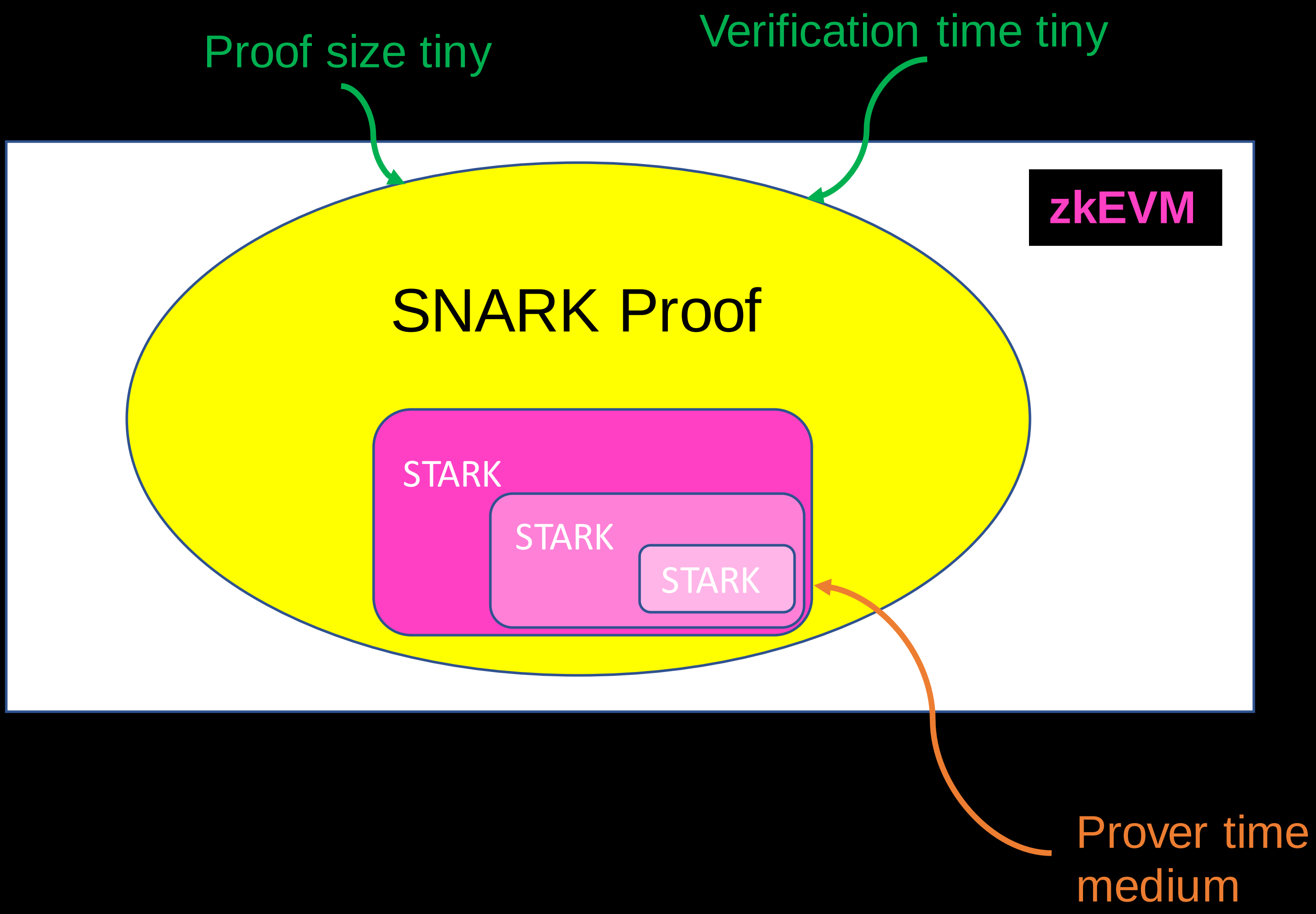
How Custom Gates are Used During Arithmetisation

The 13th BIU Winter School on Cryptography

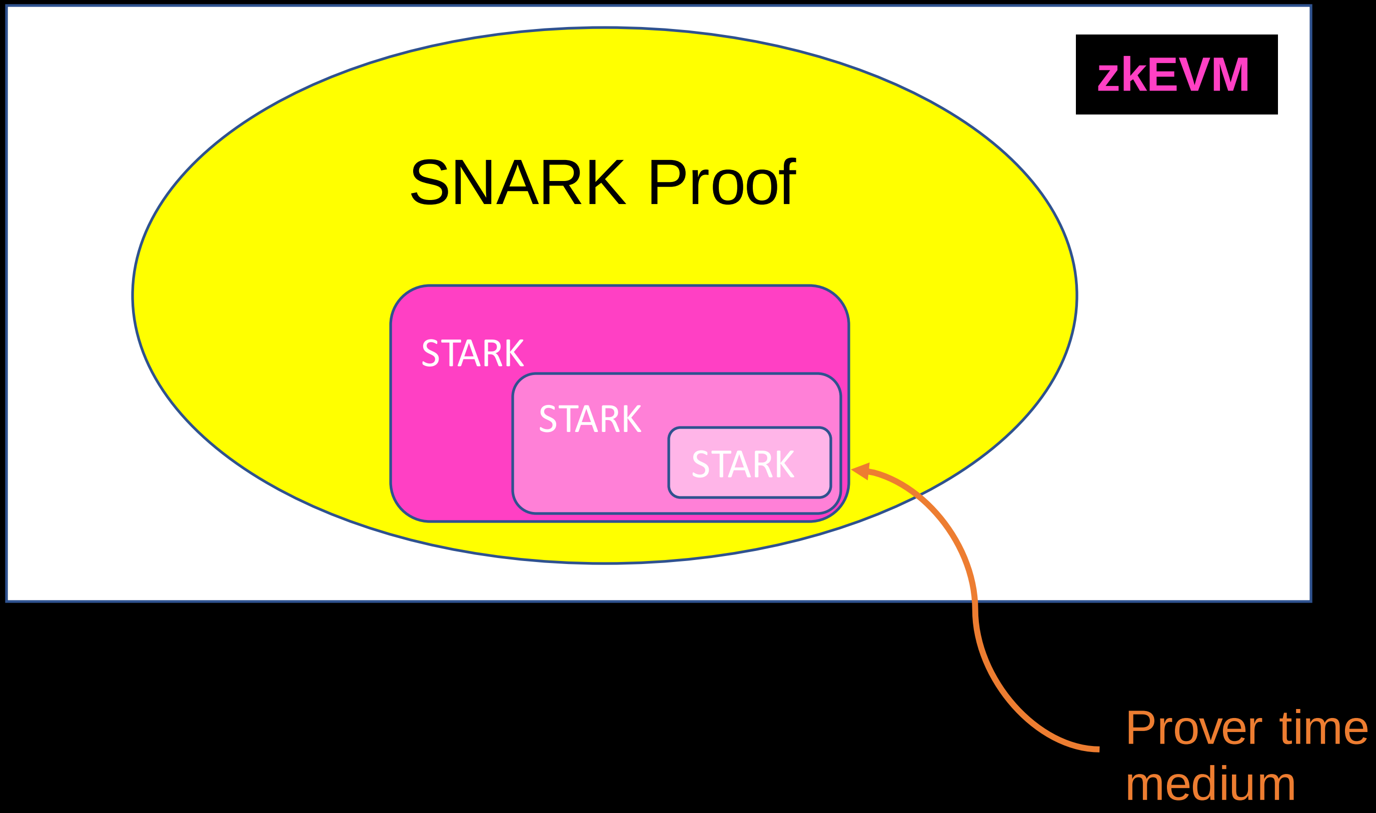
Mary Maller, Ethereum Foundation and PQShield, February 2023, Tel-Aviv

Prover Time is an important Bottleneck



Prover Time is an important Bottleneck

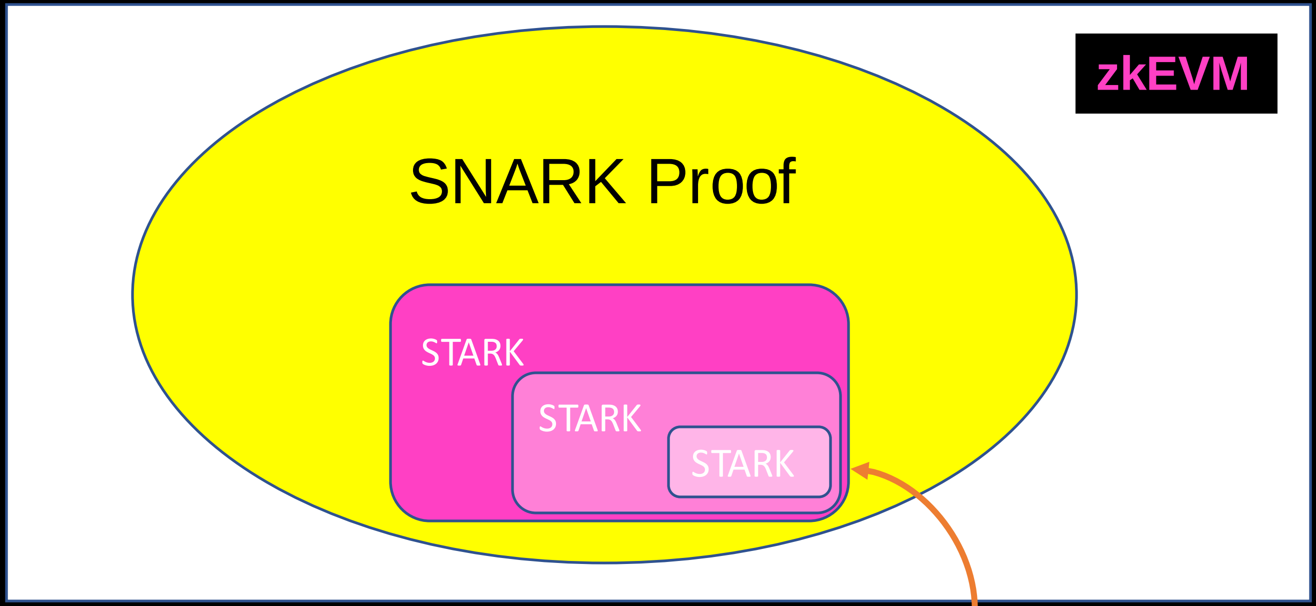
Prover time directly depends on computation size.



Prover Time is an important Bottleneck

Constants matter

Prover time directly depends on computation size.



Prover time medium

Prover Time is an important Bottleneck

Constants matter

Prover time directly depends on computation size.

$$y = x^{-1} \mod p$$

Option 1

$$x_2 = x \times x \mod p$$

$$x_4 = x_2 \times x_2 \mod p$$

$$\cdots$$

$$x_n = x_{n-1} \times x_{n-1} \mod p$$

$$y = \sum_{i=1}^{n} b_i x_i \mod p$$

- Fermat's little theorem x^{-1} = x^{p-2} mod p
- Compute x^{p-2} using double and add
- Check that y = x^{p-2}
- Costs log(p) constraints

Prover Time is an important Bottleneck

Constants matter

Prover time directly depends on computation size.

$$y = x^{-1} \mod p$$

Option 1

$$x_2 = x \times x \mod p$$

$$x_4 = x_2 \times x_2 \mod p$$

$$\cdots$$

$$x_n = x_{n-1} \times x_{n-1} \mod p$$

$$y = \sum_{i=1}^{n} b_i x_i \mod p$$

Option 2

$$1 = x \times y \mod p$$

Costs either log(p) constraints or 1 constraint depending on *arithmetisation* strategy.

Prover Time is an important Bottleneck

Constants matter

Prover time directly depends on computation size.

$$y = x^{-1} \mod p$$

Option 1
$x_2 = x \times x \mod p$
$x_4 = x_2 \times x_2 \mod p$
$\cdots$
$x_n = x_{n-1} \times x_{n-1} \mod p$
$y = \sum_{i=1}^{n} b_i x_i \mod p$

Option 2
$1 = x \times y \mod p$

Costs either log(p) constraints or 1 constraint depending on *arithmetisation* strategy.

Objectives

- Previously, discussed how the Plonk proving system worked finishing with the Plonkish arithmetisation system.

- Today, a closer look at the Plonkish arithmetisation system

  - Addition and multiplication constraints
  - Copy constraints
  - Selector polynomials
  - Custom constraints
  - Lookup constraints

A Simple Constraint System

If we just have multiplications?

Hard.. Impossible?

Prove that $0 =< c_3 < 4$?

$$a_1 \times b_1 = c_1$$

$$a_2 \times b_2 = c_2$$

$$a_3 \times b_3 = c_3$$

A Simple Constraint System

Multiplications and additions?

Prove that $0 =< c_3 < 4$?

$$a_1 \times b_1 = 0 \qquad a_1 + b_1 = 1$$

$$a_2 \times b_2 = 0 \qquad a_2 + b_2 = 1$$

$$a_3 \times b_3 = c_3 \qquad a_3 + b_3 = c_3$$

A Simple Constraint System

Prove that 0 =< c_3 < 4 ?

Multiplications and additions?

$$a_1 \times b_1 = 0 \qquad a_1 + b_1 = 1$$

$$a_2 \times b_2 = 0 \qquad a_2 + b_2 = 1$$

$$a_3 \times b_3 = c_3 \qquad a_3 + b_3 = c_3$$

Want $a_1 \in \{0,1\}$, $a_2 \in \{0,1\}$, $c_3 = a_1 + 2a_2$

Binary decomposition.

A Simple Constraint System

Prove that $0 =< c_3 < 4$?

Multiplications and additions?

$\Rightarrow b_1 = (1 - a_1)$

$$a_1 \times b_1 = 0 \qquad a_1 + b_1 = 1$$

$$a_2 \times b_2 = 0 \qquad a_2 + b_2 = 1$$

$$a_3 \times b_3 = c_3 \qquad a_3 + b_3 = c_3$$

A Simple Constraint System

Prove that 0 =< c_3 < 4 ?

Multiplications and additions?

$\Rightarrow a_1(1-a_1) = 0$

$\Rightarrow b_1 = (1-a_1)$

a_1	$\times$	b_1	$=$	0
a_2	$\times$	b_2	$=$	0
a_3	$\times$	b_3	$=$	c_3

a_1	$+$	b_1	$=$	1
a_2	$+$	b_2	$=$	1
a_3	$+$	b_3	$=$	c_3

A Simple Constraint System

Multiplications and additions?

Prove that $0 =< c_3 < 4$?

$\Rightarrow a_1(1-a_1) = 0 \Rightarrow a_1 \in \{0,1\}$

$\Rightarrow b_1 = (1-a_1)$

$$a_1 \times b_1 = 0 \qquad a_1 + b_1 = 1$$

$$a_2 \times b_2 = 0 \qquad a_2 + b_2 = 1$$

$$a_3 \times b_3 = c_3 \qquad a_3 + b_3 = c_3$$

A Simple Constraint System

Prove that $0 =< c_3 < 4$?

Multiplications and additions?

$\Rightarrow a_1(1-a_1) = 0 \Rightarrow a_1 \in \{0,1\}$

$\Rightarrow b_1 = (1-a_1)$

a_1	$\times$	b_1	$=$	0	a_1	$+$	b_1	$=$	1
a_2	$\times$	b_2	$=$	0	a_2	$+$	b_2	$=$	1
a_3	$\times$	b_3	$=$	c_3	a_3	$+$	b_3	$=$	c_3

$a_2 \in \{0,1\}$

A Simple Constraint System

Prove that $0 =< c_3 < 4$?

Multiplications and additions?

Not enough structure?

$\Rightarrow a_1(1-a_1) = 0 \Rightarrow a_1 \in \{0,1\}$

$\Rightarrow b_1 = (1-a_1)$

$a_1 \times b_1 = 0$

$a_2 \times b_2 = 0$

$a_3 \times b_3 = c_3$

$a_1 + b_1 = 1$

$a_2 + b_2 = 1$

$a_3 + b_3 = c_3$

$a_2 \in \{0,1\}$

Do <u>not</u> imply $c_3 = a_1 + 2a_2$

A Simple Constraint System

Prove that $0 =< c_3 < 4$?

Multiplications and additions and **copy**?

$a_4 = a_1$

$b_4 = b_1$

$c_4 = 1$

$c_1 = 0$

$a_1 \times b_1 = c_1$

$a_2 \times b_2 = c_2$

$a_3 \times b_3 = c_3$

$a_4 + b_4 = c_4$

$a_5 + b_5 = c_5$

$a_6 + b_6 = c_6$

A Simple Constraint System

Prove that $0 =< c_6 < 4$?

Multiplications and additions and <u>**copy**</u>?

$$a_4 = a_1$$
$$b_4 = b_1$$
$$c_4 = 1$$
$$c_1 = 0$$

$$a_1 \times b_1 = c_1$$
$$a_2 \times b_2 = c_2$$
$$a_3 \times b_3 = c_3$$

$$a_1 + b_1 = 1$$

$$a_4 + b_4 = c_4$$
$$a_5 + b_5 = c_5$$
$$a_6 + b_6 = c_6$$

A Simple Constraint System

Prove that 0 =< c_6 < 4 ?

Multiplications and additions and **copy**?

$$a_1 \times b_1 = c_1$$

$$a_2 \times b_2 = c_2$$

$$a_3 \times b_3 = c_3$$

$$a_1 + b_1 = 1$$

$$a_4 + b_4 = c_4$$

$$a_5 + b_5 = c_5$$

$$a_6 + b_6 = c_6$$

$$a_4 = a_1$$

$$b_4 = b_1$$

$$c_4 = 1$$

$$c_1 = 0$$

$$\Rightarrow a_1 \in \{0, 1\}$$

A Simple Constraint System

Prove that 0 =< c_6 < 4 ?

Multiplications and additions and **copy**?

$$a_1 \times b_1 = c_1$$

$$a_2 \times b_2 = c_2$$

$$a_3 \times b_3 = c_3$$

$$a_4 + b_4 = c_4$$

$$a_5 + b_5 = c_5$$

$$a_6 + b_6 = c_6$$

$$a_4 = a_1$$

$\Rightarrow a_1 \in \{0,1\}$

$$c_4 = 1$$

$$c_1 = 0$$

$$a_5 = a_1$$

$$b_5 = b_1$$

$$c_5 = 1$$

$$c_2 = 0$$

$\Rightarrow b_2 \in \{0,1\}$

A Simple Constraint System

Prove that 0 =< c_6 < 4 ?

Multiplications and additions and **copy**?

$$a_1 \times b_1 = c_1$$

$$a_2 \times b_2 = c_2$$

$$a_3 \times b_3 = c_3$$

$$a_4 + b_4 = c_4$$

$$a_5 + b_5 = c_5$$

$$a_6 + b_6 = c_6$$

$\Rightarrow a_1 \in \{0,1\}$

$c_1 = 0$

$\Rightarrow b_2 \in \{0,1\}$

$c_2 = 0$

$$a_3 = \frac{1}{2}$$

$$c_3 = b_2$$

A Simple Constraint System

Prove that $0 =< c_6 < 4$?

Multiplications and additions and **copy**?

$$a_1 \times b_1 = c_1$$

$$a_2 \times b_2 = c_2$$

$$a_3 \times b_3 = c_3$$

$$1/2 \times b_3 = b_2$$

$$a_4 + b_4 = c_4$$

$$a_5 + b_5 = c_5$$

$$a_6 + b_6 = c_6$$

$\Rightarrow a_1 \in \{0,1\}$

$c_1 = 0$

$\Rightarrow b_2 \in \{0,1\}$

$c_2 = 0$

$$a_3 = \frac{1}{2}$$

$$c_3 = b_2$$

A Simple Constraint System

Prove that $0 =< c_6 < 4$?

Multiplications and additions and **copy**?

$a_1 \times b_1 = c_1$

$a_2 \times b_2 = c_2$

$a_3 \times b_3 = c_3$

$\tfrac{1}{2} \times b_3 = b_2$

$\Rightarrow 2b_2 = b_3$

$a_4 + b_4 = c_4$

$a_5 + b_5 = c_5$

$a_6 + b_6 = c_6$

$\Rightarrow a_1 \in \{0,1\}$

$\Rightarrow b_2 \in \{0,1\}$

$c_1 = 0$

$c_4 = 1$

$c_2 = 0$

$c_5 = 1$

$a_3 = \frac{1}{2}$

$c_3 = b_2$

A Simple Constraint System

Prove that 0 =< c_6 < 4 ?

Multiplications and additions and **copy**?

$$a_1 \times b_1 = c_1$$
$$a_2 \times b_2 = c_2$$
$$a_3 \times b_3 = c_3$$

$$a_4 + b_4 = c_4$$
$$a_5 + b_5 = c_5$$
$$a_6 + b_6 = c_6$$

$$a_4 = a_1$$
$$b_4 = b_1$$
$$c_4 = 1$$
$$c_1 = 0$$
$$a_5 = a_1$$
$$b_5 = b_1$$
$$c_5 = 1$$
$$c_2 = 0$$
$$a_3 = \frac{1}{2}$$
$$c_3 = b_2$$
$$b_6 = b_3$$
$$a_6 = a_1$$

A Simple Constraint System

Prove that 0 =< c_6 < 4 ?

Multiplications and additions and **copy**?

$a_1 \times b_1 = c_1$

$a_2 \times b_2 = c_2$

$a_3 \times b_3 = c_3$

$a_4 + b_4 = c_4$

$a_5 + b_5 = c_5$

$a_6 + b_6 = c_6$

$\Rightarrow a_1 \in \{0,1\}$

$c_4 = 1$

$c_1 = 0$

$\Rightarrow b_2 \in \{0,1\}$

$c_5 = 1$

$c_2 = 0$

$\Rightarrow b_3 = 2b_2$

$b_6 = b_3$

$a_6 = a_1$

A Simple Constraint System

Prove that 0 =< c_6 < 4 ?

Multiplications and additions and **copy**?

$$a_1 \times b_1 = c_1$$
$$a_2 \times b_2 = c_2$$
$$a_3 \times b_3 = c_3$$

$$a_4 + b_4 = c_4$$
$$a_5 + b_5 = c_5$$
$$a_6 + b_6 = c_6$$
$$a_1 + 2b_2 = c_6$$

as required?

$\Rightarrow a_1 \in \{0,1\}$

$\Rightarrow b_2 \in \{0,1\}$

$\Rightarrow b_3 = 2b_2$

$$b_6 = b_3$$
$$a_6 = a_1$$

A Simple Constraint System

Prove that 0 =< c_6 < 4 ?

Multiplications and additions and **copy**?

Too constrained?

$$a_1 \times b_1 = c_1$$

$$a_2 \times b_2 = c_2$$

$$a_3 \times b_3 = c_3$$

$$a_4 + b_4 = c_4$$

$$a_5 + b_5 = c_5$$

$$a_6 + b_6 = c_6$$

$$a_1 + 2b_2 = c_6$$

as required?

$\Rightarrow a_1 \in \{0,1\}$

$\Rightarrow b_2 \in \{0,1\}$

$\Rightarrow b_3 = 2b_2$

$$b_6 = b_3$$

$$a_6 = a_1$$

A Simple Constraint System

Prove that $0 =< c_6 < 4$?

Multiplications and additions and **copy**?

Too constrained?

$a_1 \times b_1 = c_1$	$a_1 + b_1 = c_1$
$a_2 \times b_2 = c_2$	$a_2 + b_2 = c_2$
$a_3 \times b_3 = c_3$	$a_3 + b_3 = c_3$
$a_4 \times b_4 = c_4$	$a_4 + b_4 = c_4$
$a_5 \times b_5 = c_5$	$a_5 + b_5 = c_5$
$a_6 \times b_6 = c_6$	$a_6 + b_6 = c_6$

$\Rightarrow a_1 \in \{0,1\}$

$\Rightarrow b_2 \in \{0,1\}$

$\Rightarrow b_3 = 2b_2$

$\Rightarrow c_6 = a_1 + 2b_2$

If we check multiplication gates and addition gates at every step, problems.

A Simple Constraint System

Prove that $0 =< c_6 < 4$?

e.g. If $c_6 = 3$?

$\Rightarrow a_1 = 1,\ b_1 = 1$

$\Rightarrow a_1 + b_1 = 2 \neq 0$

$a_1 \times b_1 = c_1$	$a_1 + b_1 = c_1$
$a_2 \times b_2 = c_2$	$a_2 + b_2 = c_2$
$a_3 \times b_3 = c_3$	$a_3 + b_3 = c_3$
$a_4 \times b_4 = c_4$	$a_4 + b_4 = c_4$
$a_5 \times b_5 = c_5$	$a_5 + b_5 = c_5$
$a_6 \times b_6 = c_6$	$a_6 + b_6 = c_6$

$\Rightarrow a_1 \in \{0,1\}$

$c_1 = 0$

$\Rightarrow b_2 \in \{0,1\}$

$c_2 = 0$

$\Rightarrow b_3 = 2b_2$

$\Rightarrow c_6 = a_1 + 2b_2$

If we check multiplication gates and addition gates at every step, problems.

A Simple Constraint System

Prove that 0 =< c_6 < 4 ?

e.g. If $c_6 = 3$?

$\Rightarrow a_1 = 1,\ b_1 = 1$

$\Rightarrow a_1 + b_1 = 2 \neq 0$

First add gate not satisfied by correct witness

$c_1 = 0$

$\Rightarrow a_1 \in \{0,1\}$

$\Rightarrow b_2 \in \{0,1\}$

$c_2 = 0$

$\Rightarrow b_3 = 2b_2$

$\Rightarrow c_6 = a_1 + 2b_2$

$a_1 \times b_1 = c_1$	$a_1 + b_1 = c_1$
$a_2 \times b_2 = c_2$	$a_2 + b_2 = c_2$
$a_3 \times b_3 = c_3$	$a_3 + b_3 = c_3$
$a_4 \times b_4 = c_4$	$a_4 + b_4 = c_4$
$a_5 \times b_5 = c_5$	$a_5 + b_5 = c_5$
$a_6 \times b_6 = c_6$	$a_6 + b_6 = c_6$

If we check multiplication gates and addition gates at every step, problems.

A Simple Constraint System

Prove that 0 =< c_6 < 4 ?

Multiplications and additions and copy and **selectors**?

$$a_1 \times b_1 = c_1$$
$$a_2 \times b_2 = c_2$$
$$a_3 \times b_3 = c_3$$

$$a_4 + b_4 = c_4$$
$$a_5 + b_5 = c_5$$
$$a_6 + b_6 = c_6$$

$\Rightarrow a_1 \in \{0,1\}$

$\Rightarrow b_2 \in \{0,1\}$

$\Rightarrow b_3 = 2b_2$

$\Rightarrow c_6 = a_1 + 2b_2$

Select which gate to use at each point

A Simple Constraint System

Prove that $0 =< c_6 < 4$?

$$a_1 \times b_1 = c_1$$
$$a_2 \times b_2 = c_2$$
$$a_3 \times b_3 = c_3$$
$$a_4 + b_4 = c_4$$
$$a_5 + b_5 = c_5$$
$$a_6 + b_6 = c_6$$

Multiplications and additions and copy and **selectors**?

Works

Turn multiplication on in slots 1, 2, 3

Turn addition on in slots 4, 5, 6

$\Rightarrow a_1 \in \{0, 1\}$

$\Rightarrow b_2 \in \{0, 1\}$

$\Rightarrow b_3 = 2b_2$

$\Rightarrow c_6 = a_1 + 2b_2$

Select which gate to use at each point

To Enforce Copy Constraints

$$a_3 = a_1$$
$$b_1 = b_2$$
$$c_1 = 1$$
$$a_2 = \frac{1}{2}$$
$$c_3 = b_2$$

example copy constraints that we want to enforce.

To Enforce Copy Constraints

- Line up all public and private inputs in order.

public inputs

$1 \quad \frac{1}{2}$

private inputs

$a_1 \quad a_2 \quad a_3 \quad b_1 \quad b_2 \quad b_3 \quad c_1 \quad c_2 \quad c_3$

$a_3 = a_1$

$b_1 = b_2$

$c_1 = 1$

$a_2 = \frac{1}{2}$

$c_3 = b_2$

To Enforce Copy Constraints

- Line up all public and private inputs in order.
- Show equal to permuted inputs.

$$\sigma = (1,9)(2,4)(3,5)(6,7,11)(8)(10)$$

a_3	$=$	a_1
b_1	$=$	b_2
c_1	$=$	1
a_2	$=$	$\frac{1}{2}$
c_3	$=$	b_2

$$x_1 \quad x_2 \quad x_3 \quad x_4 \quad x_5 \quad x_6 \quad x_7 \quad x_8 \quad x_9 \quad x_{10} \quad x_{11}$$

$$=$$

$$y_9 \quad y_4 \quad y_5 \quad y_2 \quad y_3 \quad y_7 \quad y_{11} \quad y_8 \quad y_1 \quad y_{10} \quad y_6$$

$$\vec{y} = \sigma(\vec{x})$$

To Enforce Copy Constraints

$$a_3 = a_1$$
$$b_1 = b_2$$
$$c_1 = 1$$
$$a_2 = \frac{1}{2}$$
$$c_3 = b_2$$

- Line up all public and private inputs in order.
- Show equal to permuted inputs.

$$\begin{bmatrix} 1 & \frac{1}{2} & a_1 & a_2 & a_3 & b_1 & b_2 & b_3 & c_1 & c_2 & c_3 \end{bmatrix}$$

$$=$$

$$\begin{bmatrix} c_1 & a_2 & a_3 & \frac{1}{2} & a_1 & c_3 & b_1 & b_3 & 1 & c_2 & b_2 \end{bmatrix}$$

To Enforce Copy Constraints

- Line up all public and private inputs in order.
- Show equal to permuted inputs.

$a_3 = a_1$

$b_1 = b_2$

$c_1 = 1$

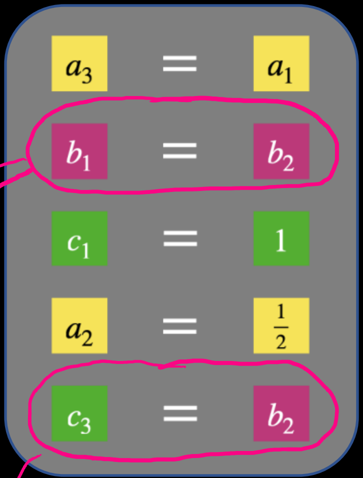
$a_2 = \frac{1}{2}$

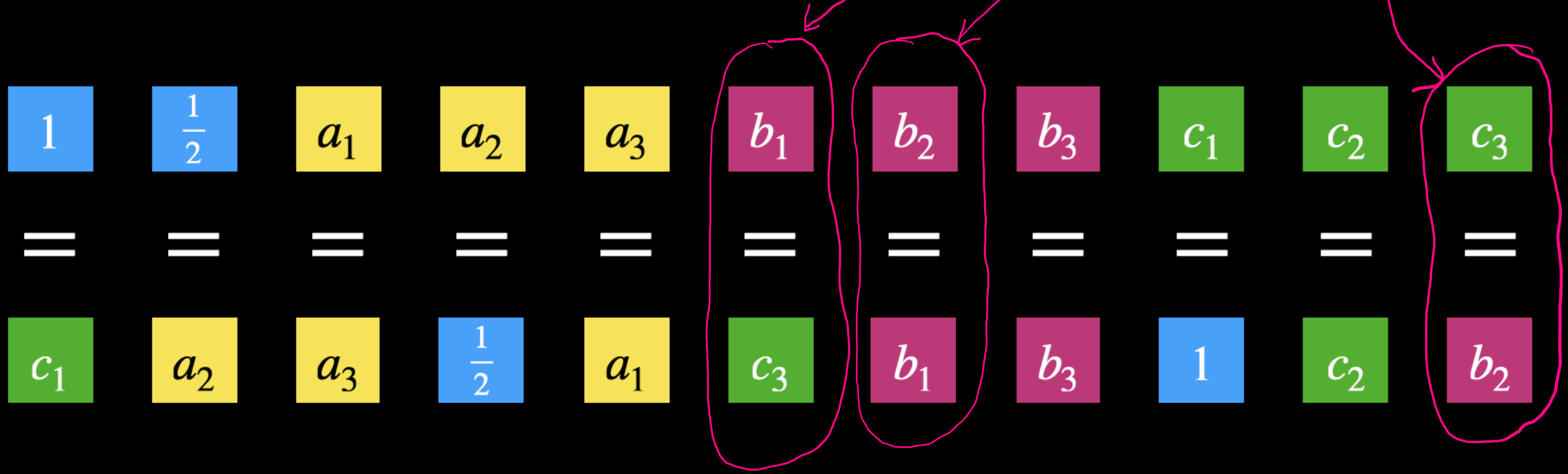
$c_3 = b_2$

1	$\frac{1}{2}$	a_1	a_2	a_3	b_1	b_2	b_3	c_1	c_2	c_3
$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$
c_1	a_2	a_3	$\frac{1}{2}$	a_1	c_3	b_1	b_3	1	c_2	b_2

To Enforce Copy Constraints

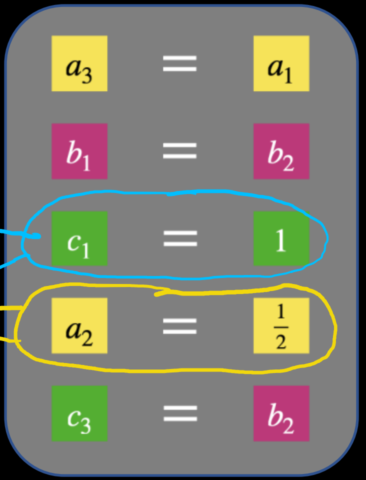
- Line up all public and private inputs in order.
- Show equal to permuted inputs.

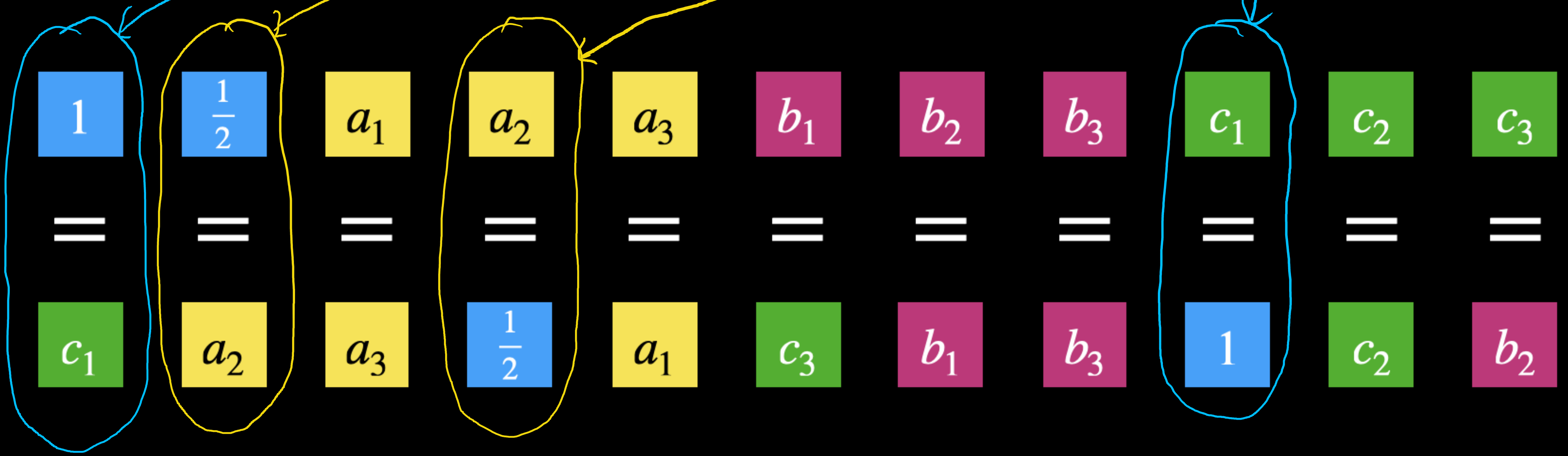




To Enforce Copy Constraints

- Line up all public and private inputs in order.
- Show equal to permuted inputs.





To Enforce Copy Constraints

$a_3 = a_1$
$b_1 = b_2$
$c_1 = 1$
$a_2 = \frac{1}{2}$
$c_3 = b_2$

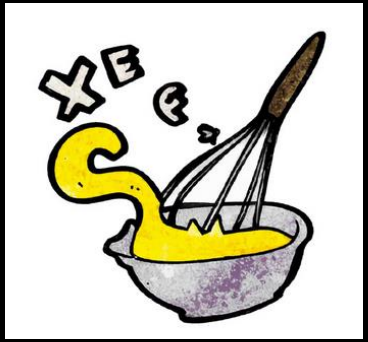
- Line up all public and private inputs in order.
- Show equal to permuted inputs.

b_3 and c_2 are unconstrained.

1	$\frac{1}{2}$	a_1	a_2	a_3	b_1	b_2	b_3	c_1	c_2	c_3
$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$	$=$
c_1	a_2	a_3	$\frac{1}{2}$	a_1	c_3	b_1	b_3	1	c_2	b_2

To Enforce Copy Constraints

- Line up all public and private inputs in order.
- Show equal to permuted inputs.
- Permutation argument by Neff, described previously in Dan Boneh's talk.



Detailed explanation in Curdleproofs, Chapter 5

https://github.com/asn-d6/curdleproofs/blob/main/doc/curdleproofs.pdf

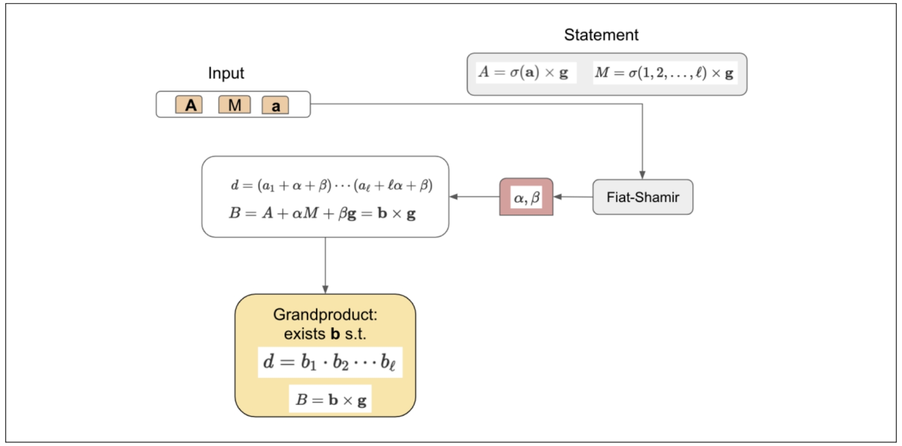
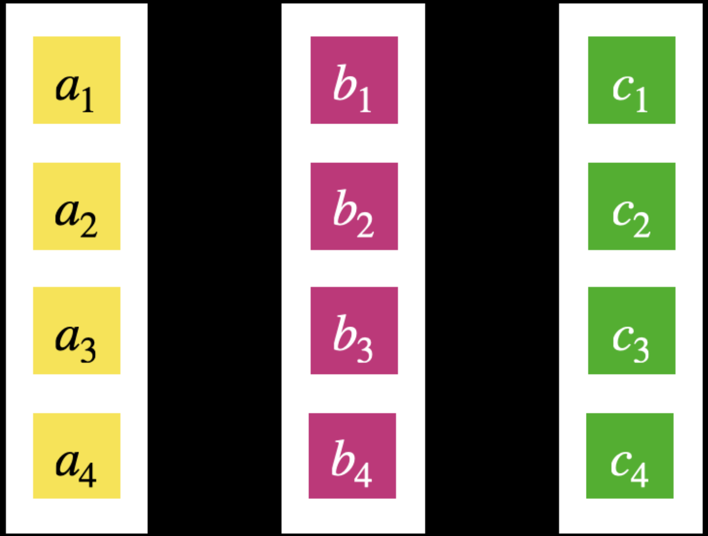


Figure 5.1: Overview of SamePerm argument. The protocol uses GrandProd argument as a subroutine.

Selector Polynomials

Turn multiplication on in slots 1, 3



- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn multiplication on in slots 1, 3

Multiplication Constraints in Polynomials?

a_1	$\times$	b_1	$=$	c_1
a_2	$\times$	b_2	$=$	c_2
a_3	$\times$	b_3	$=$	c_3
a_4	$\times$	b_4	$=$	c_4

$$a(X)b(X) - c(X) = 0 \mod (X-1)(X-2)(X-3)(X-4)$$

$= Z(X)$

(vanishing polynomial)

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn multiplication on in slots 1, 3

Multiplication Constraints in Polynomials?

$$a_1 \times b_1 = c_1$$
$$a_2 \times b_2 = c_2$$
$$a_3 \times b_3 = c_3$$
$$a_4 \times b_4 = c_4$$

$$a(X)b(X) - c(X) = 0 \mod (X-1)(X-2)(X-3)(X-4)$$

$= z(X)$

(vanishing polynomial)

$$a(X)b(X) - c(X) = q(X)z(X)$$

for some $q(X)$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn multiplication on in slots 1, 3

Multiplication Constraints in Polynomials?

$$a_1 \times b_1 = c_1$$
$$a_2 \times b_2 = c_2$$
$$a_3 \times b_3 = c_3$$
$$a_4 \times b_4 = c_4$$

$$a(X)b(X) - c(X) = q(X)z(X)$$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn multiplication on in slots 1, 3

Multiplication Constraints in Polynomials?

$$a_1 \times b_1 = c_1$$
$$a_2 \times b_2 = c_2$$
$$a_3 \times b_3 = c_3$$
$$a_4 \times b_4 = c_4$$

$$a(X)b(X) - c(X) = q(X)z(X)$$

e.g. $a(1)b(1) - c(1) = q(1)z(1)$

$= q(1) \times 0$

$= 0$

$\Rightarrow a_1 \times b_1 = c_1$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Multiplication Constraints in Polynomials?

Turn multiplication on in slots 1, 3

$$a_1 \times b_1 = c_1$$
$$a_2 \times b_2 = c_2$$
$$a_3 \times b_3 = c_3$$
$$a_4 \times b_4 = c_4$$

- Suppose that $S_M(X)$ is a polynomial such that
  - $S_M(1) = S_M(3) = 1$
  - $S_M(2) = S_M(4) = 0$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn multiplication on in slots 1, 3

Multiplication Constraints in Polynomials?

a_1	$\times$	b_1	$=$	c_1
a_2	$\times$	b_2	$=$	c_2
a_3	$\times$	b_3	$=$	c_3
a_4	$\times$	b_4	$=$	c_4

- Suppose that $S_M(X)$ is a polynomial such that
  - $S_M(1) = S_M(3) = 1$
  - $S_M(2) = S_M(4) = 0$

$$S_M(X)\big(a(X)b(X) - c(X)\big) = q(X)z(X)$$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn multiplication on in slots 1, 3

Multiplication Constraints in Polynomials?

a_1	$\times$	b_1	$=$	c_1
a_2	$\times$	b_2	$=$	c_2
a_3	$\times$	b_3	$=$	c_3
a_4	$\times$	b_4	$=$	c_4

- Suppose that $S_M(X)$ is a polynomial such that
  - $S_M(1) = S_M(3) = 1$
  - $S_M(2) = S_M(4) = 0$

$$S_M(X)\big(a(X)b(X) - c(X)\big) = q(X)z(X)$$

$$S_M(1)\left[a(1)b(1) - c(1)\right] = 0$$

$$S_M(3)\left[a(3)b(3) - c(3)\right] = 0$$

$$\Rightarrow$$

$$a_1 b_1 = c_1$$

$$a_3 b_3 = c_3$$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn addition on in slots 1, 3

Addition Constraints in Polynomials?

$$a_1 + b_1 = c_1$$
$$a_2 + b_2 = c_2$$
$$a_3 + b_3 = c_3$$
$$a_4 + b_4 = c_4$$

$$a(X) + b(X) - c(X) = q(X)z(X)$$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn addition on in slots 1, 3

Addition Constraints in Polynomials?

$$a_1 + b_1 = c_1$$
$$a_2 + b_2 = c_2$$
$$a_3 + b_3 = c_3$$
$$a_4 + b_4 = c_4$$

$$a(X) + b(X) - c(X) = q(X)z(X)$$

e.g. $a(1) + b(1) - c(1) = q(1)z(1)$

$\Rightarrow a_1 + b_1 - c_1 = q_1 \times 0$

$\Rightarrow a_1 + b_1 = c_1$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn addition on in slots 1, 3

Addition Constraints in Polynomials?

$$a_1 + b_1 = c_1$$
$$a_2 + b_2 = c_2$$
$$a_3 + b_3 = c_3$$
$$a_4 + b_4 = c_4$$

- Suppose that $S_A(X)$ is a polynomial such that
  - $S_A(1) = S_A(3) = 1$
  - $S_A(2) = S_A(4) = 0$

$$S_A(X)\big(a(X) + b(X) - c(X)\big) = q(X)z(X)$$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn addition on in slots 1, 3

Addition Constraints in Polynomials?

$$a_1 + b_1 = c_1$$
$$a_2 + b_2 = c_2$$
$$a_3 + b_3 = c_3$$
$$a_4 + b_4 = c_4$$

- Suppose that $S_A(X)$ is a polynomial such that
  - $S_A(1) = S_A(3) = 1$
  - $S_A(2) = S_A(4) = 0$

$$S_A(X)\big(a(X) + b(X) - c(X)\big) = q(X)z(X)$$

$\Rightarrow$ $S_A(1)[a_1 + b_1 - c_1] = 0$

$S_A(2)[a_2 + b_2 - c_2] = 0$

$S_A(3)[a_3 + b_3 - c_3] = 0$

$S_A(4)[a_4 + b_4 - c_4] = 0$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn addition on in slots 1, 3

Addition Constraints in Polynomials?

$a_1 + b_1 = c_1$

$a_2 + b_2 = c_2$

$a_3 + b_3 = c_3$

$a_4 + b_4 = c_4$

- Suppose that $S_A(X)$ is a polynomial such that
  - $S_A(1) = S_A(3) = 1$
  - $S_A(2) = S_A(4) = 0$

$$S_A(X)\big(a(X) + b(X) - c(X)\big) = q(X)z(X)$$

$\Rightarrow S_A(1)[a_1 + b_1 - c_1] = 0$

$\cancel{S_A(2)[a_2 + b_2 - c_2] = 0}$ $\quad S_A(2) = 0$

$S_A(3)[a_3 + b_3 - c_3] = 0$

$\cancel{S_A(4)[a_4 + b_4 - c_4] = 0}$ $\quad S_A(4) = 0$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn addition on in slots 1, 3

Addition Constraints in Polynomials?

a_1	+	b_1	=	c_1
a_2	+	b_2	=	c_2
a_3	+	b_3	=	c_3
a_4	+	b_4	=	c_4

- Suppose that $S_A(X)$ is a polynomial such that
  - $S_A(1) = S_A(3) = 1$
  - $S_A(2) = S_A(4) = 0$

$$S_A(X)\big(a(X) + b(X) - c(X)\big) = q(X)z(X)$$

$\Rightarrow S_A(1)[a_1 + b_1 - c_1] = 0$

$S_A(3)[a_3 + b_3 - c_3] = 0$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn addition on in slots 1, 3

Addition Constraints in Polynomials?

$$a_1 + b_1 = c_1$$
$$a_2 + b_2 = c_2$$
$$a_3 + b_3 = c_3$$
$$a_4 + b_4 = c_4$$

- Suppose that $S_A(X)$ is a polynomial such that
  - $S_A(1) = S_A(3) = 1$
  - $S_A(2) = S_A(4) = 0$

$$S_A(X)\big(a(X) + b(X) - c(X)\big) = q(X)z(X)$$

$\Rightarrow \cancel{S_A(1)}[a_1 + b_1 - c_1] = 0 \qquad S_A(1) = 1$

$\cancel{S_A(3)}[a_3 + b_3 - c_3] = 0 \qquad S_A(3) = 1$

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Selector Polynomials

Turn addition on in slots 1, 3

Addition Constraints in Polynomials?

a_1	$+$	b_1	$=$	c_1
a_2	$+$	b_2	$=$	c_2
a_3	$+$	b_3	$=$	c_3
a_4	$+$	b_4	$=$	c_4

- Suppose that $S_A(X)$ is a polynomial such that
  - $S_A(1) = S_A(3) = 1$
  - $S_A(2) = S_A(4) = 0$

$$S_A(X)\big(a(X) + b(X) - c(X)\big) = q(X)z(X)$$

$\Rightarrow$ $a_1 + b_1 - c_1 = 0$

$a_3 + b_3 - c_3 = 0$

as required.

- Suppose that
  - $a(X)$ is a polynomial such that $a(i) = a_i$
  - $b(X)$ is a polynomial such that $b(i) = b_i$
  - $c(X)$ is a polynomial such that $c(i) = c_i$

Custom Constraints

The MinRoot Verifiable Delay Function

- Overview:
  - Good randomness is really hard.
  - Ethereum needs (good?) randomness for consensus.
  - In future thinking of using the MinRoot verifiable delay function.

MinRoot:
Candidate Sequential Function for Ethereum VDF

Dmitry Khovratovich
Ethereum Foundation
khovratovich@gmail.com

Mary Maller
Ethereum Foundation
mary.maller@ethereum.org

Pratyush Ranjan Tiwari
Johns Hopkins University
ptiwari4@jhu.edu

November 24, 2022

Compute the round function over and over and over again

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

Custom Constraints

The MinRoot Verifiable Delay Function

- Overview:
  - Good randomness is really hard.
  - Ethereum needs (good?) randomness for consensus.
  - In future thinking of using the MinRoot verifiable delay function.

MinRoot:
Candidate Sequential Function for Ethereum VDF

Dmitry Khovratovich
Ethereum Foundation
khovratovich@gmail.com

Mary Maller
Ethereum Foundation
mary.maller@ethereum.org

Pratyush Ranjan Tiwari
Johns Hopkins University
ptiwari4@jhu.edu

November 24, 2022

Compute the round function over and over and over again

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$\Rightarrow x_{i+1}^3 = x_i + y_i$

$\Rightarrow$ we will compute many, many cubic powers

Custom Constraints

The MinRoot Verifiable Delay Function

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$$a_1 \times b_1 \times c_1 - d_1 - e_1 = 0$$

$$a_2 + b_2 - c_2 = 0$$

$$a_1 = b_1 = c_1 = d_3 = a_4$$

$$x_1 = a_2 = d_1$$

$$y_1 = e_1$$

$$1 = b_2$$

Custom Constraints

The MinRoot Verifiable Delay Function

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$$a_1 \times a_1 \times a_1 - x_1 - y_1 = 0$$

$$a_1 \times b_1 \times c_1 - d_1 - e_1 = 0$$

$$a_2 + b_2 - c_2 = 0$$

$$a_1 = b_1 = c_1 = d_3 = a_4$$

$$x_1 = a_2 = d_1$$

$$y_1 = e_1$$

$$1 = b_2$$

$$\Rightarrow a_1^3 = (x_1 + y_1)$$

$$\Rightarrow a_1 = (x_1 + y_1)^{1/3}$$

Custom Constraints

The MinRoot Verifiable Delay Function

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$$a_1 \times b_1 \times c_1 - d_1 - e_1 = 0$$

$$a_2 + b_2 - c_2 = 0$$

$$x_1 + 1 - c_2 = 0$$

$$a_1 = b_1 = c_1 = d_3 = a_4$$

$$x_1 = a_2 = d_1$$

$$y_1 = e_1$$

$$1 = b_2$$

$$a_1 = (x_1 + y_1)^{1/3}$$

$$\Rightarrow c_2 = x_1 + 1$$

Custom Constraints

The MinRoot Verifiable Delay Function

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$$a_1 \times b_1 \times c_1 - d_1 - e_1 = 0$$

$$a_2 + b_2 - c_2 = 0$$

$$a_3 \times b_3 \times c_3 - d_3 - e_3 = 0$$

$$a_4 + b_4 - c_4 = 0$$

$a_1 = b_1 =$

$x_1 = a_2 =$

$y_1 = e_1$

$1 = b_2$

$a_3 = b_3 = c_3$

$e_3 = c_2$

$2 = b_4$

$a_1 = (x_1 + y_1)^{1/3} = x_2$

$c_2 = x_1 + 1 = y_2$

Custom Constraints

The MinRoot Verifiable Delay Function

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$$a_3 \times a_3 \times a_3 - a_1 - c_2 = 0$$

$$a_3 \times b_3 \times c_3 - d_3 - e_3 = 0$$

$$a_4 + b_4 - c_4 = 0$$

$a_1 = b_1$

$x_1 = a_2$

$y_1 = e_1$

$1 = b_2$

$a_3 = b_3 = c_3$

$e_3 = c_2$

$2 = b_4$

$$a_1 = (x_1 + y_1)^{1/3} = x_2$$

$$c_2 = x_1 + 1 = y_2$$

$$\Rightarrow a_3 = (a_1 + c_2)^{1/3} = (x_2 + y_2)^{1/3}$$

Custom Constraints

The MinRoot Verifiable Delay Function

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$a_1 = b_1$

$x_1 = a_2$

$y_1 = e_1$

$1 = b_2$

$a_3 = b_3 = c_3$

$e_3 = c_2$

$2 = b_4$

$a_1 = (x_1 + y_1)^{1/3} = x_2$

$c_2 = x_1 + 1 = y_2$

$$a_3 \times b_3 \times c_3 - d_3 - e_3 = 0$$

$$a_4 + b_4 - c_4 = 0$$

$$a_1 + 2 - c_4 = 0$$

$a_3 = (x_2 + y_2)^{1/3} = x_3$

$c_4 = x_2 + 2 = y_3$

Custom Constraints

The MinRoot Verifiable Delay Function

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$$a_3 \times b_3 \times c_3 - d_3 - e_3 = 0$$

$$a_4 + b_4 - c_4 = 0$$

$$a_1 + 2 - C_4 = 0$$

$$a_1 = b_1$$
$$x_1 = a_2$$
$$y_1 = e_1$$
$$1 = b_2$$
$$a_3 = b_3 = c_3$$
$$e_3 = c_2$$
$$2 = b_4$$

$$a_1 = (x_1 + y_1)^{1/3} = x_2$$
$$C_2 = x_1 + 1 = y_2$$

$$a_3 = (x_2 + y_2)^{1/3} = x_3$$

$$C_4 = x_2 + 2 = y_3$$

Continue in this fashion

Custom Constraints

The MinRoot Verifiable Delay Function

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$$a_1 \times b_1 \times c_1 - d_1 - e_1 = 0$$

$$a_2 + b_2 - c_2 = 0$$

$$a_3 \times b_3 \times c_3 - d_3 - e_3 = 0$$

$$a_4 + b_4 - c_4 = 0$$

$$a_1 = b_1 = c_1 = d_3 = a_4$$
$$x_1 = a_2 = d_1$$
$$y_1 = e_1$$
$$1 = b_2$$
$$a_3 = b_3 = c_3$$
$$e_3 = c_2$$
$$2 = b_4$$

- These constraints are neither addition, multiplication, nor copy.
- We will use them time and time again.
- If we allow this constraint, *which is specific to our circuit*, then total number of constraints is less.

Custom Constraints

The MinRoot Verifiable Delay Function

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$$a_1 \times b_1 \times c_1 - d_1 - e_1 = 0$$

$$a_2 + b_2 - c_2 = 0$$

$$a_3 \times b_3 \times c_3 - d_3 - e_3 = 0$$

$$a_4 + b_4 - c_4 = 0$$

$$a_1 = b_1 = c_1 = d_3 = a_4$$

$$x_1 = a_2 = d_1$$

$$y_1 = e_1$$

$$1 = b_2$$

$$a_3 = b_3 = c_3$$

$$e_3 = c_2$$

$$2 = b_4$$

$$S_{\text{minroot}}(X)\big(a(X)b(X)c(X) - e(X) - f(X)\big) = q_1(X)z(X)$$

$$S_A(X)\big(a(X) + b(X) - c(X)\big) = q_2(X)z(X)$$

Custom Constraints

The MinRoot Verifiable Delay Function

$$(x_{i+1}, y_{i+1}) = ((x_i + y_i)^{\frac{1}{3}}, x_i + i)$$

$$a_1 \times b_1 \times c_1 - d_1 - e_1 = 0$$

$$a_2 + b_2 - c_2 = 0$$

$$a_3 \times b_3 \times c_3 - d_3 - e_3 = 0$$

$$a_4 + b_4 - c_4 = 0$$

$$a_1 = b_1 = c_1 = d_3 = a_4$$

$$x_1 = a_2 = d_1$$

$$y_1 = e_1$$

$$1 = b_2$$

$$a_3 = b_3 = c_3$$

$$e_3 = c_2$$

$$2 = b_4$$

custom constraint

$$S_{\text{minroot}}(X)\big(a(X)b(X)c(X) - e(X) - f(X)\big) = q_1(X)z(X)$$

$$S_A(X)\big(a(X) + b(X) - c(X)\big) = q_2(X)z(X)$$

vanishing polynomial.

selector polynomials

addition constraint

Custom Constraints

The MinRoot Verifiable Delay Function

$$a_1 \times b_1 \times c_1 - d_1 - e_1 = 0$$

$$a_2 + b_2 - c_2 = 0$$

$$a_3 \times b_3 \times c_3 - d_3 - e_3 = 0$$

$$a_4 + b_4 - c_4 = 0$$

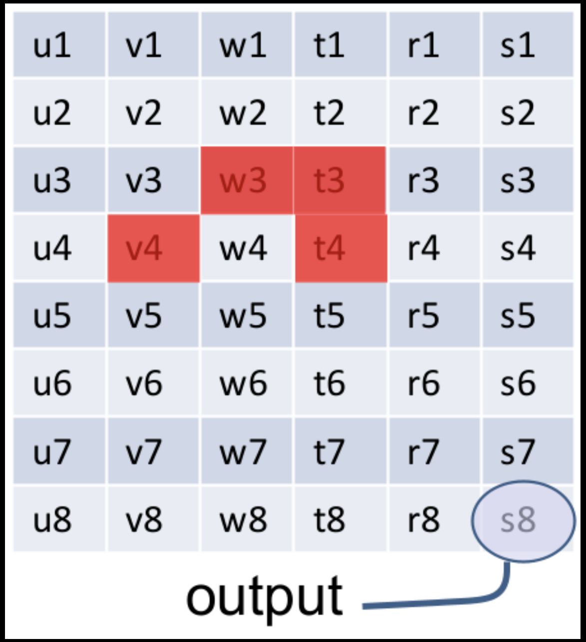
u1	v1	w1	t1	r1	s1
u2	v2	w2	t2	r2	s2
u3	v3	w3	t3	r3	s3
u4	v4	w4	t4	r4	s4
u5	v5	w5	t5	r5	s5
u6	v6	w6	t6	r6	s6
u7	v7	w7	t7	r7	s7
u8	v8	w8	t8	r8	s8

output

Custom Constraints

Trade-offs

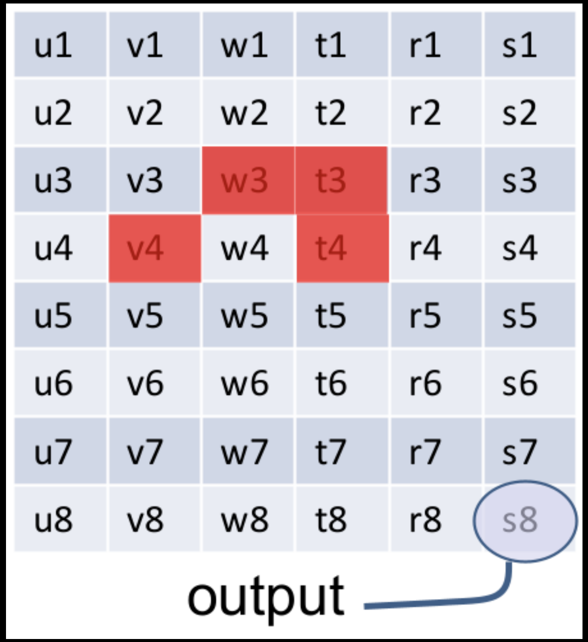
- Each additional column allows more expressive custom constraints but costs additional proof elements.
- Each additional multiplier per custom constraint allows more expressive custom constraints but costs additional proof elements.
- Each type of custom constraint costs additional proof elements.



Custom Constraints

Trade-offs

- Each additional column allows more expressive custom constraints but costs additional proof elements.
- Each additional multiplier per custom constraint allows more expressive custom constraints but costs additional proof elements.
- Each type of custom constraint costs additional proof elements.



Thus there is a trade-off between proof size/ verifier time and prover time.

Up Next...

Lookup Constraints

Lookup constraints are a very useful type of custom constraint.

Bonus Slide

Adding Zero-Knowledge to a Multiplication Constraint

$$a(X)b(X) - c(X) = q(X)z(X)$$

$$\bar{a}(X) = a(X) + r_a \times z(X)$$
$$\bar{b}(X) = b(X) + r_b \times z(X)$$
$$\bar{c}(X) = c(X) + r_c \times z(X)$$
$$\bar{q}(X) = (q(X) + r_a b(X) + r_b a(X) + r_a r_b z(X) - r_c)$$