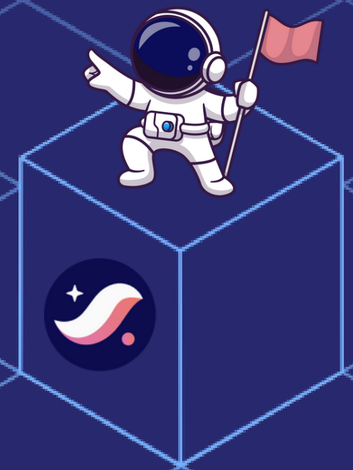
STARKWARE

Nadai Carlos

Sesión 3: Las matemáticas detrás de las STARKs

- 4 de Mayo del 2023

Stark 101: Parte 4



@Nadai02010

https://github.com/Nadai2010

@0xhasher_

https://github.com/cliraa

Recapitulemos

Compromiso

Raíz de la traza

Recapitulemos

Compromiso

Raíz de la traza

Raíz *CP*

Recapitulemos

Compromiso

Raíz de la traza

Raíz *CP*

Raíz CP_1

Raíz CP_2

:

Raíz CP_{10}

La Prueba Completa

Compromiso

- Descompromiso (Convenciendo)

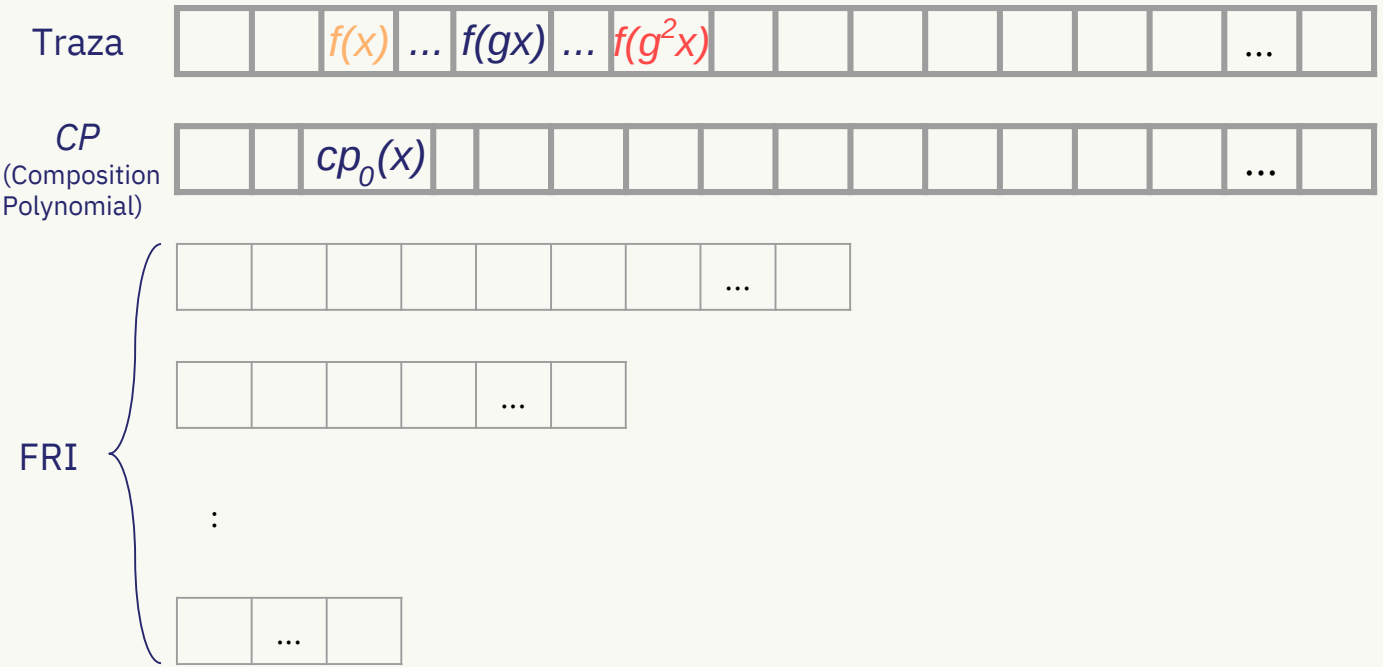
¿Cómo puede el Probador convencer al Verificador?

Verificador: Envía elementos q random

Probador: Proporciona datos de validación para cada uno

¿Qué son los datos de validación?

Traza -> *CP*



Compromiso

Raíz de la traza

Raíz *CP*

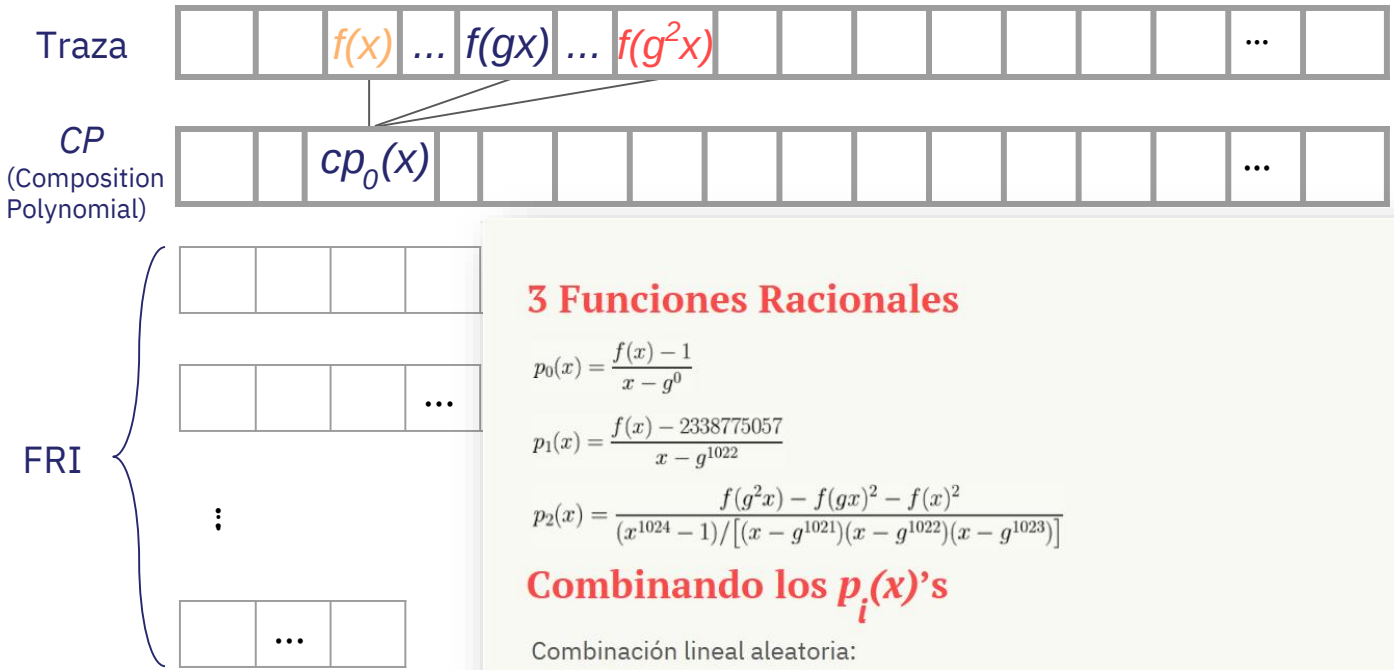
Raíz CP_1

Raíz CP_2

:

Raíz CP_{10}

Traza -> *CP*



3 Funciones Racionales

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

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

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

Combinando los $p_i(x)$'s

Combinación lineal aleatoria:

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

STARKWARE STARK 101

Compromiso

Raíz de la traza

Raíz *CP*

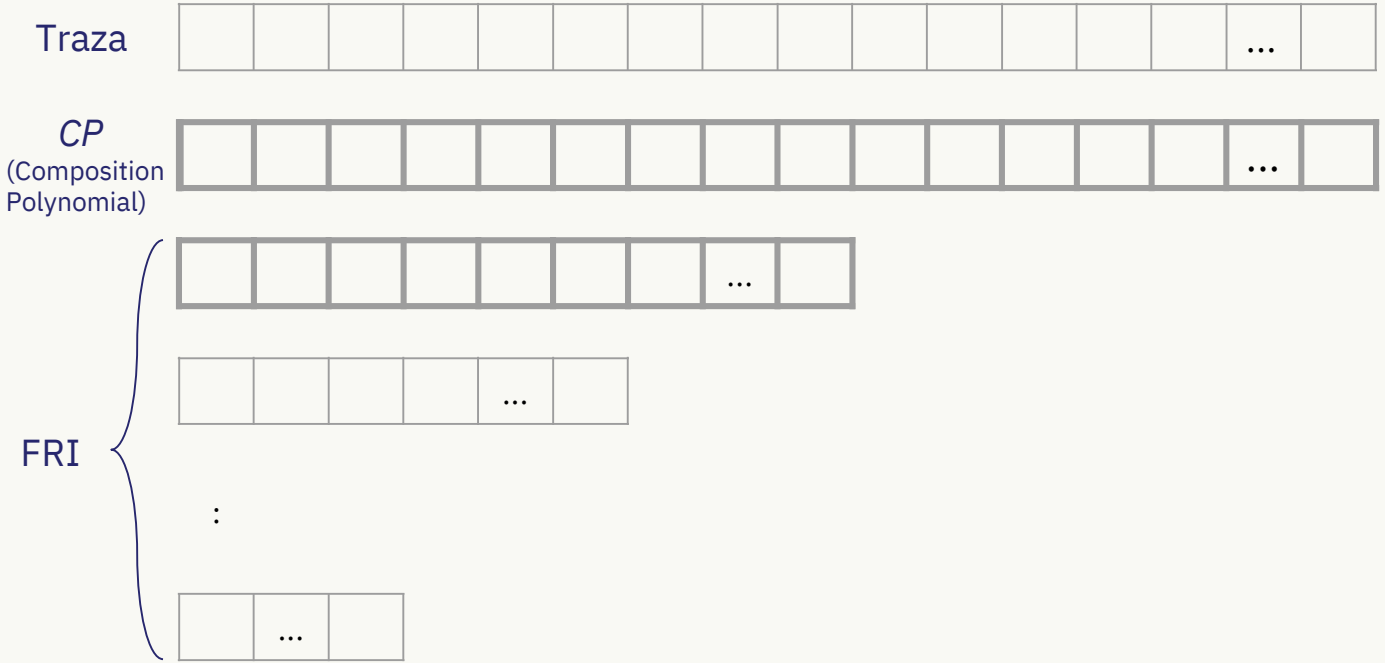
Raíz CP_1

Raíz CP_2

:

Raíz CP_{10}

FRI - Pasos



Compromiso

Raíz de la traza

Raíz *CP*

Raíz CP_1

Raíz CP_2

:

Raíz CP_{10}

FRI - Pasos

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

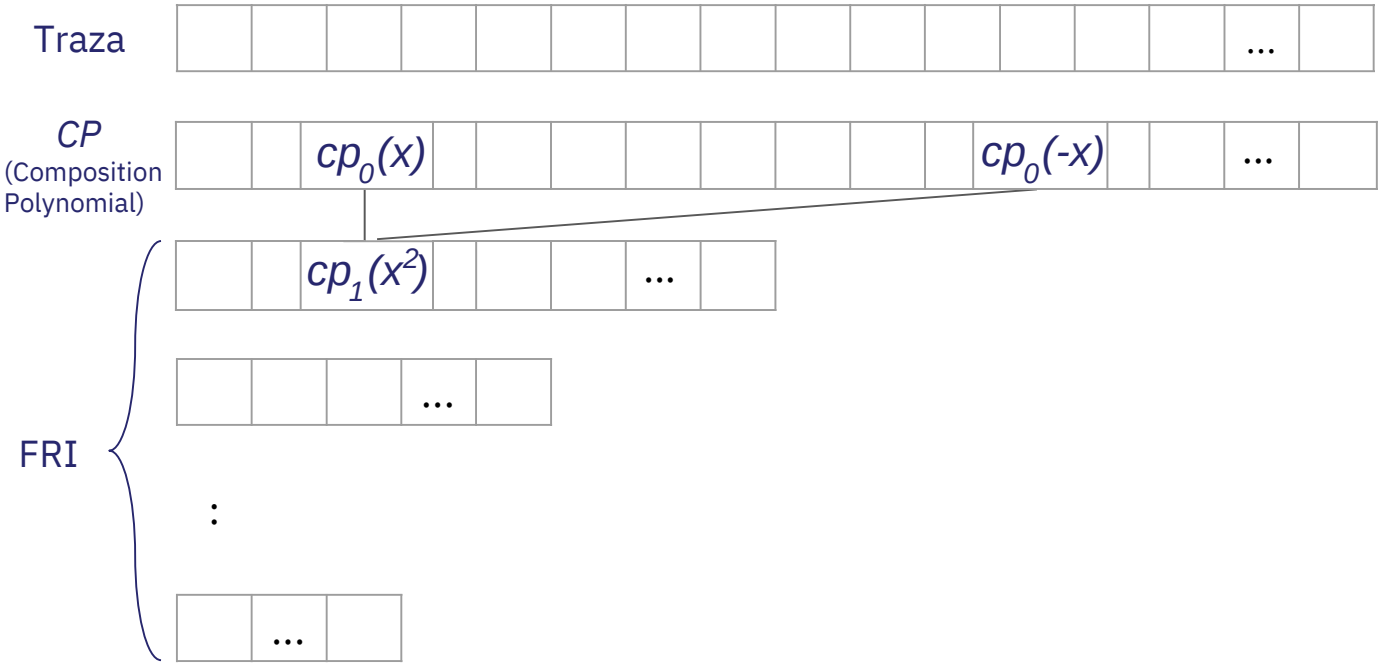
Recuerde:

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

En resumen:

Para calcular $\boldsymbol{CP_{i+1}(x^2)}$ *sólo necesitamos* $\boldsymbol{CP_i(x)}$ *y* $\boldsymbol{CP_i(-x)}$

FRI - Pasos



Compromiso

Raíz de la traza

Raíz *CP*

Raíz CP_1

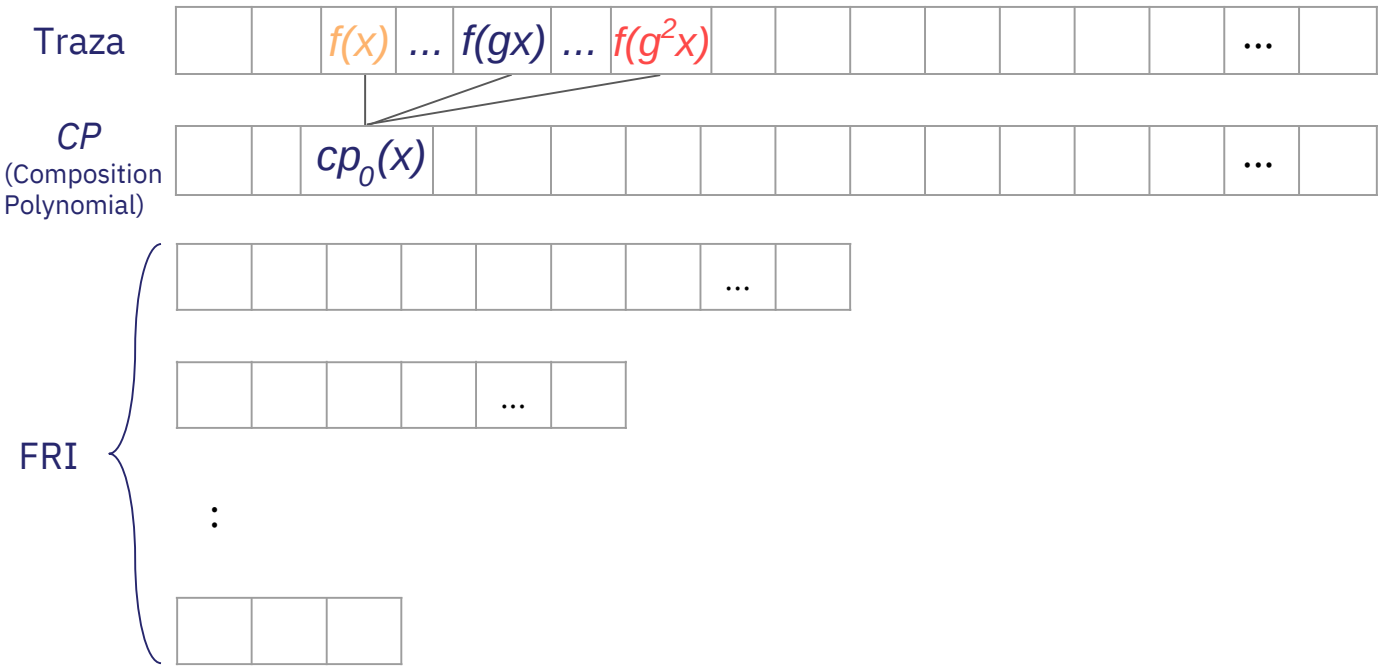
Raíz CP_2

:

Raíz CP_{10}

Fase de Descompromiso (para la consulta x)

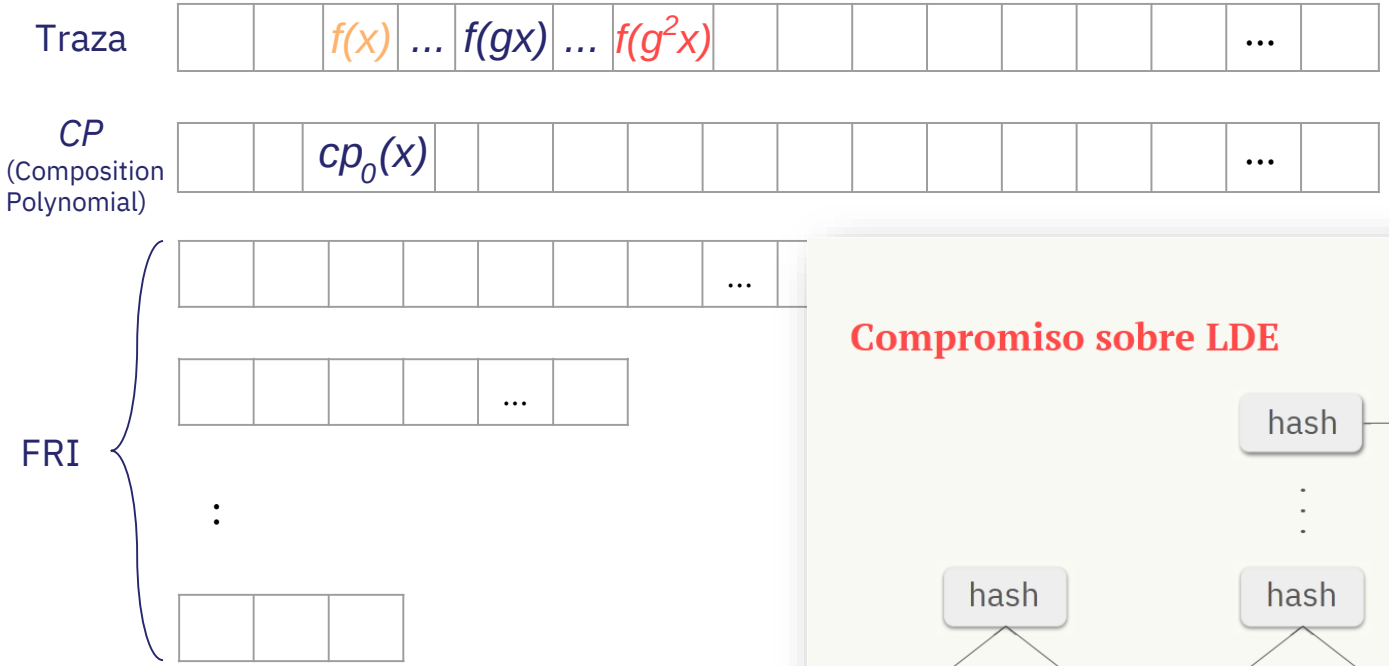
Fase de Descompromiso (para la consulta x)



Descompromiso

$f(x)$	+ ruta
$f(gx)$	+ ruta
$f(g^2x)$	+ ruta
$cp_0(x)$	+ ruta

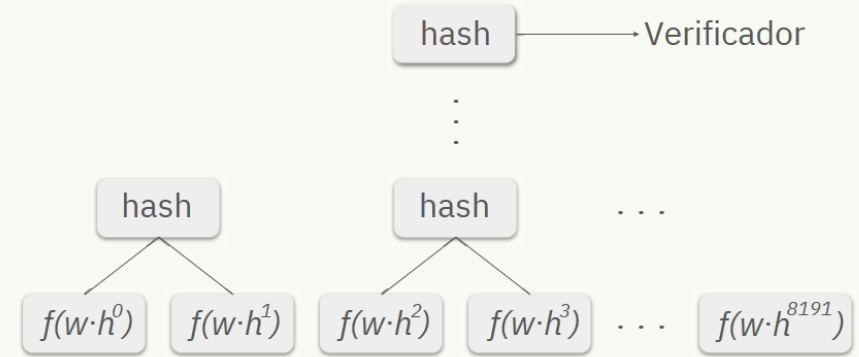
Fase de Descompromiso (para la consulta x)



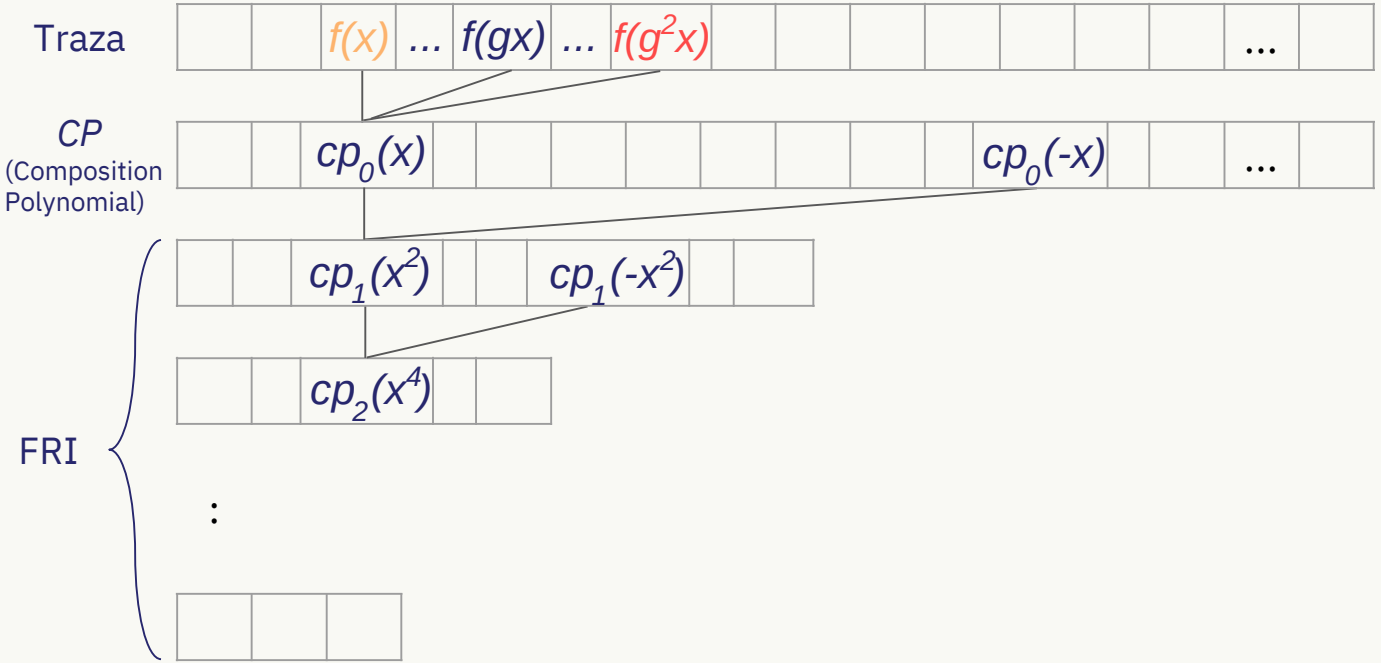
Descompromiso

$f(x)$	+ ruta
$f(gx)$	+ ruta
$f(g^2x)$	+ ruta
$cp_0(x)$	+ ruta

Compromiso sobre LDE



Fase de Descompromiso (para la consulta x)



Descompromiso

$f(x)$	+ ruta
$f(gx)$	+ ruta
$f(g^2x)$	+ ruta
$cp_0(x)$	+ ruta
$cp_0(-x)$	+ ruta
$cp_1(x^2)$	+ ruta
$cp_1(-x^2)$	+ ruta
$cp_2(x^4)$	+ ruta
$cp_2(-x^4)$	+ ruta
:	
$cp_{10}(x^{1024})$	+ ruta

La Prueba Completa

Compromiso

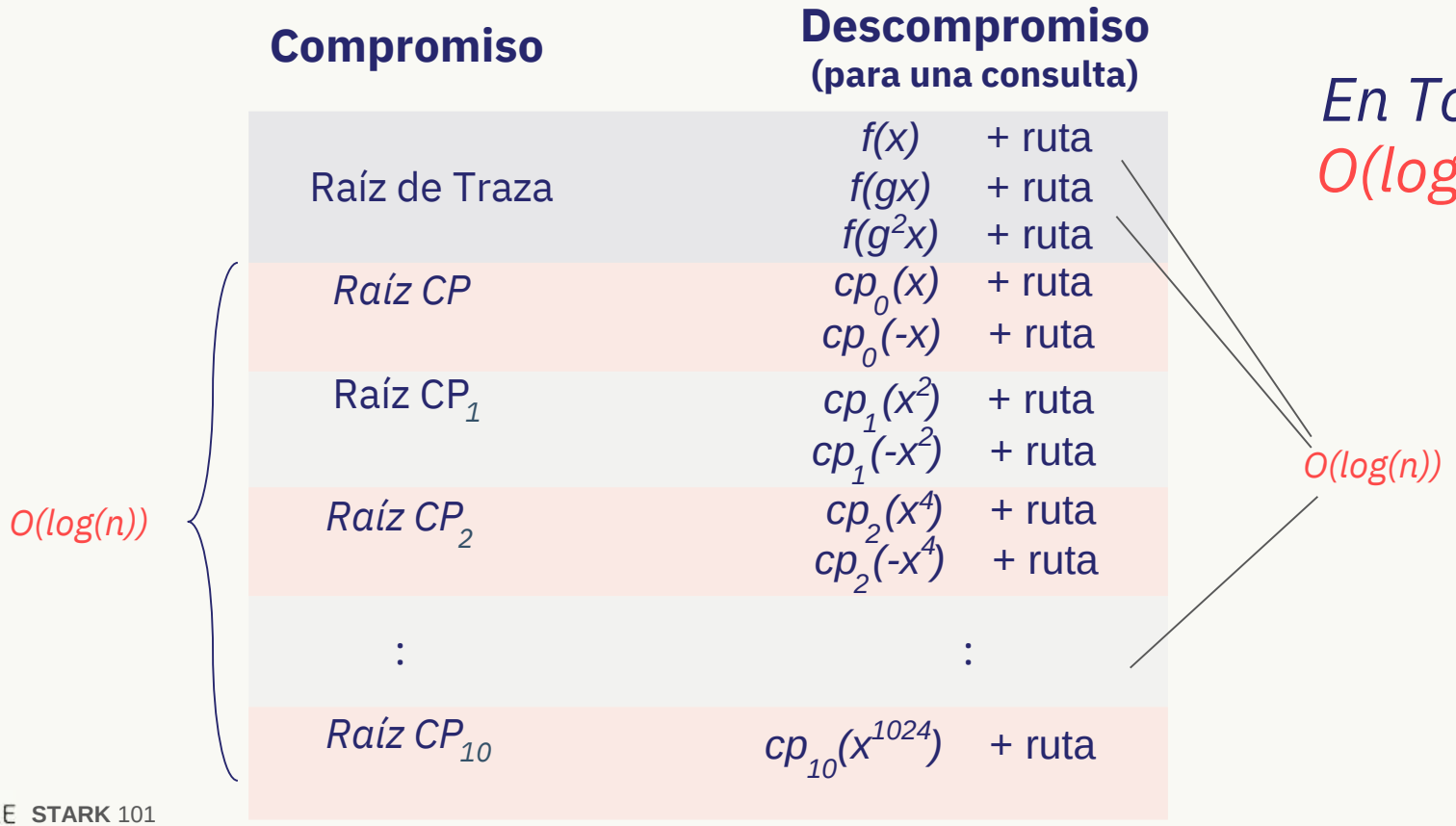
Descompromiso

- Obtener elementos q random
- Proporcionar datos de validación para cada uno

Longitud de la prueba

	Compromiso	Descompromiso (para una consulta)
	Raíz de Traza	$f(x)$ + ruta $f(gx)$ + ruta $f(g^2x)$ + ruta
$O(\log(n))$ n = longitud de traza (1023)	*Raíz CP*	$cp_0(x)$ + ruta $cp_0(-x)$ + ruta
	Raíz CP_1	$cp_1(x^2)$ + ruta $cp_1(-x^2)$ + ruta
	Raíz CP_2	$cp_2(x^4)$ + ruta $cp_2(-x^4)$ + ruta
	:	:
	Raíz CP_{10}	$cp_{10}(x^{1024})$ + ruta

Longitud de la prueba



Longitud de Prueba

Compromiso	Descompromiso (para q consultas)				
Raíz de Traza	$f(x)$	+ ruta		$f(x)$	+ ruta
	$f(gx)$	+ ruta		$f(gx)$	+ ruta
	$f(g^2x)$	+ ruta		$f(g^2x)$	+ ruta
Raíz CP	$cp_0(x)$	+ ruta		$cp_0(x)$	+ ruta
	$cp_0(-x)$	+ ruta		$cp_0(-x)$	+ ruta
Raíz CP_1	$cp_1(x^2)$	+ ruta		$cp_1(x^2)$	+ ruta
	$cp_1(-x^2)$	+ ruta	...	$cp_1(-x^2)$	+ ruta
Raíz CP_2	$cp_2(x^4)$	+ ruta		$cp_2(x^4)$	+ ruta
	$cp_2(-x^4)$	+ ruta		$cp_2(-x^4)$	+ ruta
:	:			:	
Raíz CP_{10}	$cp_{10}(x^{1024})$	+ ruta		$cp_{10}(x^{1024})$	+ ruta

$O(log^2(n))$

STARKWARE

Y ahora - Última parte del código.

Después de eso…

Se convertirá en un experto en STARK

Gracias!