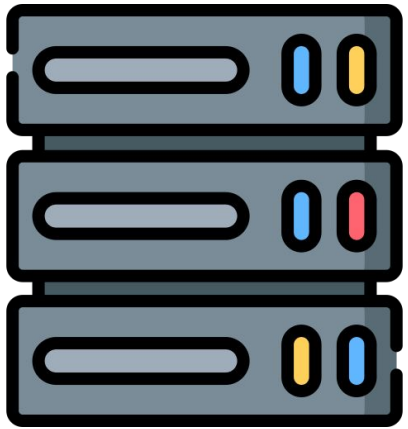
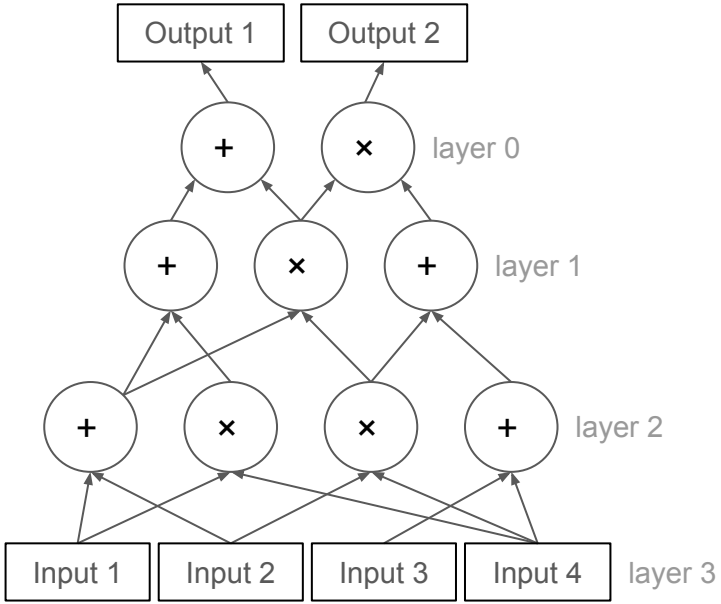
GKR Protocol

Prover P

Prover and Verifer agrees on a arithmetic circuit, meaning both parties are aware of the circuit

Verifier V





example circuit

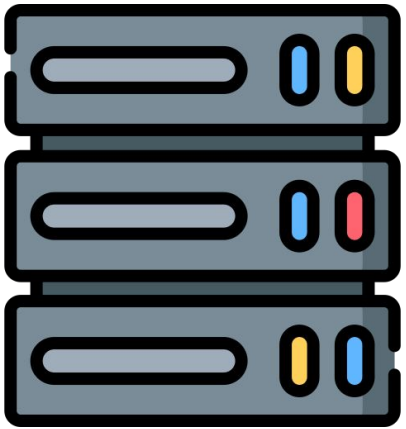
GKR Protocol

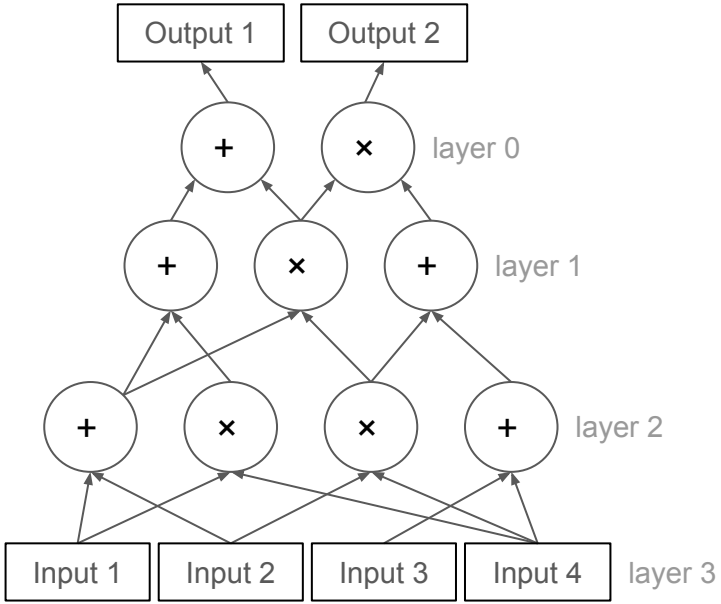
Also all relation function for each layer are given

$\{\tilde{add}_i(g,a,b), \tilde{mult}_i(g,a,b) \mid \forall i\}$

Prover P

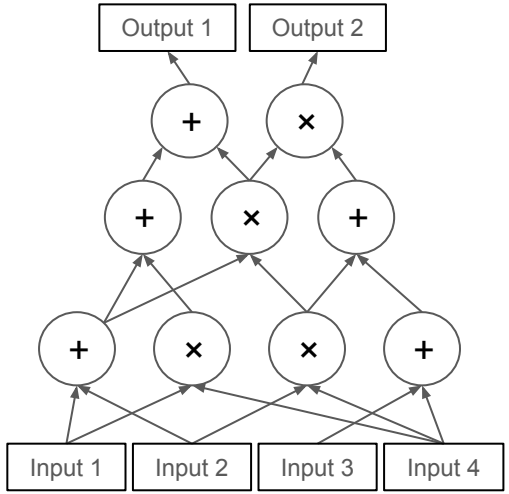
Verifier V





example circuit

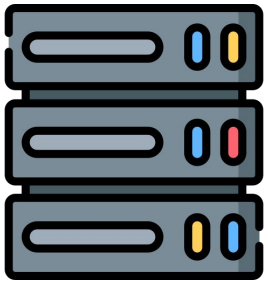
GKR Protocol



output = Output 1 Output 2

Prover P

Verifier V

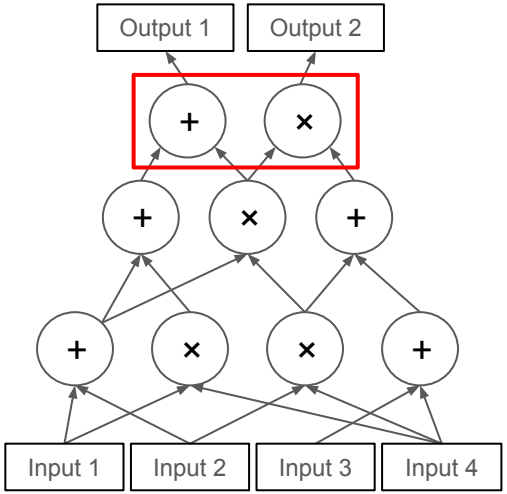


Input

Output

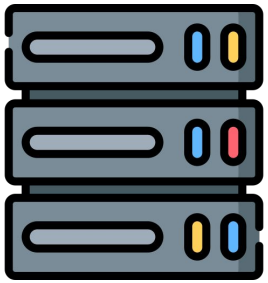
Verifier sends input and receives output

GKR Protocol



Prover P

Verifier V

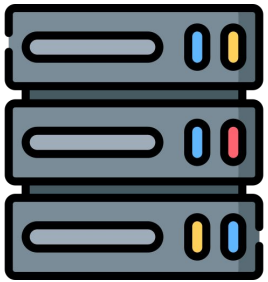


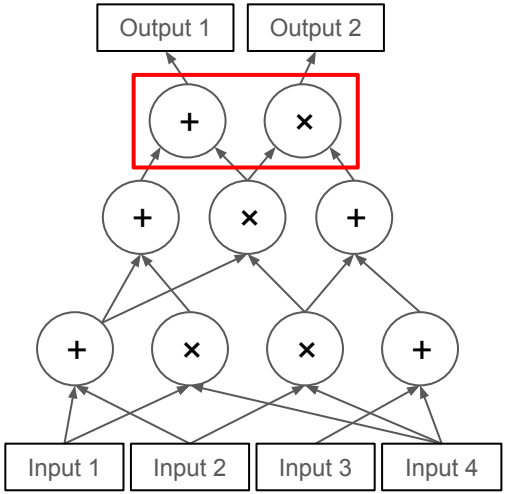
g

Verifier Picks a random label from the first layer

GKR Protocol

Prover P





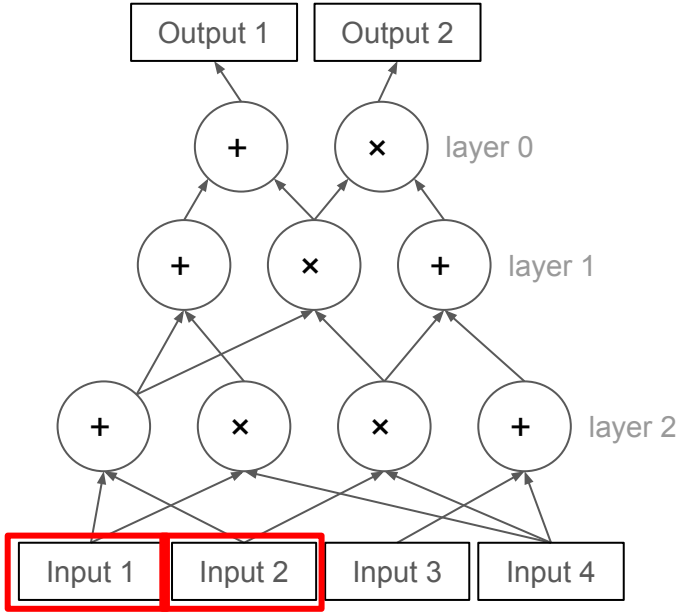
Verifier V

Both parties compute $V_0(g)$ (the g-th gate output)
Verifier validates $V_0(g)$ using sumcheck

GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$



GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

Lagrange interpolation:

$$\chi_h(x) = \prod_{h' \in H \setminus \{h\}} \frac{h' - x}{h' - h}$$

$$\begin{cases} 1, & h = x \\ 0, & h \neq x \end{cases}$$ (under binary inputs)

$$\chi_{h_1,\ldots,h_m}(x_1,\ldots,x_m) = \prod_{i=1}^{m} \chi_{h_i}(x_i)$$

$$\begin{cases} 1, & h_1 \ldots h_m = x_1 \ldots x_m \\ 0, & h_1 \ldots h_m \neq x_1 \ldots x_m \end{cases}$$ (under binary inputs)

GKR Protocol (Single Layer Sumcheck)

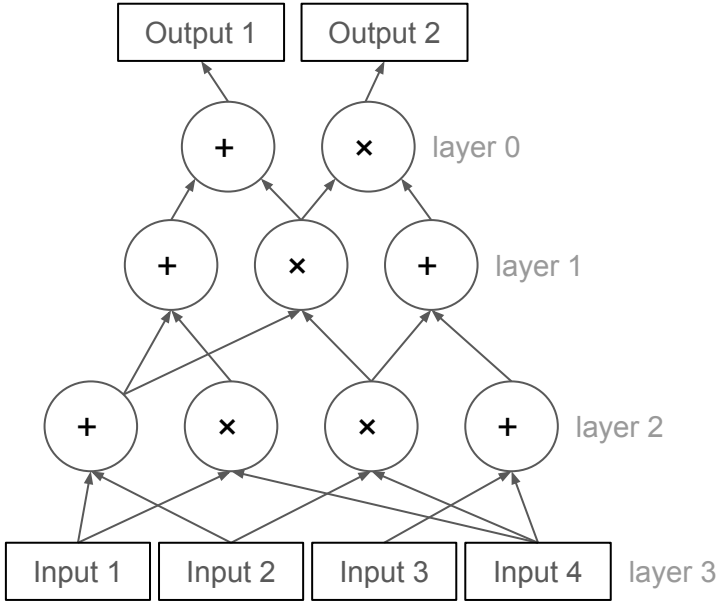
Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)\right)\left(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)\right)\left(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

Define two functions:

$in_{i,1}(g) =$ first fan in neighbor for the ith layer

$in_{i,2}(g) =$ second fan in neighbor for the ith layer



GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)\left(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)\left(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)\right)\right)$$

$$\tilde{add}_{i+1}(g,a,b) = \sum_{z \in \{0,1\}^{s_i}} \chi_{z,in_{i,1}(z),in_{i,2}(z)}(g,a,b)$$

(under binary inputs)

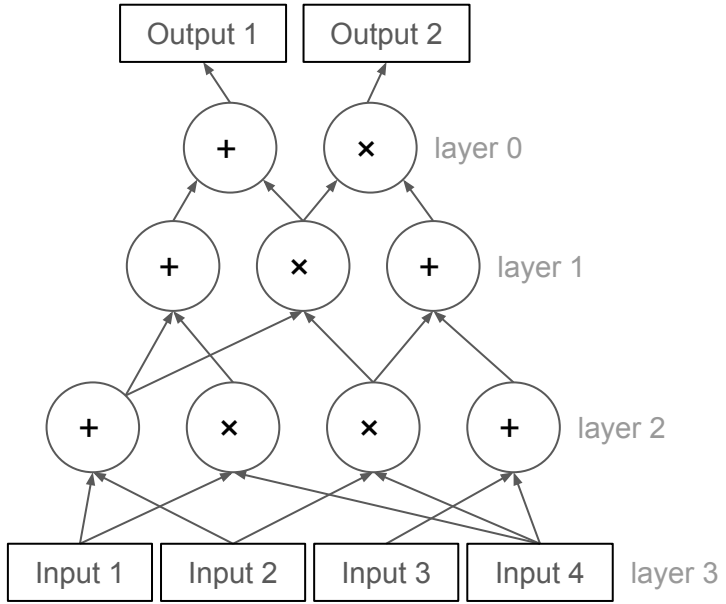
$$\begin{cases} 1, \text{ if a, b} == in_{i,1}(g), in_{i,2}(g) \\ 0, \text{ else} \end{cases}$$

$$\tilde{mult}_{i+1}(g,a,b) = \sum_{z \in \{0,1\}^{s_i}} \chi_{z,in_{i,1}(z),in_{i,2}(z)}(g,a,b)$$

(under binary inputs)

$$\begin{cases} 1, \text{ if a, b} == in_{i,1}(g), in_{i,2}(g) \\ 0, \text{ else} \end{cases}$$

function for each layer is given in the beginning
computed by verifier in the final round



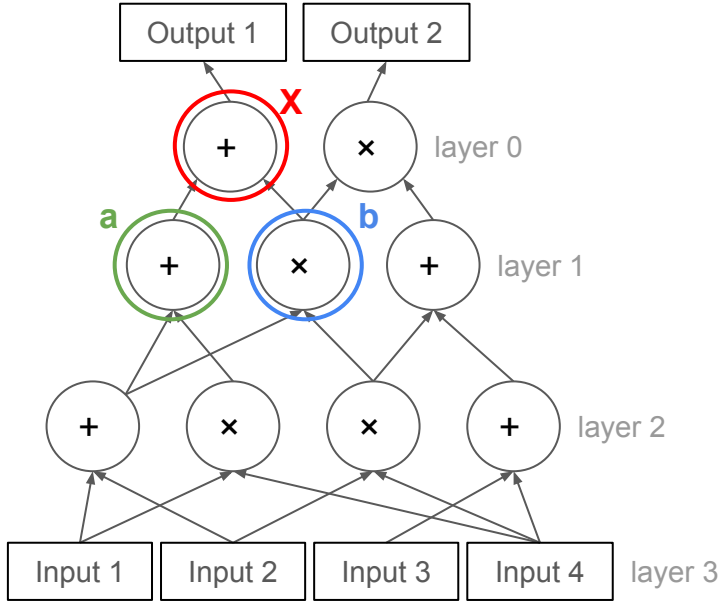
GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)\left(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)\left(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)\right)\right)$$

$\tilde{add}_{i+1}(X,a,b)$ **= 1**

$\tilde{mult}_{i+1}(X,a,b)$ **= 0**



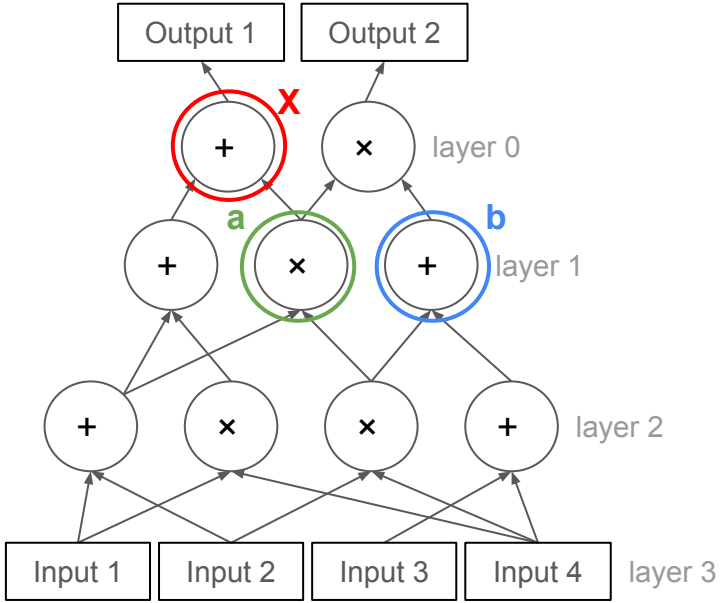
GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)\left(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)\left(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)\right)\right)$$

$$\tilde{add}_{i+1}(X,a,b) = 0$$

$$\tilde{mult}_{i+1}(X,a,b) = 0$$



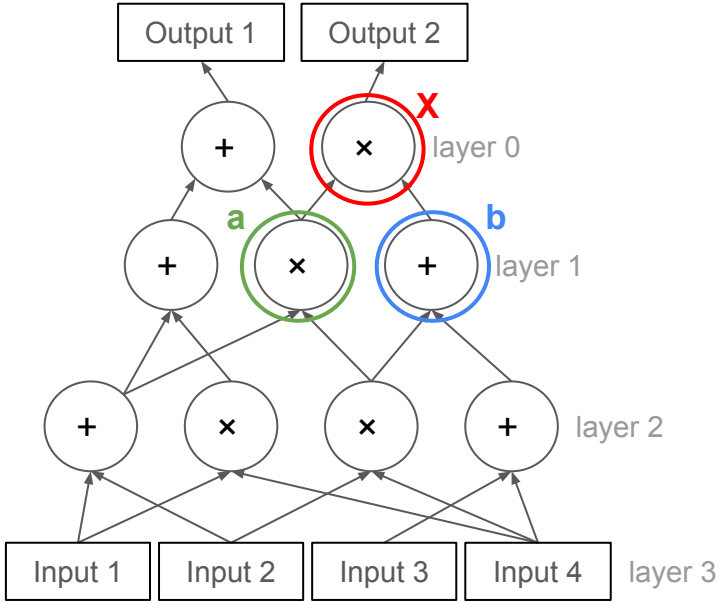
GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)\left(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)\left(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)\right)\right)$$

$\tilde{add}_{i+1}(X,a,b)$ = 0

$\tilde{mult}_{i+1}(X,a,b)$ = 1

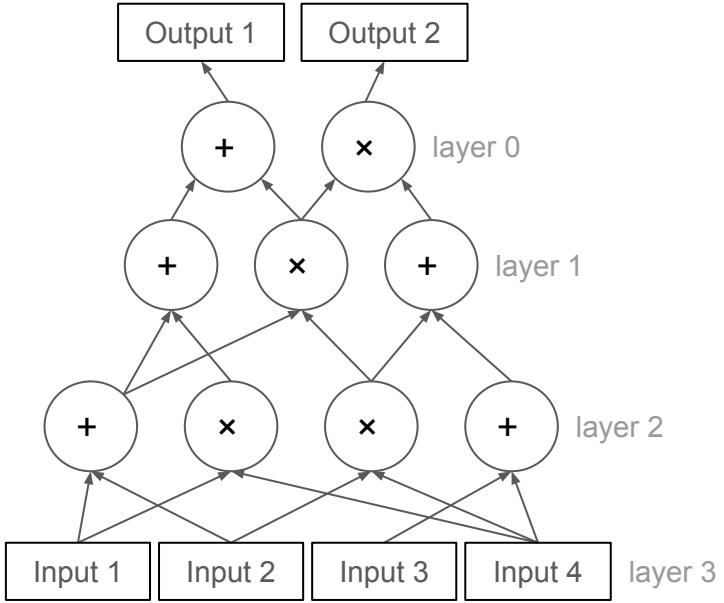


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$$\tilde{V}_{i+1}(X) = \sum_{b \in \{0,1\}^{s_{i+1}}} \chi_b(X) \cdot V(b)$$

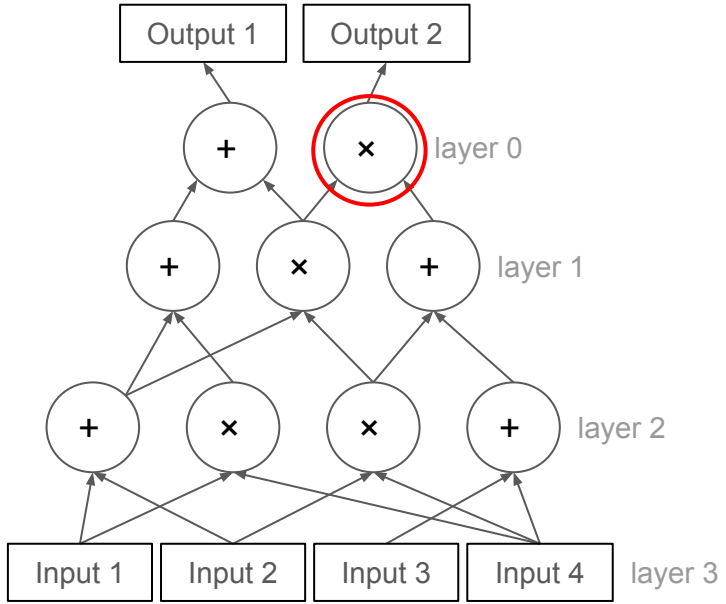


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$\tilde{V}_i(g)$ =

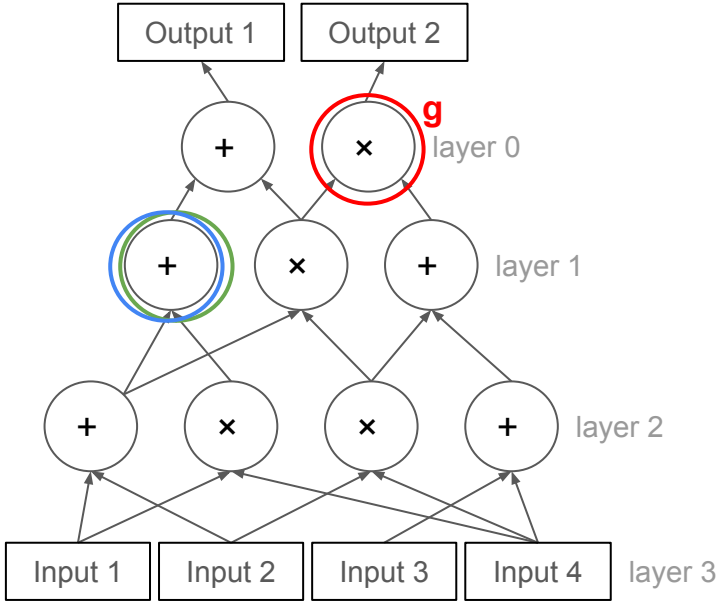


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$\tilde{V}_i(g)$ **= 0**

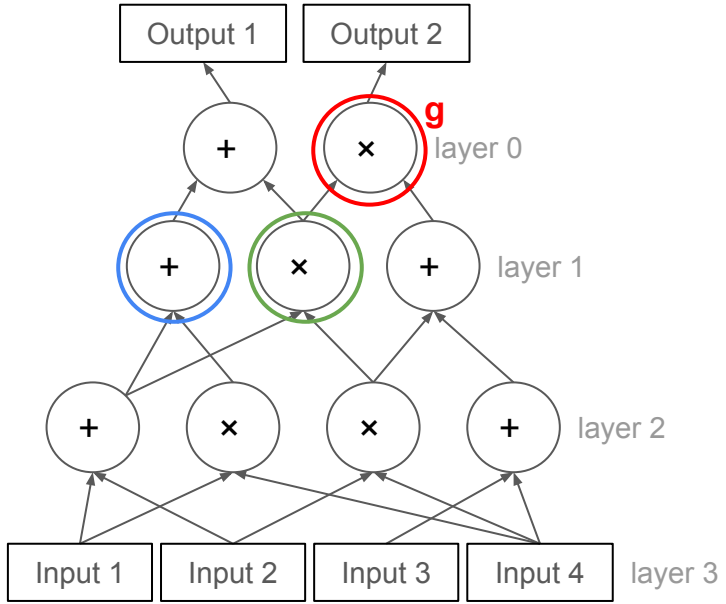


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$\tilde{V}_i(g)$ **= 0 + 0**

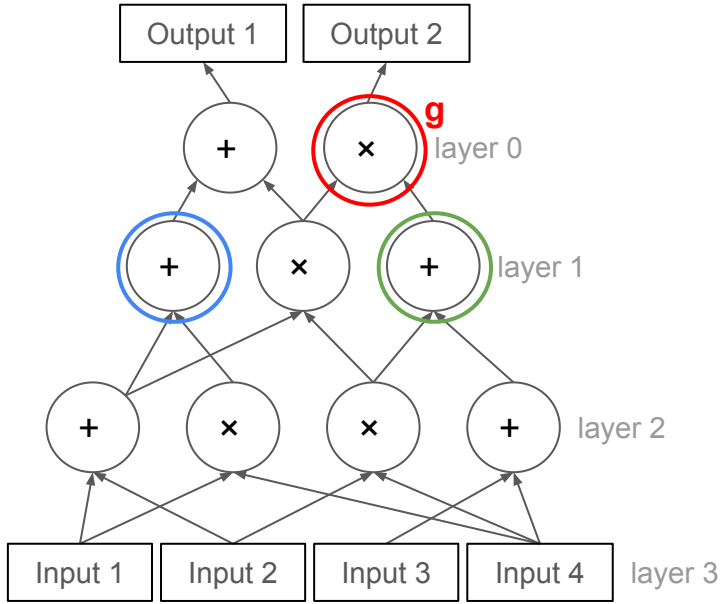


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$\tilde{V}_i(g)$ **= 0 + 0 + 0**

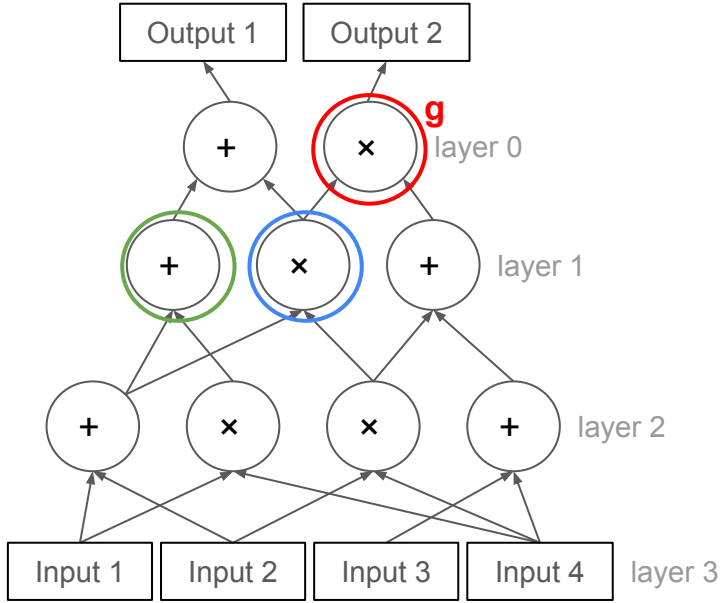


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$\tilde{V}_i(g)$ **= 0 + 0 + 0 + 0**

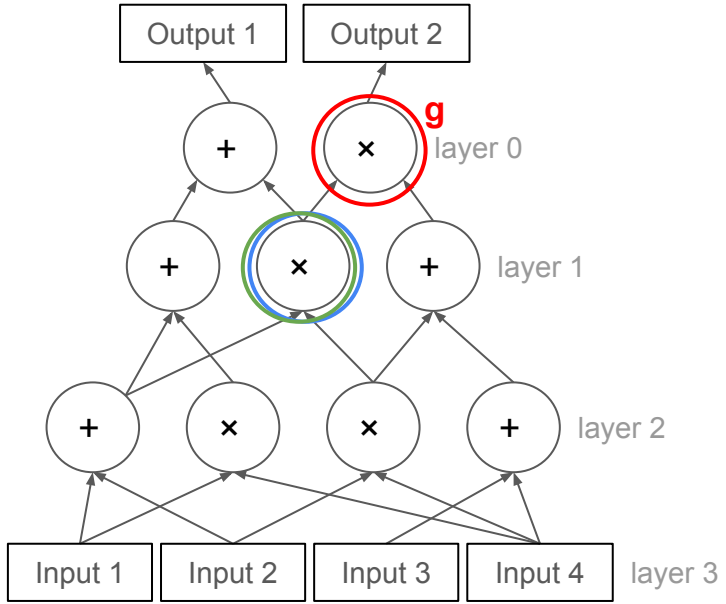


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$\tilde{V}_i(g)$ **= 0 + 0 + 0 + 0 + 0**

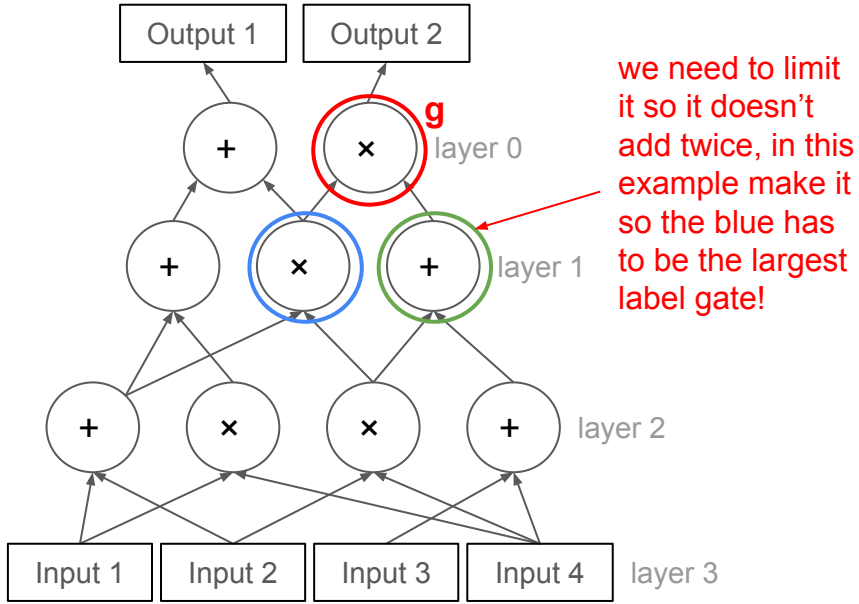


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$\tilde{V}_i(g)$ **= 0 + 0 + 0 + 0 + 0 + 0**

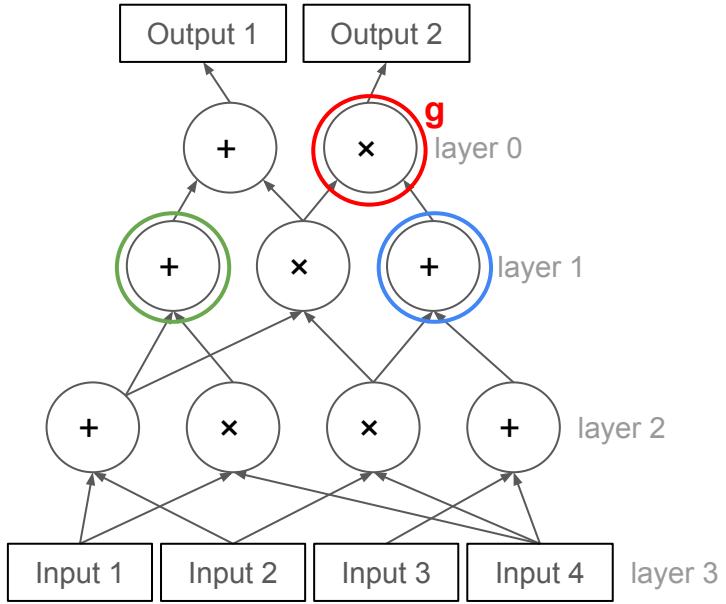


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$\tilde{V}_i(g)$ **= 0 + 0 + 0 + 0 + 0 + 0 + 0**

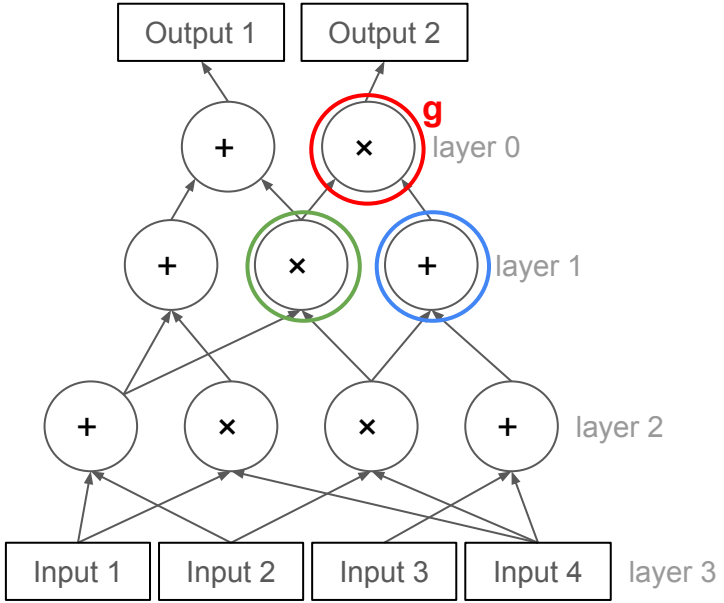


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$$\tilde{V}_i(g) = 0 + 0 + 0 + 0 + 0 + 0 + 0$$
$$+ \tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)$$

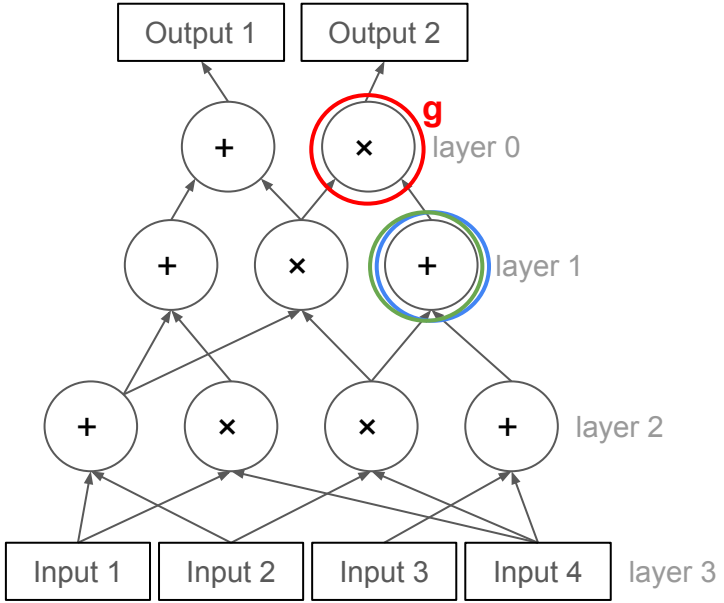


GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$$\tilde{V}_i(g) = 0 + 0 + 0 + 0 + 0 + 0 + 0 + \tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b) + 0$$



GKR Protocol (Single Layer Sumcheck)

Sumcheck is performed on the following multivariate polynomial:

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

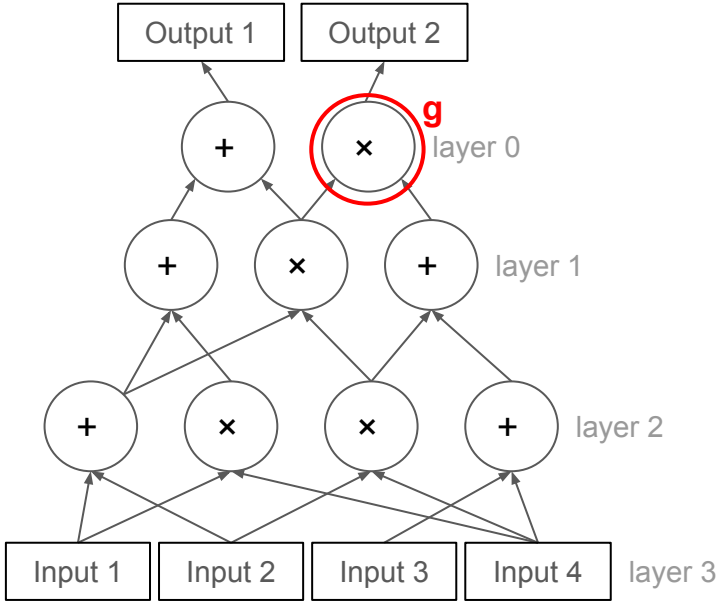
$\tilde{V}_i(g)$ **= 0 + 0 + 0 + 0 + 0 + 0 + 0**

+ $\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)$ **+ 0**

$\tilde{V}_i(g)$ **is a multivariate polynomial**

of $a_1, \ldots, a_m$ **and** $b_1, \ldots, b_m$

perform sumcheck on it!



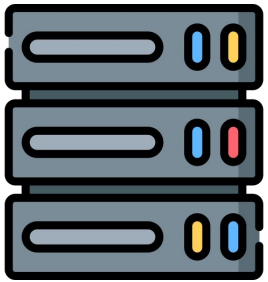
GKR Protocol (Single Layer Sumcheck)

$$\tilde{V}_0(g,t) = \sum_{a\in\{0,1\}^{(s_{i+1}-1)},b\in\{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(X,t,a,b)(\tilde{V}_{i+1}(t,a)+\tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(X,t,a,b)(\tilde{V}_{i+1}(t,a)\times\tilde{V}_{i+1}(b)\right)$$

$$\underline{a_1}, \underline{a_2}, \ldots, \underline{a_{s_{i+1}}}, \quad \underline{b_1}, \underline{b_2}, \ldots, \underline{b_{s_{i+1}}}$$

Prover P

Verifier V



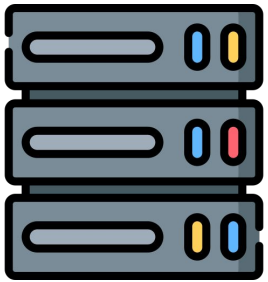
$\tilde{V}_0(g,t)$

Prover sends univariate polynomial regarding the first bit of ***a*** (a_1)

GKR Protocol (Single Layer Sumcheck)

$\underline{a_1}, \underline{a_2}, \ldots, \underline{a_{s_{i+1}}}, \quad \underline{b_1}, \underline{b_2}, \ldots, \underline{b_{s_{i+1}}}$

Prover P



$\tilde{V}_0(g) == \tilde{V}_0(g,0) + \tilde{V}_0(g,1)$

Verifier V

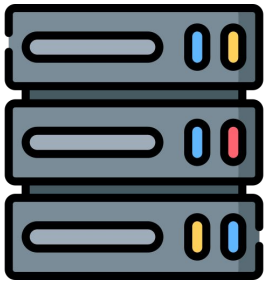
Verifier uses it to verify $\tilde{V}_0(g) == \tilde{V}_0(g,0) + \tilde{V}_0(g,1)$

GKR Protocol (Single Layer Sumcheck)

$$\underline{r_1}, \underline{a_2}, \ldots, \underline{a_{s_{i+1}}}, \quad \underline{b_1}, \underline{b_2}, \ldots, \underline{b_{s_{i+1}}}$$

Prover P

Verifier V



r_1

Verifier sends a random value r_1

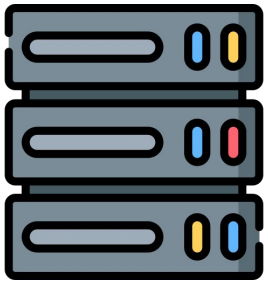
GKR Protocol (Single Layer Sumcheck)

$$\tilde{V}_0(g, r_1, t) = \sum_{a \in \{0,1\}^{(s_{i+1}-2)}, b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(X, r_1, t, a, b)(\tilde{V}_{i+1}(r_1, t, a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(X, r_1, t, a, b)(\tilde{V}_{i+1}(r_1, t, a) \times \tilde{V}_{i+1}(b)\right)$$

$$\underline{r_1}, \underline{a_2}, \ldots, \underline{a_{s_{i+1}}}, \quad \underline{b_1}, \underline{b_2}, \ldots, \underline{b_{s_{i+1}}}$$

Prover P

Verifier V



$\tilde{V}_0(g, r_1, t)$

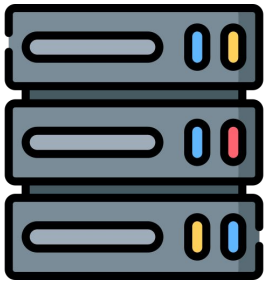
Prover uses r_1 to make the next univariate polynomial in regards to the second bit of ***a*** (a_2)

GKR Protocol (Single Layer Sumcheck)

$$\underline{r_1}, \underline{r_2}, \ldots, \underline{r_{s_{i+1}}}, \quad \underline{r_{s_{i+1}+1}}, \underline{r_{s_{i+1}+2}}, \ldots, \underline{r_{2s_{i+1}-1}}, \underline{b_{s_{i+1}}}$$

Prover P

Verifier V



r_2

$\tilde{V}_0(g, r_1, r_2, t)$

$\tilde{V}_0(g, r_1, ..., r_{2s_{i+1}-1}, t)$

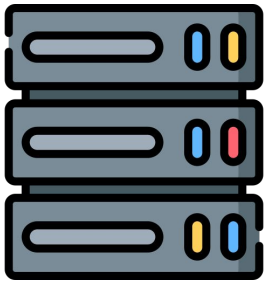
The protocol proceeds as in sumcheck until the last point is randomly selected

GKR Protocol (Single Layer Sumcheck)

u *v*

$r_1, r_2, \ldots, r_{s_{i+1}}$, $r_{s_{i+1}+1}, r_{s_{i+1}+2}, \ldots, r_{2s_{i+1}}$

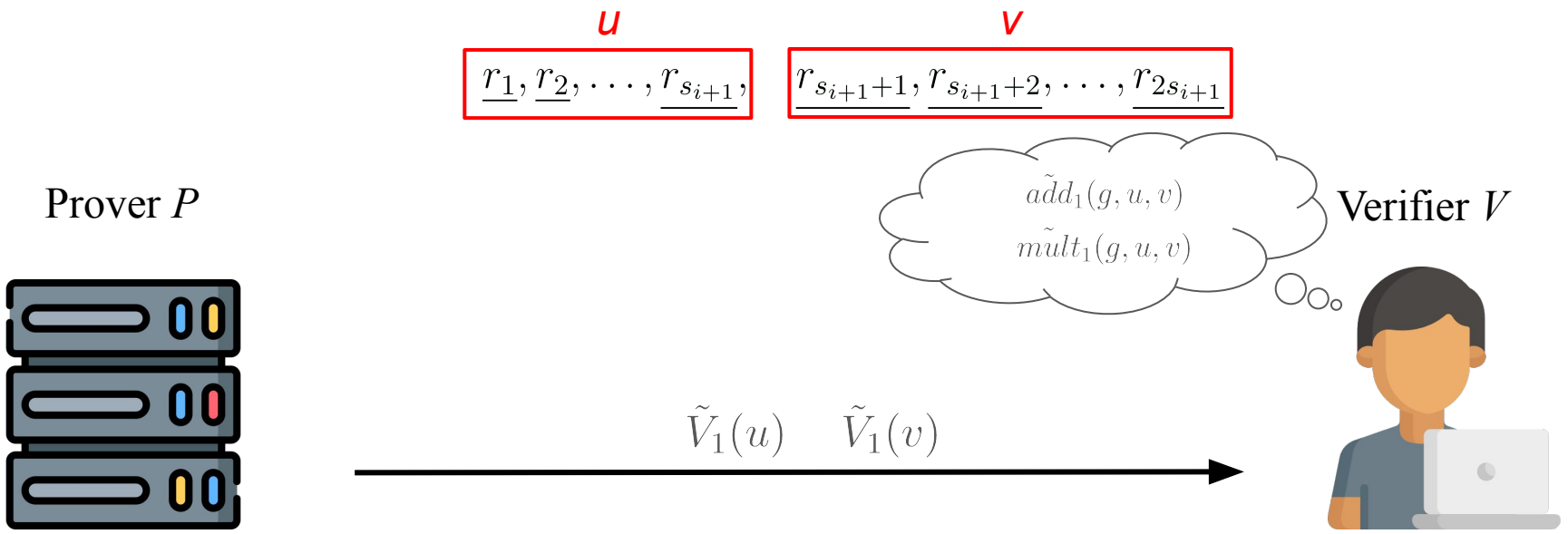
Prover P



Verifier V

Once the last point is selected denote the first half as *u* and the other half as *v*
then $\tilde{V}_0(g, r_1, \ldots, r_{2s_{i+1}})$ *needs to be verified*

GKR Protocol (Single Layer Sumcheck)



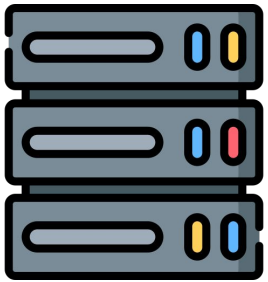
Prover sends $\tilde{V}_1(u)$ and $\tilde{V}_1(v)$

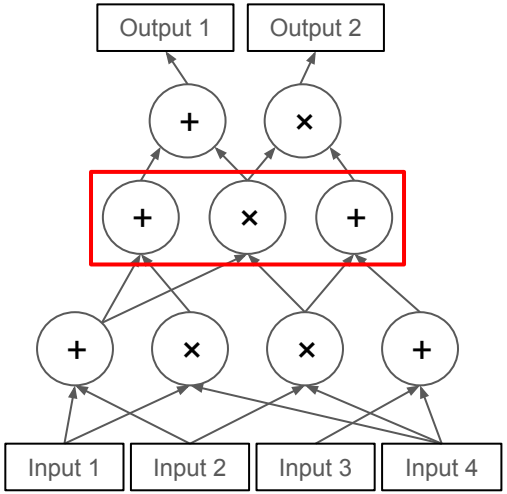
Verifier computes locally for $\tilde{add}_1(g,u,v)$ $\tilde{mult}_1(g,u,v)$

Verifier checks $\tilde{V}_0(g, r_1, ..., r_{2s_{i+1}}) == \tilde{add}_1(g,u,v)\big(\tilde{V}_1(u) + \tilde{V}_1(v)\big) + \tilde{mult}_1(g,u,v)\big(\tilde{V}_1(u)\tilde{V}_1(v)\big)$

GKR Protocol

Prover P

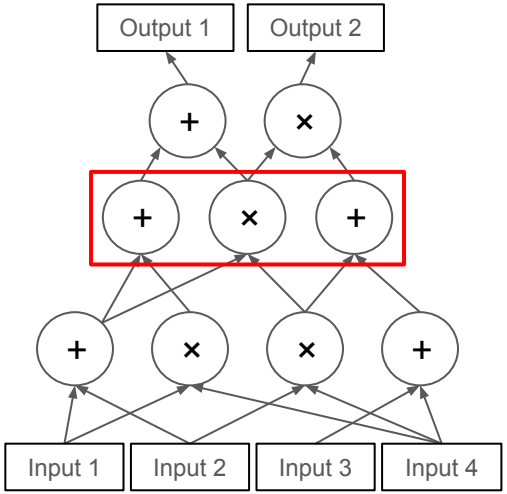




Verifier V

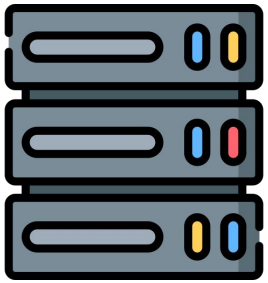
The two claims $\tilde{V}_1(u)$ and $\tilde{V}_1(v)$ on the next layer now needs to be verified

GKR Protocol



Prover P

Verifier V

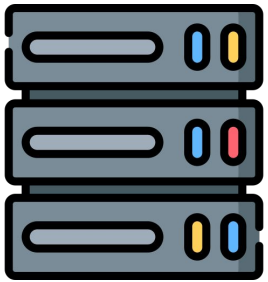


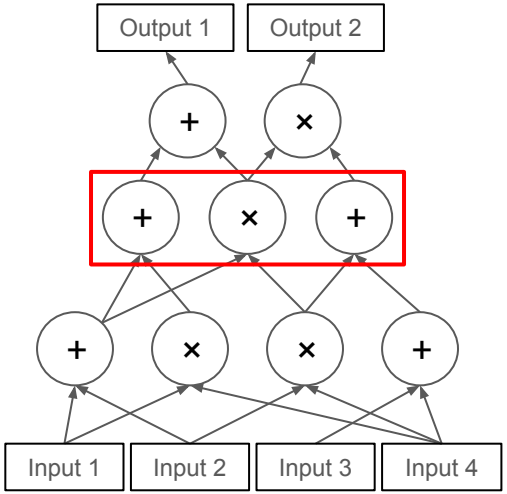
r_{1-1} r_{1-2}

For the new two claims Verifier randomly selects two random values r_{1-1}, r_{1-2}

GKR Protocol

Prover P





Verifier V

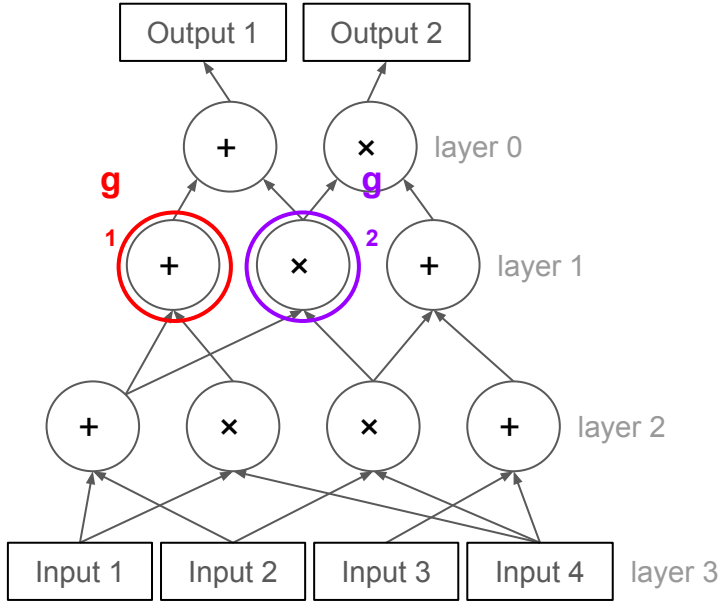
Prover uses $r_{1-1} r_{1-2}$ to perform linear combination on $\tilde{V}_1(u)$ and $\tilde{V}_1(v)$

GKR Protocol (Linear Combination)

Sumcheck is performed on the following multivariate polynomial:

$$r_{i-1}\tilde{V}_i(g_1) + r_{i-2}\tilde{V}_i(g_2) = r_{i-1} \sum_{a,b\in\{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g_1,a,b)\right)\left(\tilde{V}_{i+1}(a)+\tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g_1,a,b)\right)\left(\tilde{V}_{i+1}(a)\times\tilde{V}_{i+1}(b)\right)$$

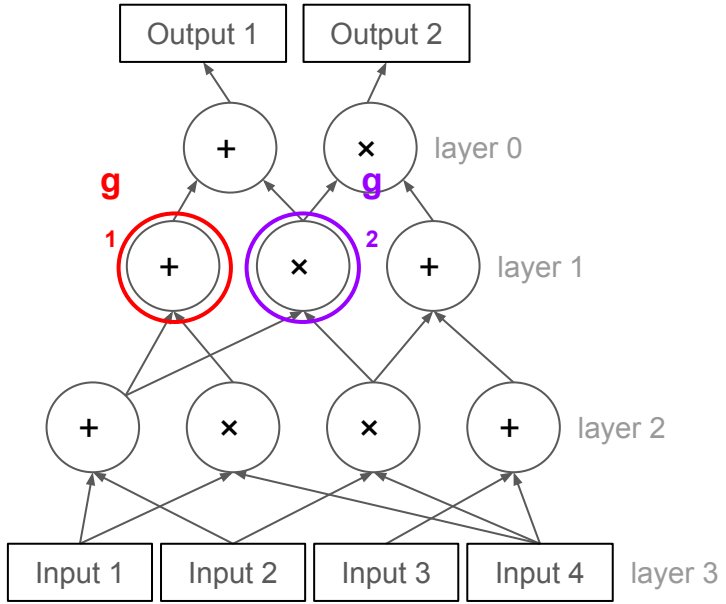
$$+ r_{i-2} \sum_{a,b\in\{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g_2,a,b)\right)\left(\tilde{V}_{i+1}(a)+\tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g_2,a,b)\right)\left(\tilde{V}_{i+1}(a)\times\tilde{V}_{i+1}(b)\right)$$



GKR Protocol (Linear Combination)

Sumcheck is performed on the following multivariate polynomial:

$$r_{i-1}\tilde{V}_i(g_1) + r_{i-2}\tilde{V}_i(g_2) = \sum_{a,b\in\{0,1\}^{s_{i+1}}} \left(r_{i-1}\tilde{add}_{i+1}(g_1,a,b) + r_{i-2}\tilde{add}_{i+1}(g_2,a,b)\right)\left(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right)$$
$$+ \left(r_{1-1}\tilde{mult}_{i+1}(g_1,a,b) + r_{1-2}\tilde{mult}_{i+1}(g_2,a,b)\right)\left(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

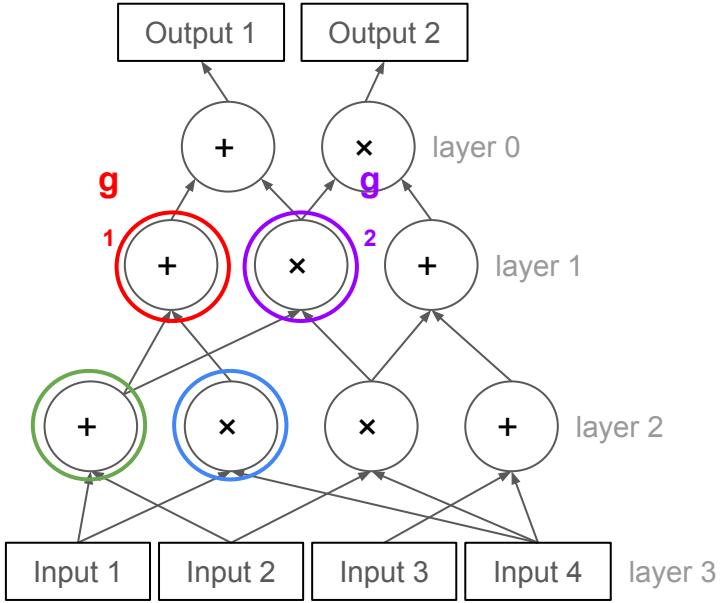


GKR Protocol (Linear Combination)

Sumcheck is performed on the following multivariate polynomial:

$$r_{i-1}\tilde{V}_i(g_1) + r_{i-2}\tilde{V}_i(g_2) = \sum_{a,b\in\{0,1\}^{s_{i+1}}} \left(r_{i-1}\tilde{add}_{i+1}(g_1,a,b) + r_{i-2}\tilde{add}_{i+1}(g_2,a,b)\right)\left(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right)$$
$$+ \left(r_{1-1}\tilde{mult}_{i+1}(g_1,a,b) + r_{1-2}\tilde{mult}_{i+1}(g_2,a,b)\right)\left(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

output : $r_{i-1}\left(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right)$

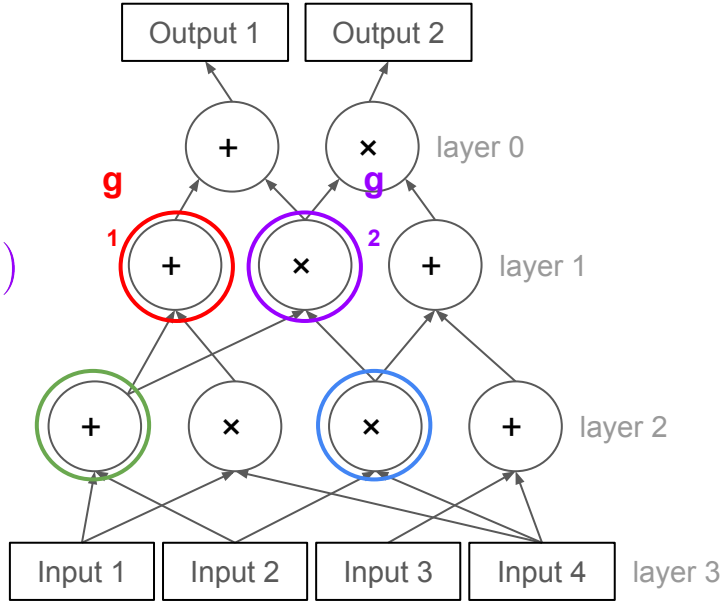


GKR Protocol (Linear Combination)

Sumcheck is performed on the following multivariate polynomial:

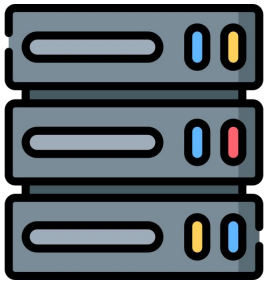
$$r_{i-1}\tilde{V}_i(g_1) + r_{i-2}\tilde{V}_i(g_2) = \sum_{a,b\in\{0,1\}^{s_{i+1}}} \left(r_{i-1}\tilde{add}_{i+1}(g_1,a,b) + r_{i-2}\tilde{add}_{i+1}(g_2,a,b)\right)\left(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right)$$
$$+ \left(r_{1-1}\tilde{mult}_{i+1}(g_1,a,b) + r_{1-2}\tilde{mult}_{i+1}(g_2,a,b)\right)\left(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

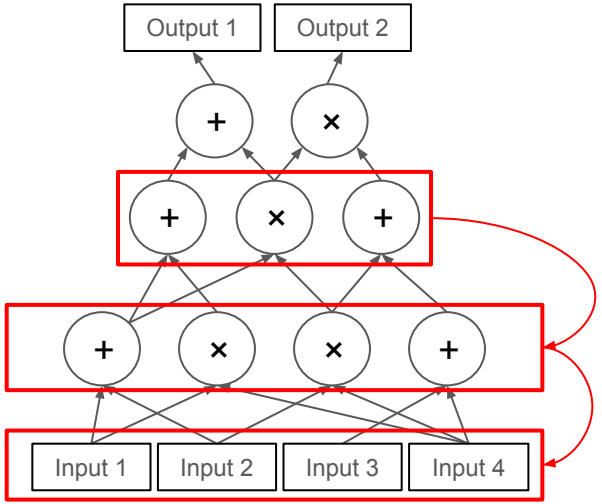
output : $r_{i-2}\left(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$



GKR Protocol

Prover P



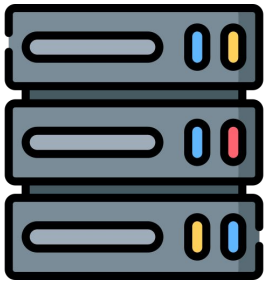


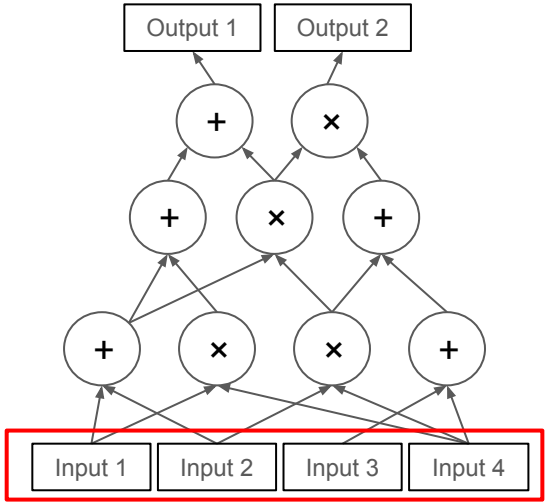
Verifier V

Sumcheck is then performed on $\tilde{V}_{i-1}(g_1) + r_{i-2}\tilde{V}_i(g_2)$, in the end verifier selects two random gates, repeat until the input layer is reached

GKR Protocol

Prover P





Verifier V

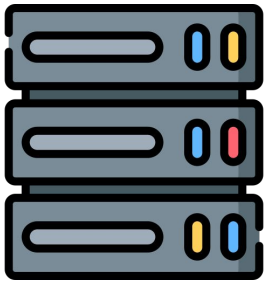
Verifier then validates the two labels values with it's own input

ZK GKR Protocol

Assume there are d layers in the arithmetic circuit

declare d random polynomials $R_1(X, w), ..., R_d(X, w)$
also commits to every polynomial with $r_1, \ldots, r_d$
to get $com_{R_1}, \ldots, com_{R_d}$

Prover P



Verifier V

Prover defines random polynomial for each layer used to mask the gate outputs
and commits to those polynomials using $r_1, \ldots, r_d$ to get $com_{R_1}, \ldots, com_{R_d}$

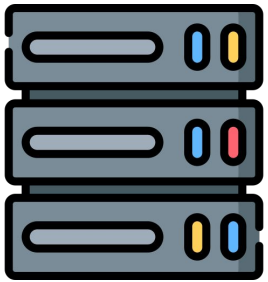
ZK GKR Protocol

$$\tilde{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

$$\dot{V}_i(g) = \sum_{a,b \in \{0,1\}^{s_{i+1}}, w \in \{0,1\}} I(\vec{0},w)\left(\tilde{add}_{i+1}(g,a,b)(\dot{V}_{i+1}(a) + \dot{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(g,a,b)(\dot{V}_{i+1}(a) \times \dot{V}_{i+1}(b)\right) + I(\vec{0},(a,b))Z(g)R_i(g_1,w)$$

Prover P

Verifier V



$\chi_{\vec{0}}(a,b)$ { 1, if (a, b) = 0
0, else

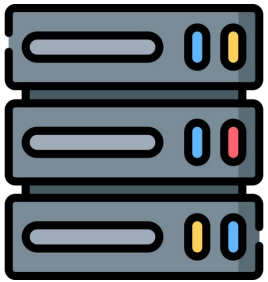
$$\prod_{i=1}^{n} z_i(1-z_i)$$

Prover defines random polynomial for each layer used to mask the gate outputs
and commits to those polynomials using $r_1, \ldots, r_d$ to get $com_{R_1}, \ldots, com_{R_d}$

ZK GKR Protocol

$$\dot{V}_0(g) = \sum_{a,b\in\{0,1\}^{s_1},w\in\{0,1\}} I(\vec{0},w)\big(\tilde{add}_1(g,a,b)(\dot{V}_1(a)+\dot{V}_1(b)\big) + \big(\tilde{mult}_1(g,a,b)(\dot{V}_1(a)\times\dot{V}_1(b)\big) + I(\vec{0},(a,b))Z(g)R_0(g_1,w)$$

Prover P



Verifier V

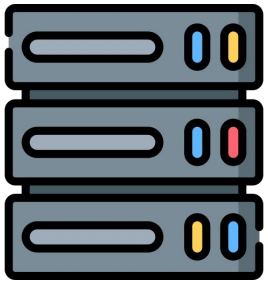
Starting from the output layer, perform ZK Sumcheck consider $R_0(X,w)=0$

ZK GKR Protocol

$$\dot{V}_0(g) = \sum_{a,b\in\{0,1\}^{s_1}, w\in\{0,1\}} I(\vec{0}, w)\big(\tilde{add}_1(g,a,b)(\dot{V}_1(a) + \dot{V}_1(b)\big) + \big(\tilde{mult}_1(g,a,b)(\dot{V}_1(a) \times \dot{V}_1(b)\big) + I(\vec{0}, (a,b))Z(g)R_0(g_1, w)$$

Prover P

Verifier V



$\dot{V}_1(u) \quad \dot{V}_1(v)$

In the last iteration for ZK Sumcheck, three points are selected $u, v \in \mathbb{F}^{s_1}, c \in \mathbb{F}$

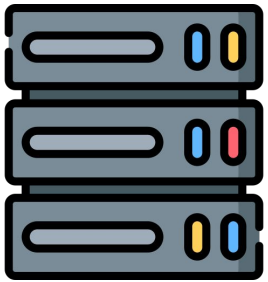
Prover aborts if $u = v$

Prover sends $\dot{V}_1(u) \quad \dot{V}_1(v)$

ZK GKR Protocol

$$\dot{V}_0(g) = \sum_{a,b\in\{0,1\}^{s_1}, w\in\{0,1\}} I(\vec{0}, w)\big(\tilde{add}_1(g,a,b)(\dot{V}_1(a) + \dot{V}_1(b)\big) + \big(\tilde{mult}_1(g,a,b)(\dot{V}_1(a) \times \dot{V}_1(b)\big) + I(\vec{0}, (a,b))Z(g)R_0(g_1, w)$$

Prover P



Verifier V

also Verifier computes $\tilde{add}_1(g,u,v) \quad \tilde{mult}_1(g,u,v)$

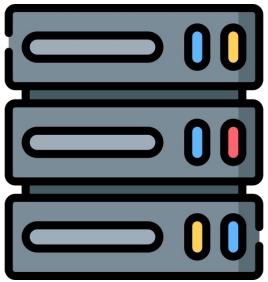
Verifier checks $h_n(r_n) - pg(r_1, ..., r_n) == \tilde{add}_1(g,a,b)(\dot{V}_1(a) + \dot{V}_1(b)) + \tilde{mult}_1(g,a,b)(\dot{V}_1(a) \times \dot{V}_1(b))$

ZK GKR Protocol

$$r_{1-1}\dot{V}_i(u) + r_{1-2}\dot{V}_i(v) = \sum_{a,b\in\{0,1\}^{s_{i+1}},w\in\{0,1\}} I(\vec{0},w)\big((r_{1-1}\tilde{add}_{i+1}(u,a,b) + r_{1-2}\tilde{add}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) + \dot{V}_{i+1}(b)\big) + \big((r_{1-1}\tilde{mult}_{i+1}(u,a,b) + r_{1-2}\tilde{mult}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) \times \dot{V}_{i+1}(b)\big) + I(\vec{0},(a,b))\big(r_{1-1}Z(u)R_i(u_1,w) + r_{1-2}Z(u)R_i(v_1,w)\big)$$

Prover P

Verifier V



r_{1-1} r_{1-2}

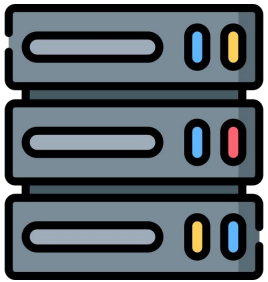
Verifier sends two randomness r_{1-1} r_{1-2} to prover for linear combination

ZK GKR Protocol

$$r_{1-1}\dot{V}_i(u) + r_{1-2}\dot{V}_i(v) = \sum_{a,b\in\{0,1\}^{s_{i+1}},w\in\{0,1\}} I(\vec{0},w)\big((r_{1-1}\tilde{add}_{i+1}(u,a,b) + r_{1-2}\tilde{add}_{i+1}(v,a,b))(\dot{V}_{i+1}(a)+\dot{V}_{i+1}(b))\big) + \big((r_{1-1}\tilde{mult}_{i+1}(u,a,b) + r_{1-2}\tilde{mult}_{i+1}(v,a,b))(\dot{V}_{i+1}(a)\times\dot{V}_{i+1}(b))\big) + I(\vec{0},(a,b))\big(r_{1-1}Z(u)R_i(u_1,w) + r_{1-2}Z(u)R_i(v_1,w)\big)$$

Prover P

Verifier V



$\dot{V}_{i+1}(u^{(i+1)})$ $\dot{V}_{i+1}(v^{(i+1)})$

At the end of ZK Sumcheck for each layer, three points are chosen $u^{(i+1)}, v^{(i+1)} \in \mathbb{F}^{s_{i+1}}, c^{(i)} \in \mathbb{F}$,Prover aborts if $u^{(i+1)} = v^{(i+1)}$

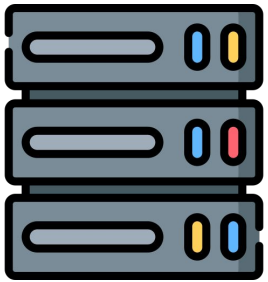
Prover sends $\dot{V}_{i+1}(u^{(i+1)})$ $\dot{V}_{i+1}(v^{(i+1)})$

ZK GKR Protocol

$$r_{1-1}\dot{V}_i(u) + r_{1-2}\dot{V}_i(v) = \sum_{a,b\in\{0,1\}^{s_{i+1}},w\in\{0,1\}} I(\vec{0},w)\big((r_{1-1}\tilde{add}_{i+1}(u,a,b) + r_{1-2}\tilde{add}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) + \dot{V}_{i+1}(b))\big) + \big((r_{1-1}\tilde{mult}_{i+1}(u,a,b) + r_{1-2}\tilde{mult}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) \times \dot{V}_{i+1}(b))\big) + I(\vec{0},(a,b))\big(r_{1-1}Z(u)R_i(u_1,w) + r_{1-2}Z(u)R_i(v_1,w)\big)$$

Prover P

Verifier V



$\dot{V}_{i+1}(u^{(i+1)})$ $\dot{V}_{i+1}(v^{(i+1)})$

Verifier computes: $r_{1-1}\tilde{add}_{i+1}(u^{(i)},u^{(i+1)},v^{(i+1)}) + r_{1-2}\tilde{add}_{i+1}(v^{(i)},u^{(i+1)},v^{(i+1)})$

$r_{1-1}\tilde{mult}_{i+1}(u^{(i)},u^{(i+1)},v^{(i+1)}) + r_{1-2}\tilde{mult}_{i+1}(v^{(i)},u^{(i+1)},v^{(i+1)})$

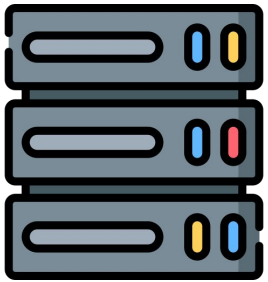
$Z(u^{(i)}), Z(v^{(i)}), I(\vec{0},c^{(i)}), I(\vec{0},(u^{(i+1)},v^{(i+1)}))$

ZK GKR Protocol

$$r_{1-1}\dot{V}_i(u) + r_{1-2}\dot{V}_i(v) = \sum_{a,b\in\{0,1\}^{s_{i+1}},w\in\{0,1\}} I(\vec{0},w)\big((r_{1-1}\tilde{add}_{i+1}(u,a,b) + r_{1-2}\tilde{add}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) + \dot{V}_{i+1}(b)\big) + \big((r_{1-1}\tilde{mult}_{i+1}(u,a,b) + r_{1-2}\tilde{mult}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) \times \dot{V}_{i+1}(b)\big) + I(\vec{0},(a,b))\big(r_{1-1}Z(u)R_i(u_1,w) + r_{1-2}Z(u)R_i(v_1,w)\big)$$

Prover P

Verifier V



$R_i(u_1^{(i)}, c^{(i)}), \pi_{i-u}, R_i(v_1^{(i)}, c^{(i)}), \pi_{i-v}$

Prover opens R_i on two points and sends $(R_i(u_1^{(i)}, c^{(i)}), \pi_{i-u})$ $(R_i(v_1^{(i)}, c^{(i)}), \pi_{i-v})$

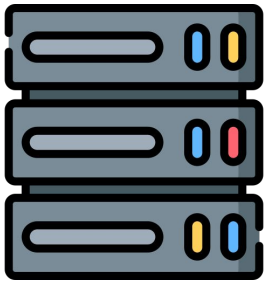
Verifier verify $R_i(u_1^{(i)}, c^{(i)})$, $R_i(v_1^{(i)}, c^{(i)})$

ZK GKR Protocol

$$r_{1-1}\dot{V}_i(u) + r_{1-2}\dot{V}_i(v) = \sum_{a,b\in\{0,1\}^{s_{i+1}},w\in\{0,1\}} I(\vec{0},w)\big((r_{1-1}\tilde{add}_{i+1}(u,a,b) + r_{1-2}\tilde{add}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) + \dot{V}_{i+1}(b)\big) + \big((r_{1-1}\tilde{mult}_{i+1}(u,a,b) + r_{1-2}\tilde{mult}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) \times \dot{V}_{i+1}(b)\big) + I(\vec{0},(a,b))\big(r_{1-1}Z(u)R_i(u_1,w) + r_{1-2}Z(u)R_i(v_1,w)\big)$$

Prover P

Verifier V



$$R_i(u^{(i)}, c^{(i)}), \pi_{i-u}, R_i(v^{(i)}, c^{(i)}), \pi_{i-v}$$

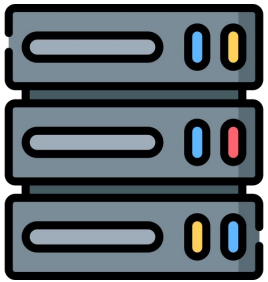
Verifier checks

$$h_n(r_n) - pg(r_1,...,r_n) == I(\vec{0},c^{(i)})\big((r_{1-1}\tilde{add}_{i+1}(u^{(i)},u^{(i+1)},v^{(i+1)}) + r_{1-2}\tilde{add}_{i+1}(v^{(i)},u^{(i+1)},v^{(i+1)}))(\dot{V}_{i+1}(u^{(i+1)}) + \dot{V}_{i+1}(v^{(i+1)}))$$
$$+(r_{1-1}mult_{i+1}(u^{(i)},u^{(i+1)},v^{(i+1)}) + r_{1-2}mult_{i+1}(v^{(i)},u^{(i+1)},v^{(i+1)}))(\dot{V}_{i+1}(u^{(i+1)}) \times \dot{V}_{i+1}(v^{(i+1)}))\big)$$
$$+I(\vec{0},(u^{(i+1)},v^{(i+1)}))(r_{1-1}Z(u^{(i)})R_i(u^{(i)},c^{(i)}) + r_{1-2}Z(v^{(i)})R_i(v^{(i)},c^{(i)}))$$

ZK GKR Protocol

$$r_{1-1}\dot{V}_i(u) + r_{1-2}\dot{V}_i(v) = \sum_{a,b\in\{0,1\}^{s_{i+1}},w\in\{0,1\}} I(\vec{0},w)\big((r_{1-1}\tilde{add}_{i+1}(u,a,b) + r_{1-2}\tilde{add}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) + \dot{V}_{i+1}(b)\big) + \big((r_{1-1}\tilde{mult}_{i+1}(u,a,b) + r_{1-2}\tilde{mult}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) \times \dot{V}_{i+1}(b)\big) + I(\vec{0},(a,b))\big(r_{1-1}Z(u)R_i(u_1,w) + r_{1-2}Z(u)R_i(v_1,w)\big)$$

Prover P



Verifier V

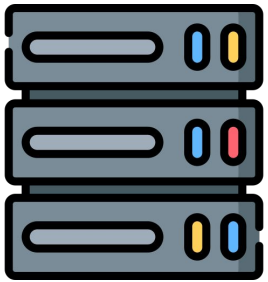
Then repeat the verifying process for the next layer

ZK GKR Protocol

$$r_{1-1}\dot{V}_i(u) + r_{1-2}\dot{V}_i(v) = \sum_{a,b\in\{0,1\}^{s_{i+1}},w\in\{0,1\}} I(\vec{0},w)\big((r_{1-1}\tilde{add}_{i+1}(u,a,b) + r_{1-2}\tilde{add}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) + \dot{V}_{i+1}(b)\big) + \big((r_{1-1}\tilde{mult}_{i+1}(u,a,b) + r_{1-2}\tilde{mult}_{i+1}(v,a,b))(\dot{V}_{i+1}(a) \times \dot{V}_{i+1}(b)\big) + I(\vec{0},(a,b))\big(r_{1-1}Z(u)R_i(u_1,w) + r_{1-2}Z(u)R_i(v_1,w)\big)$$

Prover P

Verifier V



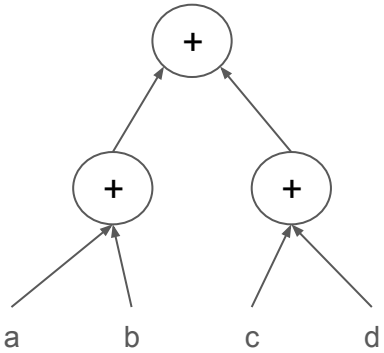
$R_d(u_1^{(d)},0), R_d(u_1^{(d)},1), R_d(v_1^{(d)},0), R_d(v_1^{(d)},1)$

Once the input layer is reached Verifier now has two claims on $\dot{V}_d(v^{(d)})$ $\dot{V}_d(u^{(d)})$

Open R_d on four points $R_d(u^{(d)},0), R_d(u^{(d)},1), R_d(v^{(d)},0), R_d(v^{(d)},1)$ and verify them,

Last Verifier checks $\dot{V}_d(u^{(d)}) == \tilde{V}_d(u^{(d)}) + \sum_{w\in\{0,1\}} R_d(u_1^{(d)},w)$ and $\dot{V}_d(v^{(d)}) == \tilde{V}_d(v^{(d)}) + \sum_{w\in\{0,1\}} R_d(v_1^{(d)},w)$

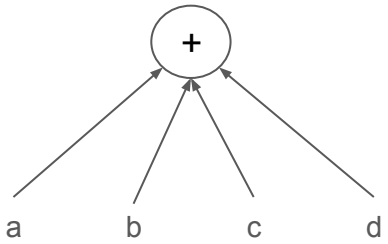
GKR Protocol (Generalized)



$$\tilde{add}_{i+1}(X, a, b)\begin{cases} 1, \text{ if gate a, b inputs to add gate} \\ X \\ 0, \text{ else} \end{cases}$$

two input per add gate

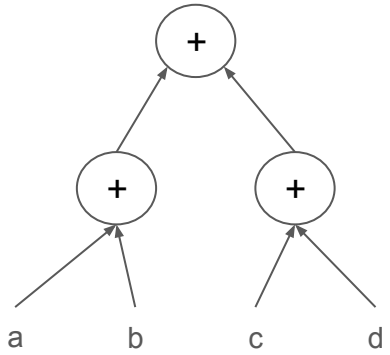
GKR Protocol (Generalized)



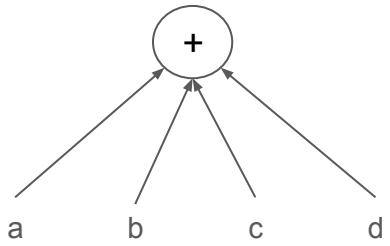
$$X\tilde{add}_{i+1}(X,a)\begin{cases}1, \text{ if gate a inputs to add gate X}\\ 0, \text{ else}\end{cases}$$

multiple input per add gate

GKR Protocol (Generalized)



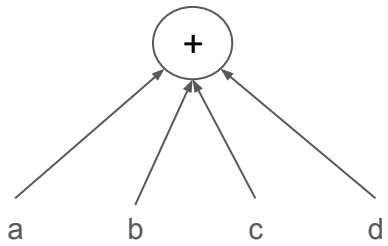
$$\tilde{V}_i(X) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\tilde{add}_{i+1}(X,a,b)(\tilde{V}_{i+1}(a) + \tilde{V}_{i+1}(b)\right) + \left(\tilde{mult}_{i+1}(X,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$



$$\tilde{V}_i(X) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\chi_0(b)\tilde{add}_{i+1}(X,a)(\tilde{V}_{i+1}(a)\right) + \left(\tilde{mult}_{i+1}(X,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

GKR Protocol (Generalized)

This is used in Convolution layer

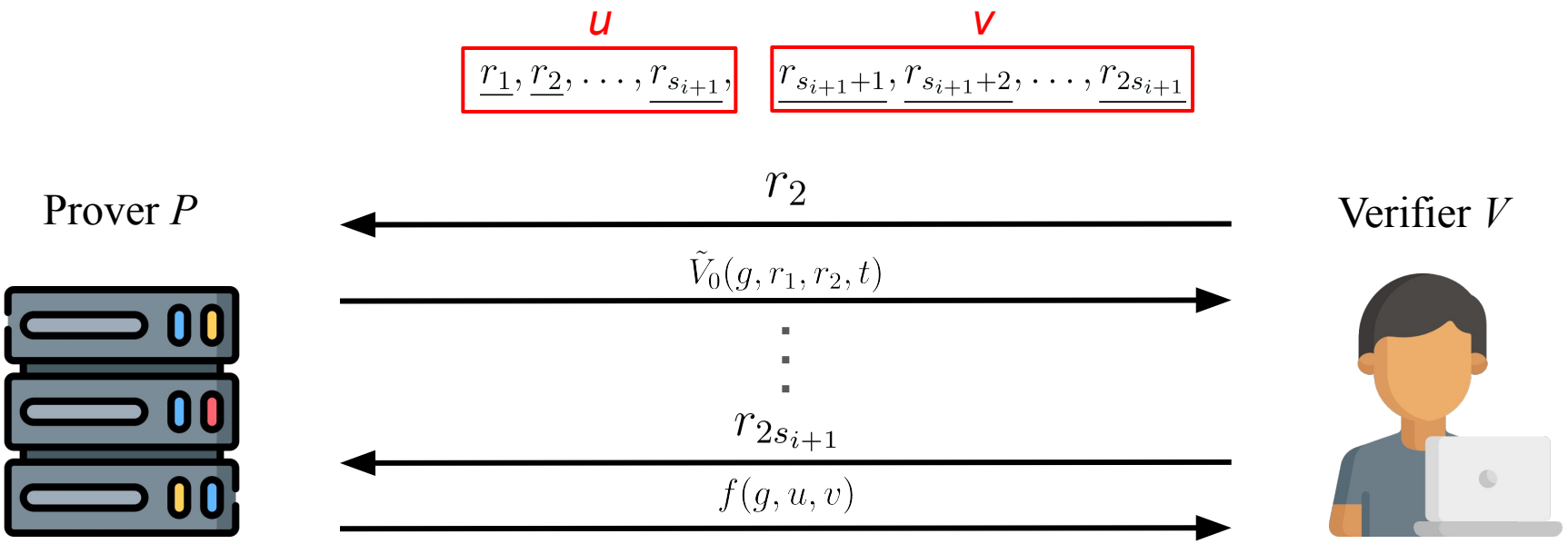


$$\tilde{V}_i(X) = \sum_{a,b \in \{0,1\}^{s_{i+1}}} \left(\chi_0(b)\tilde{add}_{i+1}(X,a)(\tilde{V}_{i+1}(a)\right) + \left(\tilde{mult}_{i+1}(X,a,b)(\tilde{V}_{i+1}(a) \times \tilde{V}_{i+1}(b)\right)$$

GKR Protocol (CMT - GKR)

Instead of combining two claims using linear combination, there is an alternative method to reduce the two claim into one

GKR Protocol (CMT - GKR)



At the end of sumcheck two random labels are given, denote the first label as ***u*** and the second label as ***v***

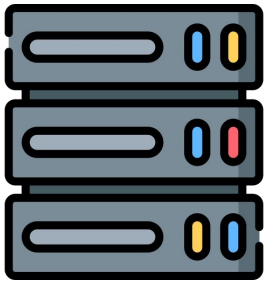
GKR Protocol (CMT - GKR)

define a line *L* used only in the next layer, where *L(0)* = *u* and *L(1)* = *v*

u *v*

$$\underline{r_1}, \underline{r_2}, \ldots, \underline{r_{s_{i+1}}}, \quad \underline{r_{s_{i+1}+1}}, \underline{r_{s_{i+1}+2}}, \ldots, \underline{r_{2s_{i+1}}}$$

Prover P



Verifier V

Instead of ending it right there, further define a line where ***L(0)* = *u*** *and* ***L(1)* = *v***

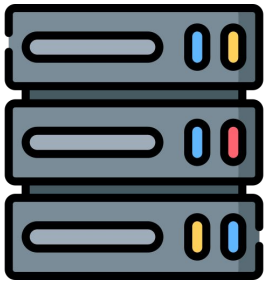
GKR Protocol (CMT - GKR)

define a line *L* used only in the next layer, where *L(0)* = *u* and *L(1)* = *v*

u *v*

$$\underline{r_1}, \underline{r_2}, \ldots, \underline{r_{s_{i+1}}}, \quad \underline{r_{s_{i+1}+1}}, \underline{r_{s_{i+1}+2}}, \ldots, \underline{r_{2s_{i+1}}}$$

Prover P



Verifier V

Prover then uses that line to make $\tilde{f}_{k_i}(r') = \tilde{V}_i(L(r'))$

In the first round of sumcheck, k' is first selected

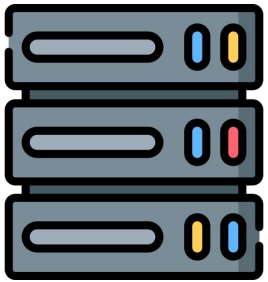
GKR Protocol (CMT - GKR)

define a line *L* used only in the next layer, where *L(0) = u* and *L(1) = v*

u $r_1, r_2, \ldots, r_{s_{i+1}}$, *v* $r_{s_{i+1}+1}, r_{s_{i+1}+2}, \ldots, r_{2s_{i+1}}$

Prover P

Verifier V



$\tilde{h}_i(r') \quad \tilde{V}_1(u) \quad \tilde{V}_1(v)$

Prover sends $\tilde{h}_i(r') \quad \tilde{V}_1(u) \quad \tilde{V}_1(v)$

Verifier uses it to verify whether $\tilde{h}_i(0) = \tilde{V}_i(u) \quad \tilde{h}_i(1) = \tilde{V}_i(v)$