STARKWARE STARK 101

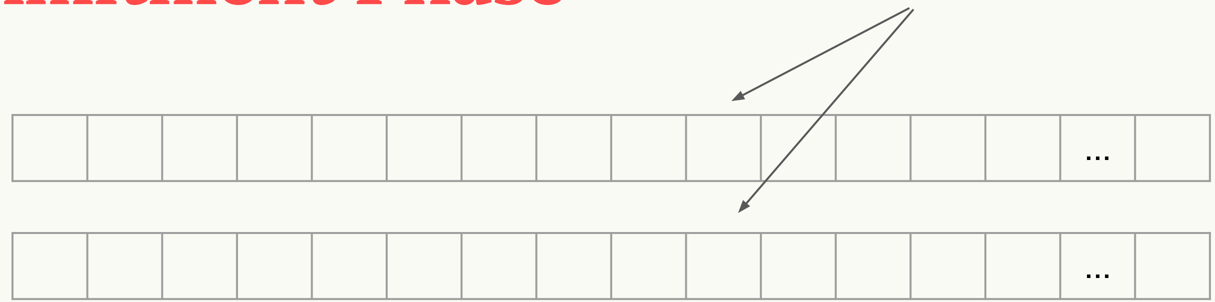
# Stark 101: Part 4

## Fri Queries

# The Entire Proof

- Commitment
- Decommitment

# Commitment Phase

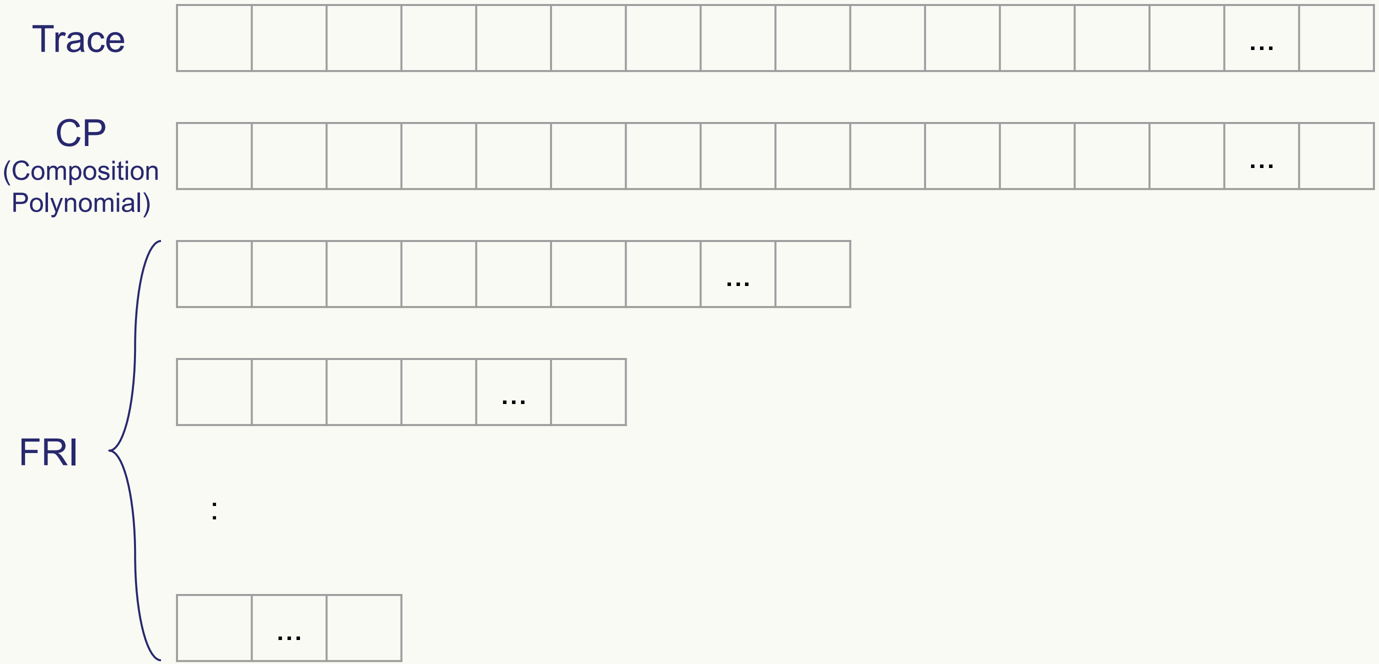


**Commitment**

Trace Root

CP Root

# Commitment Phase



## Commitment

Trace Root

CP Root

$\text{CP}_1$ Root

$\text{CP}_2$ Root

:

$\text{CP}_{10}$ Root

# The Entire Proof

- Commitment Done!

- Decommitment (Persuading)

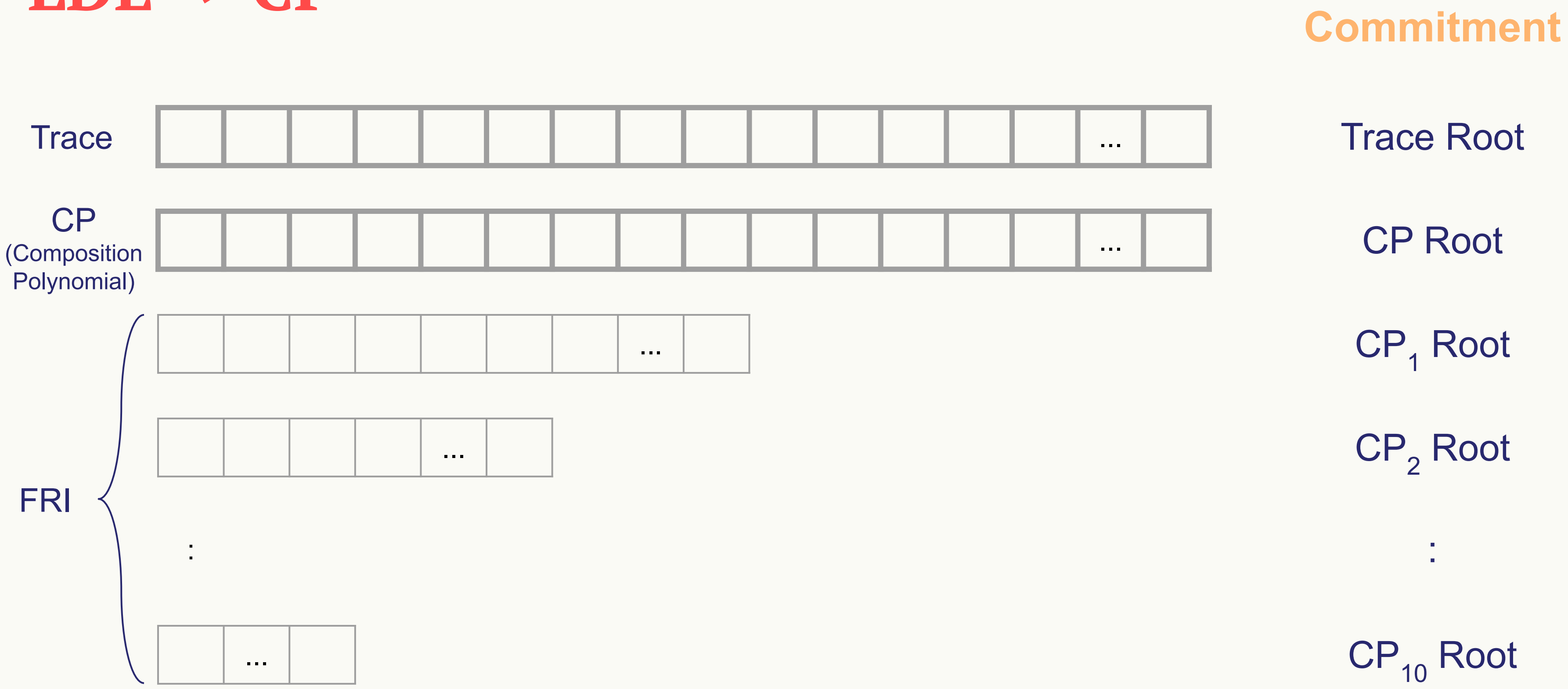
# The Entire Proof

- Commitment

Done!

- Decommitment
  - Get q random elements, provide proof for each.

# LDE -> CP



Commitment

Trace ... Trace Root

CP (Composition Polynomial) ... CP Root

FRI

... $CP_1$ Root

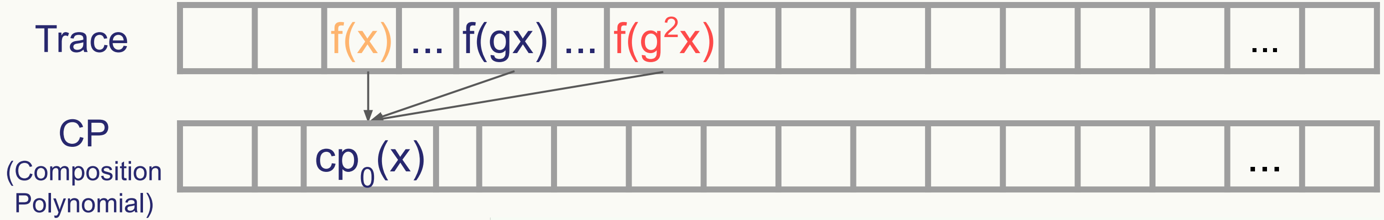
... $CP_2$ Root

: :

... $CP_{10}$ Root

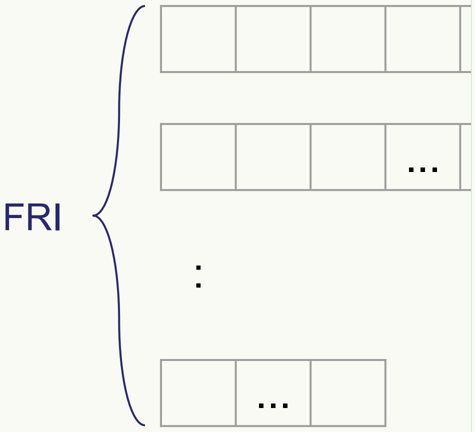
# LDE -> CP

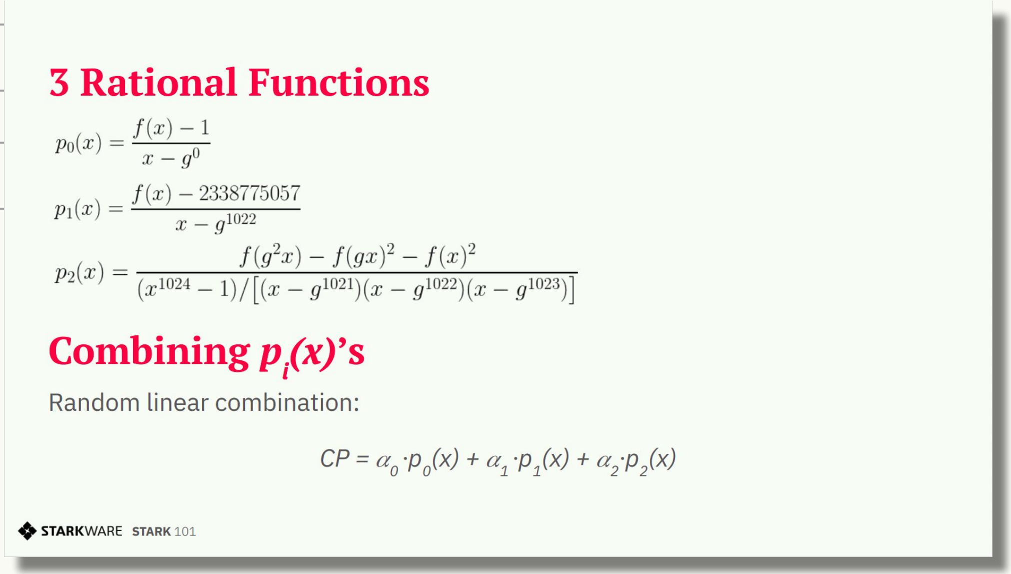
Commitment



Trace Root

CP Root





## 3 Rational Functions

$$p_0(x) = \frac{f(x) - 1}{x - g^0}$$

$$p_1(x) = \frac{f(x) - 2338775057}{x - g^{1022}}$$

$$p_2(x) = \frac{f(g^2x) - f(gx)^2 - f(x)^2}{(x^{1024} - 1)/\left[(x - g^{1021})(x - g^{1022})(x - g^{1023})\right]}$$

## Combining $p_i(x)$'s

Random linear combination:

$$CP = \alpha_0 \cdot p_0(x) + \alpha_1 \cdot p_1(x) + \alpha_2 \cdot p_2(x)$$

STARKWARE STARK 101

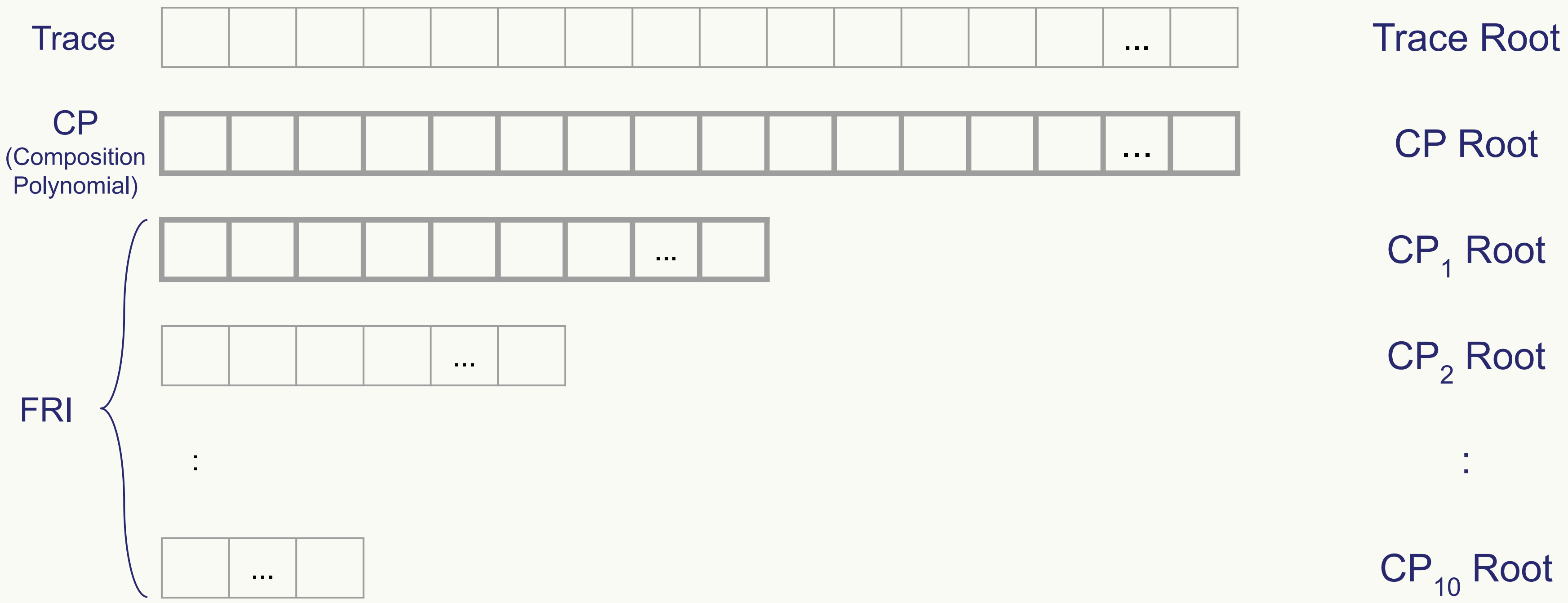
$CP_1$ Root

$CP_2$ Root

:

$CP_{10}$ Root

# FRI Step


Commitment
Trace
...
Trace Root
CP
(Composition Polynomial)
...
CP Root
...
$CP_1$ Root
...
$CP_2$ Root
FRI
:
:
...
$CP_{10}$ Root

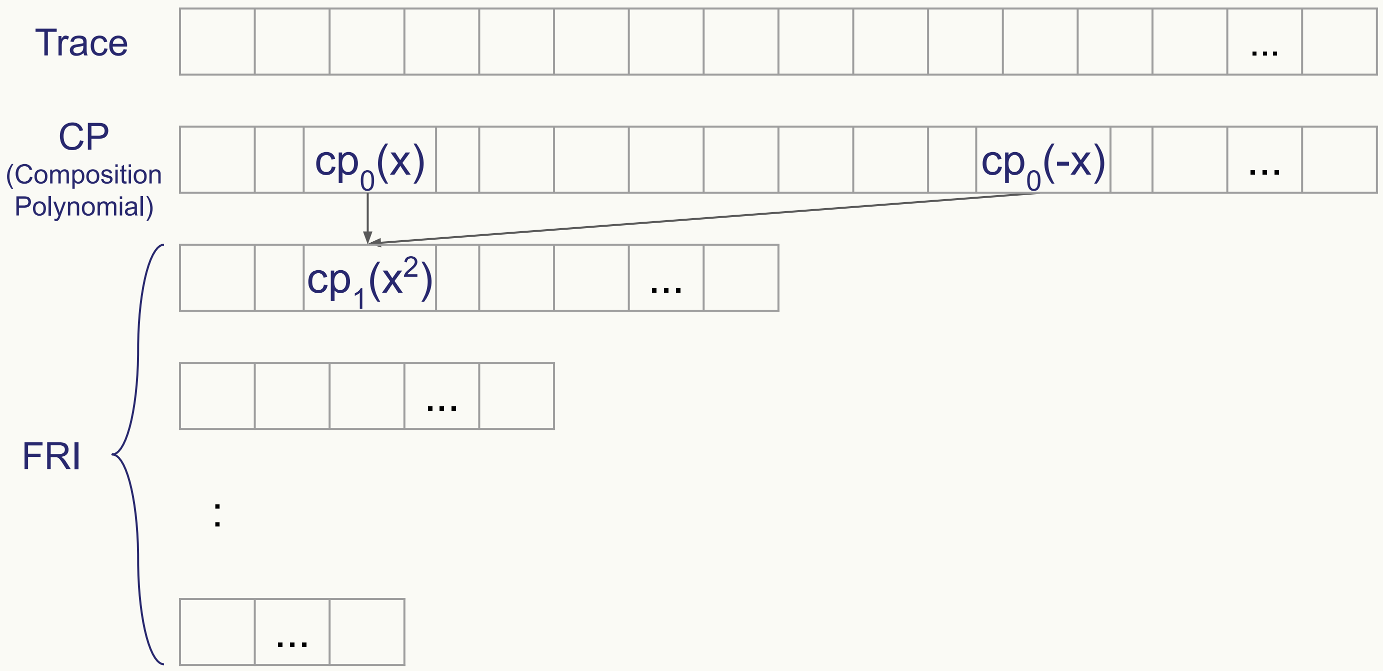
# FRI Step

$$\begin{cases} CP_i(x)=g(x^2)+xh(x^2) \\ CP_i(-x)=g(x^2)-xh(x^2) \end{cases} \longrightarrow \begin{cases} g(x^2)=\dfrac{CP_i(x)+CP_i(-x)}{2} \\ h(x^2)=\dfrac{CP_i(x)-CP_i(-x)}{2x} \end{cases}$$

$$CP_i(x)=g(x^2)+xh(x^2) \qquad CP_i(-x)=g(x^2)-xh(x^2)$$

$$CP_{i+1}(x^2)=g(x^2)+\beta_i h(x^2)$$

# Decommitment Phase (for query x)



**Commitment**

Trace Root

CP Root

$CP_1$ Root

$CP_2$ Root

:

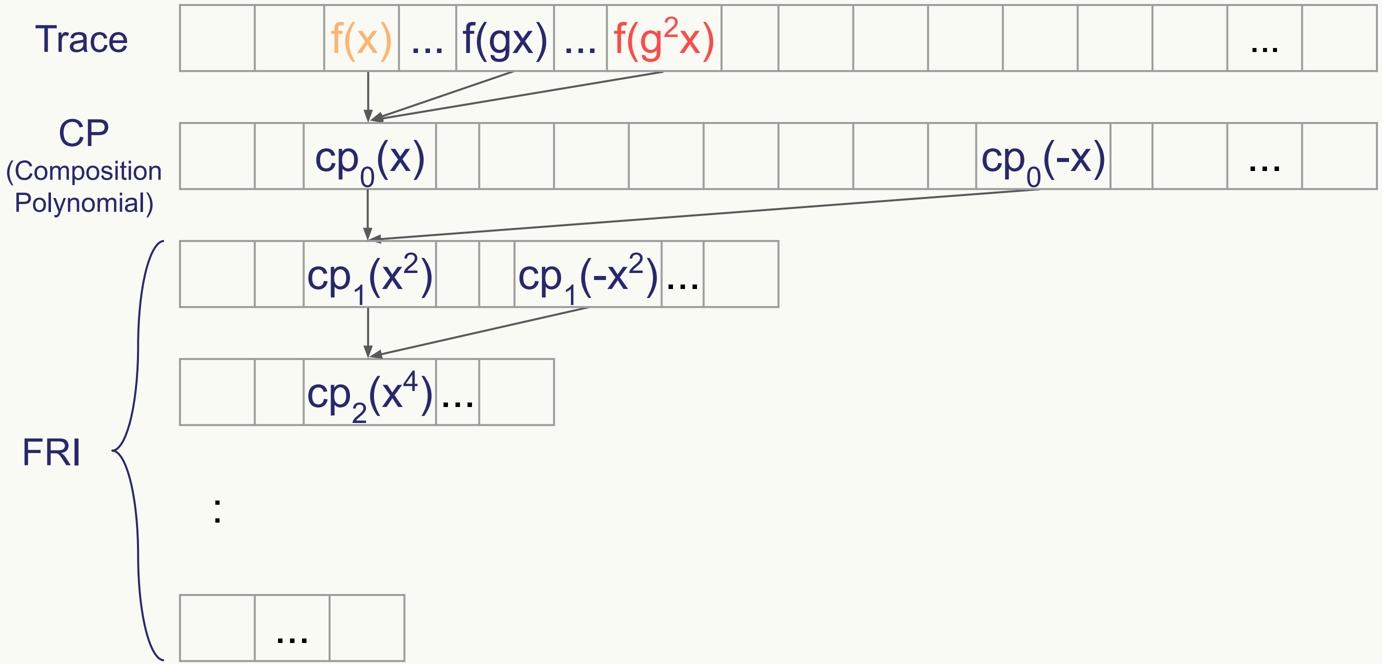
$CP_{10}$ Root

# The Entire Proof

- Commitment Done!

- Decommitment
  - Get q random elements, provide proof for each.

# Decommitment Phase (for query x)



Trace

$f(x)$ ... $f(gx)$ ... $f(g^2x)$ ...

CP

(Composition Polynomial)

$cp_0(x)$ $cp_0(-x)$ ...

FRI

$cp_1(x^2)$ $cp_1(-x^2)$ ...

$cp_2(x^4)$ ...

:

...

## Decommitment

$f(x)$ + path

$f(gx)$ + path

$f(g^2x)$ + path

$cp_0(x)$ + path

$cp_0(-x)$ + path

$cp_1(x^2)$ + path

$cp_1(-x^2)$ + path

$cp_2(x^4)$ + path

$cp_2(-x^4)$ + path

:

$cp_{10}(x^{1024})$ + path

# The Entire Proof

- Commitment

Done!

- Decommitment
  - Get q random elements.
  - Provide proof for each.

Done!

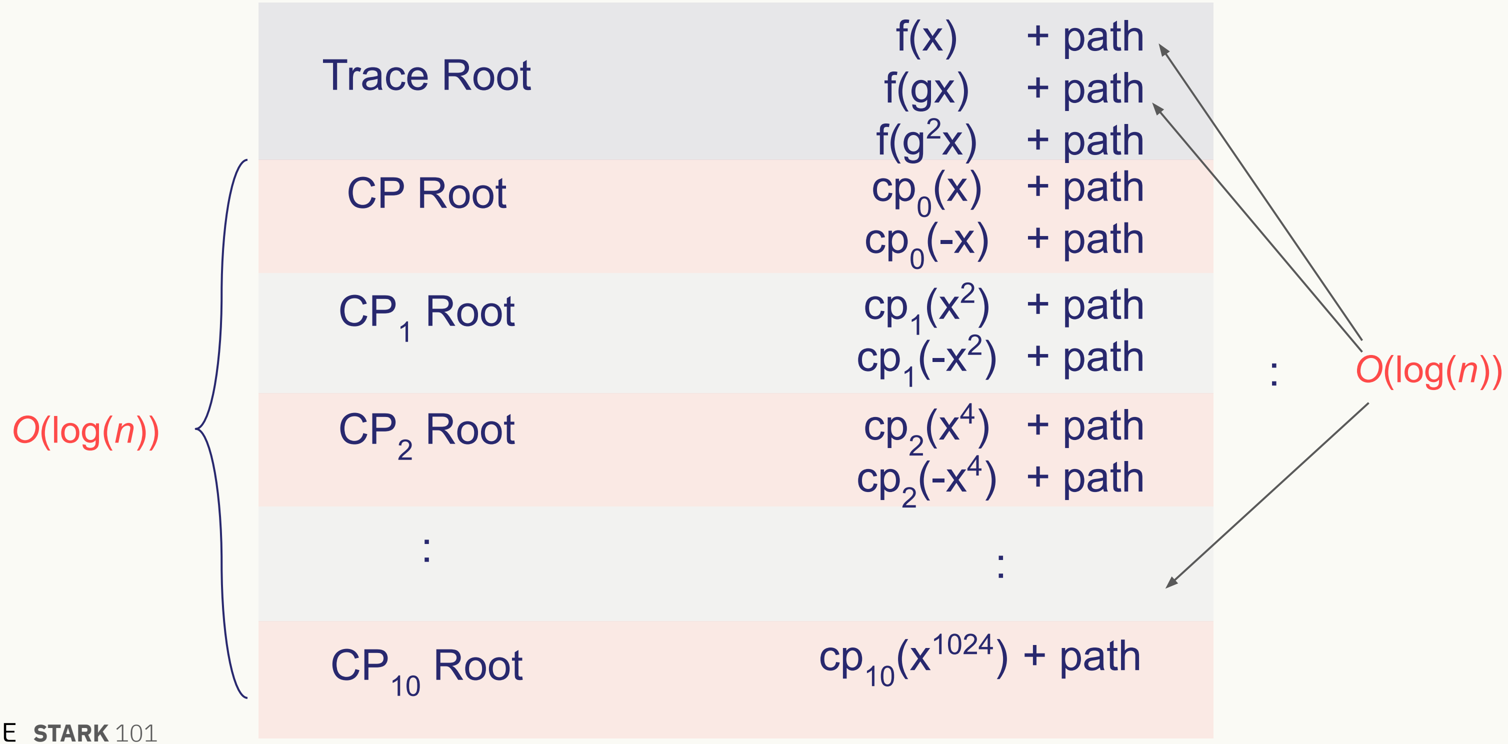
# Summary and Proof Length

| Commitment | Decommitment<br>(for one query) |
|---|---|
| Trace Root | $f(x)$ + path<br>$f(gx)$ + path<br>$f(g^2x)$ + path |
| CP Root | $cp_0(x)$ + path<br>$cp_0(-x)$ + path |
| $CP_1$ Root | $cp_1(x^2)$ + path<br>$cp_1(-x^2)$ + path |
| $CP_2$ Root | $cp_2(x^4)$ + path<br>$cp_2(-x^4)$ + path |
| : | : |
| $CP_{10}$ Root | $cp_{10}(x^{1024})$ + path |

$O(\log(n))$

$n$ = trace length

# Summary and Proof Length



| Commitment | Decommitment<br>(for one query) |
|---|---|
| Trace Root | $f(x)$ + path<br>$f(gx)$ + path<br>$f(g^2x)$ + path |
| CP Root | $cp_0(x)$ + path<br>$cp_0(-x)$ + path |
| $CP_1$ Root | $cp_1(x^2)$ + path<br>$cp_1(-x^2)$ + path |
| $CP_2$ Root | $cp_2(x^4)$ + path<br>$cp_2(-x^4)$ + path |
| : | : |
| $CP_{10}$ Root | $cp_{10}(x^{1024})$ + path |

# Summary and Proof Length

| Commitment | Decommitment<br>(for one query) |
|---|---|
| Trace Root | $f(x)$ + path<br>$f(gx)$ + path<br>$f(g^2x)$ + path |
| CP Root | $cp_0(x)$ + path<br>$cp_0(-x)$ + path |
| $CP_1$ Root | $cp_1(x^2)$ + path<br>$cp_1(-x^2)$ + path |
| $CP_2$ Root | $cp_2(x^4)$ + path<br>$cp_2(-x^4)$ + path |
| : | : |
| $CP_{10}$ Root | $cp_{10}(x^{1024})$ + path |

$O(\log^2(n))$

# Summary and Proof Length

| Commitment | Decommitment for q queries | | | | |
|---|---|---|---|---|---|
| Trace Root | $f(x)$<br>$f(gx)$<br>$f(g^2x)$ | + path<br>+ path<br>+ path | | $f(x)$<br>$f(gx)$<br>$f(g^2x)$ | + path<br>+ path<br>+ path |
| CP Root | $cp_0(x)$<br>$cp_0(-x)$ | + path<br>+ path | | $cp_0(x)$<br>$cp_0(-x)$ | + path<br>+ path |
| $CP_1$ Root | $cp_1(x^2)$<br>$cp_1(-x^2)$ | + path<br>+ path | ... | $cp_1(x^2)$<br>$cp_1(-x^2)$ | + path<br>+ path |
| $CP_2$ Root | $cp_2(x^4)$<br>$cp_2(-x^4)$ | + path<br>+ path | | $cp_2(x^4)$<br>$cp_2(-x^4)$ | + path<br>+ path |
| : | : | | | : | |
| $CP_{10}$ Root | $cp_{10}(x^{1024})$ | + path | | $cp_{10}(x^{1024})$ | + path |

$O(\log^2(n))$

# Thanks!