STARKWARE

Arithmetization FRI and PCS

Eli Ben-Sasson

February 2023

1) Arithmetization

STARKWARE

Arithmetization Converts (“reduces”) Computational Integrity problems to problems about local relations between a bunch of polynomials

Example: For public 256-bit string ***z***, Bob claims knows a SHA2-preimage of ***z***

1) Arithmetization

STARKWARE

Arithmetization Converts (“reduces”) Computational Integrity problems to problems about local relations between a bunch of polynomials

Example: For public 256-bit string ***z***, Bob claims knows a SHA2-preimage of ***z***

Pre-arithmetization claim

“I know y such that SHA2(y)=z”

1) Arithmetization

STARKWARE

Arithmetization Converts (“reduces”) Computational Integrity problems to problems about local relations between a bunch of polynomials

Example: For public 256-bit string ***z***, Bob claims knows a SHA2-preimage of ***z***

Pre-arithmetization claim	**Reduction**
“I know y such that SHA2(y)=z”	*produces 2 polynomials:* ***Q(X,Y,T,W), R(X)*** *and degree bound* ***d***

1) Arithmetization

STARKWARE

Arithmetization Converts (“reduces”) Computational Integrity problems to problems about local relations between a bunch of polynomials

Example: For public 256-bit string ***z***, Bob claims knows a SHA2-preimage of ***z***

Pre-arithmetization claim	**Reduction**	**Post-arithmetization claim**
“I know y such that SHA2(y)=z”	*produces 2 polynomials:* ***Q(X,Y,T,W), R(X)*** *and degree bound* ***d***	*I know 4 polynomials of degree* ***d*** *- A(x), B(x), C(x), D(X) - such that:* *Q(X, A(X), B(X+1), C(2*X))=D(X) * R(X)*

1) Arithmetization

STARKWARE

Arithmetization Converts (“reduces”) Computational Integrity problems to problems about local relations between a bunch of polynomials

Example: For public 256-bit string ***z***, Bob claims knows a SHA2-preimage of ***z***

Pre-arithmetization claim	**Reduction**	**Post-arithmetization claim**	**Theorem**
“I know y such that SHA2(y)=z”	*produces 2 polynomials:* ***Q(X,Y,T,W), R(X)*** *and degree bound* ***d***	*I know 4 polynomials of degree* ***d*** *- A(x), B(x), C(x), D(X) - such that:* *Q(X, A(X), B(X+1), C(2*X))=D(X) * R(X)*	*If A, B, C, D do not satisfy THIS,* *then nearly all x expose Bob’s lie*

1) Arithmetization

STARKWARE

Assuming Theorem, we get a scalable proof system for Bob's original claim:

1. Apply reduction, ask Bob to provide access to A,B,C,D of degree-d
2. Sample random x and accept Bob's claim iff equality holds for this x

Pre-arithmetization claim	**Reduction**	**Post-arithmetization claim**	**Theorem**
"I know y such that SHA2(y)=z"	*produces 2 polynomials:* ***Q(X,Y,T,W), R(X)*** *and degree bound* ***d***	*I know 4 polynomials of degree d - A(x), B(x), C(x), D(X) - such that:* *Q(X, A(X), B(X+1), C(2*X))=D(X) * R(X)*	*If A, B, C, D do not satisfy THIS,* *then nearly all x expose Bob's lie*

2) Low degreeness

STARKWARE

Assuming Theorem, we get a scalable proof system for Bob's original claim:

1. Apply reduction, ask Bob to provide access to A,B,C,D of degree-d
2. Sample random x and accept Bob's claim iff equality holds for this x

New Computational Integrity problem: Force Bob to answer all queries according to some quadruple of degree-d polynomials

Post-arithmetization claim

I know 4 polynomials of degree d - A(x), B(x), C(x), D(X) - such that:

*Q(X, A(X), B(X+1), C(2*X))=D(X) * R(X)*

Theorem

If A, B, C, D do not satisfy THIS,

then nearly all x expose Bob's lie

STARKWARE

Arithmetization Boot Camp

STARKWARE

Goal: See how Polynomials lead to Succinct Verification

STARKWARE

Goal: See how Polynomials lead to Succinct Verification

Non-Goal: Understand Why

Arithmetization Toy Problem

STARKWARE

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree d

Bob sends $P(X) \in \mathbb{F}[X]$, $\deg(P) < d$ to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with $P(a)$

Arithmetization Toy Problem

STARKWARE

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X)=\prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a) = 0 \Leftrightarrow \exists\, Q(X): P(X)=Q(X)*Z_H(X)$, $\deg(Q)=\deg(P)-|H|$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree d

Bob sends $P(X) \in \mathbb{F}[X]$, $\deg(P)<d$ to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with $P(a)$

Arithmetization Toy Problem

STARKWARE

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X)=\prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a)=0 \Leftrightarrow \exists\, Q(X): P(X)=Q(X)*Z_H(X)$, $\deg(Q)=\deg(P)-|H|$
2. If $f, g: S \rightarrow \mathbb{F}$, $\deg(f)$, $\deg(g)< d$ and $|S|=100d$, then $\Pr_a[f(a)=g(a)]<1/100$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree d

Bob sends $P(X) \in \mathbb{F}[X]$, $\deg(P)<d$ to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with $P(a)$

Arithmetization Toy Problem

STARKWARE

Clm 1: *P*, committed by PCS, vanishes on *H*

Challenge: Succinct protocol to verify Clm 1

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X)=\prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a)=0 \Leftrightarrow \exists\, Q(X): P(X)=Q(X)*Z_H(X)$, $\deg(Q)=\deg(P)-|H|$
2. If $f, g: S \to \mathbb{F}$, $\deg(f)$, $\deg(g)< d$ and $|S|=100d$, then $\Pr_a[f(a)=g(a)]<1/100$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree d

Bob sends $P(X) \in \mathbb{F}[X]$, $\deg(P)<d$ to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with $P(a)$

Arithmetization Toy Problem

STARKWARE

Clm 1: *P*, committed by PCS, vanishes on *H*

Challenge: Succinct protocol to verify Clm 1

Protocol:
* Prover Commits to *P, Q* using PCS, deg(Q)<d-|H|
* Verifier
  - samples random $a \in \mathbb{F}$,
  - queries PCS for *P(a), Q(a)*,
  - accepts iff $P(a)-Z_H(a)*Q(a) = 0$

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X)=\prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a) = 0 \Leftrightarrow \exists\ Q(X): P(X)=Q(X)*Z_H(X)$, deg(Q)=deg(P)-|H|
2. If $f, g: S \rightarrow \mathbb{F}$, deg(f), deg(g)< d and |S|=100d, then $\Pr_a[f(a)=g(a)]<1/100$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree *d*

Bob sends $P(X) \in \mathbb{F}[X]$, deg(P)<d to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with *P(a)*

Arithmetization Toy Problem

STARKWARE

Clm 1: *P*, committed by PCS, vanishes on *H*

Challenge: Succinct protocol to verify Clm 1

Protocol:
* Prover Commits to *P, Q* using PCS, deg(Q)<d-|H|
* Verifier
  - samples random $a \in \mathbb{F}$,
  - queries PCS for *P(a), Q(a)*,
  - accepts iff $P(a)-Z_H(a)*Q(a) = 0$

Efficiency: 2 queries, *O(|H|)* operations (+PCS cost)
Soundness: Prob[error] < $d/|\mathbb{F}|$.

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X)=\prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a) =0 \Leftrightarrow \exists\ Q(X): P(X)=Q(X)*Z_H(X)$, deg(Q)=deg(P)-|H|
2. If $f, g: S \rightarrow \mathbb{F}$, deg(f), deg(g)< d and |S|=100d, then $\Pr_a[f(a)=g(a)]<1/100$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree *d*

Bob sends $P(X) \in \mathbb{F}[X]$, deg(P)<d to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with *P(a)*

Arithmetization Toy Problem

STARKWARE

Clm 1: *P*, committed by PCS, vanishes on *H*

Challenge: Succinct protocol to verify Clm 1

Protocol:
* Prover Commits to *P, Q* using PCS, deg(Q)<d-|H|
* Verifier
  - samples random $a \in \mathbb{F}$,
  - queries PCS for *P(a), Q(a)*,
  - accepts iff $P(a)-Z_H(a)*Q(a) = 0$

Efficiency: 2 queries, $O(|H|)$ operations (+PCS cost)
Soundness: Prob[error] < $d/|\mathbb{F}|$.
Proof: Assume *P* doesn't vanish on *H*.
Fact 1: $P(X)-Z_H(a)*Q(a)$ is non-zero deg *d* polynomial
Fact 0: at most *d* "erroneous" values of *a* exist in $\mathbb{F}$ □

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X)=\prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a) = 0 \Leftrightarrow \exists\, Q(X): P(X)=Q(X)*Z_H(X)$, $\deg(Q)=\deg(P)-|H|$
2. If $f, g: S \to \mathbb{F}$, $\deg(f)$, $\deg(g) < d$ and $|S|=100d$, then $\Pr_a[f(a)=g(a)]<1/100$
3. For *H* a multiplicative group: $Z_H(X)= X^{|H|}-1$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree *d*

Bob sends $P(X) \in \mathbb{F}[X]$, $\deg(P)<d$ to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with *P(a)*

Arithmetization Toy Problem

STARKWARE

Clm 2: *P*, deg(P)<d, is {0,1}-valued on *H*

Challenge: Succinct protocol to verify Clm 2

Hint: C(Y) = Y * (1-Y) has roots {0,1}

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X)=\prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a)=0 \Leftrightarrow \exists\, Q(X): P(X)=Q(X)*Z_H(X)$, $\deg(Q)=\deg(P)-|H|$
2. If $f, g: S \to \mathbb{F}$, $\deg(f)$, $\deg(g)< d$ and $|S|=100d$, then $\Pr_a[f(a)=g(a)]<1/100$
3. For H a multiplicative group: $Z_H(X)= X^{|H|}-1$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree d

Bob sends $P(X) \in \mathbb{F}[X]$, $\deg(P)<d$ to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with $P(a)$

Arithmetization Toy Problem

STARKWARE

Clm 2: P, deg(P)<d, is {0,1}-valued on H

Challenge: Succinct protocol to verify Clm 2

Protocol:

* Prover Commits to P, Q using PCS, deg(Q)<2d-|H|
* Verifier
  - samples random $a \in \mathbb{F}$,
  - queries PCS for $P(a)$, $Q(a)$,
  - accepts iff $(P(a)*(1-P(a))-Z_H(a)*Q(a) = 0$

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X)=\prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a) = 0 \Leftrightarrow \exists\ Q(X): P(X)=Q(X)*Z_H(X)$, deg(Q)=deg(P)-|H|
2. If $f, g: S \to \mathbb{F}$, deg(f), deg(g)< d and $|S|=100d$, then $\Pr_a[f(a)=g(a)]<1/100$
3. For H a multiplicative group: $Z_H(X)= X^{|H|}-1$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree d

Bob sends $P(X) \in \mathbb{F}[X]$, deg(P)<d to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with $P(a)$

Arithmetization Toy Problem

STARKWARE

Clm 2: P, deg(P)<d, is {0,1}-valued on H

Challenge: Succinct protocol to verify Clm 2

Protocol:
* Prover Commits to P, Q using PCS, deg(Q)<2d-|H|
* Verifier
  - samples random $a \in \mathbb{F}$,
  - queries PCS for $P(a)$, $Q(a)$,
  - accepts iff $(P(a)*(1-P(a))-Z_H(a)*Q(a) = 0$

Efficiency: 2 queries, $O(\log |H|)$ operations (+PCS cost)
Soundness: Prob[error] < $2d/|\mathbb{F}|$.

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X)=\prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a) = 0 \Leftrightarrow \exists\, Q(X): P(X)=Q(X)*Z_H(X)$, deg(Q)=deg(P)-|H|
2. If $f, g: S \to \mathbb{F}$, deg(f), deg(g)< d and $|S|=100d$, then $\Pr_a[f(a)=g(a)]<1/100$
3. For H a multiplicative group: $Z_H(X)= X^{|H|}-1$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree d

Bob sends $P(X) \in \mathbb{F}[X]$, deg(P)<d to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with $P(a)$

Arithmetization Toy Problem

STARKWARE

Clm 2: P, deg(P)<d, is {0,1}-valued on H

Challenge: Succinct protocol to verify Clm 2

Protocol:
* Prover Commits to P, Q using PCS, deg(Q)<2d-|H|
* Verifier
  - samples random $a \in \mathbb{F}$,
  - queries PCS for $P(a)$, $Q(a)$,
  - accepts iff $(P(a)*(1-P(a))-Z_H(a)*Q(a) = 0$

Efficiency: 2 queries, $O(\log |H|)$ operations (+PCS cost)
Soundness: Prob[error] < $2d/|\mathbb{F}|$.
Proof: Assume P not {0,1}-valued
Then $P(X)*(1-P(X))$ doesn't vanish on H.
Fact 1: $P(X)*(1-P(X))-Z_H(a)*Q(a)$ is non-zero deg $2d$
Fact 0: at most $2d$ "erroneous" values of a exist in $\mathbb{F}$ □

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X)=\prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a) = 0 \Leftrightarrow \exists\, Q(X): P(X)=Q(X)*Z_H(X)$, deg(Q)=deg(P)-|H|
2. If $f, g: S \to \mathbb{F}$, deg(f), deg(g)< d and $|S|=100d$, then $\Pr_a[f(a)=g(a)]<1/100$
3. For H a multiplicative group: $Z_H(X)= X^{|H|}-1$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree d

Bob sends $P(X) \in \mathbb{F}[X]$, deg(P)<d to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with $P(a)$

Arithmetization Toy Problem

STARKWARE

Clm 3: I know $(a_0,\ldots,a_{|H|-1}) \in \{0,1\}^{|H|}$ s.t. $(b_0,\ldots,b_{|H|-1})$ satisfies
- $b_0 = b_1 = 1$ and $b_{|H|-1} = 42$ mod p
- $b_i = b_{i-2}^{\ 3} + a_i * b_{i-1}$

Challenge: Succinct protocol to verify Clm 3

Hint 1: Index sequences using g^i, for g generator of H

Hint 2: Use more than 1 constraint polynomial

Algebra Facts

For field $\mathbb{F}$, $H \subseteq \mathbb{F}$, let $Z_H(X) = \prod_{a \in H}(X-a)$

1. $\forall a \in H: P(a) = 0 \Leftrightarrow \exists\ Q(X): P(X) = Q(X) * Z_H(X)$, $\deg(Q) = \deg(P) - |H|$
2. If $f, g: S \to \mathbb{F}$, $\deg(f)$, $\deg(g) < d$ and $|S| = 100d$, then $\Pr_a[f(a) = g(a)] < 1/100$
3. For H a multiplicative group: $Z_H(X) = X^{|H|} - 1$

Ideal PCS functionality

Alice specifies field $\mathbb{F}$ and degree d

Bob sends $P(X) \in \mathbb{F}[X]$, $\deg(P) < d$ to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with $P(a)$

STARKWARE

From FRI to Polynomial Commitment Schemes

Eli Ben-Sasson

February 2023

Polynomial Commitment Scheme

STARKWARE

Ideal functionality

Alice specifies field $\mathbb{F}$ and degree d

Bob sends $P(X) \in \mathbb{F}[X]$, $\deg(P) < d$ to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with $P(a)$

Polynomial Commitment Scheme

STARKWARE

PCS for $\mathbb{F}$, degree *d*

Bob sends comm(P) to **Alice**

Alice queries **Bob** for $a \in \mathbb{F}$; **Bob** answers with *b*

Both interact, then **Alice** decides accept/reject

Want
- Completeness
- **Soundness:** Pr[Alice accepts b ≠ P(a)] < 2^{-128}
- **Efficiency:** proving time, verification, #rounds, ...

Ideal functionality

Alice specifies field $\mathbb{F}$ and degree *d*

Bob sends $P(X) \in \mathbb{F}[X]$, deg(*P*)<*d* to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with *P(a)*

Polynomial Commitment Scheme

STARKWARE

PCS for $\mathbb{F}$, degree *d*

Bob sends comm(P) to **Alice**

Alice queries **Bob** for $a \in \mathbb{F}$; **Bob** answers with *b*

Both interact, then **Alice** decides accept/reject

Want
- **Completeness**
- **Soundness:** Pr[Alice accepts b ≠ P(a)] < 2^{-128}
- **Efficiency:** proving time, verification, #rounds, ...
- **Succinctness:** verification time = polylog(d)
- **Security:** which crypto assumptions? PQ secure?
- **Universality:** all finite fields (and rings?)

Ideal functionality

Alice specifies field $\mathbb{F}$ and degree *d*

Bob sends $P(X) \in \mathbb{F}[X]$, deg(*P*)<*d* to **Tom** (trusted party)

Alice queries **Tom** for $a \in \mathbb{F}$ and **Tom** answers with *P(a)*

FRI - Fast Reed Solomon IOP of Proximity

STARKWARE

PCS for $\mathbb{F}$, degree *d*

Bob sends comm(P) to **Alice**

Alice queries **Bob** for $a \in \mathbb{F}$; **Bob** answers with *b*

Both interact, then **Alice** decides accept/reject

Want
- **Completeness**
- **Soundness:** Pr[Alice accepts b ≠ P(a)] < 2^{-128}
- **Efficiency:** proving time, verification, #rounds
- **Succinctness:** verification time = polylog(d)
- **Security:** which crypto assumptions? PQ secure?
- **Universality:** all finite fields (and rings?)

FRI [BBHR 2018]

Proving = O(d), verification, #rounds = O(log d)

PQ-secure under CRH (interactive), or Fiat-Shamir (noninteractive)

Yes! (for fields) [BCLK 22, EC-FFT/EC-FRI/EC-STARK]

FRI - Fast Reed Solomon IOP of Proximity

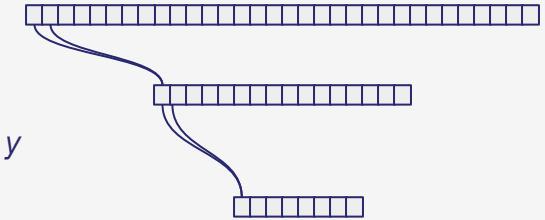
STARKWARE

Interactive Oracle Proof (IOP)
- Model that generalizes PCP and IP; equivalent to MIP
- **Bob (Prover)** provides oracle access to proof (like PCP)
- **Alice (Verifier)** sends randomness (like IP)
- **Prover** sends another oracle (based on prior history)
- **Verifier** sends more randomness,
- ...
- ...
- **Verifier** queries the oracles, based on answers decides accept/reject

FRI - Fast Reed Solomon IOP of Proximity

Interactive Oracle Proof (IOP) for the following problem:

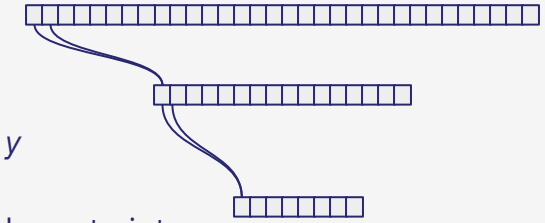
- Given $S_0 \subseteq \mathbb{F}$, $f_0 : S_0 \to \mathbb{F}$, Prover claim: $\deg(f_0) < |S_0|/16$
- Verifier sends $x_0 \in \mathbb{F}$
- Given $S_1 \subseteq \mathbb{F}$, $f_1 : S_1 \to \mathbb{F}$, Prover claim: $\deg(f_1) < |S_1|/16$
  where $f_1(y) = F(f_0(y'), f_0(y''), x_0)$; F fixed, y', y'' fixed given y
- ...



FRI - Fast Reed Solomon IOP of Proximity

Interactive Oracle Proof (IOP) for the following problem:

- Given $S_0 \subseteq \mathbb{F}$, $f_0 : S_0 \to \mathbb{F}$, Prover claim: $\deg(f_0) < |S_0|/16$
- Verifier sends $x_0 \in \mathbb{F}$
- Given $S_1 \subseteq \mathbb{F}$, $f_1 : S_1 \to \mathbb{F}$, Prover claim: $\deg(f_1) < |S_1|/16$
  where $f_1(y) = F(f_0(y'), f_0(y''), x_0)$; F fixed, y', y'' fixed given y
- ...
- Verifier picks random $y \in \mathbb{F}$ and "follows" path checking local constraints



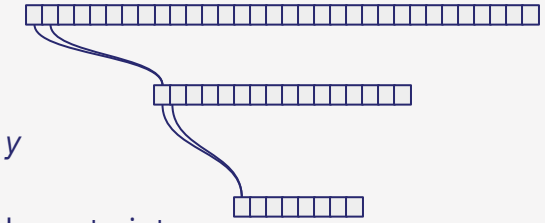
- **Efficiency:** Proof size < 2 $|S_0|$;
- **Succinctness:** Verification = $O(\log |S_0|) = O(\log d)$;
- **Perfect Completeness**
- **Knowledge Soundness [BCIKS20]:** If f_0 is accepted w.p. > ¼+0.001, can Extract P(X), $\deg(P) < |S_0|/16$ that agrees with f_0
- **Open question:** is soundness (or knowledge soundness) equal to rate (1/16) or to \sqrt(rate) (¼) ?

FRI - Fast Reed Solomon IOP of Proximity

STARKWARE

Interactive Oracle Proof (IOP) for the following problem:

- Given $S_0 \subseteq \mathbb{F}$, $f_0 : S_0 \to \mathbb{F}$, Prover claim: $\deg(f_0) < |S_0|/16$
- Verifier sends $x_0 \in \mathbb{F}$
- Given $S_1 \subseteq \mathbb{F}$, $f_1 : S_1 \to \mathbb{F}$, Prover claim: $\deg(f_1) < |S_1|/16$
  where $f_1(y) = F(f_0(y'), f_0(y''), x_0)$; F fixed, y', y'' fixed given y
- ...
- Verifier picks random $y \in \mathbb{F}$ and "follows" path checking local constraints



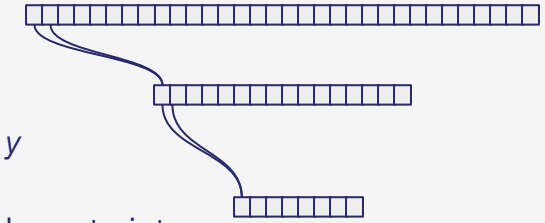
- **Efficiency:** Proof size < 2 $|S_0|$;
- **Succinctness:** Verification = $O(\log |S_0|) = O(\log d)$;
- **Perfect Completeness**
- **Knowledge Soundness [BCIKS20]:** If f_0 is accepted w.p. > ¼+0.001, can Extract P(X), $\deg(P) < |S_0|/16$ that agrees with f_0
- **Open question:** is soundness (or knowledge soundness) equal to rate (1/16) or to \sqrt(rate) (¼) ?

- **Concrete proof size:** ~10-100KB range (for $d \sim 2^{10}$-2^{40} range)

FRI - Fast Reed Solomon IOP of Proximity

Interactive Oracle Proof (IOP) for the following problem:

- Given $S_0 \subseteq \mathbb{F}$, $f_0 : S_0 \to \mathbb{F}$, Prover claim: $\deg(f_0) < |S_0|/16$
- Verifier sends $x_0 \in \mathbb{F}$
- Given $S_1 \subseteq \mathbb{F}$, $f_1 : S_1 \to \mathbb{F}$, Prover claim: $\deg(f_1) < |S_1|/16$
  where $f_1(y) = F(f_0(y'), f_0(y''), x_0)$; F fixed, y', y'' fixed given y
- ...
- Verifier picks random $y \in \mathbb{F}$ and "follows" path checking local constraints



PCS based on FRI?

- Prover commits to $f : S \to \mathbb{F}$
- Verifier queries a, prover answers b
- Both parties run FRI on $f_0 : S_0 \to \mathbb{F}$ defined by $f_0(x) := (f(x)-b)/(x-a)$