PlonK without random oracles

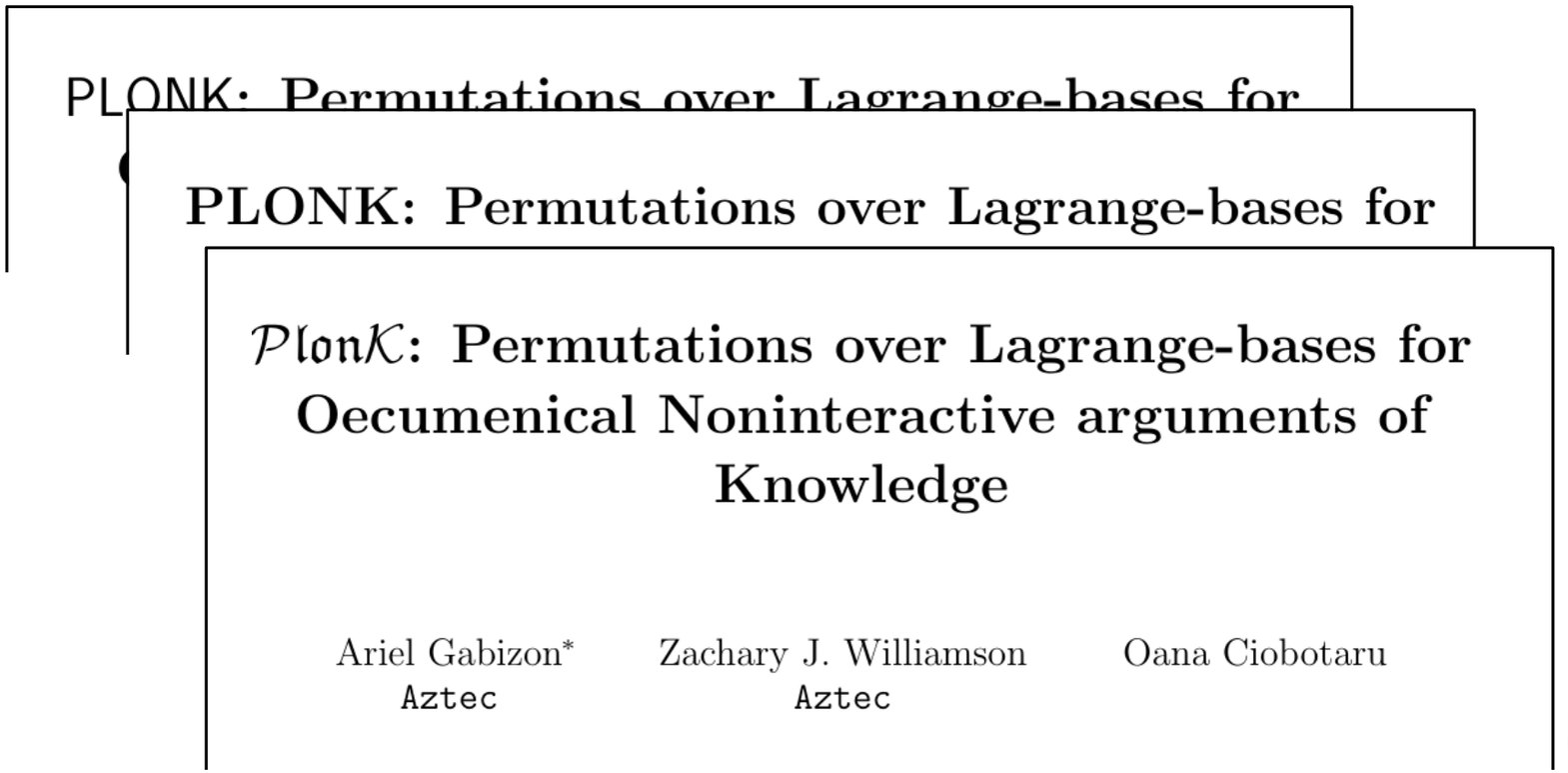
ia.cr/2026/200

Georg Fuchsbauer, joint work with **Marek Sefranek**

Wiener Wissenschafts-,
Forschungs- und Technologiefonds

Der Wissenschaftsfonds.

ZK↔SC Workshop
11 February 2026



Plonk is a zk-SNARK with

- constant-size proofs, sublinear verification time
- universal and updatable SRS

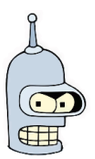
Knowledge soundness of $\mathcal{PlonK}$

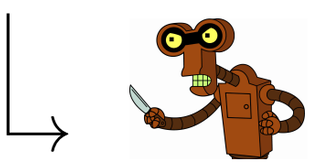
$\mathcal{PlonK}$: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge

Ariel Gabizon* Aztec
Zachary J. Williamson Aztec
Oana Ciobotaru

. . . under q-DLog
in the **AGM + ROM**

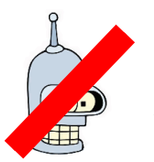
Algebraic group model (AGM) [FKL18]

$g_1, g_2, \ldots, g_q \rightarrow$  $\rightarrow \overline{g}$

 $\rightarrow \mathbf{c}$

with $\overline{g} = \prod g_i^{c_i}$

q-DLog in $\mathbb{G} = \langle g \rangle$

$g^{\tau}, \ldots, g^{\tau^q} \rightarrow$  $\rightarrow \tau$

Knowledge soundness of $\mathcal{PlonK}$

$\mathcal{PlonK}$: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge

Ariel Gabizon
Aztec

Can $\mathcal{PlonK}$ be proved secure **without random oracles**?

. . . under q-DLog in the **AGM** + **ROM**

On Knowledge-Soundness of Plonk in ROM from Falsifiable Assumptions

July 10, 2025

Helger Lipmaa[1], Roberto Parisella[2], and Janno Siim[1,2]

[1] University of Tartu, Tartu, Estonia
[2] Simula UiB, Bergen, Norway

Crypto 2025

. . . under q-{A | Split}RSDH in the **ROM**

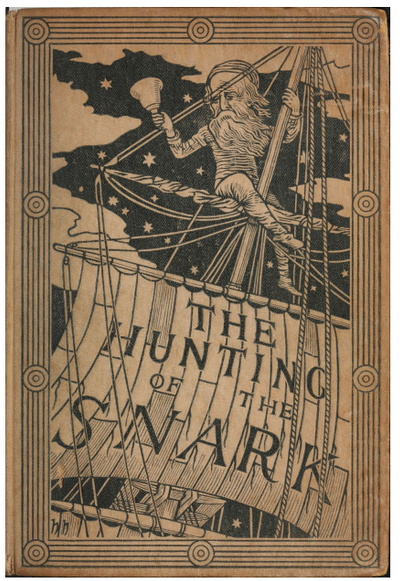
Recursive proof systems

Suppose we want to prove statements succinctly:

$$\underbrace{x_1 \quad \wedge \quad x_2 \quad \wedge \quad x_3 \quad \wedge \quad \ldots \quad \wedge \quad x_n}$$

$$\downarrow \quad \text{SNARK!}$$

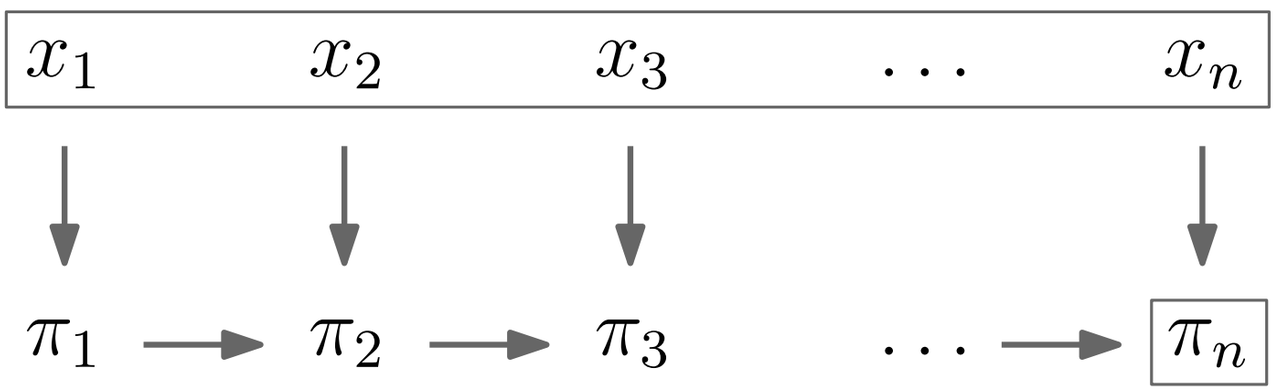
$$\pi$$



- Large circuit? (large parameters; long proving time . . .)
- If $x_i, x_{i+1}, \ldots$ not known yet? (“zk”-rollups,. . .)

Recursive proof systems

Suppose we want to prove statements succinctly:



Recursive proof! $\Rightarrow$

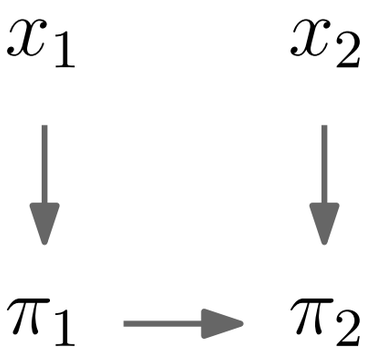
- incrementally verifiable computation
- proof-carrying data
- scalable rollups
- succinct blockchains (MINA)

Soundness / ROM

How to Prove False Statements: Practical Attacks on Fiat-Shamir

Dmitry Khovratovich* Ron D. Rothblum† Lev Soukhanov‡

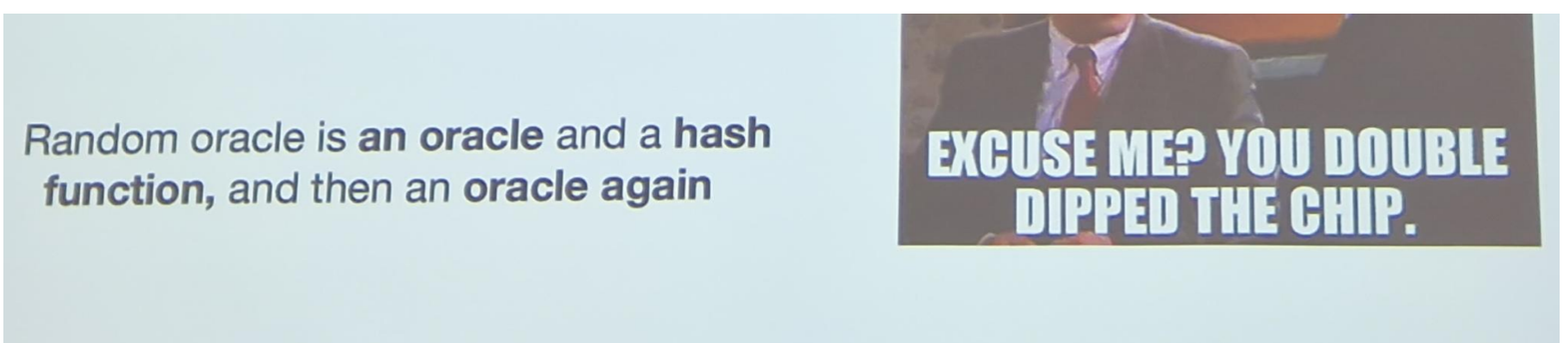
Crypto 2025



Statement: "*I know witness for* x_2 *and* π_1: $\mathsf{Verify}(x_1, \pi_1) = 1$"

SNARK secure in the **random oracle model** (ROM)

must use *real* H



Our work

Plonk Without Random Oracles

Georg Fuchsbauer and Marek Sefranek

TU Wien, Austria

ePrint 2026

$\mathcal{PlonK}$ is **knowledge-sound**

. . . in the **AGM**
under q-DLog
and zero-testing assumption

. . . and both assumptions
are necessary

$\mathcal{PlonK}$ is (comp.) **zero-knowledge**

. . . in the **standard** model
and zero-testing assumption

Our work

Plonk Without Random Oracles

Georg Fuchsbauer and Marek Sefranek

TU Wien, Austria

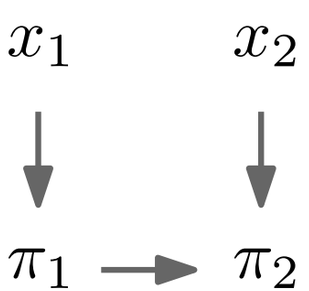
ePrint 2026

$\mathcal{PlonK}$ is **knowledge-sound**

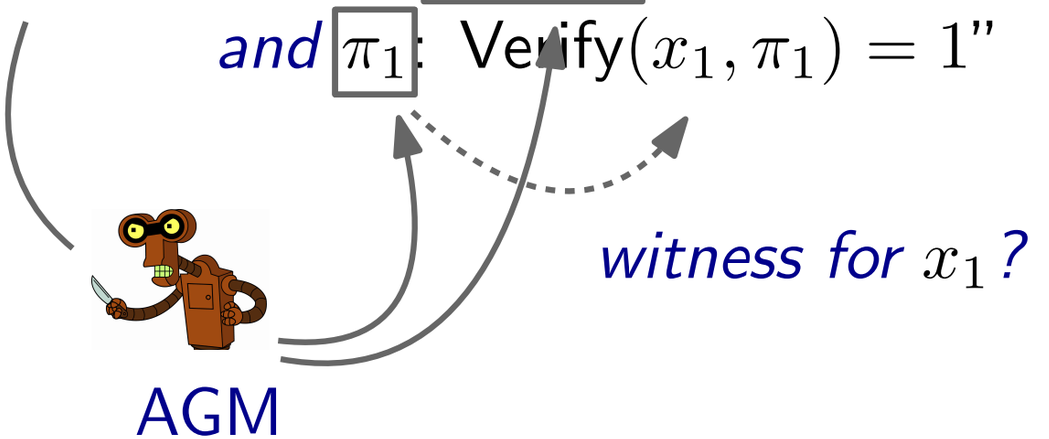
. . . in the **AGM**

under q-DLog

and zero-testing assumption



Recursive proof π_2 for "*I know witness for* x_2 *and* π_1: $\mathsf{Verify}(x_1, \pi_1) = 1$"



Recursive AGM

$\mathcal{PlonK}$ is **knowledge-sound**

. . . in the **AGM**

under q-DLog

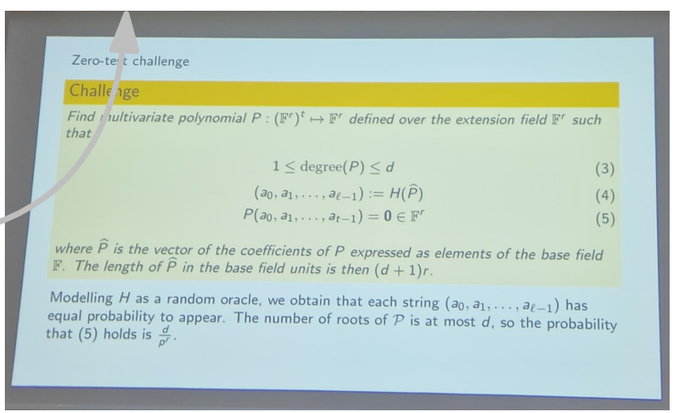
and zero-testing assumption

On the Security of Nova Recursive Proof System

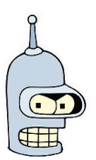
Hyeonbum Lee and Jae Hong Seo*

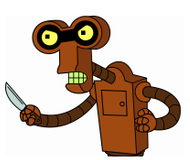
Department of Mathematics & Research Institute for Natural Sciences,
Hanyang University, Seoul 04763, Republic of Korea

ePrint 2024



Recursive AGM

$g_1, g_2, \ldots, g_q \rightarrow$  $\rightarrow \overline{g}$



$\rightarrow \mathbf{c}$ with $\overline{g} = \prod g_i^{c_i}$

If $(c_i, c_j) = g' \in \mathbb{G}$ $\rightarrow \mathbf{c}'$ with $g' = \prod g_i^{c'_i}$

If $(c'_{i'}, c'_{j'}) = g'' \in \mathbb{G}$ $\rightarrow \mathbf{c}''$ with $g'' = \prod g_i^{c''_i}$

The zero-testing assumption

Let $\mathbb{F}$ finite field, $H\colon \{0,1\}^* \to \mathbb{F}$ hash function

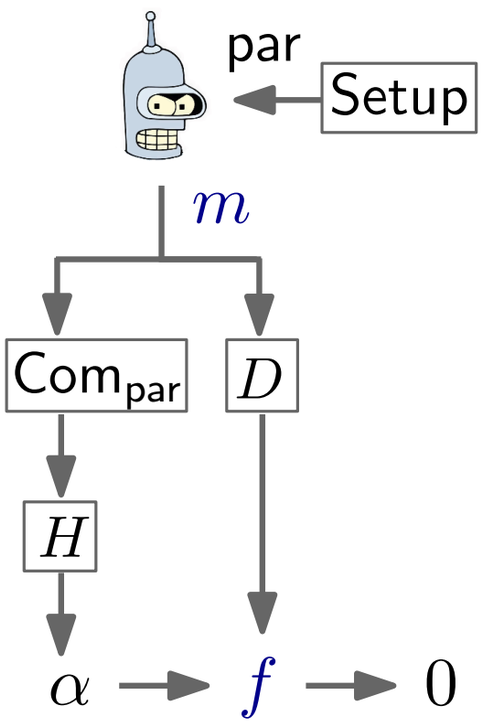
Simplification: "find polynomial $0 \not\equiv f \in \mathbb{F}^{(\leq d)}[X]$ such that $f(H(f)) = 0$"

Zero-testing.

- $H\colon \{0,1\}^* \to \mathbb{F}$
- (Setup,Com) a commitment scheme over $\mathcal{M}$
- $D\colon \mathcal{M} \to \mathbb{F}^{(\leq d)}[X]$

Given par $\leftarrow$ Setup, find m, s.t.

for $f := D(m)$:
- $f \not\equiv 0$
- $f\big(H(\mathsf{Com}_{\mathsf{par}}(m))\big) = 0$



Using ZT

I have polynomials f_1, f_2 s.t. $f_2 \equiv f_1^3$

P

V

- $\mathsf{cm}_i := \mathsf{Com}(f_i)$

$\mathsf{cm}_1, \mathsf{cm}_2$ →

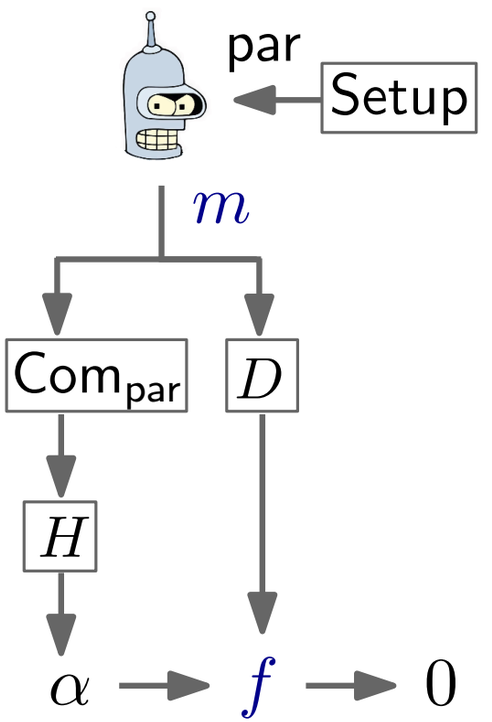
← $\alpha \leftarrow\!\!\$\ \mathbb{F}$

- $y_i := f_i(\alpha)$
- π_i . . . opening proofs

y_1, π_2, y_2, π_2 →

- check π_1, π_2
- return $y_2 \stackrel{?}{=} y_1^3$

Zero-testing



Using ZT

I have polynomials f_1, f_2 s.t. $f_2 \equiv f_1^3$

- $\mathsf{cm}_i := \mathsf{Com}(f_i)$

$\mathsf{cm}_1, \mathsf{cm}_2$ →

$\alpha := H(\mathsf{cm}_1 \| \mathsf{cm}_1)$

- $y_i := f_i(\alpha)$
- π_i . . . opening proofs

y_1, π_2, y_2, π_2 →

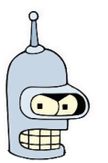
- check π_1, π_2
- return $y_2 \stackrel{?}{=} y_1^3$

$\Leftrightarrow\approx f_2(\alpha) - (f_1(\alpha))^3 = 0$

Claim. For $D(f_1, f_2) := f_2 - f_1^3 \not\equiv 0$ soundness-$\mathcal{A}$ breaks **zero-testing**

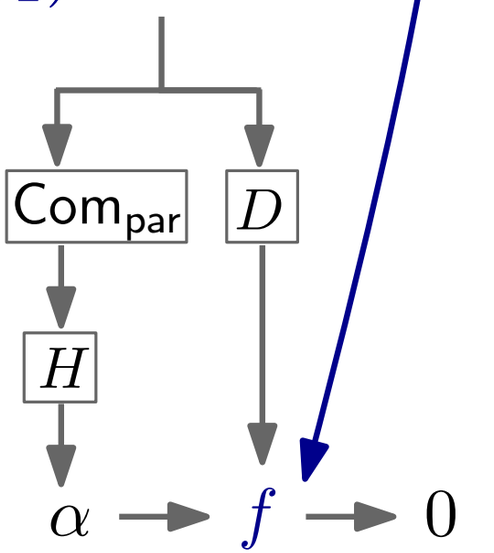
Proof.

$m := (f_1, f_2)$



par

Setup



$$\mathsf{srs} := \left(\mathcal{G}, [\tau]_1, \left[\tau^2\right]_1, \ldots, \left[\tau^{n+2}\right]_1, [\tau]_2\right).$$

$\underline{\mathsf{Index}(\mathsf{srs}, \mathbb{i})}$: Given $\mathbb{i}$, consisting of the gate constraints $(s_{\mathsf{L}i}, s_{\mathsf{R}i}, s_{\mathsf{O}i}, s_{\mathsf{M}i}, s_{\mathsf{C}i})_{i\in[n]}$ and the wire permutation σ^*, compute the polynomials

$$S_{\mathsf{L}}(X) := \sum\nolimits_{i\in[n]} s_{\mathsf{L}i}\mathcal{L}_i(X), \qquad S_{\mathsf{R}}(X) := \sum\nolimits_{i\in[n]} s_{\mathsf{R}i}\mathcal{L}_i(X),$$
$$S_{\mathsf{O}}(X) := \sum\nolimits_{i\in[n]} s_{\mathsf{O}i}\mathcal{L}_i(X), \qquad S_{\mathsf{M}}(X) := \sum\nolimits_{i\in[n]} s_{\mathsf{M}i}\mathcal{L}_i(X),$$
$$S_{\mathsf{C}}(X) := \sum\nolimits_{i\in[n]} s_{\mathsf{C}i}\mathcal{L}_i(X), \qquad S_{\sigma,1}(X) := \sum\nolimits_{i\in[n]} \sigma^*(i)\mathcal{L}_i(X),$$
$$S_{\sigma,2}(X) := \sum\nolimits_{i\in[n]} \sigma^*(n+i)\mathcal{L}_i(X), \quad S_{\sigma,3}(X) := \sum\nolimits_{i\in[n]} \sigma^*(2n+i)\mathcal{L}_i(X),$$

and their KZG commitments with respect to srs,

$$\mathsf{cm}_{S_{\mathsf{L}}} := [S_{\mathsf{L}}(\tau)]_1, \quad \mathsf{cm}_{S_{\mathsf{R}}} := [S_{\mathsf{R}}(\tau)]_1, \quad \mathsf{cm}_{S_{\mathsf{O}}} := [S_{\mathsf{O}}(\tau)]_1, \quad \mathsf{cm}_{S_{\mathsf{M}}} := [S_{\mathsf{M}}(\tau)]_1,$$
$$\mathsf{cm}_{S_{\mathsf{C}}} := [S_{\mathsf{C}}(\tau)]_1, \quad \mathsf{cm}_{S_{\sigma,1}} := [S_{\sigma,1}(\tau)]_1, \quad \mathsf{cm}_{S_{\sigma,2}} := [S_{\sigma,2}(\tau)]_1, \quad \mathsf{cm}_{S_{\sigma,3}} := [S_{\sigma,3}(\tau)]_1.$$

Return the prover and verifier parameters

$$\mathsf{pp} := (\mathsf{srs}, S_{\mathsf{L}}, S_{\mathsf{R}}, S_{\mathsf{O}}, S_{\mathsf{M}}, S_{\mathsf{C}}, S_{\sigma,1}, S_{\sigma,2}, S_{\sigma,3}),$$
$$\mathsf{vp} := (\mathsf{srs}, \mathsf{cm}_{S_{\mathsf{L}}}, \mathsf{cm}_{S_{\mathsf{R}}}, \mathsf{cm}_{S_{\mathsf{O}}}, \mathsf{cm}_{S_{\mathsf{M}}}, \mathsf{cm}_{S_{\mathsf{C}}}, \mathsf{cm}_{S_{\sigma,1}}, \mathsf{cm}_{S_{\sigma,2}}, \mathsf{cm}_{S_{\sigma,3}}).$$

$\underline{\mathsf{Prove}\big(\mathsf{pp}, (x_i)_{i\in[\ell]}, (w_i)_{i\in[3n]}\big)}$:

1. Sample blinding scalars $\rho_1, \ldots, \rho_6 \leftarrow \mathbb{F}$ and compute the wire polynomials

$$A(X) := (\rho_1 X + \rho_2)Z_{\mathbb{H}}(X) + \sum\nolimits_{i\in[n]} w_i\mathcal{L}_i(X),$$
$$B(X) := (\rho_3 X + \rho_4)Z_{\mathbb{H}}(X) + \sum\nolimits_{i\in[n]} w_{n+i}\mathcal{L}_i(X),$$
$$C(X) := (\rho_5 X + \rho_6)Z_{\mathbb{H}}(X) + \sum\nolimits_{i\in[n]} w_{2n+i}\mathcal{L}_i(X).$$

   The first part of the proof are the commitments

$$\mathsf{cm}_A := [A(\tau)]_1, \ \mathsf{cm}_B := [B(\tau)]_1, \ \mathsf{cm}_C := [C(\tau)]_1.$$

2. Let $\mathsf{trans}_0 := \mathsf{vp}\|\mathbb{x}$ with $\mathbb{x} := (x_i)_{i\in[\ell]}$. Compute the permutation challenges $\beta, \gamma \in \mathbb{F}$:

$$\beta := H(\mathsf{trans}_1), \text{ where } \mathsf{trans}_1 := \mathsf{trans}_0\|\mathsf{cm}_A\|\mathsf{cm}_B\|\mathsf{cm}_C,$$
$$\gamma := H(\mathsf{trans}_2), \text{ where } \mathsf{trans}_2 := \mathsf{trans}_1\|\beta.$$

3. Define the polynomials

$$f(X) := (A(X) + \beta S_{\mathrm{id},1}(X) + \gamma)(B(X) + \beta S_{\mathrm{id},2}(X) + \gamma)(C(X) + \beta S_{\mathrm{id},3}(X) + \gamma),$$
$$g(X) := (A(X) + \beta S_{\sigma,1}(X) + \gamma)(B(X) + \beta S_{\sigma,2}(X) + \gamma)(C(X) + \beta S_{\sigma,3}(X) + \gamma),$$

   where $S_{\mathrm{id},1}(X) := X$, $S_{\mathrm{id},2}(X) := k_1 X$, $S_{\mathrm{id},3}(X) := k_2 X$ are polynomials interpolating the identity permutation $\mathrm{id}^*\colon [3n] \to \mathbb{H}'$ over $\mathbb{H}$.

   Sample blinding scalars $\rho_7, \rho_8, \rho_9 \leftarrow \mathbb{F}$ and compute the permutation-check polynomial

$$\Phi(X) := (\rho_7 X^2 + \rho_8 X + \rho_9)Z_{\mathbb{H}}(X) + \sum_{i\in[n]} \mathcal{L}_i(X) \prod_{j=1}^{i-1} \frac{f(\omega^j)}{g(\omega^j)}$$
$$\left(\text{where } \frac{f(\omega^j)}{g(\omega^j)} = \frac{(w_j+\beta\omega^j+\gamma)(w_{n+j}+\beta k_1\omega^j+\gamma)(w_{2n+j}+\beta k_2\omega^j+\gamma)}{(w_j+\beta\sigma^*(j)+\gamma)(w_{n+j}+\beta\sigma^*(n+j)+\gamma)(w_{2n+j}+\beta\sigma^*(2n+j)+\gamma)}\right).$$

   If $g(\omega^j) = 0$ for some $j \in [n]$, abort. The second part of the proof is the commitment

$$\mathsf{cm}_\Phi := [\Phi(\tau)]_1.$$

4. Compute the quotient challenge $\alpha \in \mathbb{F}$ as

$$\alpha := H(\mathsf{trans}_3), \text{ where } \mathsf{trans}_3 := \mathsf{trans}_2\|\gamma\|\mathsf{cm}_\Phi.$$

5. Define the public-input polynomial $S_{\mathsf{PI}}(X) := \sum_{i\in[\ell]} x_i\mathcal{L}_i(X)$, and

$$\mathsf{Gates}(X) := \begin{pmatrix} S_{\mathsf{L}}(X)A(X) + S_{\mathsf{R}}(X)B(X) + S_{\mathsf{O}}(X)C(X) \\ + S_{\mathsf{M}}(X)A(X)B(X) + S_{\mathsf{C}}(X) - S_{\mathsf{PI}}(X) \end{pmatrix},$$
$$\mathsf{Copy}_1(X) := \Phi(X)f(X) - \Phi(X\omega)g(X),$$
$$\mathsf{Copy}_2(X) := \mathcal{L}_1(X)(\Phi(X) - 1).$$

   Compute the quotient polynomial of degree $\leq 3n + 5$

$$T(X) := \frac{\mathsf{Gates}(X) + \alpha \cdot \mathsf{Copy}_1(X) + \alpha^2 \cdot \mathsf{Copy}_2(X)}{Z_{\mathbb{H}}(X)},$$

   and split it into 3 unique polynomials $T'_1, T'_2, T'_3 \in \mathbb{F}^{(\leq n+1)}[X]$ such that

$$T(X) = T'_1(X) + X^{n+2} \cdot T'_2(X) + X^{2n+4} \cdot T'_3(X).$$

   Then, sample blinding scalars $\rho_{10}, \rho_{11} \leftarrow \mathbb{F}$ and define

$$T_1(X) := T'_1(X) + \rho_{10}X^{n+2},$$
$$T_2(X) := T'_2(X) - \rho_{10} + \rho_{11}X^{n+2},$$
$$T_3(X) := T'_3(X) - \rho_{11}.$$

   (These polynomials still satisfy $T(X) = T_1(X) + X^{n+2} \cdot T_2(X) + X^{2n+4} \cdot T_3(X)$.)

   The third part of the proof are the commitments

$$\mathsf{srs} := (\mathcal{G}, [\tau]_1, [\tau^2]_1, \ldots, [\tau^{n+2}]_1, [\tau]_2).$$

$\underline{\mathsf{Index}(\mathsf{srs}, \mathbb{i})}$: Given $\mathbb{i}$, consisting of the gate constraints $(s_{\mathsf{L}i}, s_{\mathsf{R}i}, s_{\mathsf{O}i}, s_{\mathsf{M}i}, s_{\mathsf{C}i})_{i\in[n]}$ and the wire permutation σ^*, compute the polynomials

$$S_{\mathsf{L}}(X) := \sum_{i\in[n]} s_{\mathsf{L}i}\mathcal{L}_i(X), \qquad S_{\mathsf{R}}(X) := \sum_{i\in[n]} s_{\mathsf{R}i}\mathcal{L}_i(X),$$
$$S_{\mathsf{O}}(X) := \sum_{i\in[n]} s_{\mathsf{O}i}\mathcal{L}_i(X), \qquad S_{\mathsf{M}}(X) := \sum_{i\in[n]} s_{\mathsf{M}i}\mathcal{L}_i(X),$$
$$S_{\mathsf{C}}(X) := \sum_{i\in[n]} s_{\mathsf{C}i}\mathcal{L}_i(X), \qquad S_{\sigma,1}(X) := \sum_{i\in[n]} \sigma^*(i)\mathcal{L}_i(X),$$
$$S_{\sigma,2}(X) := \sum_{i\in[n]} \sigma^*(n+i)\mathcal{L}_i(X), \quad S_{\sigma,3}(X) := \sum_{i\in[n]} \sigma^*(2n+i)\mathcal{L}_i(X),$$

and their KZG commitments with respect to srs,

$$\mathsf{cm}_{S_{\mathsf{L}}} := [S_{\mathsf{L}}(\tau)]_1, \quad \mathsf{cm}_{S_{\mathsf{R}}} := [S_{\mathsf{R}}(\tau)]_1, \quad \mathsf{cm}_{S_{\mathsf{O}}} := [S_{\mathsf{O}}(\tau)]_1, \quad \mathsf{cm}_{S_{\mathsf{M}}} := [S_{\mathsf{M}}(\tau)]_1,$$
$$\mathsf{cm}_{S_{\mathsf{C}}} := [S_{\mathsf{C}}(\tau)]_1, \quad \mathsf{cm}_{S_{\sigma,1}} := [S_{\sigma,1}(\tau)]_1, \quad \mathsf{cm}_{S_{\sigma,2}} := [S_{\sigma,2}(\tau)]_1, \quad \mathsf{cm}_{S_{\sigma,3}} := [S_{\sigma,3}(\tau)]_1.$$

Return the prover and verifier parameters

$$\mathsf{pp} := (\mathsf{srs}, S_{\mathsf{L}}, S_{\mathsf{R}}, S_{\mathsf{O}}, S_{\mathsf{M}}, S_{\mathsf{C}}, S_{\sigma,1}, S_{\sigma,2}, S_{\sigma,3}),$$
$$\mathsf{vp} := (\mathsf{srs}, \mathsf{cm}_{S_{\mathsf{L}}}, \mathsf{cm}_{S_{\mathsf{R}}}, \mathsf{cm}_{S_{\mathsf{O}}}, \mathsf{cm}_{S_{\mathsf{M}}}, \mathsf{cm}_{S_{\mathsf{C}}}, \mathsf{cm}_{S_{\sigma,1}}, \mathsf{cm}_{S_{\sigma,2}}, \mathsf{cm}_{S_{\sigma,3}}).$$

3. Define the polynomials

$$f(X) := (A(X) + \beta S_{\mathrm{id},1}(X) + \gamma)(B(X) + \beta S_{\mathrm{id},2}(X) + \gamma)(C(X) + \beta S_{\mathrm{id},3}(X) + \gamma),$$
$$g(X) := (A(X) + \beta S_{\sigma,1}(X) + \gamma)(B(X) + \beta S_{\sigma,2}(X) + \gamma)(C(X) + \beta S_{\sigma,3}(X) + \gamma),$$

where $S_{\mathrm{id},1}(X) := X$, $S_{\mathrm{id},2}(X) := k_1 X$, $S_{\mathrm{id},3}(X) := k_2 X$ are polynomials interpolating the identity permutation $\mathrm{id}^*\colon [3n] \to \mathbb{H}'$ over $\mathbb{H}$.

Sample blinding scalars $\rho_7, \rho_8, \rho_9 \leftarrow \mathbb{F}$ and compute the permutation-check polynomial

$$\Phi(X) := (\rho_7 X^2 + \rho_8 X + \rho_9) Z_{\mathbb{H}}(X) + \sum_{i\in[n]} \mathcal{L}_i(X) \prod_{j=1}^{i-1} \frac{f(\omega^j)}{g(\omega^j)}$$

$$\left(\text{where } \frac{f(\omega^j)}{g(\omega^j)} = \frac{(w_j+\beta\omega^j+\gamma)(w_{n+j}+\beta k_1\omega^j+\gamma)(w_{2n+j}+\beta k_2\omega^j+\gamma)}{(w_j+\beta\sigma^*(j)+\gamma)(w_{n+j}+\beta\sigma^*(n+j)+\gamma)(w_{2n+j}+\beta\sigma^*(2n+j)+\gamma)}\right).$$

If $g(\omega^j) = 0$ for some $j \in [n]$, abort. The second part

$$\mathsf{cm}_{\Phi} := [\Phi(\tau)]_1.$$

4. Compute the quotient challenge $\alpha \in \mathbb{F}$ as

$\alpha := H(\mathsf{trans}_2)$, where $\mathsf{trans}_3 := \mathsf{tr}$

$:= \sum_{i\in[$

$\mathsf{R}}(X)B(X$

$B(X) +$

$\omega)g(X),$

$\le 3n +$

$\mathsf{py}_1(X) +$

$Z_{\mathbb{H}}(X)$

$T_2', T_3' \in \mathbb{F}$

$T_2'(X) +$

and defi

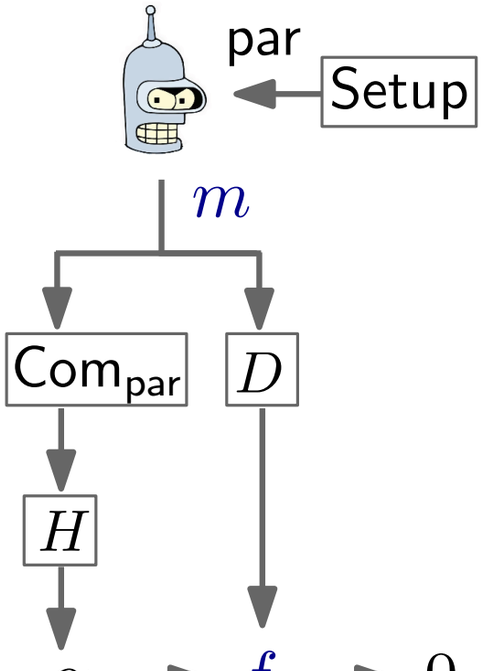
$\rho_{10}X^{n+2}$

$\rho_{10} + \rho_{11}$,

ρ_{11}.

(These polynomials still satisfy $T(X) = T_1(X) + X^{n+2} \cdot T_2(X) + X^{2n+4} \cdot T_3(X)$.)

The third part of the proof are the commitments



For $m = (S_{\mathsf{L}}, S_{\mathsf{R}}, S_{\mathsf{O}}, S_{\mathsf{M}}, S_{\mathsf{C}}, S_{\sigma,1}, S_{\sigma,2}, S_{\sigma,3}, \vec{x}, A, B, C)$, define

$$D_1(m) := \prod_{i\in[n]} f(X_\beta, X_\gamma, \omega^i) - \prod_{i\in[n]} g(X_\beta, X_\gamma, \omega^i)$$

with $f(X_\beta, X_\gamma, X_\delta) := \big(A(X_\delta) + X_\beta X_\delta + X_\gamma\big)$
$\big(B(X_\delta) + X_\beta k_1 X_\delta + X_\gamma\big)\big(C(X_\delta) + X_\beta k_2 X_\delta + X_\gamma\big)$

and $g(X_\beta, X_\gamma, X_\delta) := \big(A(X_\delta) + X_\beta S_{\sigma,1}(X_\delta) + X_\gamma\big)$
$\big(B(X_\delta) + X_\beta S_{\sigma,2}(X_\delta) + X_\gamma\big)\big(C(X_\delta) + X_\beta S_{\sigma,3}(X_\delta) + X_\gamma\big)$

Jusitifying zero-testing

Theorems.

Zero-testing holds for $H\colon \{0,1\}^* \to \mathbb{F}$, (Setup,Com)
w.r.t. $D\colon \mathcal{M} \to \mathbb{F}^{(\leq d)}[X]$

- . . . if H is modeled as a random oracle
  and (Setup,Com) is binding
- . . . if (Setup,Com) is KZG over a generic group
  and H is *balanced*

implied by *collision-resistance*

Open questions: cryptanalysis for used hash functions

Zero-testing