Speaker	Institution	Title
Robi Pedersen	DTU Compute, Copenhagen	The power of MPC(-in-the-head) techniques in the group action setting
Yizhou Yao	Shanghai Jiao Tong University	How to achieve VOLE-based ZK protocols with sublinear proof size and linear prover time?
Sunniva Engan	NTNU / Aarhus University	Succinct Aggregation of Ring Signatures for Large Rings from Vole-in-the-Head and Approximate Lower Bound Arguments
Mikhail Volkhov	O1Labs	Malleable Algebraic NIZKs and Applications
Megan Chen	Boston University	Proof-Carrying Data From Arithmetized Random Oracles
Anaïs Barthoulot	University of Montpellier, LIRMM	Exploring the Interplay of Cryptographic Accumulators and Zero-Knowledge Proofs
Marek Sefranek	TU Wien	How (Not) to Simulate PLONK
Scott Griffy	Brown University	Succinct Proofs for Privacy-Preserving Blueprints
Lorenzo Martinico	University of Edinburgh	EU Chat Control and Client-Side Scanning

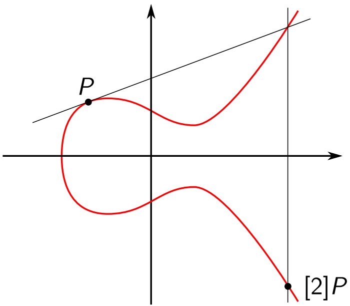
More complex zero-knowledge proofs from group actions

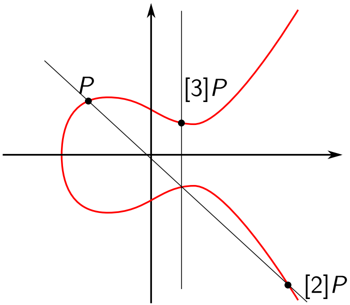
or: *The power of MPC-in-the-head techniques in the group action setting*

Robi Pedersen

based on: C. Delpech de Saint Guilhem and Robi Pedersen. New proof systems and an OPRF from CSIDH. PKC 2024.

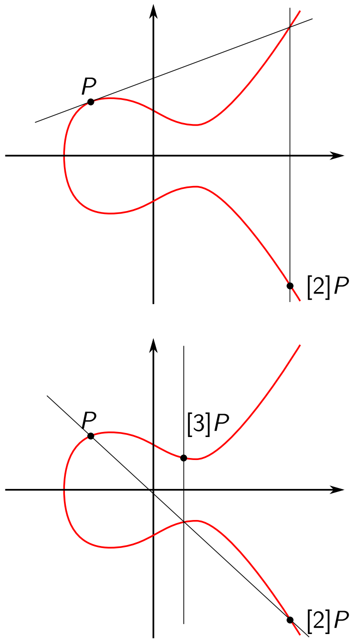
Multiplication map on elliptic curve points





Multiplication map on elliptic curve points

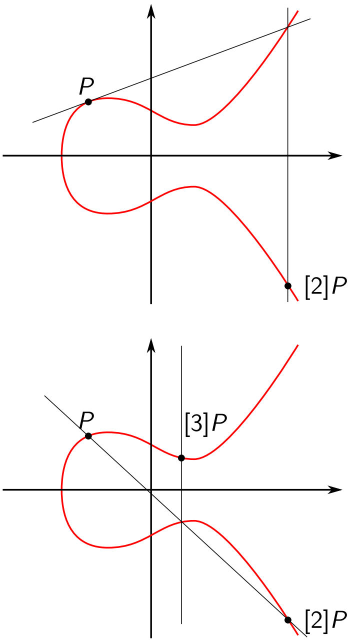
$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$



Multiplication map on elliptic curve points

$$[\;] : \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

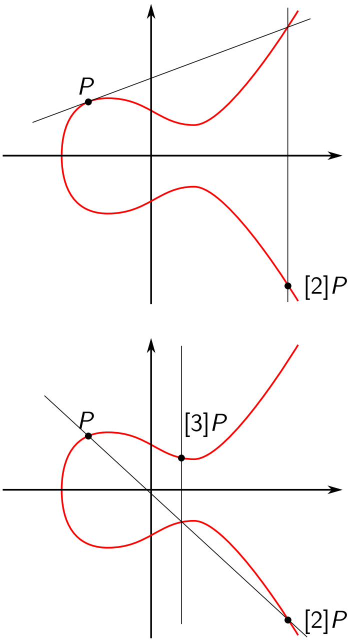


Multiplication map on elliptic curve points

$$[\ ] : \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

$$[a]([b])P = [ab]P$$



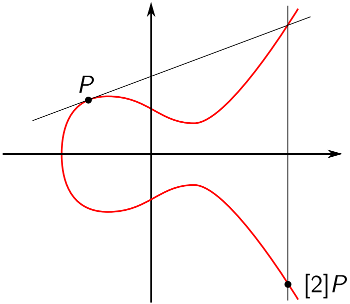
Multiplication map on elliptic curve points

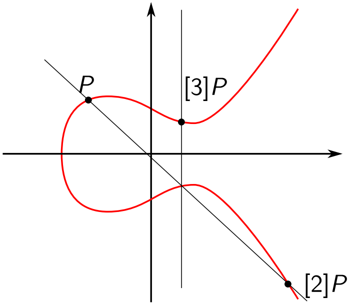
$$[\,]: \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

$$[a]([b])P = [ab]P$$

$$\begin{array}{ccc} P & \xrightarrow{\;a\;} & [a]P \\ \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle b} \\ [b]P & \xrightarrow[\;a\;]{} & [ab]P \end{array}$$



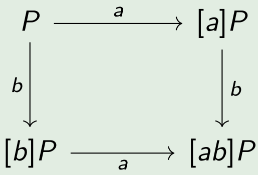


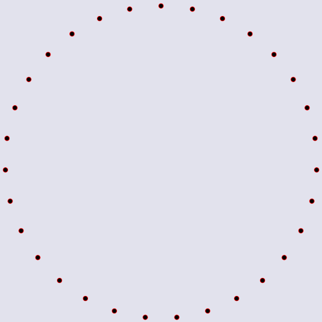
Multiplication map on elliptic curve points

$$[\ ] : \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

$$[a]([b])P = [ab]P$$





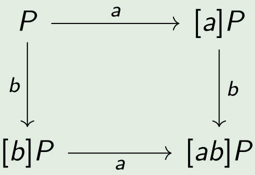
Group action on elliptic curves

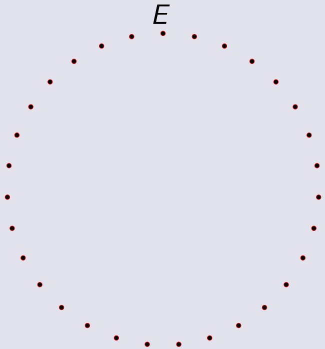
Multiplication map on elliptic curve points

$$[\,]: \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

$$[a]([b])P = [ab]P$$





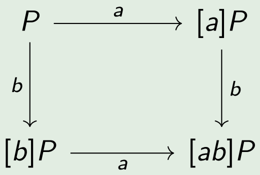
Group action on elliptic curves

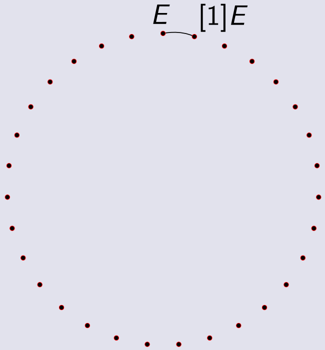
Multiplication map on elliptic curve points

$$[\ ] : \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

$$[a]([b])P = [ab]P$$





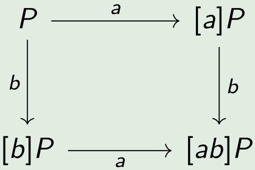
Group action on elliptic curves

Multiplication map on elliptic curve points

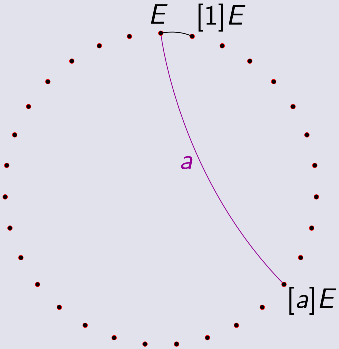
$$[\;] : \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

$$[a]([b])P = [ab]P$$



$$(a, E) \mapsto [a]E$$



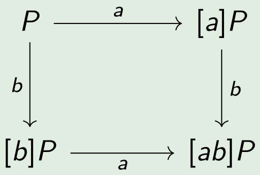
Group action on elliptic curves

Multiplication map on elliptic curve points

$$[\,]:\mathbb{Z}/M\mathbb{Z}\times E(\mathbb{F}_q)\to E(\mathbb{F}_q)$$

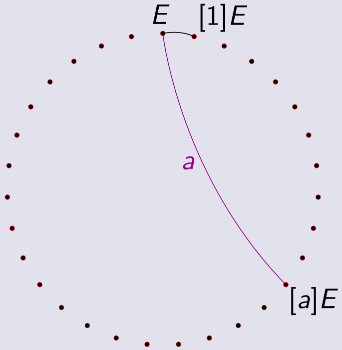
$$(a,P)\mapsto [a]P = \underbrace{P+\cdots+P}_{a\text{ times}}$$

$$[a]([b])P=[ab]P$$



$$[\,]:\mathbb{Z}/N\mathbb{Z}\times\mathcal{E}\to\mathcal{E}$$

$$(a,E)\mapsto [a]E$$



Group action on elliptic curves

Multiplication map on elliptic curve points

$$[\ ] : \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

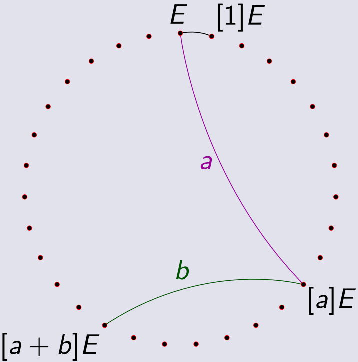
$$[a]([b])P = [ab]P$$

$$\begin{array}{ccc} P & \xrightarrow{a} & [a]P \\ \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle b} \\ [b]P & \xrightarrow[a]{} & [ab]P \end{array}$$

$$[\ ] : \mathbb{Z}/N\mathbb{Z} \times \mathcal{E} \to \mathcal{E}$$

$$(a, E) \mapsto [a]E$$

$$[a]([b]E) = [a+b]E$$



Group action on elliptic curves

Multiplication map on elliptic curve points

$$[\,]: \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

$$[a]([b])P = [ab]P$$

$$\begin{array}{ccc} P & \xrightarrow{\quad a \quad} & [a]P \\ {\scriptstyle b}\downarrow & & \downarrow{\scriptstyle b} \\ [b]P & \xrightarrow[\quad a \quad]{} & [ab]P \end{array}$$

$$[\,]: \mathbb{Z}/N\mathbb{Z} \times \mathcal{E} \to \mathcal{E}$$

$$(a, E) \mapsto [a]E$$

$$[a]([b]E) = [a+b]E$$

$$\begin{array}{ccc} E & \xrightarrow{\quad a \quad} & [a]E \\ {\scriptstyle b}\downarrow & & \downarrow{\scriptstyle b} \\ [b]E & \xrightarrow[\quad a \quad]{} & [a+b]E \end{array}$$

Group action on elliptic curves

Multiplication map on elliptic curve points

$$[\;] : \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

$$[a]([b])P = [ab]P$$

$$[a]P + [b]P = [a+b]P$$

$$\begin{array}{ccc} P & \xrightarrow{\;a\;} & [a]P \\ \big\downarrow{\scriptstyle b} & & \big\downarrow{\scriptstyle b} \\ [b]P & \xrightarrow[\;a\;]{} & [ab]P \end{array}$$

Group action on elliptic curves

$$[\;] : \mathbb{Z}/N\mathbb{Z} \times \mathcal{E} \to \mathcal{E}$$

$$(a, E) \mapsto [a]E$$

$$[a]([b]E) = [a+b]E$$

$$\begin{array}{ccc} E & \xrightarrow{\;a\;} & [a]E \\ \big\downarrow{\scriptstyle b} & & \big\downarrow{\scriptstyle b} \\ [b]E & \xrightarrow[\;a\;]{} & [a+b]E \end{array}$$

Multiplication map on elliptic curve points

$$[\,]:\mathbb{Z}/M\mathbb{Z}\times E(\mathbb{F}_q)\to E(\mathbb{F}_q)$$

$$(a,P)\mapsto [a]P = \underbrace{P+\cdots+P}_{a\text{ times}}$$

$$[a]([b])P=[ab]P$$

$$[a]P+[b]P=[a+b]P$$

$$\begin{array}{ccc} P & \xrightarrow{\ a\ } & [a]P \\ {\scriptstyle b}\downarrow & & \downarrow{\scriptstyle b} \\ [b]P & \xrightarrow[\ a\ ]{} & [ab]P \end{array}$$

$$[\,]:\mathbb{Z}/N\mathbb{Z}\times\mathcal{E}\to\mathcal{E}$$

$$(a,E)\mapsto [a]E$$

$$[a]([b]E)=[a+b]E$$

~~$[a]E+[b]E=$~~

$$\begin{array}{ccc} E & \xrightarrow{\ a\ } & [a]E \\ {\scriptstyle b}\downarrow & & \downarrow{\scriptstyle b} \\ [b]E & \xrightarrow[\ a\ ]{} & [a+b]E \end{array}$$

Group action on elliptic curves

Multiplication map on elliptic curve points

Group

$$[\,]: \mathbb{Z}/M\mathbb{Z} \times \boxed{E(\mathbb{F}_q)} \to \boxed{E(\mathbb{F}_q)}$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

$$[a]([b])P = [ab]P$$

$$[a]P + [b]P = [a+b]P$$

$$\begin{array}{ccc} P & \xrightarrow{\;a\;} & [a]P \\ \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle b} \\ [b]P & \xrightarrow[\;a\;]{} & [ab]P \end{array}$$

Set (no operation)

$$[\,]: \mathbb{Z}/N\mathbb{Z} \times \boxed{\mathcal{E}} \to \boxed{\mathcal{E}}$$

$$(a, E) \mapsto [a]E$$

$$[a]([b]E) = [a+b]E$$

~~$[a]E + [b]E =$~~

$$\begin{array}{ccc} E & \xrightarrow{\;a\;} & [a]E \\ \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle b} \\ [b]E & \xrightarrow[\;a\;]{} & [a+b]E \end{array}$$

Group action on elliptic curves

Multiplication map on elliptic curve points

Group

$$[\,]:\mathbb{Z}/M\mathbb{Z}\times E(\mathbb{F}_q)\to E(\mathbb{F}_q)$$

$$(a,P)\mapsto [a]P = \underbrace{P+\cdots+P}_{a \text{ times}}$$

$$[a]([b])P=[ab]P$$

$$[a]P+[b]P=[a+b]P$$

$$e([a]P,[b]Q)=e(P,Q)^{ab}$$

$$\begin{array}{ccc} P & \xrightarrow{\;a\;} & [a]P \\ \downarrow b & & \downarrow b \\ [b]P & \xrightarrow[\;a\;]{} & [ab]P \end{array}$$

Set (no operation)

$$[\,]:\mathbb{Z}/N\mathbb{Z}\times \mathcal{E}\to \mathcal{E}$$

$$(a,E)\mapsto [a]E$$

$$[a]([b]E)=[a+b]E$$

~~$[a]E+[b]E=$~~

$$\begin{array}{ccc} E & \xrightarrow{\;a\;} & [a]E \\ \downarrow b & & \downarrow b \\ [b]E & \xrightarrow[\;a\;]{} & [a+b]E \end{array}$$

Group action on elliptic curves

Multiplication map on elliptic curve points

Group

$$[\,] : \mathbb{Z}/M\mathbb{Z} \times E(\mathbb{F}_q) \to E(\mathbb{F}_q)$$

$$(a, P) \mapsto [a]P = \underbrace{P + \cdots + P}_{a \text{ times}}$$

$$[a]([b])P = [ab]P$$

$$[a]P + [b]P = [a+b]P$$

$$e([a]P, [b]Q) = e(P, Q)^{ab}$$

$$\begin{array}{ccc} P & \xrightarrow{\;a\;} & [a]P \\ {\scriptstyle b}\downarrow & & \downarrow{\scriptstyle b} \\ [b]P & \xrightarrow[\;a\;]{} & [ab]P \end{array}$$

Group action on elliptic curves

Set (no operation)

$$[\,] : \mathbb{Z}/N\mathbb{Z} \times \mathcal{E} \to \mathcal{E}$$

$$(a, E) \mapsto [a]E$$

$$[a]([b]E) = [a+b]E$$

~~$[a]E + [b]E =$~~

No pairings !

$$\begin{array}{ccc} E & \xrightarrow{\;a\;} & [a]E \\ {\scriptstyle b}\downarrow & & \downarrow{\scriptstyle b} \\ [b]E & \xrightarrow[\;a\;]{} & [a+b]E \end{array}$$

Set (no operation)

$$[\,]:\mathbb{Z}/N\mathbb{Z}\times\mathcal{E}\to\mathcal{E}$$

$$(a,E)\mapsto[a]E$$

$$[a]([b]E)=[a+b]E$$

~~$[a]E+[b]E=$~~

No pairings !

$$\begin{array}{ccc} E & \xrightarrow{\;a\;} & [a]E \\ \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle b} \\ [b]E & \xrightarrow[\;a\;]{} & [a+b]E \end{array}$$

Group action on elliptic curves

$[a+b]E$

Addition

Set (no operation)

$[\,]:\mathbb{Z}/N\mathbb{Z}\times\mathcal{E}\to\mathcal{E}$

$(a,E)\mapsto[a]E$

$[a]([b]E)=[a+b]E$

~~$[a]E+[b]E=$~~

No pairings !

$$\begin{array}{ccc} E & \xrightarrow{a} & [a]E \\ \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle b} \\ [b]E & \xrightarrow[a]{} & [a+b]E \end{array}$$

Group action on elliptic curves

$[a+b]E$

Addition

$[ab]E$

(Scalar) Multiplication

$[a^e]E$

Exponentiation

$[f(a)]E$

Polynomial Evaluation

Pairings?

Set (no operation)

$$[\,]:\mathbb{Z}/N\mathbb{Z}\times\mathcal{E}\to\mathcal{E}$$

$$(a,E)\mapsto[a]E$$

$$[a]([b]E)=[a+b]E$$

~~$[a]E+[b]E=$~~

No pairings !

$$\begin{array}{ccc} E & \xrightarrow{a} & [a]E \\ \downarrow b & & \downarrow b \\ [b]E & \xrightarrow[a]{} & [a+b]E \end{array}$$

Group action on elliptic curves

Zero-knowledge proof systems

$[a+b]E$
Addition

$[ab]E$
(Scalar) Multiplication

$[a^e]E$
Exponentiation

$[f(a)]E$
Polynomial Evaluation

Pairings?

Zero-knowledge proof systems

$[a+b]E$
Addition

$[ab]E$
(Scalar) Multiplication

$[a^e]E$
Exponentiation

$[f(a)]E$
Polynomial Evaluation

Pairings?

$$(E, [a]E, [b]E, [a+b]E)$$

Zero-knowledge proof systems

$[a+b]E$
Addition

$[ab]E$
(Scalar) Multiplication

$[a^e]E$
Exponentiation

$[f(a)]E$
Polynomial Evaluation

Pairings?

$$(E, [a]E, [b]E, [a+b]E)$$

$$(E, [a]E, c, [ca]E)$$

Zero-knowledge proof systems

$[a+b]E$
Addition

$[ab]E$
(Scalar) Multiplication

$[a^e]E$
Exponentiation

$[f(a)]E$
Polynomial Evaluation

Pairings?

$$(E, [a]E, [b]E, [a+b]E)$$

$$(E, [a]E, c, [ca]E)$$
$$(E, [a]E, [b]E, [ab]E)$$

Zero-knowledge proof systems

$[a+b]E$
Addition

$(E, [a]E, [b]E, [a+b]E)$

$[ab]E$
(Scalar) Multiplication

$(E, [a]E, c, [ca]E)$
$(E, [a]E, [b]E, [ab]E)$

$[a^e]E$
Exponentiation

$(E, [a]E, e, [a^e]E)$

$[f(a)]E$
Polynomial Evaluation

Pairings?

Zero-knowledge proof systems

$[a+b]E$

Addition

$[ab]E$

(Scalar) Multiplication

$[a^e]E$

Exponentiation

$[f(a)]E$

Polynomial Evaluation

Pairings?

$$(E, [a]E, [b]E, [a+b]E)$$

$$(E, [a]E, c, [ca]E)$$

$$(E, [a]E, [b]E, [ab]E)$$

$$(E, [a]E, e, [a^e]E)$$

Zero-knowledge proof systems

$[a+b]E$ Addition	$(E, [a]E, [b]E, [a+b]E)$
$[ab]E$ (Scalar) Multiplication	$(E, [a]E, c, [ca]E)$ $(E, [a]E, [b]E, [ab]E)$
$[a^e]E$ Exponentiation	$(E, [a]E, e, [a^e]E)$
$[f(a)]E$ Polynomial Evaluation	$(E, [a]E, f(x), [f(a)]E)$
Pairings?	

Zero-knowledge proof systems

$[a+b]E$
Addition

$(E, [a]E, [b]E, [a+b]E)$

$[ab]E$
(Scalar) Multiplication

$(E, [a]E, c, [ca]E)$

$(E, [a]E, [b]E, [ab]E)$

$[a^e]E$
Exponentiation

$(E, [a]E, e, [a^e]E)$

$[f(a)]E$
Polynomial Evaluation

$(E, [a]E, f(x), [f(a)]E)$

$(E, [f_1]E, \ldots, [f_n]E, [a]E, [f(a)]E)$

Pairings?

Zero-knowledge proof systems

$[a+b]E$ Addition	$(E, [a]E, [b]E, [a+b]E)$
$[ab]E$ (Scalar) Multiplication	$(E, [a]E, c, [ca]E)$ $(E, [a]E, [b]E, [ab]E)$
$[a^e]E$ Exponentiation	$(E, [a]E, e, [a^e]E)$
$[f(a)]E$ Polynomial Evaluation	$(E, [a]E, f(x), [f(a)]E)$ $(E, [f_1]E, \ldots, [f_n]E, [a]E, [f(a)]E)$
Pairings?	

Zero-knowledge proof systems

$[a+b]E$ Addition	$(E, [a]E, [b]E, [a+b]E)$
$[ab]E$ (Scalar) Multiplication	$(E, [a]E, c, [ca]E)$ $(E, [a]E, [b]E, [ab]E)$
$[a^e]E$ Exponentiation	$(E, [a]E, e, [a^e]E)$
$[f(a)]E$ Polynomial Evaluation	$(E, [a]E, f(x), [f(a)]E)$ $(E, [f_1]E, \ldots, [f_n]E, [a]E, [f(a)]E)$
Pairings?	$e([a]P, [b]Q) = e([ab]P, Q)$

Zero-knowledge proof systems

$[a+b]E$ Addition	$(E, [a]E, [b]E, [a+b]E)$
$[ab]E$ (Scalar) Multiplication	$(E, [a]E, c, [ca]E)$ $(E, [a]E, [b]E, [ab]E)$
$[a^e]E$ Exponentiation	$(E, [a]E, e, [a^e]E)$
$[f(a)]E$ Polynomial Evaluation	$(E, [a]E, f(x), [f(a)]E)$ $(E, [f_1]E, \ldots, [f_n]E, [a]E, [f(a)]E)$
Pairings?	$e([a]P, [b]Q) = e([ab]P, Q)$

Similar statements, but needs a prover!

A BLS-type signature

public key $[a]P$

$$e([aH(m)]P, P) = e([H(m)]P, [a]P)$$

A ZSS-type signature

public key $[a]P$

$$e\left(\left[(a + H(m))^{-1}\right] P, [H(m)]P + [a]P\right) = e(P, P)$$

A BLS-type signature

public key $[a]P$
$[a]E$

$$e([aH(m)]P, P) = e([H(m)]P, [a]P)$$

$$(E, [a]E, H(m), [aH(m)]E)$$

Scalar multiplication

A ZSS-type signature

public key $[a]P$

$$e\left(\left[(a + H(m))^{-1}\right] P, [H(m)]P + [a]P\right) = e(P, P)$$

A BLS-type signature

public key $[a]P$

$[a]E$

$$e([aH(m)]P, P) = e([H(m)]P, [a]P)$$

$$(E, [a]E, H(m), [aH(m)]E)$$

Scalar multiplication

A ZSS-type signature

public key $[a]P$

$[a]E$

$$e\left(\left[(a + H(m))^{-1}\right] P, [H(m)]P + [a]P\right) = e(P, P)$$

$$(E, [H(m)][a]E, \left[(a + H(m))^{-1}\right] E, [1]E)$$

Multiplication

A BLS-type signature

public key $[a]P$
$[a]E$

$$e([aH(m)]P, P) = e([H(m)]P, [a]P)$$

$$(E, [a]E, H(m), [aH(m)]E)$$

Scalar multiplication

A ZSS-type signature

public key $[a]P$
$[a]E$

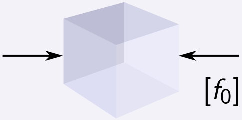
$$e\left(\left[(a + H(m))^{-1}\right] P, [H(m)]P + [a]P\right) = e(P, P)$$

$$\left(E, [H(m)][a]E, \left[(a + H(m))^{-1}\right] E, [1]E\right)$$

Multiplication

A new OPRF

Client
m



Server
$[f_0]E, \ldots, [f_n]E$

A BLS-type signature

public key $[a]P$
$[a]E$

$$e([aH(m)]P, P) = e([H(m)]P, [a]P)$$

$$(E, [a]E, H(m), [aH(m)]E)$$

Scalar multiplication

A ZSS-type signature

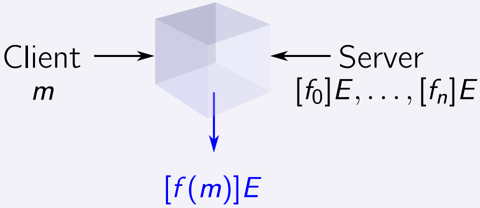
public key $[a]P$
$[a]E$

$$e\left(\left[(a + H(m))^{-1}\right] P, [H(m)]P + [a]P\right) = e(P, P)$$

$$(E, [H(m)][a]E, \left[(a + H(m))^{-1}\right] E, [1]E)$$

Multiplication

A new OPRF



A BLS-type signature

public key $[a]P$

$[a]E$

$$e([aH(m)]P, P) = e([H(m)]P, [a]P)$$

$$(E, [a]E, H(m), [aH(m)]E)$$

Scalar multiplication

A ZSS-type signature

public key $[a]P$

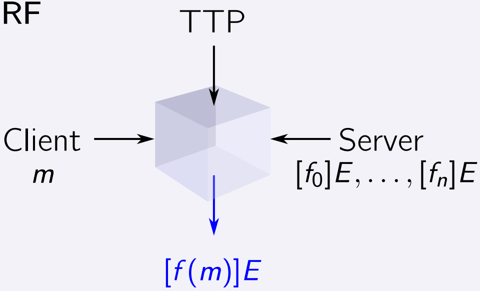
$[a]E$

$$e\left(\left[(a + H(m))^{-1}\right] P, [H(m)]P + [a]P\right) = e(P, P)$$

$$\left(E, [H(m)][a]E, \left[(a + H(m))^{-1}\right] E, [1]E\right)$$

Multiplication

A new OPRF



A BLS-type signature

public key $[a]P$
$[a]E$

$$e([aH(m)]P, P) = e([H(m)]P, [a]P)$$

$$(E, [a]E, H(m), [aH(m)]E)$$

Scalar multiplication

A ZSS-type signature

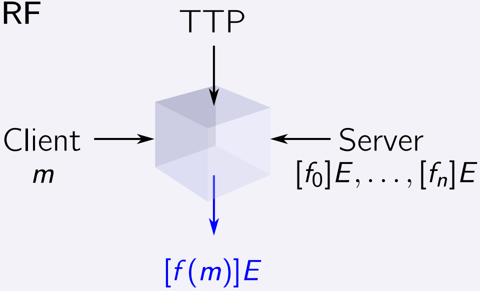
public key $[a]P$
$[a]E$

$$e\left(\left[(a + H(m))^{-1}\right] P, [H(m)]P + [a]P\right) = e(P, P)$$

$$(E, [H(m)][a]E, \left[(a + H(m))^{-1}\right] E, [1]E)$$

Multiplication

A new OPRF



Round-optimal

100x faster and smaller

Malicious client and verifiable

A BLS-type signature

public key $[a]P$
$[a]E$

$$e([aH(m)]P, P) = e([H(m)]P, [a]P)$$

$$(E, [a]E, H(m), [aH(m)]E)$$

Scalar multiplication

A ZSS-type signature

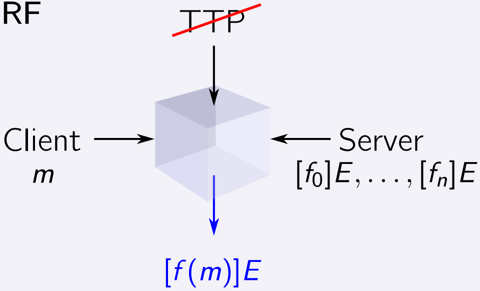
public key $[a]P$
$[a]E$

$$e\left(\left[(a + H(m))^{-1}\right] P, [H(m)]P + [a]P\right) = e(P, P)$$

$$(E, [H(m)][a]E, \left[(a + H(m))^{-1}\right] E, [1]E)$$

Multiplication

A new OPRF



Round-optimal

100x faster and smaller

Malicious client and verifiable

For more informations, visit https://eprint.iacr.org/2023/1614.pdf

C. Delpech de Saint Guilhem and Robi Pedersen. New proof systems and an OPRF from CSIDH.

上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

Interactive Line-Point Zero-Knowledge with Sublinear Communication and Linear Computation

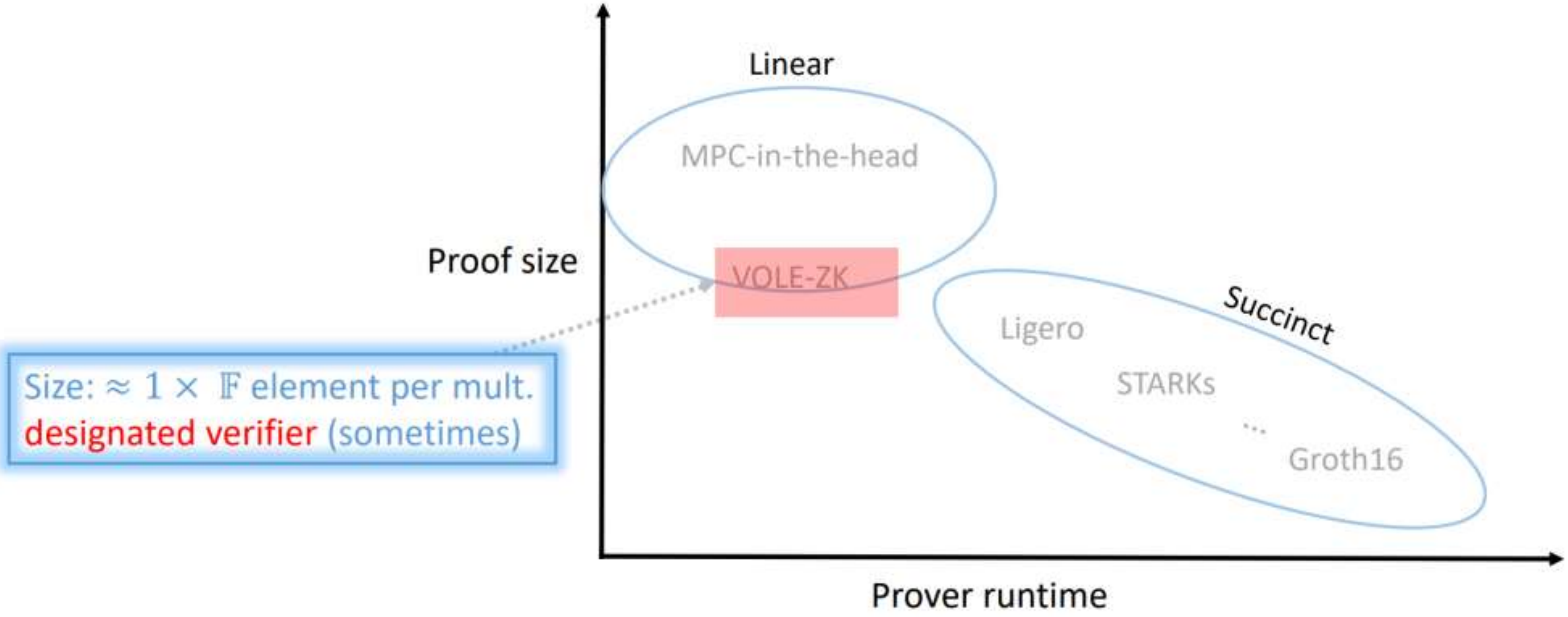
Fuchun Lin, Chaoping Xing, and Yizhou Yao

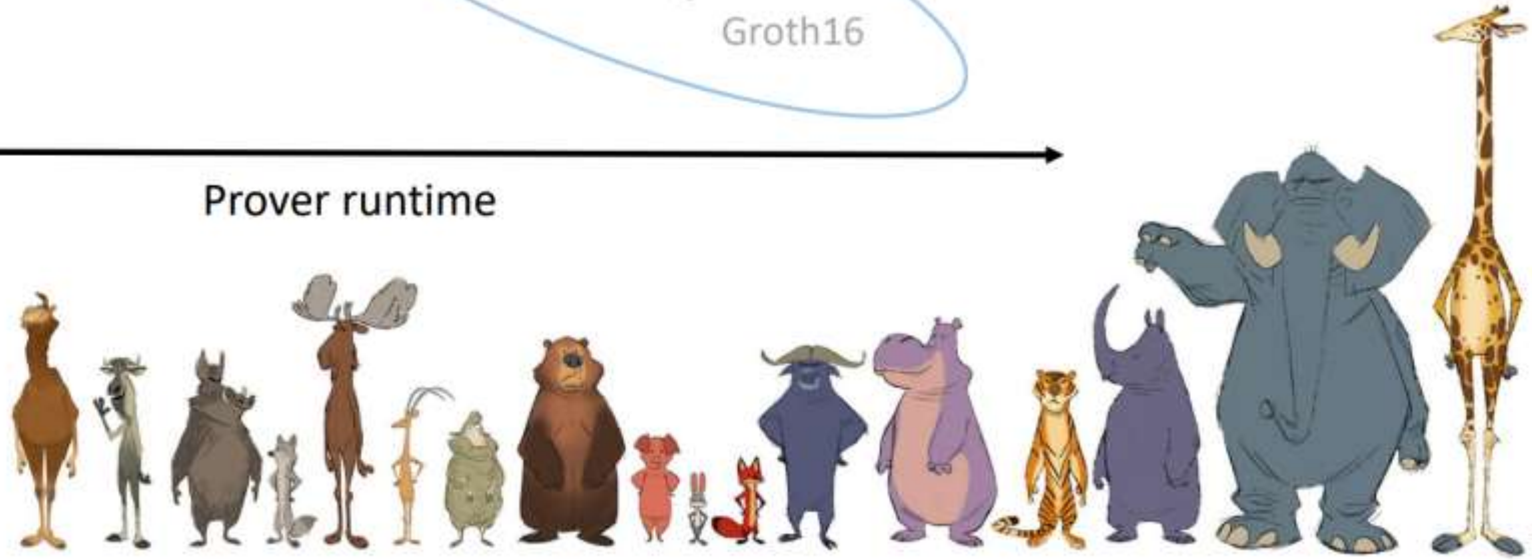
Shanghai Jiao Tong University

04/09/2024, Edinburgh

饮 水 思 源 • 爱 国 荣 校

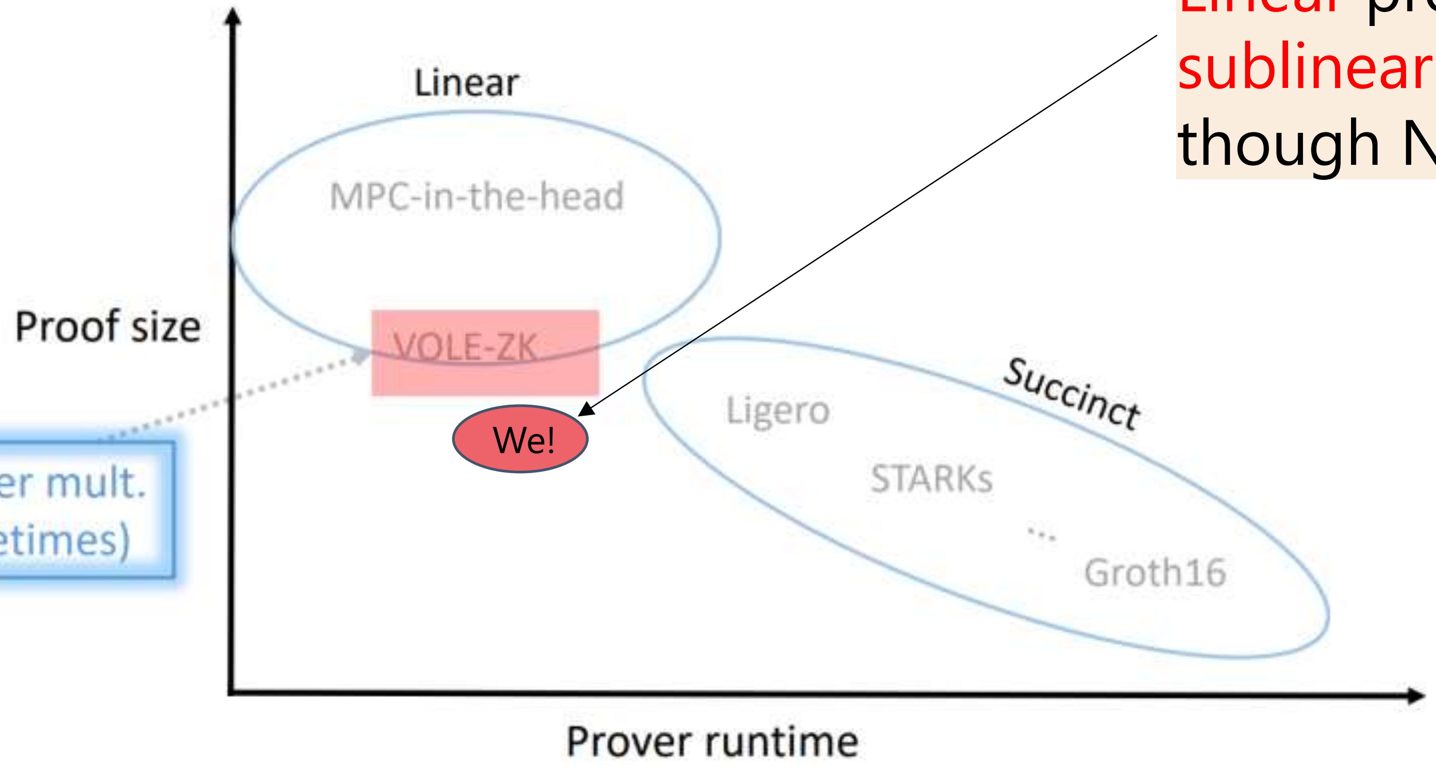
Families of ZK Proofs



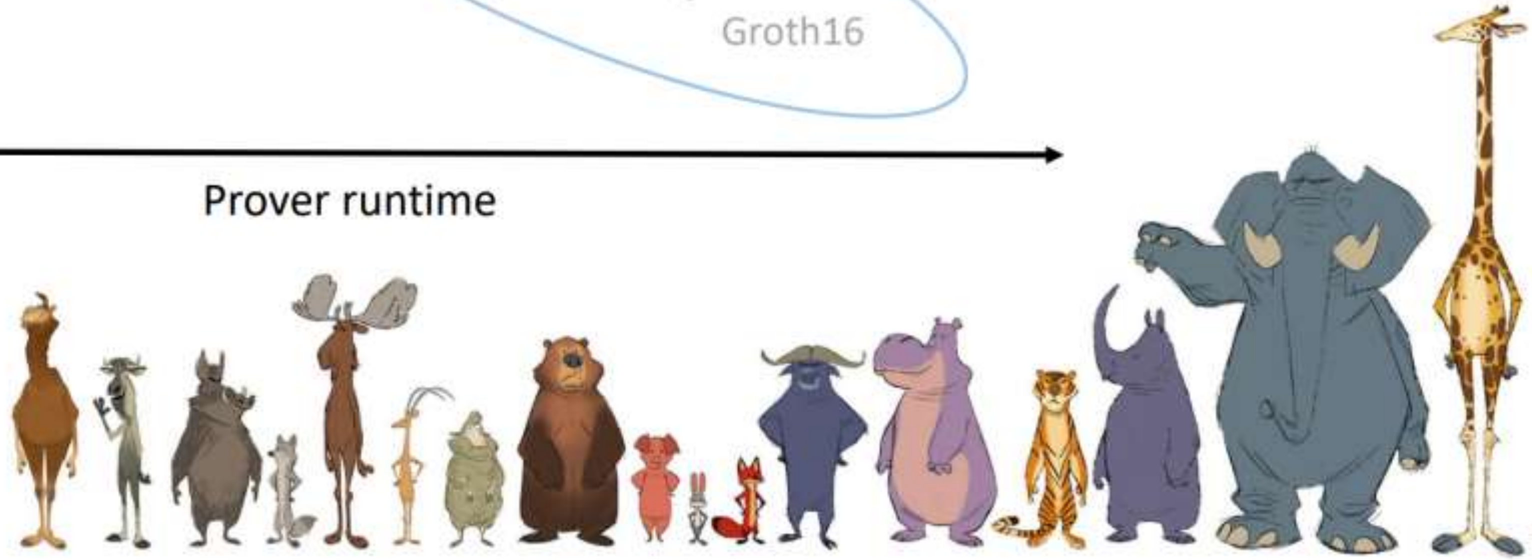


Families of ZK Proofs

Linear prover time & sublinear proof size though NOT succinct



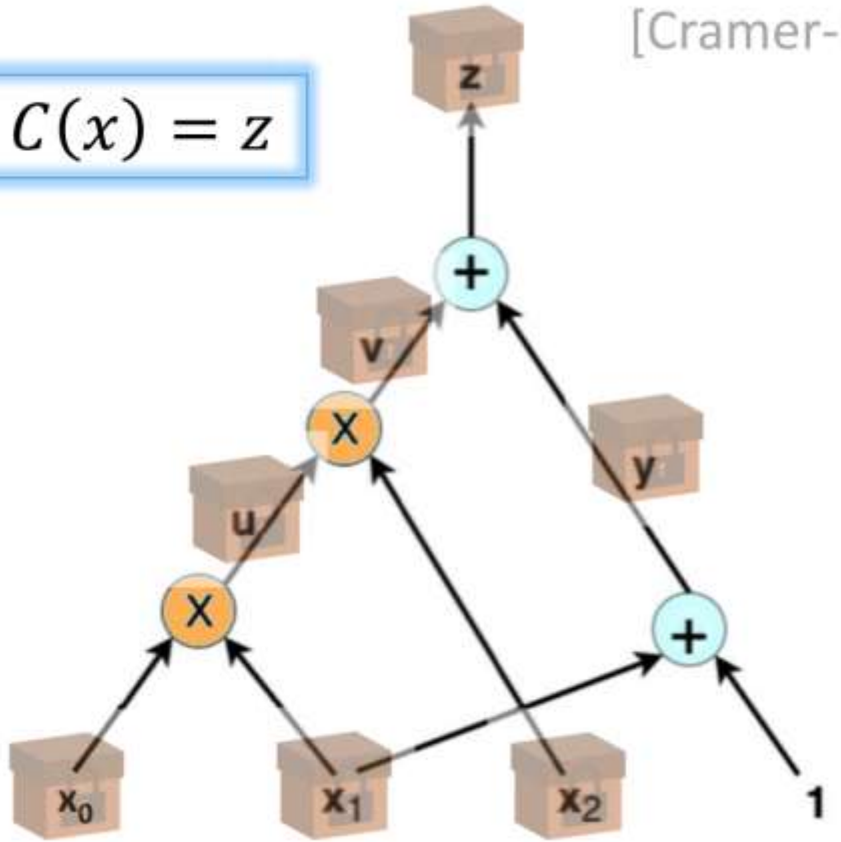
Size: ≈ 1 × $\mathbb{F}$ element per mult.
designated verifier (sometimes)



Proving circuits with linear commitments

[Cramer-Damgård 97]

Goal: prove knowledge of x such that $C(x) = z$



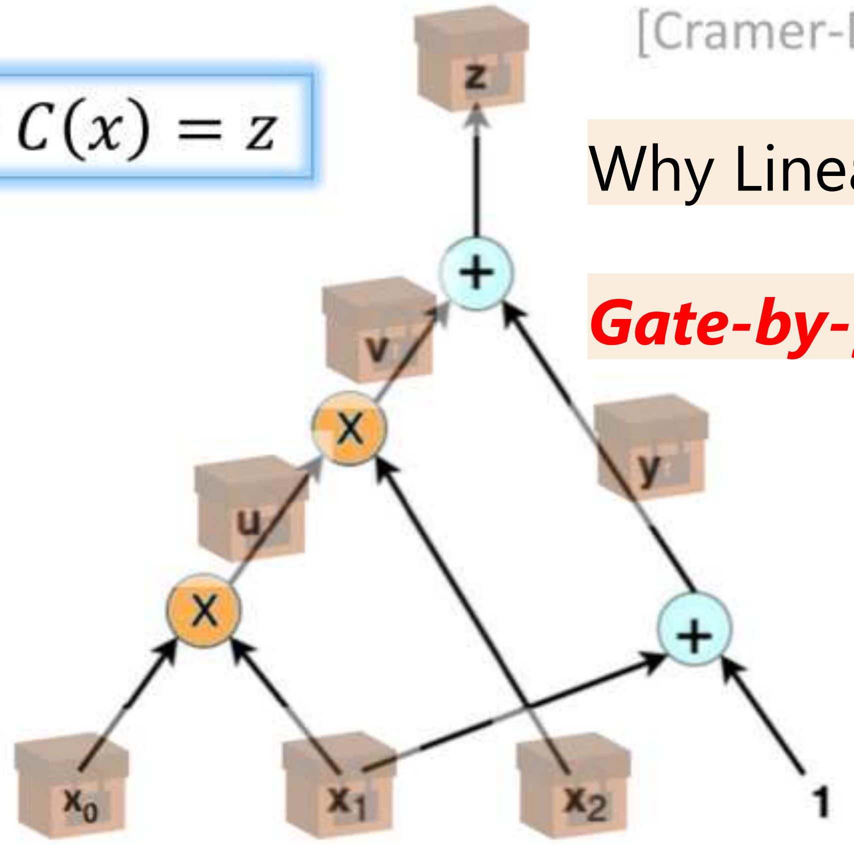
- Commit to extended witness $\vec{w}$
  - ➢inputs, + output wire of every mult.
- Evaluate linear gates
  - ➢Using linear homomorphism
- Prove correctness of multiplications

Proving circuits with linear commitments

[Cramer-Damgård 97]

Goal: prove knowledge of x such that $C(x) = z$

- Commit to extended witness $\vec{w}$
  - inputs, + output wire of every mult.
- Evaluate linear gates
  - Using linear homomorphism
- Prove correctness of multiplications



Why Linear proof size?

Gate-by-gate flavor!

The GKR protocol—core idea

Common input: C and $\mathbf{x}$, which defines $W_d : \{0,1\}^{s_d} \to \mathbb{F}$

1. P sends $\mathbf{y} = C(\mathbf{x})$, which defines $W_0^* : \{0,1\}^{s_0} \to \mathbb{F}$
2. V chooses $r \leftarrow \mathbb{F}^{s_0}$, sends r to P, and sets $H_0 := \widetilde{W}_0^*(r)$
3. P, V run the sum-check protocol to show $H_0 = \sum_{b,c} \tilde{p}_1(r, b, c)$

Layer-by-layer to the Rescue!

Intuition:

- Let W_0 be the function corresponding to the correct output
- If $W_0^* \neq W_0$, then $\widetilde{W}_0^*(r) \neq \widetilde{W}_0(r)$ w.h.p.
- If $\widetilde{W}_0^*(r) \neq \widetilde{W}_0(r)$, V will reject in the sum-check protocol w.h.p.

IP+ Linear Com -> ZKP

[Cramer-Damgård 97]

Combine linear-time GKR (Libra [XZZ+19], [ZLW+21]) with VOLE-based commitments.

Construction & Intuition:

1. Prover runs GKR-Prover except that all messages are committed by VOLE

2. Verifier checks whether a GKR verifier will accept the "proof"

Recall that the GKR verifier only checks degree-2 relations!

Equivalent to multiplication check!

Our Approach

IP+ Linear Com -> ZKP

[Cramer-Damgård 97]

Combine linear-time GKR (Libra [XZZ+19], [ZLW+21]) with VOLE-based commitments.

Construction & Intuition:

1. Prover runs GKR-Prover except that all messages are committed by VOLE

2. Verifier checks whether a GKR verifier will accept the "proof"

In particular, we can extend GKR to Z_{2k} and incorporate it with MozZarella's commitment for Z_{2k}.

Hence, we obtain ZK for Z_{2k} with *linear time prover* and *sublinear proof size*.

Sum-check protocol for $\mathbb{Z}_{2^k}$

$\deg(p) \le 2$, $\ell = k + 2s$

Sum-check protocol

Common inputs: $p \in \mathbb{F}[x_1, \ldots, x_n]$ ($\mathbb{Z}_{2^k}$), sum

$$H_0 := \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} p(x_1, \ldots, x_n) \mod 2^k$$

$\hat{H}_0 = \sum p(x_1, \ldots, x_n) \mod 2^\ell$ $\quad$ $\hat{H}_0 = H_0 \mod 2^k$

1. For $i = 1, \ldots, n$ do:
   1. P sends $p_i(x_i) := \sum_{x_{i+1}} \cdots \sum_{x_n} p(r_1, \ldots, r_{i-1}, x_i, \ldots, x_n)$ $\mod 2^\ell$
   2. V checks the degree of p_i and that $p_i(0) + p_i(1) = \hat{H}_{i-1}$ $\mod 2^\ell$
   3. V chooses $r_i \leftarrow \mathbb{F}$ ($\mathbb{Z}_{2^s}$), sets $\hat{H}_i := p_i(r_i)$ $\mod 2^\ell$, and sends r_i to P
2. V checks that $\hat{H}_n = p(r_1, \ldots, r_n)$ $\mod 2^\ell$

Completeness is clear...

Analysis of sum-check protocol

Theorem

Let p be an n-variate polynomial of degree d_i in each variable. Then the sum-check protocol has soundness error $\leq \sum_i d_i/|\mathbb{F}|$.

Proof.

By induction on n...

Inductive step: Say $H_0 \neq \sum_{x_1 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} p(x_1, \ldots, x_n)$. Let $p_1^*(x_1) = \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} p(x_1, \ldots, x_n)$

- If $p_1 = p_1^*$, then $p_1(0) + p_1(1) \neq H_0$ and V rejects
- If $p_1 \neq p_1^*$, then $\Pr_{r_1}[p_1(r_1) \neq p_1^*(r_1)] \geq 1 - d_1/|\mathbb{F}|$
- When that is the case, $H_1 \neq \sum_{x_2 \in \{0,1\}} \cdots \sum_{x_n \in \{0,1\}} p(r_1, x_2, \ldots, x_n)$ and we can apply the induction hypothesis

上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

Thank You

饮 水 思 源　爱 国 荣 校

Vector-OLE based Zero-Knowledge Proof

Linearly homomorphic commitment from VOLE:

MAC tags $\mathbf{M}_x$ and values $\mathbf{x}$ $[\mathbf{x}]$ MAC keys $\mathbf{K}_x$ and global key Δ

cf. Wolverine [WYKW21] for fields, MozZarella [BBMS22] for rings

Gate-by-gate flavor of classical VOLE-based ZK:

"Commit-and-prove" paradigm: Prover first commits all intermediate wire values via VOLE, then proves to Verifier values underneath the commitments satisfy the circuit topology.

Protocols vary in designing CheckZero, Open, CheckMultiplication. Most techniques are distilled from MPC literature.

Motivation

Appealing features of VOLE-based ZK:

Fast proving

Small memory

F_2/Z_{2k}-friendly

Other typical properties:

Plausibly post-quantum

UC-security

Interactive

Designated-verifier from a PCG-setup

Publicly verifiable via VOLEitH

Downsides:

Linear proof size → Sublinear ?

Linear verification

while maintain most of good properties

Our Results

Efficiency Metrics	QuickSilver [YSWW21]	AntMan [WYY+22]	**This work [LXY24]**
P Comp.	linear	quasilinear	linear
P/V Mem.	small, streaming	larger, streaming	larger
Comm.	linear	sublinear	sublinear
V Comp.	linear	linear, but larger	linear, slightly larger
Interaction	interactive	interactive	interactive

Our Approach: Combine linear-time GKR (Libra [XZZ+19], [ZLW+21]) with VOLE-based commitments, thus inherit a layer-by-layer flavor.

IP+ Com -> ZKP

Our Results

Efficiency Metrics	QuickSilver [YSWW21]	AntMan [WYY+22]	**This work [LXY24]**
P Comp.	linear	quasilinear	linear
P/V Mem.	small, streaming	larger, streaming	larger
Comm.	linear	sublinear	sublinear
V Comp.	linear	linear, but larger	linear, slightly larger
Interaction	interactive	interactive	interactive

In particular, we also extend GKR to Z_{2^k} and incorporate it with MozZarella's commitment for Z_{2^k}.

Hence, we obtain ZK for Z_{2^k} with *linear time prover* and *sublinear proof size*.

Threshold Ring Signatures for Large Rings from VOLE-in-the-Head and Approximate Lower Bound Arguments

James Chiang, Ivan Damgård, William Duro, Sunniva Engan, Sebastian Kolby, Peter Scholl

Aarhus University

Threshold Ring Signature

- Construct a t-out-of-n threshold ring signature from OWF + ZK
  - Each user has their own $(\mathsf{pk}, \mathsf{sk}) = ((x, y), k)$ such that $E_k(x) = y$ pair for signing

Threshold Ring Signature

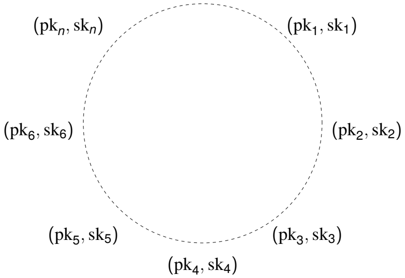


Figure: Ring of n users

Threshold Ring Signature

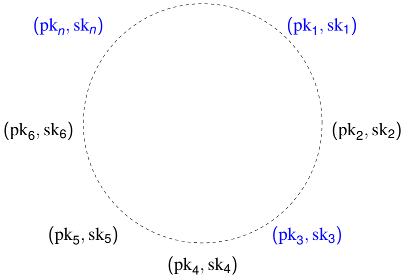


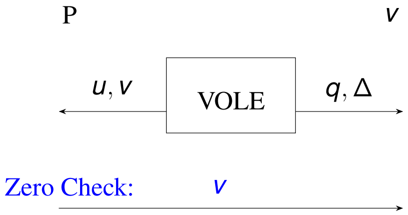
Figure: Ring of n users, with threshold 3

Threshold Ring Signature

- Construct a t-out-of-n threshold ring signature from OWF + ZK
  - Each user has their own $(\mathsf{pk}, \mathsf{sk}) = ((x, y), k)$ such that $E_k(x) = y$ pair for signing
- Each signing member in the ring contribute with a partial signature
  - No signer can contribute twice, due to collision-resistance of a deterministic substring (referred to as a tag)
  - Combine partial signatures using string concatenation to obtain the final signature

VOLE Commitments

- Homomorphic vector commitments of the form $q = u \cdot \Delta + v$



- We can make VOLE commitments non-interactive, which is referred to as VOLE-in-the-head
- Obtained from GGM tree vector commitments, where we make use of an $(n-1)$-out-of-n commitment scheme.

Scalability for Large Rings

Signatures scale sublinearly to the number of users in the ring

- Compressing OR statements
- Approximate Lower Bound Arguments (ALBA)
  - Make use of the uniqueness of tags

Malleable Algebraic NIZKs

& applications

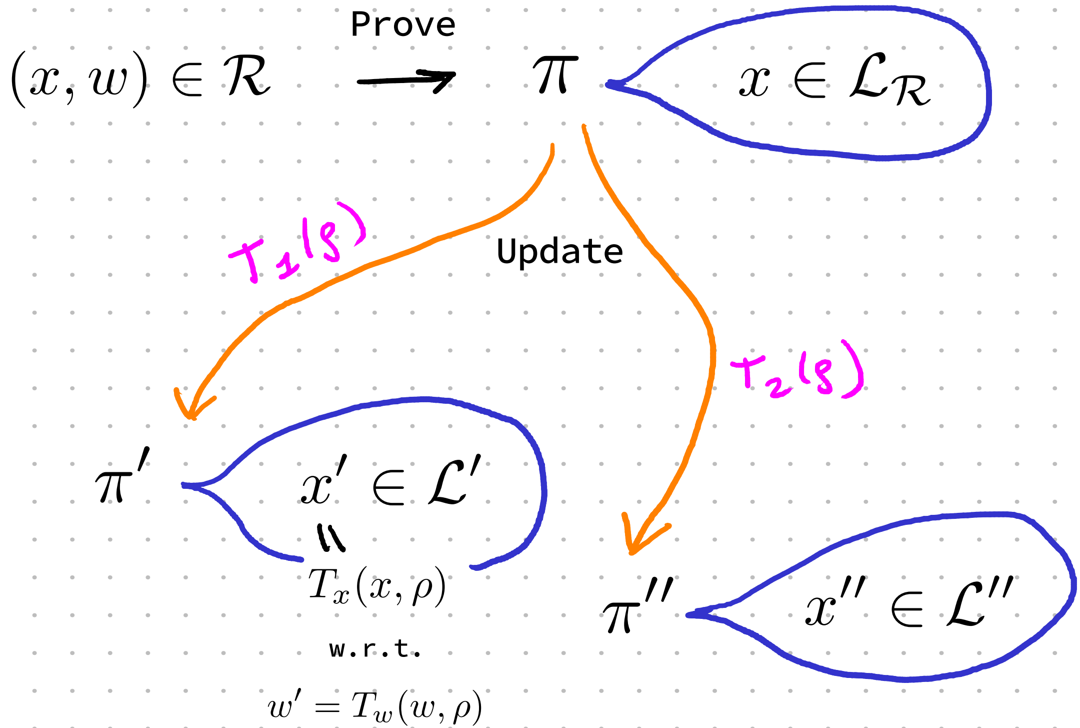
Mikhail Volkhov

O1Labs

ex University of Edinburgh

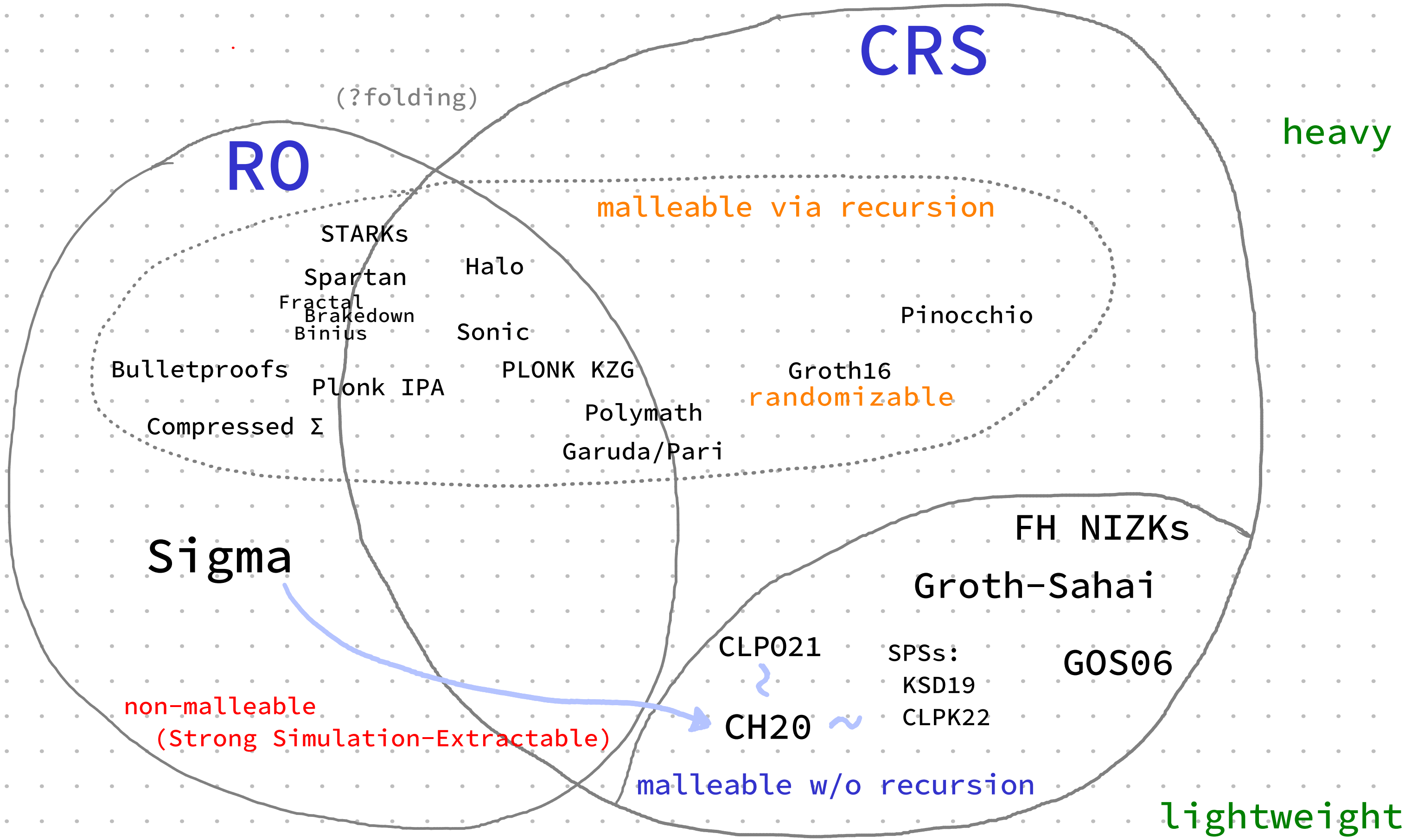
mv@volhovm.com

Controlled* Malleability in NIZKs



* NB: Not to be confused with Controlled Malleability as a security notion

Landscape of Malleable NIZKs



CH20 is like the basic Sigma-protocol

$$(\mathbf{M}, \mathbf{\Theta}) \xleftarrow{\$} \mathcal{D}_{par}$$

$\mathcal{P}$		$\mathcal{V}$
$[\mathbf{x}], \mathbf{w}$		$[\mathbf{x}]$
$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_p^k$ $[\mathbf{a}] := [\mathbf{M}(\mathbf{x})]\mathbf{r}$	$[\mathbf{a}]$ $\longrightarrow$	
	$\longleftarrow$ e	$e \xleftarrow{\$} \mathbb{Z}_p$
$\mathbf{d} := e\mathbf{w} + \mathbf{r}$	$\mathbf{d}$ $\longrightarrow$	
		check $[\mathbf{M}(\mathbf{x})]\mathbf{d} \stackrel{?}{=} [\mathbf{\Theta}(\mathbf{x})]e + [\mathbf{a}]$

For the algebraic language:

$$\mathcal{L}_{\mathsf{alg}} = \{\vec{x} \in \mathbb{G}^l \mid \exists \vec{w} \in \mathbb{Z}_p^t : M(\vec{x}) \cdot \vec{w} = \vec{x}\}$$

where $M(\vec{X}) \in \mathcal{P}^{l \times t}$

CH20 NIZK

... but done with pairings

CRSGen (1^λ):

$par := \mathcal{PG} \xleftarrow{\$} PGGen(1^\lambda)$
$e \xleftarrow{\$} \mathbb{Z}_p$
$\text{CRS} := (\mathcal{PG}, [e]_2), \mathcal{T} := e$
$\text{return } (par, \text{CRS}, \mathcal{T})$

Prove $(\text{CRS}, ([\mathbf{M}]_1, [\mathbf{\Theta}]_1), [\mathbf{x}]_1 \in \mathbb{G}_1^l, \mathbf{w} \in \mathbb{Z}_p^t)$:

$\mathbf{r} \xleftarrow{\$} \mathbb{Z}_p^t$
$[\mathbf{a}]_1 := [\mathbf{M}(\mathbf{x})]_1 \mathbf{r}$
$[\mathbf{d}]_2 := [e]_2 \mathbf{w} + [\mathbf{r}]_2$
$\text{return } \sigma := ([\mathbf{a}]_1, [\mathbf{d}]_2)$

Verify $(\text{CRS}, ([\mathbf{M}]_1, [\mathbf{\Theta}]_1), [\mathbf{x}]_1, \sigma = ([\mathbf{a}]_1, [\mathbf{d}]_2))$:

check

$$[\mathbf{M}(\mathbf{x})]_1 \bullet [\mathbf{d}]_2 \stackrel{?}{=} [\mathbf{\Theta}(\mathbf{x})]_1 \bullet [e]_2 + [\mathbf{a}]_1 \bullet [1]_2$$

CH20 NIZK is updatable!

π

Define $\mathsf{Update}(([\boldsymbol{a}]_1, [\boldsymbol{d}]_2), T := (T_{\mathsf{am}}, T_{\mathsf{aa}}, T_{\mathsf{xm}}, T_{\mathsf{xa}}, T_{\mathsf{wm}}, T_{\mathsf{wa}}))$ as a function returning $\pi' = ([\boldsymbol{a}']_1, [\boldsymbol{d}']_2)$ constructed as follows:

$\hat{\pi}$

$$[\boldsymbol{a}']_1 = T_{\mathsf{am}} \cdot \begin{pmatrix} [\boldsymbol{a}]_1 \\ \mathsf{x} \end{pmatrix} + [1]_1 \cdot T_{\mathsf{aa}} + [M(\mathsf{x}')]_1 \cdot \hat{\boldsymbol{s}}$$

$$[\boldsymbol{d}']_2 = T_{\mathsf{wm}} \cdot [\boldsymbol{d}]_2 + [z]_2 \cdot T_{\mathsf{wa}} + [1]_2 \cdot T_{\mathsf{wa}} + [1]_2 \cdot \hat{\boldsymbol{s}}$$

where $\hat{\boldsymbol{s}}$ is sampled uniformly at random.

CH20 NIZK is updatable!

π

Define $\mathsf{Update}(([\boldsymbol{a}]_1, [\boldsymbol{d}]_2), T := (T_{\mathsf{am}}, T_{\mathsf{aa}}, T_{\mathsf{xm}}, T_{\mathsf{xa}}, T_{\mathsf{wm}}, T_{\mathsf{wa}}))$ as a function returning $\pi' = ([\boldsymbol{a}']_1, [\boldsymbol{d}']_2)$ constructed as follows:

$\hat{\pi}$

$$[\boldsymbol{a}']_1 = T_{\mathsf{am}} \cdot \begin{pmatrix} [\boldsymbol{a}]_1 \\ \mathsf{x} \end{pmatrix} + [1]_1 \cdot T_{\mathsf{aa}} + [M(\mathsf{x}')]_1 \cdot \hat{\boldsymbol{s}}$$

$$[\boldsymbol{d}']_2 = T_{\mathsf{wm}} \cdot [\boldsymbol{d}]_2 + [z]_2 \cdot T_{\mathsf{wa}} + [1]_2 \cdot T_{\mathsf{wa}} + [1]_2 \cdot \hat{\boldsymbol{s}}$$

where $\hat{\boldsymbol{s}}$ is sampled uniformly at random.

...for blinding-compatible transformations:

$$T_{\mathsf{am}} \cdot \begin{pmatrix} M(\vec{x}) \cdot \vec{s} \\ \vec{x} \end{pmatrix} + T_{\mathsf{aa}} = M(T_{\mathsf{xm}} \cdot \vec{x}) + T_{\mathsf{xa}} \cdot \left(T_{\mathsf{wm}} \cdot \vec{s} + T_{\mathsf{wa}}\right)$$

$$\forall x \in \mathcal{L}, \forall s$$

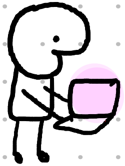
Application:

Updatable Blueprints

charlie

y

pk



bob

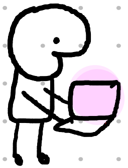
ElGamal

$$\{\mathsf{Enc}_{\mathsf{pk}}(x^i y^j)\}$$

Application:

Updatable Blueprints

charlie



bob

ElGamal

update

$$\{\mathsf{Enc}_{\mathsf{pk}}(x^i y^j)\} \Longrightarrow \{\mathsf{Enc}_{\mathsf{pk}}(\hat{x}^i y^j)\}$$

where

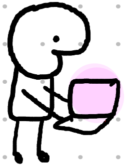
$$\hat{x} = \alpha x + \beta$$

ia.cr/2023/1787

Application:

Updatable Blueprints

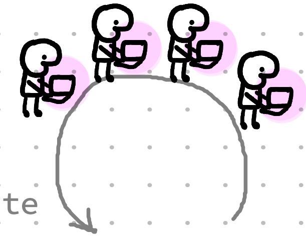
charlie



bob

ElGamal

update



$$\{\mathsf{Enc}_{\mathsf{pk}}(x^i y^j)\} \Longrightarrow \{\mathsf{Enc}_{\mathsf{pk}}(\hat{x}^i y^j)\}$$

where

$$\hat{x} = \alpha x + \beta$$

Application:

Updatable Blueprints

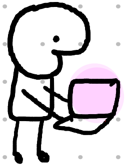
charlie

y

pk

charlie learns:

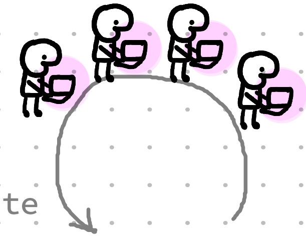
$$\text{if } F(\hat{x}, y) = 0 \text{ then } G(\hat{x}, y)$$



bob

ElGamal

update



eval

$$\{\mathsf{Enc}_{\mathsf{pk}}(x^i y^j)\} \Longrightarrow \{\mathsf{Enc}_{\mathsf{pk}}(\hat{x}^i y^j)\} \Longrightarrow \begin{array}{l}\mathsf{Enc}_{\mathsf{pk}}(r_1 \cdot F(\hat{x}, y)),\\ \mathsf{Enc}_{\mathsf{pk}}(r_2 \cdot F(\hat{x}, y) + G(\hat{x}, y))\end{array}$$

where

$$\hat{x} = \alpha x + \beta$$

ia.cr/2023/1787

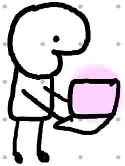
Application:

Updatable Blueprints

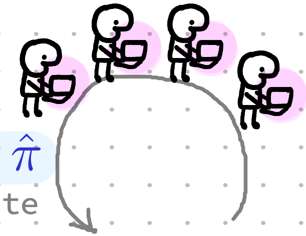
charlie

y

pk



bob



charlie learns:

if $F(\hat{x}, y) = 0$ then $G(\hat{x}, y)$

$\pi \mapsto \hat{\pi}$

update

ElGamal

$\{\mathsf{Enc}_{\mathsf{pk}}(x^i y^j)\} \Longrightarrow \{\mathsf{Enc}_{\mathsf{pk}}(\hat{x}^i y^j)\} \Longrightarrow$

eval

$\mathsf{Enc}_{\mathsf{pk}}(r_1 \cdot F(\hat{x}, y)),$

$\mathsf{Enc}_{\mathsf{pk}}(r_2 \cdot F(\hat{x}, y) + G(\hat{x}, y))$

π $\hat{\pi}$

$\hat{\pi}$ verifies

where

$\hat{x} = \alpha x + \beta$

Use CH20 to prove consistency of update/eval

ia.cr/2023/1787

Open Questions

Limits of malleability:

- Which languages are blinding compatible?
    * All algebraic? Can we show a universal transformation?
- Restricted malleability:
    * Can we "block" certain transformations?

Open Questions

Limits of malleability:

- Which languages are blinding compatible?
    * All algebraic? Can we show a universal transformation?
- Restricted malleability:
    * Can we "block" certain transformations?

Applications:

- Updatable Blueprints:
    * Fast prover for bigger polynomials?
    * Logarithmic size?
- Polynomial commitment schemes?
- Graph statistics & MPC?

Thank you!

Questions?

Proof-Carrying Data from Arithmetized Random Oracles

Megan Chen

Boston University

Edinburgh lightning talk
September 4, 2024

Based on joint work with Alessandro Chiesa, Tom Gur, Jack O'Connor, Nicholas Spooner

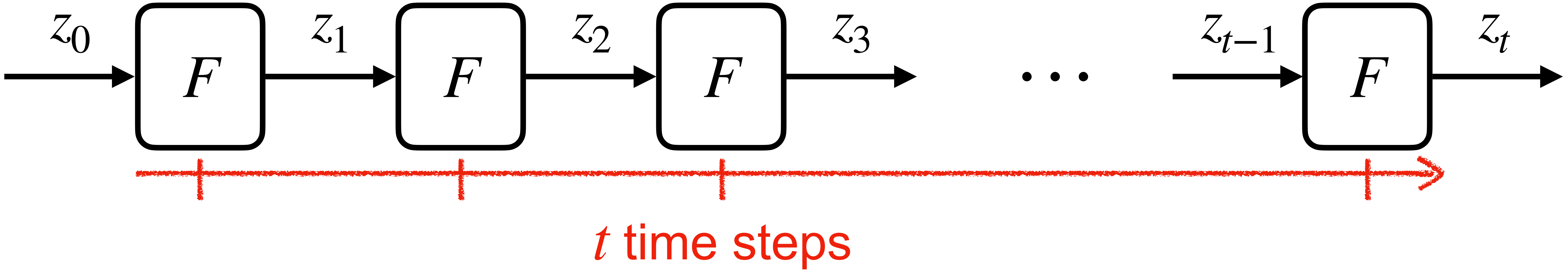
A long time ago…

(in a galaxy far, far away…)

someone started a computation that continues running today.

But… how do we check that the computation is correct?

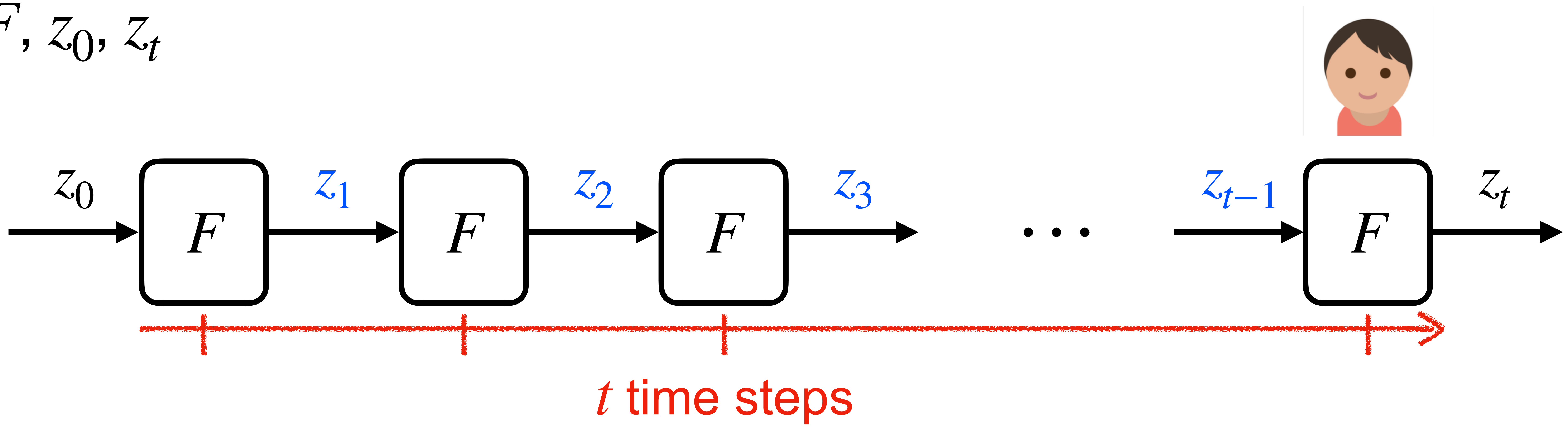
Setting: Streaming computation



Motivation: Verifying streaming computation

Goal: check correctness of a t-step computation.

Given: F, z_0, z_t



Verify: there exists messages

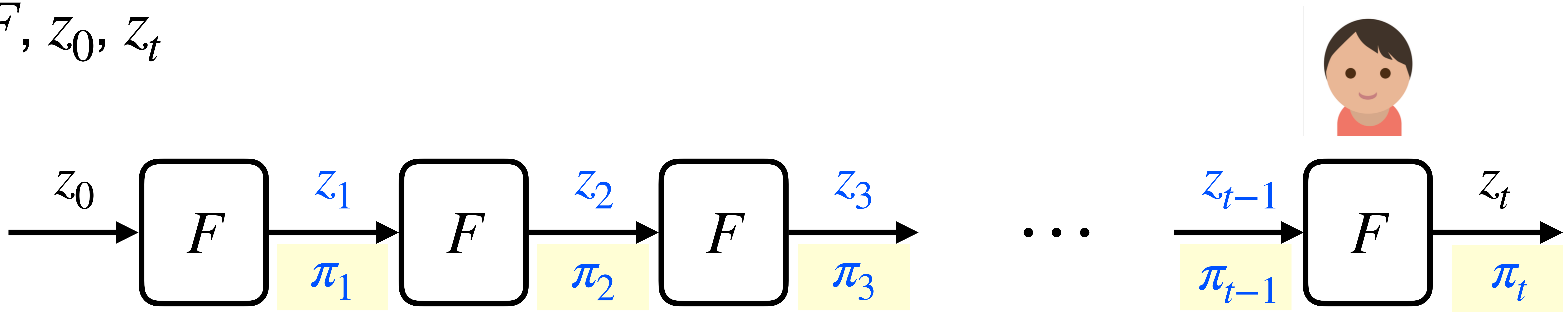
$z_1, \ldots, z_{t-1}$ such that

$F(z_i) = z_{i+1}$ at each step $i \in [t]$.

Motivation: Verifying streaming computation

Goal: check correctness of a t-step computation.

Given: F, z_0, z_t



Verify: there exists messages $z_1, \ldots, z_{t-1}$ such that $F(z_i) = z_{i+1}$ at each step $i \in [t]$.

Incrementally verifiable computation (IVC) [Valiant 08]: Augment each message with a proof.

Proof-carrying data (PCD) [CT10, BCCT13]: Generalize from path graph to DAG.

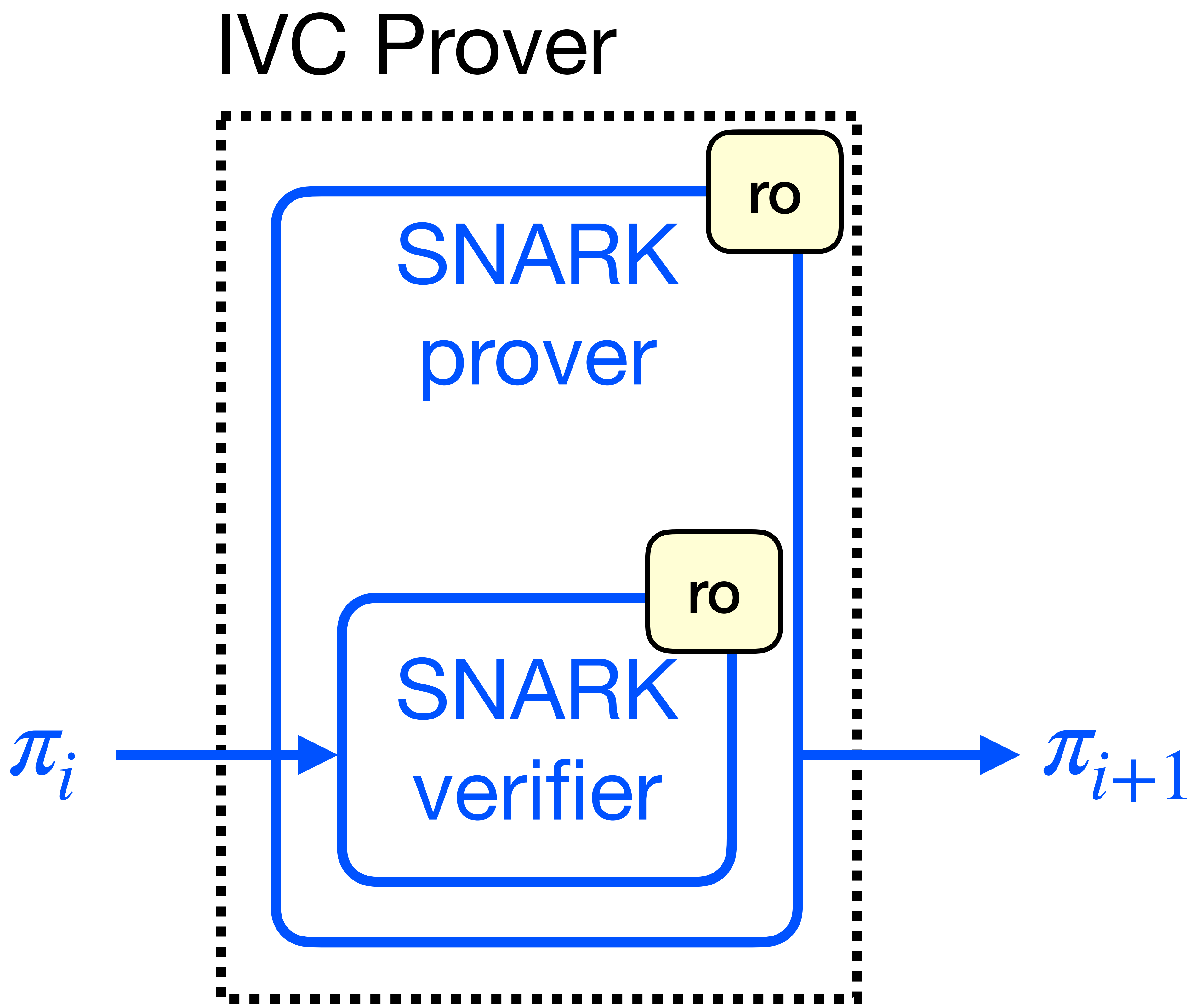
Applications of IVC / PCD

Verifying:

1. **Long-running computations**
    - Verifiable delay functions [BBBF19]
    - Succinct blockchains: Mina (https://minaprotocol.com)
2. **Distributed computations**
    - Zero-knowledge cluster computing
    - MapReduce

Constructing IVC from SNARKs [CT10, BCCT13]

This work: Can we get IVC from SNARKs in the ROM?



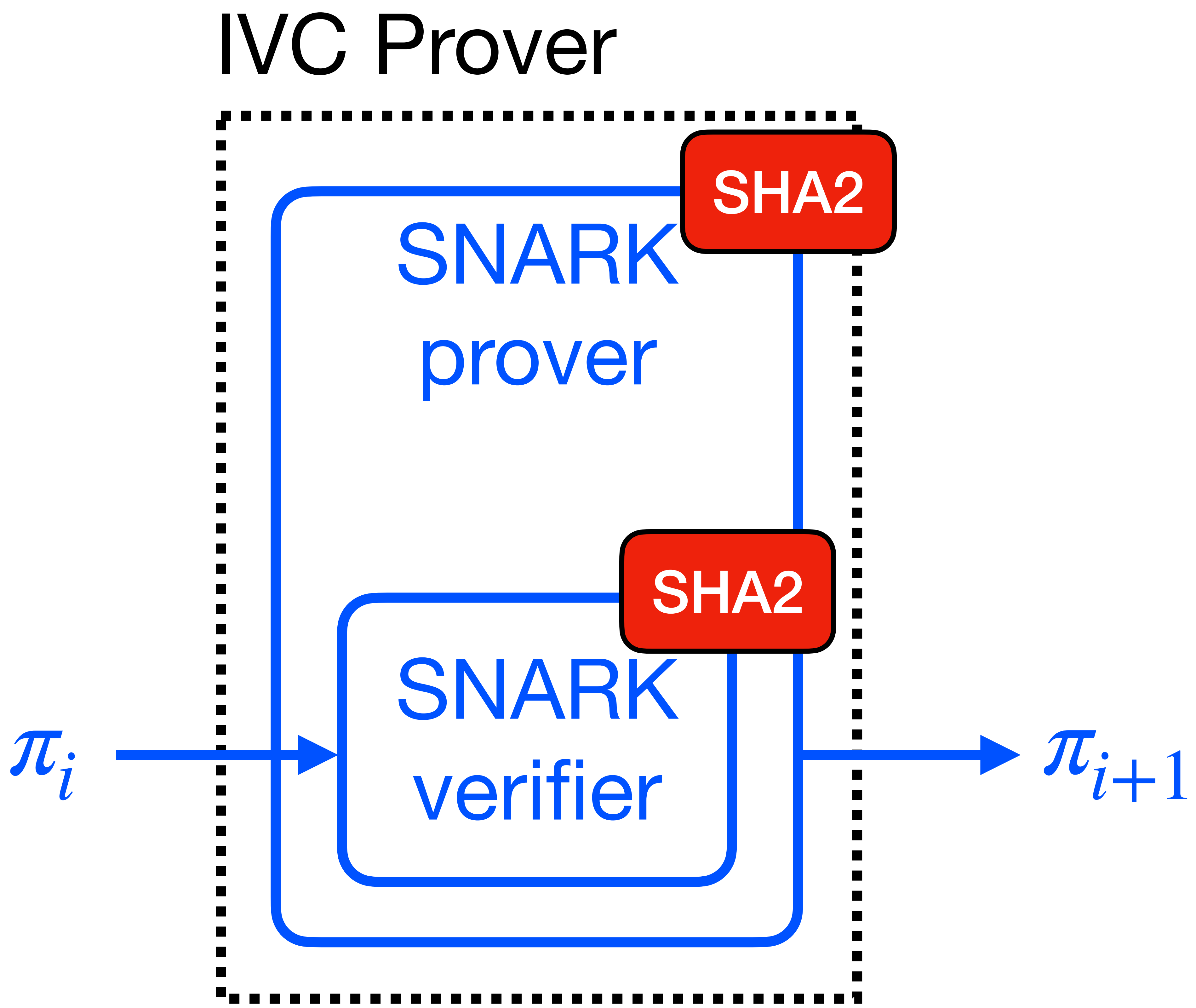
SNARK = succinct non-interactive arguments of knowledge

Recursive composition:

The SNARK prover proves that the SNARK verifier accepts.

Problem: SNARK verifier makes oracle queries, but SNARKs prove **non-oracle** (circuit) computations!

Constructing IVC from SNARKs [CT10, BCCT13]



SNARK = succinct non-interactive arguments of knowledge

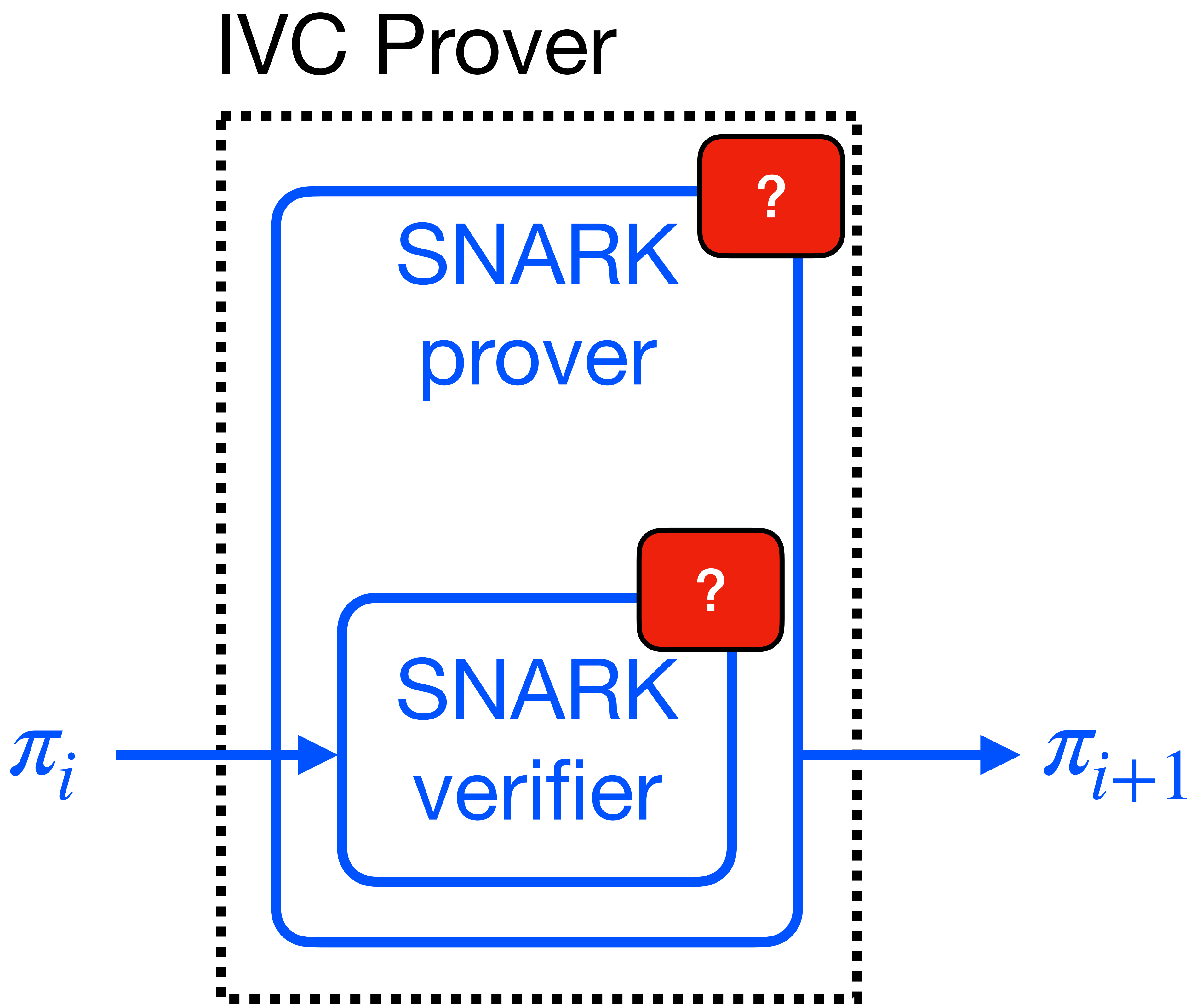
[ChiesaOS20] **Heuristically** instantiate RO with a hash circuit.

Downsides:

- **Theory**: SNARK and IVC security proofs are in different models.
- **Practical:** SNARKs of hash functions are expensive!

[CT10, CCS22]: Defined oracle models addressing these concerns, but **no efficient (software-only) instantiations of oracle.**

Research question



Does there exist an oracle model for which:

Can "accumulate" oracle queries and batch verify

1. There exists IVC in this oracle model under standard (cryptographic) assumptions; and

2. The oracle can be heuristically-instantiated in software?

Our result: **YES!**

Contributions:

We propose the **arithmetized random oracle model (AROM).**

Before: Low-degree ROM [CCS22]

- Uses **random low-degree polynomial structure**, for accumulation and batched verification of AROM queries.
- Infeasible to (heuristically) instantiate.

➡ Arithmetizing a hash circuit H gate-by-gate gives a polynomial of degree $>2^{\mathrm{depth}(H)}$.

$(25 \leq \mathrm{depth}(H) \leq 3000)$

Reduce depth of H with Cook-Levin CSAT to 3CNF reduction?

Cook-Levin is **non-blackbox** in H.

The AROM

- Uses **random low-degree polynomial structure**, for accumulation and batched verification of AROM queries.
- **Models applying non-blackbox operations** to (real world) hash circuits.

See paper for details!

Contributions:

We propose the arithmetized random oracle model (AROM).

- ✅ Construct transparent ZK IVC/PCD in the AROM, assuming CRH in the standard model.
- ✅ Theorem: security in the ROM implies security in the AROM.

Thanks!

Me: https://meganchen.xyz

Paper: https://ia.cr/2023/587

Exploring the Interplay of Cryptographic Accumulators and Zero-Knowledge Proofs

Anaïs Barthoulot

University of Montpellier, LIRMM

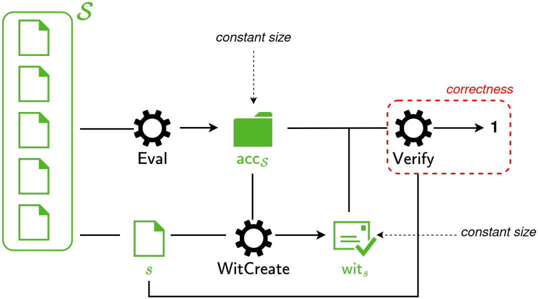
Foundations and Applications of Zero-Knowledge Proofs

4th September 2024

(Asymmetric) Cryptographic Accumulators

Definition (simplified) [1] [2]

- $\mathsf{Setup}(\lambda) \rightarrow \mathsf{pk}, \mathsf{sk}$
- $\mathsf{Eval}(\mathsf{pk}, (\mathsf{sk},)\ \mathcal{S}) \rightarrow \mathsf{acc}_{\mathcal{S}}$
- $\mathsf{WitCreate}(\mathsf{pk}, (\mathsf{sk},)\ \mathsf{acc}_{\mathcal{S}}, \mathcal{S}, s) \rightarrow \mathsf{wit}_s$
- $\mathsf{Verify}(\mathsf{pk}, \mathsf{acc}_{\mathcal{S}}, s, \mathsf{wit}_s) \rightarrow 0/1$



[1] One-way accumulators: A decentralized alternative to digital signatures, Benaloh and de Mare,EUROCRYPT 1993

[2] Revisiting Cryptographic Accumulators, Additional Properties and Relations to other Primitives, Derler, Hanser, and Slamanig CT-RSA 2015

Accumulator Security Properties

In Brief

- Lots of properties such as

Accumulator Security Properties

In Brief

- Lots of properties such as *zero-knowledge*

Accumulator Security Properties

In Brief

- Lots of properties such as *zero-knowledge* $\neq$ **zero-knowledge proofs of knowledge**

Accumulator Security Properties

In Brief

- Lots of properties such as *zero-knowledge* $\neq$ **zero-knowledge proofs of knowledge**

Zero-knowledge accumulator

- Accumulated value and witnesses leak *nothing* about the underlying set, not even the size of the set

Accumulator Security Properties

In Brief

- Lots of properties such as *zero-knowledge* $\neq$ **zero-knowledge proofs of knowledge**

Zero-knowledge accumulator

- Accumulated value and witnesses leak *nothing* about the underlying set, not even the size of the set

$\rightarrow$ **Not considered in this talk**

Accumulator Security Properties

In Brief

- Lots of properties such as *zero-knowledge* $\neq$ **zero-knowledge proofs of knowledge**

Zero-knowledge accumulator

- Accumulated value and witnesses leak *nothing* about the underlying set, not even the size of the set

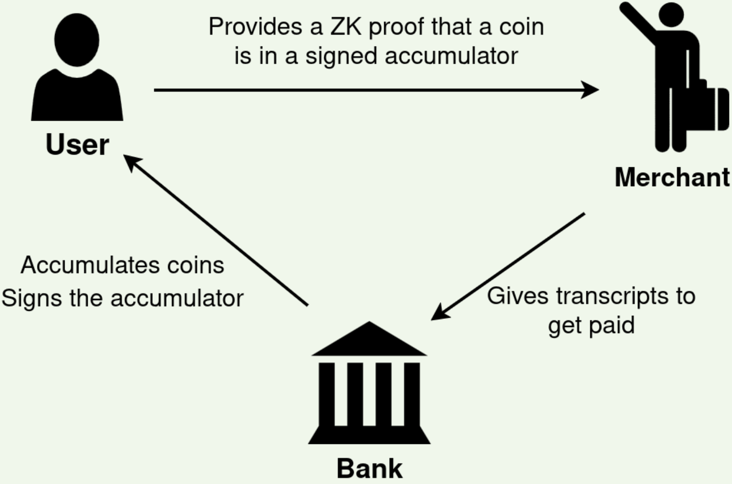
$\longrightarrow$ **Not considered in this talk**

Accumulator with **zero-knowledge proofs of knowledge**

- Prove membership of an element, while keeping the element hidden

Accumulators and ZK Proofs: Example of Application

E-Cash



Other applications: anonymous credentials, ...

Interplay of Accumulators and ZK Proofs

- **Efficiently Provable**: combined with a commitment scheme
  example: RSA-based accumulators and Pedersen commitments[3]

[3] Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials, Camenisch and Lysyanskaya, Crypto 2002

Interplay of Accumulators and ZK Proofs

- **Efficiently Provable**: combined with a commitment scheme
  example: RSA-based accumulators and Pedersen commitments[3]
- **SNARK-friendly**: verification done with (zk) SNARKs
  example: Merkle trees, RSA-based accumulators [4]

[3] Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials, Camenisch and Lysyanskaya, Crypto 2002

[4] Scaling Verifiable Computation Using Efficient Set Accumulators, Ozdemir, Wahby, Whitehat, Boneh, SEC 2020

Interplay of Accumulators and ZK Proofs

- **Efficiently Provable**: combined with a commitment scheme
  example: RSA-based accumulators and Pedersen commitments[3]

- **SNARK-friendly**: verification done with (zk) SNARKs
  example: Merkle trees, RSA-based accumulators [4]

- **Determinantal Accumulators**: designed to construct special NIZK proofs [5]

[3] Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials, Camenisch and Lysyanskaya, Crypto 2002

[4] Scaling Verifiable Computation Using Efficient Set Accumulators, Ozdemir, Wahby, Whitehat, Boneh, SEC 2020

[5] Set (Non-)Membership NIZKs from Determinantal Accumulators, Lipmaa and Parisella, Latincrypt 2023

Key Takeaways

- **Combining ZK Proofs and Accumulators**
  - Enhances privacy of accumulators
  - Applied in E-Cash, anonymous credentials, and blockchain technologies

Active Research Area

How (Not) to Simulate PLONK

https://ia.cr/2024/848

Marek Sefranek
TU Wien

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

PLONK

- State-of-the-art zk-SNARK by Gabizon, Williamson & Ciobotaru [GWC19]
- A proof is ≈0.5 kB and can be verified in milliseconds
- Universal & updatable structured reference string (SRS)
- Knowledge sound in AGM + ROM (or just ROM [LPS24])
- Supports custom gates and lookup gates
- Deployed in a variety of real-world projects

Aztec polygon Espresso Matter Labs DUSK

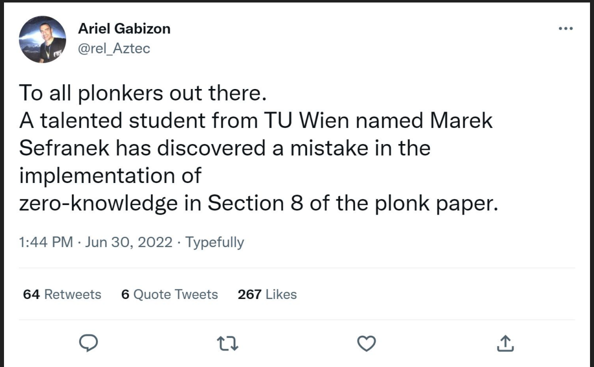
TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Main Contribution

- But no proof that PLONK is zero-knowledge!

Main Contribution

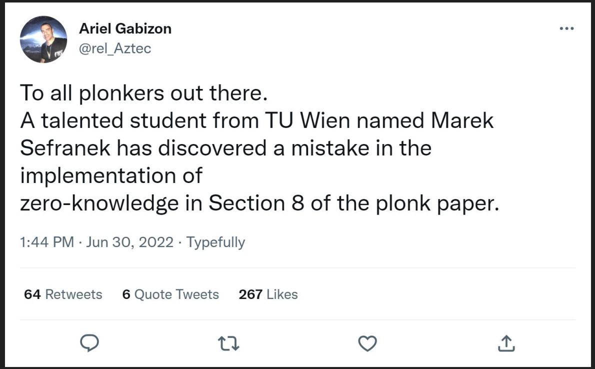
- But no proof that PLONK is zero-knowledge!
- Found vulnerability in its ZK implementation & proposed fix



TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Main Contribution

- But no proof that PLONK is zero-knowledge!
- Found vulnerability in its ZK implementation & proposed fix


Ariel Gabizon
@rel_Aztec

To all plonkers out there.
A talented student from TU Wien named Marek Sefranek has discovered a mistake in the implementation of
zero-knowledge in Section 8 of the plonk paper.

1:44 PM · Jun 30, 2022 · Typefully

64 Retweets 6 Quote Tweets 267 Likes

- Formal security proof that it now achieves statistical ZK

PLONK – Simplified Overview

- For $Z(X) := (X - \omega^1)(X - \omega^2)\cdots(X - \omega^n)$, want to show $Z(X) \mid C(X)$

PLONK – Simplified Overview

- For $Z(X) := (X - \omega^1)(X - \omega^2)\cdots(X - \omega^n)$, want to show $Z(X) \mid C(X)$
- Prover commits to $C(X)$ and quotient polynomial $T(X)$ [KZG10]

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

PLONK – Simplified Overview

- For $Z(X) := (X - \omega^1)(X - \omega^2)\cdots(X - \omega^n)$, want to show $Z(X) \mid C(X)$
- Prover commits to $C(X)$ and quotient polynomial $T(X)$ [KZG10]
- Its degree is $3n$, where n is the number of gates

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

PLONK – Simplified Overview

- For $Z(X) := (X - \omega^1)(X - \omega^2)\cdots(X - \omega^n)$, want to show $Z(X) \mid C(X)$
- Prover commits to $C(X)$ and quotient polynomial $T(X)$ [KZG10]
- Its degree is $3n$, where n is the number of gates
- Other polynomials have degree $n \implies$ SRS has to be 3x as long

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

PLONK – Simplified Overview

- For $Z(X) := (X - \omega^1)(X - \omega^2)\cdots(X - \omega^n)$, want to show $Z(X) \mid C(X)$
- Prover commits to $C(X)$ and quotient polynomial $T(X)$ [KZG10]
- Its degree is $3n$, where n is the number of gates
- Other polynomials have degree $n \Longrightarrow$ SRS has to be 3x as long
- To avoid this, PLONK splits T into 3 degree-n polynomials T_1, T_2, T_3 s.t.

$$T(X) = T_1(X) + X^n\, T_2(X) + X^{2n}\, T_3(X)$$

Zero Knowledge Vulnerability

- Without splitting $T(X)$:
  - Can be simulated as $T(\tau)$ can be computed given the KZG trapdoor τ
  - Proof independent of witness

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Zero Knowledge Vulnerability

- Without splitting $T(X)$:
  - Can be simulated as $T(\tau)$ can be computed given the KZG trapdoor τ
  - Proof independent of witness
- With the optimization:
  - T_1, T_2, T_3 leak too much information about $T(X)$
  - Proof no longer independent of witness!

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

Zero Knowledge Fix

- Randomize T_1, T_2, T_3 so they are uniform conditioned on satisfying

$$T(X) = T_1(X) \quad + X^n \, T_2(X) \quad + X^{2n} \, T_3(X)$$

Zero Knowledge Fix

- Randomize T_1, T_2, T_3 so they are uniform conditioned on satisfying

$$T(X) = T_1(X) + r_1 X^n + X^n (T_2(X) - r_1 \quad) + X^{2n} \; T_3(X)$$

for randomly chosen $r_1 \quad \in \mathbb{F}$

Zero Knowledge Fix

- Randomize T_1, T_2, T_3 so they are uniform conditioned on satisfying

$$T(X) = T_1(X) + r_1 X^n + X^n (T_2(X) - r_1 + r_2 X^n) + X^{2n} (T_3(X) - r_2)$$

for randomly chosen $r_1, r_2 \in \mathbb{F}$

Zero Knowledge Fix

- Randomize T_1, T_2, T_3 so they are uniform conditioned on satisfying

$$T(X) = T_1(X) + r_1 X^n + X^n (T_2(X) - r_1 + r_2 X^n) + X^{2n} (T_3(X) - r_2)$$

for randomly chosen $r_1, r_2 \in \mathbb{F}$

Zero Knowledge Fix

- Randomize T_1, T_2, T_3 so they are uniform conditioned on satisfying

$$T(X) = T_1(X) + r_1 X^n + X^n (T_2(X) - r_1 + r_2 X^n) + X^{2n} (T_3(X) - r_2)$$

  for randomly chosen $r_1, r_2 \in \mathbb{F}$

- Can now be simulated as the value $T(\tau)$ can be:
  1. Choose uniform values for $T_2(\tau)$ and $T_3(\tau)$
  2. Set $T_1(\tau) := T(\tau) - \tau^n T_2(\tau) - \tau^{2n} T_3(\tau)$

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

More in the Full Paper…

- Proof of statistical zero knowledge in the ROM
- Unbounded attack on witness indistinguishability of previous PLONK

https://ia.cr/2024/848

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

More in the Full Paper…

- Proof of statistical zero knowledge in the ROM
- Unbounded attack on witness indistinguishability of previous PLONK

https://ia.cr/2024/848

Thanks!

Questions?

TU WIEN CYSEC CYBERSECURITYCENTER S&P Security & Privacy

References

[GWC19] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge. Cryptology ePrint Archive, Paper 2019/953, 2019. https://eprint.iacr.org/2019/953.

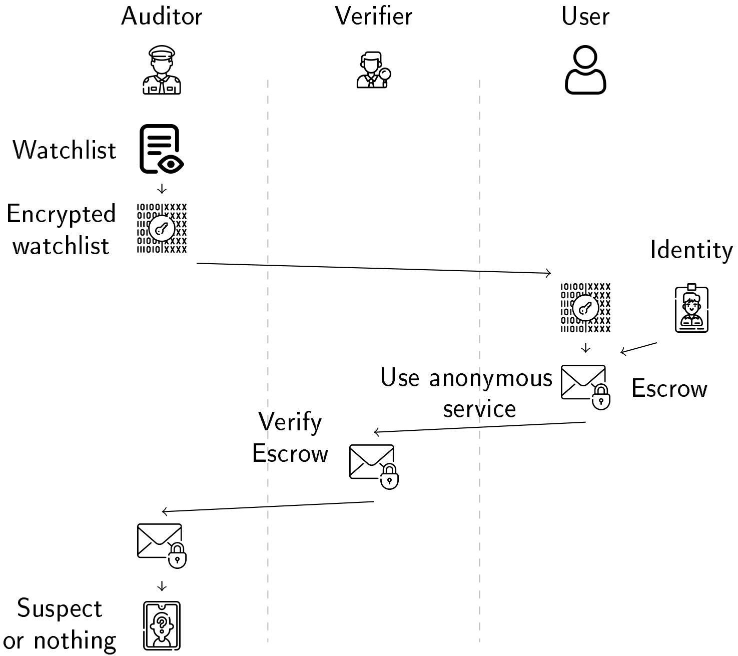
[KZG10] Aniket Kate, Gregory M. Zaverucha, and Ian Goldberg. Constant-Size Commitments to Polynomials and Their Applications. In Advances in Cryptology – ASIACRYPT 2010, volume 6477 of LNCS, pages 177–194. Springer, 2010. https://doi.org/10.1007/978-3-642-17373-8_11.

[LPS24] Helger Lipmaa, Roberto Parisella, and Janno Siim. On Knowledge-Soundness of Plonk in ROM from Falsifiable Assumptions. Cryptology ePrint Archive, Paper 2024/994, 2024. https://eprint.iacr.org/2024/994.

Privacy-Preserving Blueprints via Succinctly Verifiable Computation over Additively-Homomorphically Encrypted Data

Scott Griffy[1], Markulf Kohlweiss[2], Anna Lysyanskaya[1], and Meghna Sengupta[3]

[1]Brown University, [2]University of Edinburgh and IOG, [3]University of Edinburgh


Auditor
Verifier
User
Watchlist
Encrypted watchlist
Identity
Use anonymous service
Escrow
Verify Escrow
Suspect or nothing

Contributions

Compared to [KLN23]:

- Definition for non-framing (auditors cannot frame users)
- Larger message space for escrows
- Logarithmic escrows (as opposed to linear) and additive-ciphertext framework

Logarithmic escrow proofs

Our paper [GKLS24] uses the Schwartz-Zippel lemma, similar to [Sha90, GKR08, Pie19, HHKP23] but applied to encryptions which requires *commitments to additively-homomorphic encryptions* (new primitive).

Polynomial which represents the watchlist: $P(X)$.
Encrypted coefficients of polynomial: $\forall i \in [n], c_i = \mathsf{Enc}(P_i)$
Want to prove correct encryption (c_y) of $P(y)$
(y is the user's identity, the verifier has only a commitment to y)

Naively we'd prove directly: $c_y = \prod_{i=0}^{n-1} c_i^{y^i}$

Instead, compute: $c'_y = \prod_{i=0}^{n/2-1} c_i^{y^i} \quad c^*_y = \prod_{i=n/2}^{n-1} c_i^{y^{i-n/2}}$

and prove: $c^\dagger_y = c'_y + (c^*_y)^\alpha$ where α is a challenge from the verifier.

Scott Griffy, Markulf Kohlweiss, Anna Lysyanskaya, and Meghna Sengupta.
Privacy-preserving blueprints via succinctly verifiable computation over additively-homomorphically encrypted data.
Cryptology ePrint Archive, Paper 2024/675, 2024.

Shafi Goldwasser, Yael Tauman Kalai, and Guy N. Rothblum.
Delegating computation: interactive proofs for muggles.
pages 113–122, 2008.

Charlotte Hoffmann, Pavel Hubácek, Chethan Kamath, and Krzysztof Pietrzak.
Certifying giant nonprimes.
pages 530–553, 2023.

Markulf Kohlweiss, Anna Lysyanskaya, and An Nguyen.
Privacy-preserving blueprints.
pages 594–625, 2023.

Krzysztof Pietrzak.
Simple verifiable delay functions.

pages 60:1–60:15, 2019.

Adi Shamir.
IP=PSPACE.
pages 11–15, 1990.

Icons from freepik and flaticon

EU Chat Control and Client-Side Scanning

Markulf Kohlweiss, Lorenzo Martinico, Mikhail Volkhov

Edinburgh, September 2024

What is Chat Control (v2)

- Formally: EU's Child Sexual Abuse Regulation (CSA or CSAR)
  - Proposed by the European Commission in May 2022
  - V1 (passed 2021) allows services to voluntarily scan messages. V2 would make this mandatory.
- In other countries:
  - 🇦🇺 Online Safety Act (2021), data encryption law (2018).
    - "The laws of mathematics are very commendable, but the only law that applies in Australia is the law of Australia," - Malcolm Turnball, Prime Minister of Australia
  - 🇬🇧 UK: Online safety act (passed 2023), requires in principle E2EE backdoors (not implemented, Ofcom does not approve tech).
  - 🇨🇳 China: Telegram/Whatsapp/Signal/Threads are banned from chinese app stores April 2024. 🇷🇺 Russia: Signal banned August 2024. 🇫🇷 France: Durov arrested August 2024.
    - More on https://freedomhouse.org/report/freedom-net

History of Chat Control

- Academic open letter: July 2023, 300+ signatures. ↗️

Australia
Dr. Shaanan Cohney — University of Melbourne
Prof. Vanessa Teague — Australian / Thinking C

Austria
Prof. Dr. Elena Andreeva — TU Wien
Univ.-Prof. Dr. Rainer Böhme — Universitä
Prof. Maria Eichlseder — TU Graz
Prof. Daniel Gruss — TU Graz
Prof. Dr. Martina Lindorfer — TU Wien
Univ.-Prof. Dr. Matteo Maffei — TU Wien
Prof. Stefan Mangard — TU Graz
Univ.-Prof. Dr. René Mayrhofer — Johannes
Prof. Elisabeth Oswald — University
Univ.-Prof. Dr. Christian Rechberger — TU Graz
Dr. Michael Roland — Johannes
Univ.-Prof. Edgar Weippl — University

Belgium
Prof. Dr. Rosamunde van Brakel — Vrije Unive
Prof. Claudia Diaz — KU Leuven
Prof. Dr. Gloria González Fuster — Vrije Unive
Prof. Dr. Joris van Hoboken — University
Prof. Olivier Pereira — UCLouvai
Prof. Thomas Peters — UCLouvai
Prof. Bart Preneel — KU Leuver
Prof. François-Xavier Standaert — UCLouvai
Prof. Florentin Rochet — University
Prof. Nigel Smart — KU Leuve
Prof. Mathy Vanhoef — KU Leuve
Prof. Ingrid Verbauwhede — KU Leuve

Brazil
Prof. Ian Brown — Centre for
Prof. Alexandre Augusto Giron — Federal U
Dr. Jean Martina — U
Prof. Dr. Marcos Antonio Simplicio Jr — Universida

Canada
Prof. Ian Goldberg — University
Prof. Florian Kerschbaum — University
Prof. David Lie — University
Prof. Nicolas Papernot — University

Czechia
Dr. Vit Bukac — Masaryk U
Prof. Vashek Matyas — M
Prof. Kamil Malinka — Br
Dr. Petr Svenda — M
Dr. Martin Ukrop

Denmark
Prof. Diego F. Aranha — Aa
Prof. Carsten Baum — Te
Prof. Joan Boyar — Ur
Prof. Ivan Damgård — Aa
Dr. Christian Majenz — Te
Prof. Claudio Orlandi — Aa
Prof. Luisa Siniscalchi — Te
Prof. Tyge Tiessen — Te
Prof. Dr. Emmanouil Vasilomanolakis — Te

Estonia
Dr. Dan Bogdanov — Pe

Finland
Prof. Kimmo Halunen — Ur

France
Dr. Daniele Antonioli — EU
Dr. Gustavo Banegas — In
Mr. Karthikeyan Bhargavan — Cr
Dr. Bruno Blanchet — In
Prof. Olivier Blazy — Éc
Prof. Christina Boura — Ur
Dr. Anne Canteaut — In
Dr. Veronique Cortier — Cr
Dr. Jannik Dreier
Prof. Antonio Faonio — EU
Dr. Caroline Fontaine — Cr
Dr. Aurélien Francillon — EU
Dr. Aymeric Fromherz — In
Prof. Pierrick Gaudry — Cr
Prof. Elham Kashefi — Cr
Dr. Steve Kremer — In
Dr. Gaëtan Leurent — In
Dr. Pierre Laperdrix — Cr
Dr. P. G. Macioti — M
Prof. Melek Önen — EU
Dr. Maria Naya Plasencia — In
Dir. Research Catuscia Palamidessi — In
Dr. Léo Perrin — In
Dr. Yann Rote — Ur
Dr. Emmanuel Thomé — In

Germany
Dr. Ali Abassi — Cl
Prof. Patricia Arias Cabarcos — Pa
Dr. Gilles Barthe
Dr. Sebastian Berndt — Ur
Dr. Asia Biega — Max Planck Institute for Security and Privacy
Prof. Dr. Kevin Borgolte — Ruhr University Bochum
Dr. Sven Bugiel — CISPA Helmholtz Center for Information Security
Dr. Rebekka Burkholz — CISPA Helmholtz Center for Information Security
Prof. Dr. Cas Cremers — CISPA Helmholtz Center for Information Security
Prof. Thomas Eisenbarth — University of Lübeck
Prof. Thorsten Holz — CISPA Helmholtz Center for Information Security
Prof. Tibor Jager — University of Wuppertal
Prof. Dr. Stefan Katzenbeisser — University of Passau
Dr. Dietmar Kammerer — Weizenbaum Institute for the Networked Society
Dr. Franziskus Kiefer — Cryspen
Dr. Katharina Krombholz — CISPA
Prof. Anja Lehmann — Hasso
Dr. Wouter Lueks — CISPA
Dr. Christian Mainka — Ruhr
Prof. Dr. Esfandiar Mohammadi — Univer
Dr. Veelasha Moonsamy — Ruhr
Prof. Dr. Andreas Peter — Univer
Dr. Giancarlo Pellegrino — CISPA
Prof. Joachim Posegga — Univer
Dr. Elissa Redmiles — Max P
Dipl. Ir. Rainer Rehak — Weize
Prof. Konrad Rieck — Techn
Prof. Paul Rösler — FAU E
Prof. Dr. Christian Rossow — CISPA
Prof. Dr. Sebastian Schinzel — Münst
Prof. Thomas Schneider — Techn
Prof. Dr. Dominique Schröder — Friedri
Dr. Peter Schwabe — Max P
Prof. Juraj Somorovsky — Pader
Dr. Ben Stock — CISPA
Prof. Thorsten Strufe — KAST / Centre
Prof. Florian Tschorsch — TU Be
Dr. Nils Ole Tippenhauer — CISPA
Prof. Christian Wressnegger — Karlsr
Prof. Dr. Yuval Yarom — Ruhr
Dr. Xiao Zhang — CISPA
Dr. Yixin Zou — Max P

Greece
Prof. Vasiliki Diamantopoulou — Univer
Prof. Christos Kalloniatis — Univer
Prof. Georgios Kambourakis — Univer
Prof. Costas Lambrinoudakis — Univer
Prof. Emmanouil Magkos — Ionian
Prof. Stefanos Gritzalis — Univer / Hellen

Ireland
Dr. TJ McIntyre — Univer
Dr. Stephen Farrell — Digital / Trinity

Israel
Prof. Orr Dunlekman — Univer
Dr. Yossi Oren — Ben-G
Dr. Eyal Ronen — Tel Av
Dr. Mahmood Sharif — Tel Av

Italy
Prof. Stefano Calzavara — Univer
Prof. Mauro Conti — Univer
Prof. Bruno Crispo — Univer
Prof. Paolo Falcarin — Univer
Prof. Fabio Massacci — University of
Prof. Giuseppe Persiano — Università di
Prof. Daniele Venturi — Sapienza Un
Prof. Stefano Zanero — Politecnico d

Liechtenstein
Prof. Giovanni Apruzzese — University of

Luxembourg
Prof. Dr. Gabriele Lenzini — University of
Prof. Peter Y A Ryan — University of

The Netherlands
Dr. Gunes Acar — Radboud Un
Prof. Dr. Lejla Batina — Radboud Un
Prof. Dr. ir. Herbert Bos — Vrije Univers
Dr. Corinne Cath — Delft Univers
Dr. Andrea Continella — University of
Prof. Joan Daemen — Radboud Un
Dr. Zekeriya Erkin — Delft Univers
Prof. Cristiano Giuffrida — Vrije Univers
Dr. Seda Gürses — Delft Univers
Prof. Jaap-Henk Hoepman — Radboud Un
Prof. Andreas Hülsing — Eindhoven U
Prof. Bart Jacobs — Radboud Un
Prof. Dr. Tanja Lange — Eindhoven U
Prof. Ot van Daalen — University of
Prof. Michel van Eeten — Delft Univers
Dr. Heloise Vieira — Eindhoven U
Prof. Ben Wagner — Delft Univers

New Zealand
Prof. Steven Galbraith — University of

Norway
Prof. Helger Lipmaa — Simula UiB

Poland
Prof. Stefan Dziembowski — University of
Dr. Anna Ratecka — Jagiellonian

Portugal
Ms. Sofia Celi — Brave
Prof. Manuel Eduardo Correia — University of
Prof. Manuel Barbosa — University of
Prof. Hugo Pacheco — University of
Prof. Bernardo Portela — University of
Prof. Henrique Santos — Universidade
Prof. Nuno Santos — INESC-ID an

Taiwan
Dr. Lorenz Panny — Academia Si

Turkey
Prof. Cihangir Tezcan — Middle East Technical University

United Arab Emirates
Prof. Michail Maniatakos — New York University Abu Dhabi
Prof. Chirstina Pöpper — New York University Abu Dhabi

United Kingdom
Dr. Ruba Abu-Salma — King's College London
Prof. Martin Albrecht — King's College London
Prof. Ross Anderson — Universities of Cambridge and Edinburgh
Prof. Reuben Binns — University of Oxford
Prof. Ioana Boureanu — University of Surrey
Dr. Jaya Klara Brekke — Nym Tech
Prof. Lorenzo Cavallaro — University
Dr. Michele Ciampi — University
Prof. Liqun Chen — University
Dr. Richard Clayton — University
Prof. Angela Daly — University
Dr. Partha Das Chowdhury — University
Dr. Benjamin Dowling — University
Dr. François Dupressoir — University
Dr. Tariq Elahi — University
Prof. Hamed Haddadi — Imperial C
Prof. Julio Hernandez-Castro — University
Dr. Alice Hutchings — University
Dr. Dennis Jackson — Mozilla
Dr. Rikke Jensen — Royal Holl
Prof. Adam Joinson — University
Dr. Philipp Jovanovic — University
Prof. Vasilis Katos — Bournemo
Prof. Aggelos Kiayias — University
Dr. Bernardo Magri — University
Prof. Corinne May-Chahal — University
Prof. Keith Martin — Royal Holl
Dr. Maryam Mehrnezhad — Royal Holl
Prof. Sarah Meiklejohn — University
Prof. Steven Murdoch — University
Prof. Douwe Korff — London M
Dr. Daniel Page — University
Dr. Claudia Peersman — University
Dr. Fabio Pierazzi — King's Col
Prof. Awais Rachid — University
Dr. Luc Rocher — University
Dr. Kaspar Rosager Ludvigsen — University
Dr. Christos Sagredos — King's Col
Dr. Siamak Shahandashti — University
Dr. Jose Tomas Llanos — University
Dr. Michael Veale — University
Dr. Niovi Vavoula — Queen Ma
Dr. Christian Weinert — Royal Holl
Prof. Alan Woodward — University

United States of America
Prof. Giuseppe Ateniese — George M
Prof. Adam J. Aviv — George W
Prof. Steven Bellovin — Columbia
Prof. Matt Blaze — Georgetow
Prof. Álvaro Cárdenas — University
Prof. Chandrasekaran — University
Prof. Nicolas Christin — Carnegie
Mr. Roger Dingledine — The Tor P
Prof. Zakir Durumeric — Stanford U
Dr. Kelsey Fulton — Colorado
Dr. Simson L. Garfinkel — Digital Co
Prof. Christina Garman — Purdue U
Prof. Matthew D. Green — Johns Hop
Prof. Daniel Genkin — Georgia Tech
Prof. Paul Grubbs — University of Michig
Dr. Joseph Lorenzo Hall — Internet Society
Dr. Britta Hale — Independent resear
Prof. Emeritus Martin Hellman — Stanford University
Prof. Nadia Heninger — University of Califor
Prof. Nicholas Hopper — University of Minne
Prof. Gabriel Kaptchuk — Boston University
Prof. Vasileios Kemerlis — Brown University
Dr. Jennifer King — Stanford University
Prof. Engin Kirda — Northeastern Unive
Prof. Susan Landau — Tufts University
Prof. Anna Lysyanskaya — Brown University
Prof. Abigail Marsh — Macalester College
Prof. Michelle Mazurek — University of Maryla
Prof. Ian Miers — University of Maryla
Prof. Prateek Mittal — Princeton University
Ms. Riana Pfefferkorn — Stanford University
Prof. Michalis Polychronakis — Stony Brook Univer
Dr. Niels Provos — Independent resear
Prof. Aanjhan Ranganathan — Northeastern Unive
Prof. Amir Rahmati — Stony Brook Univer
Prof. Franziska Roesner — University of Washi
Prof. Ronald L. Rivest — MIT
Dr. Sarah Scheffler — Princeton University
Prof. Barbara van Schewick — Stanford University
Prof. Bruce Schneier — Harvard Kennedy S
Prof. Adam Shostack — University of Washi
Nick Sullivan — Independent
Dr. Santiago Torres-Arias — Purdue University
Prof. Daniel Votipka — Tufts University
Prof. David Wagner — UC Berkeley
Prof. Daniel J. Weitzner — MIT
Dr. Lian Wang — Princeton University
Prof. Christo Wilson — Northeastern Unive
Prof. Matthew Wright — Rochester Institute

Singapore
Prof. Thomas Peyrin — Nanyang Technolog

South Korea
Prof. Sang Kil Cha — KAIST

Spain
Dr. Jorge Blasco Alis — Universidad Politéc
Prof. Pino Caballero-Gil — University of La Lag
Dr. Ignacio Cascudo — IMDEA Software Ins
Prof. Josep Domingo-Ferrer — Universitat Rovira i
Dr. Dario Fiore — IMDEA Software Ins
Dr. Gemma Galdon Clavell — Eticas Tech
Prof. Maribel González Vasco — Universidad Carlos
Dr. Marco Guarnieri — IMDEA Software Ins
Dr. Jordi Herrera-Joancomartí — Universitat Autònom
Prof. Llorenç Huguet — Balearic Island Univ
Dr. Guillermo Navarro-Arribas — Universitat Autònom
Prof. Fernando Pérez-González — University of Vigo
Dr. Cristina Perez-Sola — Universitat Autònom
Prof. Jose Such — Universitat Politècnica de València
Dr. Carla Ràfols — Universitat Pompeu Fabra
Prof. Josep Rifà — Universitat Autònoma de Barcelona
Prof. Juan Tapiador — Universidad Carlos III de Madrid
Dr. Narseo Vallina-Rodriguez — IMDEA Networks Institute

Sweden
Prof. Simone Fischer-Hübner — Karlstad University & Chalmers University of Technology
Prof. Dr.-Ing. Meiko Jensen — Karlstad University
Prof. Panos Papadimitratos — KTH Royal Institute of Technology — Fellow IEEE
Dr. Tobias Pulls — Karlstad University
Prof. Vicenç Torra — Umeå University — Fellow IEEE

Switzerland
Prof. Srdjan Capkun — ETH Zurich — Fellow IEEE
Prof. Bryan Ford — EPFL
Dr. Julia Hesse — IBM Zurich
Prof. Kenneth Paterson — ETH Zurich — Fellow IACR
Prof. Mathias Payer — EPFL
Dr. Apostolos Pyrgelis — EPFL
Dr. Raphael M. Reischuk — National Test Institute for Cybersecurity NTC
Prof. Shweta Shinde — ETH Zurich
Prof. Carmela Troncoso — EPFL

EDRi

History of Chat Control

- Academic open letter: July 2023, 300+ signatures. ↗️
- Parliament rejected some major provisions of the bill in November 2023
    - Security by design, cleaning the net proactively, removing known content.
    - Most EU governments continue to support the original chat control proposal of the EU Commission without significant compromises.

History of Chat Control

EDRi

- Academic open letter: July 2023, 300+ signatures. ↗️
- Parliament rejected some major provisions of the bill in November 2023
  - Security by design, cleaning the net proactively, removing known content.
  - Most EU governments continue to support the original chat control proposal of the EU Commission without significant compromises.
- ❎ Rejected by Council in June 20th 2024
  - Narrow minority: 63%/65% was achieved.
  - 4th different presidencies of the EU council (Belgium) failed to reach a compromise
  - Proposed changes included optional “upload moderation”: opt-out from E2EE scanning => no media sharing

History of Chat Control

EDRi

- Academic open letter: July 2023, 300+ signatures. ↗️
- Parliament rejected some major provisions of the bill in November 2023
  - Security by design, cleaning the net proactively, removing known content.
  - Most EU governments continue to support the original chat control proposal of the EU Commission without significant compromises.
- ❎ Rejected by Council in June 20th 2024
  - Narrow minority: 63%/65% was achieved.
  - 4th different presidencies of the EU council (Belgium) failed to reach a compromise
  - Proposed changes included optional “upload moderation”: opt-out from E2EE scanning => no media sharing
- ⚠️ Now revived by Hungary presidency with minimal changes
- If a majority is reached on the council, Trilogue negotiations will begin

What does the proposed law mandate

- Mandatory scanning of all messages for known or suspected** CSAM
  - All commercial communication services in scope, regardless of size, location, or **e2ee usage***
  - Not targeted to specific suspects*
  - Matches automatically reported to the police
  - Military and intelligence services' accounts are excluded (conjecture: politicians too?)
- "High risk" services require mandatory age controls (no user under 16 allowed)
- Mandatory detection of grooming behaviour**
- ISPs required to block access to illicit content*
- Creates Centre on Child Sexual Abuse as single point of contact for reporting

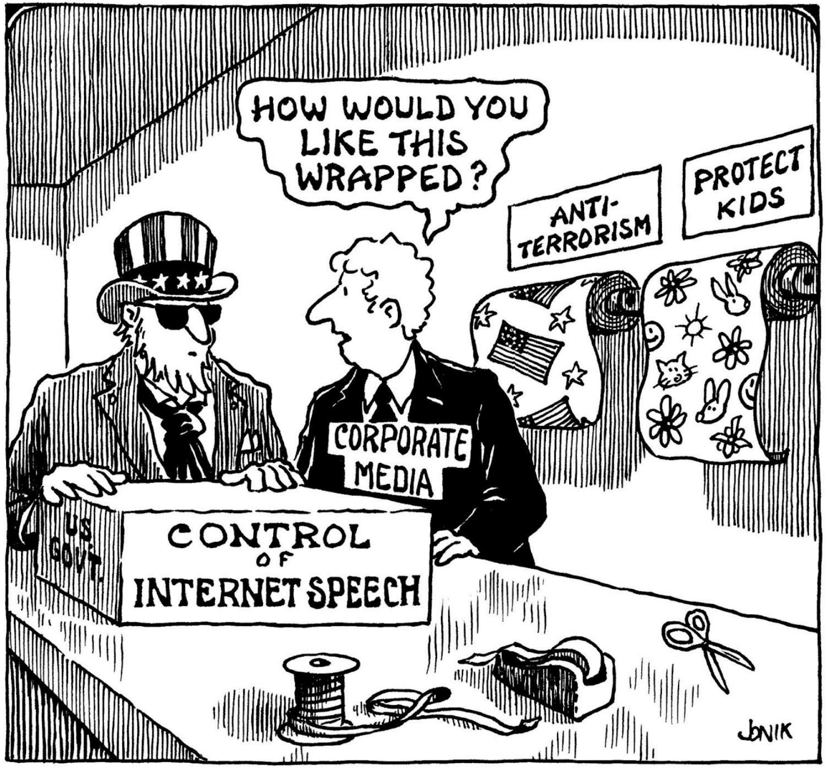
Motivation *for* Client-side Scanning

- Chat control-specific motivation: CSAM & grooming
- For CSS generally, EU included terrorism and organized crime as reasons.
  - Protecting the privacy and security of communications through encryption and at the same time upholding the possibility for competent authorities …to lawfully access relevant data … for fighting organized crimes and terrorism… are extremely important.

Council Resolution on Encryption – Security through encryption and security despite encryption (13084/1/20)

- Implicit / connected motivations:
  - Preventing / stopping "unwanted" political protests
  - Drug trade
  - Money Laundering, Fraud / Scams
  - Preventing hate crimes and harassment
  - Lobbying…

Motivation *for* Client-side Scanning



Against Chat Control & CSS

EDRI Position Paper
(best 3 page summary)

https://edri.org/wp-content/uploads/2022/10/EDRi-Position-Paper-CSAR-short.pdf

- Technical arguments
  - Soundness: no CSS method is working well. Evasion attacks.
  - Privacy: leaking models to client, revealing non-targeted content.
  - Security: false positive attacks, targeting people, larger attack surface.
  - Gives more power not only to authorised (gov), but also unauthorised (foreign govs), local (family abuse) advs.
- Legal/political arguments
  - Likely to be struck down by ECHR as incompatible with other European laws.
    - "The legislative proposal fails to meet the key human rights principles of necessity and proportionality, violates several fundamental rights, and lacks a sufficient legal basis."
  - Backsliding risks, discrimination/fairness (CSS & age verification), code origin/server origin/more power to companies.
  - Legitimate users are put are risk, including the population the law is trying to protect

Bugs in our Pockets: The Risks of Client-Side Scanning

Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Jon Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague, Carmela Troncoso

October 15, 2021

https://arxiv.org/abs/2110.07450

What can we do?

Scroll till this part ⤵️

Take action now

These are ideas for what you can do in the short-term or with some preparation. **Start with**:

- Ask you government to call on the European Commission to **withdraw the chat control proposal**. Point them to a joint letter that was recently sent by children's rights and digital rights groups from across Europe. Click here to find the letter and more information.
- Check your government's position (see above) and, if they voted in favour or abstained, ask them to explain why. **Tell them that as a citizen you want them to reject the proposal**, that chat control is widely criticised by experts and that none of the proposals tabled in the Council of the EU so far are acceptable. Ask them to protect the privacy of your communication and your IT security.
- **Share this call to action** online.

When reaching out to your government, the ministries of the interior (in the lead) of justice and of digitisation/telecommunications/economy are your best bet. You can additionally contact the permanent representation of your country with the EU.

Pressure on the negotiators + media attention + *harm reduction if law passes*

https://www.patrick-breyer.de/en/take-action-to-stop-chat-control-now/

Communities and Organisations

- We need forums for political action related to digital privacy…
    - **Among cryptographers** and other researchers

Are we going to wait for crypto's Manhattan project?

-
    - Interacting with policy-makers and general public
- Orgs to join / support financially:
    - EDRI: edri.org
    - Open Rights Group (UK): openrightsgroup.org
    - None Of Your Business: noyb.eu
    - Liberty: libertyhumanrights.org.uk

Learn More

Home reading ➡️

The Moral Character of Cryptographic Work*

Phillip Rogaway

Department of Computer Science
University of California, Davis, USA
rogaway@cs.ucdavis.edu

December 2015
(minor revisions March 2016)

Abstract. Cryptography rearranges power: it configures who can do what, from what. This makes cryptography an inherently *political* tool, and it confers on the field an intrinsically *moral* dimension. The Snowden revelations motivate a reassessment of the political and moral positioning of cryptography. They lead one to ask if our inability to effectively address mass surveillance constitutes a failure of our field. I believe that it does. I call for a community-wide effort to develop more effective means to resist mass surveillance. I plead for a reinvention of our disciplinary culture to attend not only to puzzles and math, but, also, to the societal implications of our work.

Keywords: cryptography · ethics · mass surveillance · privacy · Snowden · social responsibility

https://web.cs.ucdavis.edu/~rogaway/papers/moral-fn.pdf

Learn More

PATRICK BREYER
Digitaler Freiheitskämpfer

patrick-breyer.de/en/posts/chat-control/

Stop Scanning Me

stopscanningme.eu

EDRi
European Digital Rights

Statement on the future of the CSA Regulation

July 2024

https://edri.org/wp-content/uploads/2024/07/Statement_-The-future-of-the-CSA-Regulation.pdf