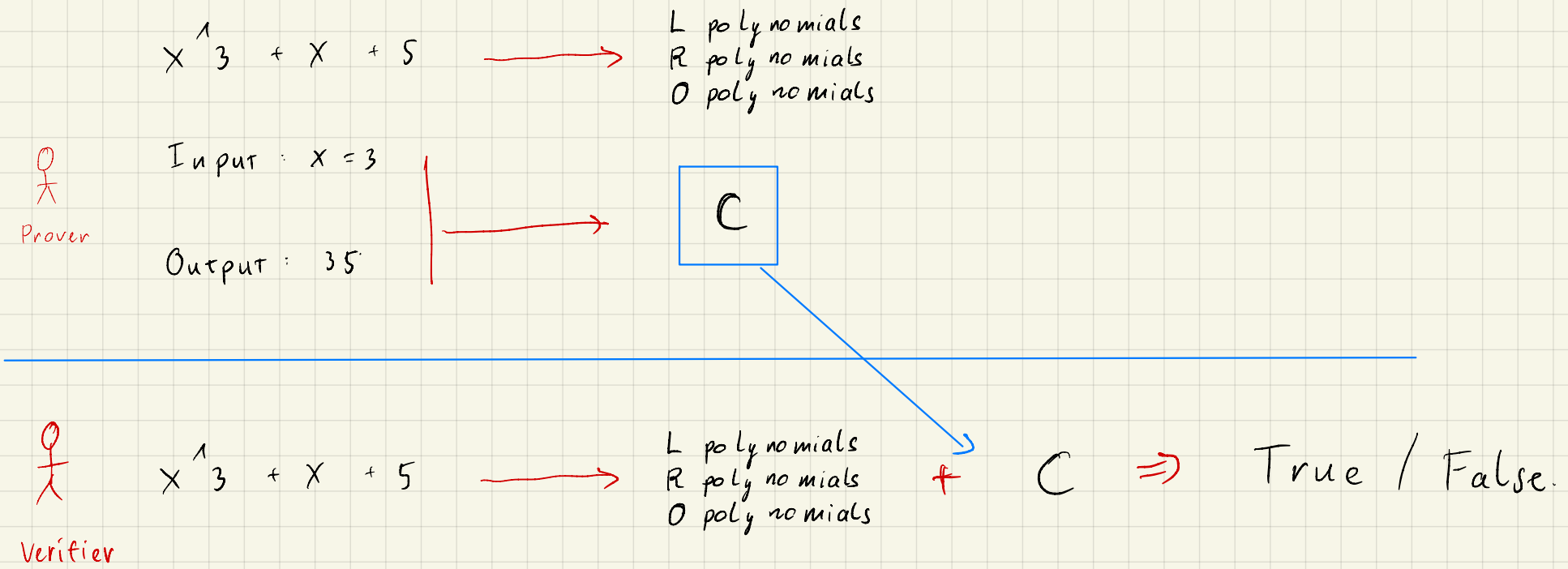
ZKP

Overall.


$x^3 + x + 5$
L polynomials
R polynomials
O polynomials
Prover
Input : x = 3
Output : 35
C
Verifier
$x^3 + x + 5$
L polynomials
R polynomials
O polynomials
+
C
⇒
True / False.

$x^3 + x + 5$

R1CS

Gates

$sym\_1 = x * x$

$y = sym\_1 * x$

$sym\_2 = (y + x) * 1$

$out = (sym\_2 + 5) * 1$

'one', 'x', 'out', 'sym_1', 'y', 'sym_2'

L
[0, 1, 0, 0, 0, 0]
[0, 0, 0, 1, 0, 0]
[0, 1, 0, 0, 1, 0]
[5, 0, 0, 0, 0, 1]

R
[0, 1, 0, 0, 0, 0]
[0, 1, 0, 0, 0, 0]
[1, 0, 0, 0, 0, 0]
[1, 0, 0, 0, 0, 0]

O
[0, 0, 0, 1, 0, 0]
[0, 0, 0, 0, 1, 0]
[0, 0, 0, 0, 0, 1]
[0, 0, 1, 0, 0, 0]

Input : x = 3

Output : 35

'one', 'x', 'out', 'sym_1', 'y', 'sym_2'

C [1, 3, 35, 9, 27, 30]

$$L C * R C - O C = 0$$

R1CS

'one' , 'x' , 'out' , 'sym_1' , 'y' , 'sym_2'

L

0	1	0	0	0	0
0	0	0	1	0	0
0	1	0	0	1	0
5	0	0	0	0	1

R

0	1	0	0	0	0
0	1	0	0	0	0
1	0	0	0	0	0
1	0	0	0	0	0

O

0	0	0	1	0	0
0	0	0	0	1	0
0	0	0	0	0	1
0	0	1	0	0	0

Lagrange interpolation

QAP

L polynomials

-5.0	9.166	-5	0,833
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...

R polynomials

...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...

O polynomials

...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...

$$F(x) = -5 + 9{,}166\,x - 5\,x^2 + 0{,}833\,x^3$$

$x = 1$	$\Rightarrow$	$F(x) = 0$
$x = 2$	$\Rightarrow$	$F(x) = 0$
$x = 3$	$\Rightarrow$	$F(x) = 0$
$x = 4$	$\Rightarrow$	$F(x) = 5$

'one', 'x', 'out', 'sym_1', 'y', 'sym_2'

C [1 , 3 , 35 , 9 , 27 , 30]

QAP

polynomials

L

[-5.0 , 9.166 , -5 , 0,833]
[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]

R polynomials

[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]

O polynomials

[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]
[... , ... , ... , ...]

$$T = L.C \ * \ R.C - O.C$$

$$= [-88, 592.6, -1063.7, 805, -294]$$

minimal polynomial V:

$$V = (x-1)(x-2)(x-3)(x-4)$$

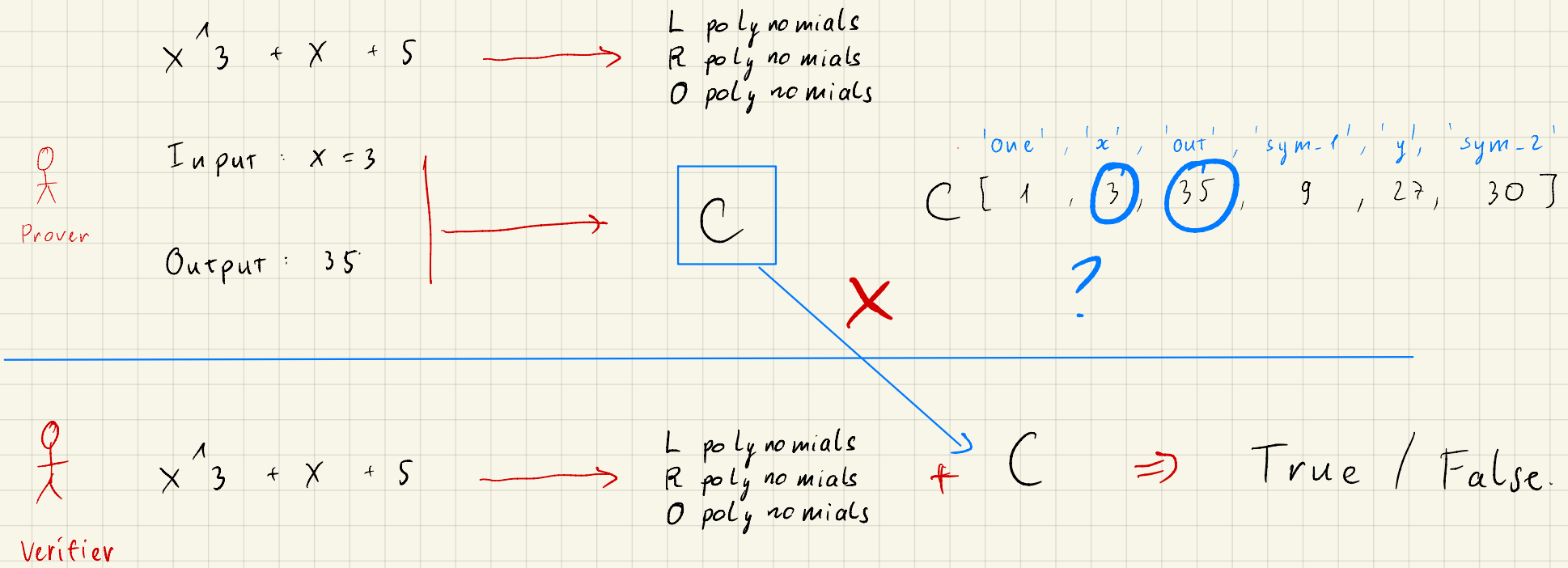
$$= [24, -50, 35, -10, 1]$$

Check if T / V has no remainder

$$Q = T / V = [-3, 37, -3]$$

⇓

$$L.C * RC - OC = Q.V$$

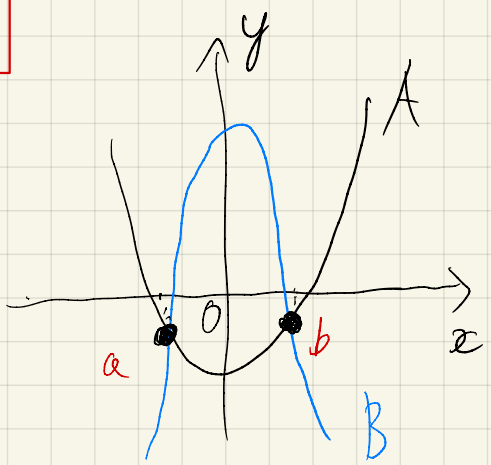

x^3 + x + 5
L polynomials
R polynomials
O polynomials
Prover
Input : x = 3
Output : 35
C
'one', 'x', 'out', 'sym_1', 'y', 'sym_2'
C [1 , 3 , 35 , 9 , 27 , 30]
?
x
x^3 + x + 5
L polynomials
R polynomials
O polynomials
Verifier
C
⇒ True / False.

Reed - Solomon

$A: 3x^2 - 3x + 2$

$B: x^2 + 2x + 1$

$C: 2x^2 - x + 3$



$x \in \{0, \dots, n\}$

$\rightarrow pR = \frac{2}{n} \simeq 0$ $\rightarrow$

Random t

$C(t) = 0$

$\hookrightarrow A \equiv B$

$10^k \rightarrow k$? HARD

Knouledge of exponent.

Private.

$A \qquad B = (10^{K})^{A} = 10^{K*A}$

$\downarrow \qquad \downarrow$

$C \qquad D = 10^{KC}$?

$\Rightarrow$

$C = xA$

$\downarrow$

$D = 10^{K*xA} = (10^{KA})^{x} = (B)^{x}$

$\Rightarrow$ Given A, $B = 10^{K*A}$ $\Rightarrow$

C must be derived from A. so that D is calculatable.

$\Rightarrow$ Given A_i, $B_i = 10^{K*A_i}$ with i from 1 to m $\Rightarrow$

C must be derived from $A_1, A_2, \ldots$ so that D is calculatable.

$C = 3A_1 + 4A_2 + \ldots$

Pairings

$$e(x, y) = \left(10^{\log_g(x)}\right)^{\log_g(y)}$$

$$= 10^{\log_g(x)\,\log_g(y)}$$

$$e_a - e_b = \frac{e(x, y)}{e(k, z)} = \frac{10^{\log_g(x)\,\log_g(y)}}{10^{\log_g(k)\,\log_g(z)}}$$

$$= 10^{\log_g(x)\,\log_g(y) - \log_g(k)\,\log_g(z)}$$

$$e_a + e_b = e(x, y) * e(k, z)$$

$$e(x, g) = 10^{\log_g(x)\,\log_g(g)} = 10^{\log_g(x) * 1}$$

Pairings

$x * y \Leftrightarrow$??

$a - b$

$\Rightarrow \frac{e(a)}{e(b)}$

$$\frac{e(x,y)}{e(z,k)} = \frac{10^{xy}}{10^{zk}} = 10^{xy - zk}$$

$a + b$

$\Rightarrow e(a) * e(b)$

$$e(x,y) * e(z,k) = 10^{xy} \cdot 10^{zk} = 10^{xy + zk}$$

Preparing

$g^{l_i(t)}, g^{r_i(t)}, g^{o_i(t)}$ for $i = 1, \ldots, m$

$g^t, g^{t^2}, \ldots, g^{t^m}$

$g^{V(t)}$

L polynomials

$L_1(x)$ [-5.0, 9.166, -5, 0,833]

$L_2(x)$ [... , ... , ... , ...]

$L_3(x)$ [... , ... , ... , ...]

[... , ... , ... , ...]

[... , ... , ... , ...]

[... , ... , ... , ...]

$L_m(x)$

Prover

$\pi_1 = g^{\sum_{i=1}^{m} c_i \times l_i(t)}$

$\pi_2 = g^{\sum_{i=1}^{m} c_i \times r_i(t)}$

$\pi_3 = g^{\sum_{i=1}^{m} c_i \times o_i(t)}$

$\pi_4 = g^{q(t)}$

$\pi_1 = g^{\sum_{i=1}^{m} c_i \times l_i(t)}$

$= g^{(c_1 \times l_1) + (c_2 \times l_2) + \ldots}$

$= g^{c_1 \times l_1} * g^{c_2 l_2} * \ldots$

$= (g^{l_1})^{c_1} * (g^{l_2})^{c_2} * \ldots$

$Q = T / V = [-3, 37, -3]$

$\pi_4 = g^{q(t)} = g^{a_0 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots}$

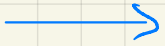
$= g^{a_0} (g^t)^{a_1} (g^{t^2})^{a_2} \ldots$

$$\pi_1 = g^{\sum_{i=1}^{m} c_i \times l_i(t)}$$

$$\pi_2 = g^{\sum_{i=1}^{m} c_i \times r_i(t)}$$

$$\pi_3 = g^{\sum_{i=1}^{m} c_i \times o_i(t)}$$

$$\pi_4 = g^{q(t)}$$



$L * R - O * (1)$

$e(\pi_1, \pi_2) / e(\pi_3, g)$

???

$e(g^{V(t)}, \pi_4)$

$V * Q$

$$\frac{e(\pi_1, \pi_2)}{e(\pi_3, g)} \Rightarrow 10^{\log_g(\pi_1)\ \log_g(\pi_2) - \log_g(\pi_3)}$$

$$= 10^{\log_g g^{\sum c_i l_i} \times \log_g g^{\sum c_i r_i} - \log_g g^{\sum c_i o_i}}$$

$$= 10^{\sum c_i l_i \times \sum c_i r_i - \sum c_i o_i}$$

$$= 10^{L * R - O}$$

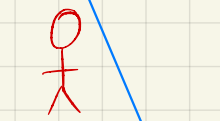
$$e(g^{V(t)}, \pi_4) = 10^{\log_g g^{V(t)}\ \log_g g^{q(t)}} = 10^{V(t)\ Q(t)}$$

C_i problem ?

Setup.

$g^{\beta [l_i(t) + r_i(t) + o_i(t)]}$ for $i \in [m]$

g^{β}



$$\pi_1 = g^{\sum_{i=1}^{m} c_i \times l_i(t)}$$

$$\pi_2 = g^{\sum_{i=1}^{m} c_i \times r_i(t)}$$

$$\pi_3 = g^{\sum_{i=1}^{m} c_i \times o_i(t)}$$

$$\pi_4 = g^{q(t)}$$

$$\pi_5 = \prod_{i=1}^{m} \left(g^{\beta [l_i(t) + r_i(t) + o_i(t)]} \right)^{c_i}$$

$$\left(g^{\beta [l_1 + r_1 + o_1]} \right)^{c_1} \left(g^{\beta [l_2 + r_2 + o_2]} \right)^{c_2}$$

$$= g^{\beta (c_1 l_1 + c_1 r_1 + c_1 o_1)} \cdot g^{\beta (c_2 l_2 + c_2 r_2 + c_2 o_2)}$$

$$= g^{\beta (c_1 l_1 + c_1 r_1 + c_1 o_1 + c_2 l_2 + c_2 r_2 + c_2 o_2)}$$

$$e(\pi_1, \pi_2, \pi_3, g^{\beta}) = e(\pi_5, g)$$

$$\Leftrightarrow \left(\sum_{i=1}^{m} c_i \times l_i + \sum_{i}^{m} c_i \times r_i + \sum_{i=1}^{m} c_i \times o_i \right) \times \beta = \square$$

Public, private ?

I_{Pub} I_{priv}

$$\pi_1 = g^{\sum_{i=1}^{m} c_i \times l_i}$$

Verifier

$$\pi_1^* = g^{\sum_{i \in I_{priv}} c_i \times l_i}$$

$$g^{\sum_{i \in I_{Pub}} c_i \times l_i}$$

$$\pi_1 = \pi_1^* * g^{\sum_{i \in I_{Pub}} c_i \times l_i}$$