RUB

Into the asymmetry

Journey through the mathematics of public key cryptography

Antonio Sanso

December 5, 2022

Overview

The Genesis

1976 - Diffie and Hellman release *"New directions in cryptography"*

The Resistance

1985 - Koblitz and Victor Miller proposed independently elliptic curve cryptographic schemes

The Cambrian

2008 - Satoshi Nakamoto publishes seminal Bitcoin white paper

Main characters

Alice

Bob

Eve

The Genesis

In the beginning was the Word

The Resistance

Resistance Is Futile

Discrete Logarithm Problem (DLP)

Let G be a finite cyclic group with generator g, given $g \in G, h = g^a$, find a

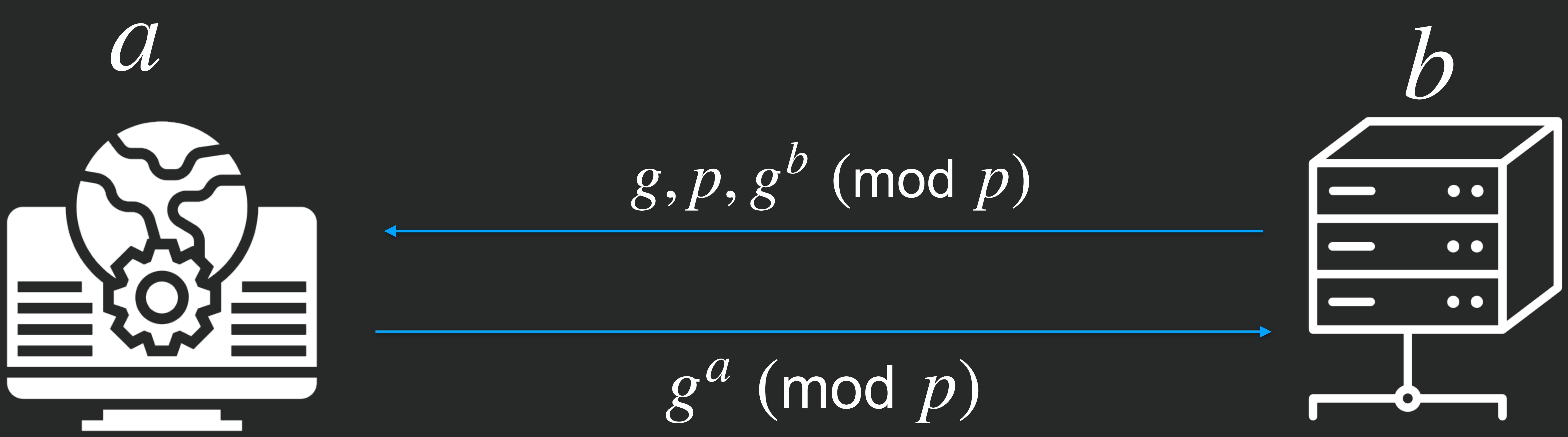
Diffie Hellman Key Exchange over F_p^*

- Group elements: non negative integers smaller than p
- Operation: *multiplication* (mod p)
- Order: $p - 1$
- DLP is believed to be hard in this group

Diffie Hellman Key Exchange

TLS_DHE_RSA_WITH_AES_128....

simplified



$$g^{ab} \pmod{p}$$

Pre master key (PMK)

Diffie Hellman Key Exchange

TLS_DHE_RSA_WITH_AES_128....

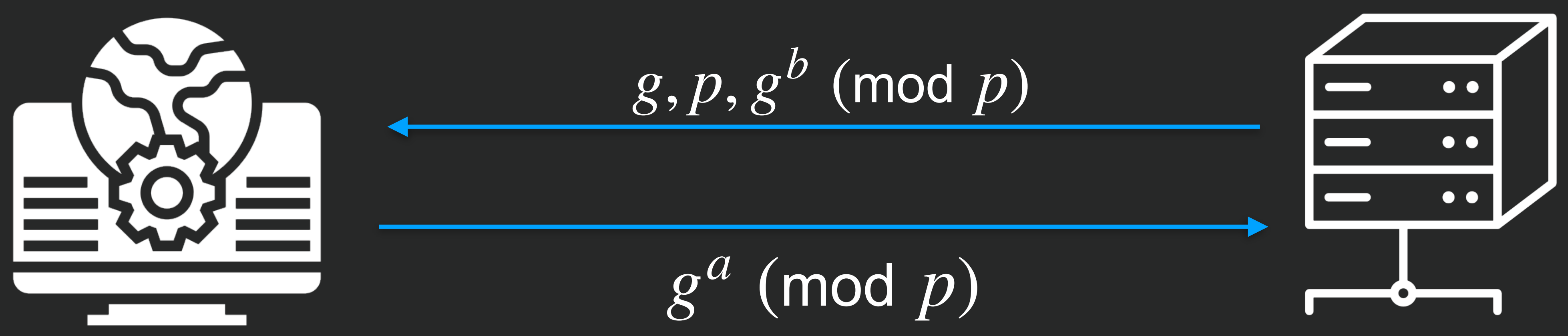
simplified

$g^{ab} \pmod{p}$

Diffie Hellman Key Exchange

TLS_DHE_RSA_WITH_AES_128....

simplified



Which p to use ?

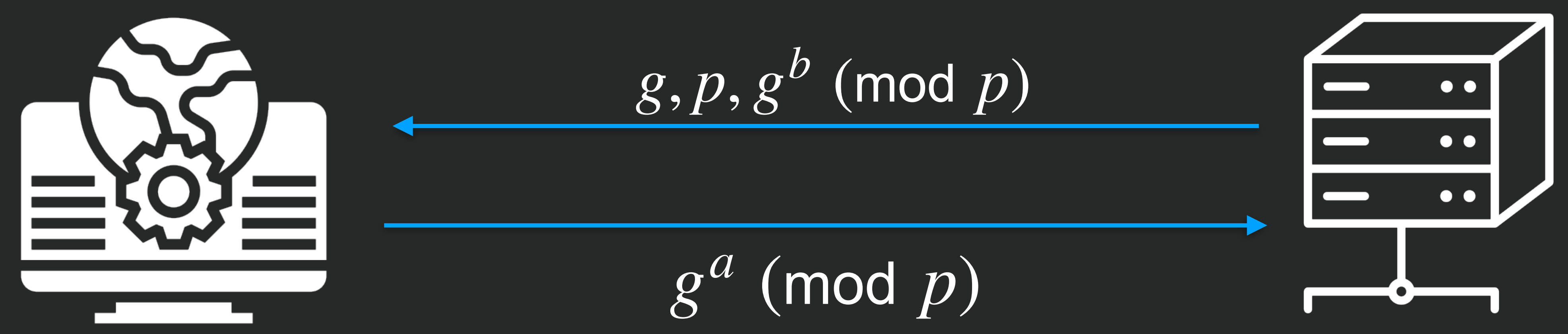
Consensus is to use safe primes (RFC 7919):

p such that $q = \dfrac{p-1}{2}$ is also prime

Diffie Hellman Key Exchange

TLS_DHE_RSA_WITH_AES_128....

simplified

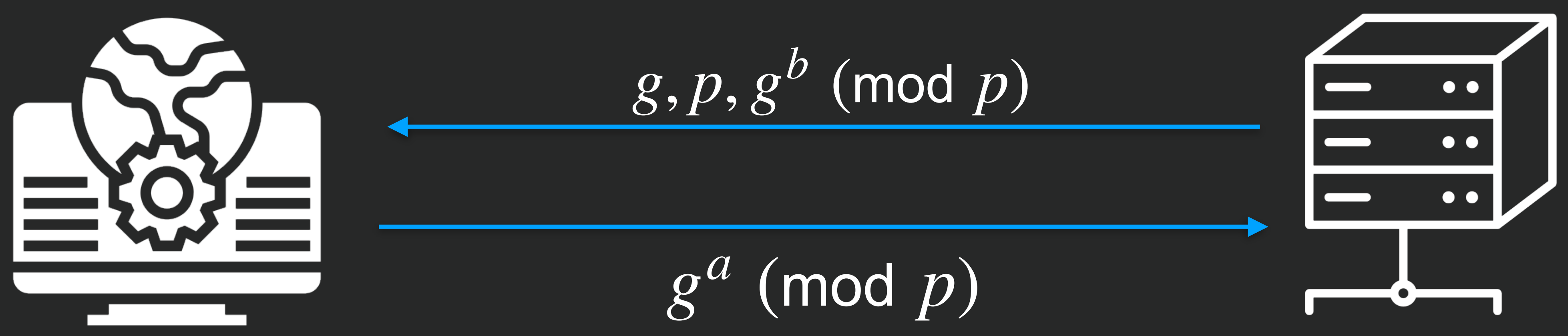


Group		
Source	**Prime Size**	**Subgroup Size**
RFC 5114 Group 22	1024	160
Amazon Load Balancer	1024	160
JDK	768	160
JDK	1024	160
RFC 5114 Group 24	2048	256
JDK	2048	224
Epson Device	1024	< 948
RFC 5114 Group 23	2048	224
Mistyped OpenSSL 512	512	497

Diffie Hellman Key Exchange - RFC5114

“Measuring small subgroup attacks against Diffie-Hellman”

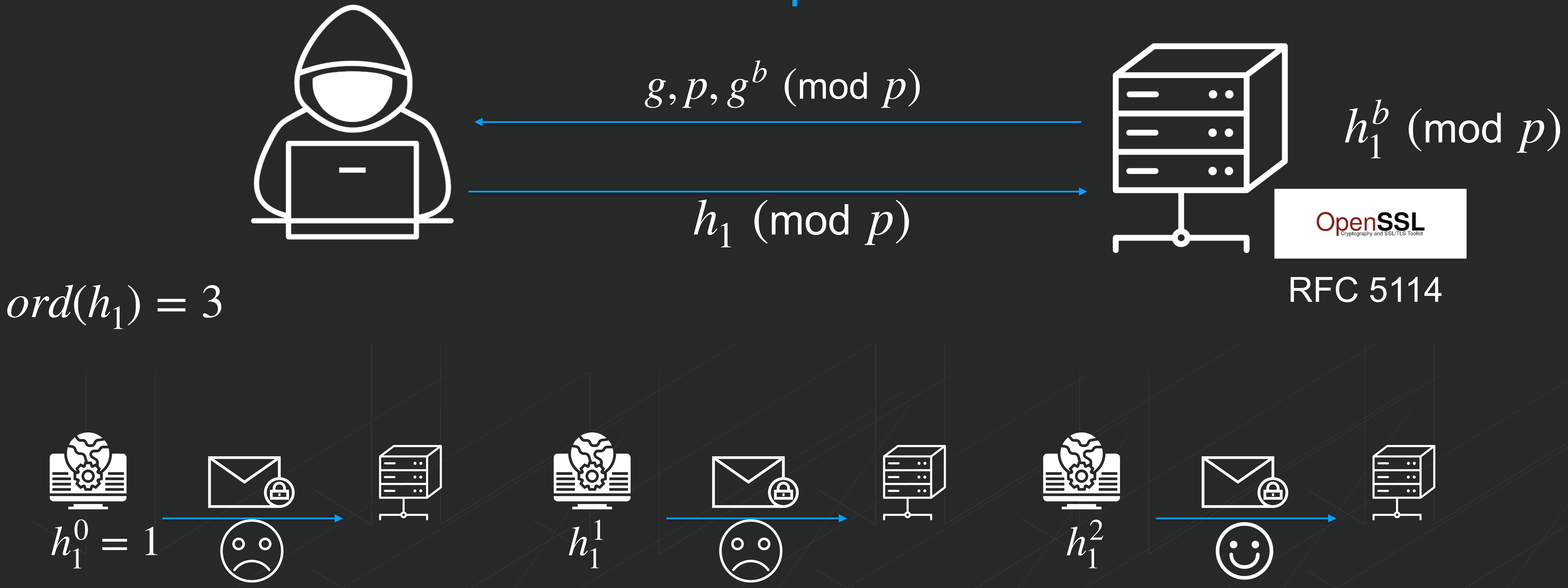
[NDSS 2017 VASCFHHH]



Source	Completely?	Order Factorization
RFC 5114 Group 22	Yes	2^3 * 7 * df * 183a872bdc5f7a7e88170937189 * 228c5a311384c02e1f287 c6b7b2d * 5a857d66c65a60728c353e32ece8be1 * 518aa8781a8df278aba4e7 d64b7cb9fd49462353 * 1a3adf8 d6a69682661ca6e590b447e66ebd1bbdeab5e 6f3744f06f46cf2a8300622ed50011479f18143d471a53d30113995663a447dcb8 e81bc24d988edc41f21
RFC 5114 Group 23	No	3^2 * 5 * 2b * 49 * 9d * 5e9a5 * 93ee1 * 2c3f0539 * 136c58359 * 1a 30b7358d * 335a378eb0d * 801c0d34c58d93fe997177101f80535a4738cebcb f389a99b36371eb * 22bbe4b573f6fc6dc24fef3f56e1c216523b3210d27b6c07 8b32b842aa48d35f230324e48f6dc2a10dd23d28d382843a78f264495542be4a95 cb05e41f80b013f8b0e3ea26b84cd497b43cc932638530a068ecc44af8ea3cc841 39f0667100d426b60b9ab82b8de865b0cbd633f41366622011006632e0832e827f ebb7066efe4ab4f1b2e99d96adfaf1721447b167cb49c372efcb82923b3731433c ecb7ec3ebbc8d67ef441b5d11fb3328851084f74de823b5402f6b038172348a147 b1ceac47722e31a72fe68b44ef4b
RFC 5114 Group 24	Yes	7 * d * 9f5 * 22acf * bd9f34b1 * 8cf83642a709a097b447997640129da29 9b1a47d1eb3750ba308b0fe64f5fbd3 * 15adfe949ebb242e5cd0978fac1b43fd bd2e5b0c5f48924fbbd370195c0eb20596d98ad0a9e3fd98876413d926f41a8b91 8d2ec4b018a30efe5e336bf3c7ce60d515cf46af5facf3bb389f68ad0c4ed2f0b1 dbb970293741eb6509c64e731802259a639a7f57d4a9c0d9445241f5bcdbdc5055 5b76d9c335c1fa4e11a8351f1bf4730dd67ffed877cc13e8ea40c7d51441c1f4e5 9155ef1159eca75a2359f5e0284cd7f3b982c32e5c51dbf51b45f4603ef46bae52 8739315ca679703c1ffcf3b44fe3da5999daadf5606eb828fc57e46561be8c6a86 6361

Diffie Hellman Key Exchange

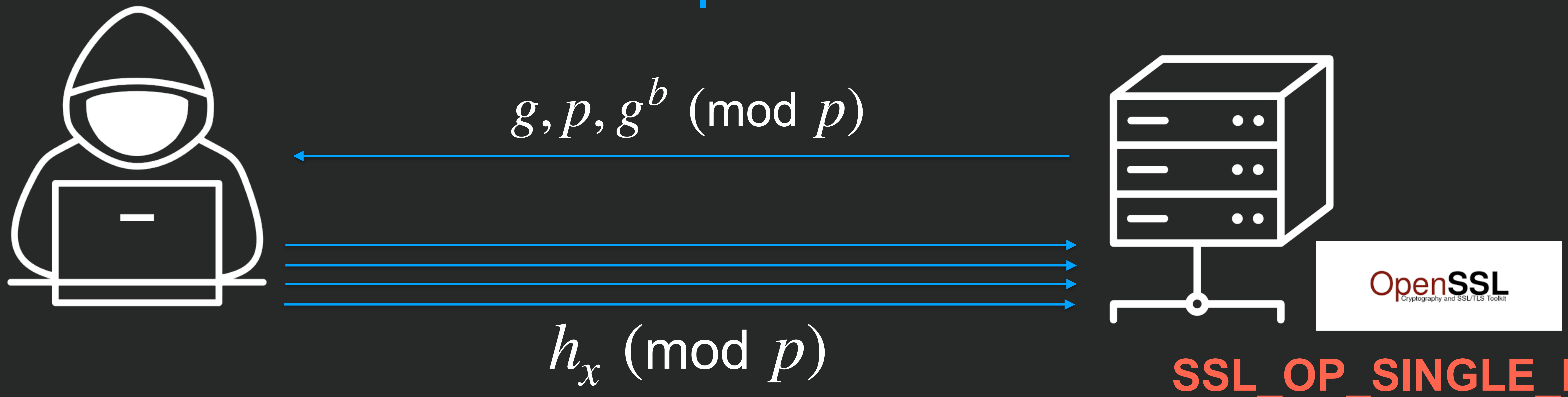
Small subgroup attack - TLS_DHE_RSA_WITH_AES_128.... simplified



Attacker recovered the value of $b \pmod{3}$

Diffie Hellman Key Exchange

Small subgroup attack - TLS_DHE_RSA_WITH_AES_128.... simplified



SSL_OP_SINGLE_DH_USE
Not set by default

$$ord(h_1) = 3$$

$$ord(h_2) = 5$$

$$ord(h_3) = 43$$

$$\dots$$

$$ord(h_i) = 3528910760717$$

Finally we can combine the result using the Chinese Remainder Theorem **(CRT)!!**

Group	Exponent Size	Online Work	Offline Work
Group 22	160	8	72
Group 23	224	33	47
Group 24	256	32	94

Measurements

40.6 M

1% sample of HTTPS hosts on the Internet

1.6 M (4%)

Used a non-safe prime

309 K (0.8%)

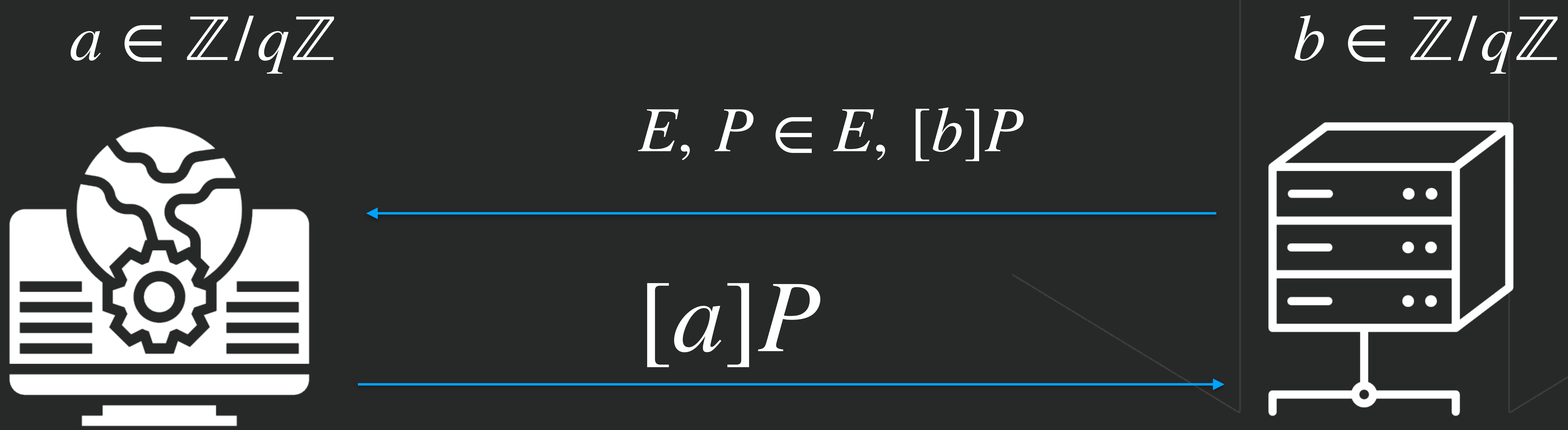
Candidates for a small subgroup key recovery attack

We also performed SSH, IKEv1 and IKEv2 baseline scans

Diffie Hellman Key Exchange over $E(F_q)$

- Group elements: points on elliptic curve E
- Operation: *point addition*
- Identity element: point at infinity (∞)
- Order: number of points (SEA)
- (EC)DLP is believed to be hard in this group

Diffie Hellman Key Exchange over $E(F_q)$



$$[ab]P$$

Measurements

"In search of CurveSwap: Measuring elliptic curve implementations in the wild" [Euro S&P 2018 VSSH]

41 M

Supported ECDHE (TLS)

19.2 K (1.5%)

Lack of point validation (port 8443)

0 (0%)

Candidates for a CurveSwap attack (via twist)

We also performed SSH, IKEv1 and IKEv2 baseline scans

Outline of contributions

- *“Measuring small subgroup attacks against Diffie-Hellman”* [NDSS 2017 VASCFHHH]
- *“In search of CurveSwap: Measuring elliptic curve implementations in the wild”* [Euro S&P 2018 VSSH]

Outline of contributions

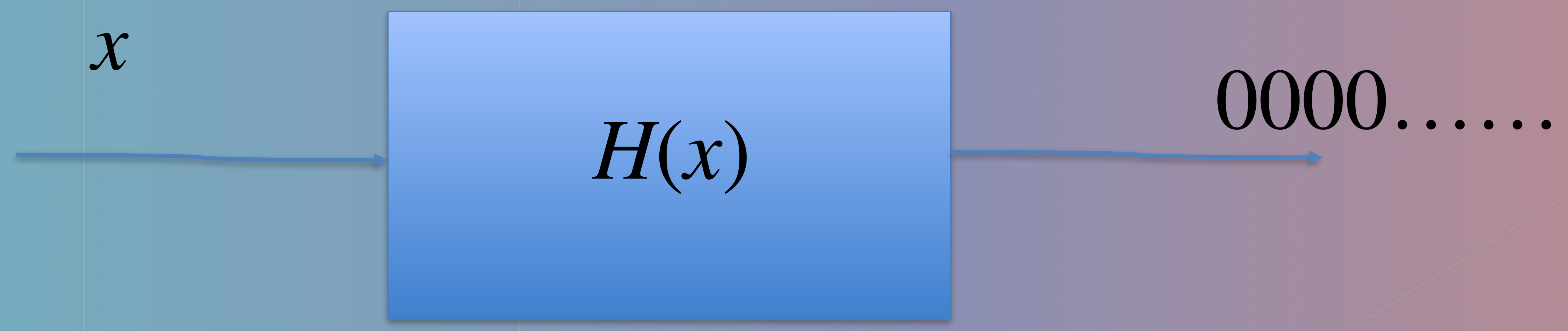
- *”OpenSSL Key Recovery Attack on DH small subgroups”* [CVE-2016-0701 finalist for the Pwnie Award for Best Cryptographic Attack at Black Hat 2017]
- *”Small Subgroups Key Recovery Attack on Firefox’s WebCrypto DH”* [Finalist for the Pwnie Award for Best Cryptographic Attack at Black Hat 2020]
- *”Critical vulnerability in JSON Web Encryption (JWE) - RFC 7516”* [Finalist for the Pwnie Award for Best Cryptographic Attack at Black Hat 2018]

The Cambrian

Needless to say this appearance of sudden life has delighted creationists

Blockchains

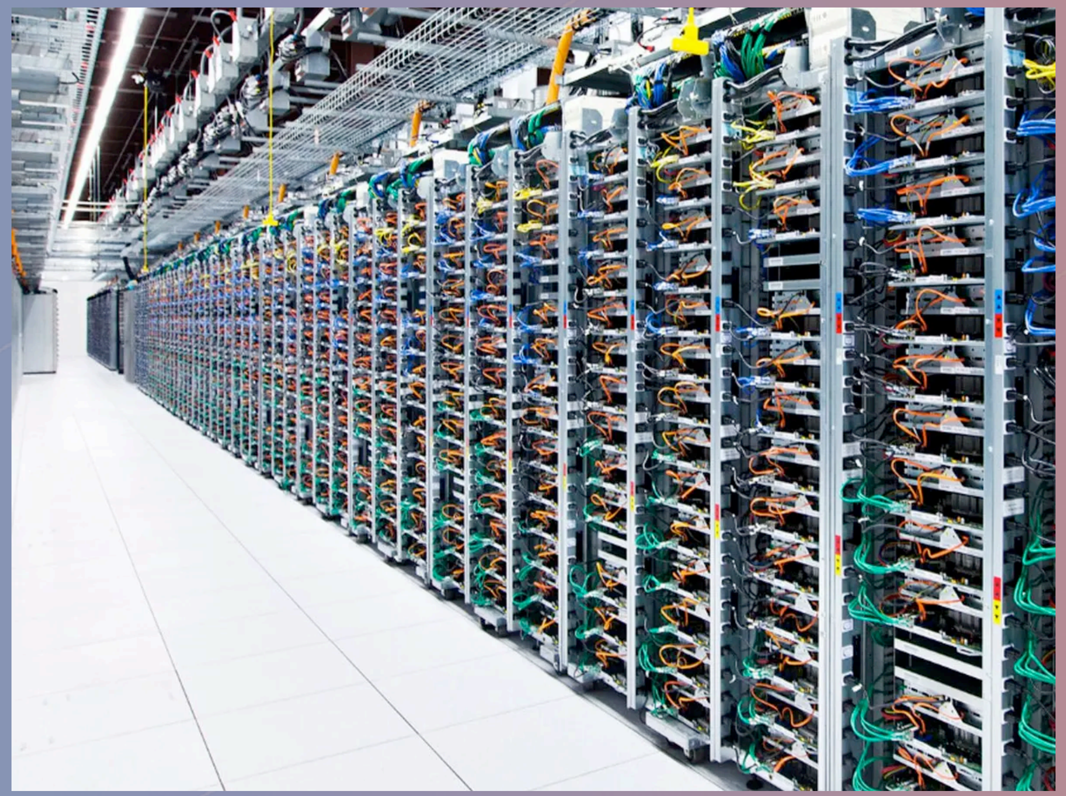
Proof of work vs. Proof of stake

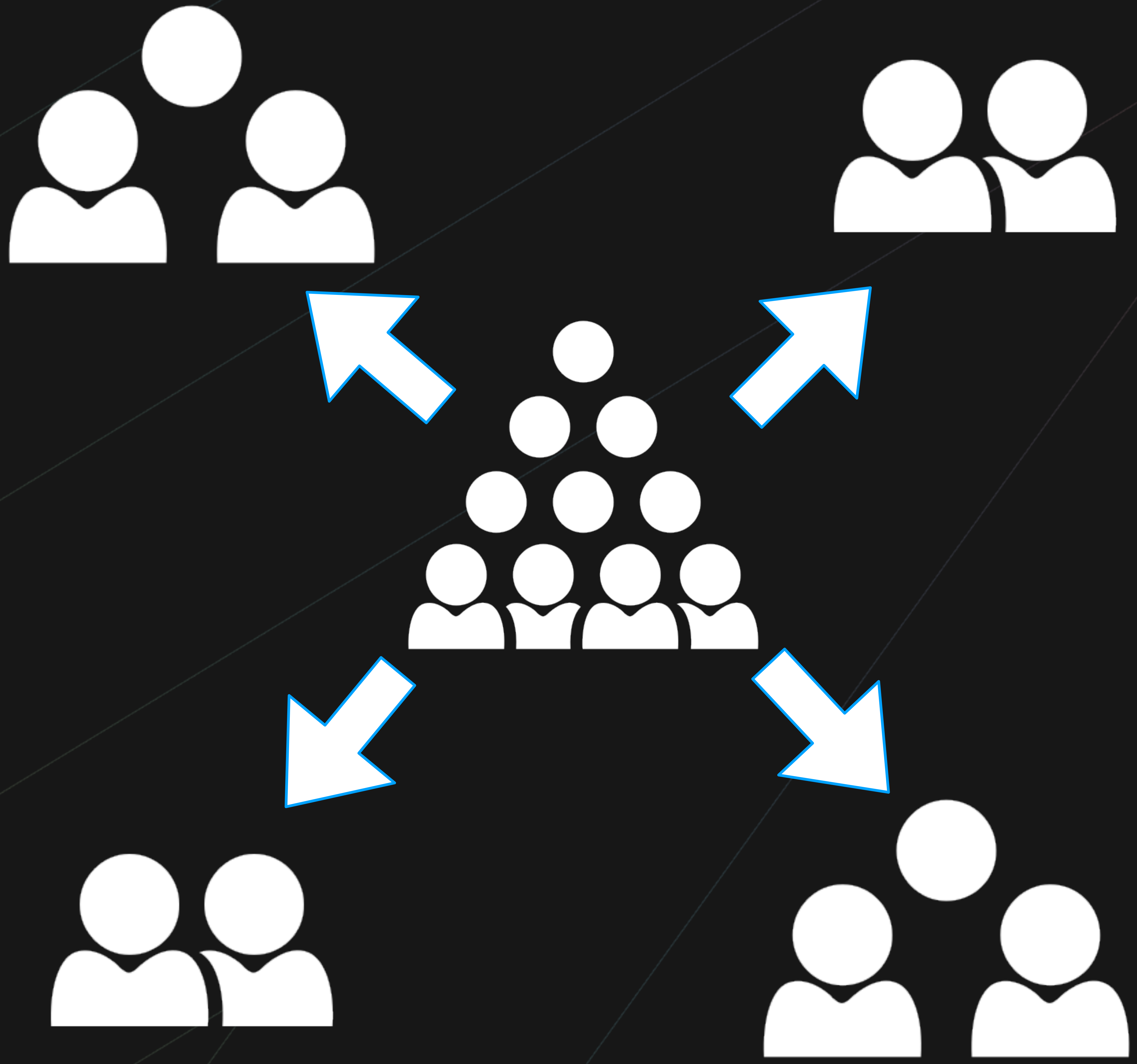


Find x such that

$$H(x) = 0000\ldots\ldots.$$

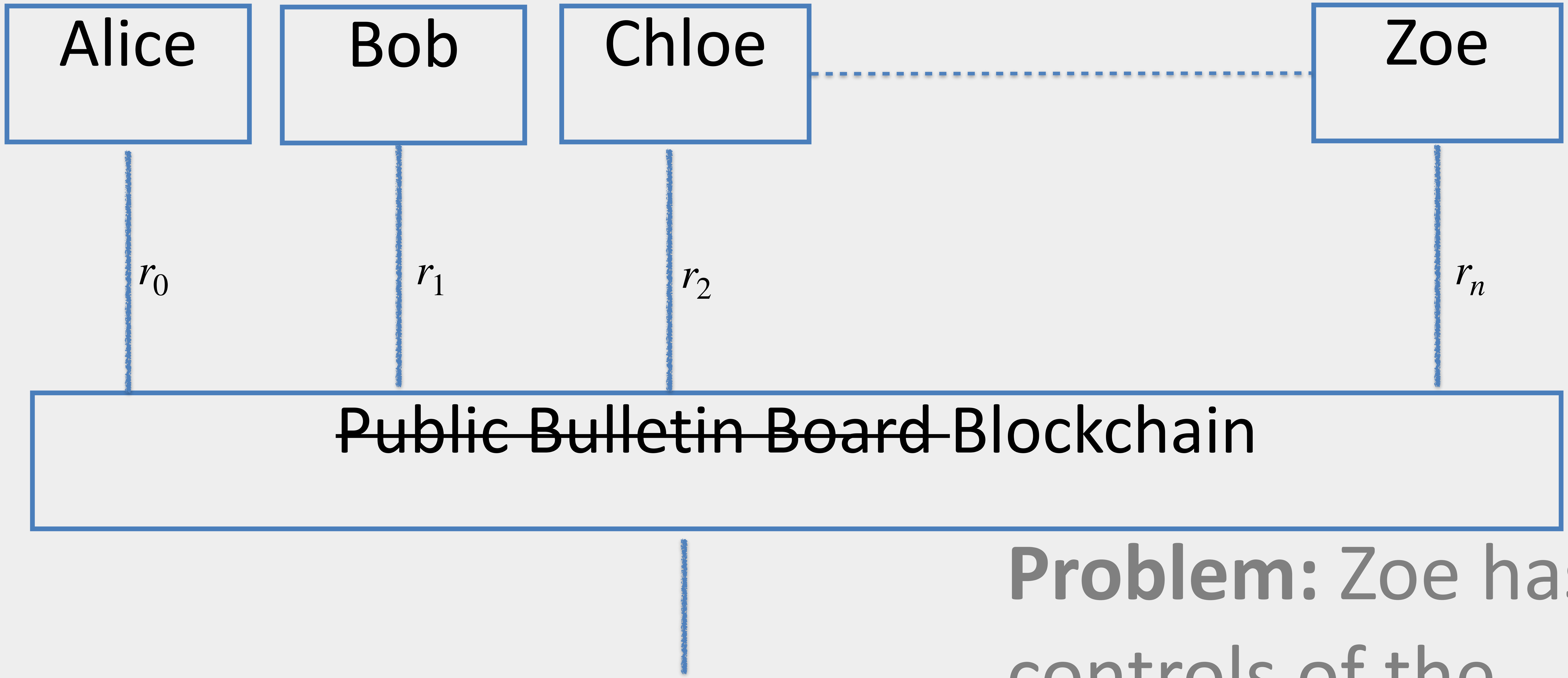
Parallelizible





Committees

Generate verifiable randomness



Rand = $r_0 \oplus r_1 \oplus r_2 \ldots \oplus r_n$

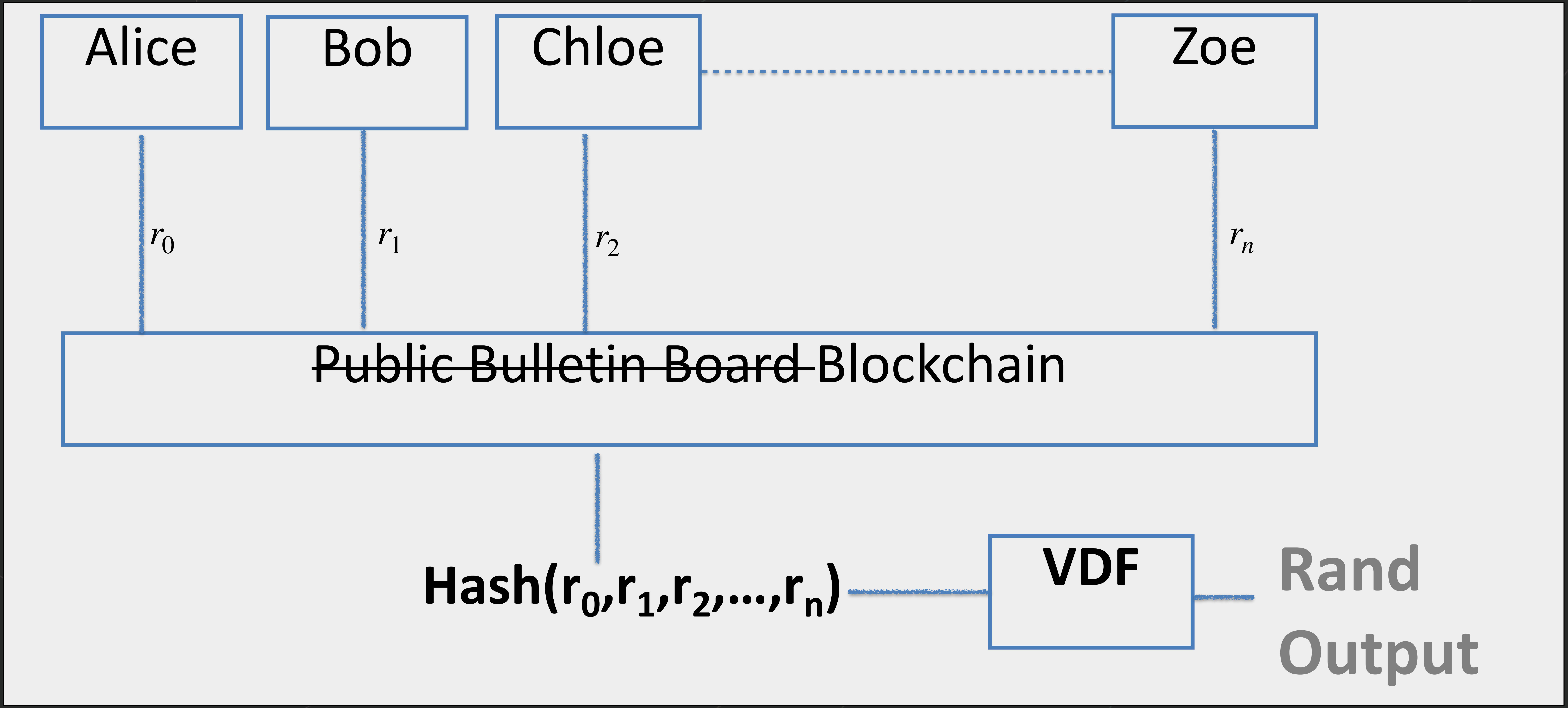
Problem: Zoe has controls of the output

What is a Verifiable Delay Function (VDF)?

1. Takes **T steps** to evaluate even with unbounded parallelism
2. The output can be verified efficiently

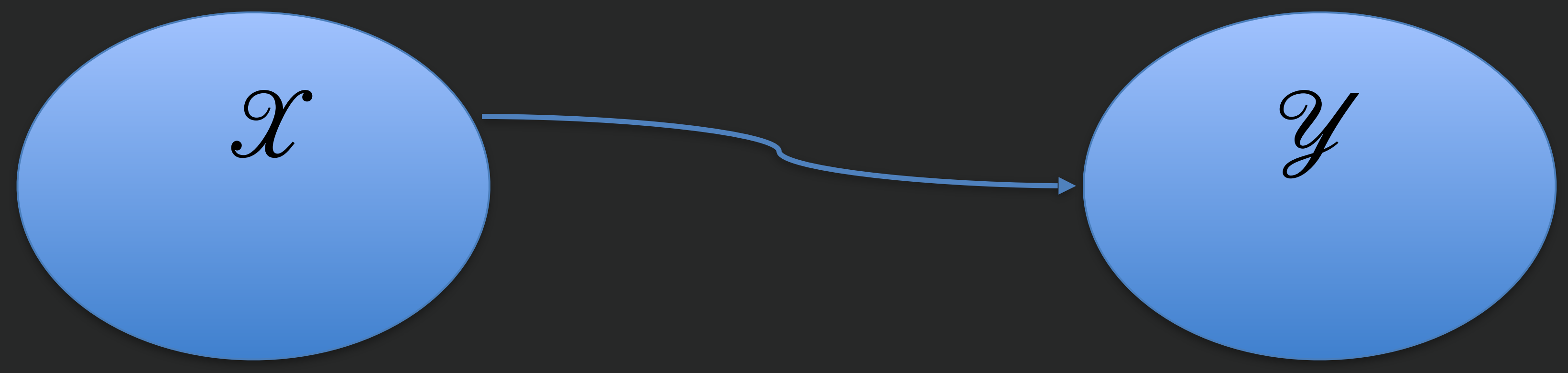
VDF Application

Generate **verifiable** randomness



What is a Verifiable Delay Function (VDF)?

- Function



- Delay

- Verifiable

Verifiable Delay Function (VDF)

- Setup$(\lambda, T) \rightarrow$ public parameters pp
- Eval$(pp, x) \rightarrow$ outputs y such that $y = f(x)$ and a proof π (requires T steps)
- Verify$(pp, x, y, \pi) \rightarrow$ true or false

VDF minus any property is “easy”

- Not Verifiable:

$$s \to H(s) \to H(H(s)) \to \cdots \to H^{(T)}(s) = a$$

- No Delay: Easy (many trapdoors example in cryptography)
- Not Function: Proof of sequential work

VDF History

https://vdfresearch.org/

2018 (12 June)

Seminal paper by Boneh, Bonneau, Bünz, Fisch (BBBF), no actual VDF construction

2018 (20 June)

Wesolowski's VDF

2018 (22 June)

Pietrzak's VDF

Wesolowski and Pietrzak VDFs

Time Lock Puzzle

(RSW - Repeated squaring)

+

Fast Verification

(without revealing the order of the group)

“Verifiable Delay Functions from Supersingular Isogenies and Pairings” [Asiacrypt 2019 DMPS]

https://github.com/isogenies-vdf

Slow Evaluation

T isogenies sequentially

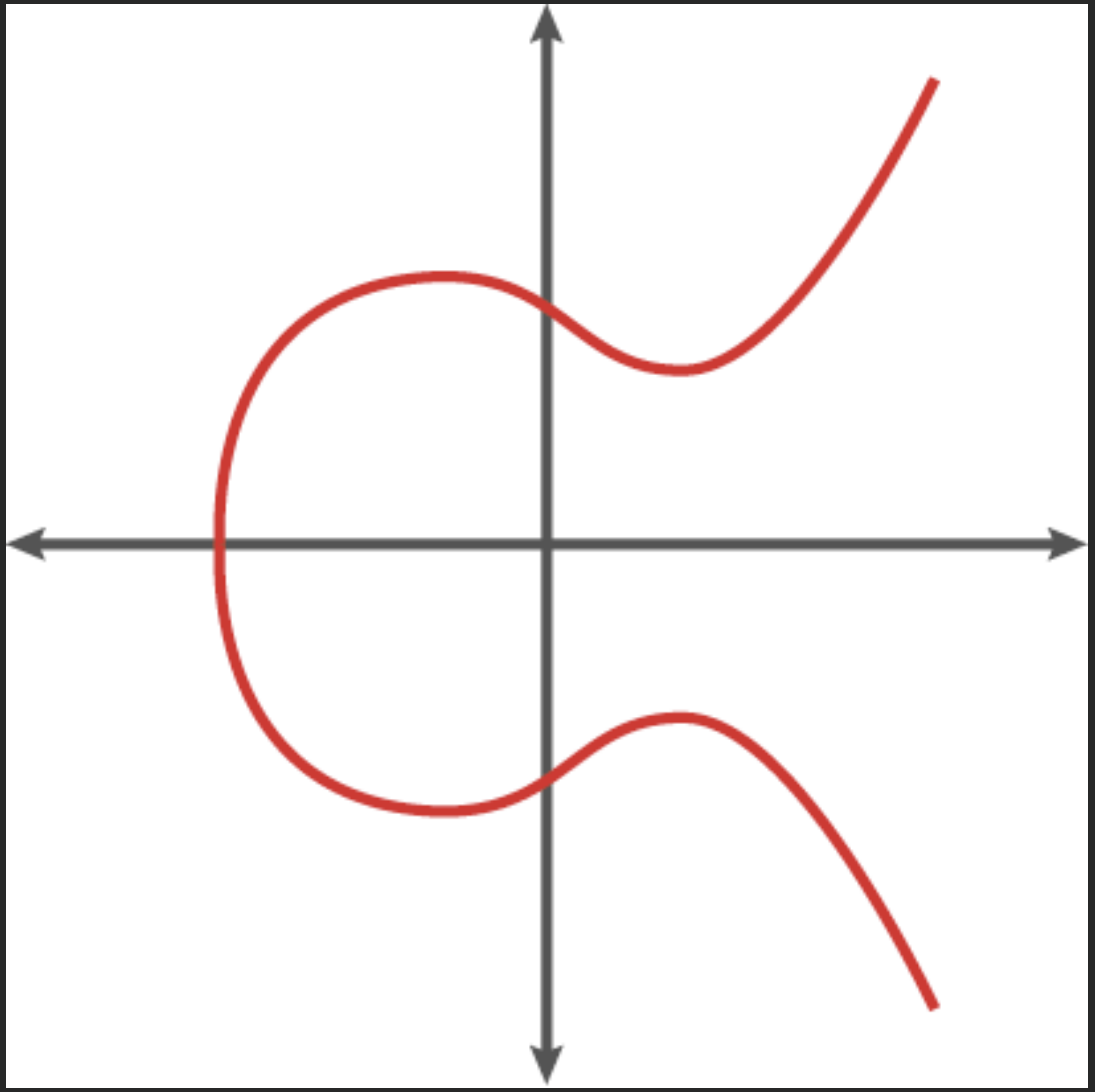
+

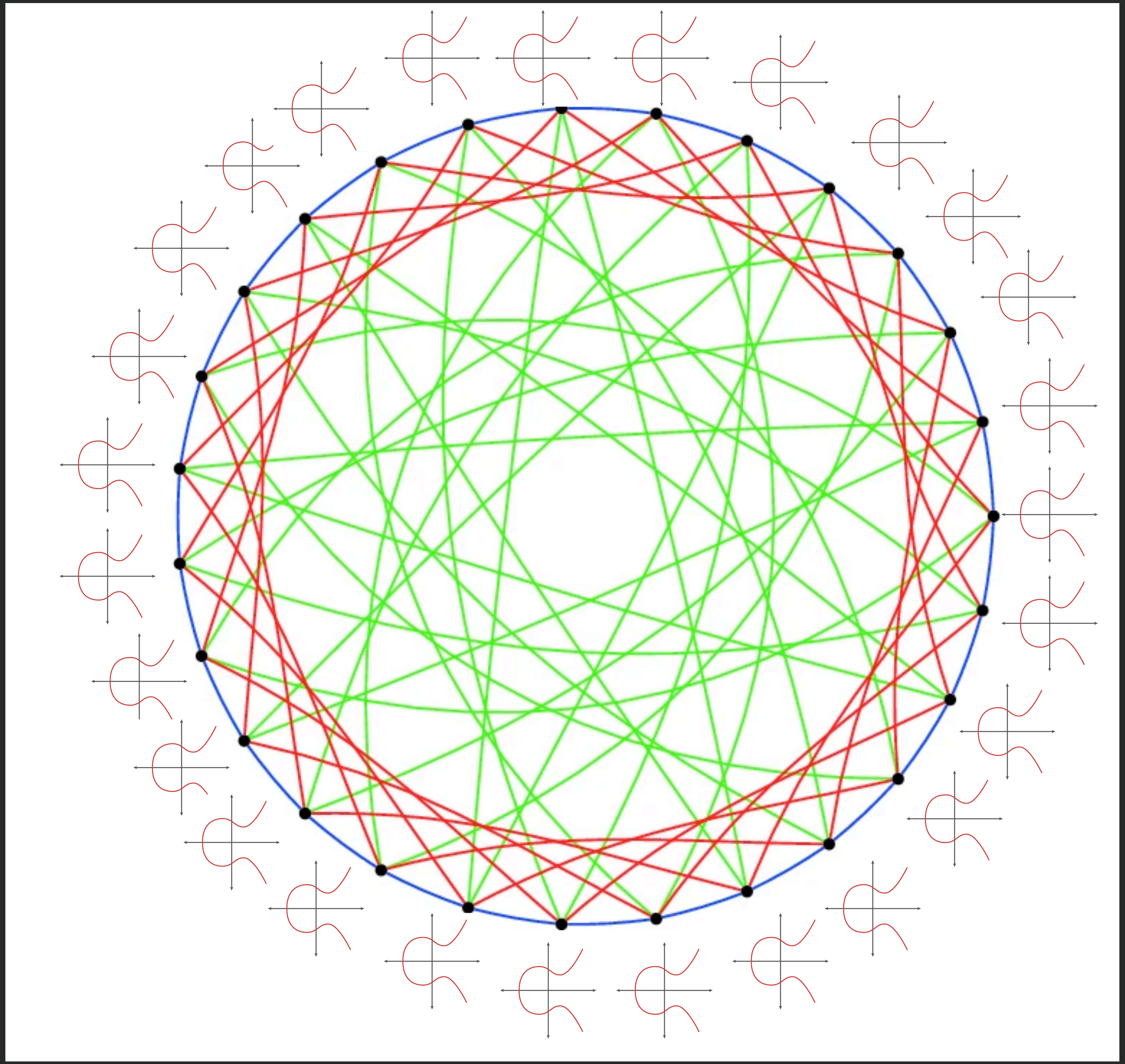
Fast Verification

Compute pairings on the domain and the codomain curve

Isogenies graphs

Credit: Lorenz Panny





Hard Homogenous Spaces (HHS)

[Couveignes]

A set $\mathscr{E}$ equipped with a group action by a group G

$$G \times \mathscr{E} \to \mathscr{E}$$

$$[\mathfrak{g}]E = E'$$

Vectorization Problem

Given $E, E' \in \mathscr{E}$, $\mathfrak{g} \in G$ such that

$$[\mathfrak{g}]E = E'$$

It resembles the DLOG problem

HHS - Isogeny instantiation

[CSIDH]

Set $\mathscr{E}$

Supersingular elliptic curves

Isogeny

Non constant rational map (ratio of polynomials) between two elliptic curves $\phi : E \to E'$. Degree of the isogeny is equal to the degree of the ratio of polynomials

Group G

Ideal class group acting on $\mathscr{E}$ via isogenies

Action of $\mathfrak{g}$ on E

Compute codomain of degree l isogeny $\phi : E \to E'$

Isogenies VDF

Setup

Starting curve E_0

Isogeny $\phi : E \to E_T$ of degree 2^T

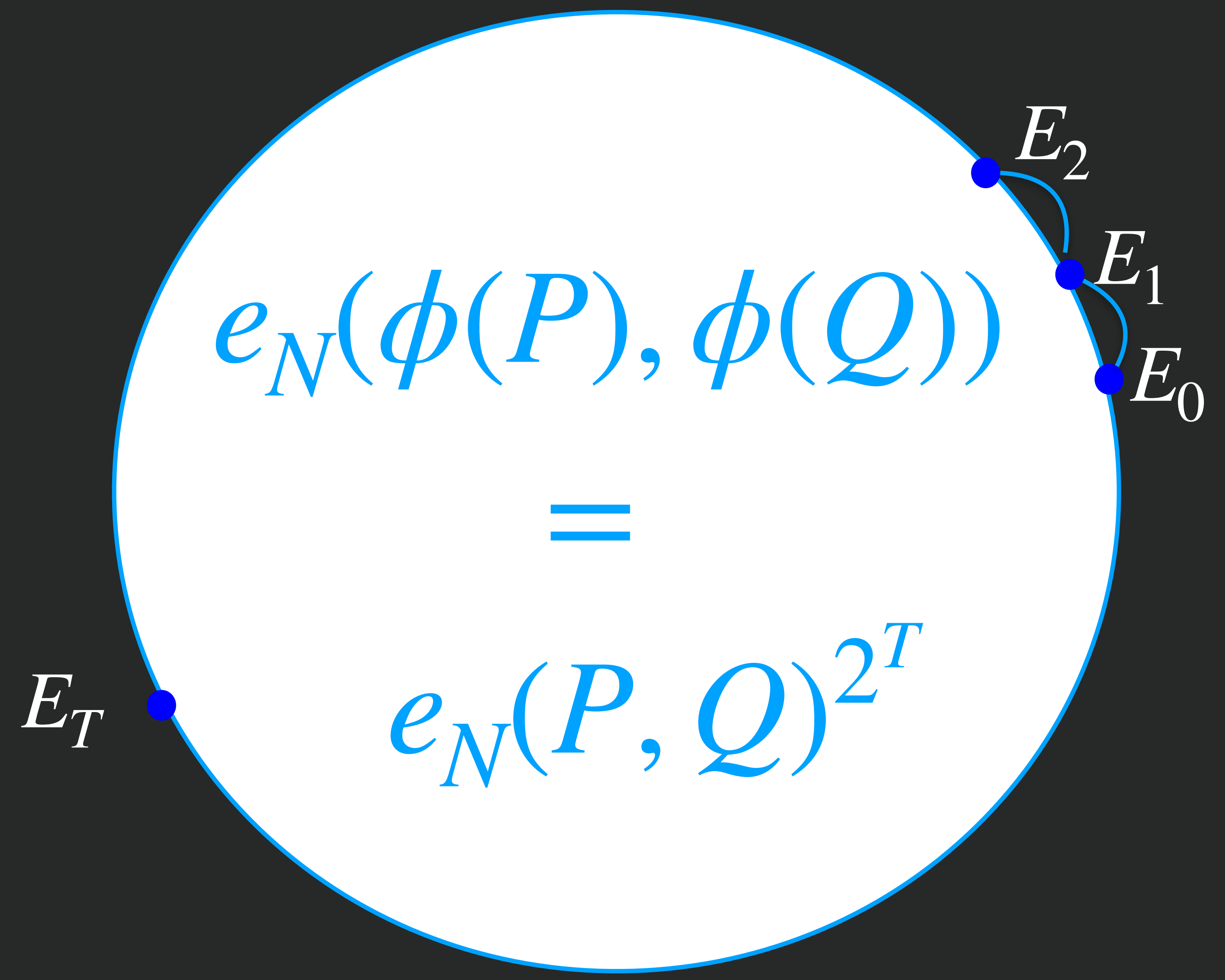
Eval

$\phi : E_0(\mathbb{F}_p) \to E_T(\mathbb{F}_p)$

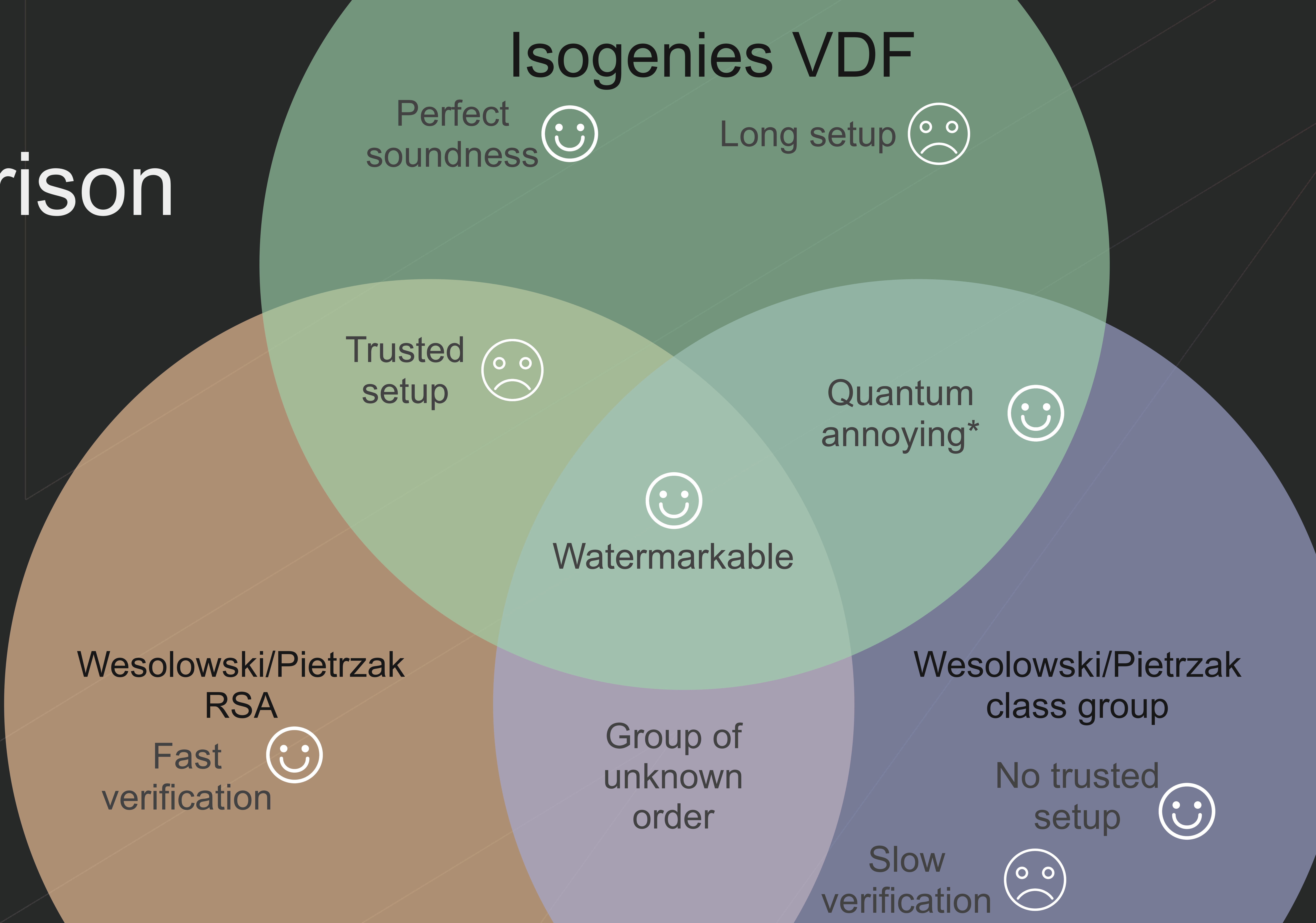
$P \to \phi(P)$

Verify

$e_N(\phi(P), \phi(Q)) = e_N(P, Q)^{2^T}$



VDFs comparison



*only the one defined over F_{p^2}

Outline of contributions

- *"Verifiable Delay Functions from Supersingular Isogenies and Pairings"* [Asiacrypt 2019 DMPS]
- *"A note on the low order assumption in class group of an imaginary quadratic number fields"* [Mathematical Cryptology (conditional accepted) BKSW]
- *"Cryptanalysis of an Oblivious PRF from Supersingular Isogenies"* [Asiacrypt 2020 BKMPS]

Questions?