Adding zero-knowledge to STARKs

(a tail of traps and pitfalls)

U. Haböck and Al Kindi

StarkWare, Polygon Labs

March 24, 2025

Intro

STARKs

Intro

STARKs

...are a poly IOP

Intro

STARKs

...are a poly IOP

- permutation arguments, and lookups,

Intro

STARKs

...are a poly IOP

- permutation arguments, and lookups,
- decompose overall quotient polynomial

Intro

STARKs

...are a poly IOP

- permutation arguments, and lookups,
- decompose overall quotient polynomial

Intro

STARKs

...are a poly IOP

- permutation arguments, and lookups,
- decompose overall quotient polynomial

...not a poly IOP

Intro

STARKs

...are a poly IOP

- permutation arguments, and lookups,
- decompose overall quotient polynomial

...not a poly IOP

- FRI low-degree test

Intro

STARKs

...are a poly IOP

- permutation arguments, and lookups,
- decompose overall quotient polynomial

...not a poly IOP

- FRI low-degree test

  (and its queries!)

Intro

STARKs

...are a poly IOP

- permutation arguments, and lookups,
- decompose overall quotient polynomial

...not a poly IOP

- FRI low-degree test

  (and its queries!)

Intro

STARKs

...are a poly IOP

- permutation arguments, and lookups,
- decompose overall quotient polynomial

...not a poly IOP

- FRI low-degree test

  (and its queries!)

...and use small fields

Intro

Gaps:

Intro

Gaps:

- plonky2, Risc0, Triton

Intro

Gaps:

- plonky2, Risc0, Triton

Intro

Gaps:

- plonky2, Risc0, Triton

not only STARKs:

Intro

Gaps:

- plonky2, Risc0, Triton

not only STARKs:

- halo2 book

Intro

Gaps:

- plonky2, Risc0, Triton

not only STARKs:

- halo2 book
- Plonk paper [GWC19] (former version)

Intro

Gaps:

- plonky2, Risc0, Triton

not only STARKs:

- halo2 book
- Plonk paper [GWC19] (former version)

Intro

Gaps:

- plonky2, Risc0, Triton

not only STARKs:

- halo2 book
- Plonk paper [GWC19] (former version)

...FRI survey [Hab22] 🤐

Basics

Witness polys w_1, ...,w_m satisfying constraint

$$C(w_1(X), \ldots, w_m(X)) = q(X) \cdot v_H(X),$$

Basics

Witness polys w_1, ...,w_m satisfying constraint

$$C(w_1(X), \ldots, w_m(X)) = q(X) \cdot v_H(X),$$

tested at $z \stackrel{\$}{\leftarrow} F \setminus H$.

Basics

Witness polys w_1, ...,w_m satisfying constraint

$$C(w_1(X), \ldots, w_m(X)) = q(X) \cdot v_H(X),$$

tested at $z \xleftarrow{\$} F \setminus H$.

...reveals

$$w_1(z), \ldots, w_m(z), \quad q(z), v_H(z)$$

Basics

Randomize outside H:

Basics

Randomize outside H:

$$\hat{w}_i(X) = w_i(X) + c_i \cdot v_H(X), \quad c_i \xleftarrow{\$} F.$$

Basics

Randomize outside H:

$$\hat{w}_i(X) = w_i(X) + c_i \cdot v_H(X), \quad c_i \xleftarrow{\$} F.$$

Still

$$C(\hat{w}_1(X), \ldots, \hat{w}_m(X)) = q(X) \cdot v_H(X),$$

with new $q(X)$.

Basics

Randomize outside H:

$$\hat{w}_i(X) = w_i(X) + c_i \cdot v_H(X), \quad c_i \xleftarrow{\$} F.$$

Still

$$C(\hat{w}_1(X), \ldots, \hat{w}_m(X)) = q(X) \cdot v_H(X),$$

with new $q(X)$.

At $z \xleftarrow{\$} F \setminus H$

$$\hat{w}_1(z), \ldots, \hat{w}_m(z), \quad q(z), v_H(z)$$

Basics

Randomize outside H:

$$\hat{w}_i(X) = w_i(X) + c_i \cdot v_H(X), \quad c_i \xleftarrow{\$} F.$$

Still

$$C(\hat{w}_1(X), \ldots, \hat{w}_m(X)) = q(X) \cdot v_H(X),$$

with new $q(X)$.

At $z \xleftarrow{\$} F \setminus H$

$$\underbrace{\hat{w}_1(z), \ldots, \hat{w}_m(z)}_{\text{uniform over} F^m}, \quad q(z), v_H(z)$$

Basics

Randomize outside H:

$$\hat{w}_i(X) = w_i(X) + c_i \cdot v_H(X), \quad c_i \xleftarrow{\$} F.$$

Still

$$C(\hat{w}_1(X), \ldots, \hat{w}_m(X)) = q(X) \cdot v_H(X),$$

with new $q(X)$.

At $z \xleftarrow{\$} F \setminus H$

$$\underbrace{\hat{w}_1(z), \ldots, \hat{w}_m(z)}_{\text{uniform over} F^m}, \quad q(z), v_H(z)$$

$$\frac{C(\qquad\qquad)}{v_H(z)} \rightarrow q(z)$$

Basics

Randomize outside H:

$$\hat{w}_i(X) = w_i(X) + c_i \cdot v_H(X), \quad c_i \stackrel{\$}{\leftarrow} F.$$

Still

$$C(\hat{w}_1(X), \dots, \hat{w}_m(X)) = q(X) \cdot v_H(X),$$

with new $q(X)$.

At $z \stackrel{\$}{\leftarrow} F \setminus H$

$$\underbrace{\hat{w}_1(z), \dots, \hat{w}_m(z)}_{\text{uniform over} F^m}, \quad q(z), v_H(z)$$

$$\frac{C(\qquad\qquad)}{v_H(z)} \rightarrow q(z)$$

Basics

easy!

Basics

easy!

Basics

easy!

...what can go wrong?

Quot. decomp.

$$C(\hat{w}_1(X), \ldots, \hat{w}_m(X)) = \underbrace{q(X)}_{\text{split into small polys}} \cdot v_H(X),$$

Quot. decomp.

$$C(\hat{w}_1(X), \ldots, \hat{w}_m(X)) = \underbrace{q(X)}_{\text{split into small polys}} \cdot v_H(X),$$

Quot. decomp.

$$C(\hat{w}_1(X), \ldots, \hat{w}_m(X)) = \underbrace{q(X)}_{\text{split into small polys}} \cdot v_H(X),$$

E.g. $\deg C = 3$,

Quot. decomp.

$$C(\hat{w}_1(X), \ldots, \hat{w}_m(X)) = \underbrace{q(X)}_{\text{split into small polys}} \cdot v_H(X),$$

E.g. $\deg C = 3$,

$$q(X) = q_0(X^2) + X \cdot q_1(X^2)$$

Quot. decomp.

At $z \xleftarrow{\$} F \setminus H$

$$C(\hat{w}_1(z), \ldots, \hat{w}_m(z)) = \underbrace{q(z)}_{\text{split into small polys}} \cdot v_H(z),$$

E.g. $\deg C = 3$,

$$q(z) = q_0(z^2) + z \cdot q_1(z^2)$$

Quot. decomp.

At $z \xleftarrow{\$} F \setminus H$

$$C(\hat{w}_1(z), \ldots, \hat{w}_m(z)) = \underbrace{q(z)}_{\text{split into small polys}} \cdot v_H(z),$$

E.g. $\deg C = 3$,

$$q(z) = q_0(z^2) + z \cdot q_1(z^2)$$

additional info revealed

Quot. decomp.

FFT decomp. $=$ local map

Quot. decomp.

FFT decomp. $=$ local map

$$q(z), q(-z) \longrightarrow q_1(z^2), q_0(z^2)$$

$$q_0(z^2) = \frac{q(z) + q(-z)}{2}$$

$$q_1(z^2) = \frac{q(z) - q(-z)}{2 \cdot z}$$

Quot. decomp.

FFT decomp. = local map

$$q(z), q(-z) \longrightarrow q_1(z^2), q_0(z^2)$$

$$q_0(z^2) = \frac{q(z) + q(-z)}{2}$$

$$q_1(z^2) = \frac{q(z) - q(-z)}{2 \cdot z}$$

$\rightarrow$ secure $\hat{w}_i$ against opening at z *and* $-z$

Quot. decomp.

FFT decomp. = local map

$$q(z), q(-z) \longrightarrow q_1(z^2), q_0(z^2)$$

$$q_0(z^2) = \frac{q(z) + q(-z)}{2}$$

$$q_1(z^2) = \frac{q(z) - q(-z)}{2 \cdot z}$$

$\rightarrow$ secure $\hat{w}_i$ against opening at *z and $-z$*

$$\hat{w}_i(X) = w_i(X) + (a_i + b_i \cdot X) \cdot v_H(X), \quad a_i, c_i \overset{\$}{\leftarrow} F$$

Quot. decomp

still easy!

Quot. decomp

With FRI:

Quot. decomp

With FRI: we also ask $q_0(x)$ and $q_1(x)$ at points $x \in D$.

Quot. decomp

With FRI: we also ask $q_0(x)$ and $q_1(x)$ at points $x \in D$.

- x might not be of the form $x = z^2$

Quot. decomp

With FRI: we also ask $q_0(x)$ and $q_1(x)$ at points $x \in D$.

- x might not be of the form $x = z^2$
- need to move to an extension field with $z = \sqrt{x}$.

$$q(z), q(-z) \longrightarrow q_0(x), q_1(x)$$

Quot. decomp

With FRI: we also ask $q_0(x)$ and $q_1(x)$ at points $x \in D$.

- x might not be of the form $x = z^2$
- need to move to an extension field with $z = \sqrt{x}$.

$$q(z), q(-z) \longrightarrow q_0(x), q_1(x)$$

- need to secure against eval in extension field!

Quot. decomp

ok...

Quot. decomp

ok...

...maybe we should be cautious

Extension fields

- Randomize over base field F

Extension fields

- Randomize over base field F
- $\hat{w}(X) = w(X) + r(X) \cdot v_H(X)$ with $r(X) \overset{\$}{\leftarrow} F[X]^{<d}$,

Extension fields

- Randomize over base field F
- $\hat{w}(X) = w(X) + r(X) \cdot v_H(X)$ with $r(X) \xleftarrow{\$} F[X]^{<d}$,
- query at z from extension $K > F$.

Extension fields

- Randomize over base field F
- $\hat{w}(X) = w(X) + r(X) \cdot v_H(X)$ with $r(X) \xleftarrow{\$} F[X]^{<d}$,
- query at z from extension $K > F$.
- $\hat{w}(z) \in K$ is a vector of $[K : F]$ values in F.

Extension fields

- Randomize over base field F
- $\hat{w}(X) = w(X) + r(X) \cdot v_H(X)$ with $r(X) \stackrel{\$}{\leftarrow} F[X]^{<d}$,
- query at z from extension $K > F$.
- $\hat{w}(z) \in K$ is a vector of $[K : F]$ values in F.

Extension fields

- Randomize over base field F
- $\hat{w}(X) = w(X) + r(X) \cdot v_H(X)$ with $r(X) \stackrel{\$}{\leftarrow} F[X]^{<d}$,
- query at z from extension $K > F$.
- $\hat{w}(z) \in K$ is a vector of $[K : F]$ values in F.

$\rightarrow$ for each query $[K : F]$ free coeffs in $r(X)$.

Extension fields

prove it! :)

FRI

Chain of domains under $\pi(x) = x^2$,

$$D_0 \xrightarrow{\pi} D_1 \xrightarrow{\pi} \dots \xrightarrow{\pi} D_k$$

FRI

Chain of domains under $\pi(x) = x^2$,

$$D_0 \xrightarrow{\pi} D_1 \xrightarrow{\pi} \dots \xrightarrow{\pi} D_k$$

foldings

$$h_0 \xrightarrow{\pi} h_1 \xrightarrow{\pi} \dots \xrightarrow{\pi} h_k$$

FRI

Chain of domains under $\pi(x) = x^2$,

$$D_0 \xrightarrow{\pi} D_1 \xrightarrow{\pi} \dots \xrightarrow{\pi} D_k$$

foldings

$$h_0 \xrightarrow{\pi} h_1 \xrightarrow{\pi} \dots \xrightarrow{\pi} h_k$$

- each folding opened at two points

$$h_{i+1}(x^2) = \frac{h_i(x) + h_i(-x)}{2} + \lambda_i \cdot \frac{h_i(x) - h(-x)}{2 \cdot x}$$

FRI

Chain of domains under $\pi(x) = x^2$,

$$D_0 \xrightarrow{\pi} D_1 \xrightarrow{\pi} \ldots \xrightarrow{\pi} D_k$$

foldings

$$h_0 \xrightarrow{\pi} h_1 \xrightarrow{\pi} \ldots \xrightarrow{\pi} h_k$$

- each folding opened at two points

$$h_{i+1}(x^2) = \frac{h_i(x) + h_i(-x)}{2} + \lambda_i \cdot \frac{h_i(x) - h(-x)}{2 \cdot x}$$

- last folding h_k at every point.

FRI

Cannot be randomized via

$$\hat{h}(X) = h(X) + r(X) \cdot v_H(X)$$

FRI

Cannot be randomized via

$$\hat{h}(X) = h(X) + r(X) \cdot v_H(X)$$

because entropy is halved!

$$\mathsf{F}_\lambda(\hat{h})(X) = \mathsf{F}_\lambda(h)(X) + v_{H^2}(X) \cdot \mathsf{F}_\lambda(r)(X)$$

FRI

$\rightarrow$ [Ben+19] overlay mask polynomial in batching step

$$h_0(x) = r(x) + \sum_{i=1}^{m} \lambda^i \cdot w_i(x)$$

with $r(X) \xleftarrow{\$} F[X]^{<d}$ with $d > \deg w_i$.

Recap

Ok...

Recap

Ok... lets recap...

Recap

Ok... lets recap...

- Each DEEP query amounts to $[K : F]$ basefield values,

Recap

Ok... lets recap...

- Each DEEP query amounts to $[K : F]$ basefield values,
- Quotient FFT decomposition into d components: each query needs to be secured by d

Recap

Ok... lets recap...

- Each DEEP query amounts to $[K : F]$ basefield values,
- Quotient FFT decomposition into d components: each query needs to be secured by d
- use FRI mask poly

Recap

Ok... lets recap...

- Each DEEP query amounts to $[K : F]$ basefield values,
- Quotient FFT decomposition into d components: each query needs to be secured by d
- use FRI mask poly

Degree of freedom

$$n_{DEEP} \cdot [K : F] \cdot d + n_{FRI} \cdot d$$

Recap

Ok... lets recap...

- Each DEEP query amounts to $[K:F]$ basefield values,
- Quotient FFT decomposition into d components: each query needs to be secured by d
- use FRI mask poly

Degree of freedom

$$n_{DEEP} \cdot [K:F] \cdot d + n_{FRI} \cdot d + n_{FRI}$$

queries behind $q_i(x)$ do not overlap with $w_i(x)$!

...and we did not even talk about permutation arguments

...and we did not even talk about permutation arguments

For details $\rightarrow$ `https://eprint.iacr.org/2024/1037`

...and we did not even talk about permutation arguments

For details → `https://eprint.iacr.org/2024/1037`

Thank you!

Bib

[Ben+19] Eli Ben-Sasson et al. "Aurora: Transparent Succinct Arguments for R1CS.". In: *EUROCRYPT 2019.* Ed. by Y. Ishai and Vincent Rijmen. Vol. 11476. LNCS. Springer, 2019. DOI: 10.1007/978-3-030-17653-2_4.

[GWC19] Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. "PLONK: Permutations over Lagrange-bases for Oecumenical Non-interactive Arguments of Knowledge". In: *IACR ePrint Archive 2019/953.* https://eprint.iacr.org/2019/953. 2019.

[Hab22] Ulrich Haböck. "A Summary on the FRI low-degree test". In: *IACR ePrint Archive 2022/1216.* https://eprint.iacr.org/2022/1216. 2022.