

# $\omega(1/\lambda)$ -Rate Boolean Garbling Scheme from Generic Groups

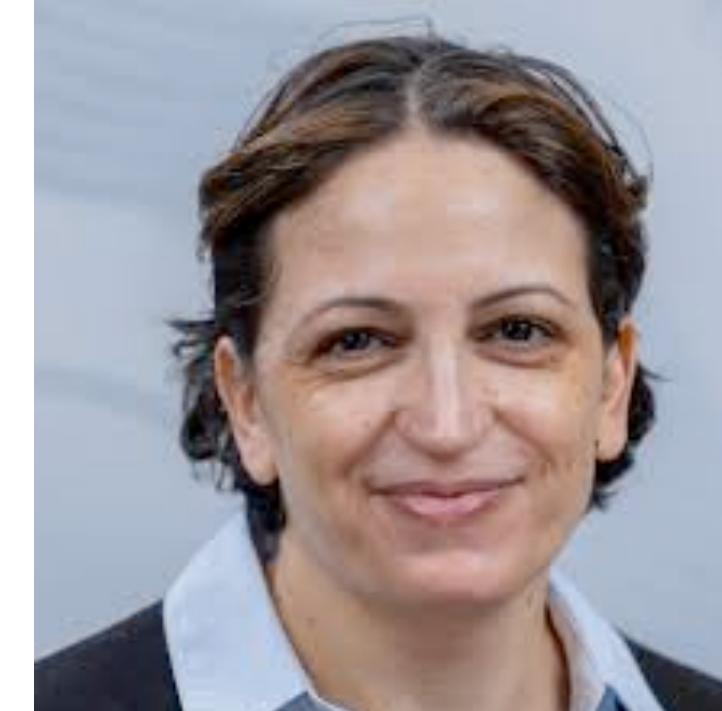
CRYPTO 2025



Geoffroy Couteau

CNRS, IRIF

Université Paris Citè



Carmit Hazay

Bar-Ilan University



**Aditya Hegde**

JHU

Naman Kumar

Oregon State University

# Garbled Circuits

[Yao'86]



Garbler



Evaluator

# Garbled Circuits

[Yao'86]



Garbler



Evaluator

Boolean Circuit  $C$

# Garbled Circuits

[Yao'86]



Garbler



Evaluator

Boolean Circuit  $C$   $\xrightarrow{\text{Garble}}$  Garbled Circuit  $\widehat{C}$



# Garbled Circuits

[Yao'86]



Garbler



Evaluator

Boolean Circuit  $C$   $\xrightarrow{\text{Garble}}$  Garbled Circuit  $\widehat{C}$



Input  $x$

# Garbled Circuits

[Yao'86]



Garbler



Evaluator

Boolean Circuit  $C$   $\xrightarrow{\text{Garble}}$  Garbled Circuit  $\widehat{C}$

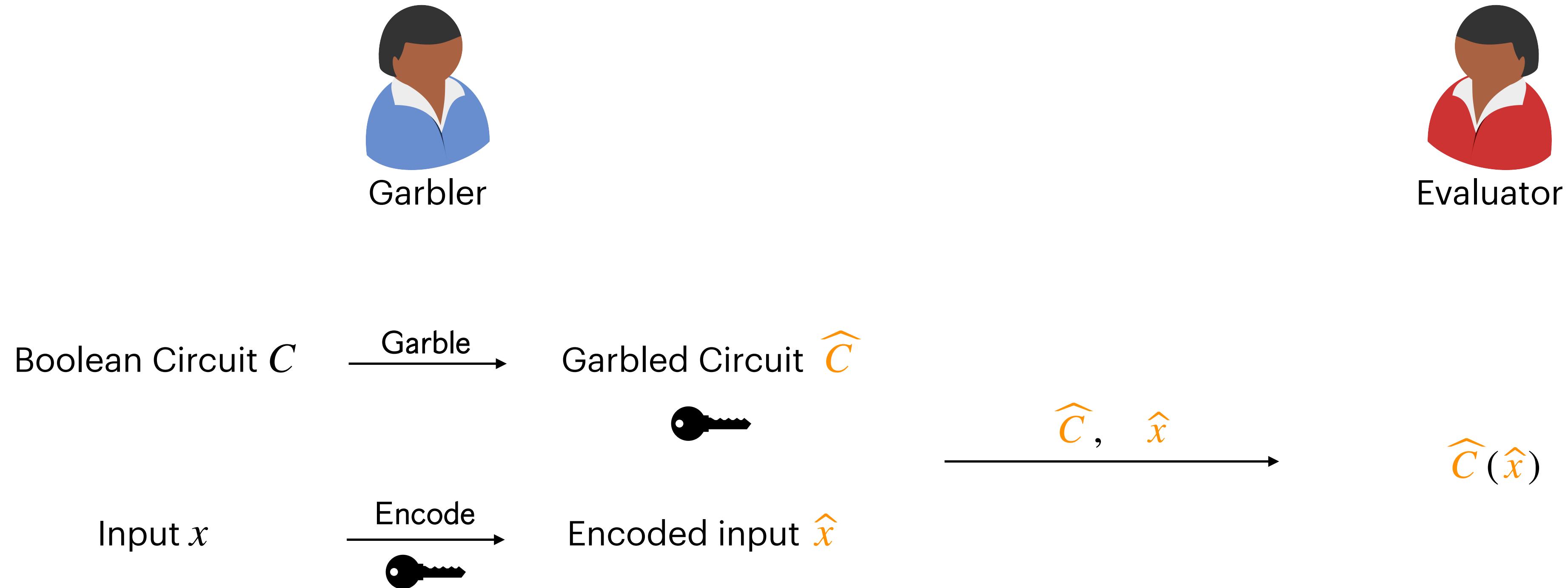


Input  $x$   $\xrightarrow{\text{Encode}}$  Encoded input  $\widehat{x}$



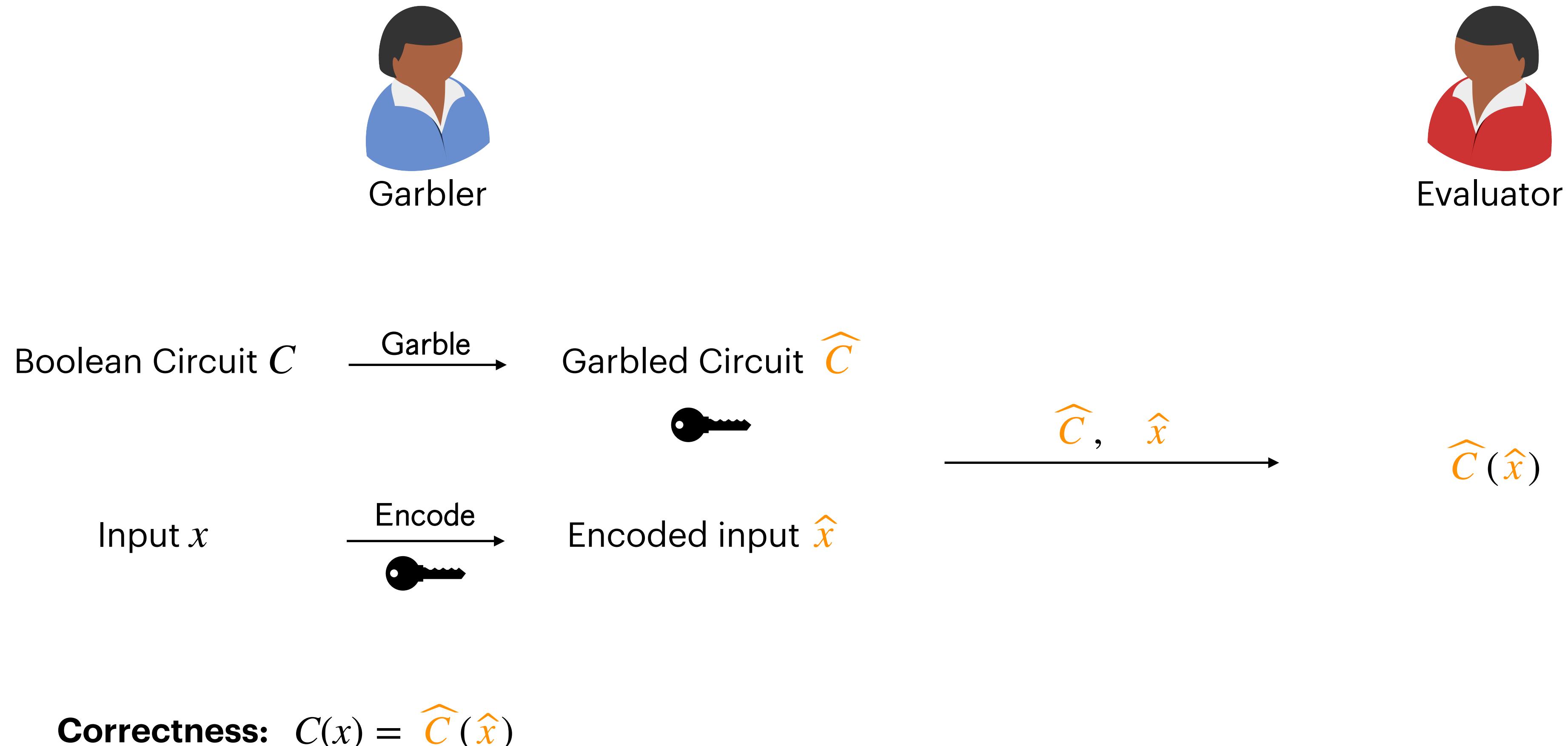
# Garbled Circuits

[Yao'86]



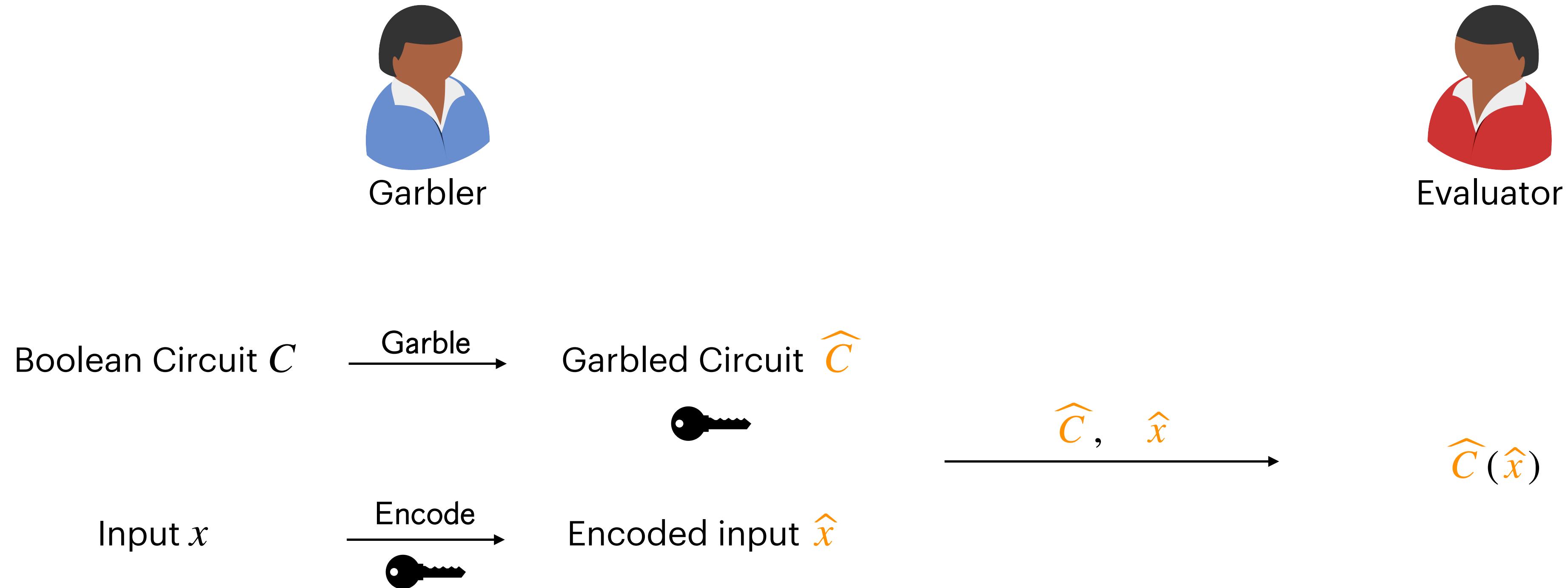
# Garbled Circuits

[Yao'86]



# Garbled Circuits

[Yao'86]

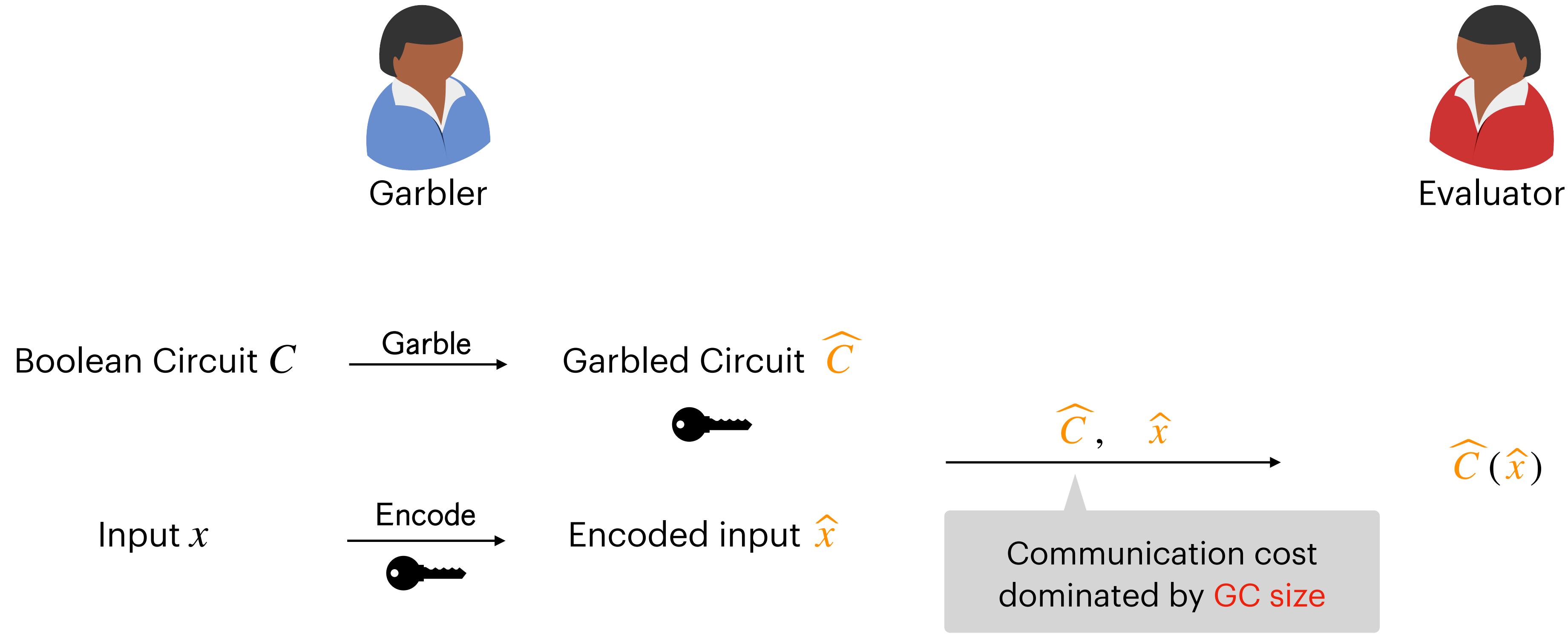


**Correctness:**  $C(x) = \widehat{C}(\widehat{x})$

**Privacy:**  $(\widehat{C}, \widehat{x}) \leftarrow \text{Simulator}(C, C(x))$

# Garbled Circuits

[Yao'86]



**Correctness:**  $C(x) = \widehat{C}(\widehat{x})$

**Privacy:**  $(\widehat{C}, \widehat{x}) \leftarrow \text{Simulator}(C, C(x))$

# Garbled Circuits

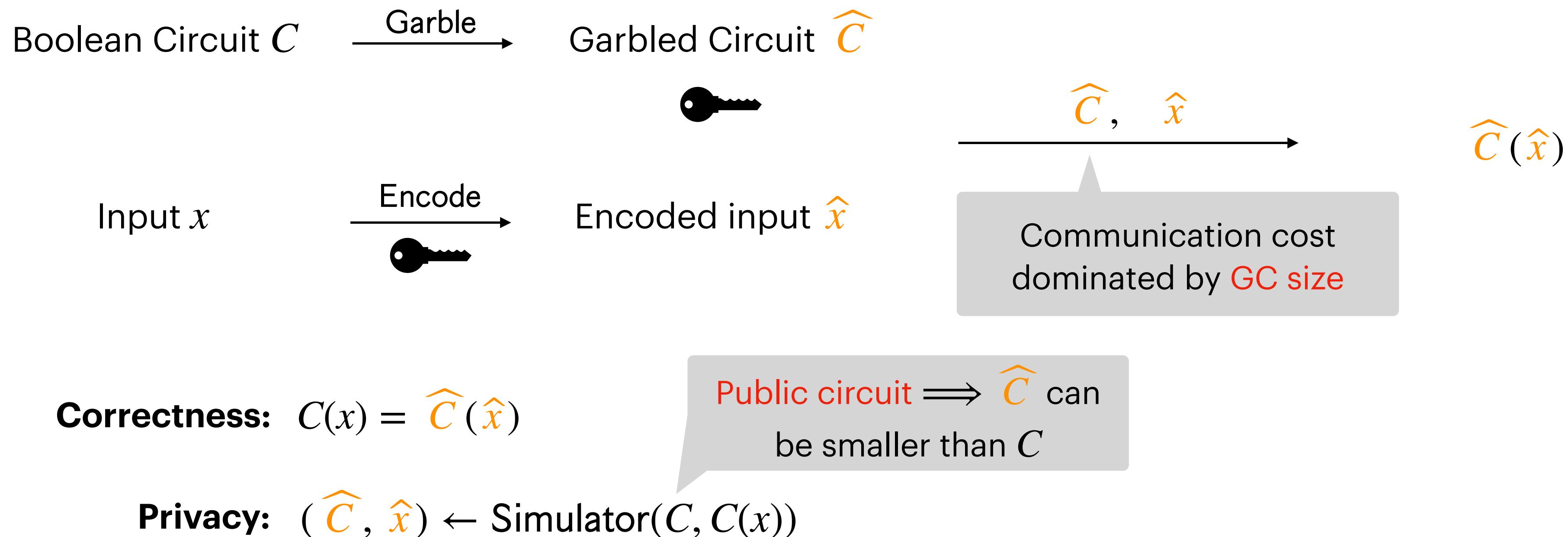
[Yao'86]



Garbler

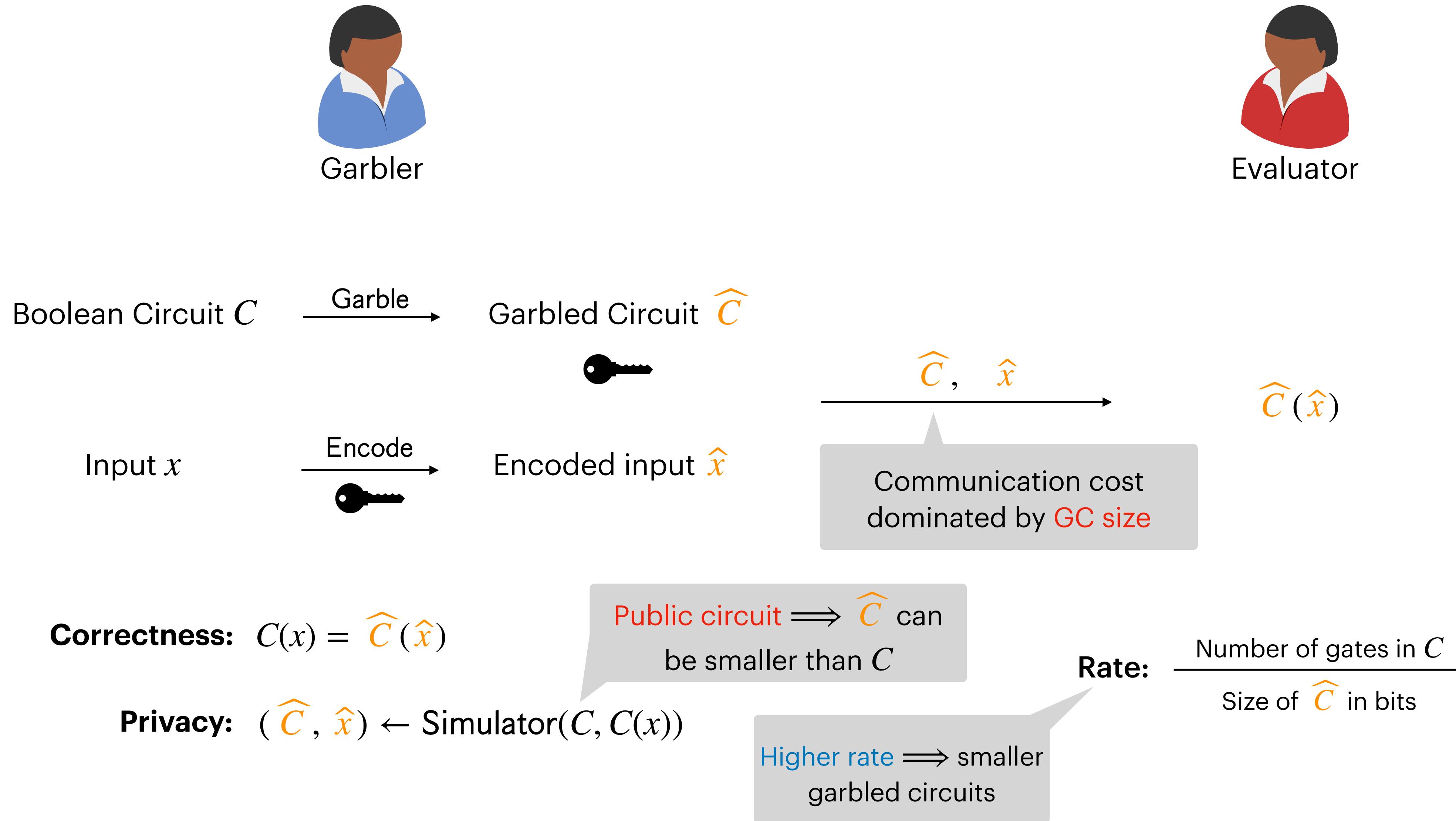


Evaluator



# Garbled Circuits

[Yao'86]



# Landscape of Garbling Schemes

# Landscape of Garbling Schemes

Rate- $\Omega(1/\lambda)$

Symmetric-key crypto

Black-box use of crypto

[Yao'86] [Lindell-Pinkas'07] [Kolesnikov-Schneider'08] [Zahur-Rosulek-Evans'15] [Rosulek-Roy'21]

# Landscape of Garbling Schemes

**Rate- $\Omega(1/\lambda)$**

Symmetric-key crypto

Black-box use of crypto

[Yao'86] [Lindell-Pinkas'07] [Kolesnikov-Schneider'08] [Zahur-Rosulek-Evans'15] [Rosulek-Roy'21]

**Rate- $\omega(1)$**

ABE + FHE / iO + OWF

Non-black-box use of crypto

[Boneh-Gentry-Grobunov-Halevi-Nikolaenko-Segev-Vaikuntanathan-Vinayagamurthy'14] [Lin-Pass'14]  
[Goldwasser-Kalai-Popa-Vaikuntanathan-Zeldovich'13] [Koppula-Lewko-Waters'15] [Hsieh-Lin-Luo'23]

# Landscape of Garbling Schemes

**Rate- $\Omega(1/\lambda)$**

Symmetric-key crypto

Black-box use of crypto

[Yao'86] [Lindell-Pinkas'07] [Kolesnikov-Schneider'08] [Zahur-Rosulek-Evans'15] [Rosulek-Roy'21]

**Rate-1**

Ring LWE / NTRU

Non-black-box use of crypto

[Liu-Wang-Yang-Yu'24]

**Rate- $\omega(1)$**

ABE + FHE / iO + OWF

Non-black-box use of crypto

[Boneh-Gentry-Grobunov-Halevi-Nikolaenko-Segev-Vaikuntanathan-Vinayagamurthy'14] [Lin-Pass'14]  
[Goldwasser-Kalai-Popa-Vaikuntanathan-Zeldovich'13] [Koppula-Lewko-Waters'15] [Hsieh-Lin-Luo'23]

# Landscape of Garbling Schemes

**Rate- $\Omega(1/\lambda)$**

Symmetric-key crypto

Black-box use of crypto

[Yao'86] [Lindell-Pinkas'07] [Kolesnikov-Schneider'08] [Zahur-Rosulek-Evans'15] [Rosulek-Roy'21]

Can we get  $\omega(1/\lambda)$ -rate garbling while making black-box use of crypto?

**Rate-1**

Ring LWE / NTRU

Non-black-box use of crypto

[Liu-Wang-Yang-Yu'24]

**Rate- $\omega(1)$**

ABE + FHE / iO + OWF

Non-black-box use of crypto

[Boneh-Gentry-Grobunov-Halevi-Nikolaenko-Segev-Vaikuntanathan-Vinayagamurthy'14] [Lin-Pass'14]  
[Goldwasser-Kalai-Popa-Vaikuntanathan-Zeldovich'13] [Koppula-Lewko-Waters'15] [Hsieh-Lin-Luo'23]

# Our Results

In the **Generic Group Model**, there exists a garbling scheme that garbles a boolean circuit  $C$  into  $\widehat{C}$  such that

$$|\widehat{C}| = \frac{\lambda}{\sqrt{\log \lambda}} \cdot O(C) + \text{poly}(\lambda)$$

# Our Results

In the **Generic Group Model**, there exists a garbling scheme that garbles a boolean circuit  $C$  into  $\widehat{C}$  such that

$$|\widehat{C}| = \frac{\lambda}{\sqrt{\log \lambda}} \cdot O(C) + \text{poly}(\lambda)$$

Assuming **Power-DDH** and a **Tweakable Correlation Robust Hash** function, there exists a garbling scheme that garbles a **layered** boolean circuit  $C$  into  $\widehat{C}$  such that

$$|\widehat{C}| = \frac{\lambda}{\sqrt{\log \lambda}} \cdot O(C) + \text{poly}(\lambda) \cdot \text{depth}(C)$$

# Our Results

In the **Generic Group Model**, there exists a garbling scheme that garbles a boolean circuit  $C$  into  $\widehat{C}$  such that

$$|\widehat{C}| = \frac{\lambda}{\sqrt{\log \lambda}} \cdot O(C) + \text{poly}(\lambda)$$

Assuming **Power-DDH** and a **Tweakable Correlation Robust Hash** function, there exists a garbling scheme that garbles a **layered** boolean circuit  $C$  into  $\widehat{C}$  such that

$$|\widehat{C}| = \frac{\lambda}{\sqrt{\log \lambda}} \cdot O(C) + \text{poly}(\lambda) \cdot \text{depth}(C)$$

$\omega(1/\lambda)$ -rate and black-box use of crypto

# Our Results

In the **Generic Group Model**, there exists a garbling scheme that garbles a boolean circuit  $C$  into  $\widehat{C}$  such that

$$|\widehat{C}| = \frac{\lambda}{\sqrt{\log \lambda}} \cdot O(C) + \text{poly}(\lambda)$$

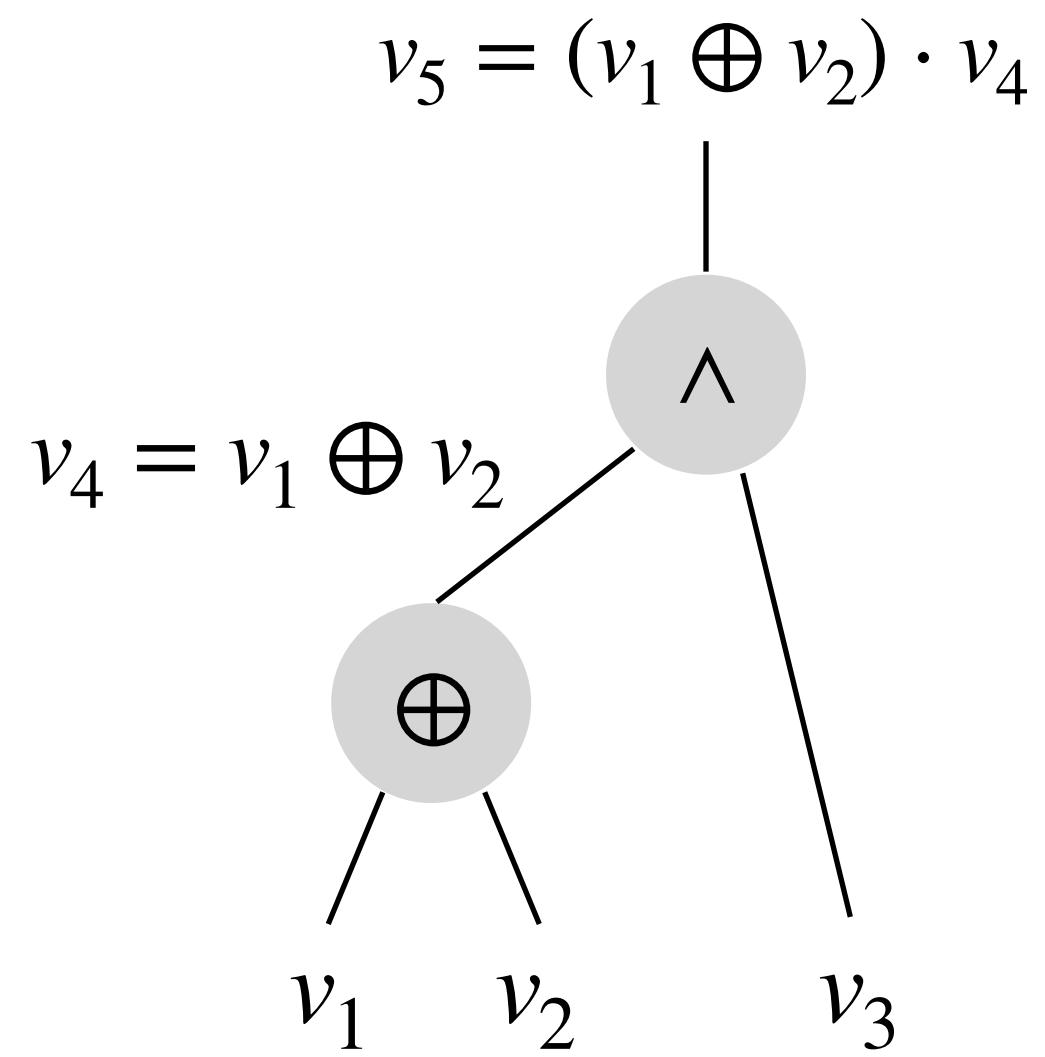
Assuming **Power-DDH** and a **Tweakable Correlation Robust Hash** function, there exists a garbling scheme that garbles a **layered** boolean circuit  $C$  into  $\widehat{C}$  such that

$$|\widehat{C}| = \frac{\lambda}{\sqrt{\log \lambda}} \cdot O(C) + \text{poly}(\lambda) \cdot \text{depth}(C)$$

$\omega(1/\lambda)$ -rate and black-box use of crypto

$o(\lambda)$ -bits per gate scheme from assumptions not known to imply FHE

# Template for Garbling Circuits



Boolean Circuit

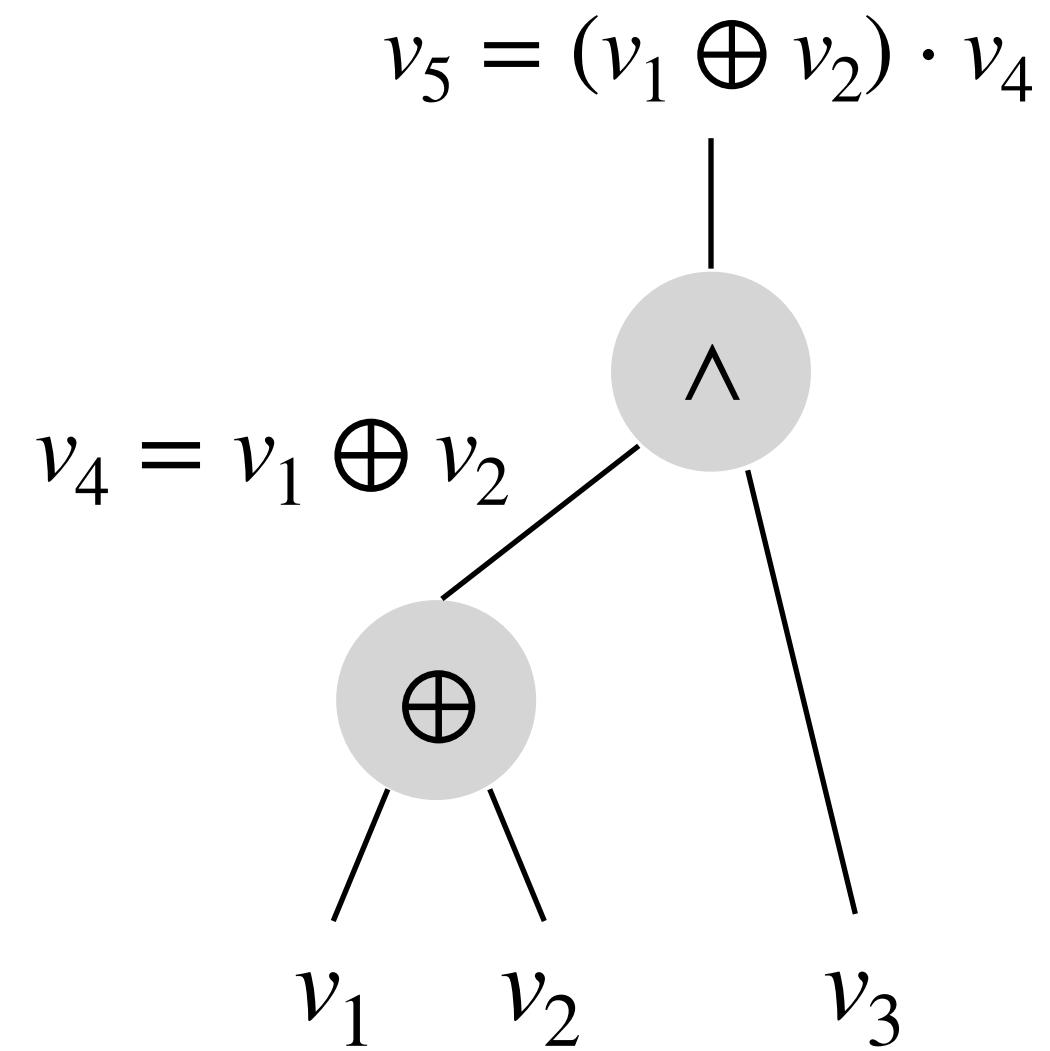
# Template for Garbling Circuits



Garbler



Evaluator



Boolean Circuit

# Template for Garbling Circuits

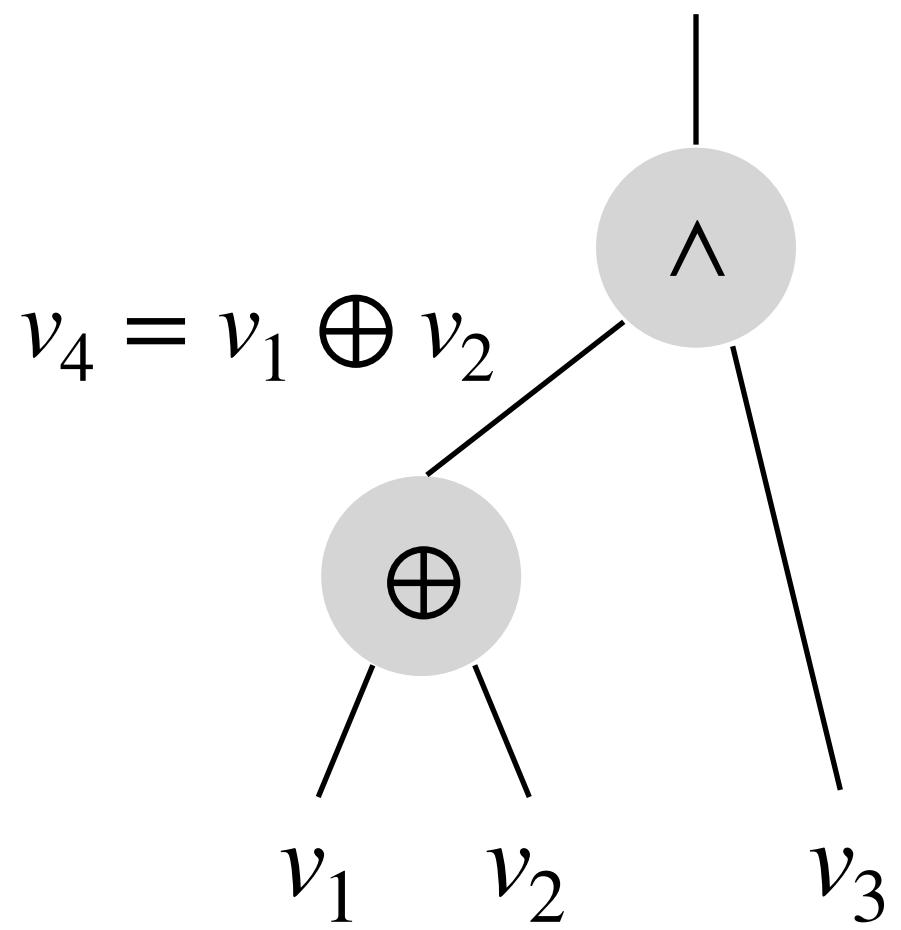


Garbler

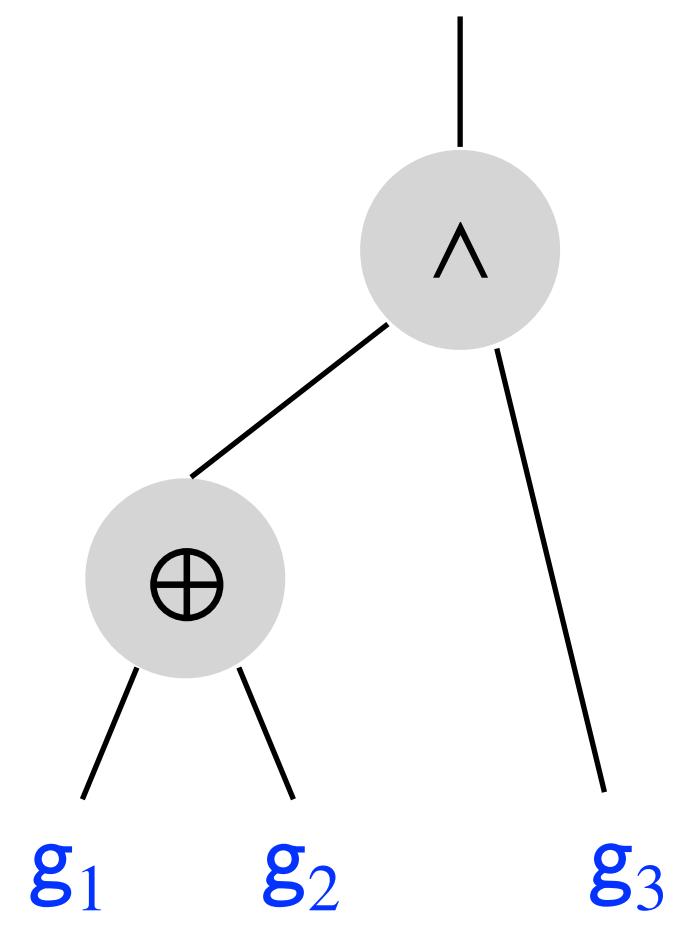


Evaluator

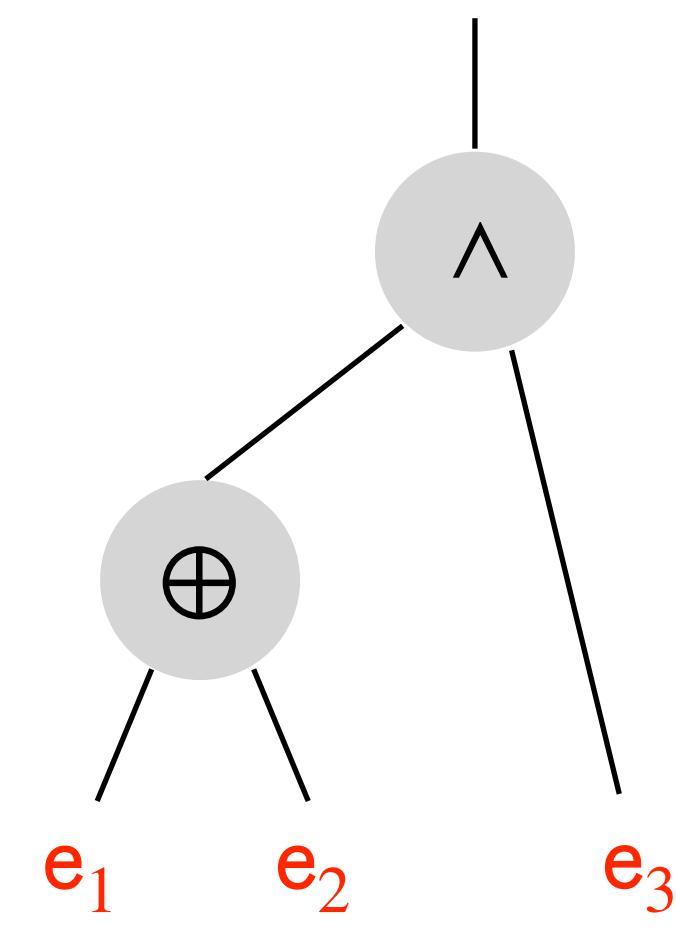
$$v_5 = (v_1 \oplus v_2) \cdot v_4$$



Boolean Circuit



**Invariant**  
 $g_i \oplus e_i = v_i$



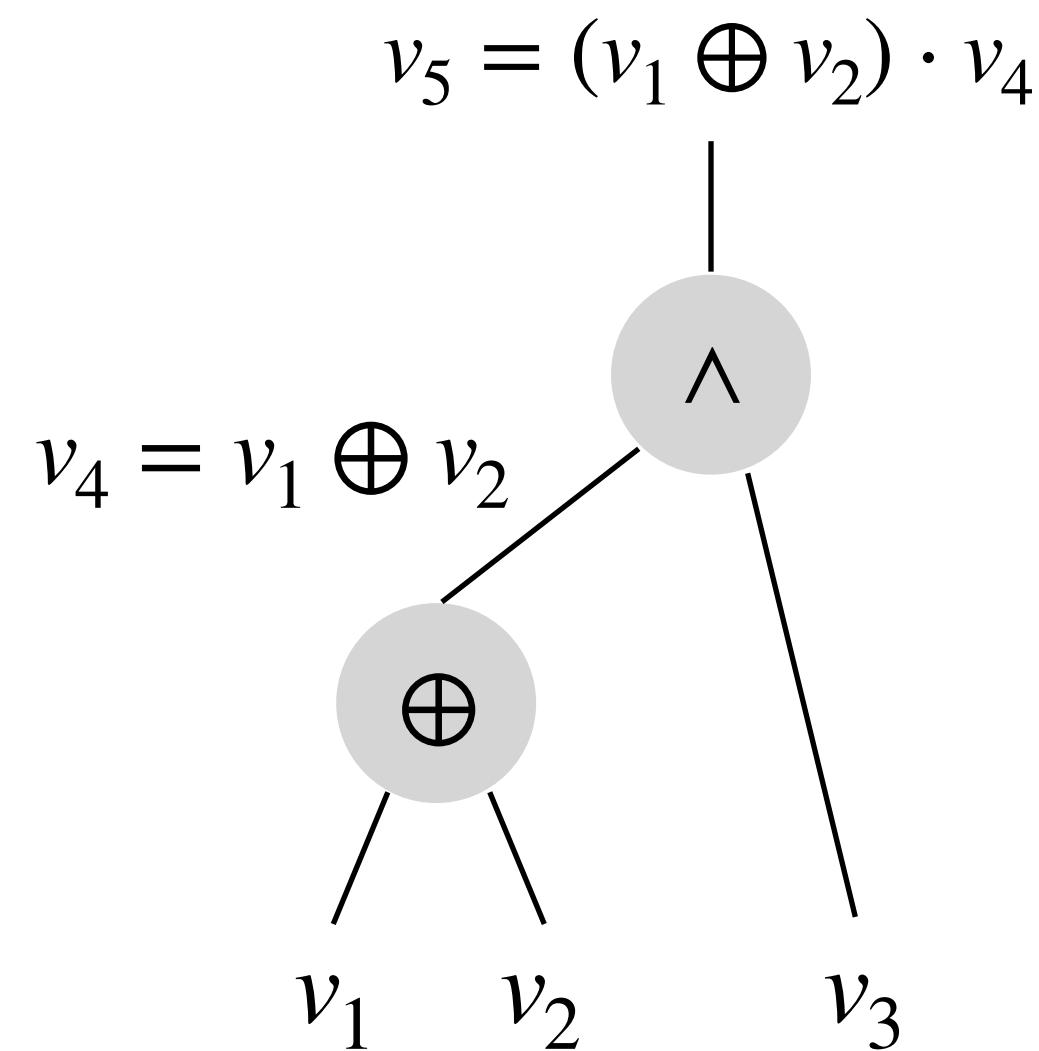
# Template for Garbling Circuits



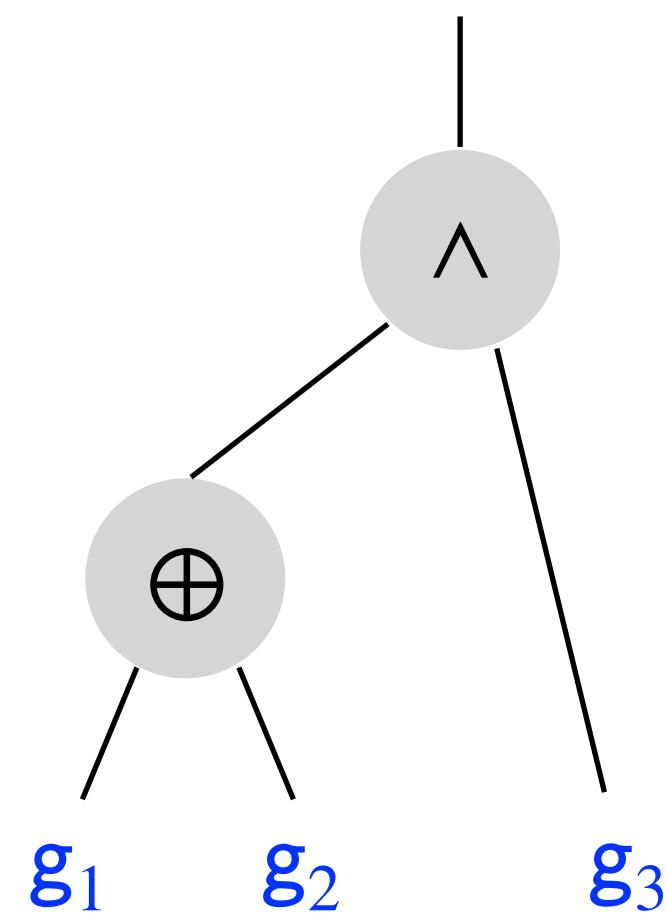
Garbler



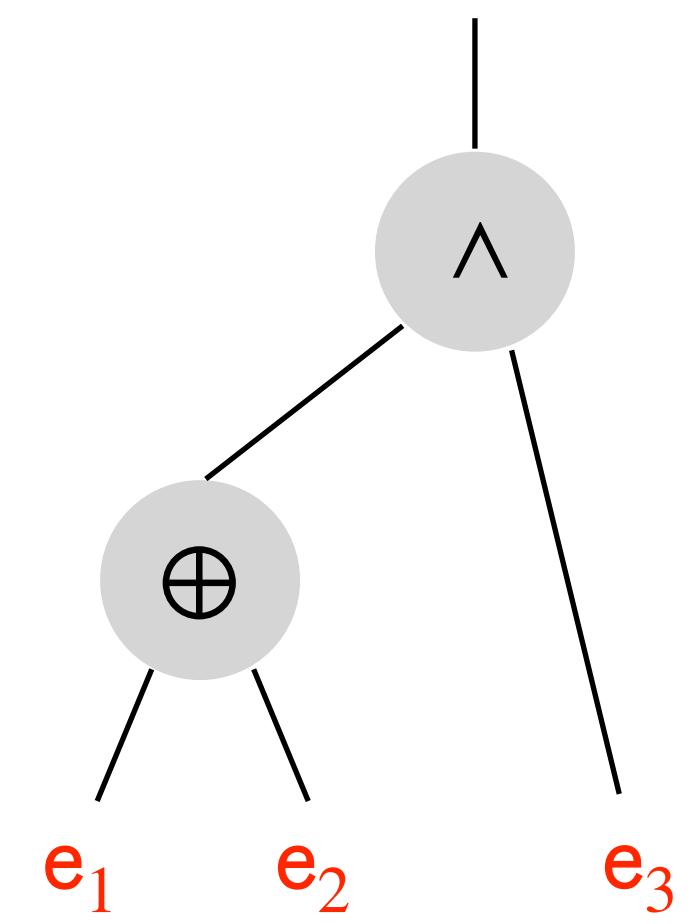
Evaluator



Boolean Circuit



Invariant  
 $g_i \oplus e_i = v_i$



Garbled Circuit  $\widehat{C}$

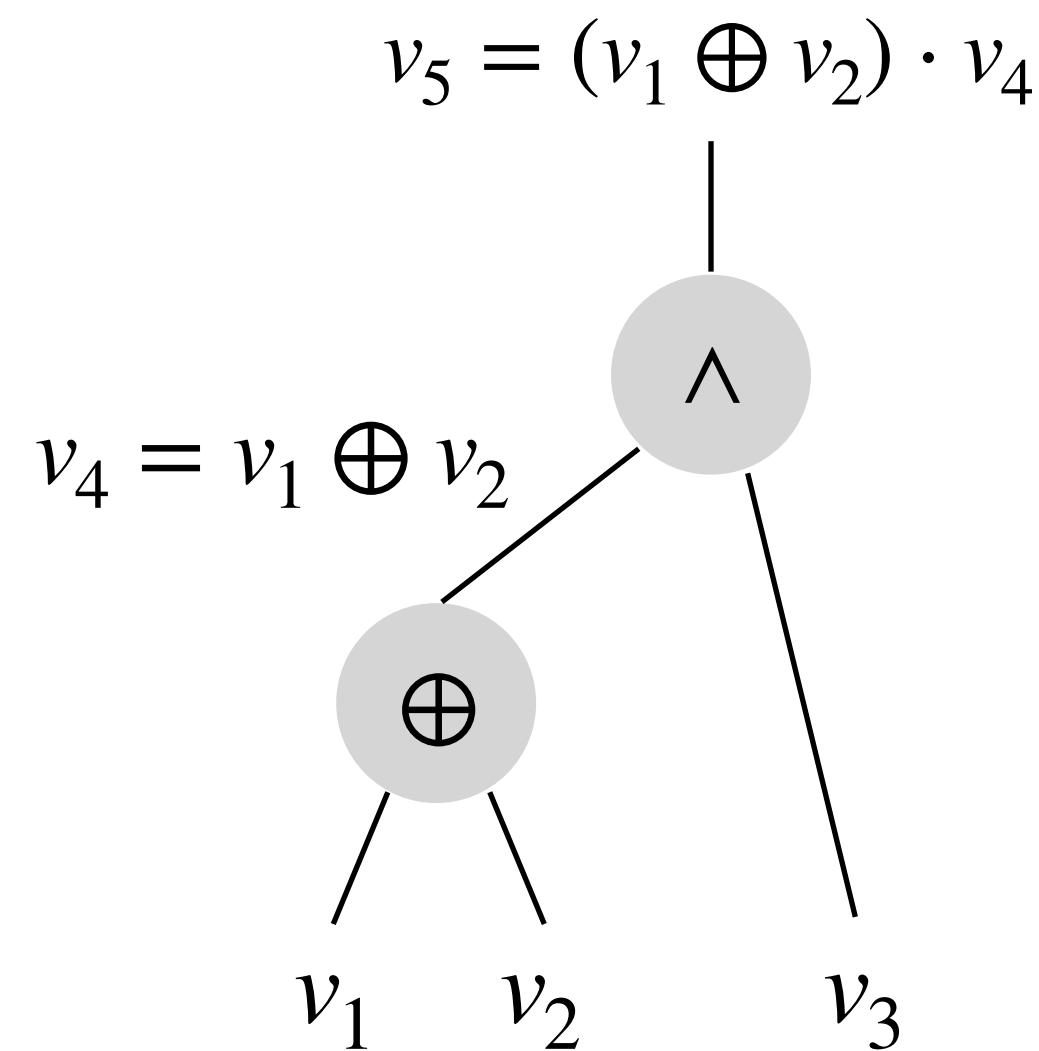
# Template for Garbling Circuits



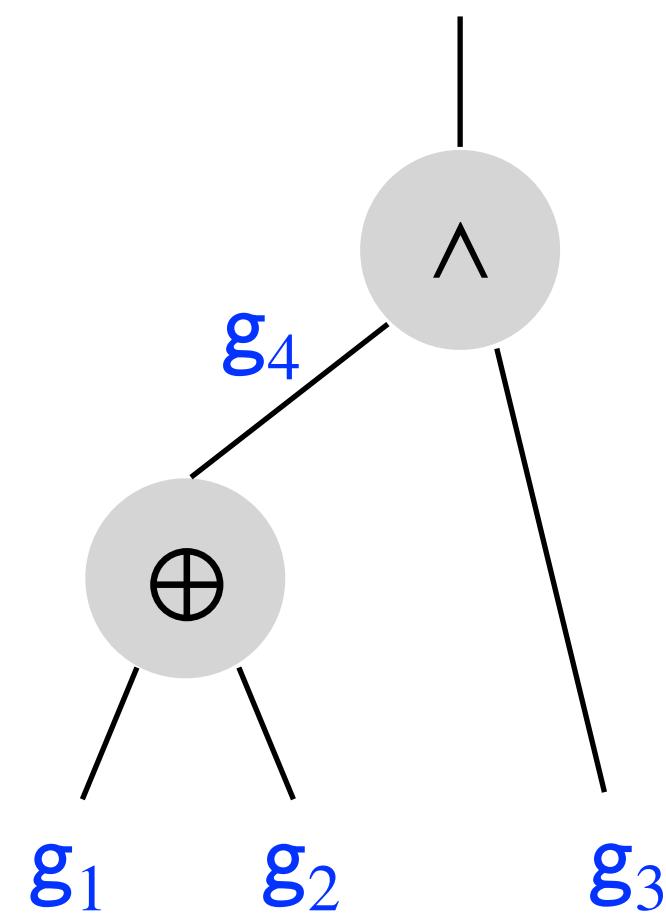
Garbler



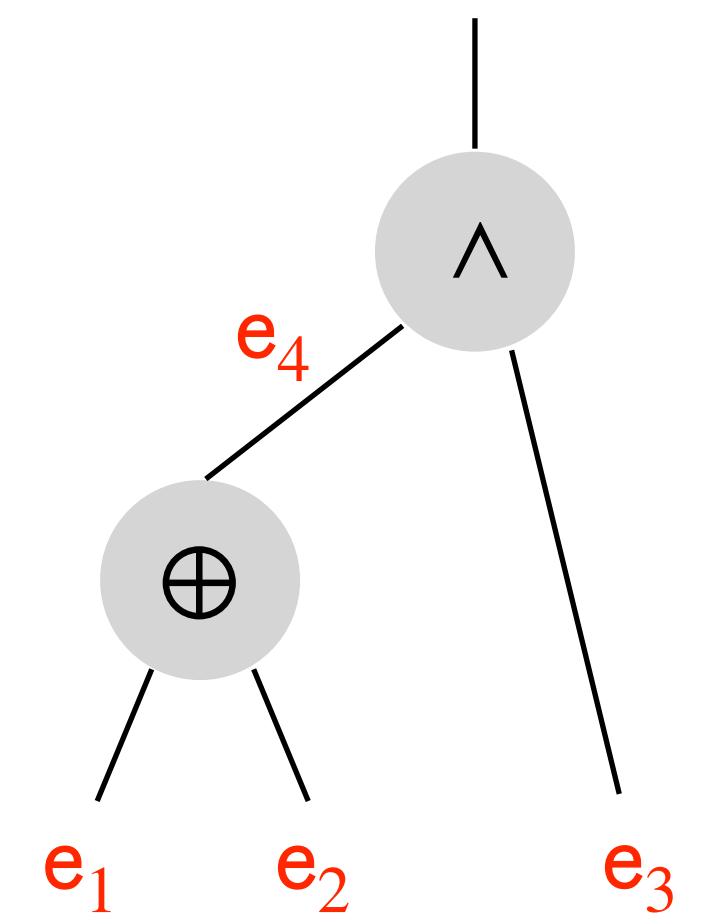
Evaluator



Boolean Circuit



**Invariant**  
 $g_i \oplus e_i = v_i$



Garbled Circuit  $\widehat{C}$

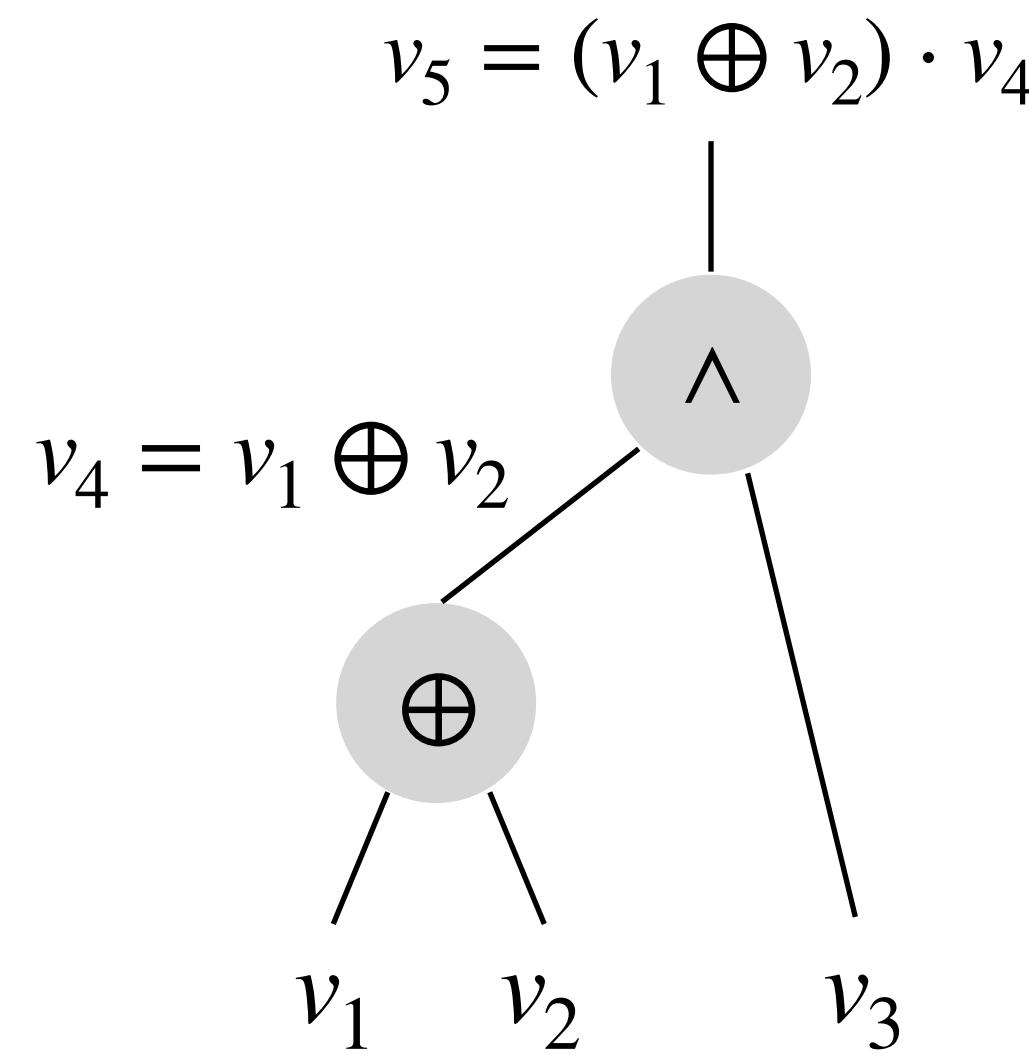
# Template for Garbling Circuits



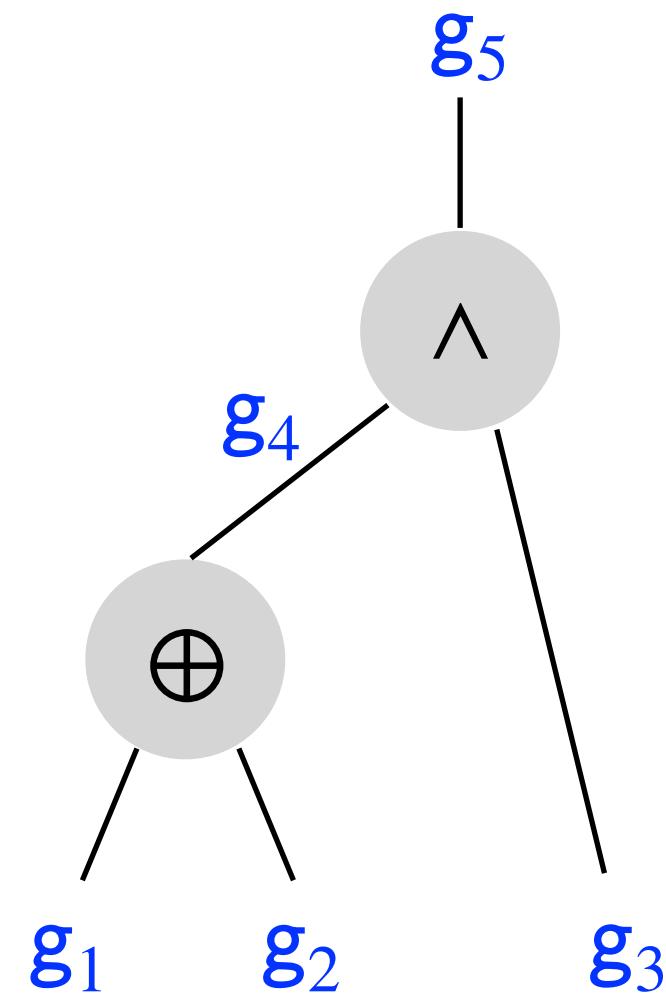
Garbler



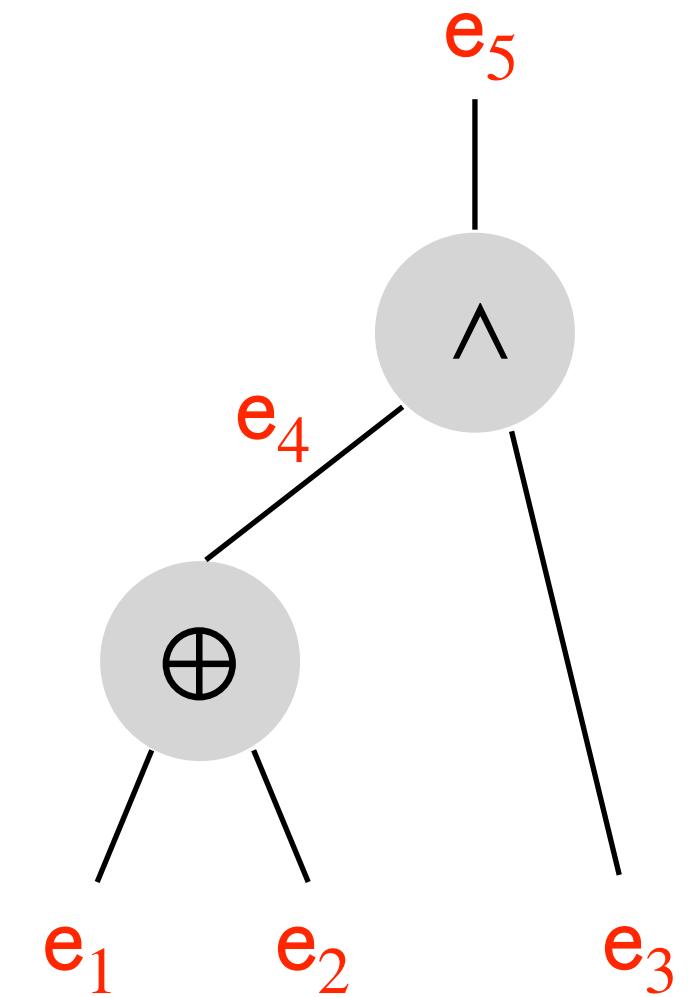
Evaluator



Boolean Circuit

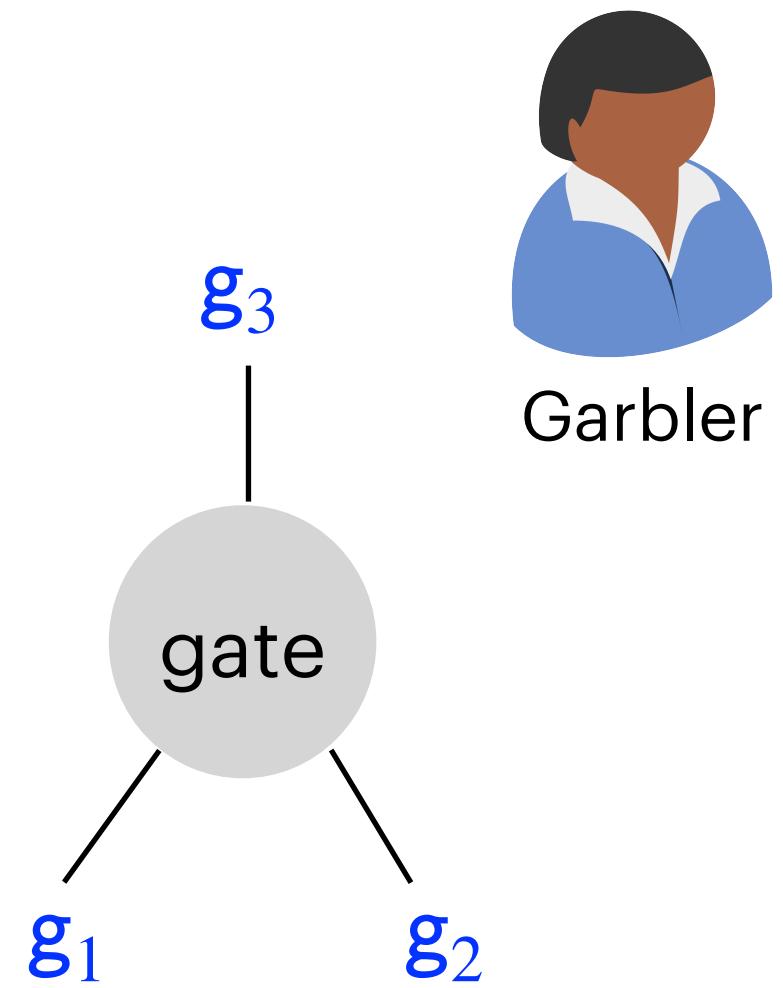


Invariant  
 $g_i \oplus e_i = v_i$



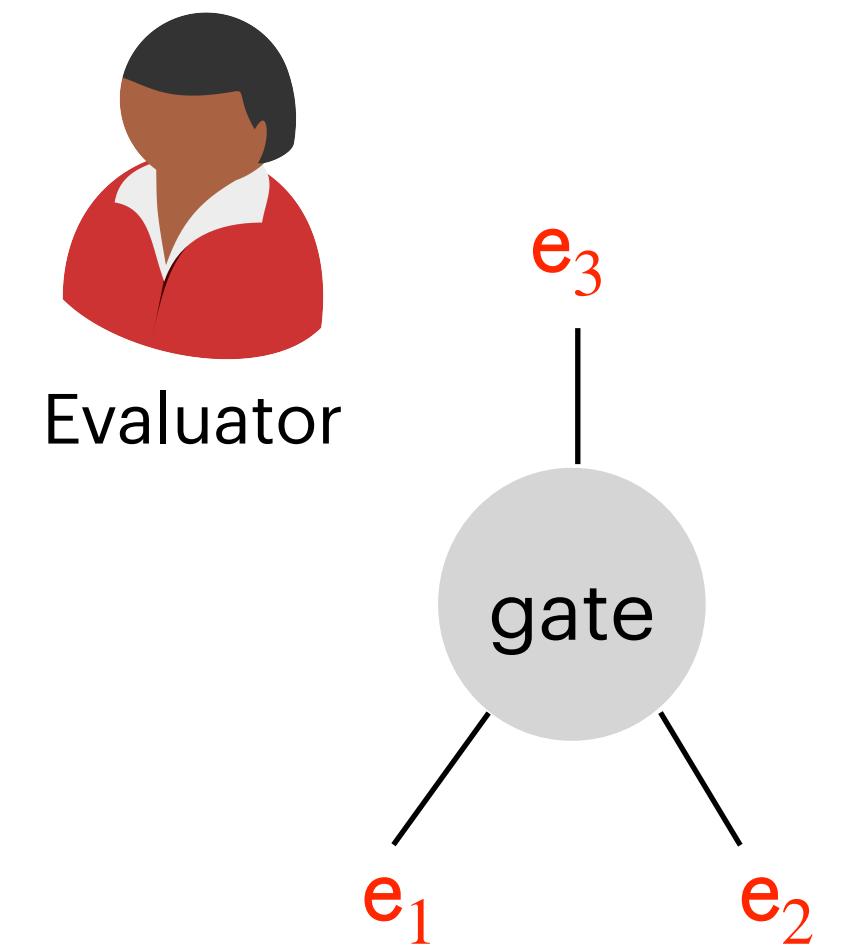
Garbled Circuit  $\widehat{C}$

# Template for Garbling Circuits

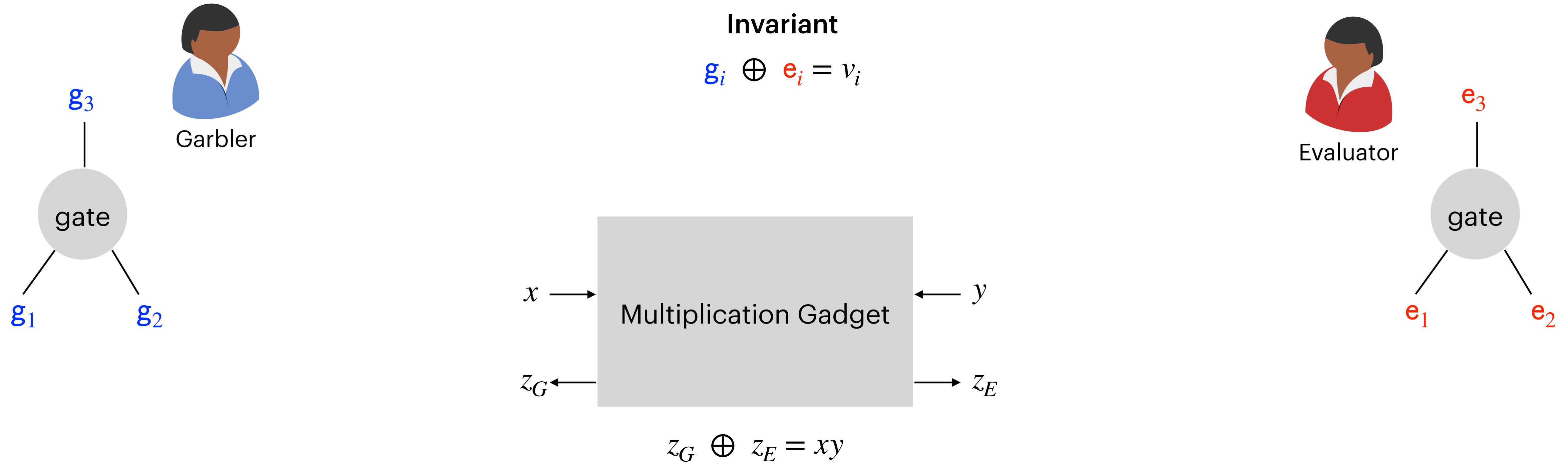


Invariant

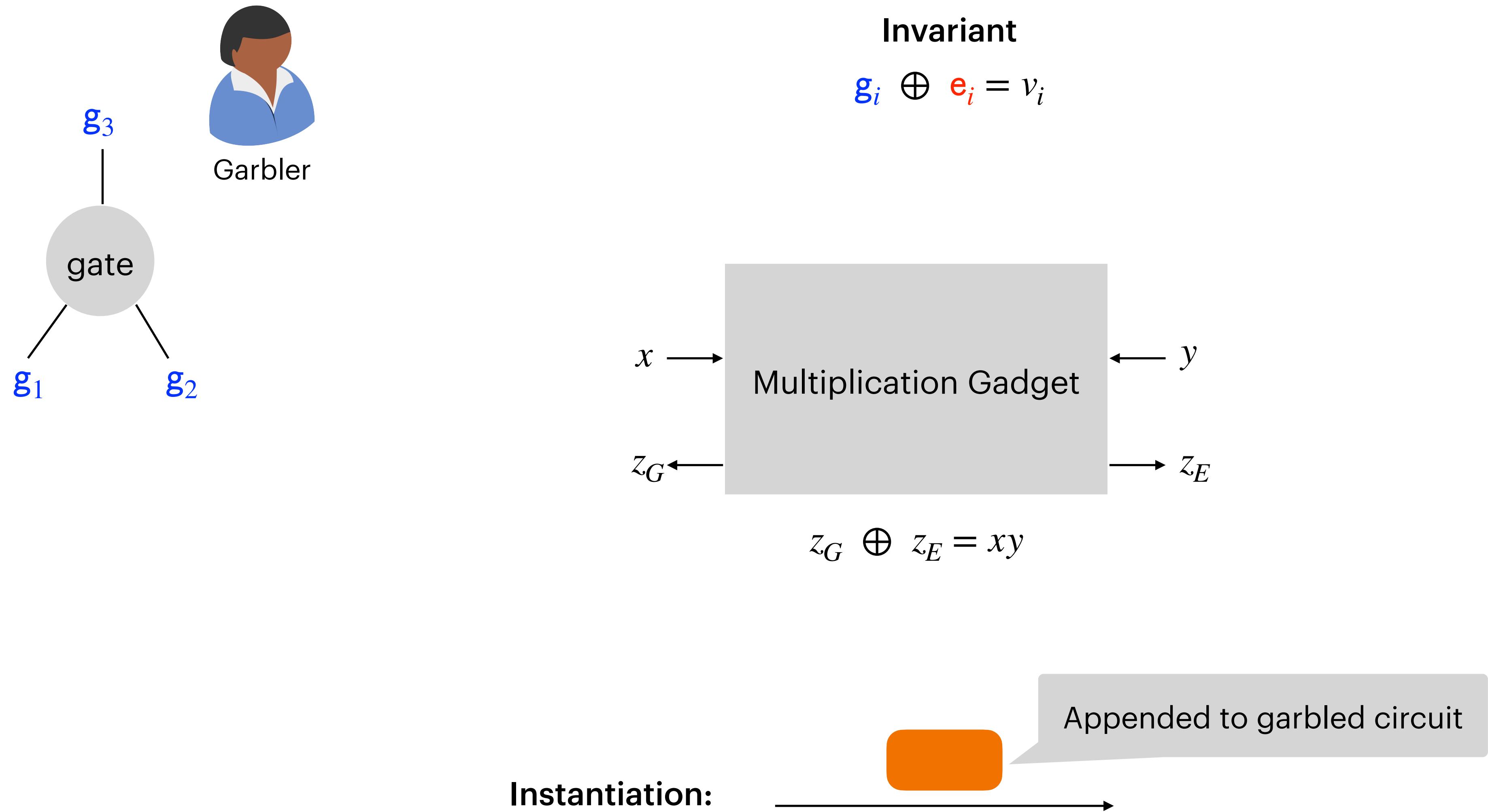
$$g_i \oplus e_i = v_i$$



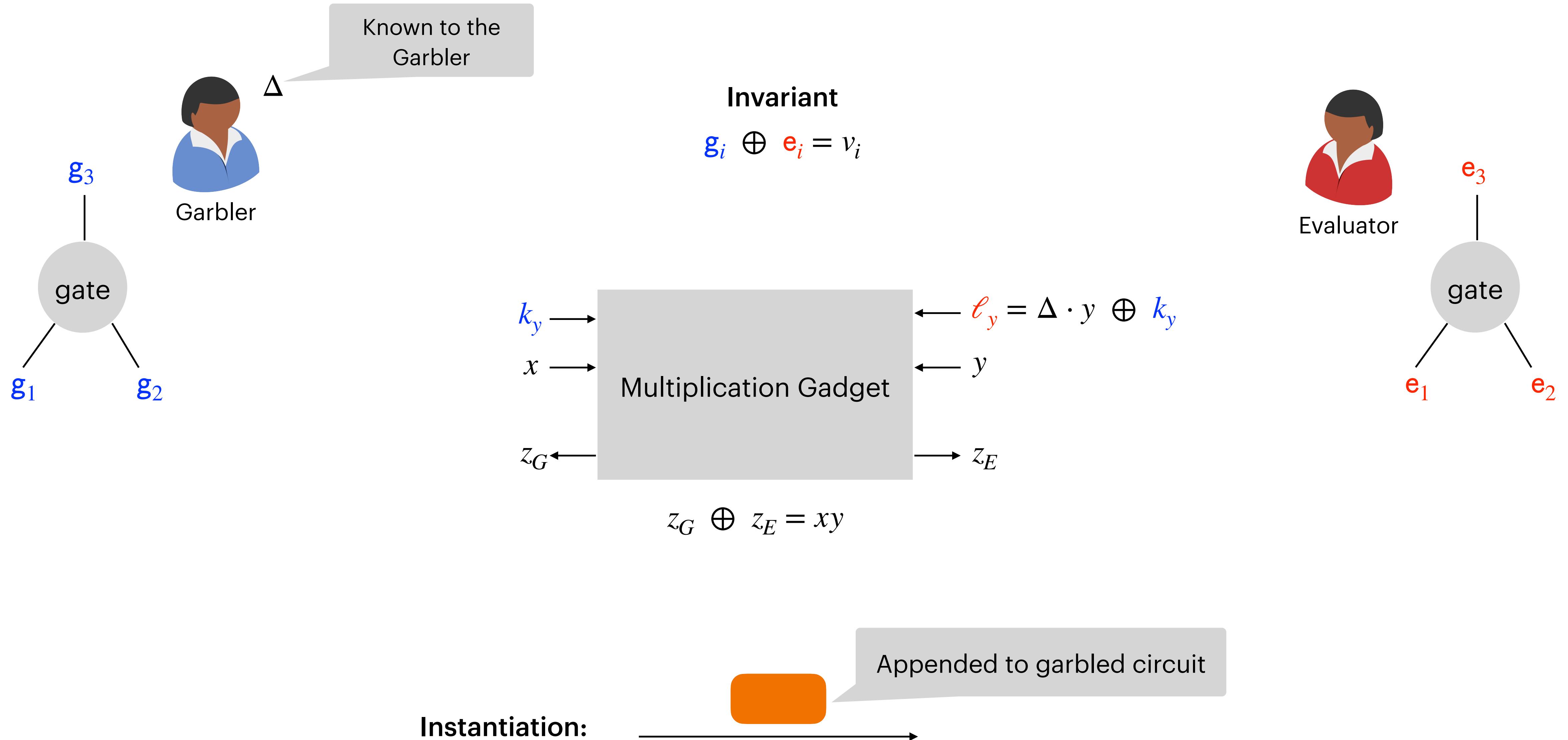
# Template for Garbling Circuits



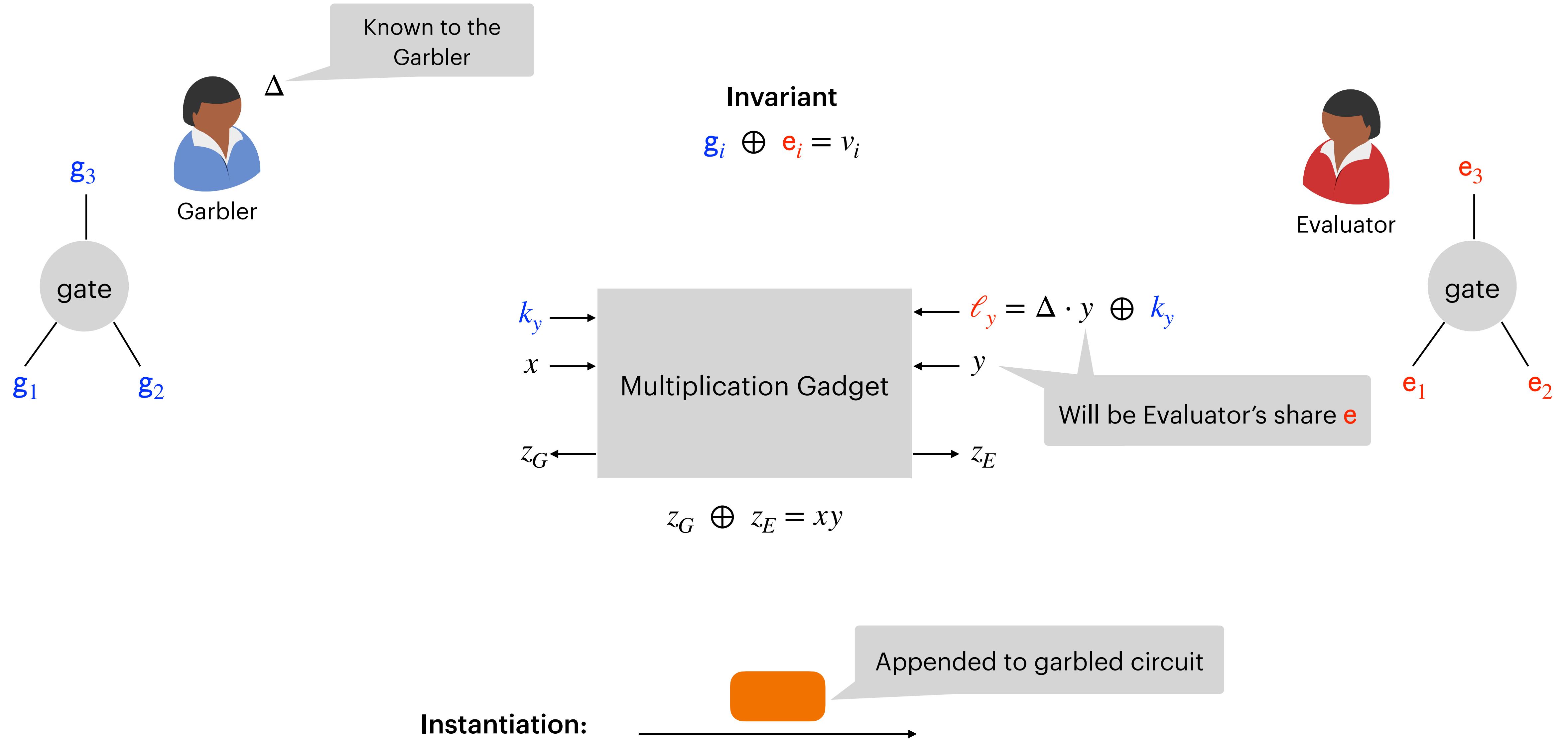
# Template for Garbling Circuits



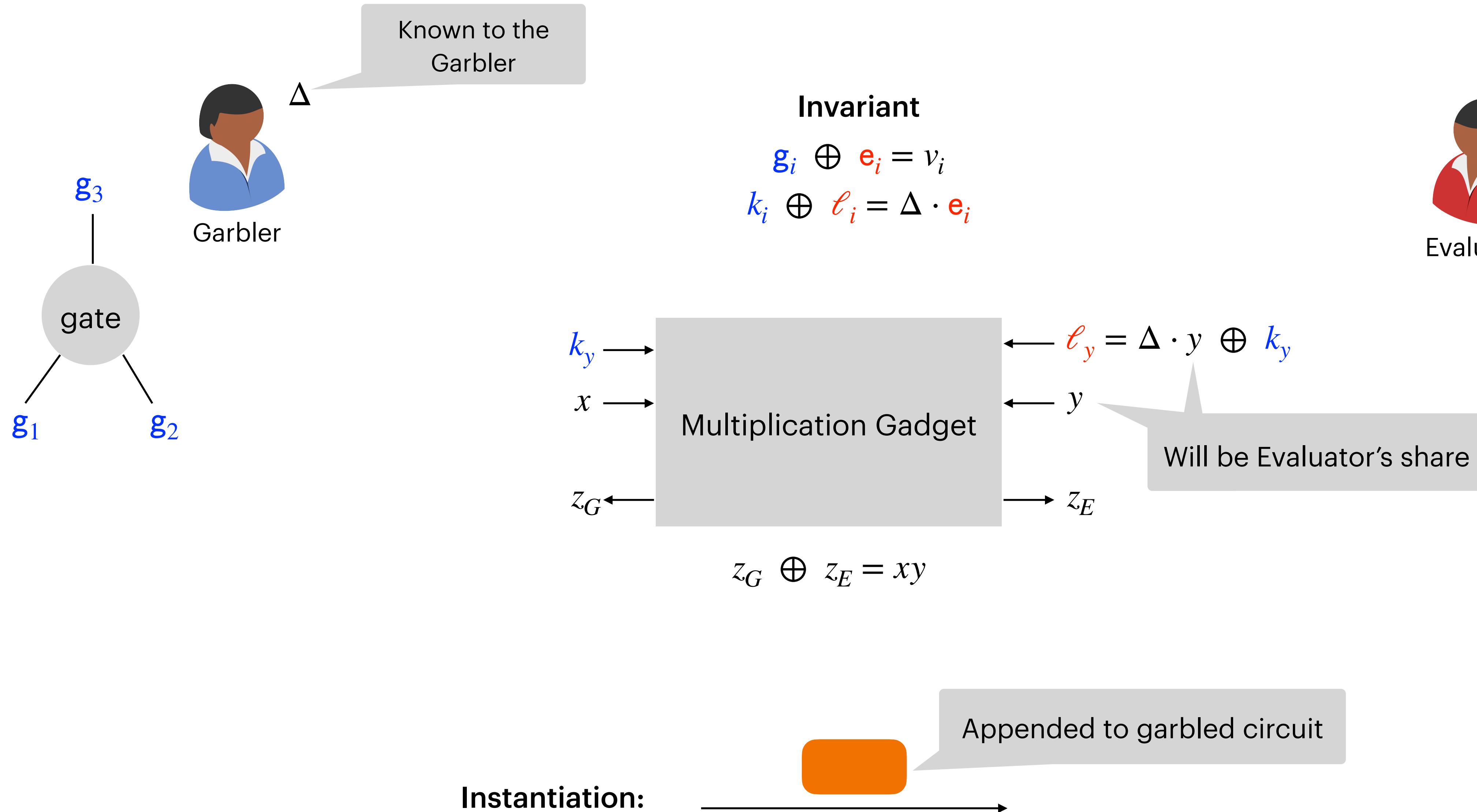
# Template for Garbling Circuits



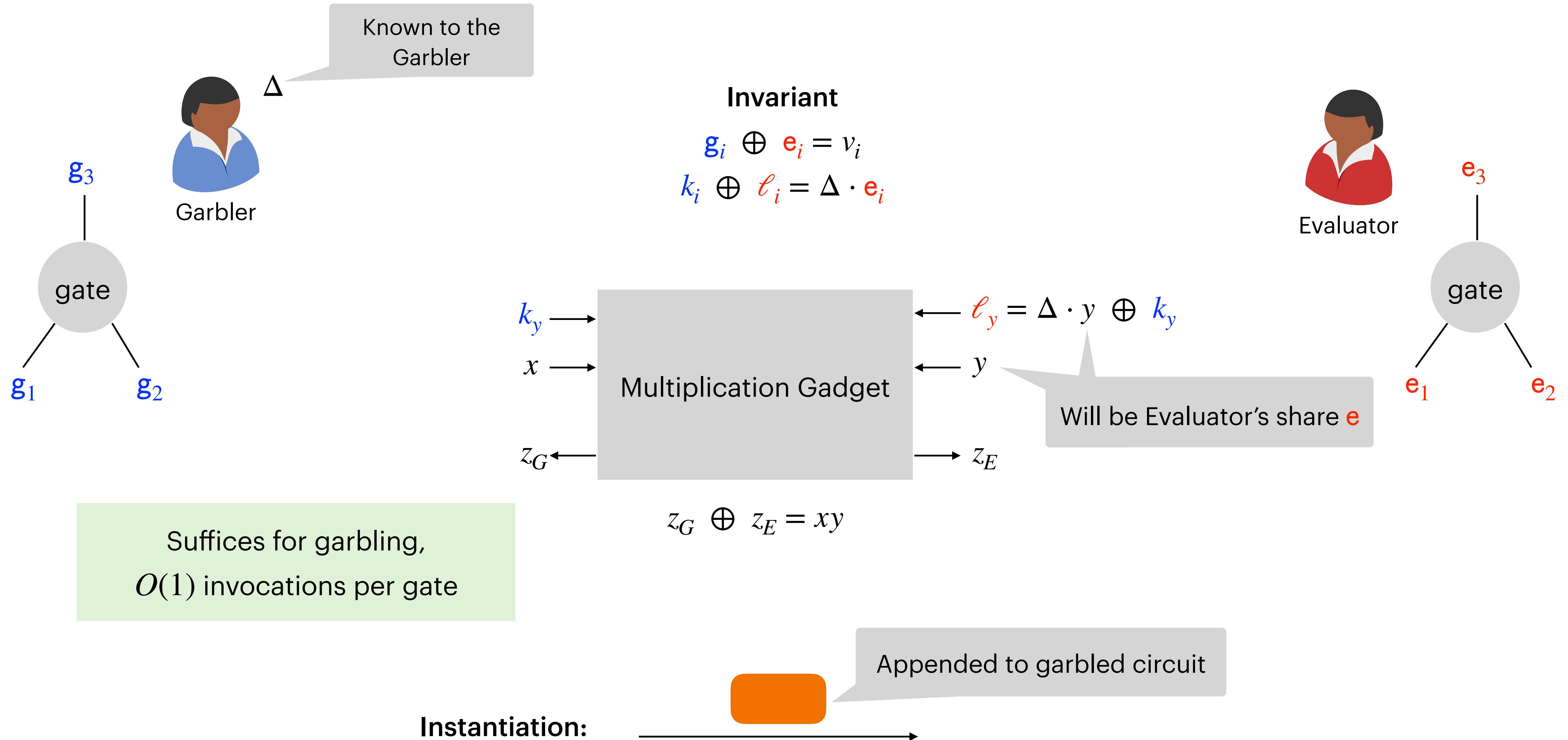
# Template for Garbling Circuits



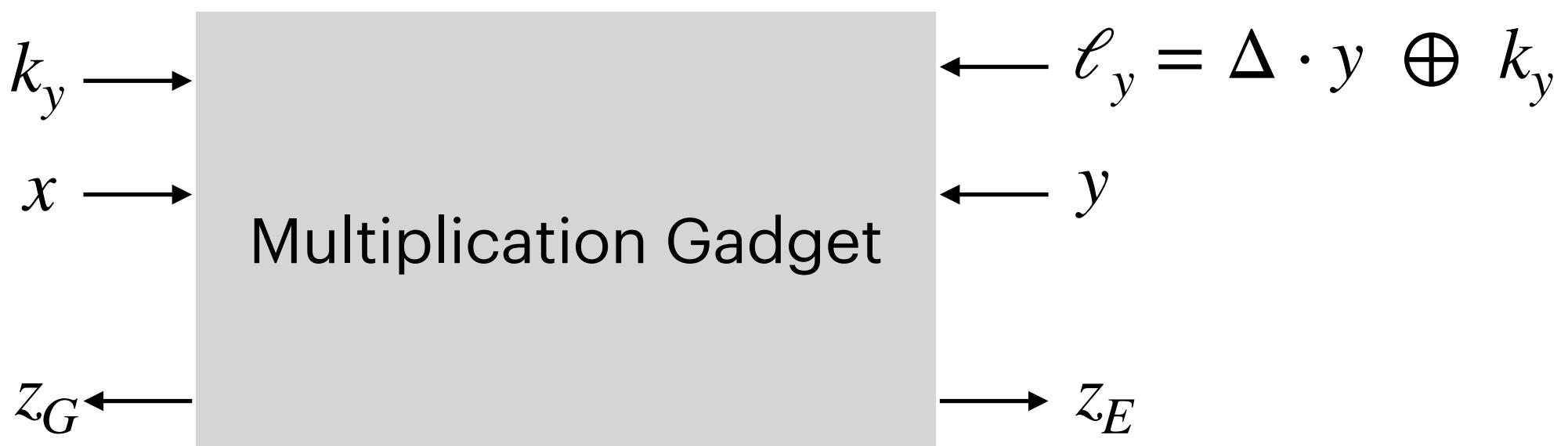
# Template for Garbling Circuits



# Template for Garbling Circuits

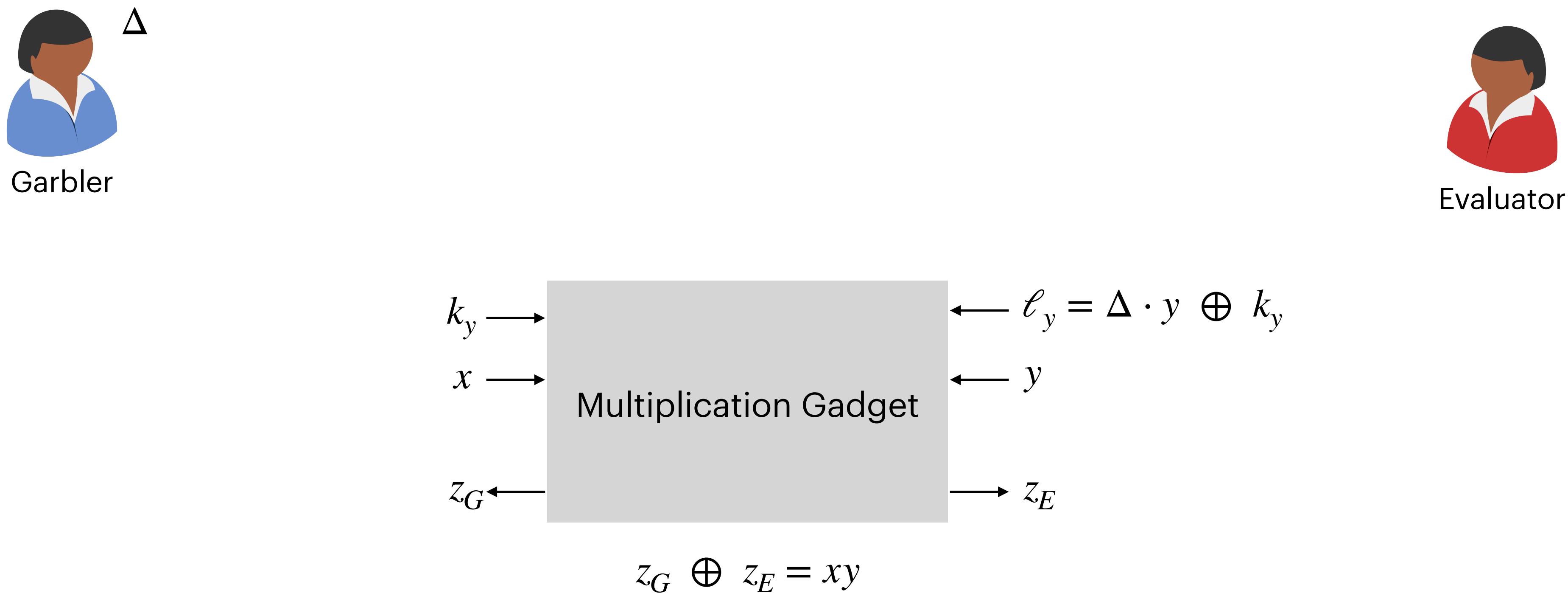


# Towards $\omega(1/\lambda)$ -Rate Garbling



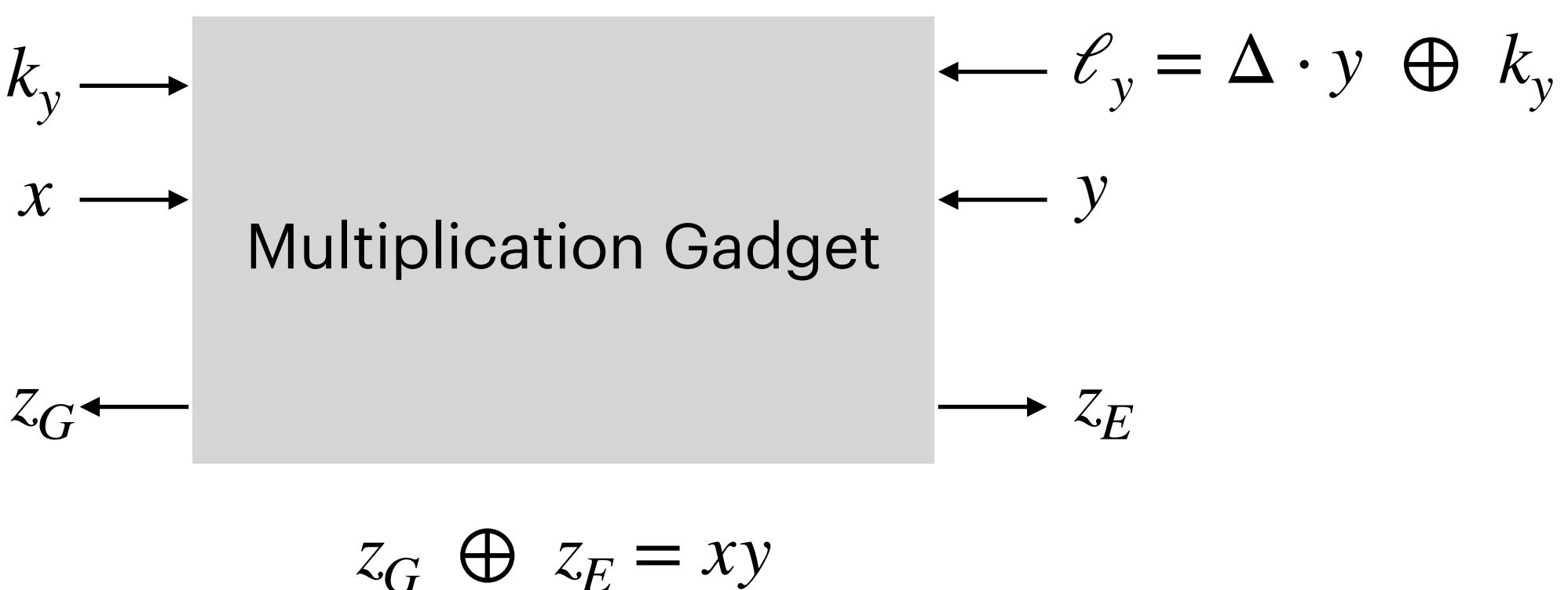
$$z_G \oplus z_E = xy$$

# Towards $\omega(1/\lambda)$ -Rate Garbling



**Yao's Garbling:** Instantiation with  $O(\lambda)$ -bit message

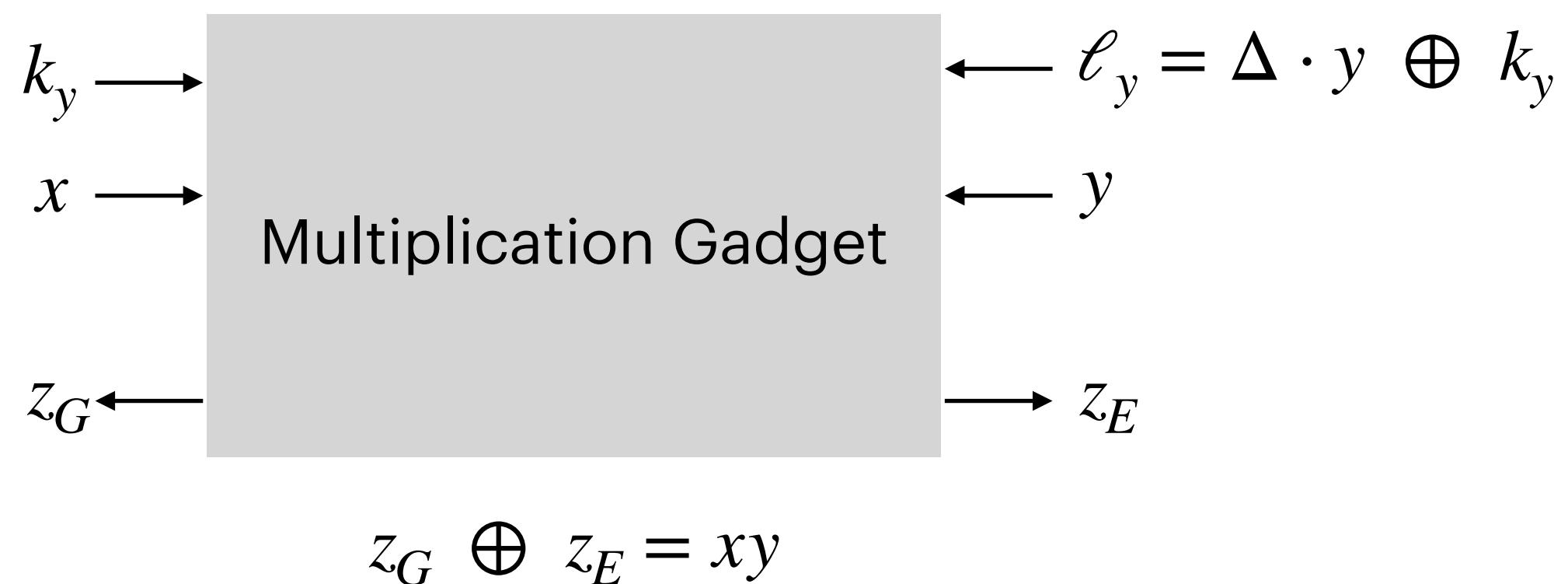
# Towards $\omega(1/\lambda)$ -Rate Garbling



**Yao's Garbling:** Instantiation with  $O(\lambda)$ -bit message

**$\omega(1/\lambda)$ -Rate Garbling:** Requires instantiation with  $o(\lambda)$ -bit message

# Towards $\omega(1/\lambda)$ -Rate Garbling



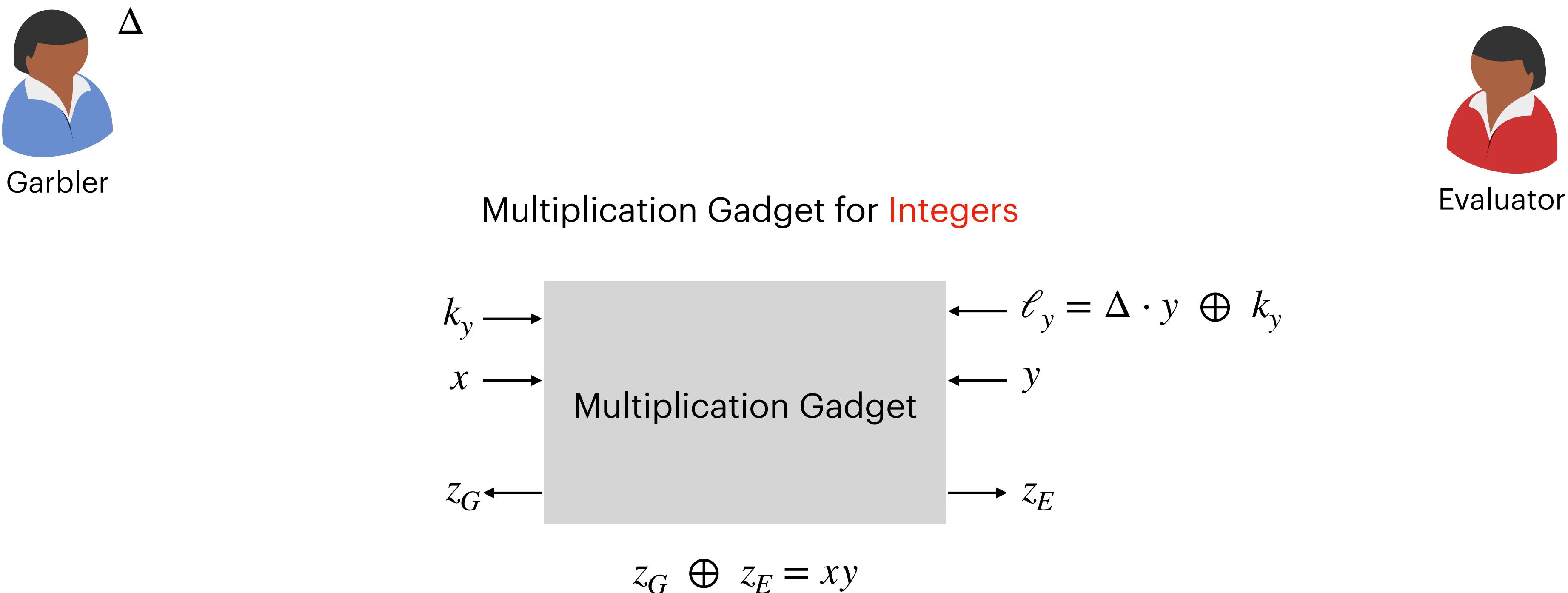
**Yao's Garbling:** Instantiation with  $O(\lambda)$ -bit message

**$\omega(1/\lambda)$ -Rate Garbling:** Requires instantiation with  $o(\lambda)$ -bit message

Leverage recent advances in  
Arithmetic Garbling

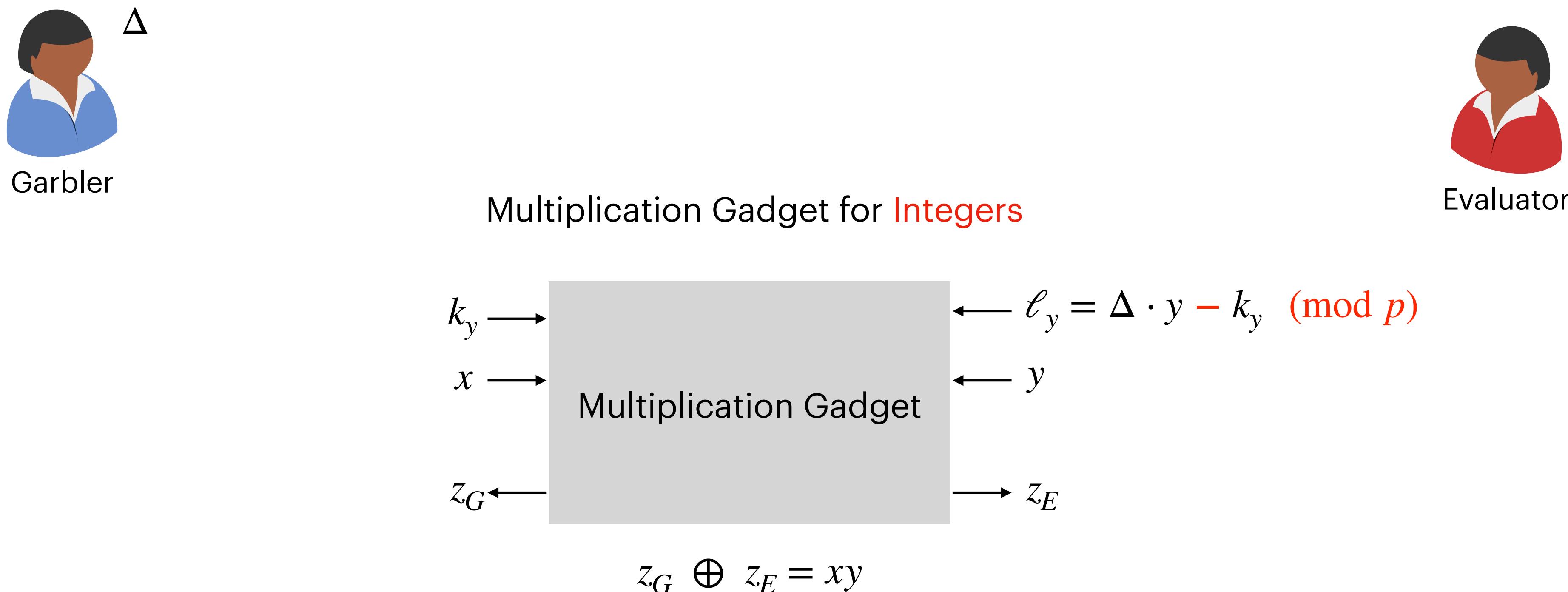
# Towards $\omega(1/\lambda)$ -Rate Garbling

Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]



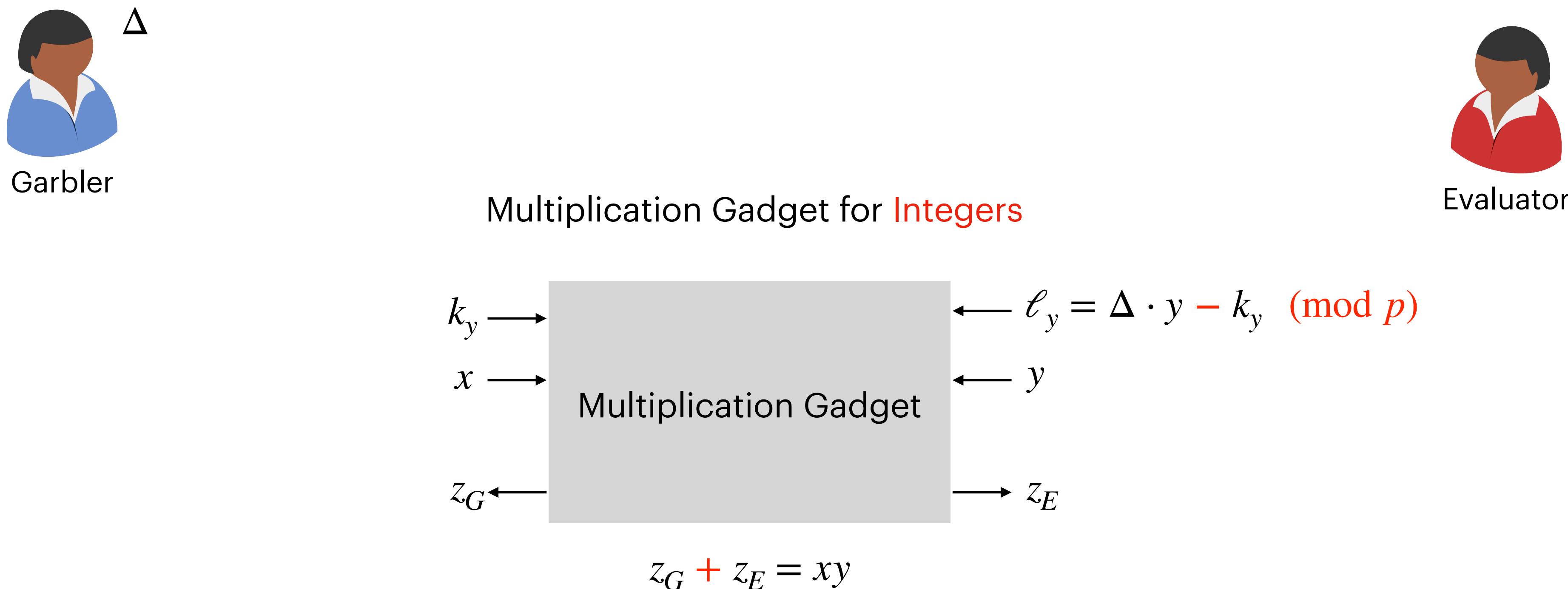
# Towards $\omega(1/\lambda)$ -Rate Garbling

Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]



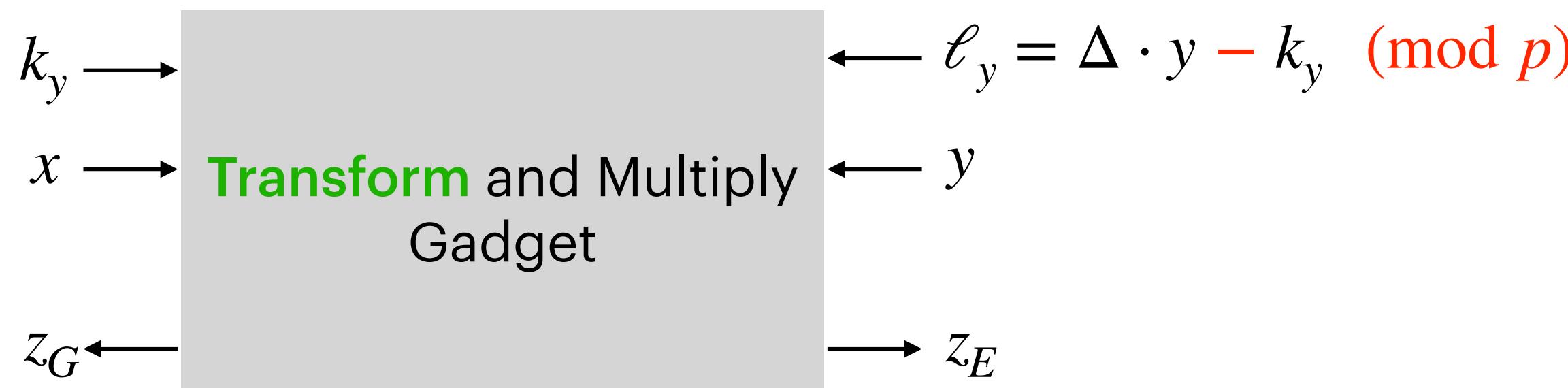
# Towards $\omega(1/\lambda)$ -Rate Garbling

Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]



# Towards $\omega(1/\lambda)$ -Rate Garbling

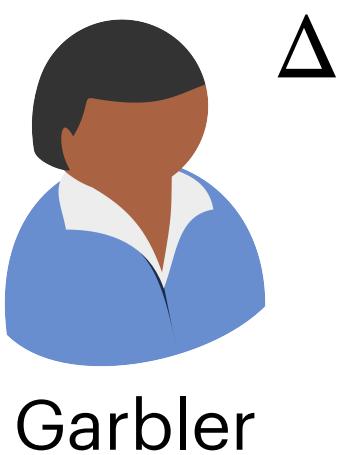
Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]



$$z_G + z_E = x \cdot f(y)$$

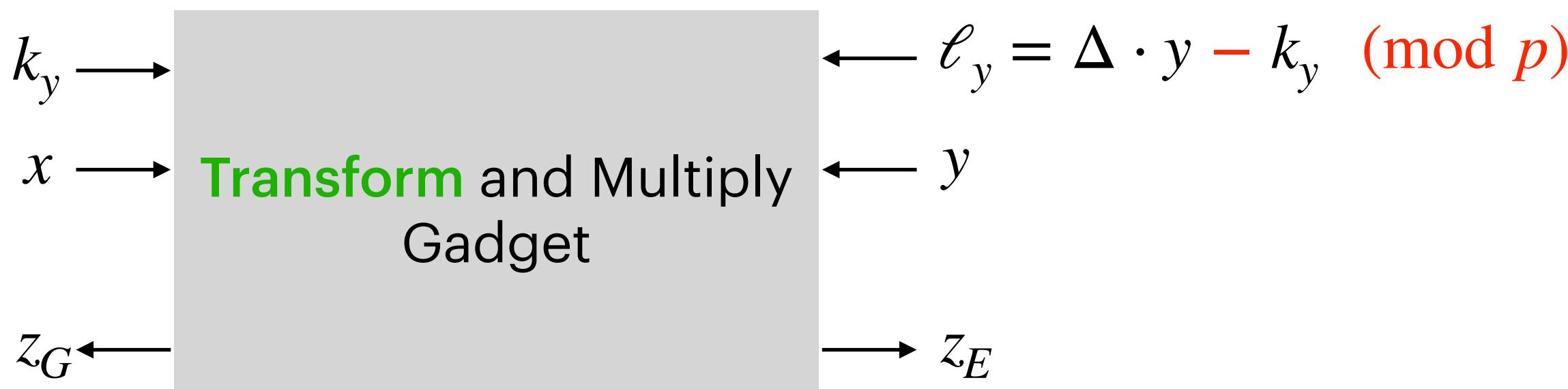
# Towards $\omega(1/\lambda)$ -Rate Garbling

Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]

 $\Delta$ 

**Observation:** Black-box use of crypto  
and secure in the **GGM**

Multiplication Gadget for **Integers**



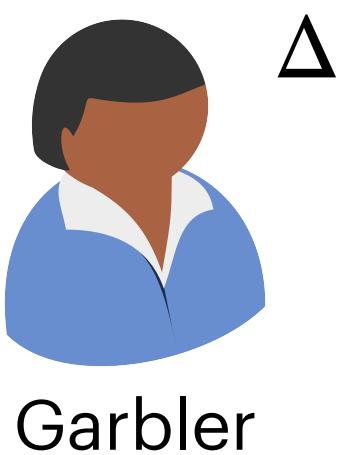
$$z_G + z_E = x \cdot f(y)$$



Evaluator

# Towards $\omega(1/\lambda)$ -Rate Garbling

Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]



Garbler

$\Delta$

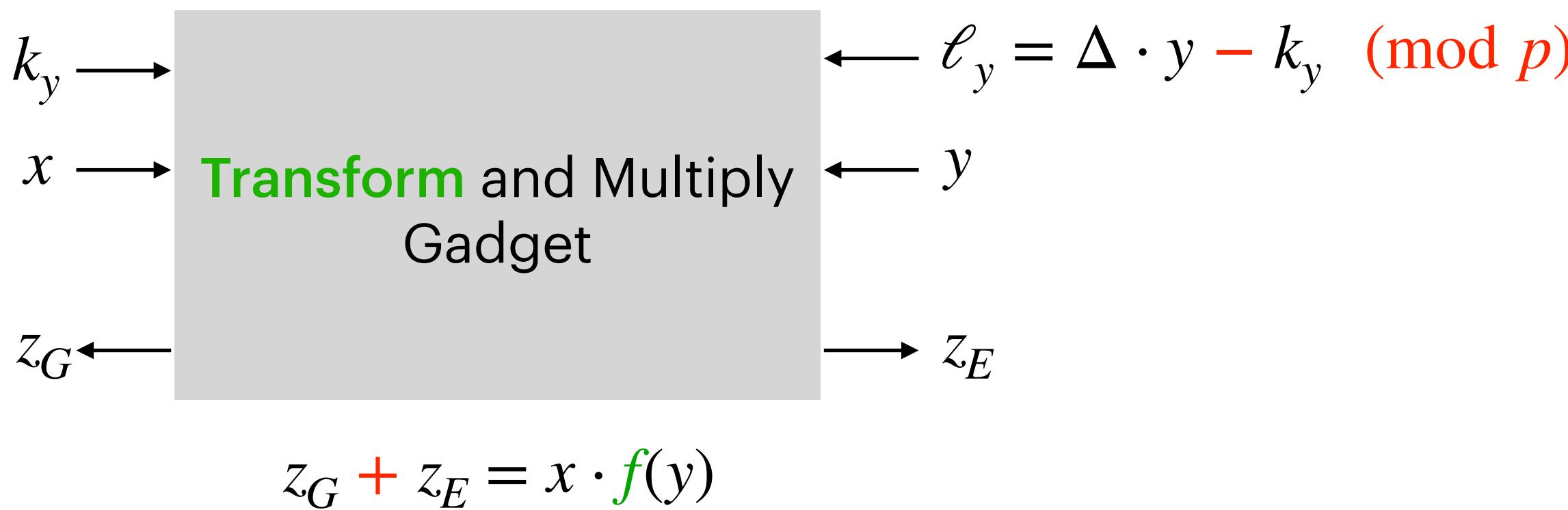


Evaluator

Multiplication Gadget for Integers

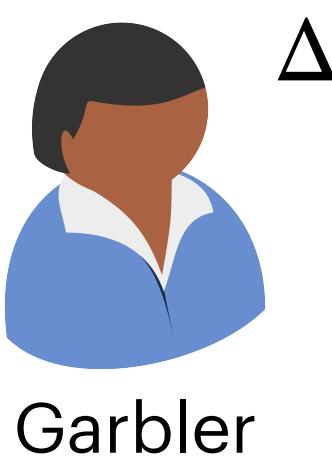
**Observation:** Black-box use of crypto  
and secure in the **GGM**

Garbler sends  $O(\lambda)$ -bit message



# Towards $\omega(1/\lambda)$ -Rate Garbling

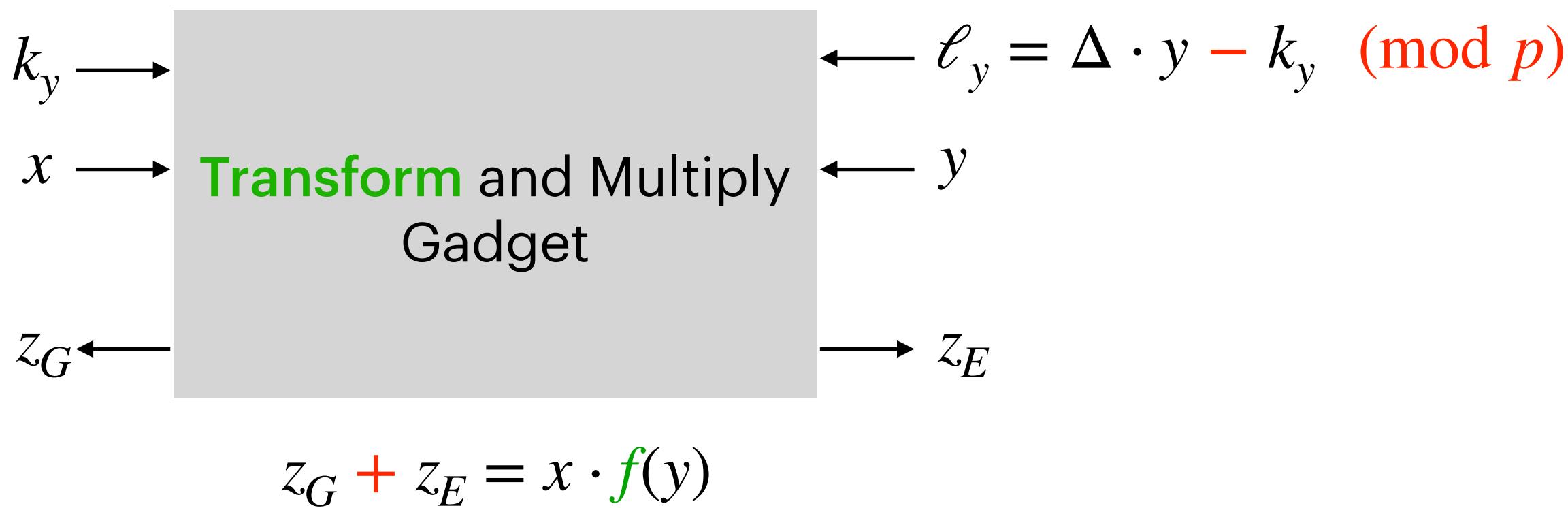
Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]

 $\Delta$ 

**Observation:** Black-box use of crypto  
and secure in the **GGM**

Garbler sends  $O(\lambda)$ -bit message

Multiplication Gadget for **Integers**



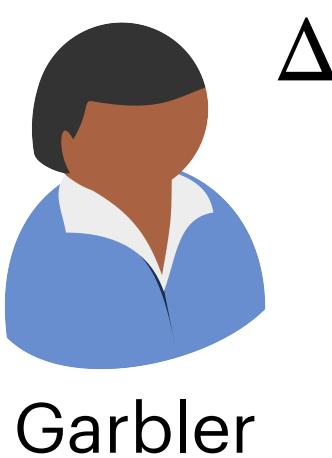
Rate of Arithmetic Garbling over  $\mathbb{Z}_B$ :  $\frac{|C| \cdot \log B}{|\widehat{C}|}$



Evaluator

# Towards $\omega(1/\lambda)$ -Rate Garbling

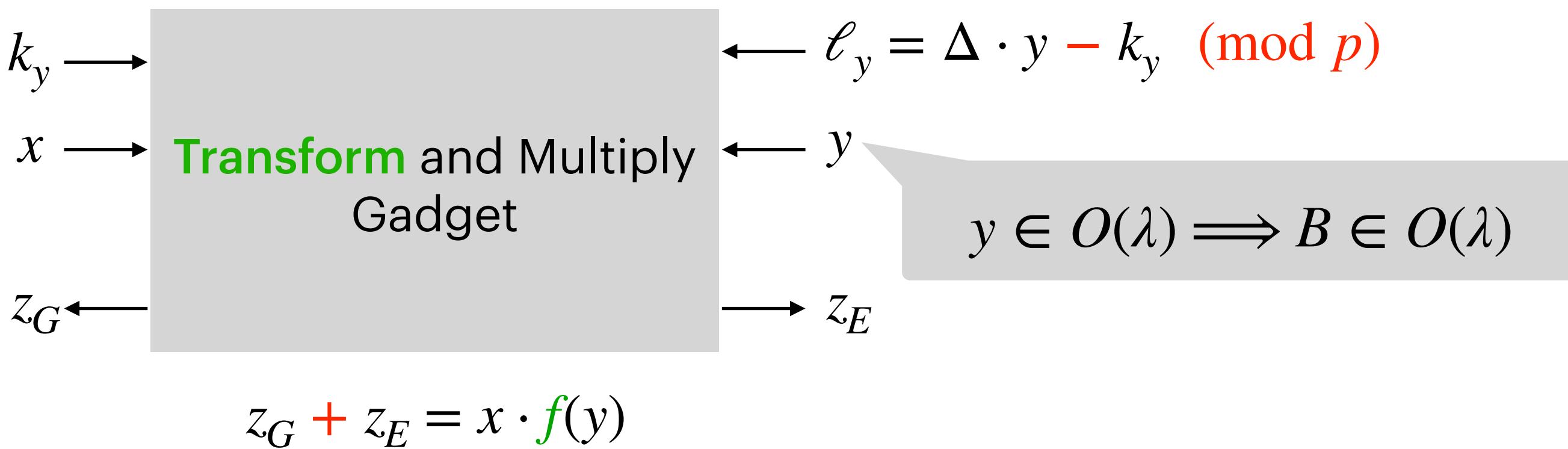
Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]

 $\Delta$ 

**Observation:** Black-box use of crypto  
and secure in the **GGM**

Garbler sends  $O(\lambda)$ -bit message

Multiplication Gadget for **Integers**



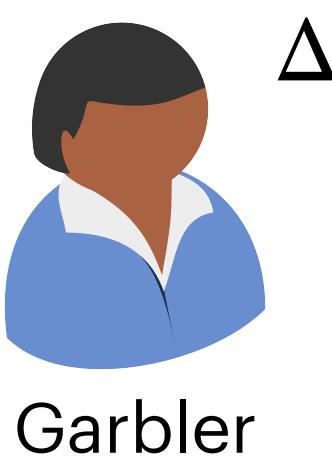
Rate of Arithmetic Garbling over  $\mathbb{Z}_B$ :  $\frac{|C| \cdot \log B}{|\widehat{C}|}$



Evaluator

# Towards $\omega(1/\lambda)$ -Rate Garbling

Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]



Garbler

$\Delta$

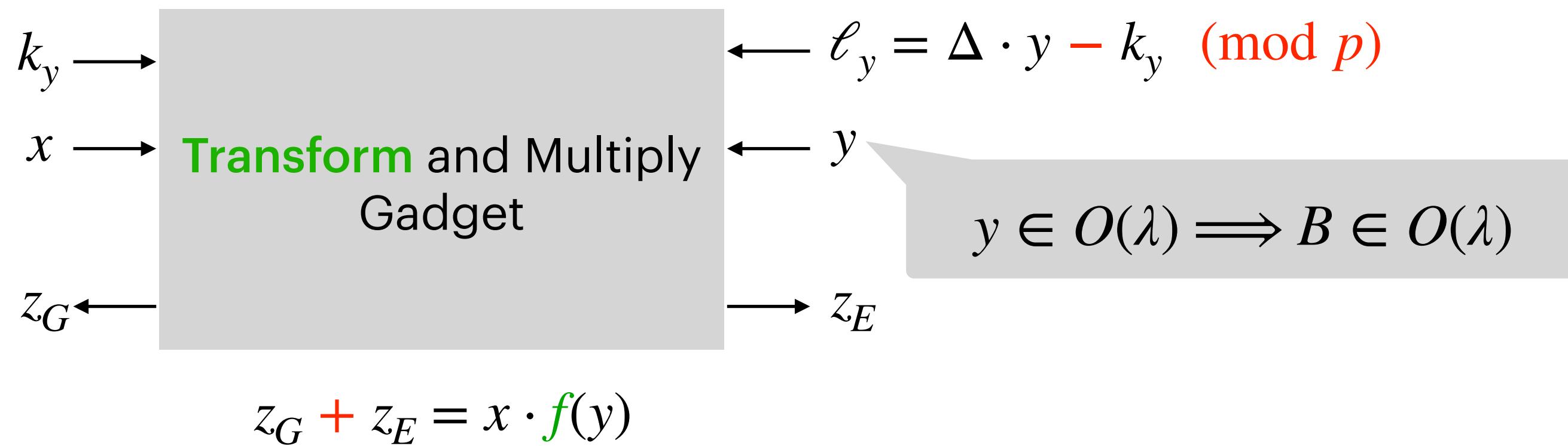


Evaluator

Multiplication Gadget for Integers

**Observation:** Black-box use of crypto and secure in the GGM

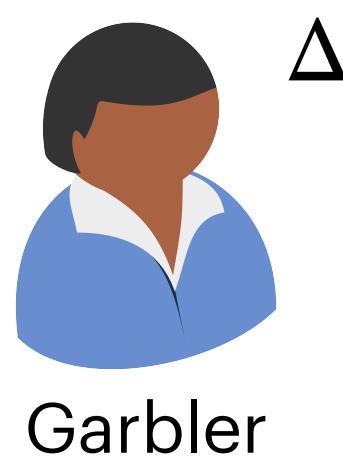
Garbler sends  $O(\lambda)$ -bit message



Rate of Arithmetic Garbling over  $\mathbb{Z}_B$ :  $\frac{|C| \cdot \log B}{|\widehat{C}|} = O\left(\frac{\log \lambda}{\lambda}\right)$

# Towards $\omega(1/\lambda)$ -Rate Garbling

Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]



Garbler

$\Delta$

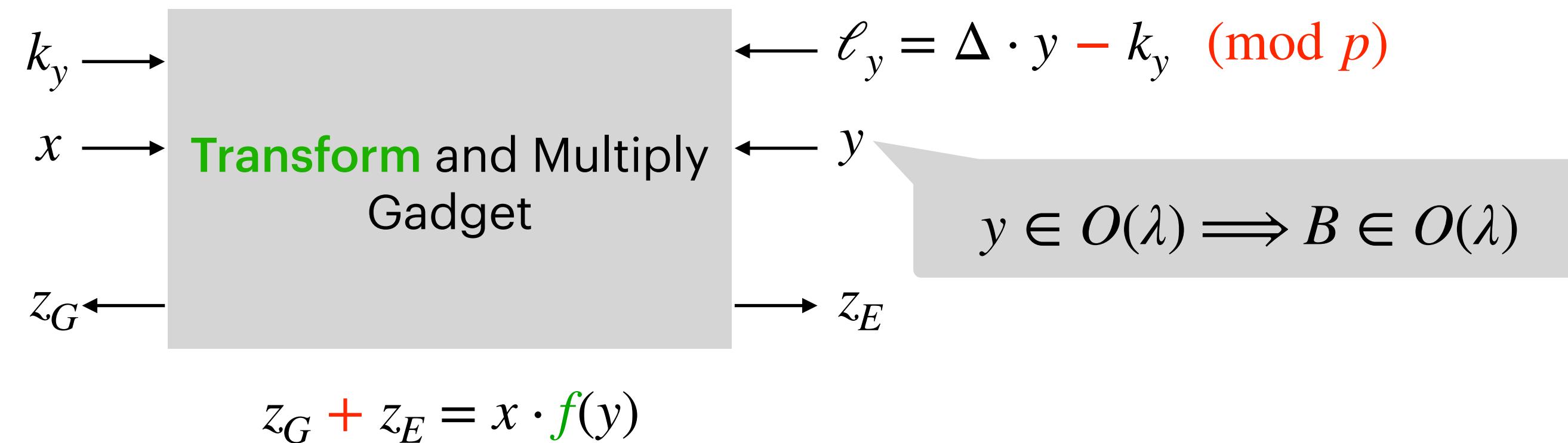


Evaluator

Multiplication Gadget for Integers

**Observation:** Black-box use of crypto  
and secure in the **GGM**

Garbler sends  $O(\lambda)$ -bit message

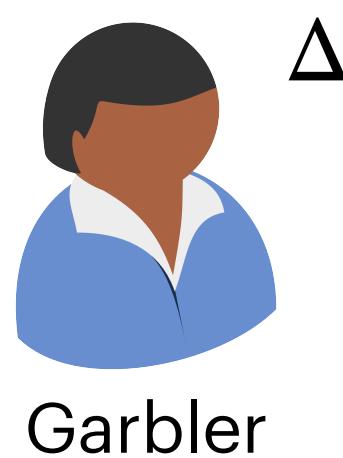


Rate of Arithmetic Garbling over  $\mathbb{Z}_B$ :  $\frac{|C| \cdot \log B}{|\widehat{C}|} = O\left(\frac{\log \lambda}{\lambda}\right)$

Rate of Boolean Garbling:  $O\left(\frac{1}{\lambda}\right)$

# Towards $\omega(1/\lambda)$ -Rate Garbling

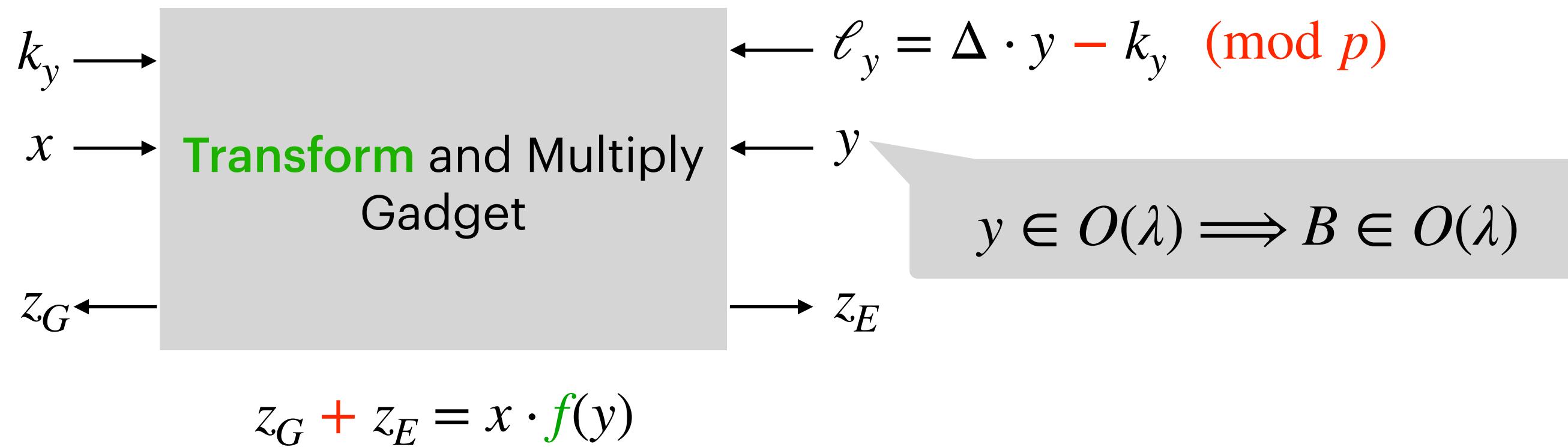
Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]

 $\Delta$ 

**Observation:** Black-box use of crypto and secure in the [GGM](#)

Garbler sends  $O(\lambda)$ -bit message

Multiplication Gadget for [Integers](#)

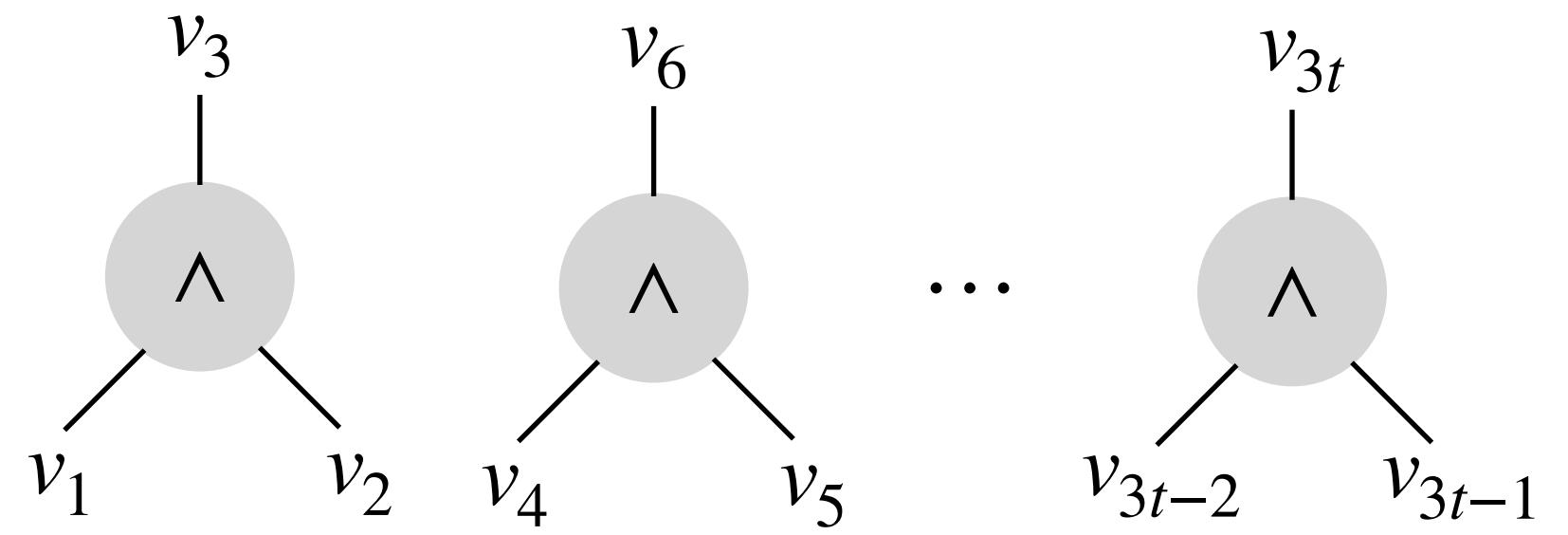


Rate of Arithmetic Garbling over  $\mathbb{Z}_B$ :  $\frac{|C| \cdot \log B}{|\widehat{C}|} = O\left(\frac{\log \lambda}{\lambda}\right)$

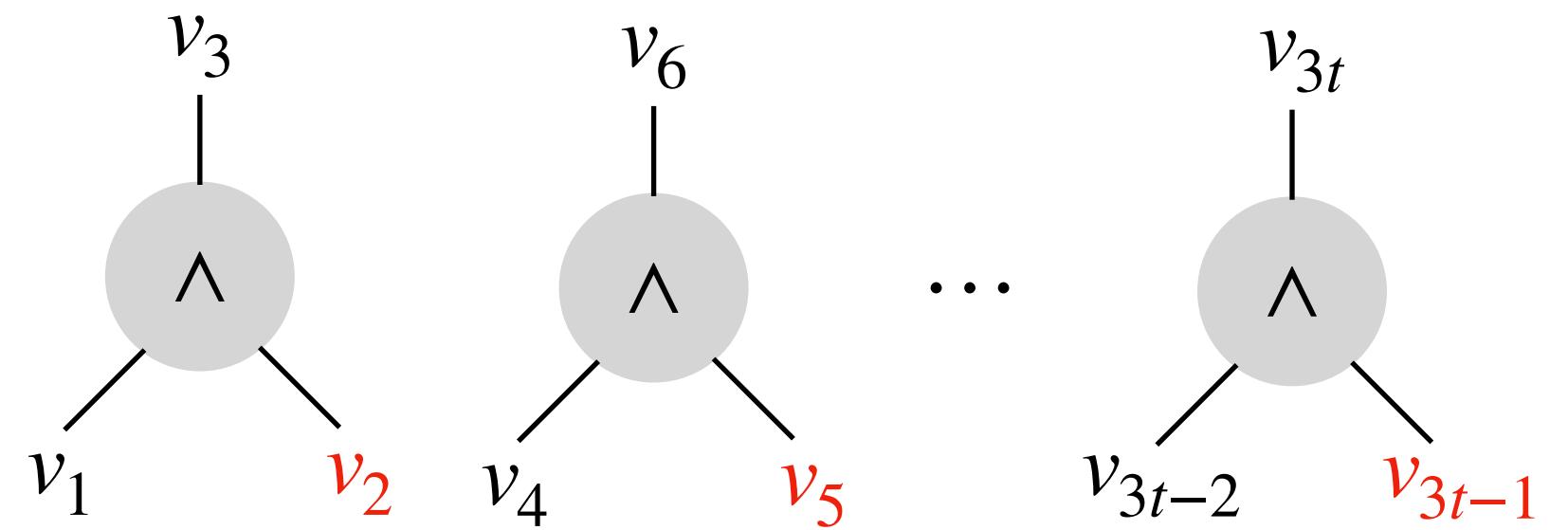
Rate of Boolean Garbling:  $O\left(\frac{1}{\lambda}\right)$

**Key Ingredient:** A [packing](#) from  $\mathbb{F}_2^t$  to  $\log \lambda$ -bit integers

# Template for $\omega(1/\lambda)$ -Rate Garbling



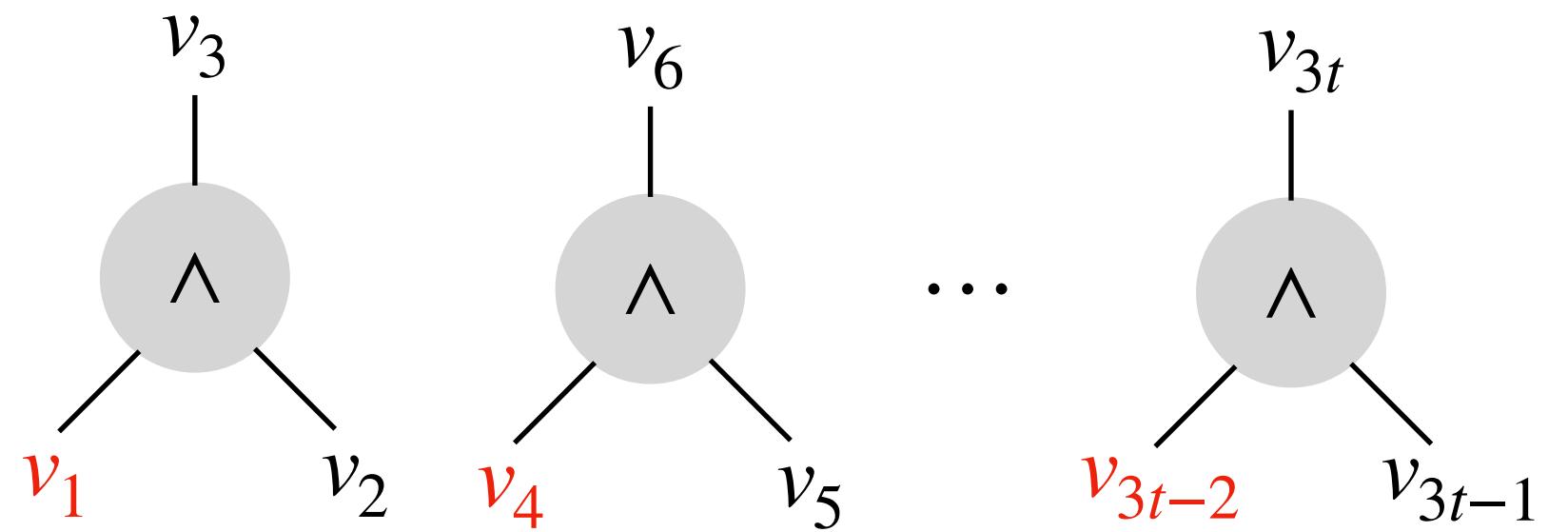
# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

# Template for $\omega(1/\lambda)$ -Rate Garbling

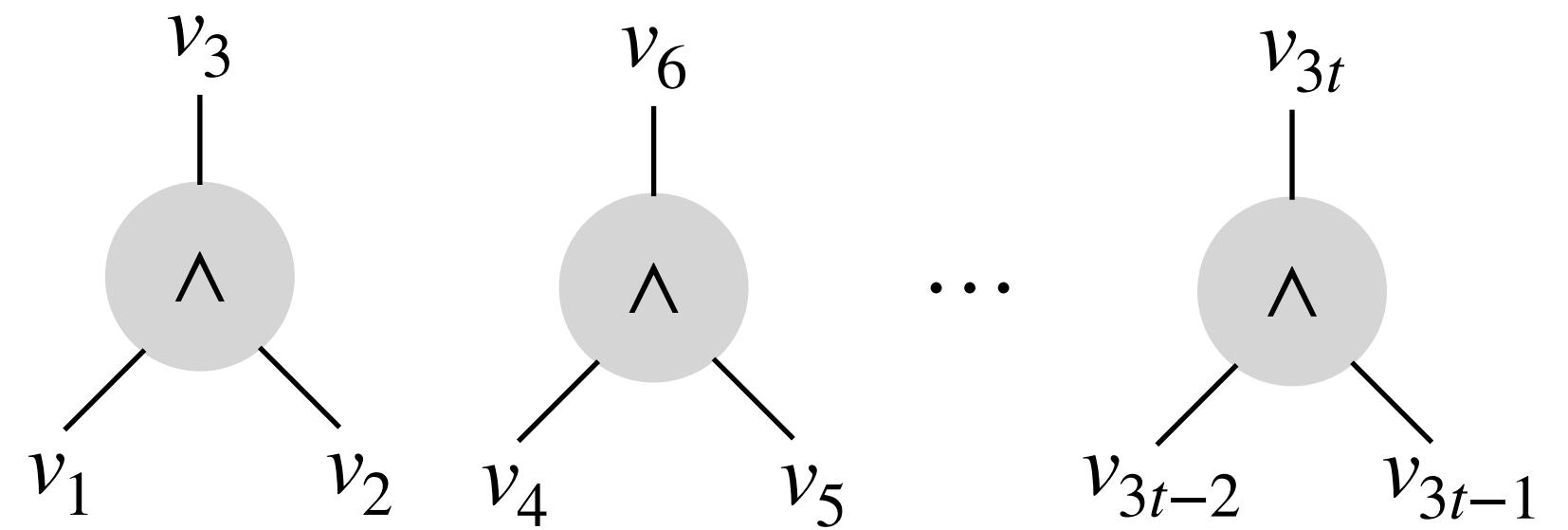


## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

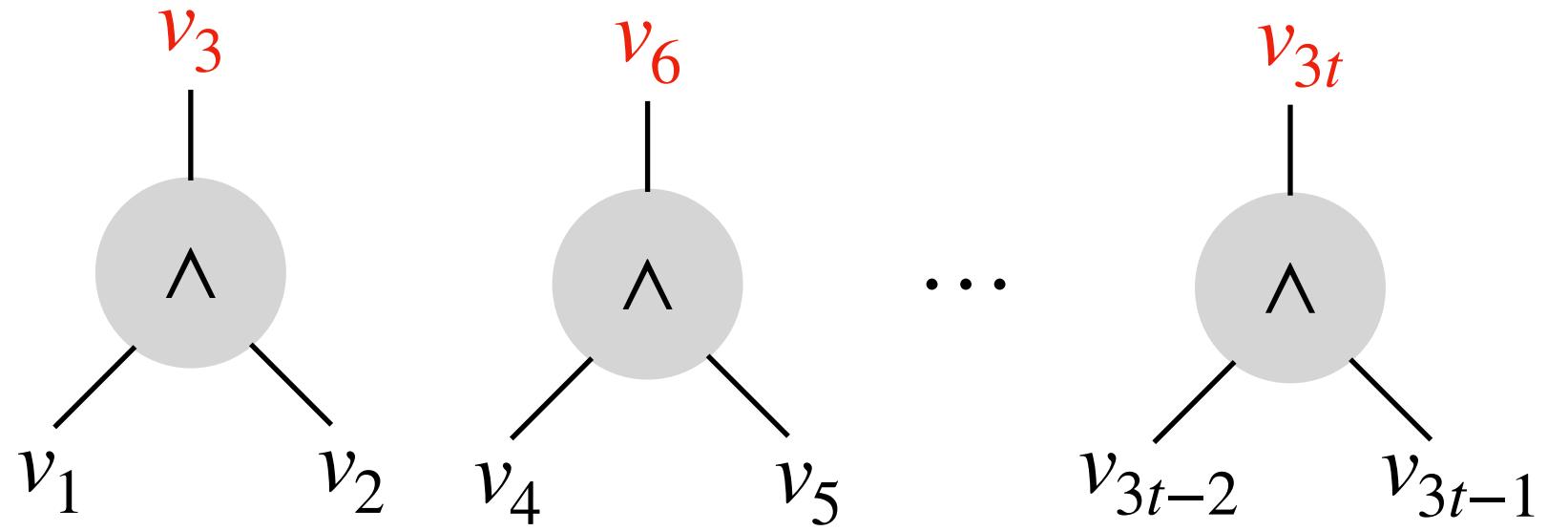
$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

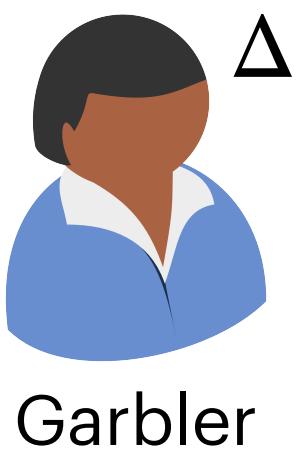
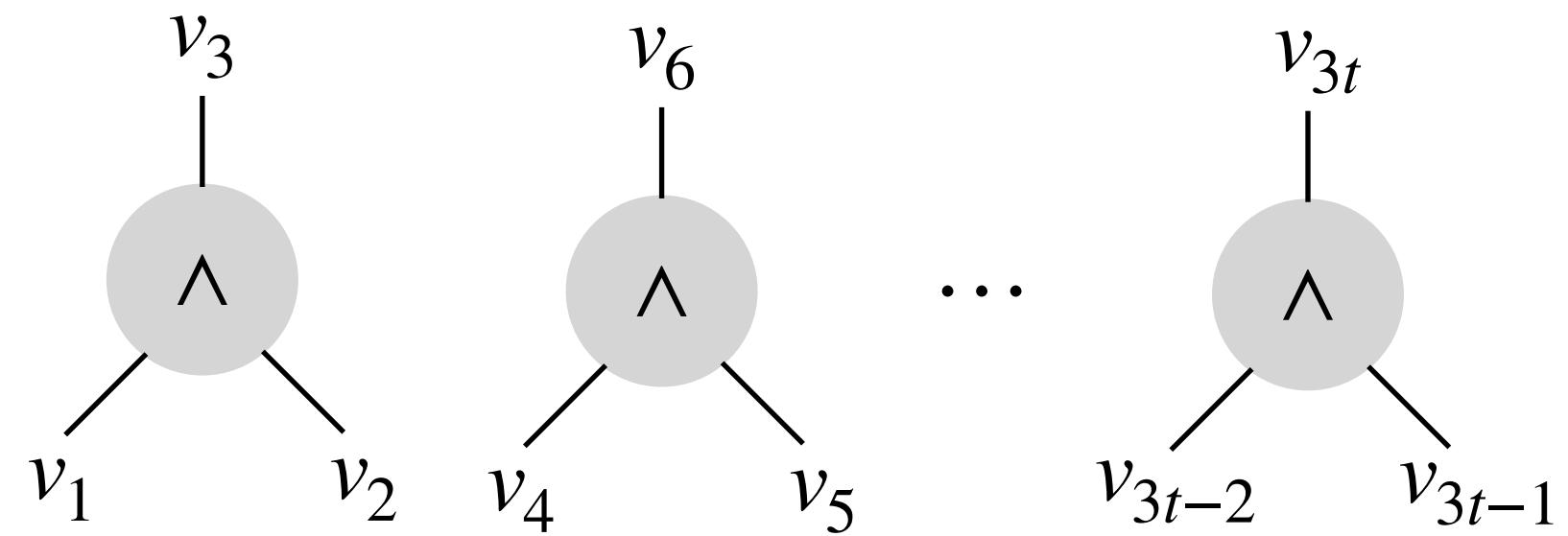
## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



**Invariant**

$$g_i \oplus e_i = v_i$$

$$k_i + \ell_i = \Delta \cdot e_i \pmod{p}$$



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

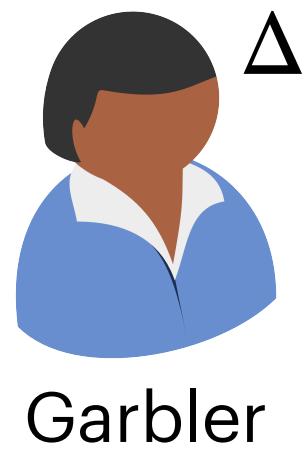
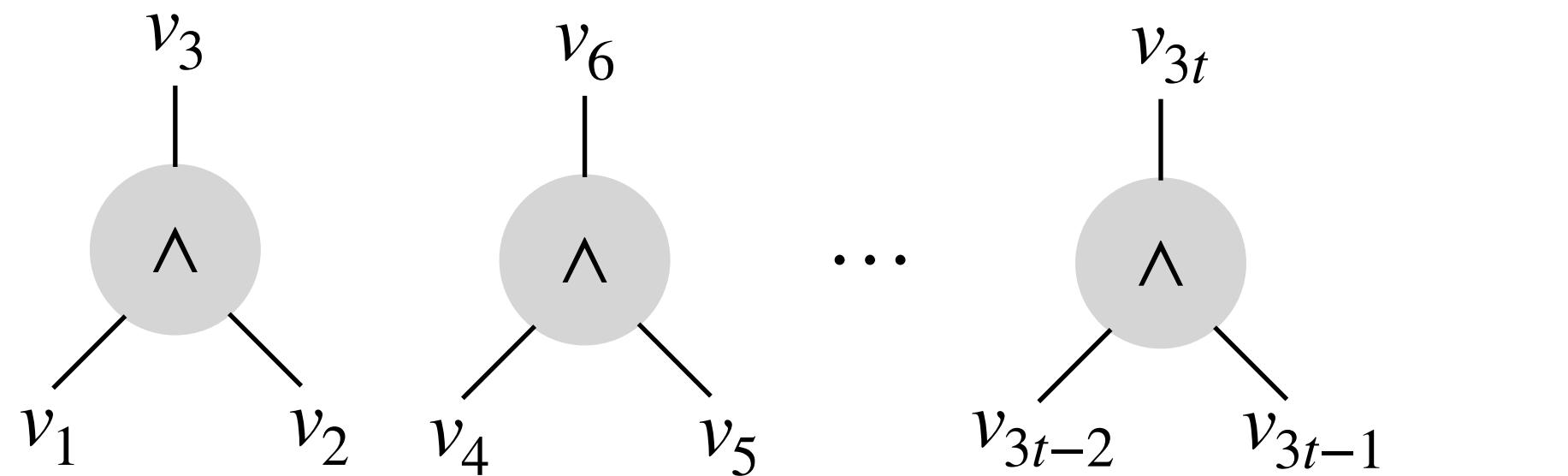
## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



**Invariant**

$$g_i \oplus e_i = v_i$$

$$k_i + \ell_i = \Delta \cdot e_i \pmod{p}$$



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

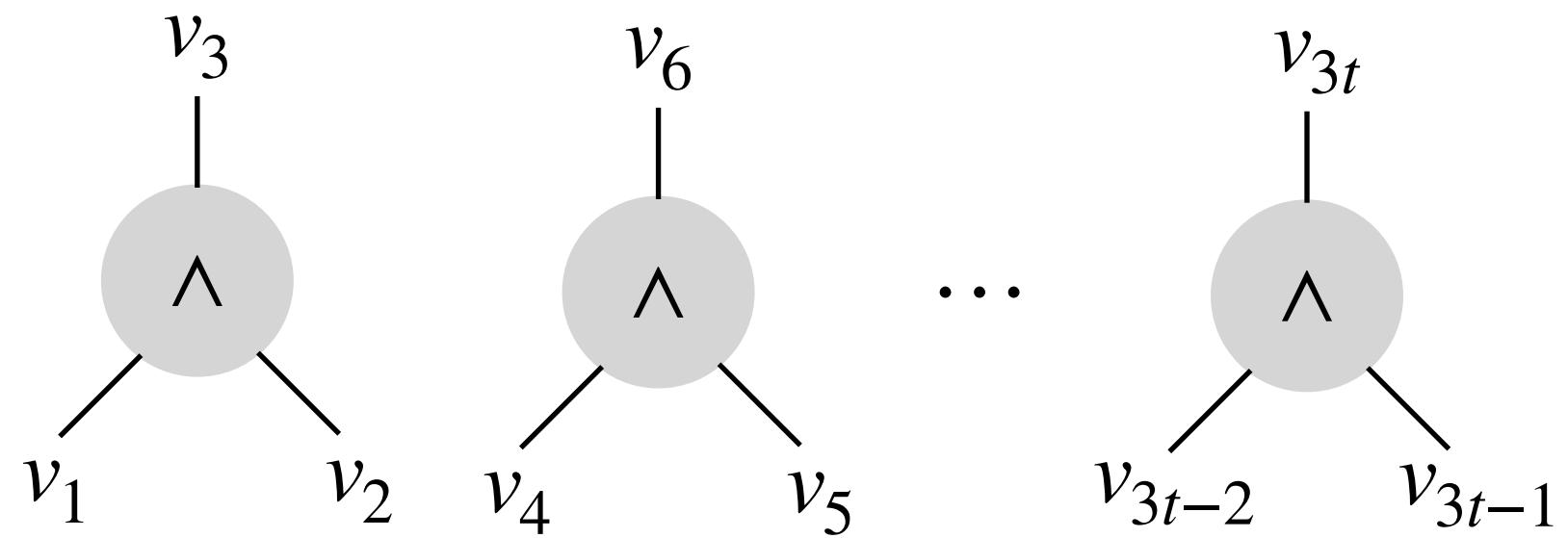
$$V = V_1 \cdot V_2$$

Evaluate over **shares** of packed encodings using **multiplication gadget**

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



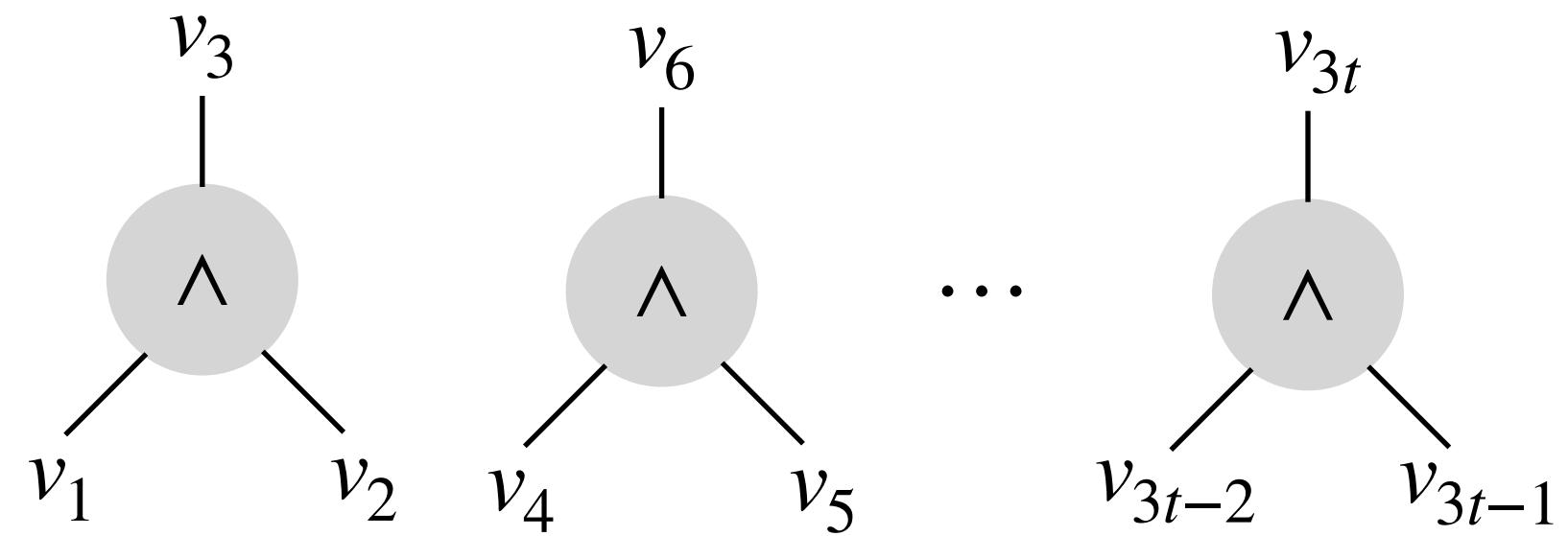
**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

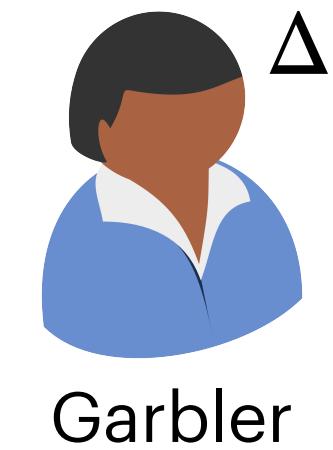
$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

Pack is  $\mathbb{F}_2$ -linear

$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$



### Invariant

$$g_i \oplus e_i = v_i$$

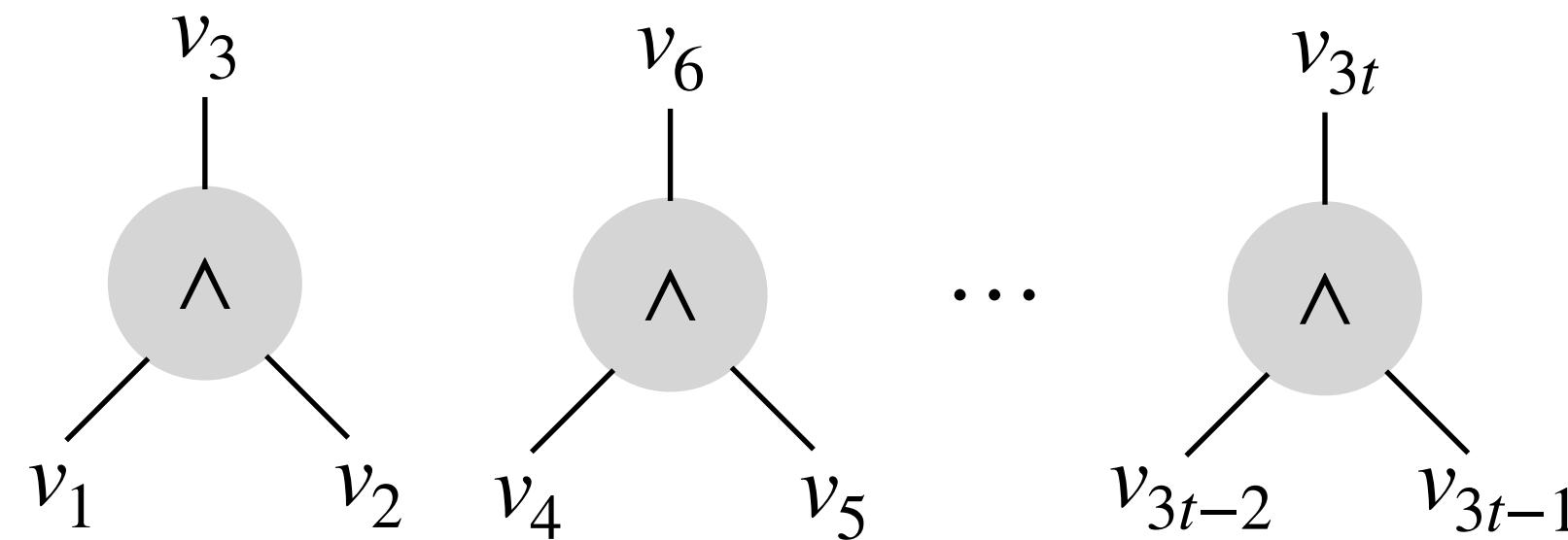
$$k_i + \ell_i = \Delta \cdot e_i \pmod{p}$$



## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

Pack is  $\mathbb{F}_2$ -linear

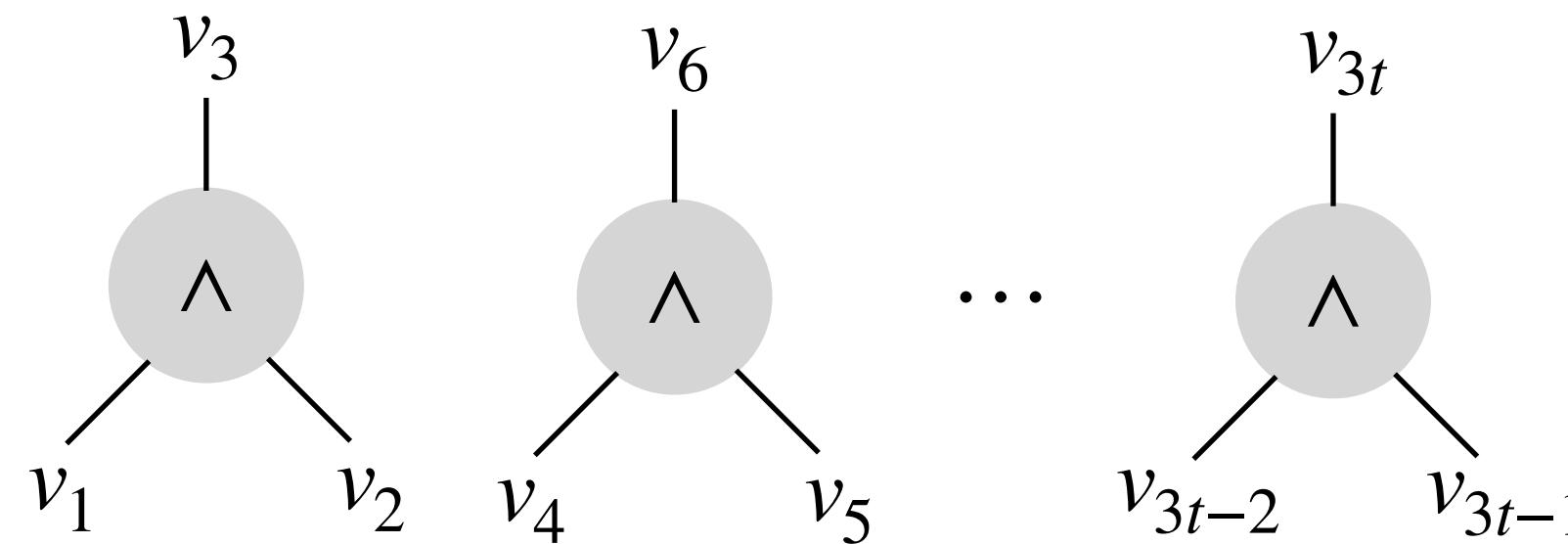
$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

We will need shares of  $\Delta \cdot E_R$  for evaluating the gate

$$K_R$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

Pack is  $\mathbb{F}_2$ -linear

$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

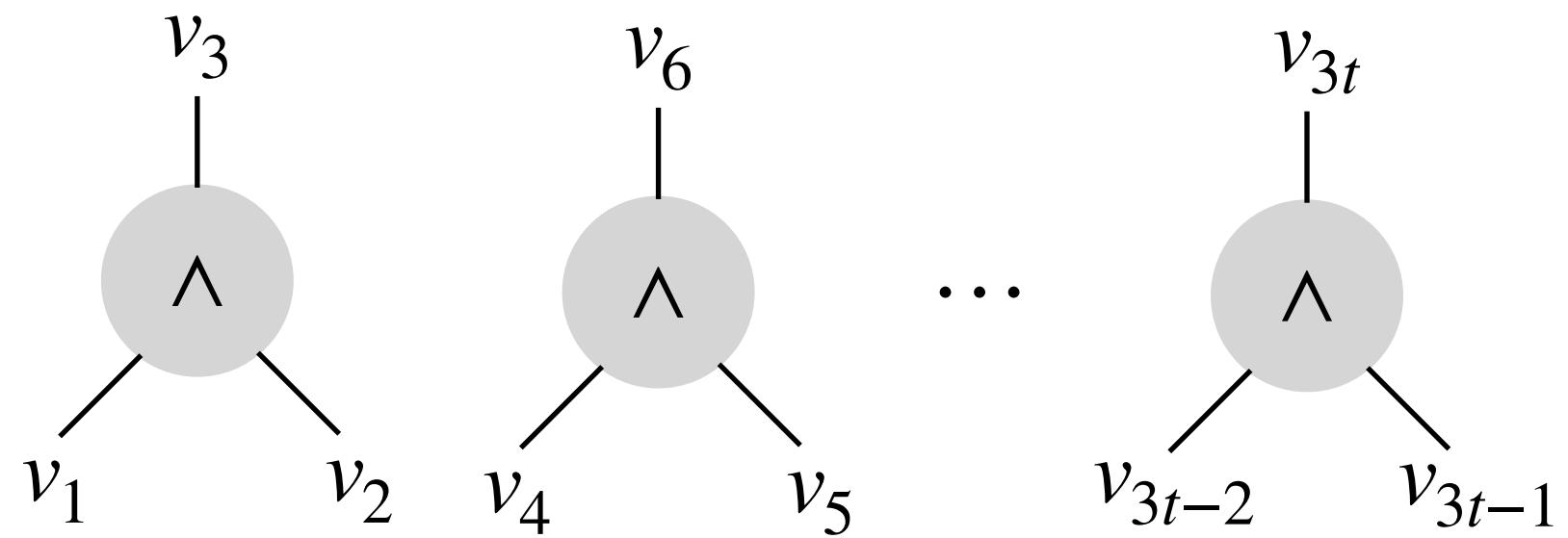
We will need shares of  $\Delta \cdot E_R$  for evaluating the gate

$$K_R$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$(k_i, \ell_i)$  are shares over  $\mathbb{Z}_p \implies$  Can't use Pack directly

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

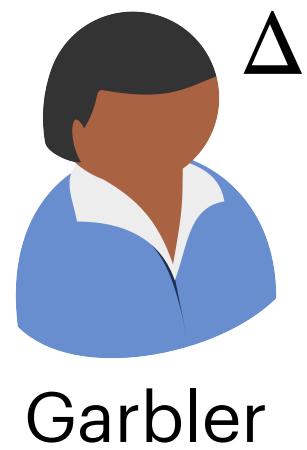
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



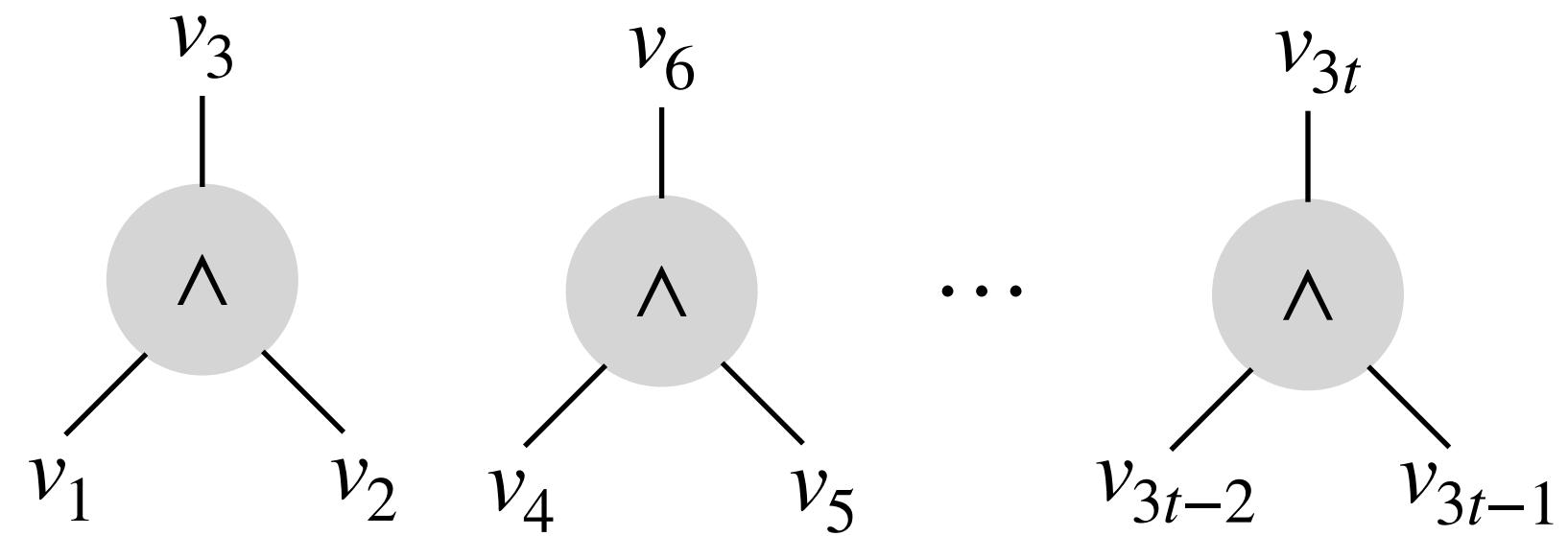
**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

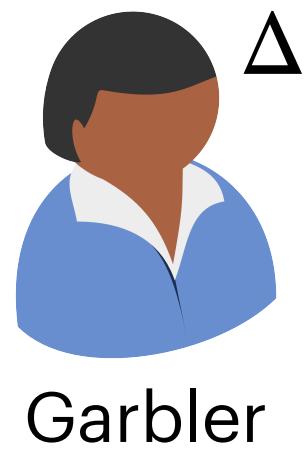
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\mathbf{g}_i \oplus \mathbf{e}_i = v_i$$

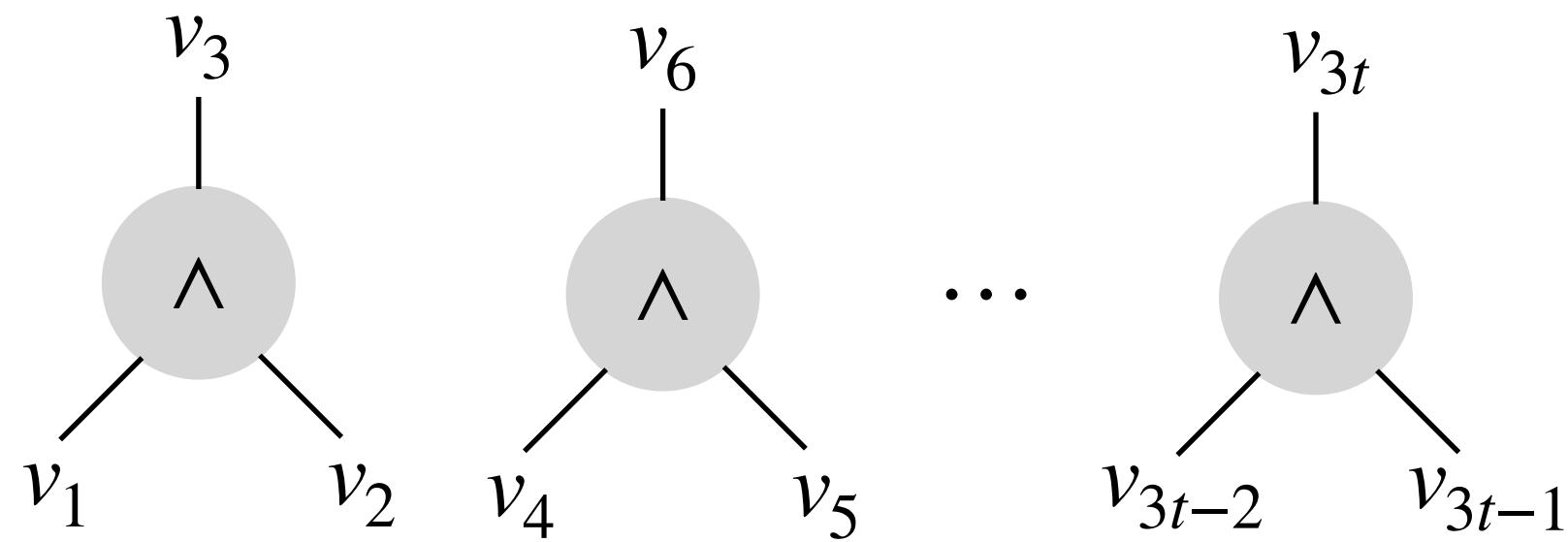
$$k_i + \ell_i = \Delta \cdot \mathbf{e}_i \pmod{p}$$



$$E_R = \text{Pack}(\mathbf{e}_2, \mathbf{e}_5, \dots, \mathbf{e}_{3t-1})$$

$$E^* = \sum_{i=1}^t \mathbf{e}_{3i-1} \cdot 2^i$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

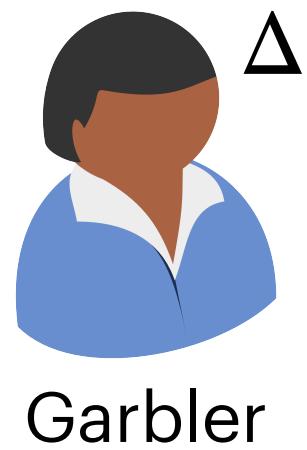
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\mathbf{g}_i \oplus \mathbf{e}_i = v_i$$

$$k_i + \ell_i = \Delta \cdot \mathbf{e}_i \pmod{p}$$



$$G_R = \text{Pack}(\mathbf{g}_2, \mathbf{g}_5, \dots, \mathbf{g}_{3t-1})$$

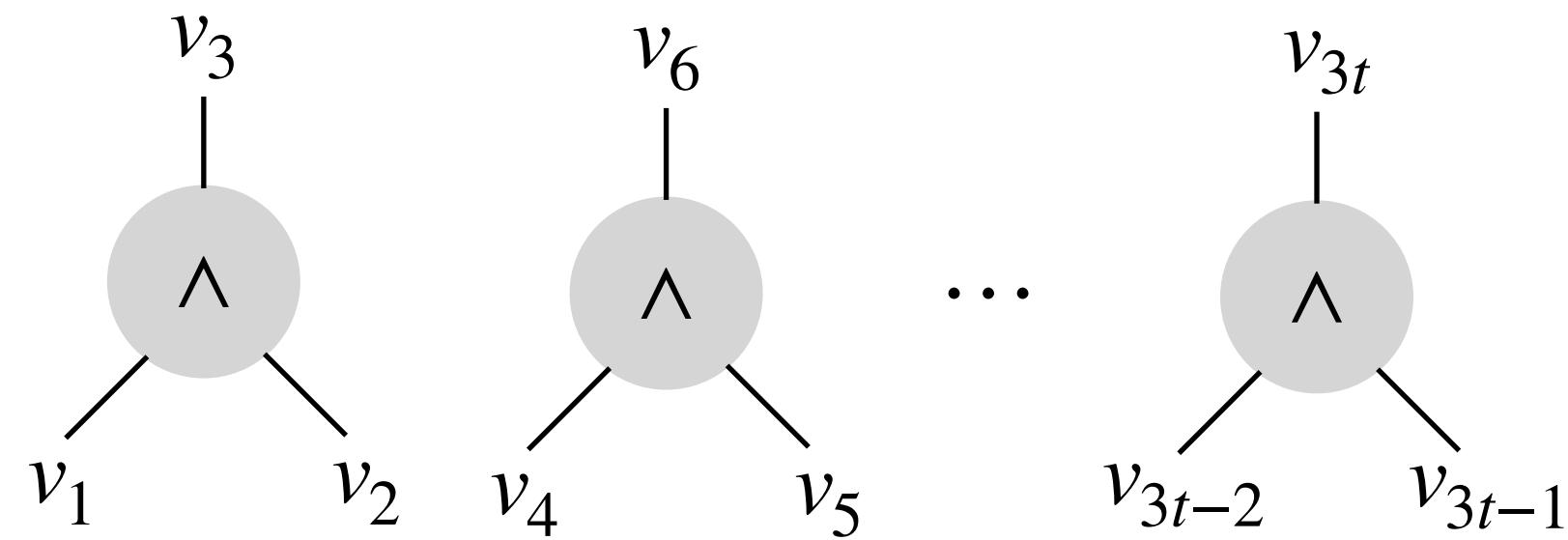
$$E_R = \text{Pack}(\mathbf{e}_2, \mathbf{e}_5, \dots, \mathbf{e}_{3t-1})$$

$$E^* = \sum_{i=1}^t \mathbf{e}_{3i-1} \cdot 2^i$$

$$L^* = \sum_{i=1}^t \ell_{3i-1} \cdot 2^i \pmod{p}$$

$$K^* = \sum_{i=1}^t k_{3i-1} \cdot 2^i \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

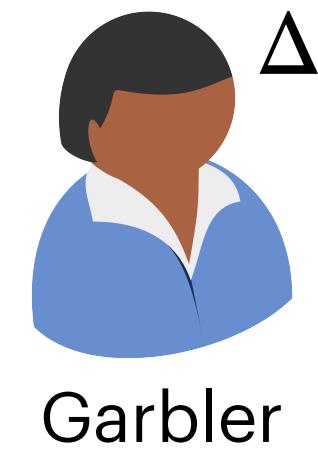
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



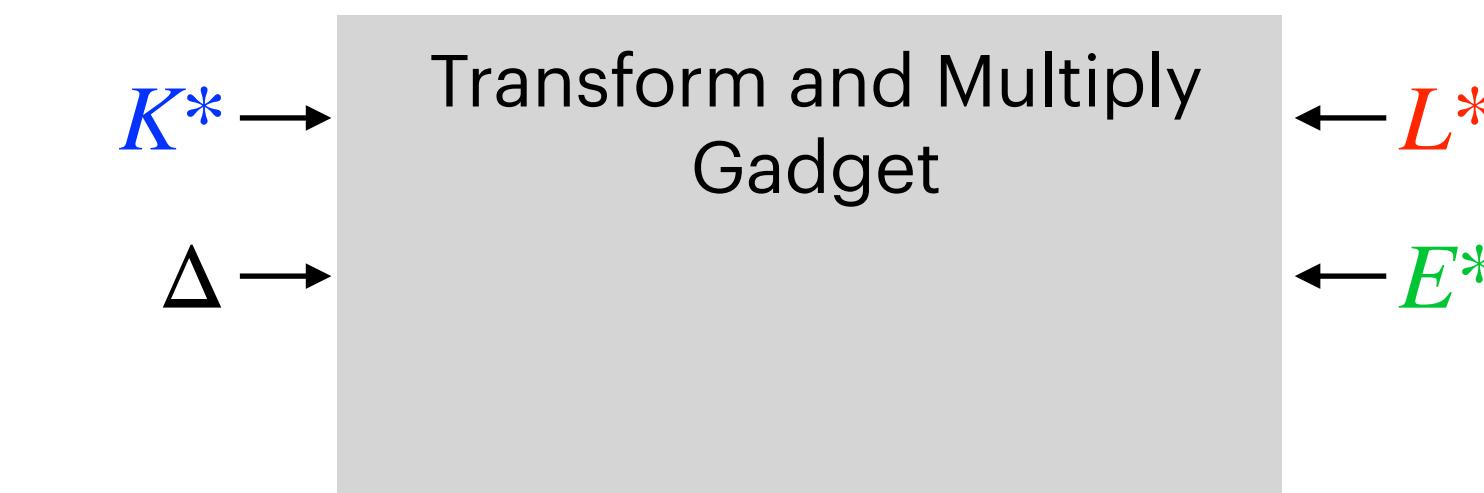
$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

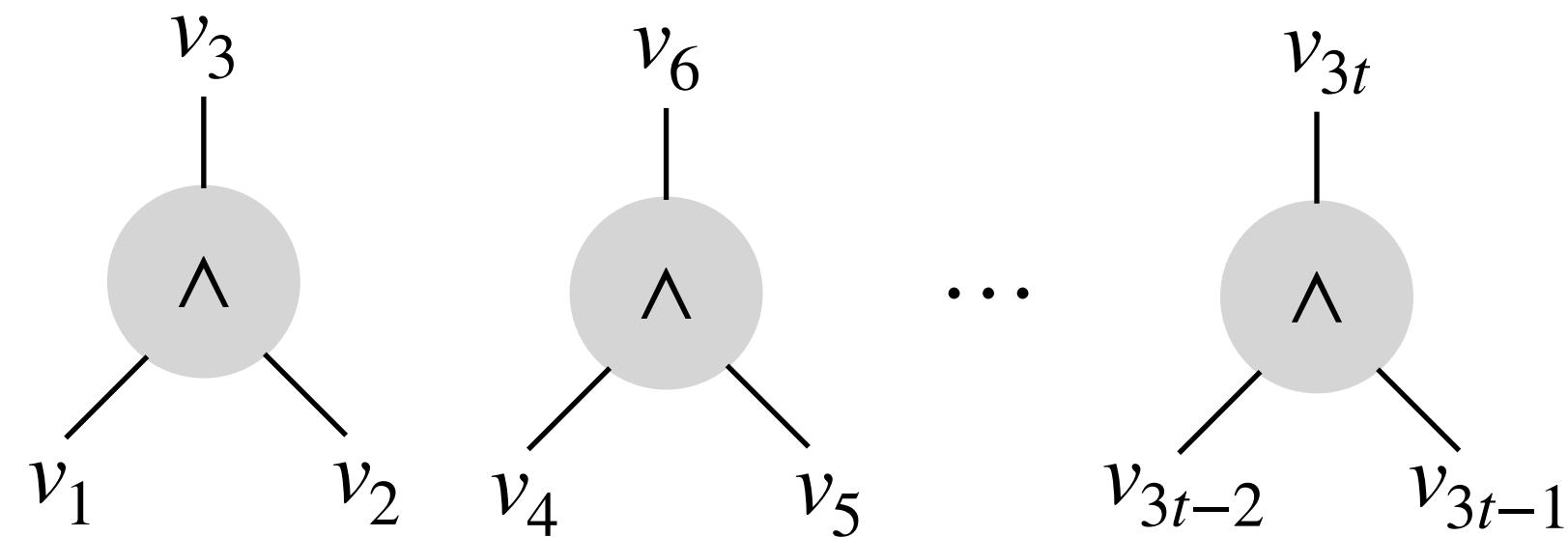
$$E^* = \sum_{i=1}^t e_{3i-1} \cdot 2^i$$

$$K^* = \sum_{i=1}^t k_{3i-1} \cdot 2^i \pmod{p}$$

$$L^* = \sum_{i=1}^t \ell_{3i-1} \cdot 2^i \pmod{p}$$



# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E^* = \sum_{i=1}^t e_{3i-1} \cdot 2^i$$

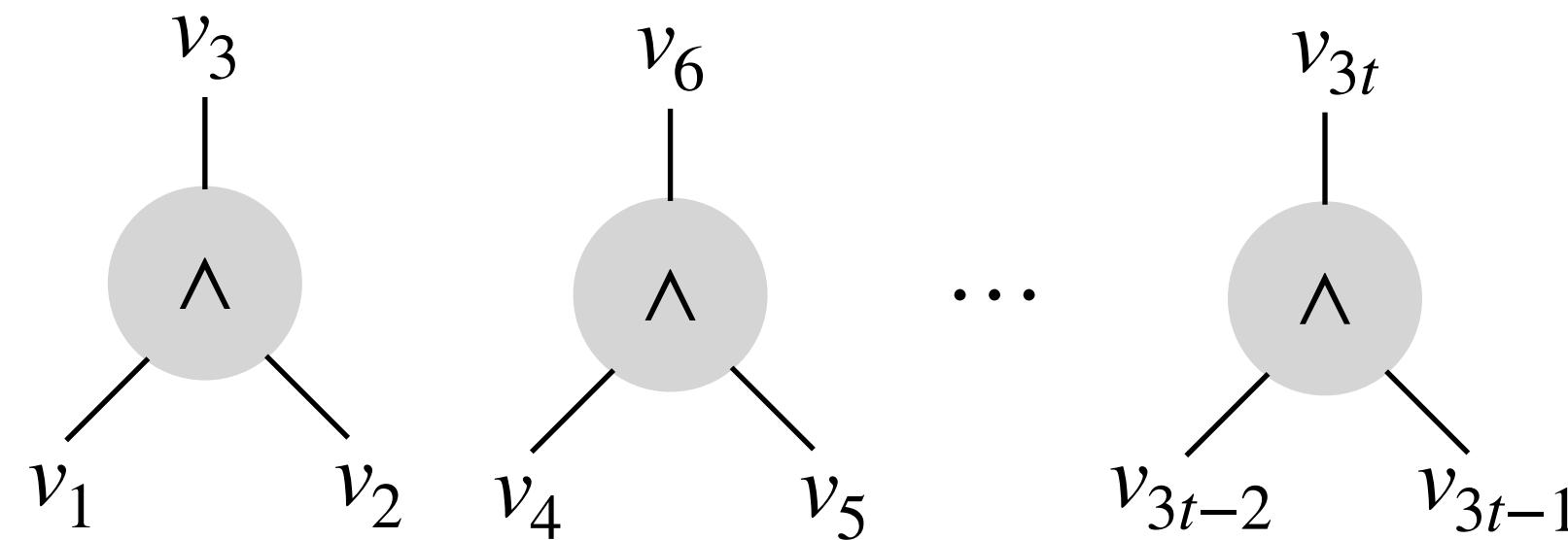
$$L^* = \sum_{i=1}^t \ell_{3i-1} \cdot 2^i \pmod{p}$$

$$K^* = \sum_{i=1}^t k_{3i-1} \cdot 2^i \pmod{p}$$

$K^* \rightarrow$  Transform and Multiply Gadget  
 $\Delta \rightarrow$

$$\begin{aligned} \leftarrow L^* &= \Delta \cdot E^* - K^* \pmod{p} \\ \leftarrow E^* & \end{aligned}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E^* = \sum_{i=1}^t e_{3i-1} \cdot 2^i$$

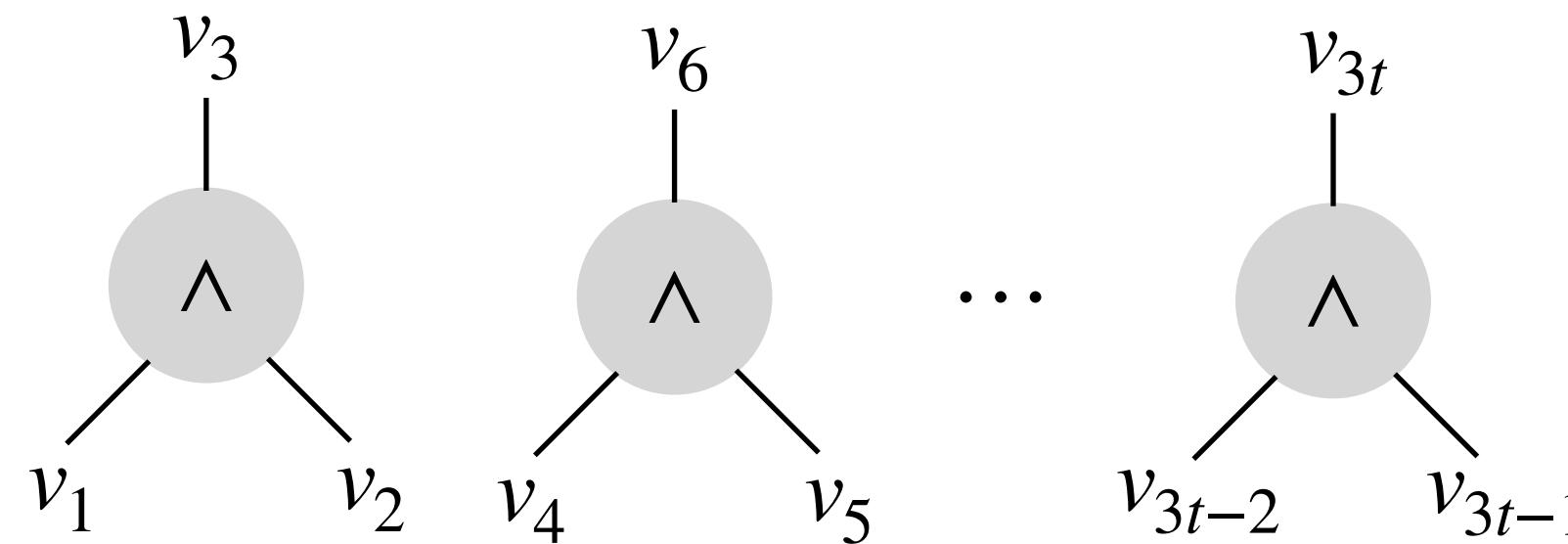
$$L^* = \sum_{i=1}^t \ell_{3i-1} \cdot 2^i \pmod{p}$$

$$K^* = \sum_{i=1}^t k_{3i-1} \cdot 2^i \pmod{p}$$

$K^* \rightarrow$  Transform and Multiply Gadget  
 $\Delta \rightarrow$   
 $f(x) = \text{Pack}(\text{Bits}(x))$

$$\begin{aligned} \leftarrow L^* &= \Delta \cdot E^* - K^* \pmod{p} \\ \leftarrow E^* \end{aligned}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &\equiv \Delta \cdot e_i \pmod{p} \end{aligned}$$



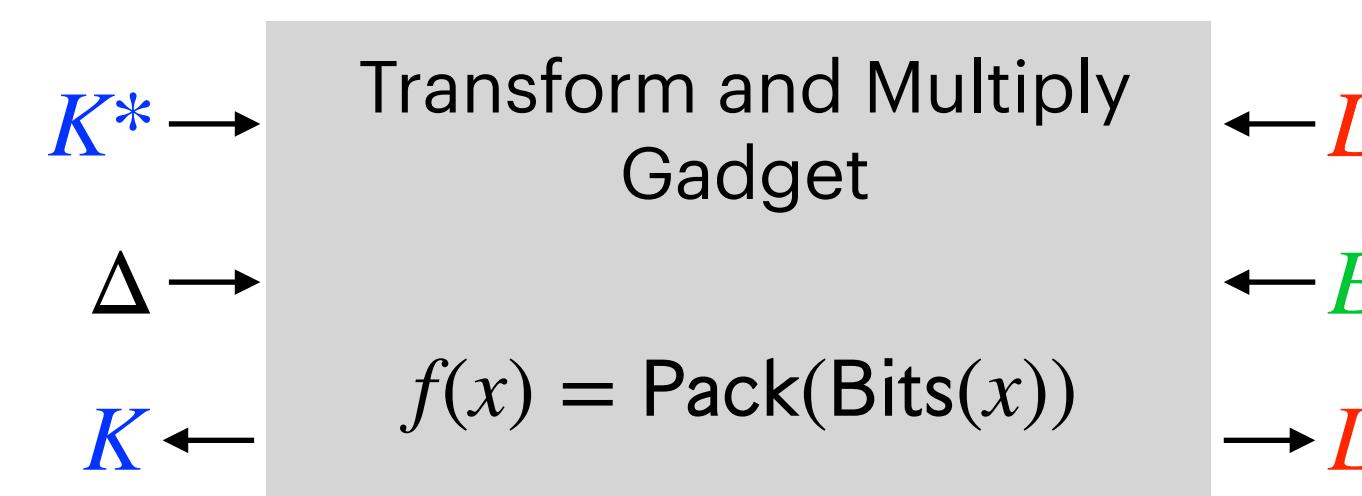
$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E^* = \sum_{i=1}^t e_{3i-1} \cdot 2^i$$

$$L^* = \sum_{i=1}^t \ell_{3i-1} \cdot 2^i \pmod{p}$$

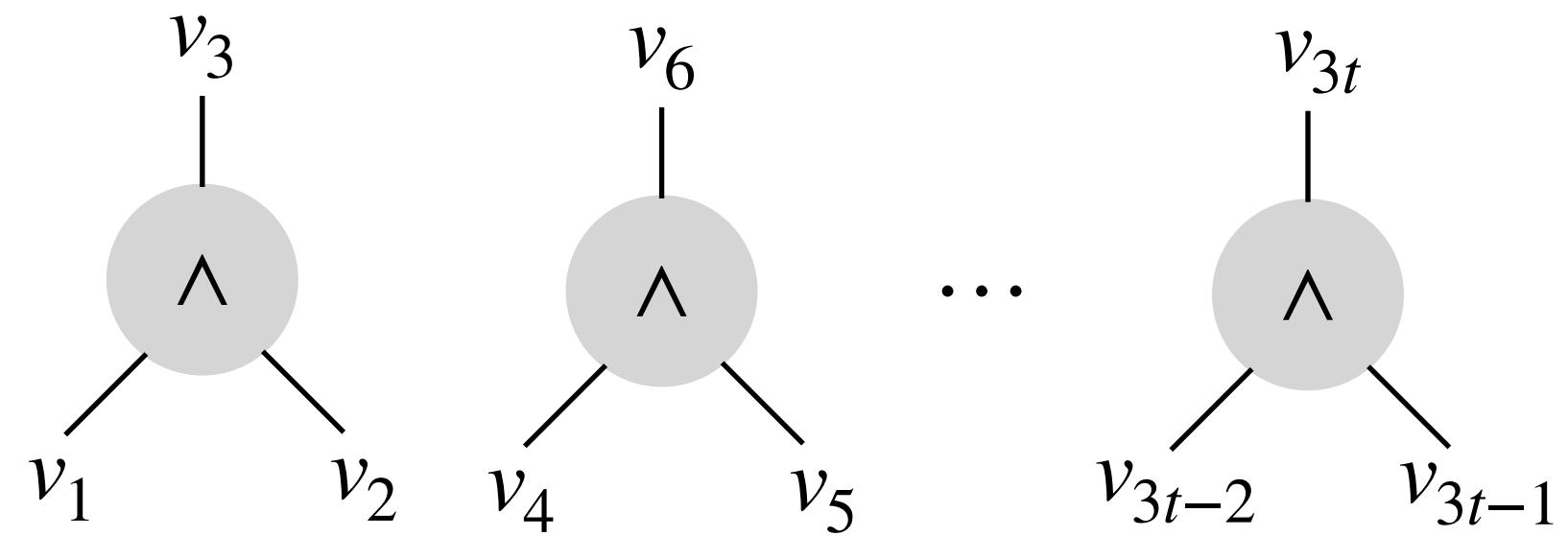
$$K^* = \sum_{i=1}^t k_{3i-1} \cdot 2^i \pmod{p}$$



$$K + L = \Delta \cdot f(E^*)$$

$$= \Delta \cdot E_R$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

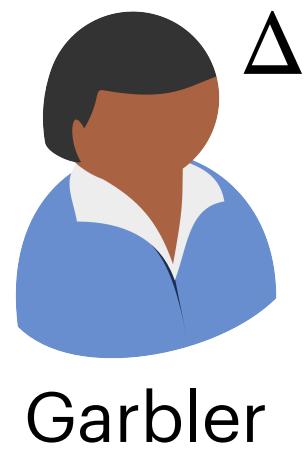
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



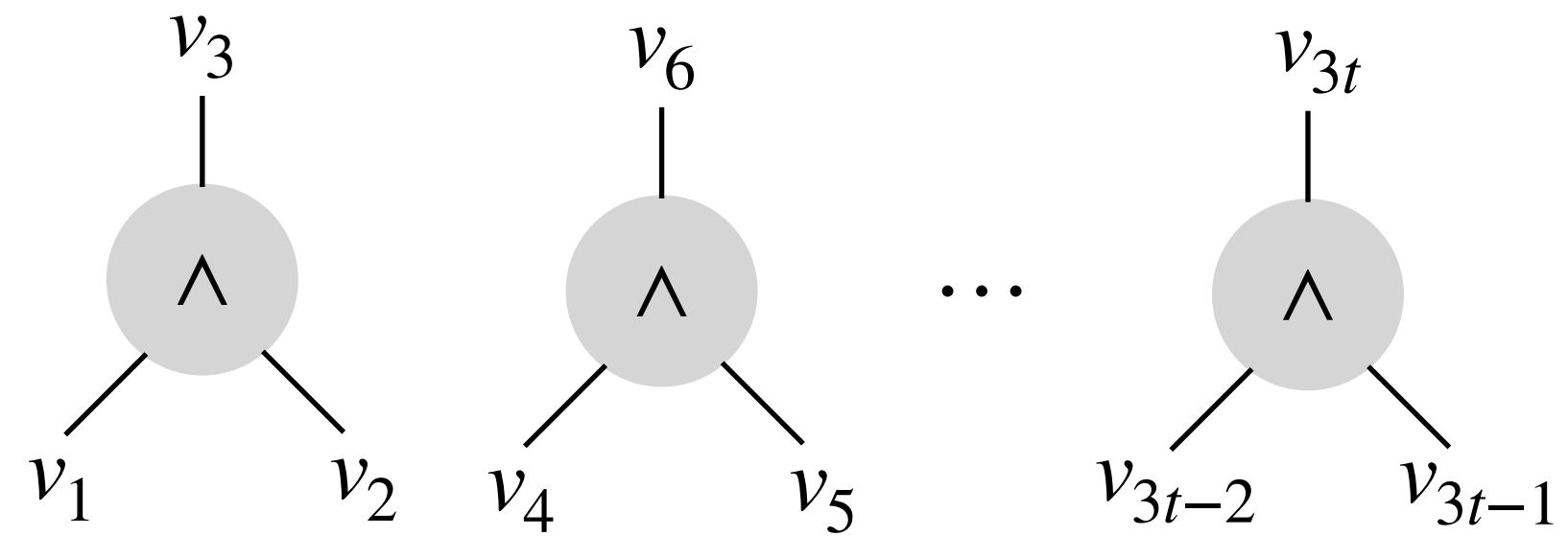
**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

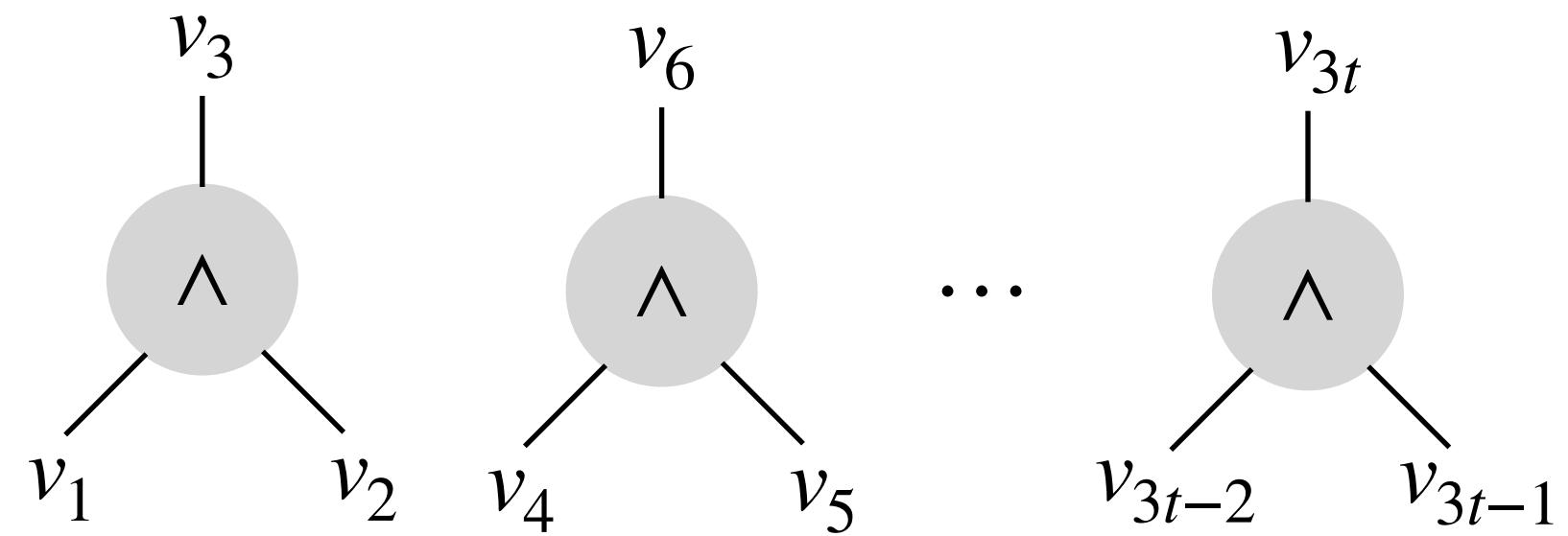
$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$K_R$$



$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

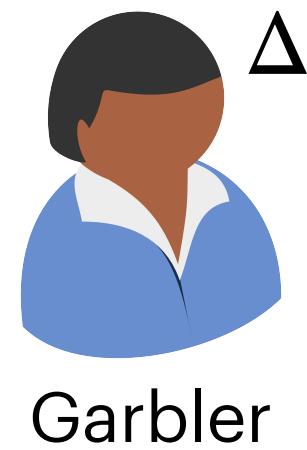
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



**Invariant**

$$g_i \oplus e_i = v_i$$

$$k_i + \ell_i = \Delta \cdot e_i \pmod{p}$$



$$K_L \quad K_R$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

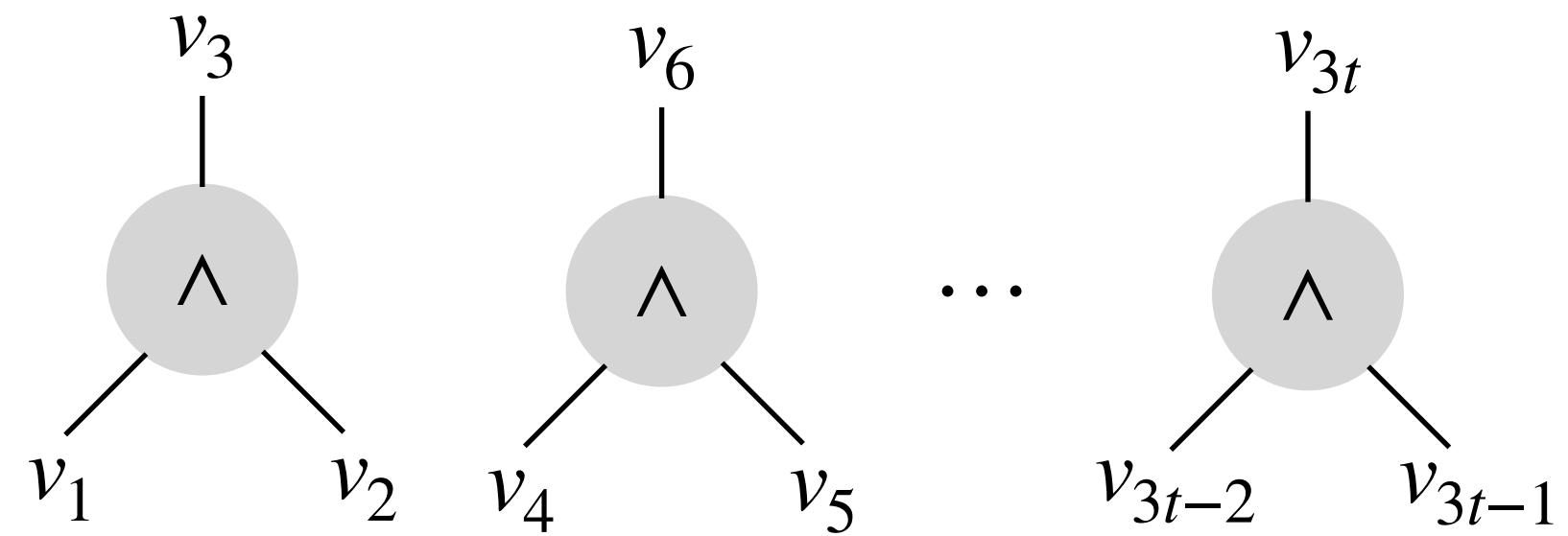
$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

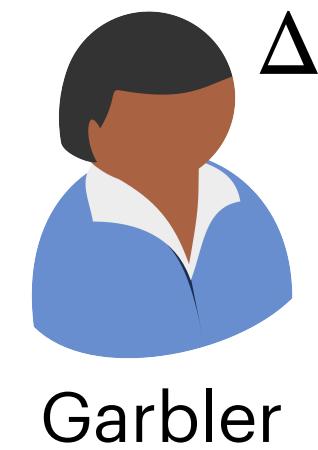
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$K_L \quad K_R$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

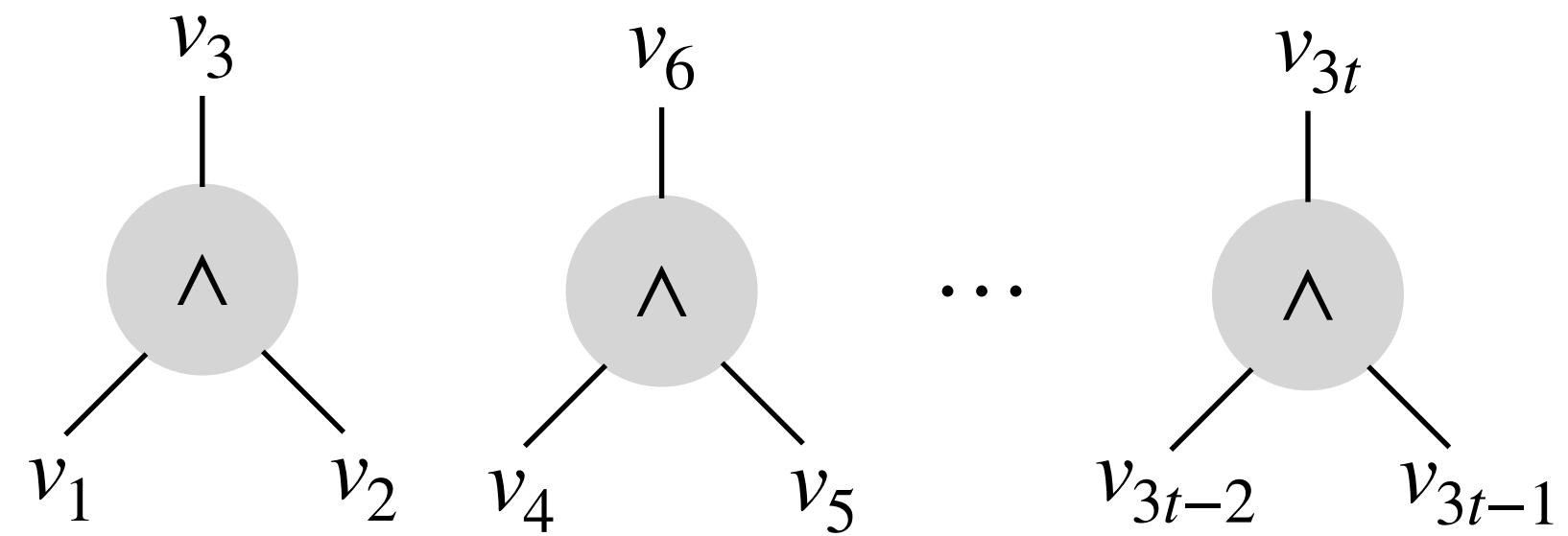
$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

$$K_L \quad K_R$$

$$V = V_1 \cdot V_2 = (G_L + E_L) \cdot (G_R + E_R)$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



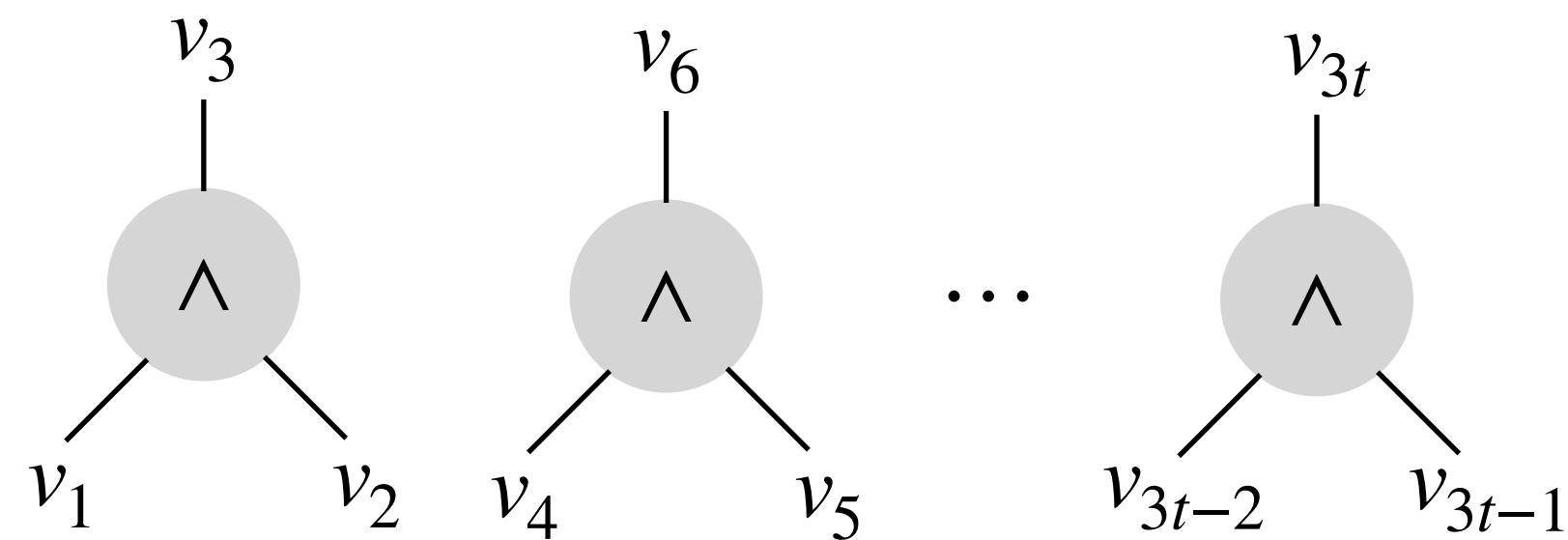
$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

$$K_L \quad K_R$$



**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

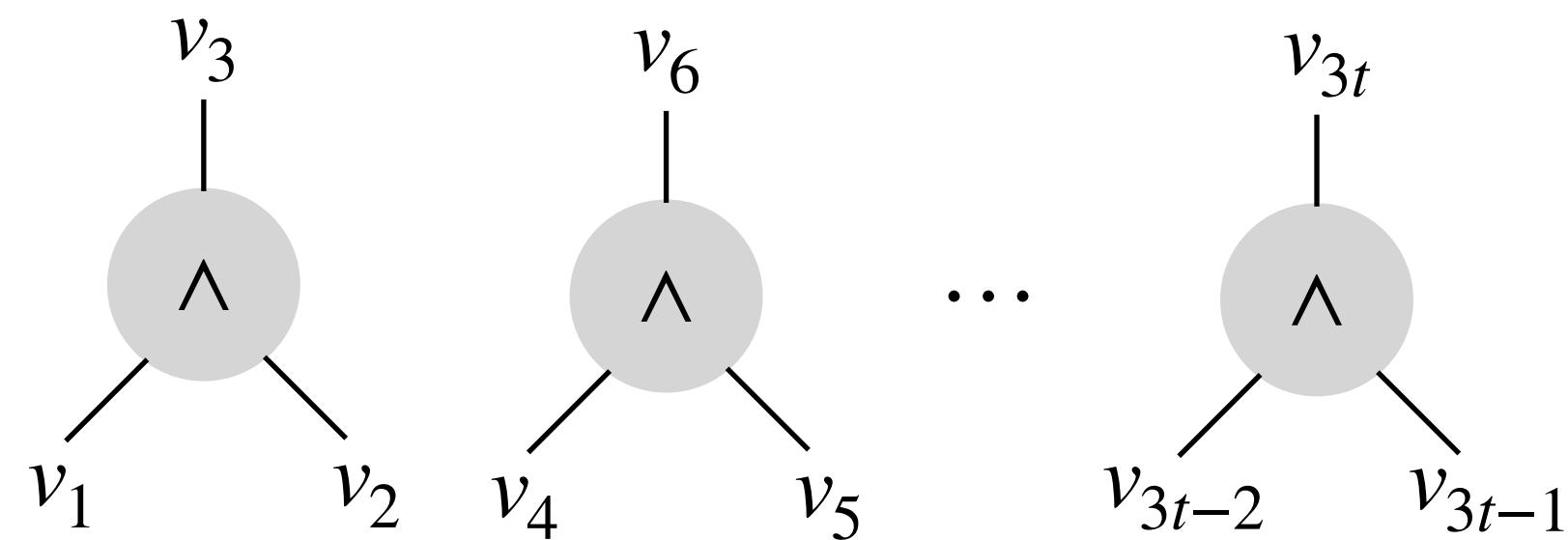
$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

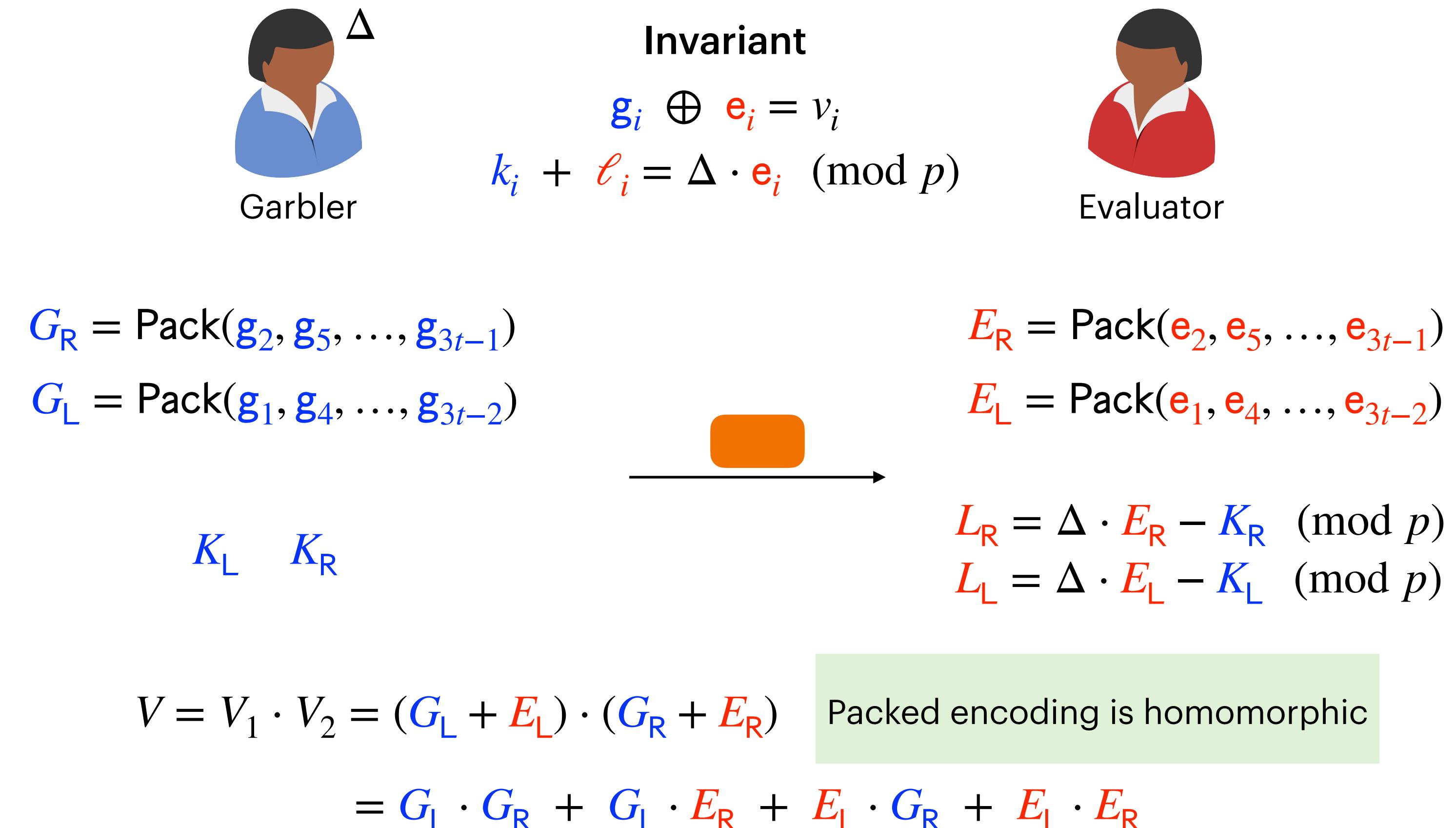
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

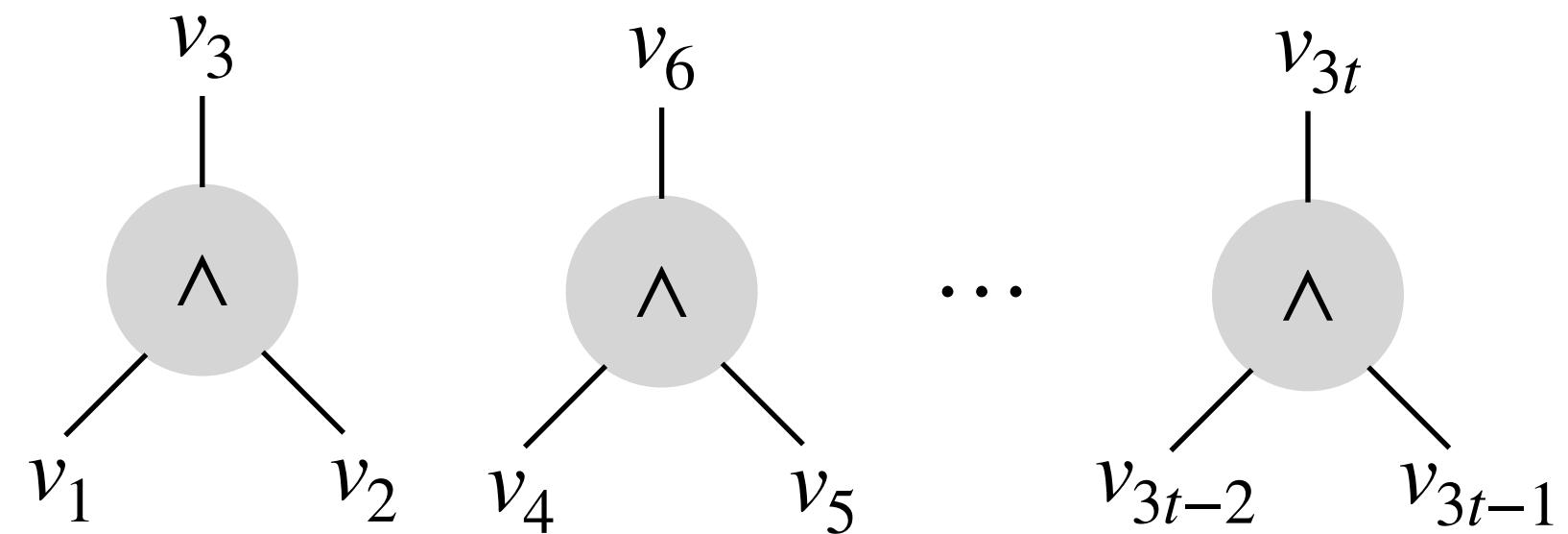
$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

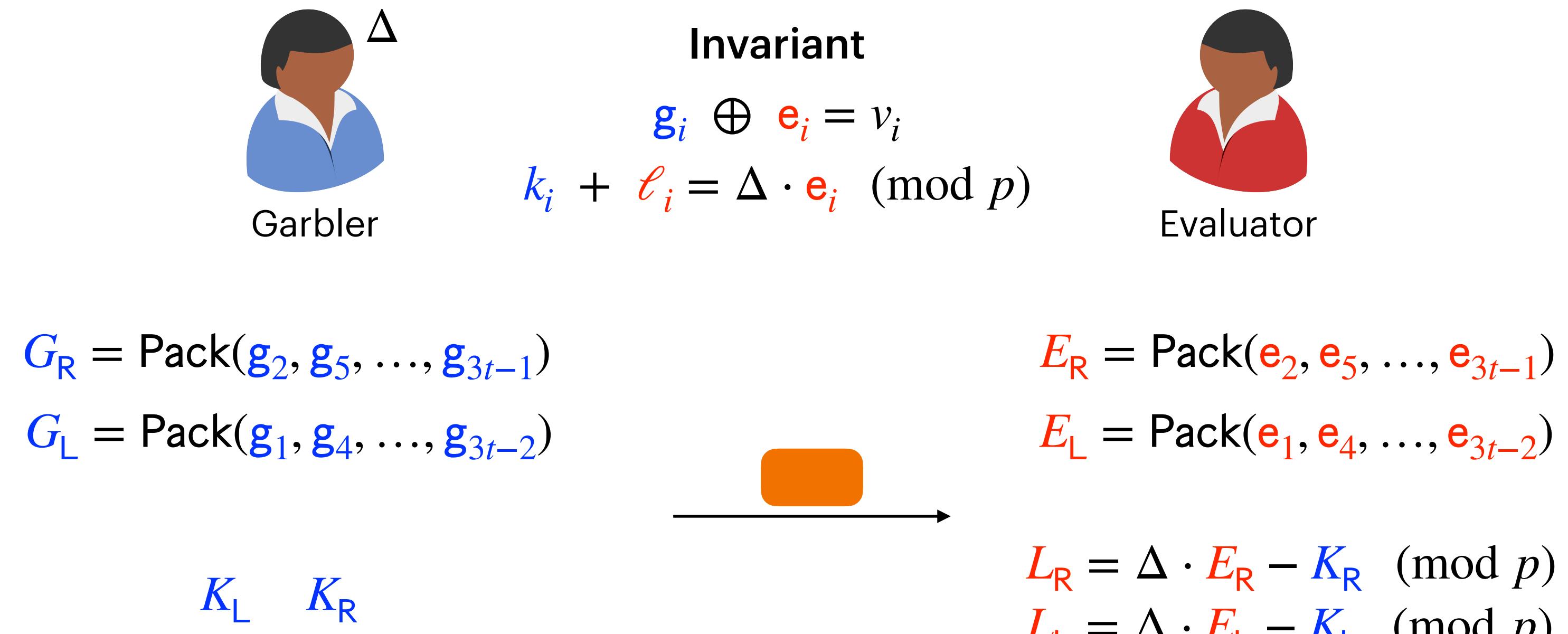
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

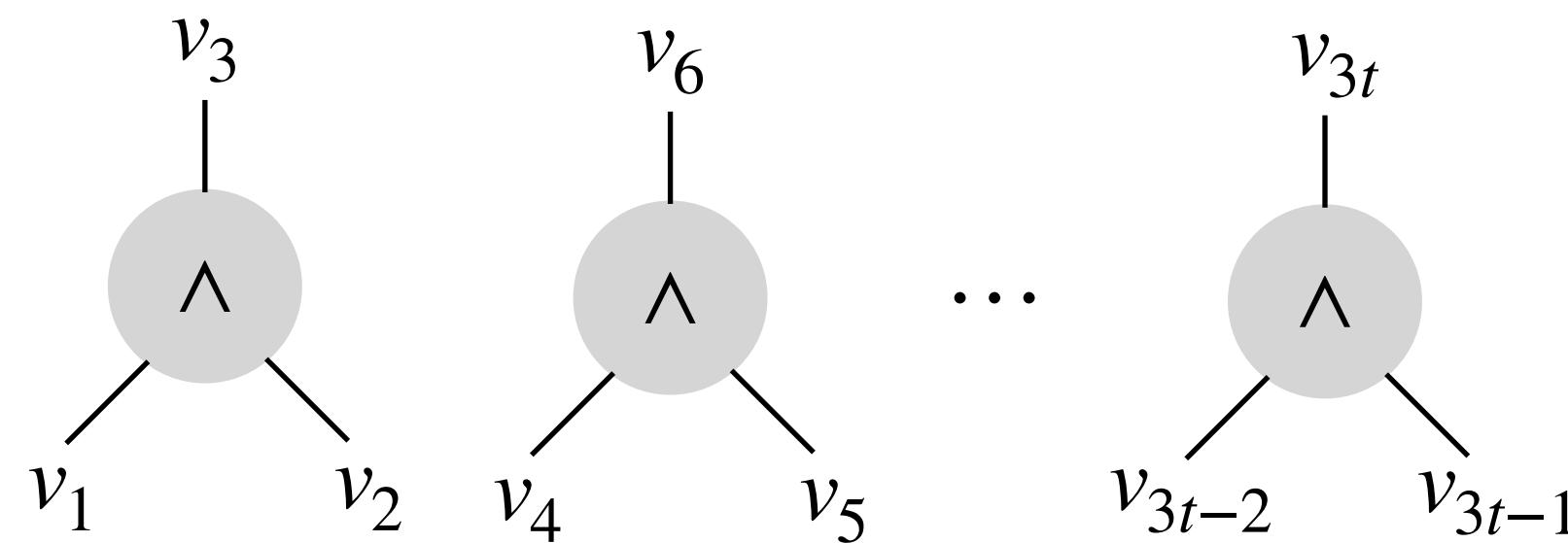
$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

$$K_L \quad K_R$$

$$V = V_1 \cdot V_2 = (G_L + E_L) \cdot (G_R + E_R)$$

$$= G_L \cdot G_R + G_L \cdot E_R + E_L \cdot G_R + E_L \cdot E_R$$

Locally computed by  
Garbler

## Invariant

$$g_i \oplus e_i = v_i$$

$$k_i + \ell_i = \Delta \cdot e_i \pmod{p}$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

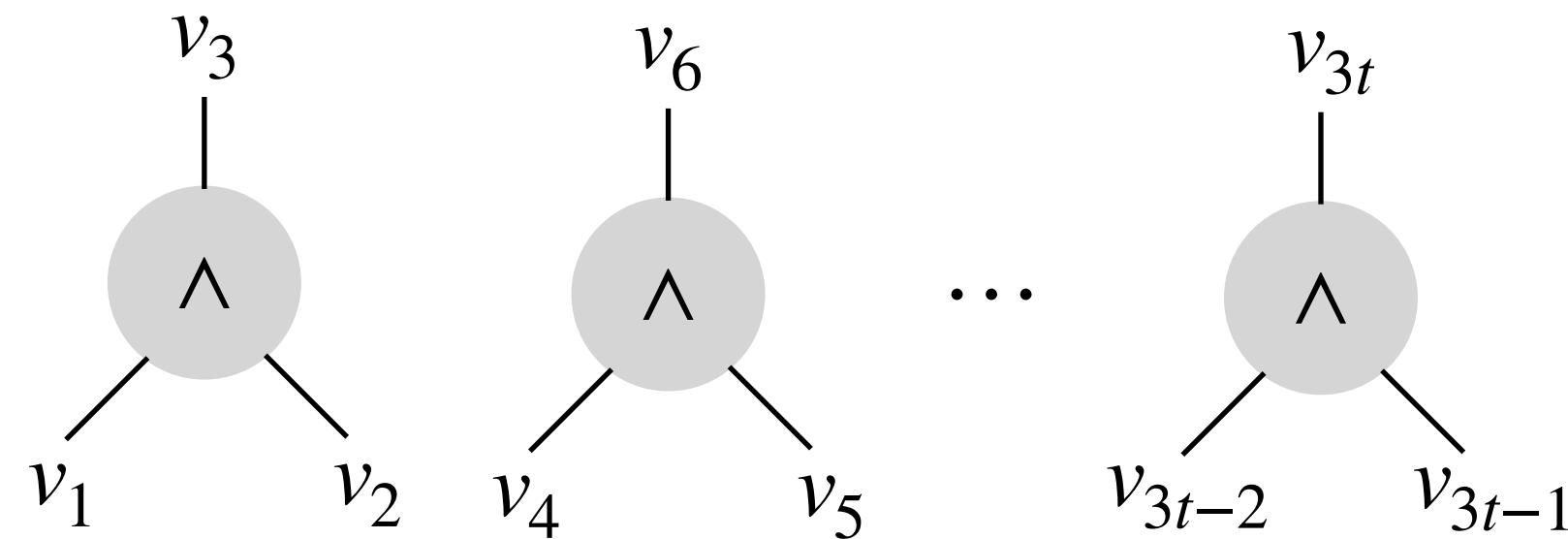
$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

Packed encoding is homomorphic

Use multiplication  
gadget

Locally computed by  
Evaluator

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

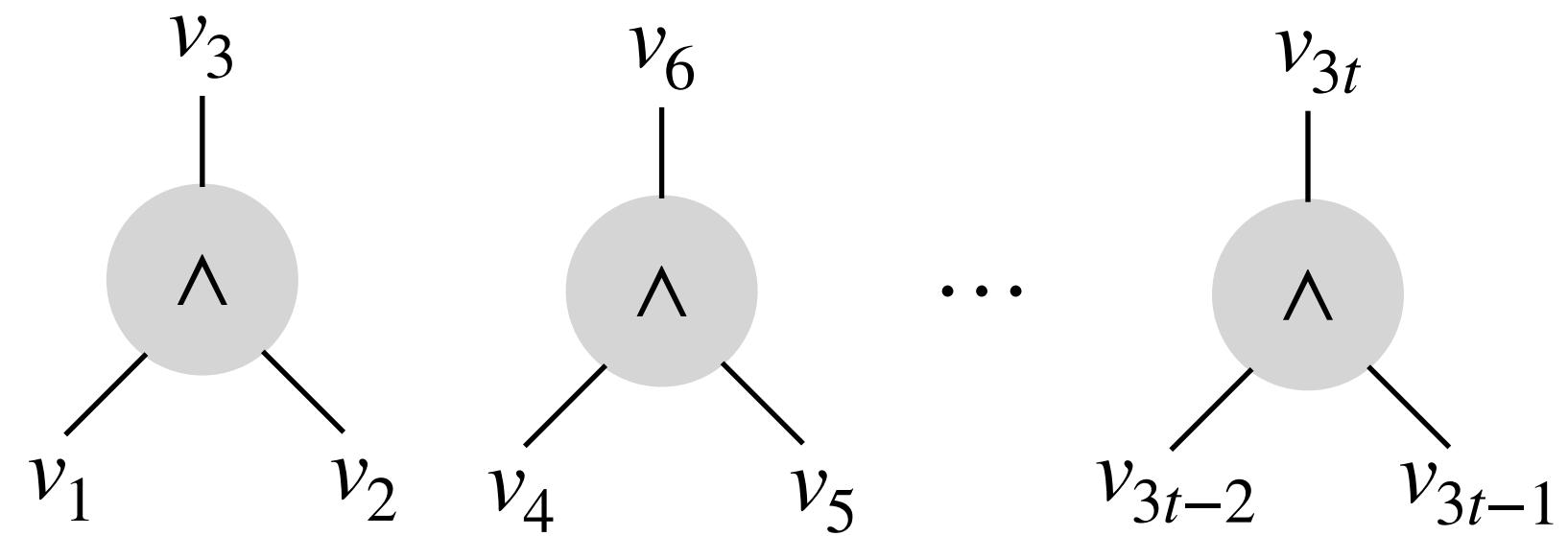
$$K_L \quad K_R$$

$$V = V_1 \cdot V_2 = (G_L + E_L) \cdot (G_R + E_R)$$

$$= G_L \cdot G_R + G_L \cdot E_R + E_L \cdot G_R + E_L \cdot E_R$$

Use multiplication  
gadget

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &\equiv \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$K_L \quad K_R$$

$$G$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

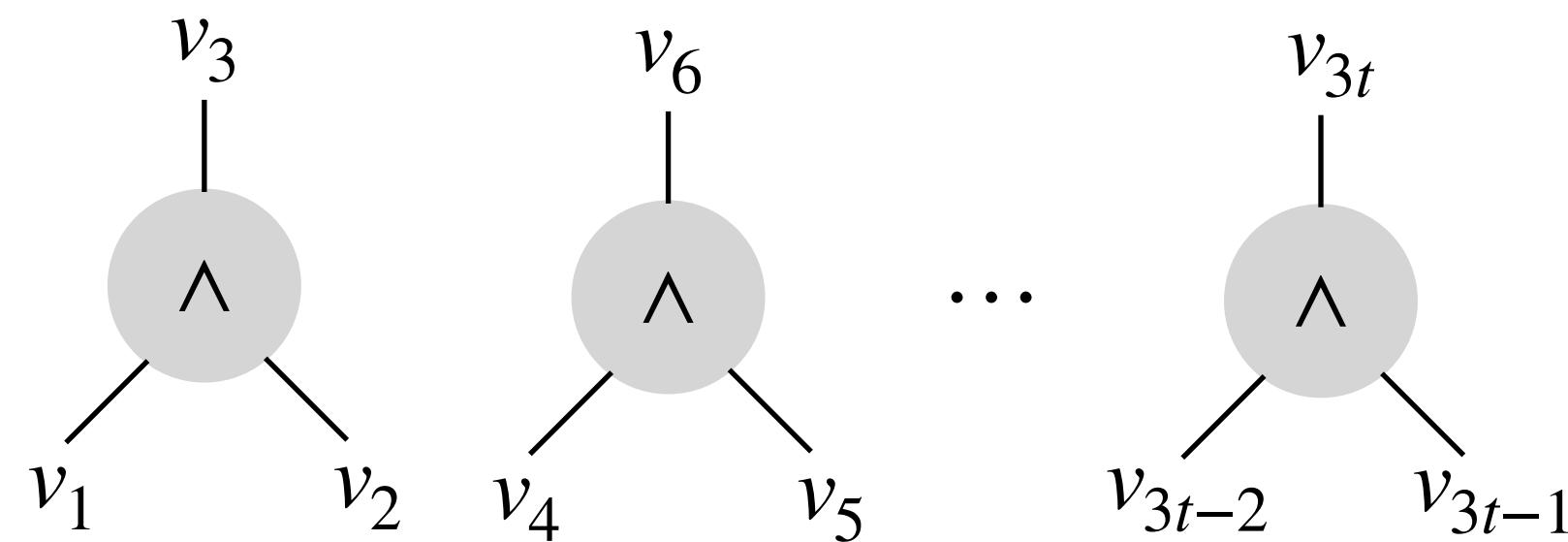
$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

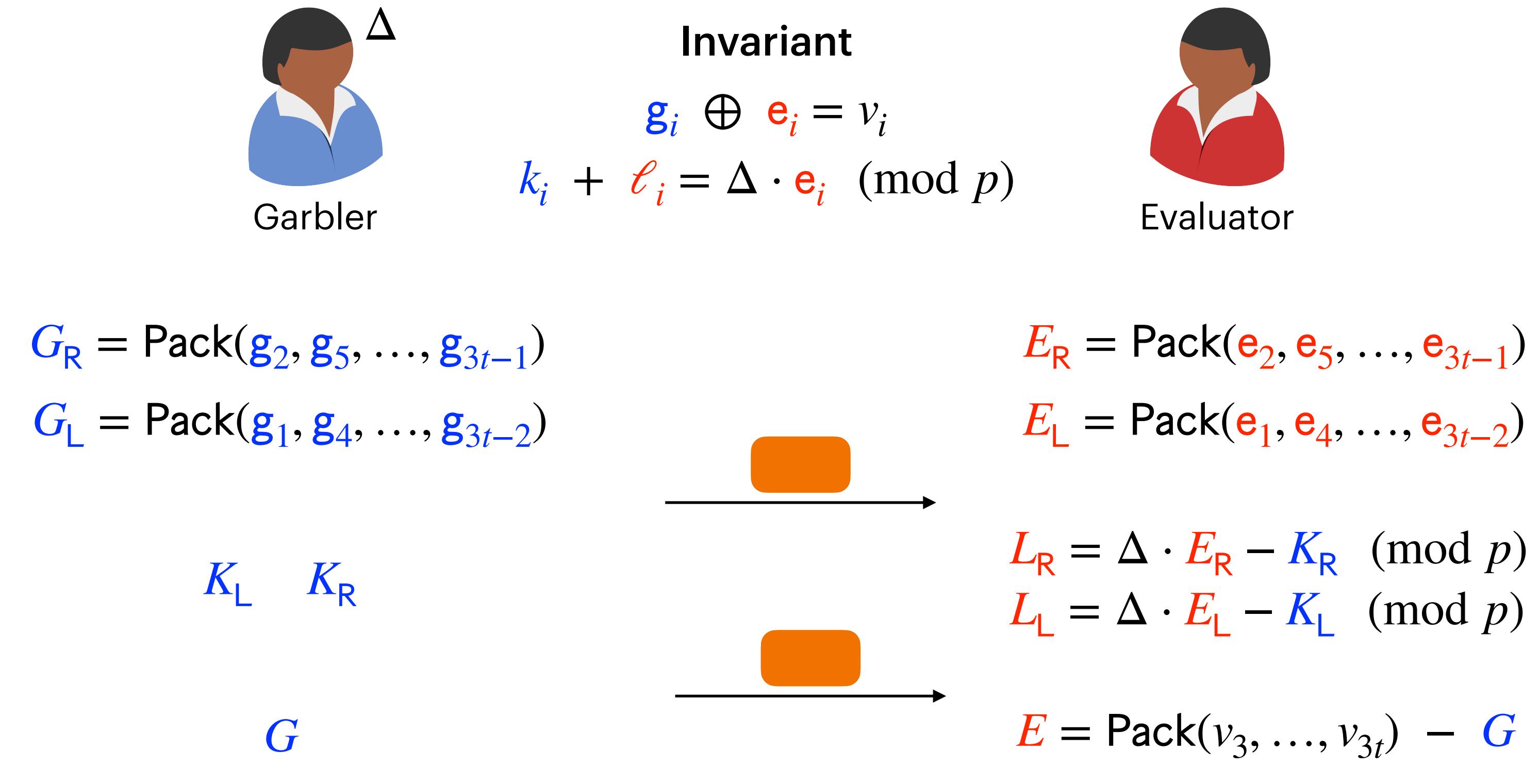
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

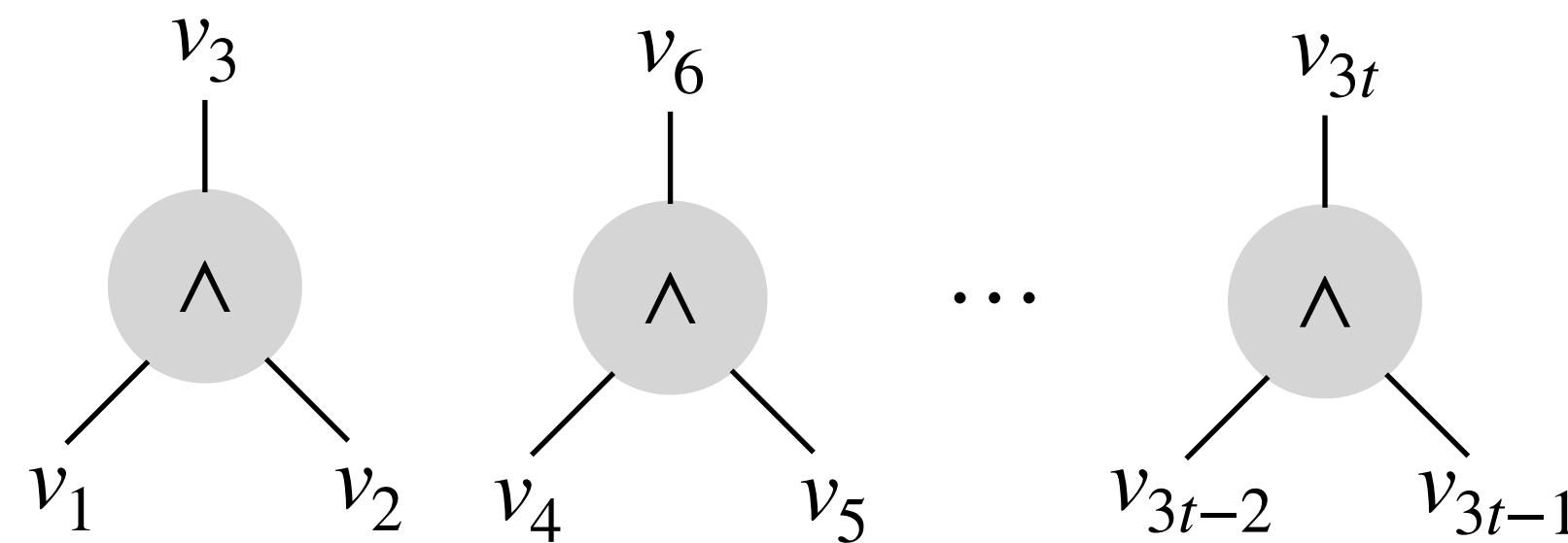
## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



Technically involved but transform and multiply gadget suffices for computing shares of  $\Delta \cdot E$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

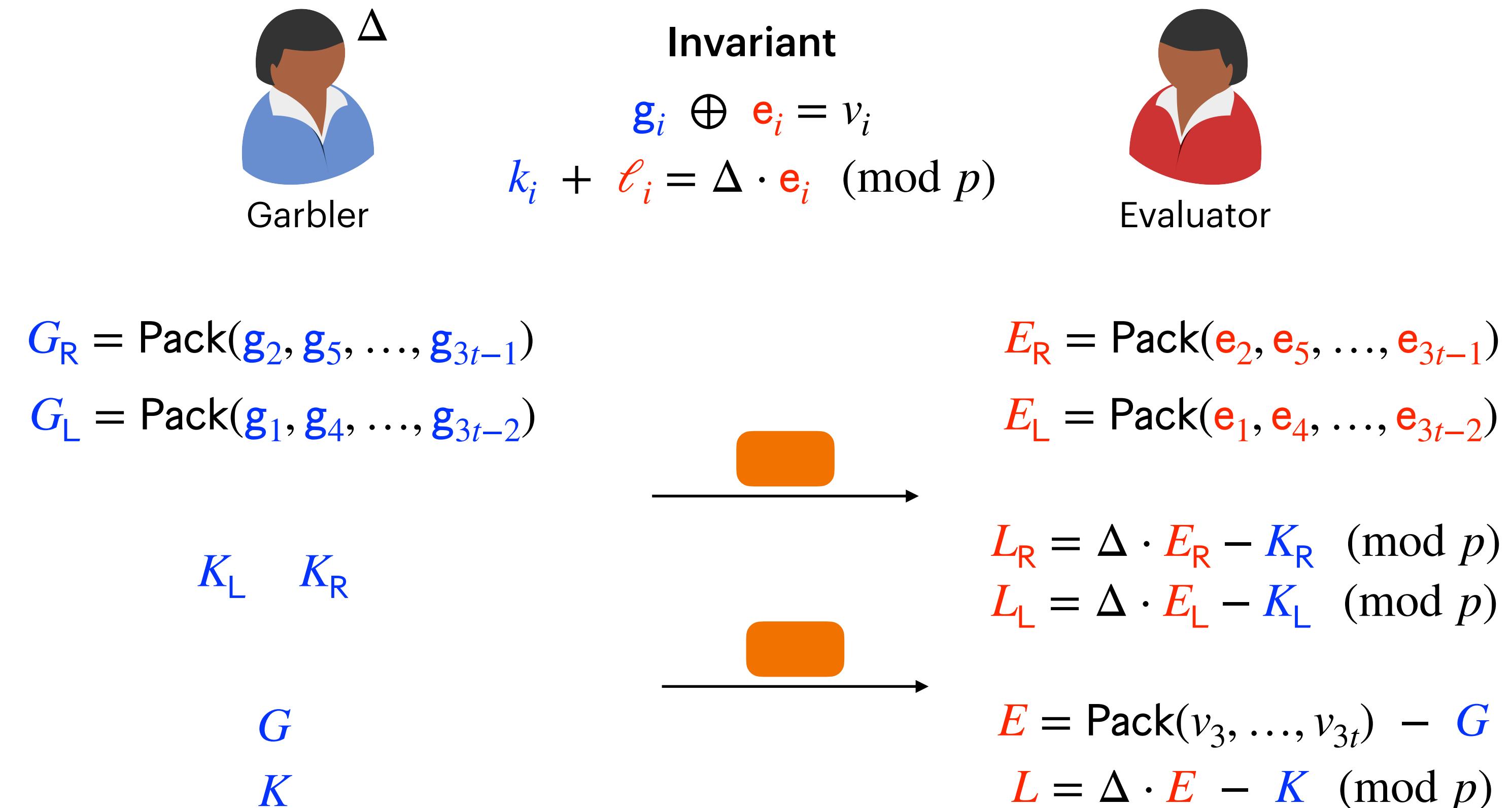
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

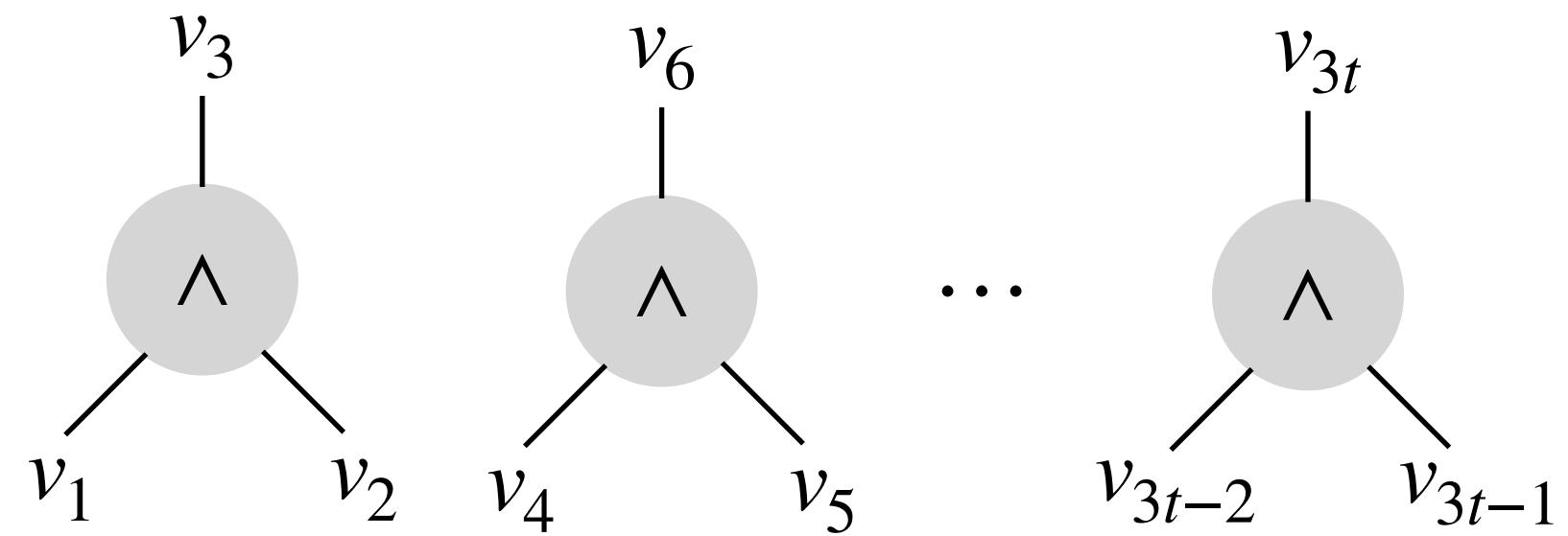
## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



Technically involved but transform and multiply gadget suffices for computing shares of  $\Delta \cdot E$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

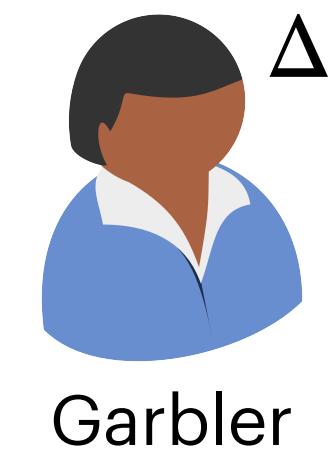
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

$$K_L \quad K_R$$

$$G \\ K$$

$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

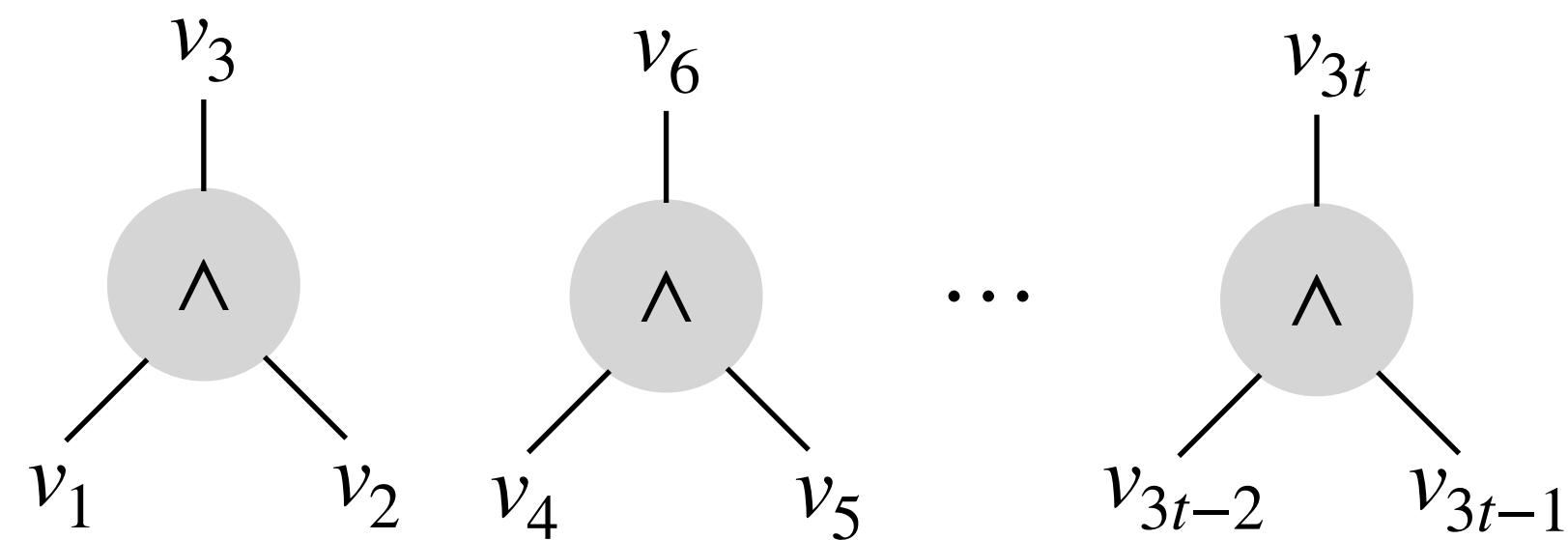
$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

$$K_L \quad K_R$$

$$G \\ K$$

$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$



## Invariant

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

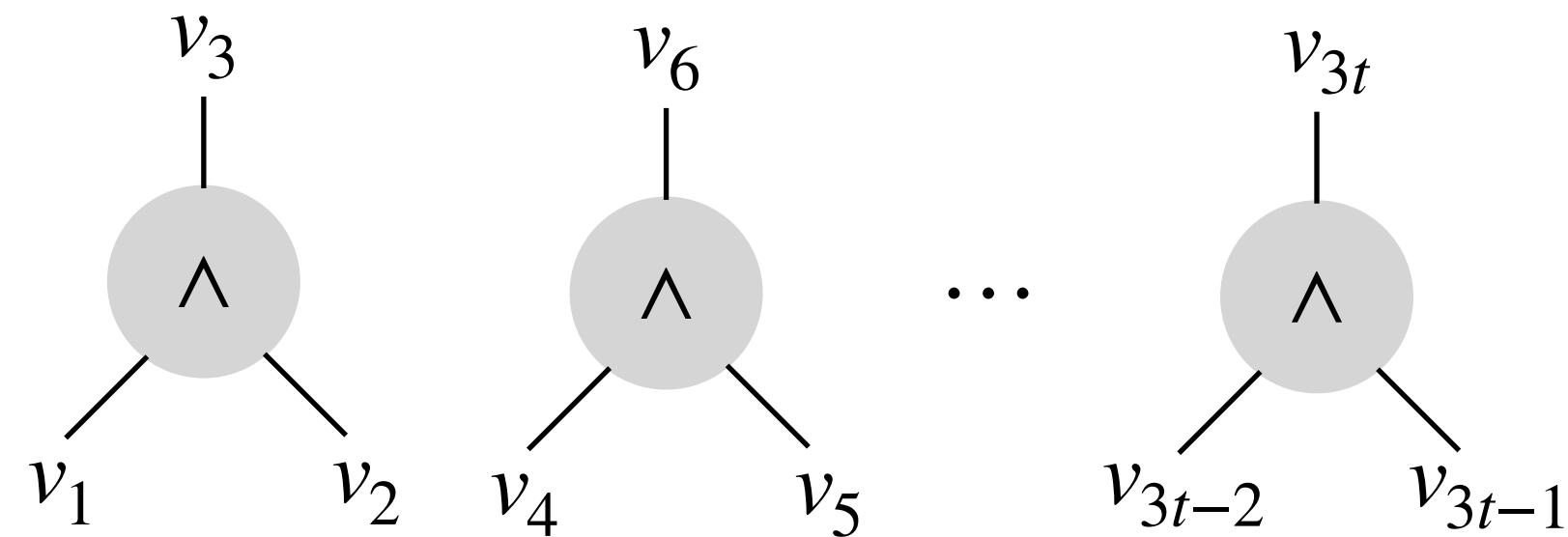
$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$



# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

$$K_L \quad K_R$$

$$G \\ K$$

$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$

**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

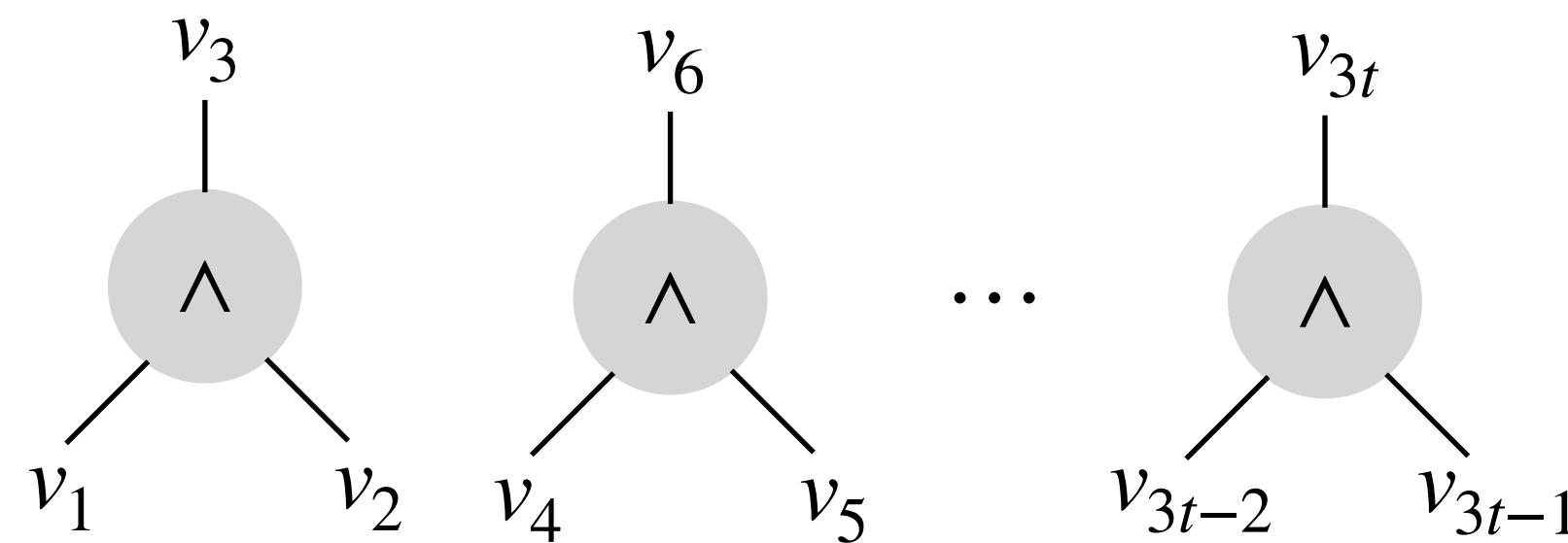
$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$

UnPack is  $\mathbb{F}_2$ -linear

$$(e_3, e_6, \dots, e_{3t}) = \text{UnPack}(E)$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

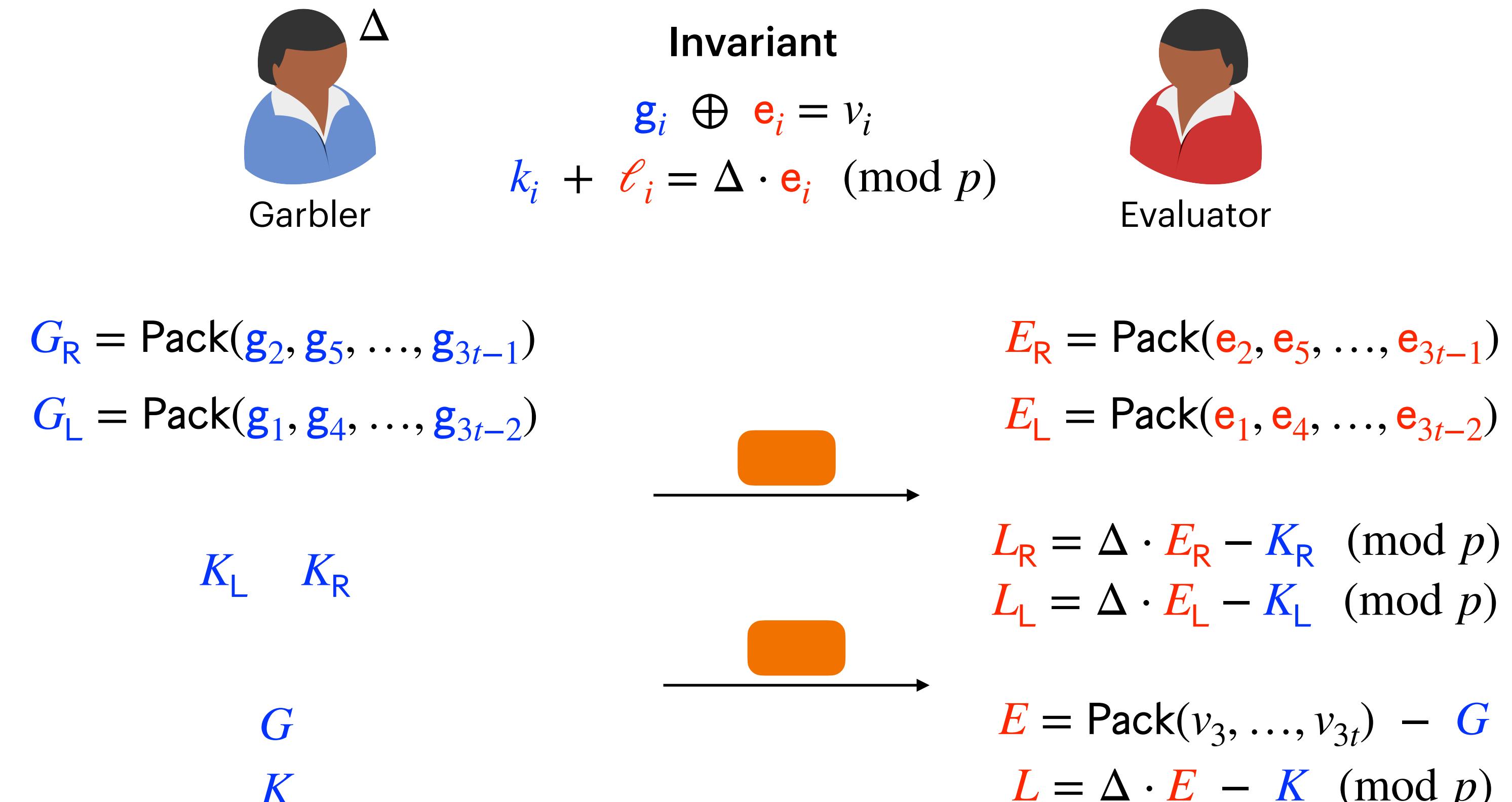
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



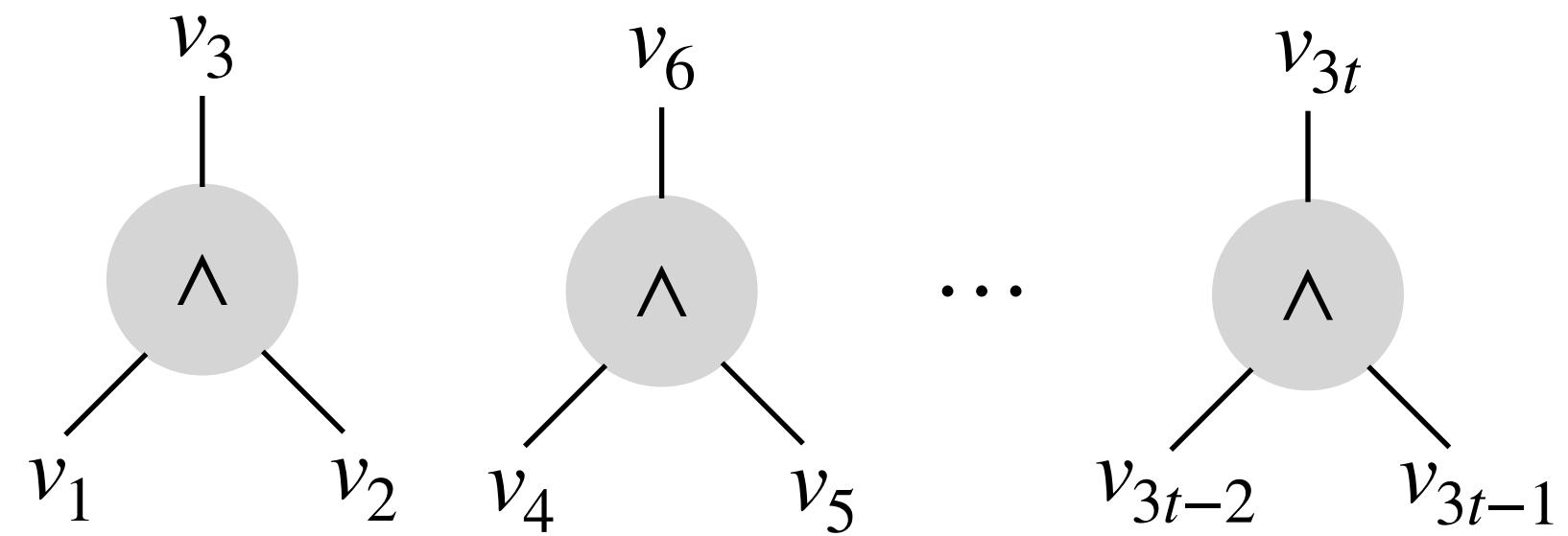
$$(\mathbf{g}_3, \mathbf{g}_6, \dots, \mathbf{g}_{3t}) = \text{UnPack}(G)$$

UnPack is  $\mathbb{F}_2$ -linear

$$(\mathbf{e}_3, \mathbf{e}_6, \dots, \mathbf{e}_{3t}) = \text{UnPack}(E)$$

$(K, L)$  are shares over  $\mathbb{Z}_p \implies$  Can't use UnPack directly

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

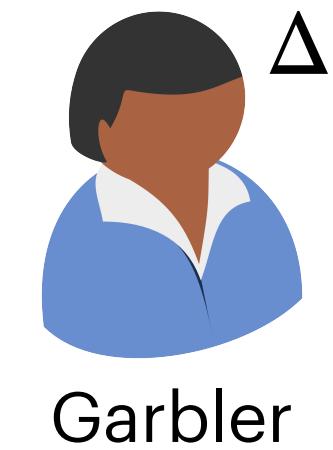
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



**Invariant**

$$\mathbf{g}_i \oplus \mathbf{e}_i = v_i$$

$$k_i + \ell_i = \Delta \cdot \mathbf{e}_i \pmod{p}$$



$G$   
 $K$

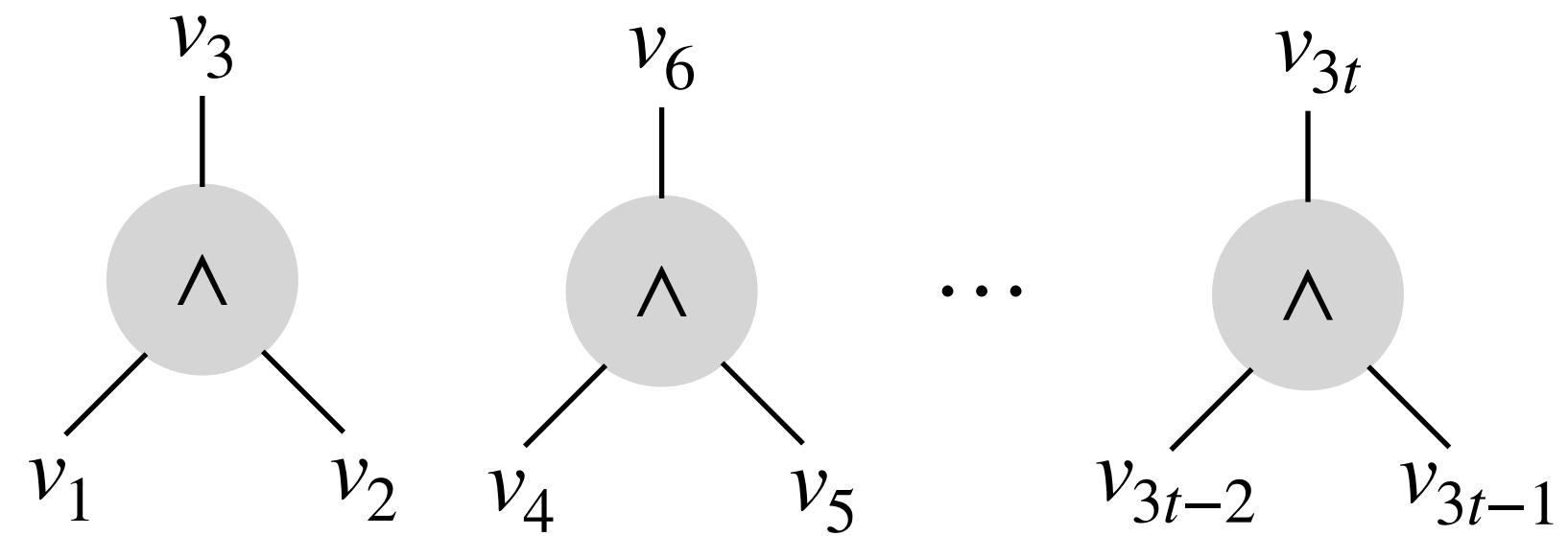
$$(\mathbf{g}_3, \mathbf{g}_6, \dots, \mathbf{g}_{3t}) = \text{UnPack}(G)$$

$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$

$$(\mathbf{e}_3, \mathbf{e}_6, \dots, \mathbf{e}_{3t}) = \text{UnPack}(E)$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\mathbf{g}_i \oplus \mathbf{e}_i = v_i$$

$$k_i + \ell_i = \Delta \cdot \mathbf{e}_i \pmod{p}$$



$G$   
 $K$

$$(\mathbf{g}_3, \mathbf{g}_6, \dots, \mathbf{g}_{3t}) = \text{UnPack}(G)$$

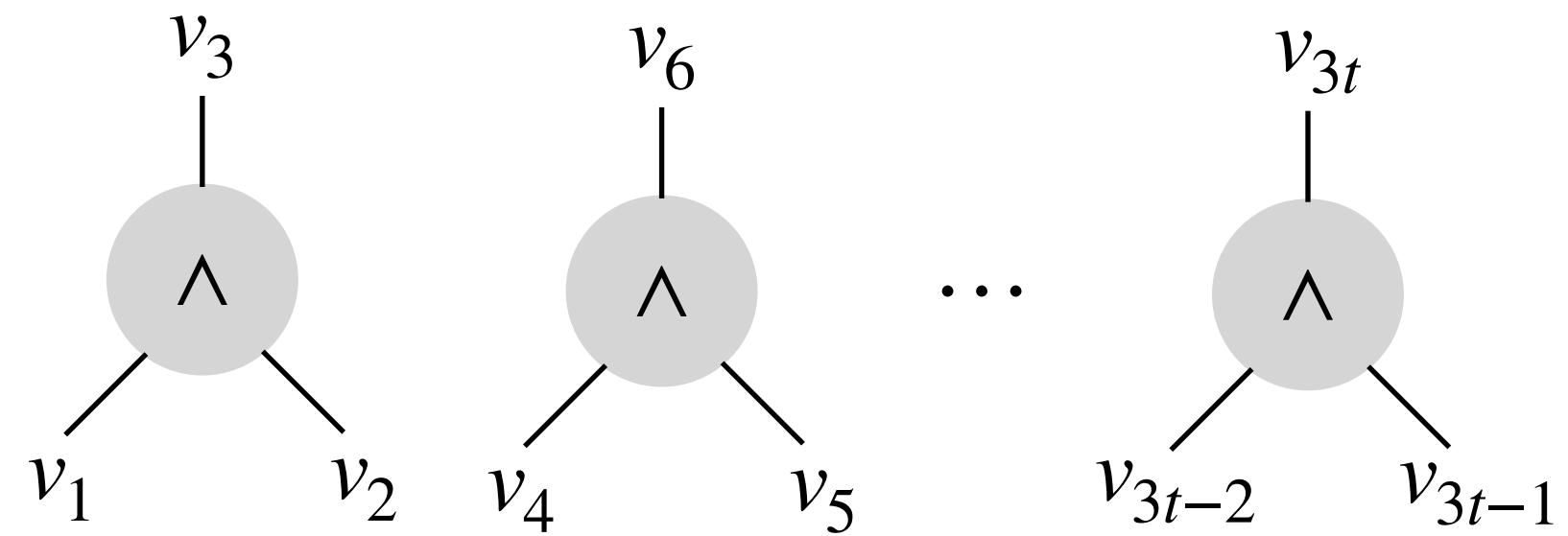
$$\begin{aligned} E &= \text{Pack}(v_3, \dots, v_{3t}) - G \\ L &= \Delta \cdot E - K \pmod{p} \end{aligned}$$

$$(\mathbf{e}_3, \mathbf{e}_6, \dots, \mathbf{e}_{3t}) = \text{UnPack}(E)$$

$K \rightarrow$  Transform and Multiply  
Gadget  
 $\Delta \rightarrow$

$$\begin{aligned} \leftarrow L &= \Delta \cdot E - K \pmod{p} \\ \leftarrow E & \end{aligned}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



**Invariant**

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$G$   
 $K$

$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$

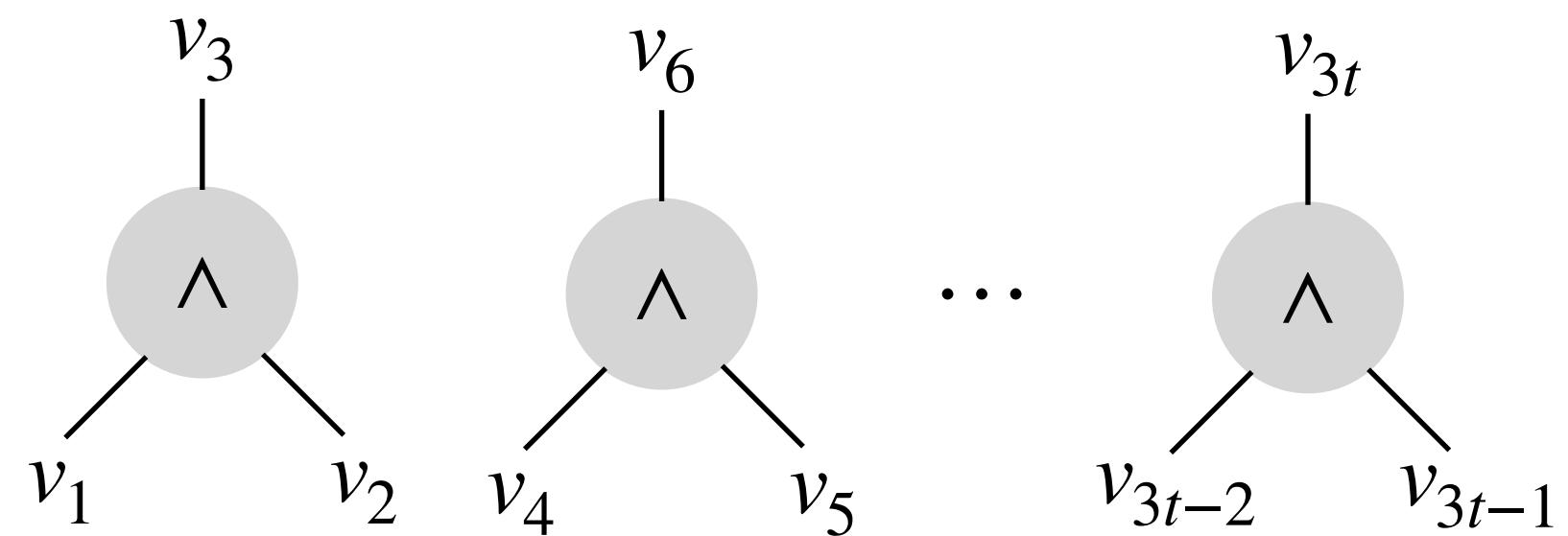
$$\begin{aligned} E &= \text{Pack}(v_3, \dots, v_{3t}) - G \\ L &= \Delta \cdot E - K \pmod{p} \end{aligned}$$

$$(e_3, e_6, \dots, e_{3t}) = \text{UnPack}(E)$$

$K \rightarrow$  Transform and Multiply Gadget  
 $\Delta \rightarrow$   
 $f_i(x) = \text{Index}(i, \text{UnPack}(x))$

$$\begin{aligned} \leftarrow L &= \Delta \cdot E - K \pmod{p} \\ \leftarrow E & \end{aligned}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

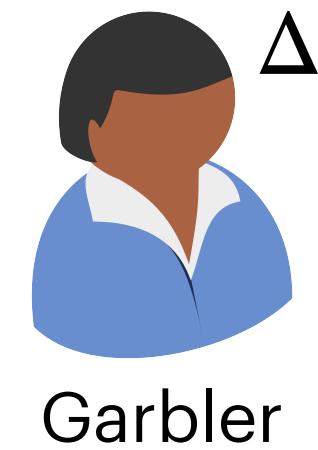
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



$G$   
 $K$

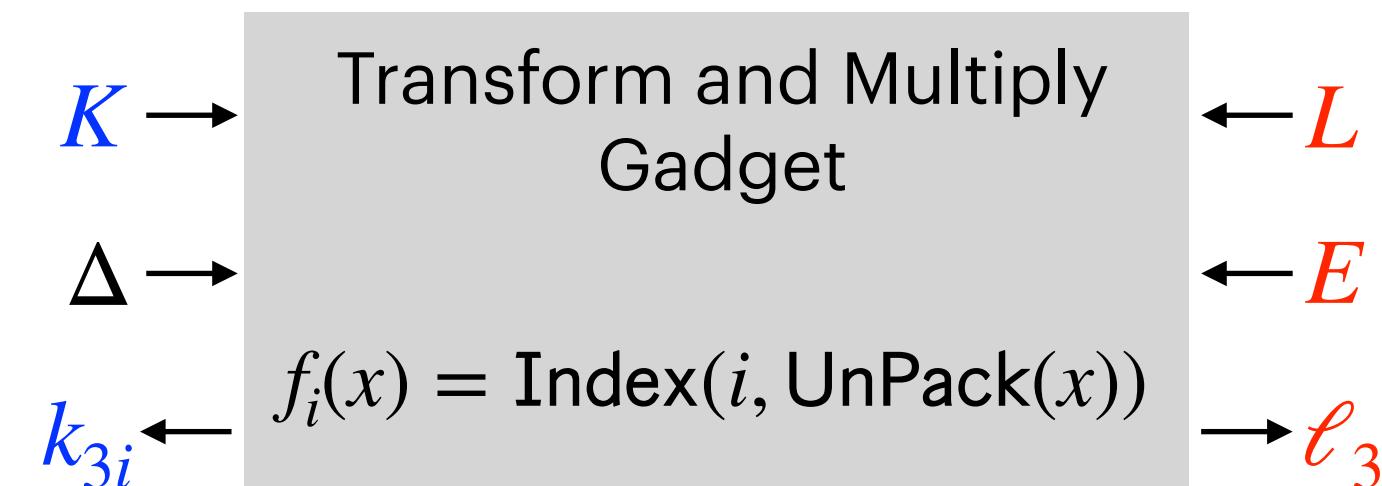
$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$



## Invariant

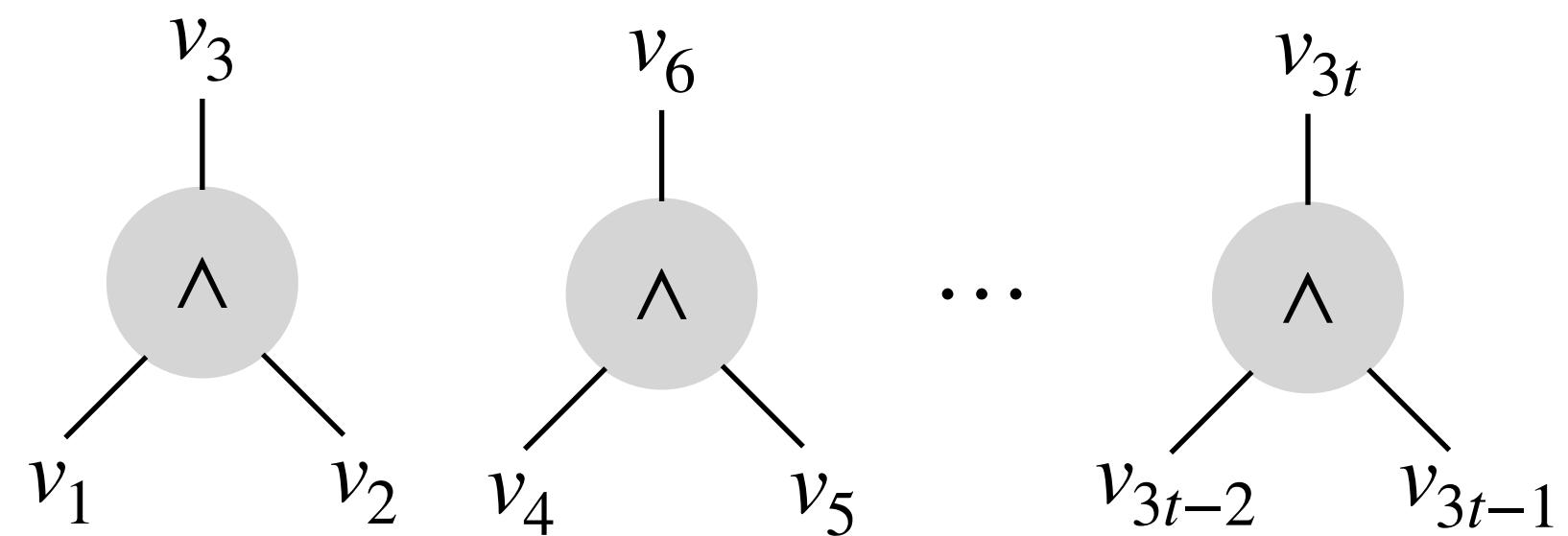
$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$

$$\begin{aligned} E &= \text{Pack}(v_3, \dots, v_{3t}) - G \\ L &= \Delta \cdot E - K \pmod{p} \end{aligned}$$



$$\begin{aligned} k_{3i} + \ell_{3i} &= \Delta \cdot f_i(E) \\ &= \Delta \cdot e_{3i} \end{aligned}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



**Invariant**

$$\mathbf{g}_i \oplus \mathbf{e}_i = v_i$$

$$k_i + \ell_i = \Delta \cdot \mathbf{e}_i \pmod{p}$$

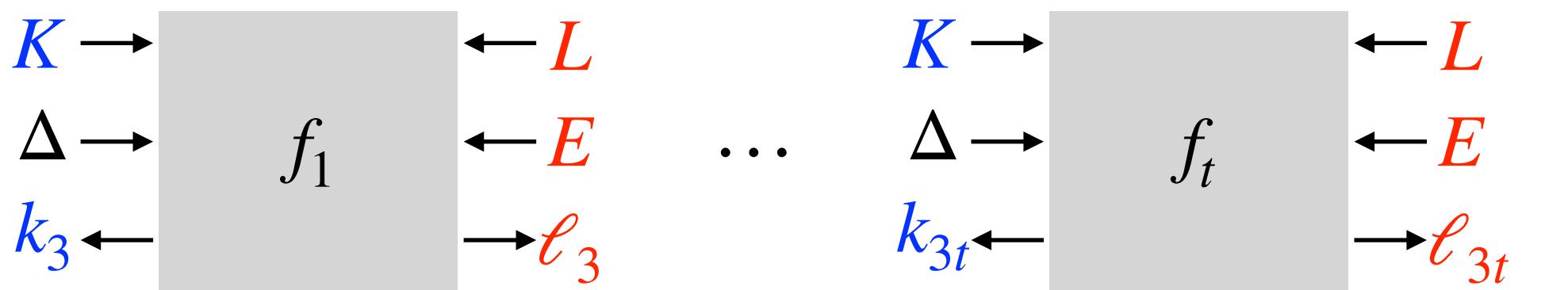


$G$   
 $K$

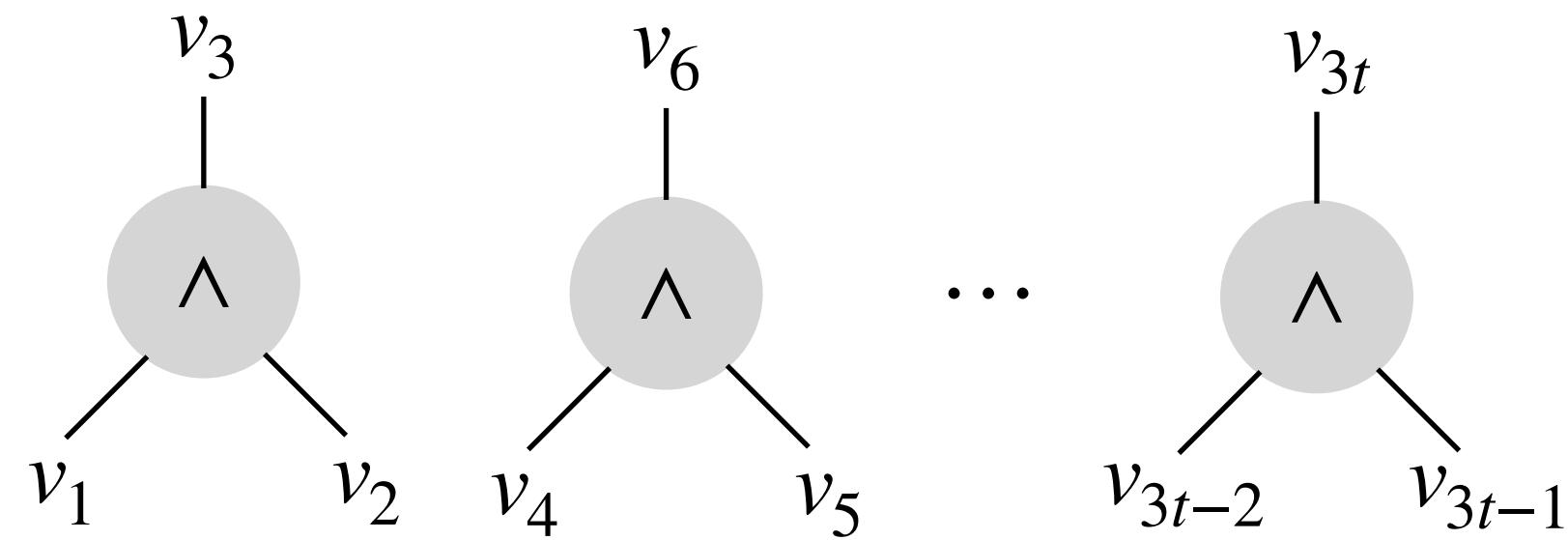
$$(\mathbf{g}_3, \mathbf{g}_6, \dots, \mathbf{g}_{3t}) = \text{UnPack}(G)$$

$$\begin{aligned} E &= \text{Pack}(v_3, \dots, v_{3t}) - G \\ L &= \Delta \cdot E - K \pmod{p} \end{aligned}$$

$$(\mathbf{e}_3, \mathbf{e}_6, \dots, \mathbf{e}_{3t}) = \text{UnPack}(E)$$



# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$



### Invariant

$$\mathbf{g}_i \oplus \mathbf{e}_i = v_i$$

$$k_i + \ell_i = \Delta \cdot \mathbf{e}_i \pmod{p}$$



$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$

$$G$$

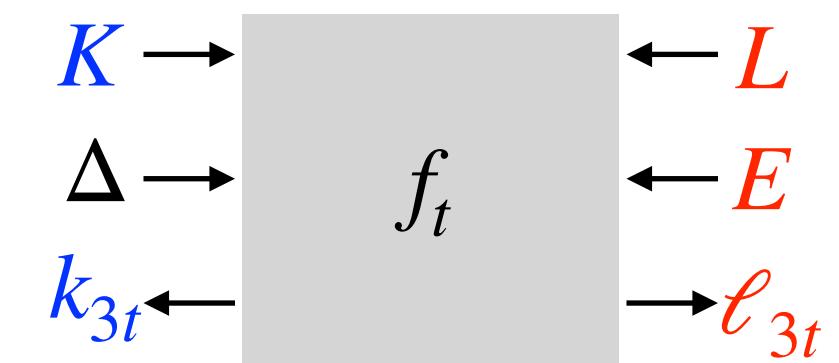
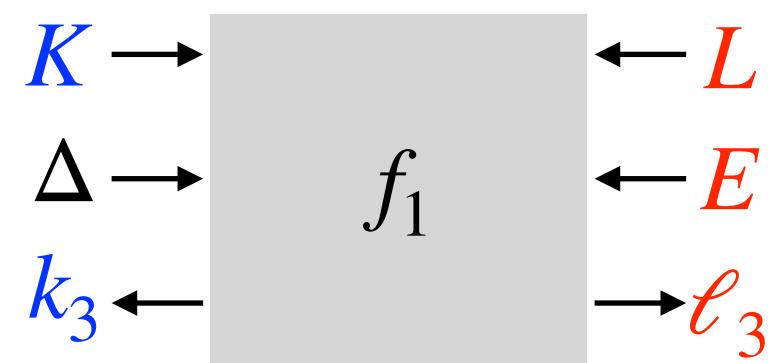
$$K$$

$$(\mathbf{g}_3, \mathbf{g}_6, \dots, \mathbf{g}_{3t}) = \text{UnPack}(G)$$

$$(\mathbf{e}_3, \mathbf{e}_6, \dots, \mathbf{e}_{3t}) = \text{UnPack}(E)$$

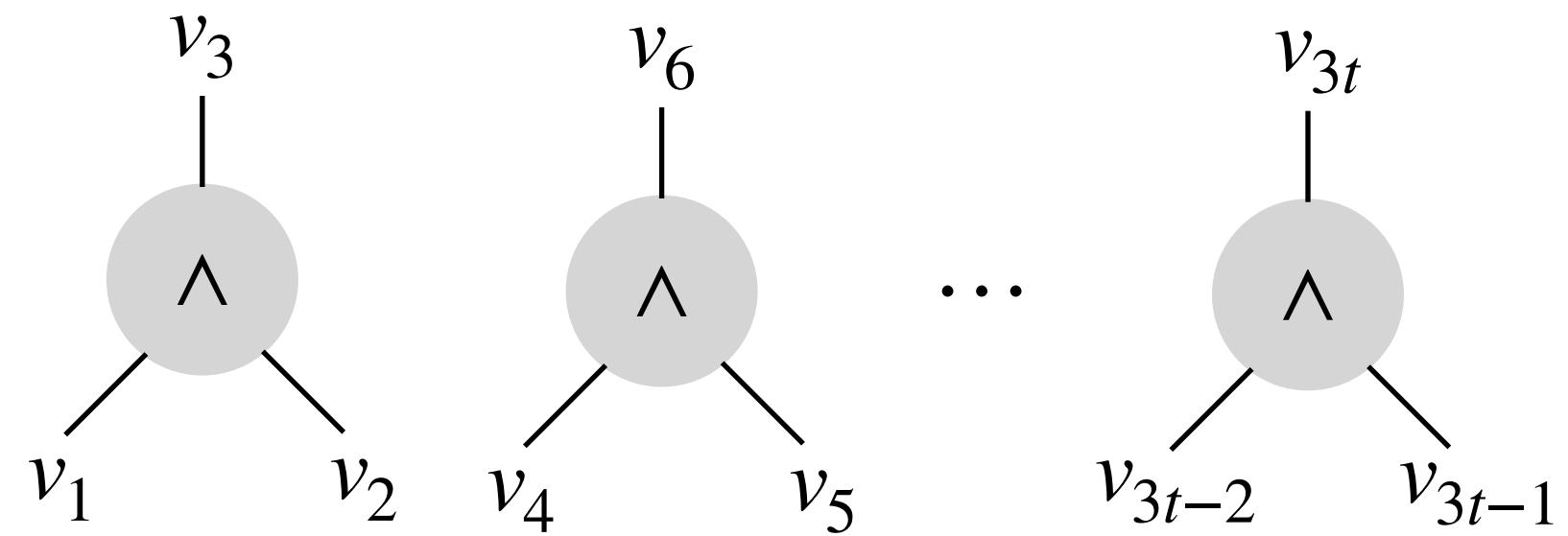
## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



$t$  invocations  $\implies O(\lambda)$ -bit communication per gate

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\mathbf{g}_i \oplus \mathbf{e}_i = v_i$$

$$k_i + \ell_i = \Delta \cdot \mathbf{e}_i \pmod{p}$$

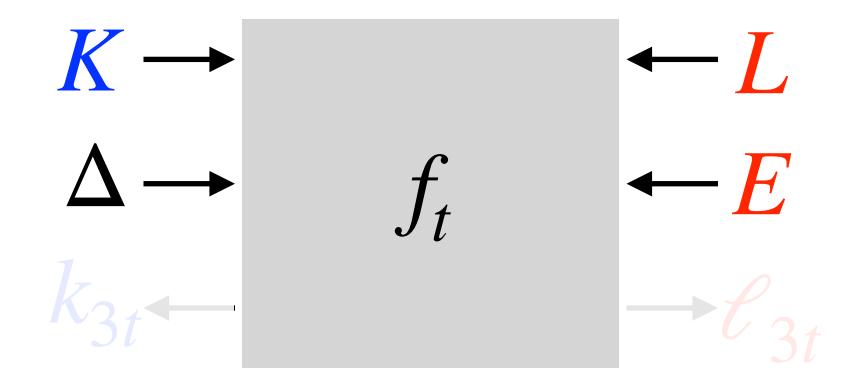
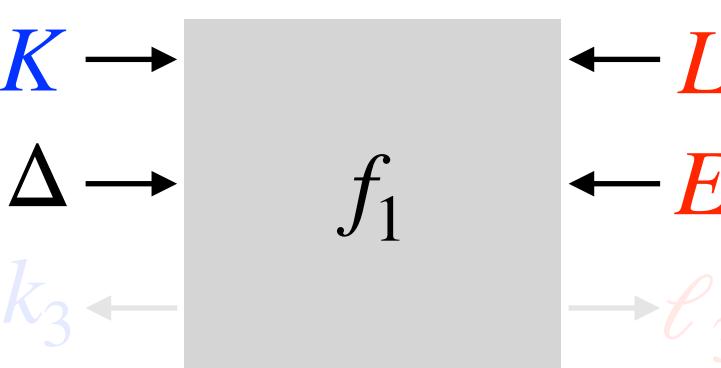


$G$   
 $K$

$$(\mathbf{g}_3, \mathbf{g}_6, \dots, \mathbf{g}_{3t}) = \text{UnPack}(G)$$

$$\begin{aligned} E &= \text{Pack}(v_3, \dots, v_{3t}) - G \\ L &= \Delta \cdot E - K \pmod{p} \end{aligned}$$

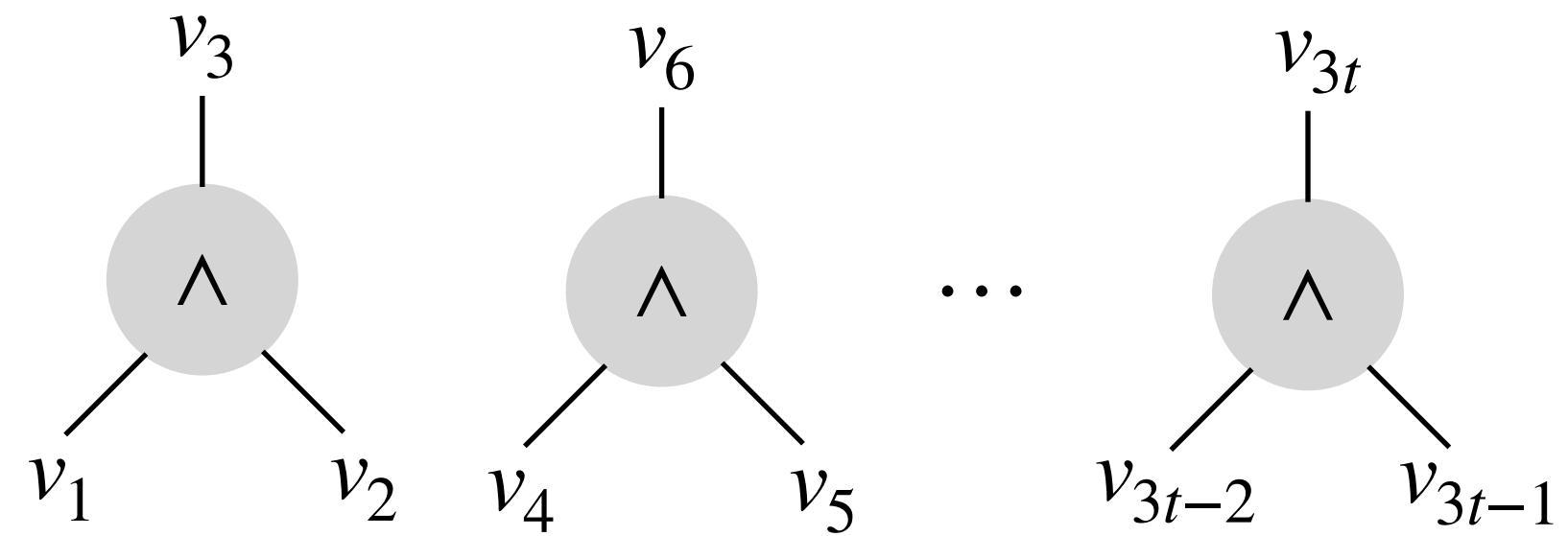
$$(\mathbf{e}_3, \mathbf{e}_6, \dots, \mathbf{e}_{3t}) = \text{UnPack}(E)$$



$t$  invocations  $\implies O(\lambda)$ -bit communication per gate

**Observation:** Different functions on same inputs  $\implies O(\lambda)$  communication across all invocations

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

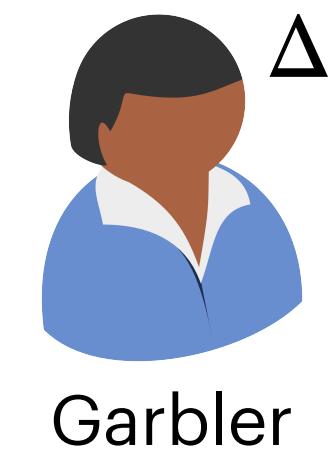
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



### Invariant

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

$$K_L \quad K_R$$

$$G \\ K$$

$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

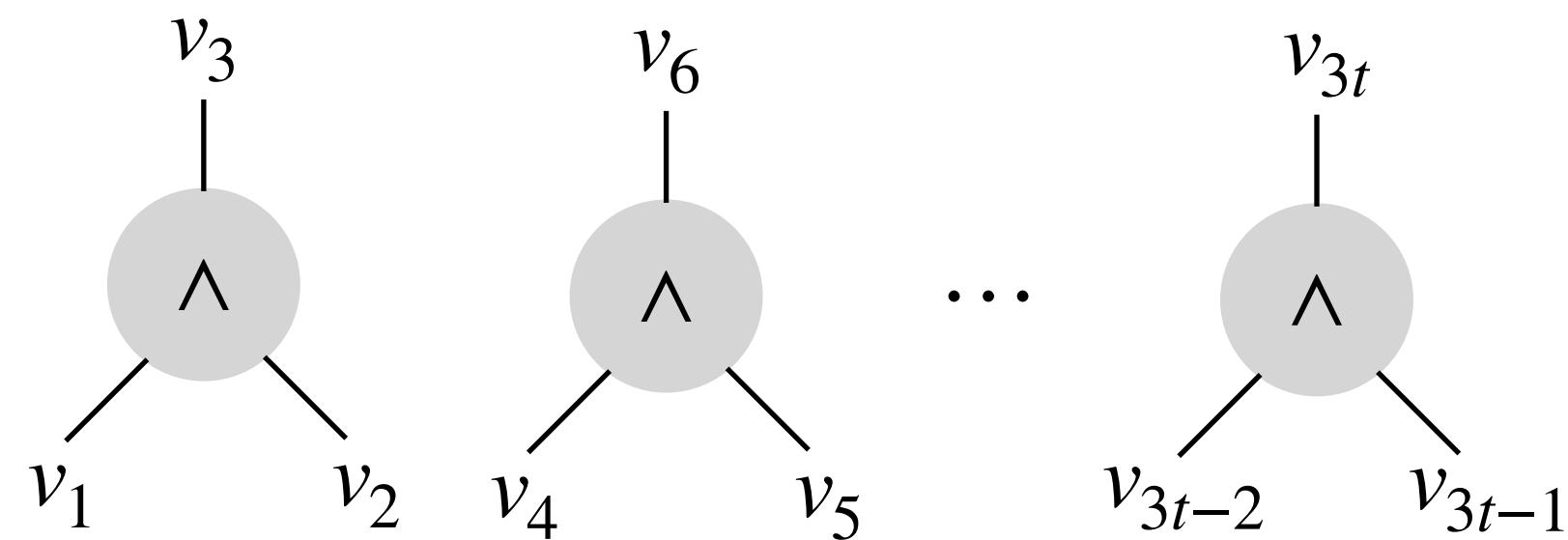
$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

$$K_L \quad K_R$$

$$G \\ K$$

$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$



## Invariant

$$\begin{aligned} g_i \oplus e_i &= v_i \\ k_i + \ell_i &= \Delta \cdot e_i \pmod{p} \end{aligned}$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

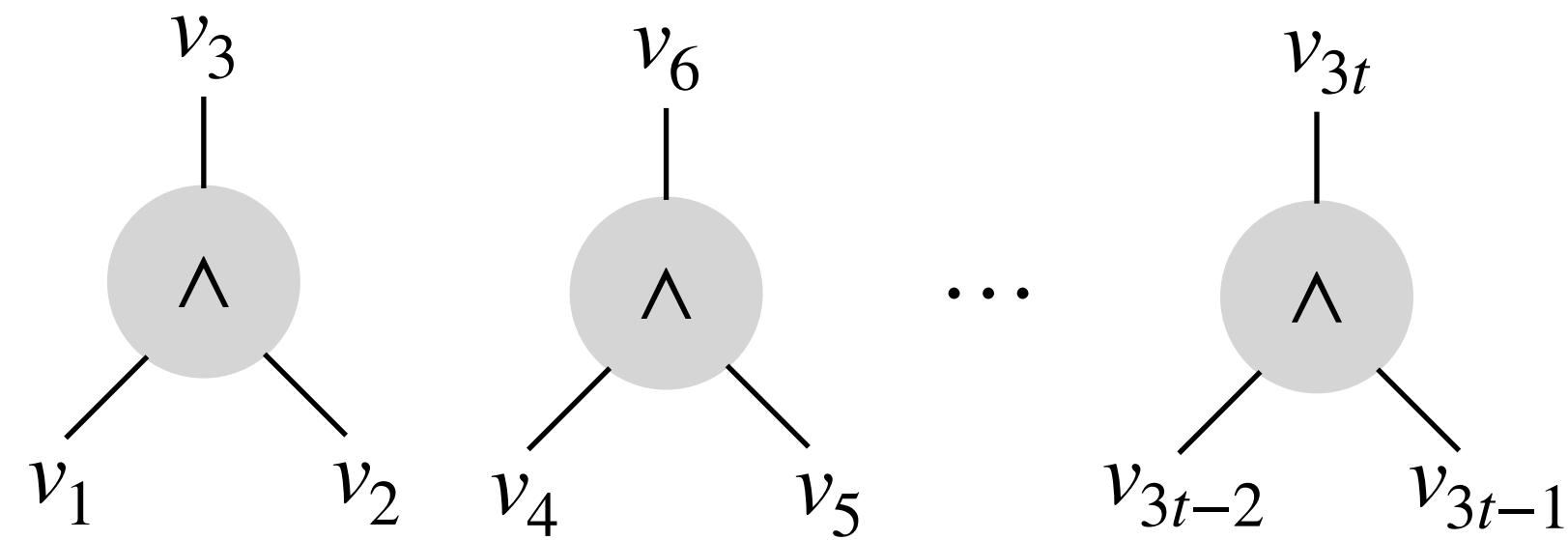
$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$



# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

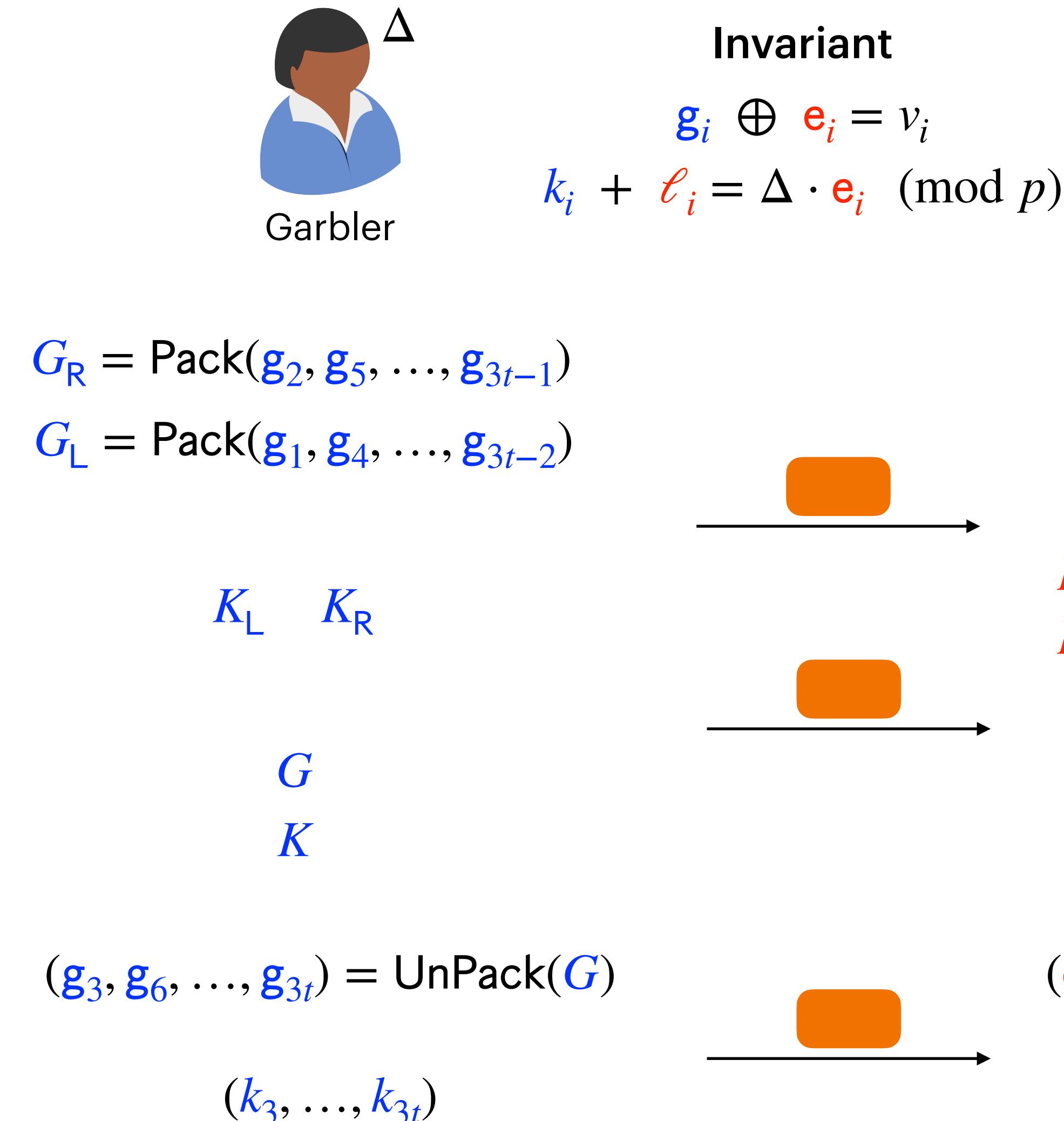
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

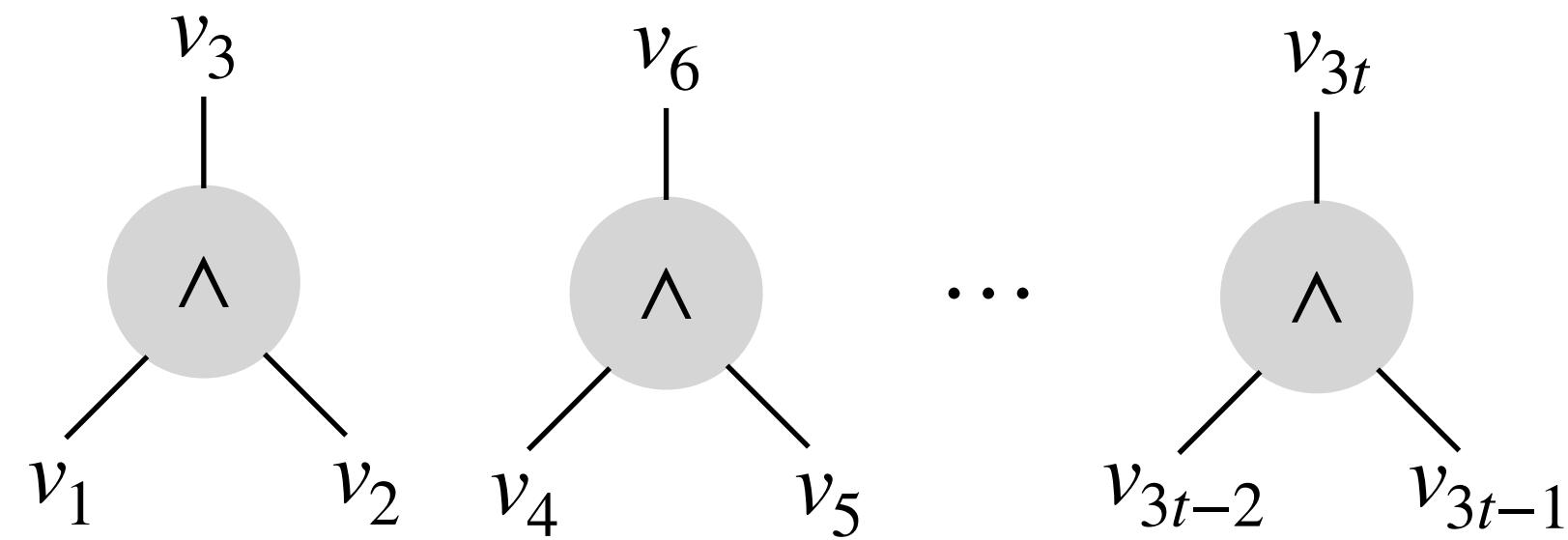
$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



# Template for $\omega(1/\lambda)$ -Rate Garbling



## 1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

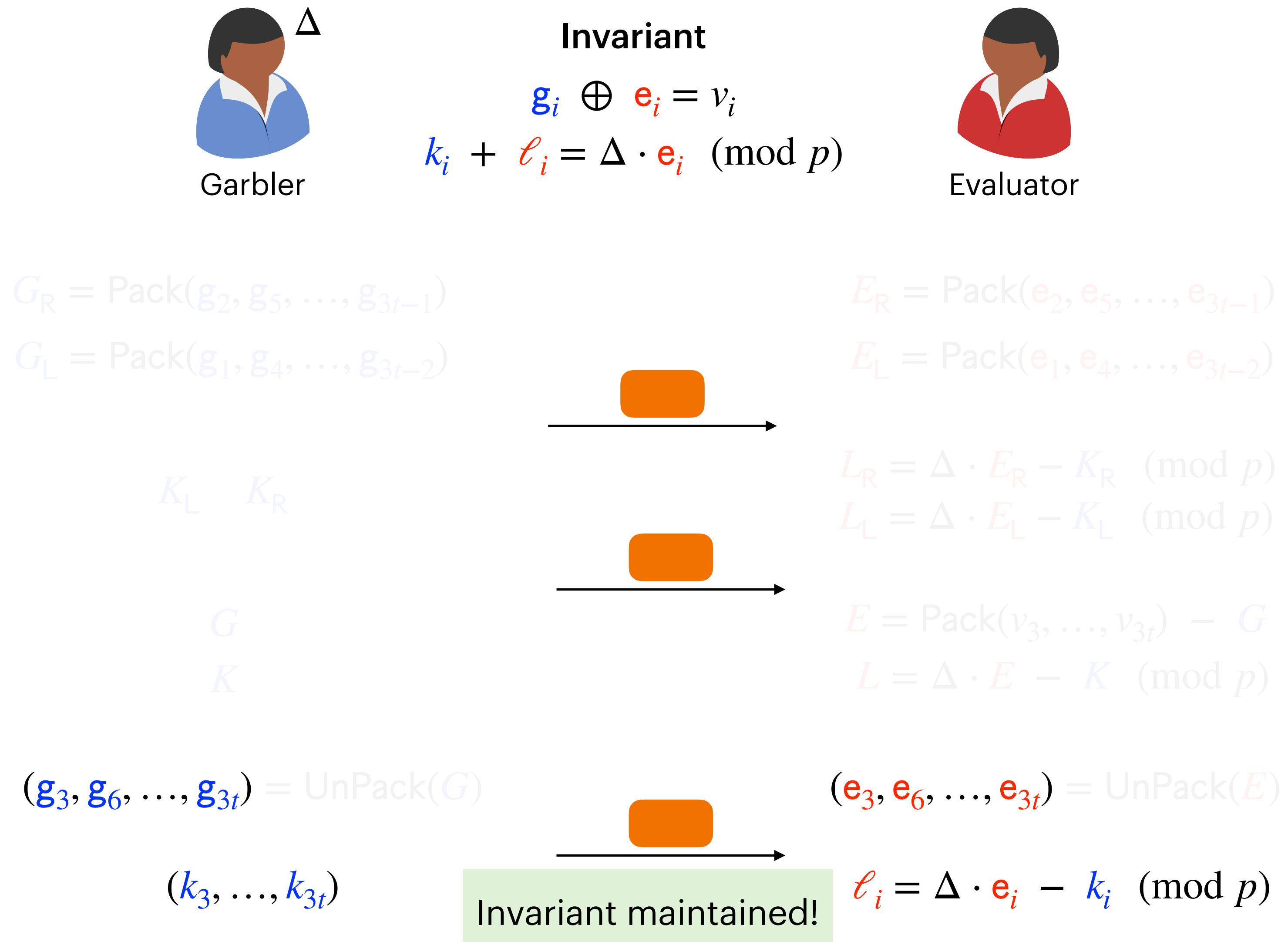
$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

## 2. Gate Evaluation

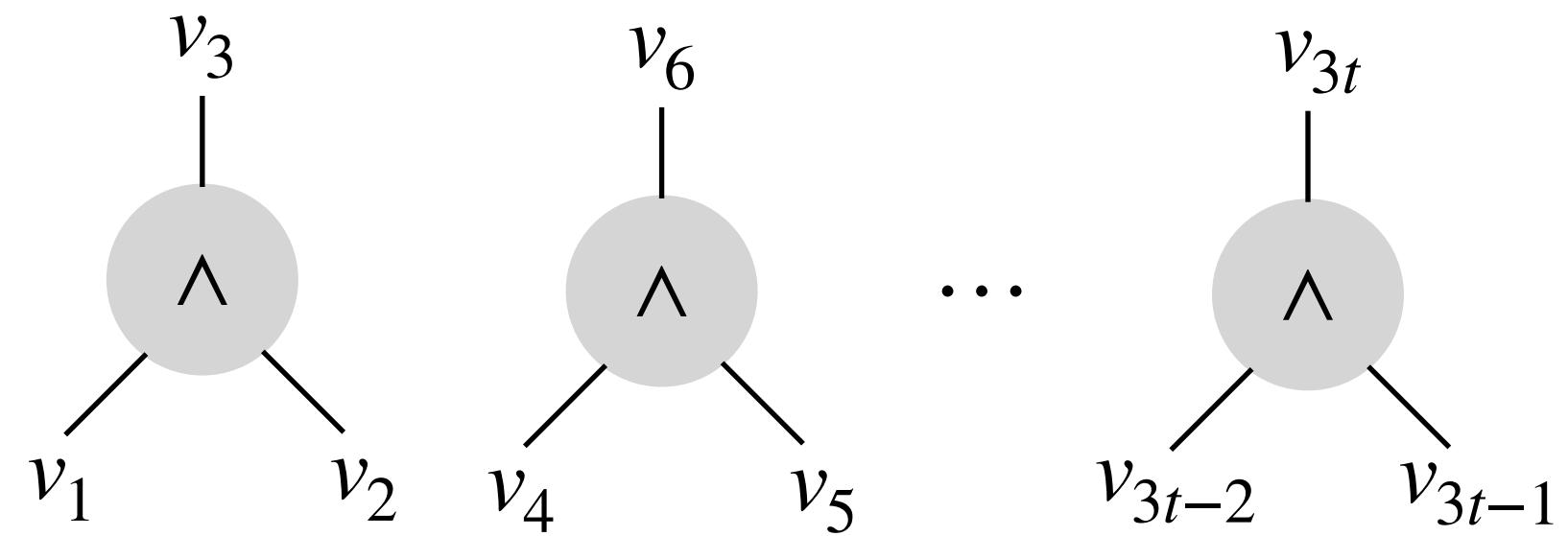
$$V = V_1 \cdot V_2$$

## 3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



# Template for $\omega(1/\lambda)$ -Rate Garbling



**Invariant**

$$\begin{aligned} \mathbf{g}_i \oplus \mathbf{e}_i &= v_i \\ k_i + \ell_i &= \Delta \cdot \mathbf{e}_i \pmod{p} \end{aligned}$$



1. Packing

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

$$G_R = \text{Pack}(\mathbf{g}_2, \mathbf{g}_5, \dots, \mathbf{g}_{3t-1})$$

$$G_L = \text{Pack}(\mathbf{g}_1, \mathbf{g}_4, \dots, \mathbf{g}_{3t-2})$$

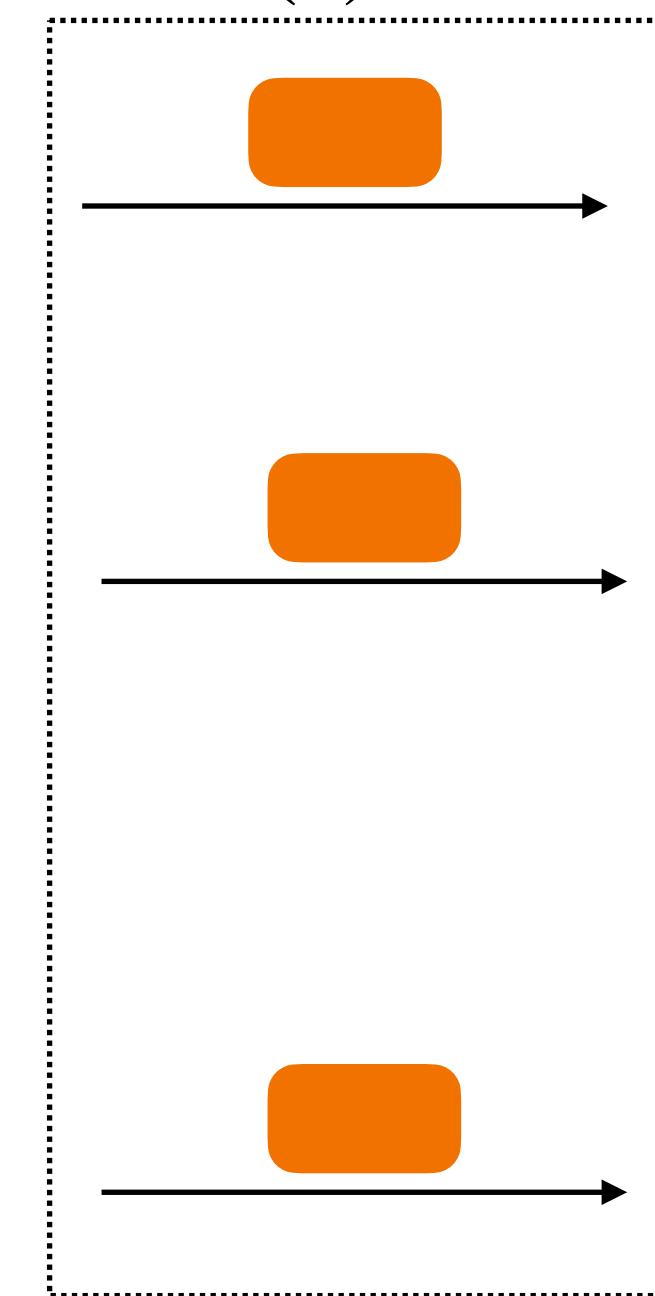
$$K_L - K_R$$

$$\begin{matrix} G \\ K \end{matrix}$$

$$(\mathbf{g}_3, \mathbf{g}_6, \dots, \mathbf{g}_{3t}) = \text{UnPack}(G)$$

$$(k_3, \dots, k_{3t})$$

$O(\lambda)$  bits



$$E_R = \text{Pack}(\mathbf{e}_2, \mathbf{e}_5, \dots, \mathbf{e}_{3t-1})$$

$$E_L = \text{Pack}(\mathbf{e}_1, \mathbf{e}_4, \dots, \mathbf{e}_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

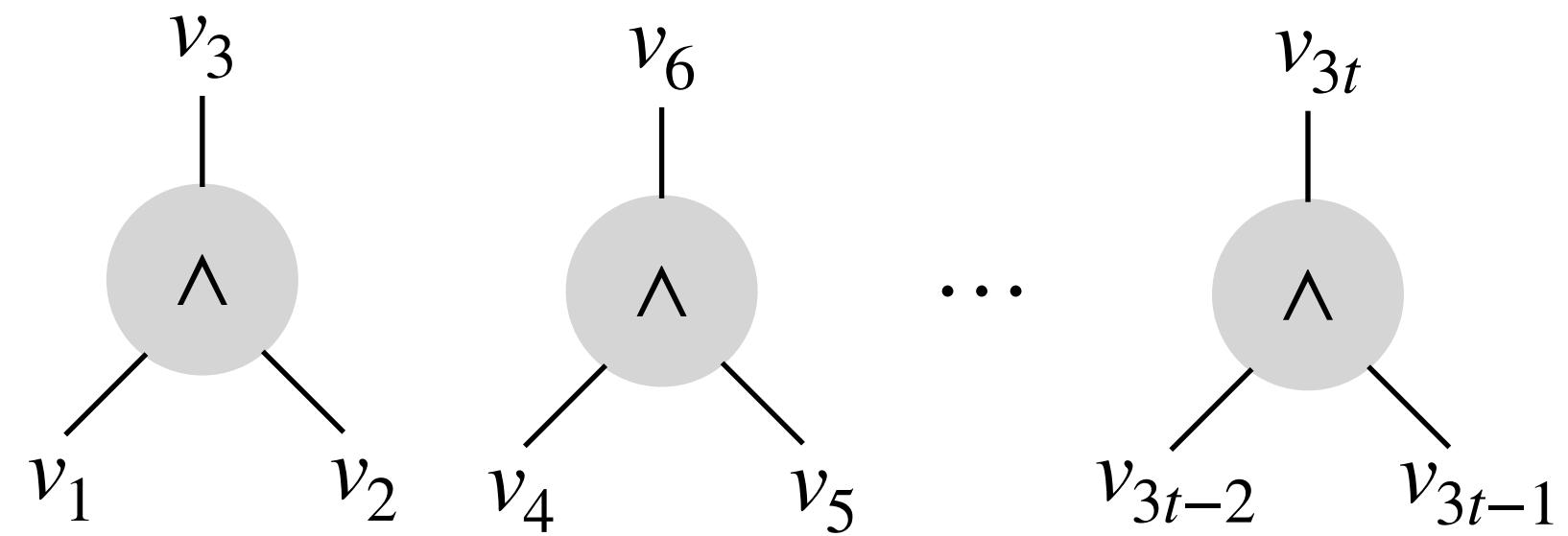
$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$

$$(\mathbf{e}_3, \mathbf{e}_6, \dots, \mathbf{e}_{3t}) = \text{UnPack}(E)$$

$$\ell_i = \Delta \cdot \mathbf{e}_i - k_i \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



**Invariant**

$$\begin{aligned} \mathbf{g}_i \oplus \mathbf{e}_i &= v_i \\ k_i + \ell_i &= \Delta \cdot \mathbf{e}_i \pmod{p} \end{aligned}$$



1. Packing

$$\begin{aligned} V_R &= \text{Rate: } O\left(\frac{t}{\lambda}\right), v_{3t-1} \\ V_L &= \text{Pack}(v_1, v_4, \dots, v_{3t-2}) \end{aligned}$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

$$K_L - K_R$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

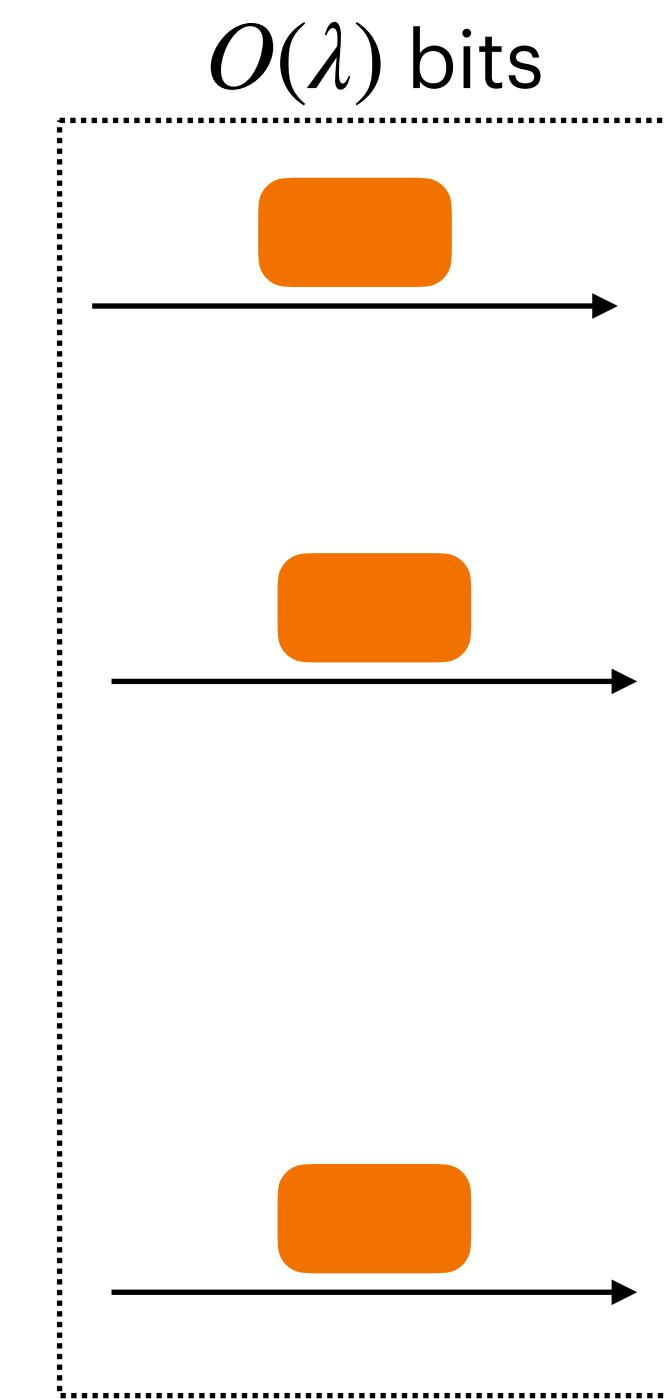
$$\begin{matrix} G \\ K \end{matrix}$$

3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$

$$(k_3, \dots, k_{3t})$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

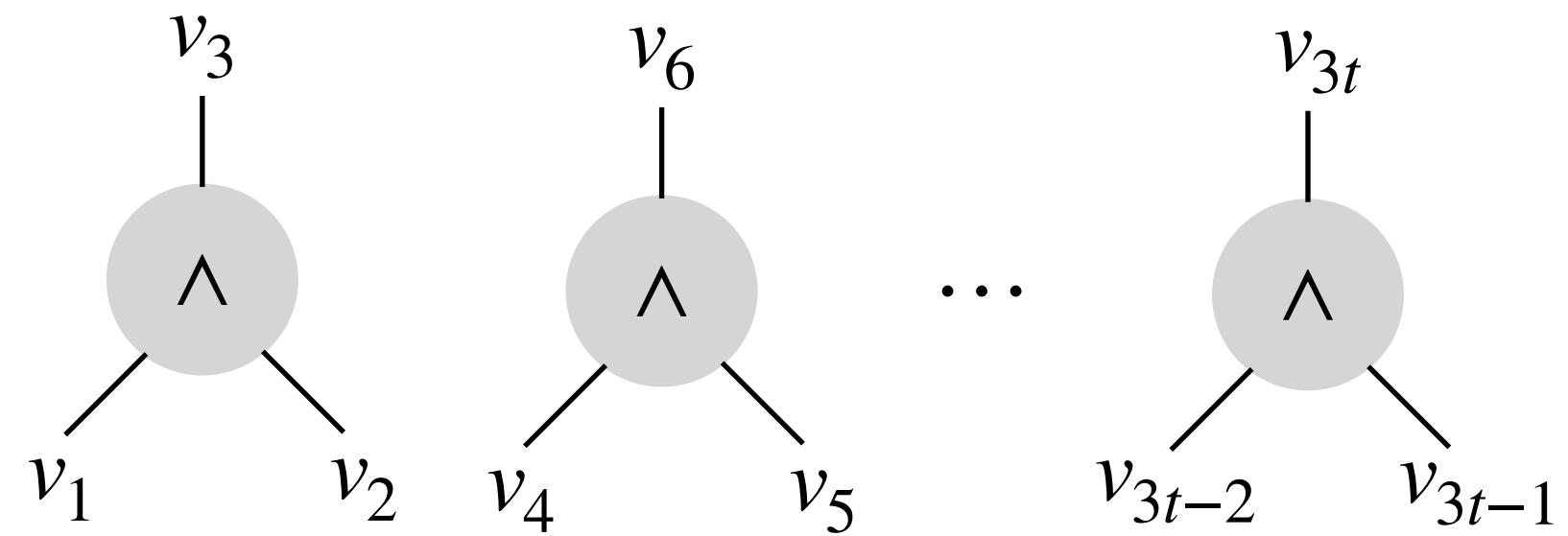
$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$

$$(e_3, e_6, \dots, e_{3t}) = \text{UnPack}(E)$$

$$\ell_i = \Delta \cdot e_i - k_i \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



**Invariant**

$$\begin{aligned} \mathbf{g}_i \oplus \mathbf{e}_i &= v_i \\ k_i + \ell_i &= \Delta \cdot \mathbf{e}_i \pmod{p} \end{aligned}$$



1. Packing

$$\begin{aligned} V_R &= \text{Pack}(v_2, v_5, \dots, v_{3t-1}) \\ V_L &= \text{Pack}(v_1, v_4, \dots, v_{3t-2}) \end{aligned}$$

2. Gate Evaluation

$$t = O\left(\sqrt{\log \lambda}\right)$$

$$V = V_L \cdot V_R$$

3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

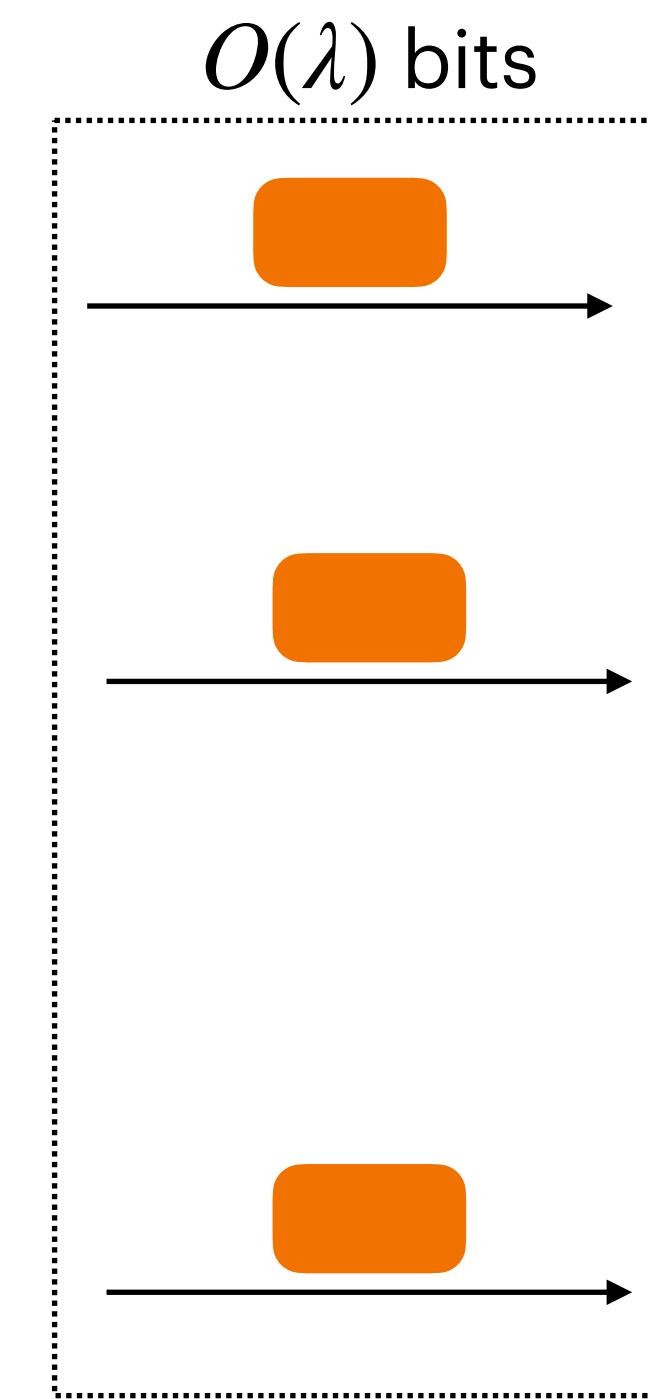
$$K_L \quad K_R$$

$$G$$

$$K$$

$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$

$$(k_3, \dots, k_{3t})$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

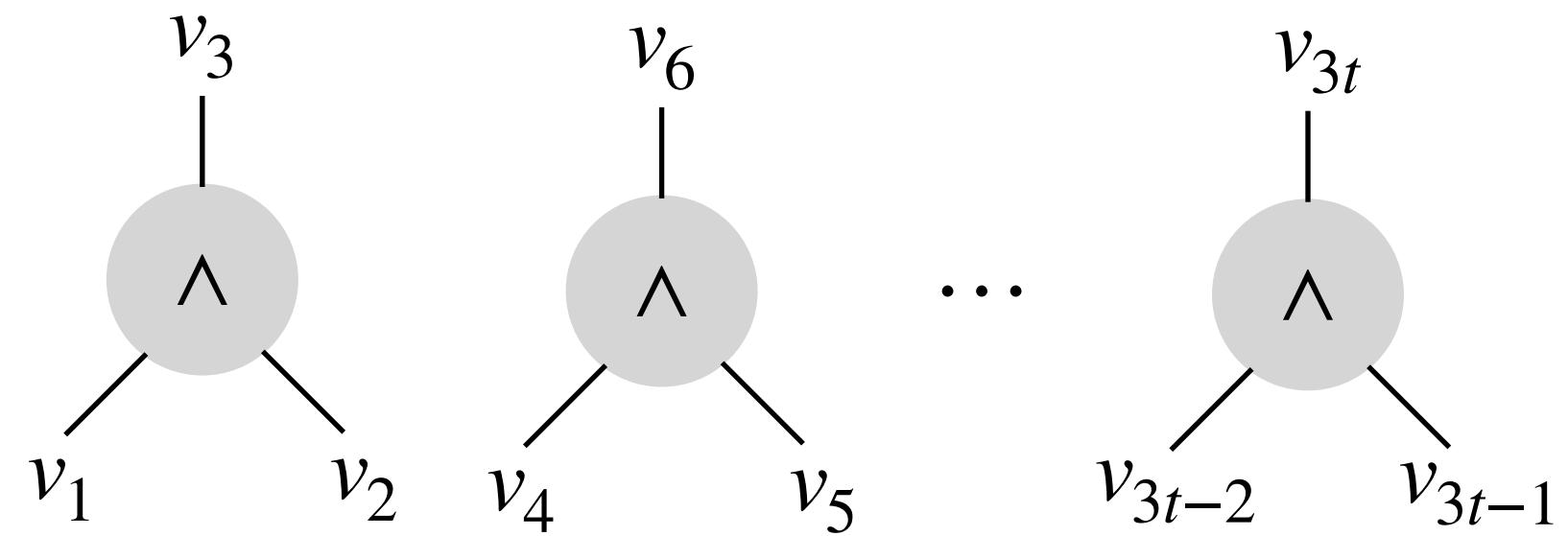
$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$

$$(e_3, e_6, \dots, e_{3t}) = \text{UnPack}(E)$$

$$\ell_i = \Delta \cdot e_i - k_i \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



**Invariant**

$$\mathbf{g}_i \oplus \mathbf{e}_i = v_i$$

$$k_i + \ell_i = \Delta \cdot \mathbf{e}_i \pmod{p}$$



1. Packing

**Rate:**  $O\left(\frac{t}{\lambda}\right) = O\left(\frac{\sqrt{\log \lambda}}{\lambda}\right)$

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

2. Gate Evaluation

$$t = O\left(\sqrt{\log \lambda}\right)$$

$$V = V_1 \cdot V_2$$

$$K_L \quad K_R$$

$$G$$

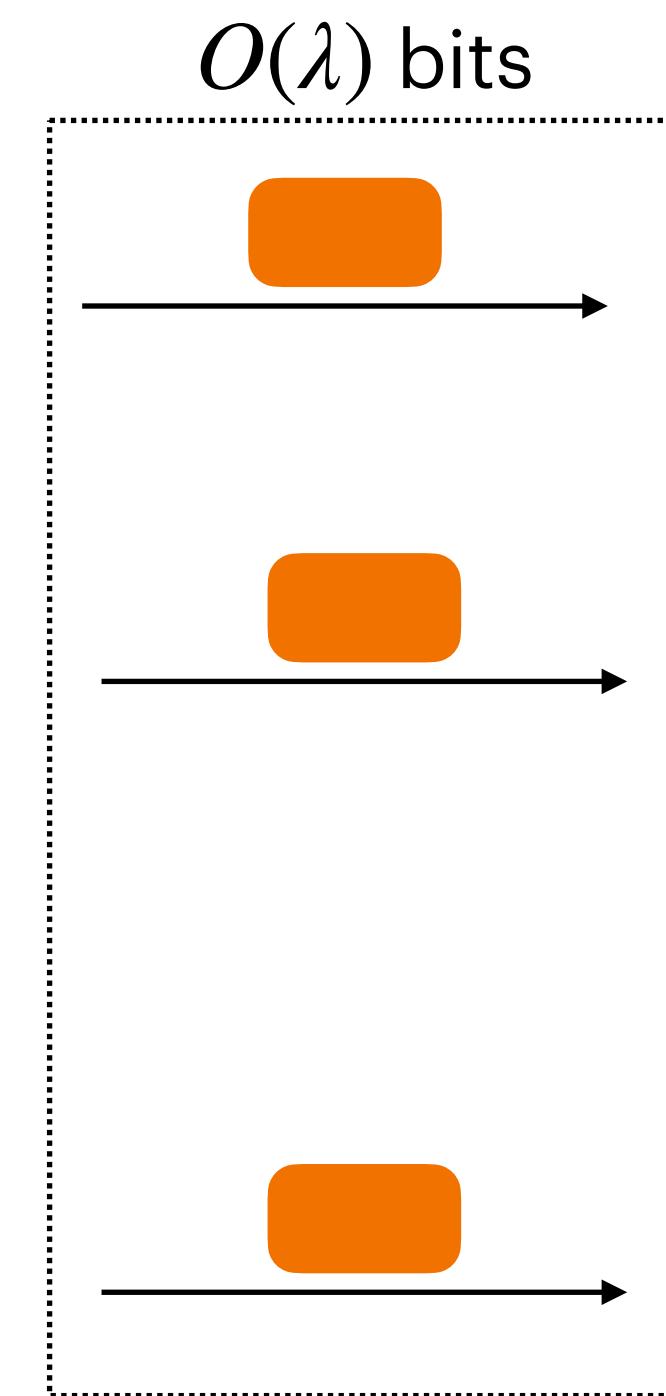
$$K$$

$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$

$$(k_3, \dots, k_{3t})$$

3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$



$$E_R = \text{Pack}(e_2, e_5, \dots, e_{3t-1})$$

$$E_L = \text{Pack}(e_1, e_4, \dots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

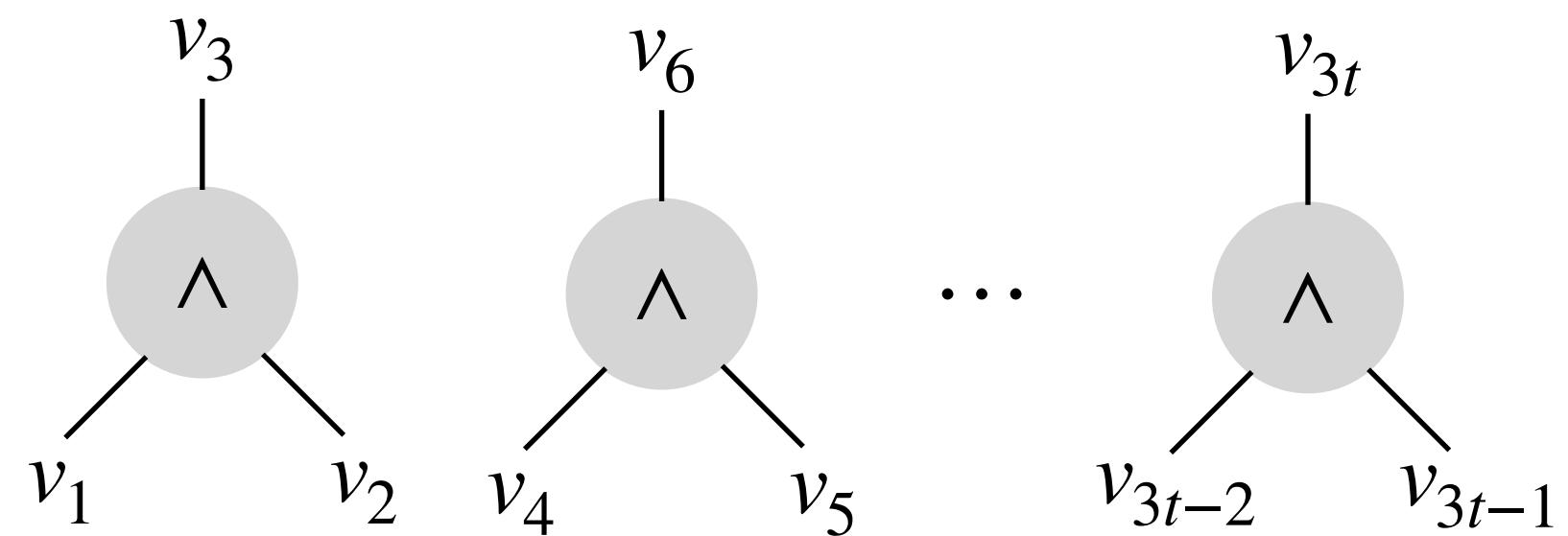
$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$

$$(e_3, e_6, \dots, e_{3t}) = \text{UnPack}(E)$$

$$\ell_i = \Delta \cdot e_i - k_i \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



**Invariant**

$$g_i \oplus e_i = v_i$$

$$k_i + \ell_i = \Delta \cdot e_i \pmod{p}$$



1. Packing

**Rate:**  $O\left(\frac{t}{\lambda}\right) = O\left(\frac{\sqrt{\log \lambda}}{\lambda}\right)$

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

$$K_L \quad K_R$$

$$G$$

$$K$$

$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$

$$(k_3, \dots, k_{3t})$$

$$(e_3, e_6, \dots, e_{3t}) = \text{UnPack}(E)$$

$$(e_3, e_6, \dots, e_{3t}) = \text{UnPack}(E)$$

3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

$$L_R = \Delta \cdot E_R - K_R \pmod{p}$$

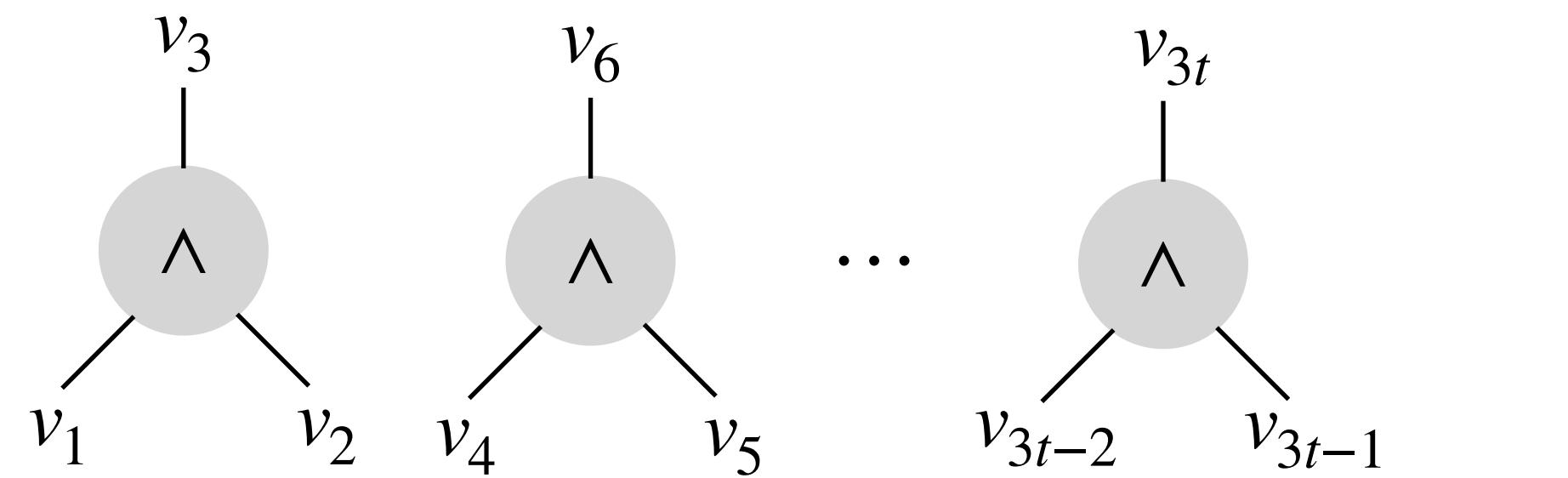
$$L_L = \Delta \cdot E_L - K_L \pmod{p}$$

$$E = \text{Pack}(v_3, \dots, v_{3t}) - G$$

$$L = \Delta \cdot E - K \pmod{p}$$

$$\ell_i = \Delta \cdot e_i - k_i \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



# Invariant

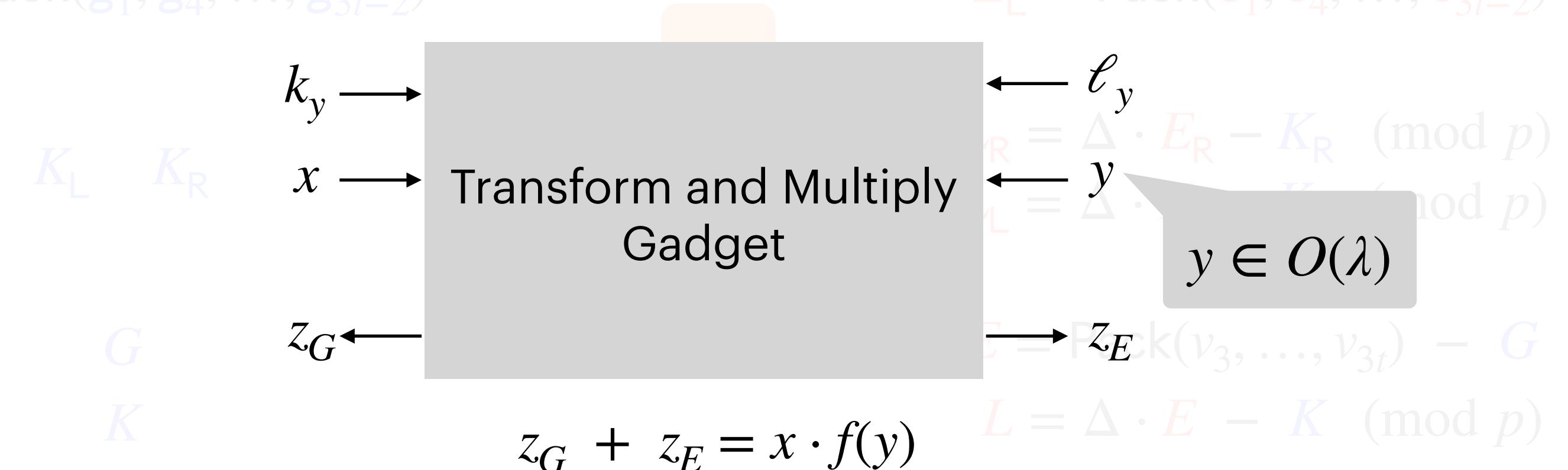
$$g_i \oplus e_i = v_i$$

$$k_i + \ell_i = \Delta \cdot \mathbf{e}_i \pmod{p}$$

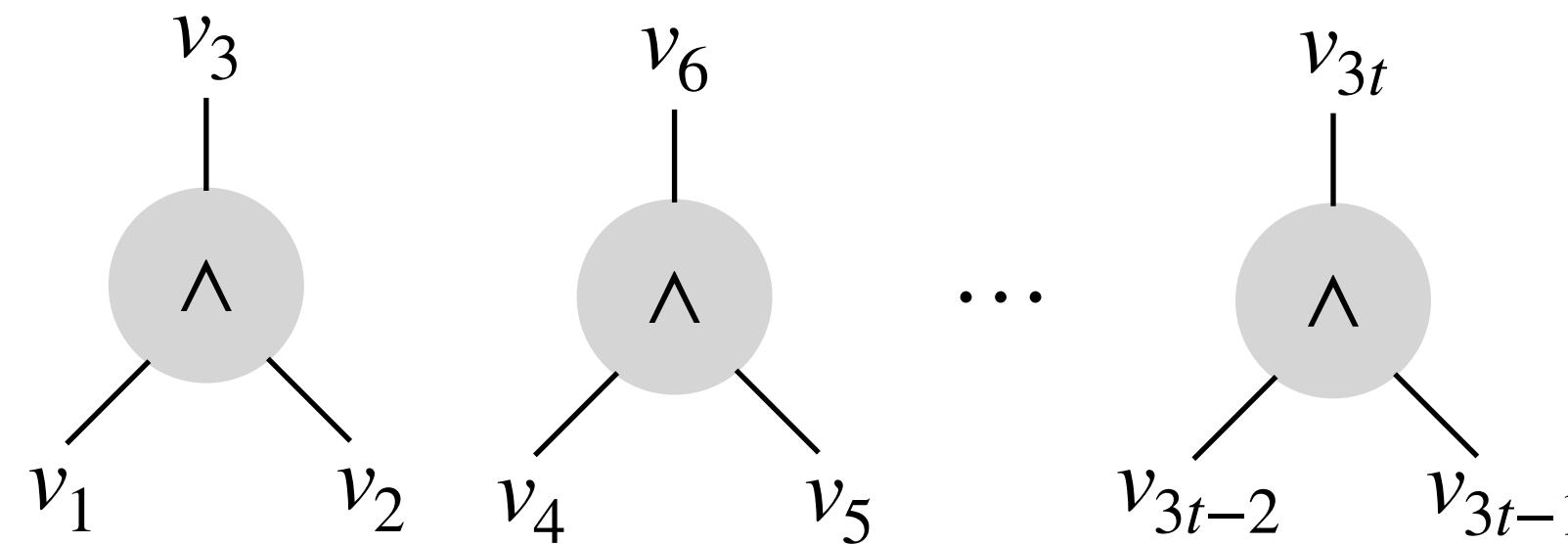


$$V_R = \mathbf{Rate:} O\left(\frac{t}{\lambda}\right) = O\left(\frac{\sqrt{\log \lambda}}{\lambda}\right)$$

# Why $t = O(\sqrt{\log \lambda})$ ?



# Template for $\omega(1/\lambda)$ -Rate Garbling



**Invariant**

$$\begin{aligned} \mathbf{g}_i \oplus \mathbf{e}_i &= v_i \\ k_i + \ell_i &\equiv \Delta \cdot \mathbf{e}_i \pmod{p} \end{aligned}$$



1. Packing

**Rate:**  $O\left(\frac{t}{\lambda}\right) = O\left(\frac{\sqrt{\log \lambda}}{\lambda}\right)$

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

Why  $t = O(\sqrt{\log \lambda})$ ?

2. Gate Evaluation

$$V \cdot t \in O(\log \lambda)$$

3. Unpacking

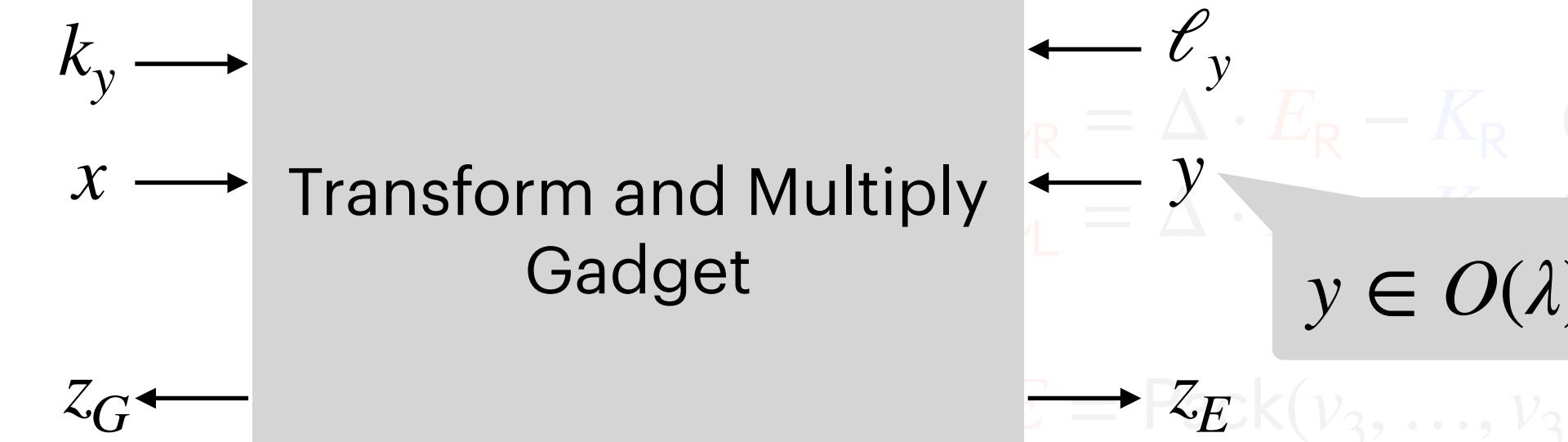
$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

$$K_L - K_R$$

$$G$$

$$K$$

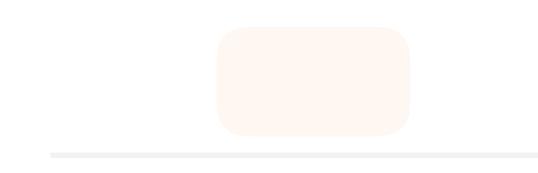
$$(k_3, \dots, k_{3t})$$



$$z_G + z_E = x \cdot f(y)$$

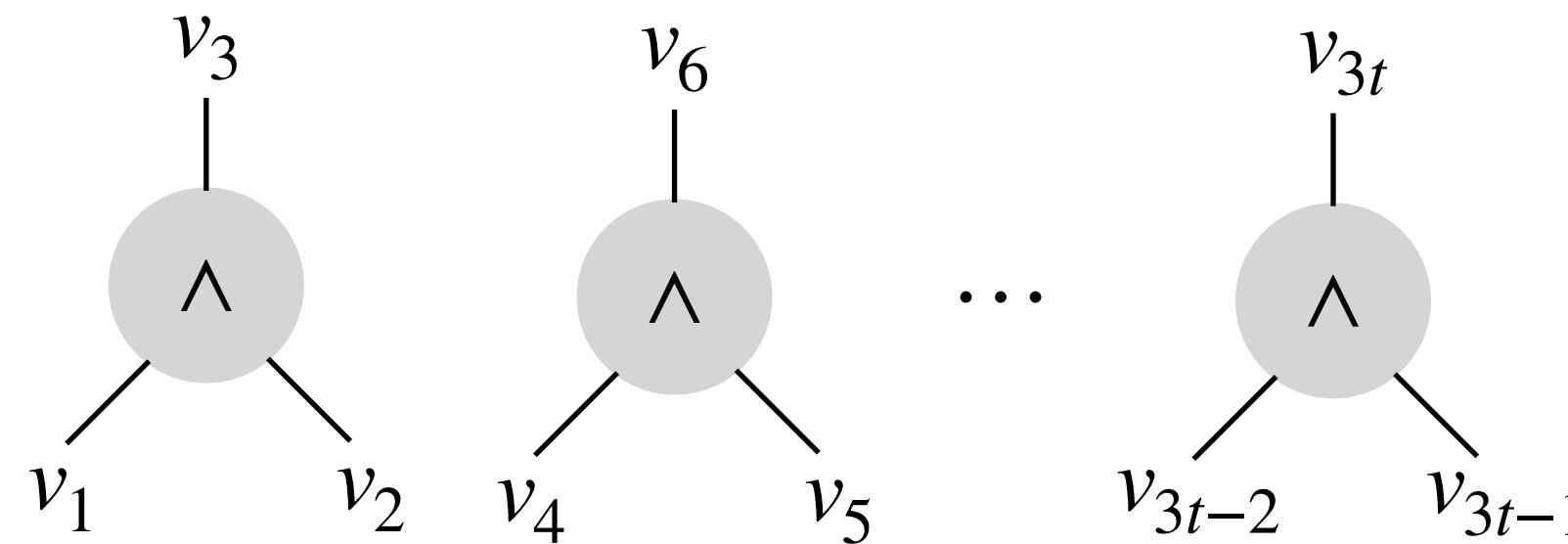
$$(\mathbf{g}_3, \mathbf{g}_6, \dots, \mathbf{g}_{3t}) = \text{UnPack}(G)$$

$$(\mathbf{e}_3, \mathbf{e}_6, \dots, \mathbf{e}_{3t}) = \text{UnPack}(E)$$



$$\ell_i = \Delta \cdot \mathbf{e}_i - k_i \pmod{p}$$

# Template for $\omega(1/\lambda)$ -Rate Garbling



**Invariant**

$$g_i \oplus e_i = v_i$$

$$k_i + \ell_i = \Delta \cdot e_i \pmod{p}$$



1. Packing

**Rate:**  $O\left(\frac{t}{\lambda}\right) = O\left(\frac{\sqrt{\log \lambda}}{\lambda}\right)$

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

Why  $t = O(\sqrt{\log \lambda})$ ?

2. Gate Evaluation

$$V \cdot t \in O(\log \lambda)$$

3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$

$$(k_3, \dots, k_{3t}) = \Delta \cdot e_i - k_i \pmod{p}$$

- Gadget adds noise to ensure **privacy**, which **increases magnitude** of shares
- Retaining **homomorphism** over these shares requires **packing fewer bits**

2. Gate Evaluation

$$K_L$$

$$K_R$$

$$E$$

$$G$$

$$V$$

$$V = V_1 \cdot V_2 = (G_L + E_L) \cdot (G_R + E_R)$$

$$= G_L \cdot G_R + G_L \cdot E_R + E_L \cdot G_R + E_L \cdot E_R$$

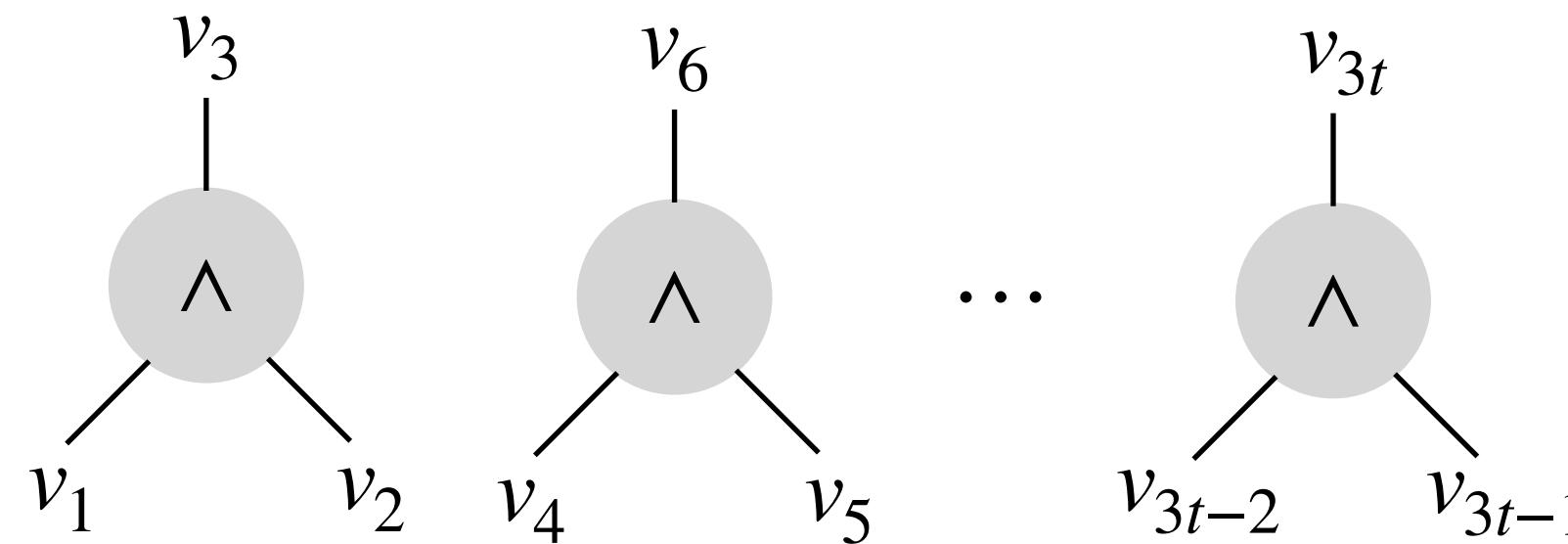
$$= \Delta \cdot E - K \pmod{p}$$

$$(e_3, e_6, \dots, e_{3t}) = \text{UnPack}(E)$$

$$(k_3, \dots, k_{3t}) = \Delta \cdot e_i - k_i \pmod{p}$$

Use multiplication  
gadget

# Template for $\omega(1/\lambda)$ -Rate Garbling



**Invariant**

$$g_i \oplus e_i = v_i$$

$$k_i + \ell_i = \Delta \cdot e_i \pmod{p}$$



1. Packing

**Rate:**  $O\left(\frac{t}{\lambda}\right) = O\left(\frac{\sqrt{\log \lambda}}{\lambda}\right)$

$$V_R = \text{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$G_R = \text{Pack}(g_2, g_5, \dots, g_{3t-1})$$

$$V_L = \text{Pack}(v_1, v_4, \dots, v_{3t-2})$$

$$G_L = \text{Pack}(g_1, g_4, \dots, g_{3t-2})$$

Why  $t = O(\sqrt{\log \lambda})$ ?

2. Gate Evaluation

$$V = t \in O(\log \lambda)$$

$$\bullet t \in O(\sqrt{\log \lambda})$$

3. Unpacking

$$(v_3, v_6, \dots, v_{3t}) = \text{UnPack}(V)$$

- Gadget adds noise to ensure **privacy**, which **increases magnitude** of shares
- Retaining **homomorphism** over these shares requires **packing fewer bits**

$$K_L$$

$$K_R$$

$$G$$

$$V = V_1 \cdot V_2 = (G_L + E_L) \cdot (G_R + E_R)$$

$$= G_L \cdot G_R + G_L \cdot E_R + E_L \cdot G_R + E_L \cdot E_R$$

$$(g_3, g_6, \dots, g_{3t}) = \text{UnPack}(G)$$

$$(k_3, \dots, k_{3t})$$

Use multiplication  
gadget

$$e_i = \Delta \cdot e_i - k_i \pmod{p}$$

# Packing Scheme

# Packing Scheme

Packing from  $\mathbb{F}_2^t$  to  $\mathbb{Z}$ :

1) Pack and UnPack are  $\mathbb{F}_2$ -linear

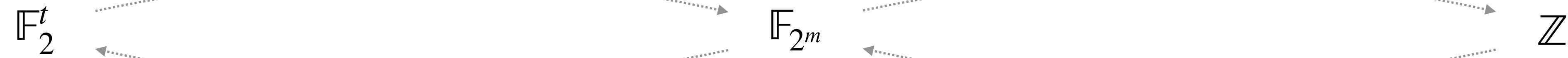
2) Homomorphic for sum of products

# Packing Scheme

Packing from  $\mathbb{F}_2^t$  to  $\mathbb{Z}$ :

1) Pack and UnPack are  $\mathbb{F}_2$ -linear

2) Homomorphic for sum of products



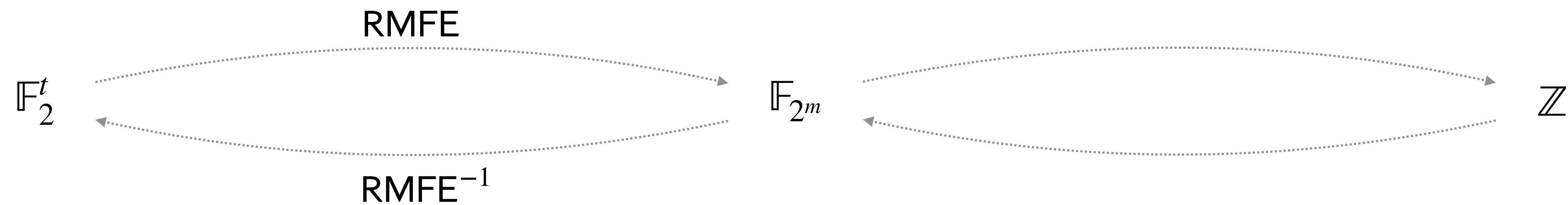
# Packing Scheme

Packing from  $\mathbb{F}_2^t$  to  $\mathbb{Z}$ :

1) Pack and UnPack are  $\mathbb{F}_2$ -linear

2) Homomorphic for sum of products

**Reverse Multiplication-Friendly Embeddings**  
[Cascudo-Cramer-Xing-Yuan'18]



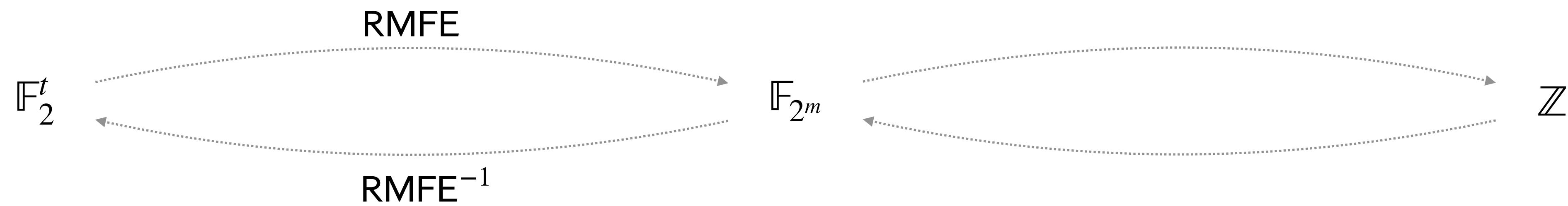
# Packing Scheme

Packing from  $\mathbb{F}_2^t$  to  $\mathbb{Z}$ :

1) Pack and UnPack are  $\mathbb{F}_2$ -linear

2) Homomorphic for sum of products

**Reverse Multiplication-Friendly Embeddings**  
[Cascudo-Cramer-Xing-Yuan'18]



RMFE and  $\text{RMFE}^{-1}$  are  $\mathbb{F}_2$ -linear

Homomorphic for sum of products

$$m = \Theta(t)$$

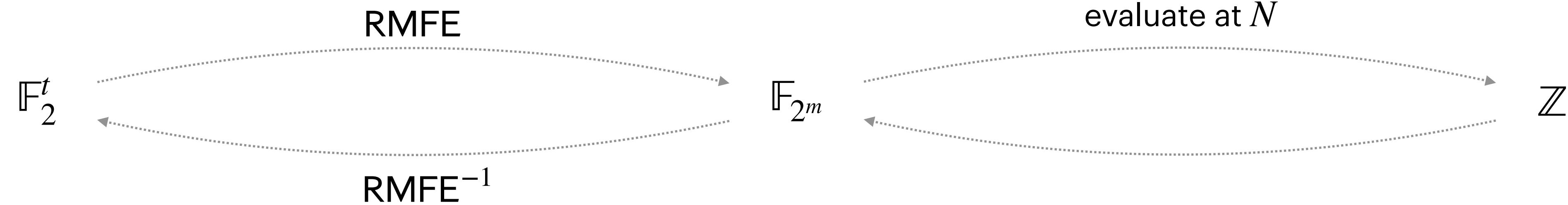
# Packing Scheme

Packing from  $\mathbb{F}_2^t$  to  $\mathbb{Z}$ :

1) Pack and UnPack are  $\mathbb{F}_2$ -linear

2) Homomorphic for sum of products

**Reverse Multiplication-Friendly Embeddings**  
[Cascudo-Cramer-Xing-Yuan'18]



$\text{Eval}(x)$  : Lift  $x \in \mathbb{F}_2[X]$  to  $\mathbb{Z}[X]$  and  
evaluate at  $N$

RMFE and  $\text{RMFE}^{-1}$  are  $\mathbb{F}_2$ -linear

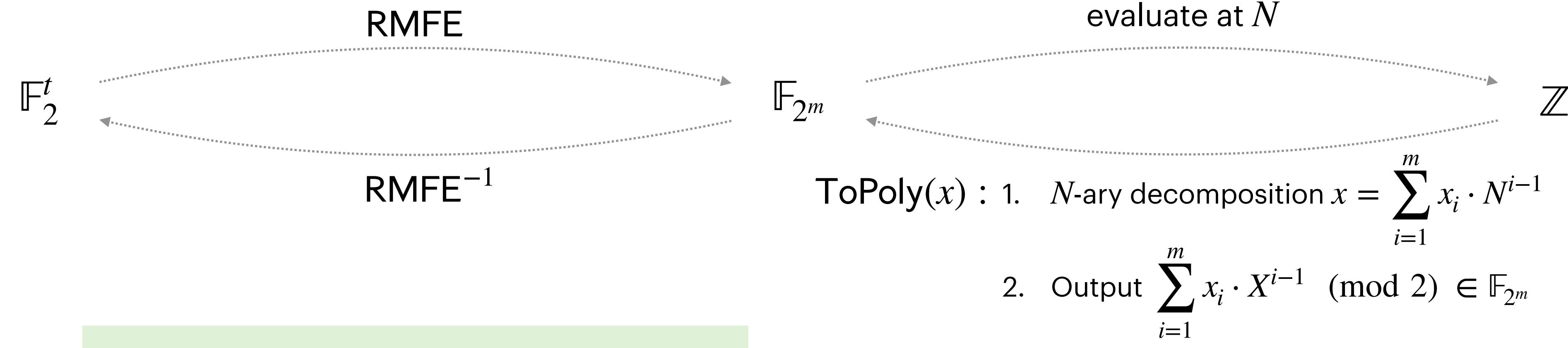
Homomorphic for sum of products

$$m = \Theta(t)$$

# Packing Scheme

Packing from  $\mathbb{F}_2^t$  to  $\mathbb{Z}$ :      1) Pack and UnPack are  $\mathbb{F}_2$ -linear      2) Homomorphic for sum of products

## Reverse Multiplication-Friendly Embeddings [Cascudo-Cramer-Xing-Yuan'18]



RMFE and  $\text{RMFE}^{-1}$  are  $\mathbb{F}_2$ -linear

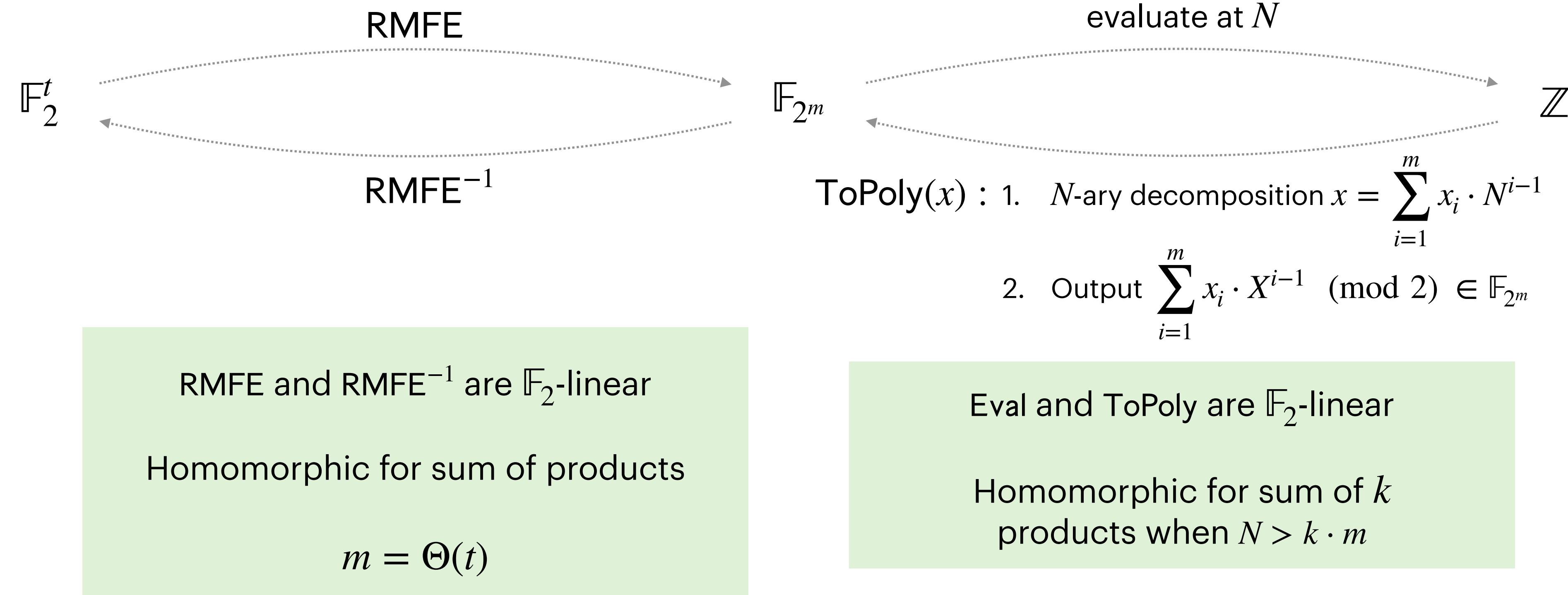
Homomorphic for sum of products

$$m = \Theta(t)$$

# Packing Scheme

Packing from  $\mathbb{F}_2^t$  to  $\mathbb{Z}$ :      1) Pack and UnPack are  $\mathbb{F}_2$ -linear      2) Homomorphic for sum of products

## Reverse Multiplication-Friendly Embeddings [Cascudo-Cramer-Xing-Yuan'18]



# Conclusion

**Rate- $\Omega(1/\lambda)$**

Symmetric-key crypto

Black-box use of crypto

[Yao'86] [Lindell-Pinkas'07] [Kolesnikov-Schneider'08] [Zahur-Rosulek-Evans'15] [Rosulek-Roy'21]

**Rate-1**

Ring LWE / NTRU

Non-black-box use of crypto

[Liu-Wang-Yang-Yu'24]

**Rate- $\omega(1)$**

ABE + FHE / iO + OWF

Non-black-box use of crypto

[Boneh-Gentry-Grobunov-Halevi-Nikolaenko-Segev-Vaikuntanathan-Vinayagamurthy'14] [Lin-Pass'14]  
[Goldwasser-Kalai-Popa-Vaikuntanathan-Zeldovich'13] [Koppula-Lewko-Waters'15] [Hsieh-Lin-Luo'23]

# Conclusion

**Rate- $\Omega(1/\lambda)$**

Symmetric-key crypto

Black-box use of crypto

[Yao'86] [Lindell-Pinkas'07] [Kolesnikov-Schneider'08] [Zahur-Rosulek-Evans'15] [Rosulek-Roy'21]

**Rate- $O(\sqrt{\log \lambda} / \lambda)$**

Generic Group Model

Black-box use of crypto

This Work

**Rate-1**

Ring LWE / NTRU

Non-black-box use of crypto

[Liu-Wang-Yang-Yu'24]

**Rate- $\omega(1)$**

ABE + FHE / iO + OWF

Non-black-box use of crypto

[Boneh-Gentry-Grobunov-Halevi-Nikolaenko-Segev-Vaikuntanathan-Vinayagamurthy'14] [Lin-Pass'14]  
[Goldwasser-Kalai-Popa-Vaikuntanathan-Zeldovich'13] [Koppula-Lewko-Waters'15] [Hsieh-Lin-Luo'23]

# Conclusion

**Rate- $\Omega(1/\lambda)$**

Symmetric-key crypto

Black-box use of crypto

[Yao'86] [Lindell-Pinkas'07] [Kolesnikov-Schneider'08] [Zahur-Rosulek-Evans'15] [Rosulek-Roy'21]

**Rate- $O(\sqrt{\log \lambda} / \lambda)$**

Generic Group Model

Black-box use of crypto

This Work

**Rate-1**

Ring LWE / NTRU

DDH / DCR

Non-black-box use of crypto

[Liu-Wang-Yang-Yu'24] [Meyer-Orlandi-Roy-Scholl'25] [Ishai-Li-Lin'25]

**Rate- $\omega(1)$**

ABE + FHE / iO + OWF

Non-black-box use of crypto

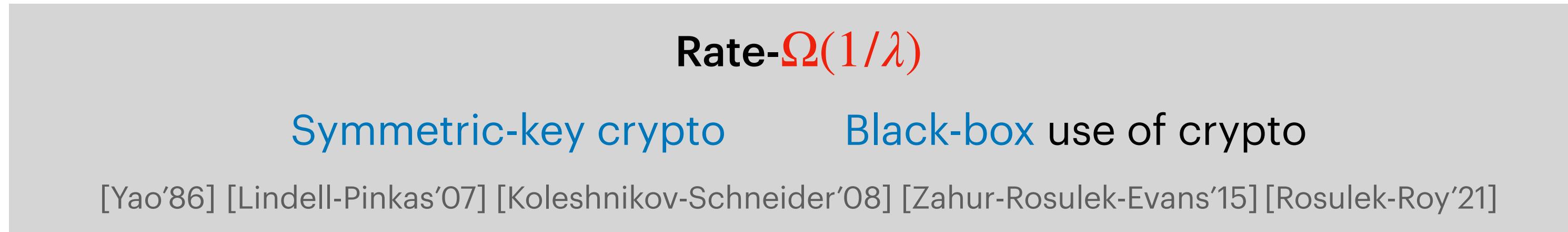
[Boneh-Gentry-Grobunov-Halevi-Nikolaenko-Segev-Vaikuntanathan-Vinayagamurthy'14] [Lin-Pass'14]  
[Goldwasser-Kalai-Popa-Vaikuntanathan-Zeldovich'13] [Koppula-Lewko-Waters'15] [Hsieh-Lin-Luo'23]

# Conclusion

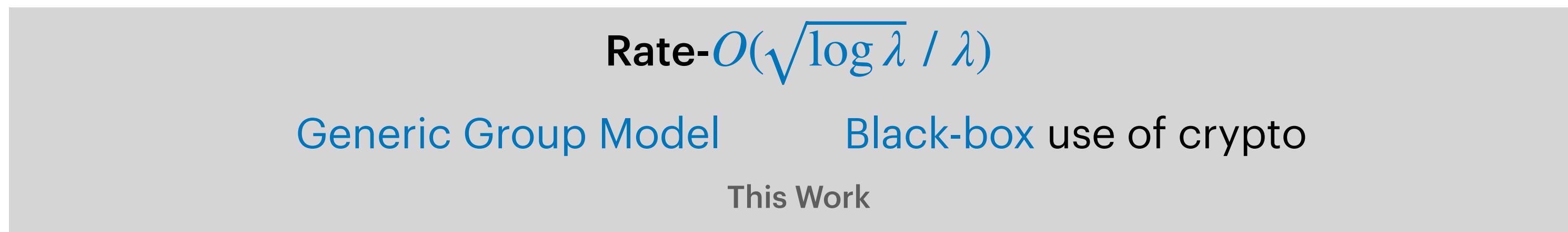
| Rate- $\Omega(1/\lambda)$  |   |
|--|---|
| Symmetric-key crypto   | Black-box use of crypto                   |
| [Yao'86] [Lindell-Pinkas'07] [Kolesnikov-Schneider'08]   | [Zahur-Rosulek-Evans'15] [Rosulek-Roy'21] |
| Rate- $O(\sqrt{\log \lambda} / \lambda)$   |   |
| Generic Group Model  | Black-box use of crypto                   |
| This Work  |   |
| Rate-1   |   |
| Ring LWE / NTRU  | Non-black-box use of crypto               |
| DDH / DCR  |   |
| [Liu-Wang-Yang-Yu'24]  | [Meyer-Orlandi-Roy-Scholl'25]             |
|  | [Ishai-Li-Lin'25]                         |
| Rate- $\omega(1)$  |   |
| ABE + FHE / iO + OWF   | Non-black-box use of crypto               |
| [Boneh-Gentry-Grobunov-Halevi-Nikolaenko-Segev-Vaikuntanathan-Vinayagamurthy'14] [Lin-Pass'14]   |   |
| [Goldwasser-Kalai-Popa-Vaikuntanathan-Zeldovich'13] [Koppula-Lewko-Waters'15] [Hsieh-Lin-Luo'23] |   |

Can we get better rate while being black-box in crypto?

# Conclusion



Can we get  $\omega(1/\lambda)$ -rate from other assumptions?



Can we get better rate while being black-box in crypto?



# Conclusion

**Rate- $\Omega(1/\lambda)$**   
Symmetric-key crypto      Black-box use of crypto  
[Yao'86] [Lindell-Pinkas'07] [Kolesnikov-Schneider'08] [Zahur-Rosulek-Evans'15] [Rosulek-Roy'21]

**Rate- $O(\sqrt{\log \lambda} / \lambda)$**   
Generic Group Model      Black-box use of crypto  
This Work

**Rate-1**  
Ring LWE / NTRU      Non-black-box use of crypto  
DDH / DCR  
[Liu-Wang-Yang-Yu'24] [Meyer-Orlandi-Roy-Scholl'25] [Ishai-Li-Lin'25]

**Rate- $\omega(1)$**   
ABE + FHE / iO + OWF      Non-black-box use of crypto  
[Boneh-Gentry-Grobunov-Halevi-Nikolaenko-Segev-Vaikuntanathan-Vinayagamurthy'14] [Lin-Pass'14]  
[Goldwasser-Kalai-Popa-Vaikuntanathan-Zeldovich'13] [Koppula-Lewko-Waters'15] [Hsieh-Lin-Luo'23]

Can we get  $\omega(1/\lambda)$ -rate from other assumptions?

Can we get better rate while being black-box in crypto?



[ia.cr/2025/268](https://ia.cr/2025/268)

**Thank You**