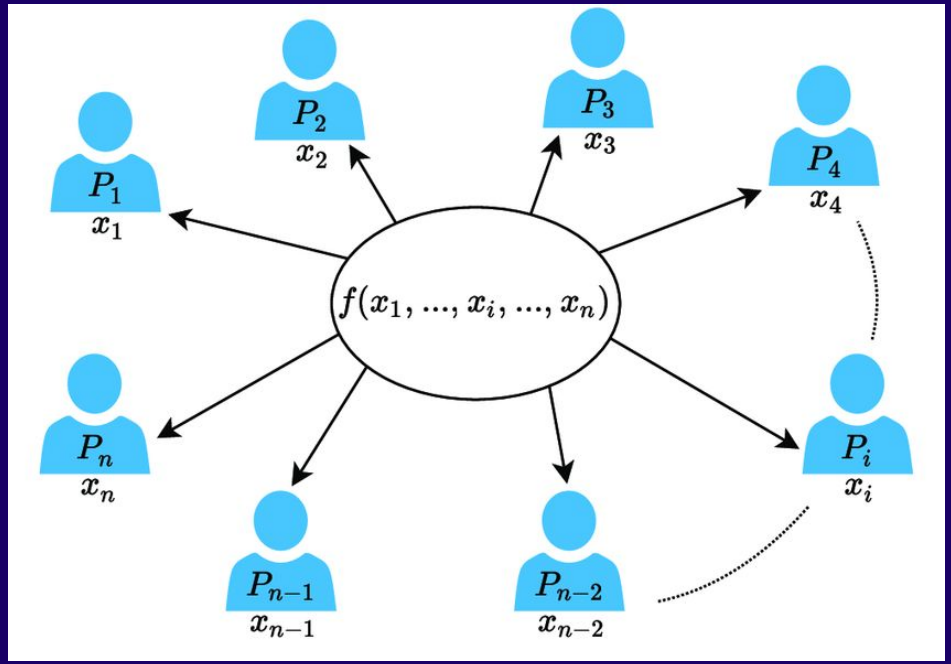
$$f(1), \ldots, f(n) \rightarrow_{\text{find}} f(x)$$

$$s = f(0)$$



Linea

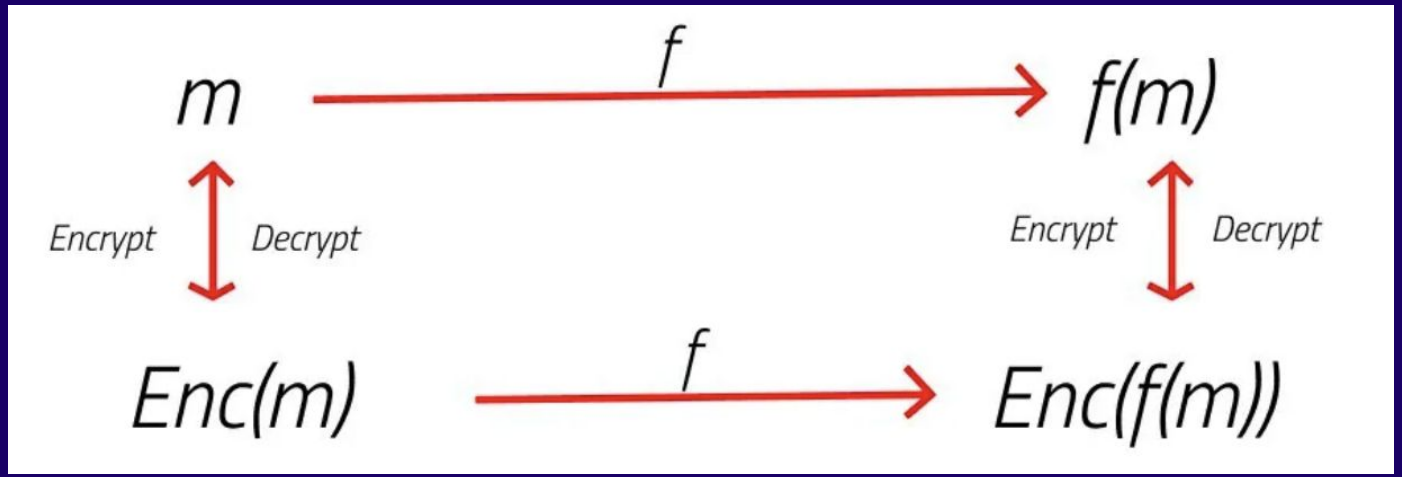
Multi-party computation



N people sign (collaboratively) a transaction

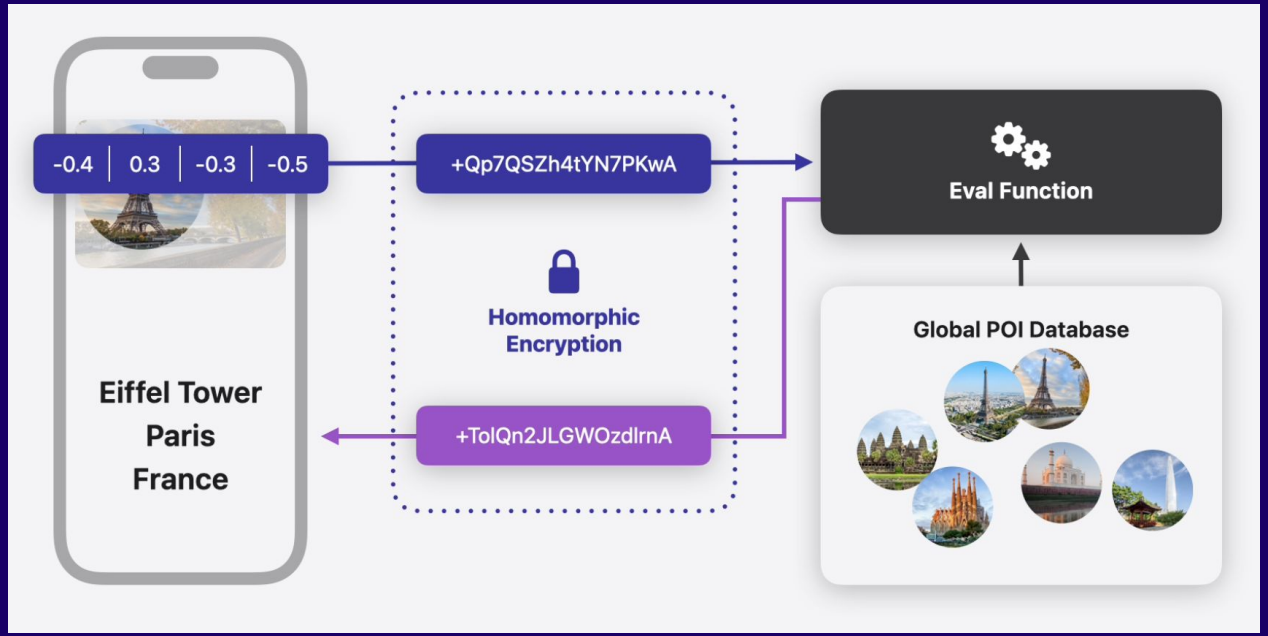
Linea

Fully Homomorphic Encryption



Linea

Apple's Private Nearest Neighbor Search

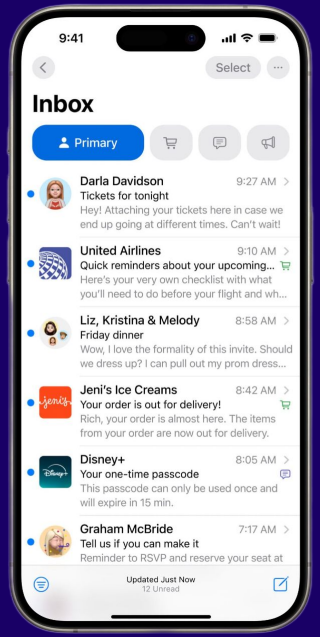


https://machinelearning.apple.com/research/homomorphic-encryption

Linea

Apple's Private Information Retrieval

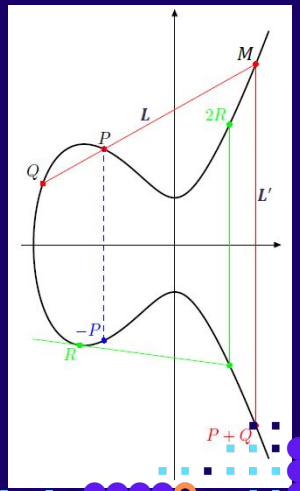
$$A_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

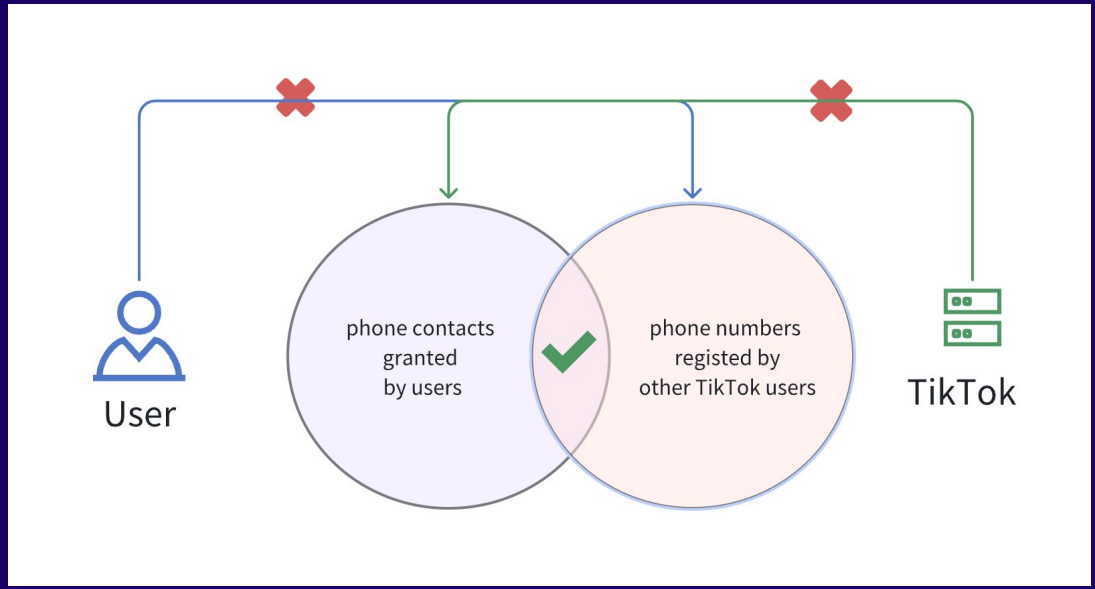


https://machinelearning.apple.com/research/homomorphic-encryption

Linea

Tiktok's Private Set Intersection

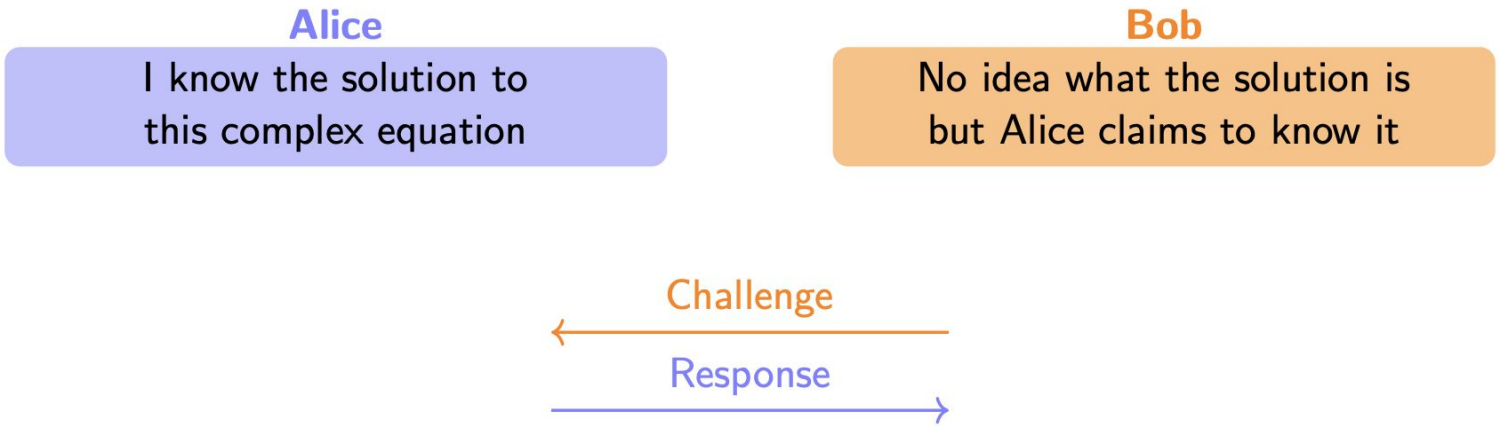




https://developers.tiktok.com/blog/tiktok-practices-in-privacy-enhancing-technologies

Linea

Zero-knowledge proofs



- **Sound**: Alice has a wrong solution $\Longrightarrow$ Bob is not convinced.
- **Complete**: Alice has the solution $\Longrightarrow$ Bob is convinced.
- **Zero-knowledge**: Bob does NOT learn the solution.

Linea

$$f(x) = a_0 + a_1 x + \cdots + x_n x^n, a_i \in \mathbb{Z}/p\mathbb{Z}$$

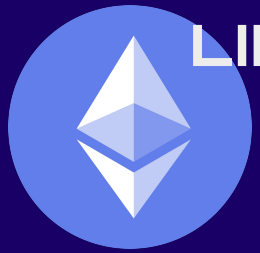
Zero-knowledge proofs

$$A_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

I have a zk proof that
X sent $Z to Y

$$\mathbb{P}(X) \quad \mathbb{P}(X) \quad \mathbb{P}\left(\frac{X}{2}\right)$$

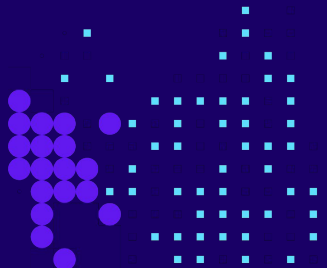
$$\mathbb{P}(X \mid Y) \quad \mathbb{P}(X \mid Y) \quad \mathbb{P}\left(\frac{X}{2} \,\middle|\, Y\right)$$

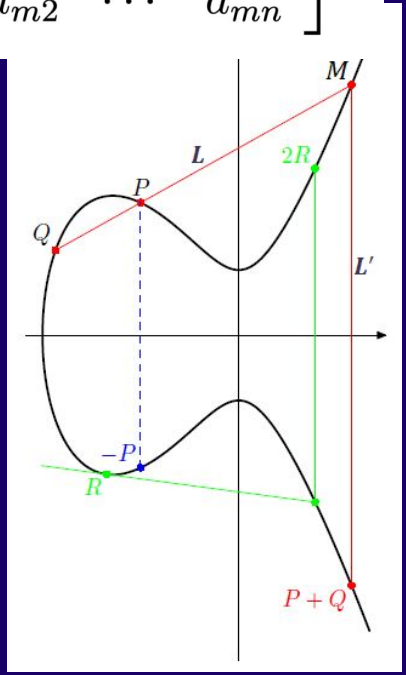


Linea

I have a short proof that
the transaction X is correct

|transaction| >> |proof|





https://z.cash
https://www.getmonero.org
https://ethereum.org
https://linea.build

Linea

Zero-knowledge proofs

- Free Cryptography library: https://github.com/Consensys/gnark-crypto
- Free ZKP library: https://github.com/Consensys/gnark
- Playground: https://play.gnark.io/
  - Factorisation example: http://play.gnark.io/?id=petqlbhyng

EdMSM: Multi-Scalar-Multiplication for SNARKs and Faster Montgomery multiplication

Gautam Botrel and Youssef El Housni

Linea, ConsenSys
gautam.botrel@consensys.net

Families of prime-order endomorphism-equipped embedded curves on pairing-friendly curves

Antonio Sanso[1] and Youssef El Housni[2]

[1] Ethereum Foundation
[2] Linea

Pairings in Rank-1 Constraint Systems

Youssef El Housni[1,2,3][0000−0003−2873−3479]

[1] ConsenSys R&D, gnark team, Paris, France
[2] LIX, CNRS, École Polytechnique, Institut Polytechnique d
[3] Inria

Optimized and secure pairing-friendly elliptic curves suitable for one layer proof composition

Youssef El Housni[1,2,3][0000−0003−2873−3479] and Aurore Guillevic[4][0000−0002−0824−7273]

[1] EY Blockchain, Paris, France
[2] LIX, CNRS, École Polytechnique, Institut Polytechnique de Paris
[3] INRIA
youssef.el.housni@fr.ey.com
[4] Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
aurore.guillevic@inria.fr

A survey of elliptic curves for proof systems*

Diego F. Aranha[1][0000−0002−2457−0783], Youssef El Housni[2,3,4][0000−0003−2873−3479], and Aurore Guillevic[1,5][0000−0002−0824−7273]

[1] Aarhus University, Aarhus, Denmark
dfaranha@cs.au.dk
[2] ConsenSys, gnark, Paris, France
[3] LIX, CNRS, École Polytechnique, Institut Polytechnique de Paris
[4] Inria
youssef.elhousni@consensys.net
[5] Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
aurore.guillevic@inria.fr

Co-factor clearing and subgroup membership testing on pairing-friendly curves*

Youssef El Housni[1,2,3][0000−0003−2873−3479], Aurore Guillevic[4,5][0000−0002−0824−7273], and Thomas Piellard[1]

[1] ConsenSys, gnark
youssef.elhousni@consensys.net

Families of SNARK-friendly 2-chains of elliptic curves*

Youssef El Housni[1,2,3][0000−0003−2873−3479] and Aurore Guillevic[4,5][0000−0002−0824−7273]

[1] ConsenSys, gnark, Paris, France
[2] LIX, CNRS, École Polytechnique, Institut Polytechnique de Paris
[3] Inria
youssef.elhousni@consensys.net
[4] Université de Lorraine, CNRS, Inria, LORIA, Nancy, France
[5] Aarhus University, Aarhus, Denmark
aurore.guillevic@inria.fr

Linea

Cryptanalysis
a.k.a. Attacks

- Underlying math
- Implementation
- Side-channel
- Social/frontend
- Political
- Future

An efficient key recovery attack on SIDH

Wouter Castryck[1,2] and Thomas Decru[1]

[1] imec-COSIC, KU Leuven, Belgium
[2] Vakgroep Wiskunde: Algebra en Meetkunde, Universiteit Gent, Belgium

27th Chaos Communication Congress

Console Hacking 2010

PS3 Epic Fail

fail0verflow

bushing, marcan, segher, sven

North Korean hackers cash out hundreds of millions from $1.5bn ByBit hack

10 March 2025

Share Save

Apple pulls data protection tool after UK government security row

22 February 2025

Share Save

TPM-Fail

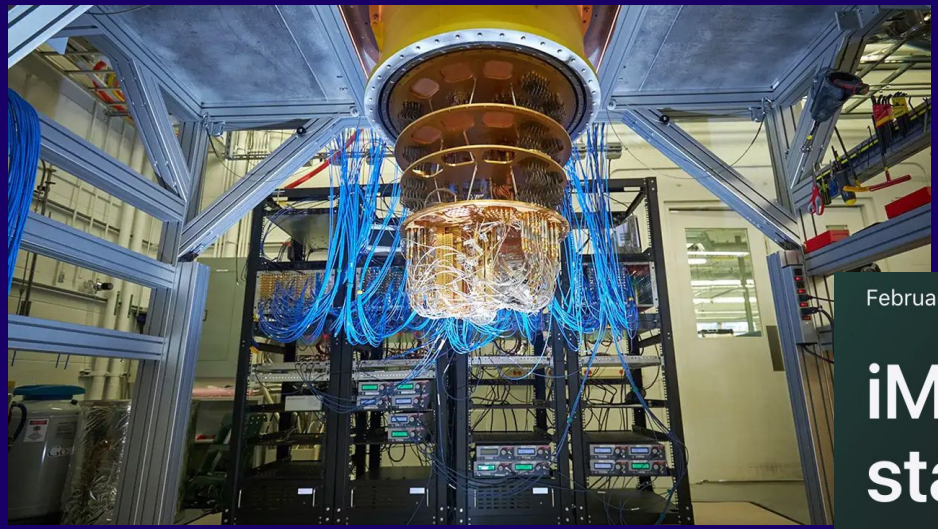
TPM meets Timing and Lattice Attacks

DOWNLOAD PAPER

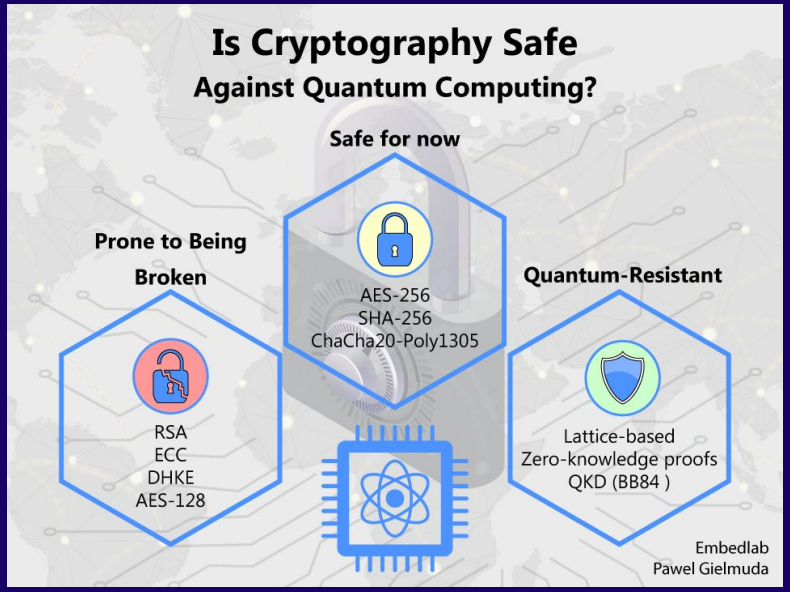
CITE PAPER

LINEA

Future attacks



Quantum computer



February 21, 2024

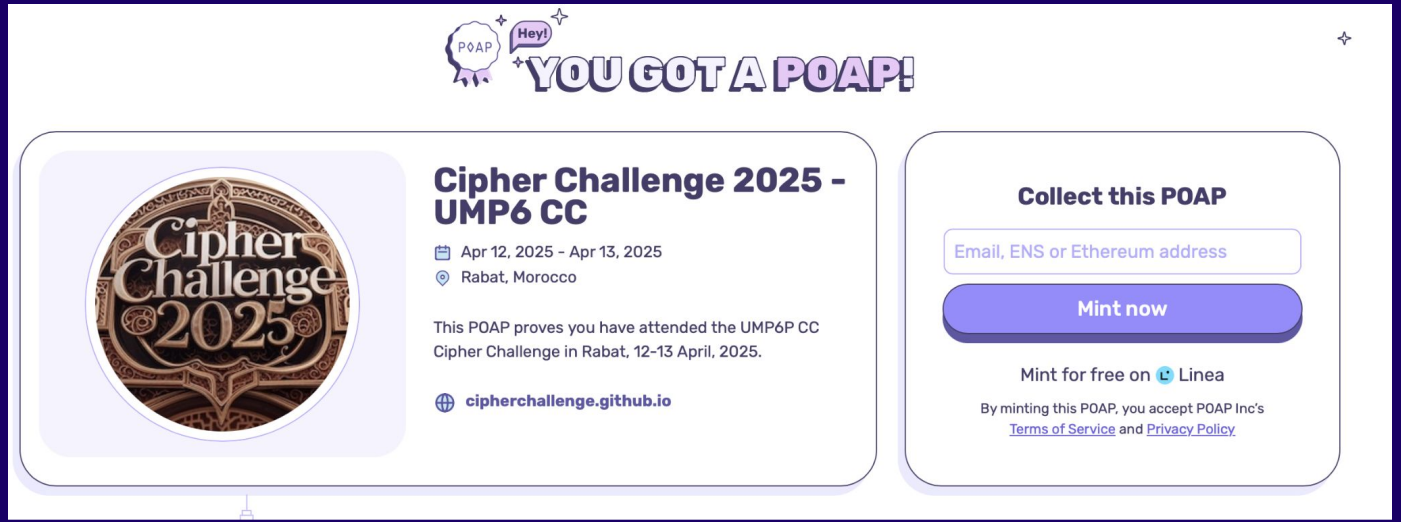
iMessage with PQ3: The new state of the art in quantum-secure messaging at scale

Posted by Apple Security Engineering and Architecture (SEAR)

https://security.apple.com/blog/imessage-pq3/

Linea

Proof of Attendance Protocol (POAP)



Linea

Thank you

yelhousni.eth.limo
linea.build
gnark.io

youssef.elhousni@consensys.net

Telegram: @ElMarroqui
GitHub: @yelhousni
X: @YoussefElHousn3