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

CRYPTO 2025

Geoffroy Couteau
CNRS, IRIF
Universitè Paris Citè

Carmit Hazay
Bar-Ilan University

Aditya Hegde
JHU

Naman Kumar
Oregon State University

Garbled Circuits

[Yao’86]

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

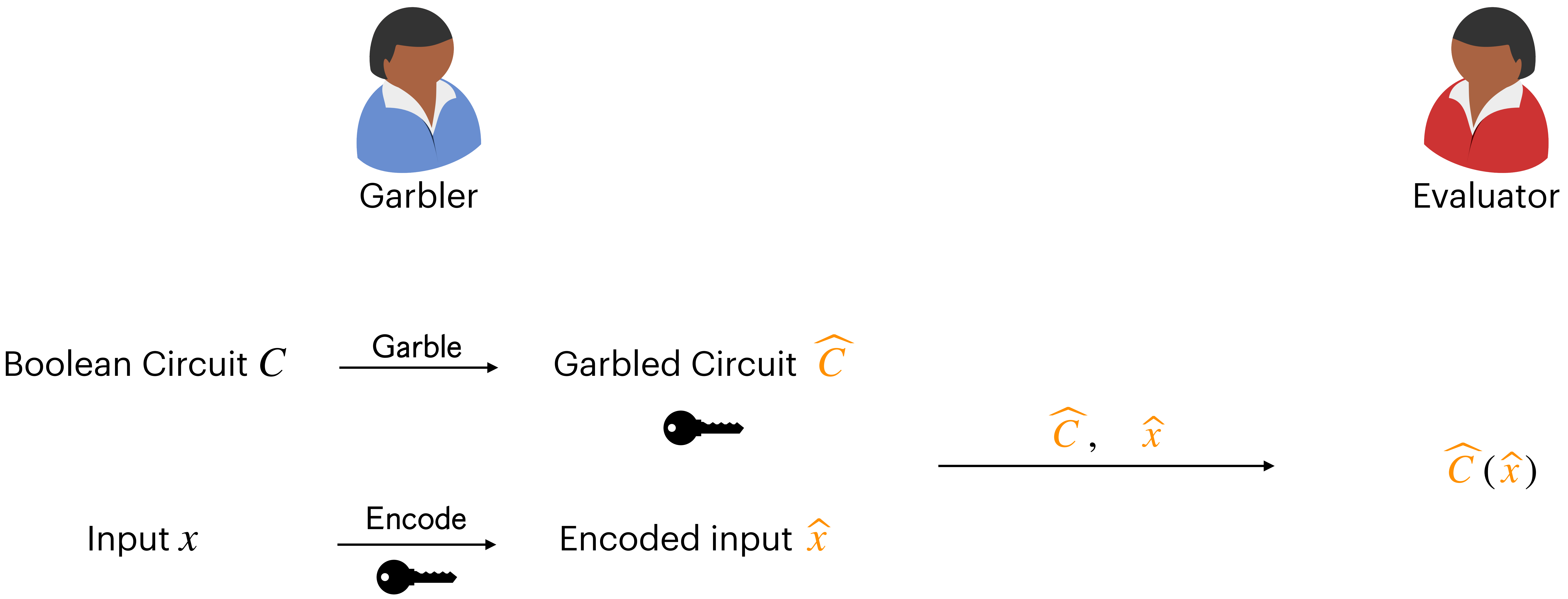
Evaluator

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

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

Garbled Circuits

[Yao’86]



Garbler

Evaluator

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

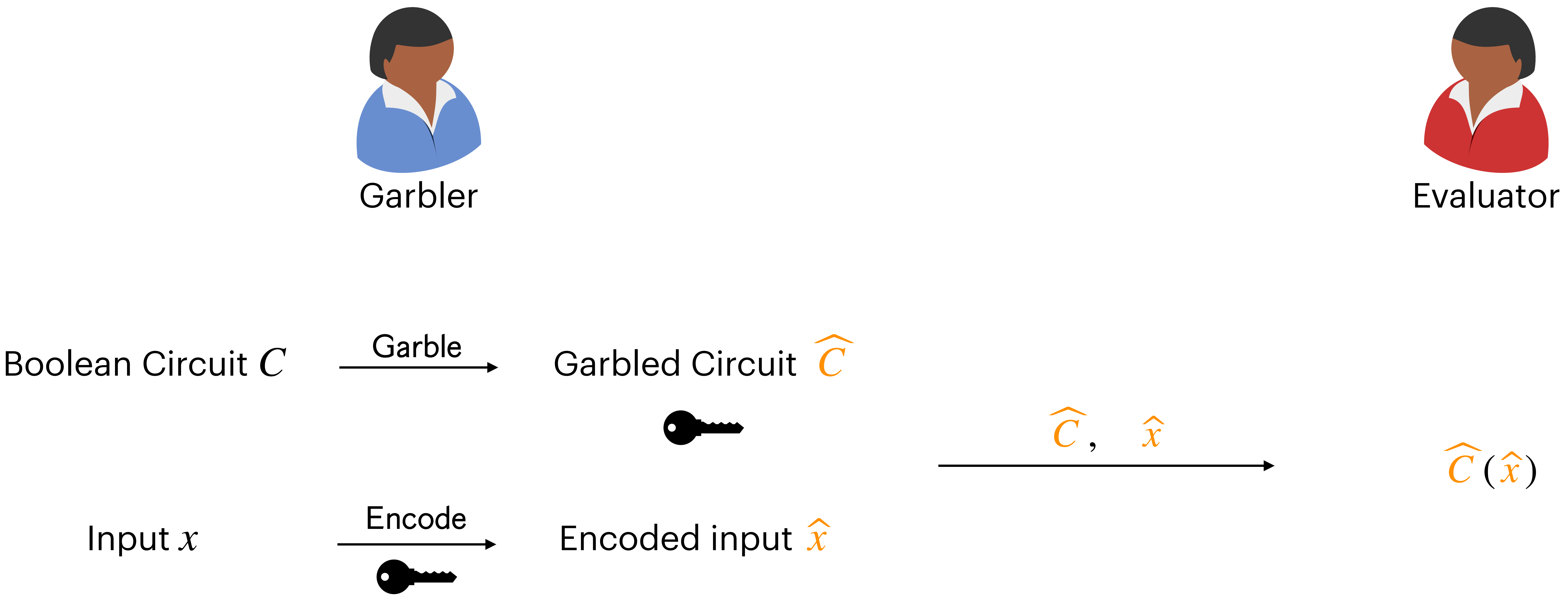
Input x $\xrightarrow{\text{Encode}}$ Encoded input $\hat{x}$

$\xrightarrow{\widehat{C},\ \hat{x}}$

$\widehat{C}(\hat{x})$

Garbled Circuits

[Yao'86]



Garbler

Evaluator

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

🔑

Input x $\xrightarrow[\text{🔑}]{\text{Encode}}$ Encoded input $\hat{x}$

$\xrightarrow{\widehat{C},\ \hat{x}}$

$\widehat{C}(\hat{x})$

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

Garbled Circuits

[Yao’86]

Garbler

Evaluator

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

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

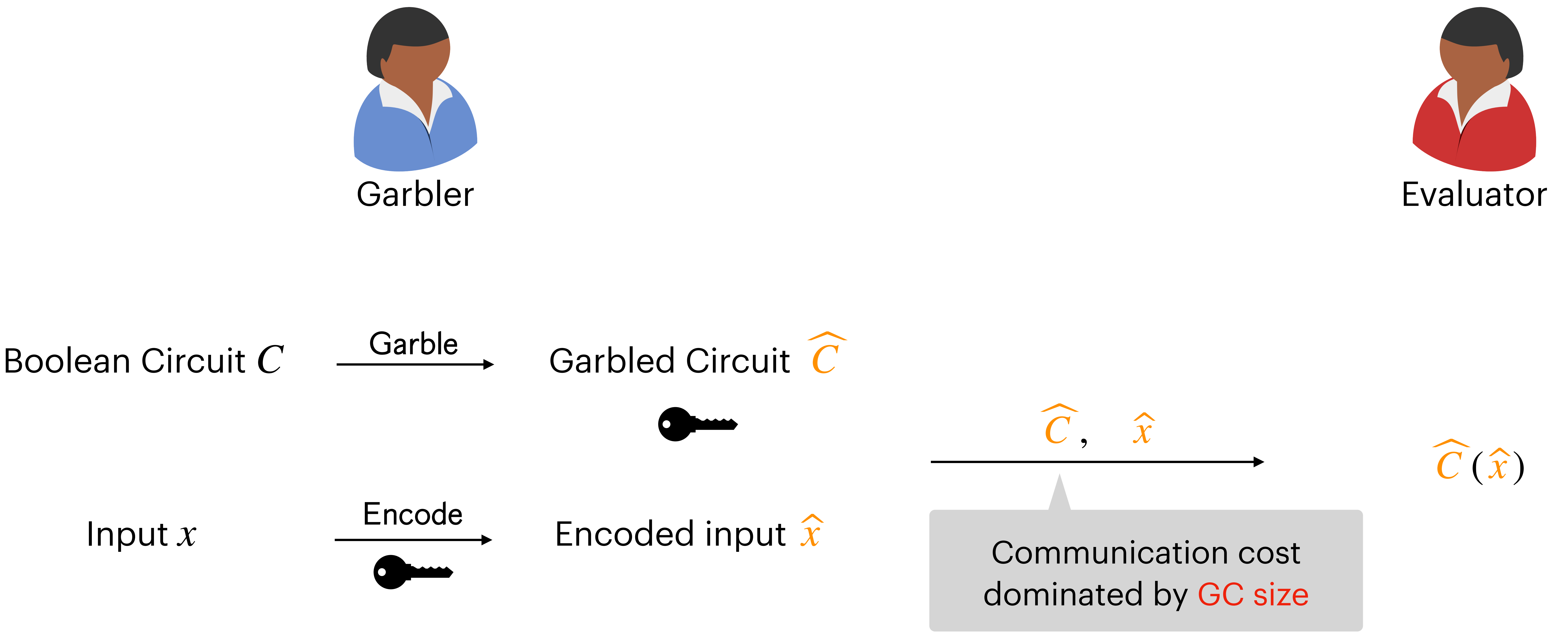
$\xrightarrow{\widehat{C},\ \hat{x}}$ $\widehat{C}(\hat{x})$

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

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

Garbled Circuits

[Yao’86]



Garbler

Evaluator

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

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

$\xrightarrow{\widehat{C},\ \hat{x}}$

Communication cost dominated by GC size

$\widehat{C}(\hat{x})$

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

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

Garbled Circuits

[Yao'86]

Garbler

Evaluator

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

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

$\xrightarrow{\widehat{C},\ \hat{x}}$ $\widehat{C}(\hat{x})$

Communication cost dominated by GC size

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

Public circuit $\Longrightarrow$ $\widehat{C}$ can be smaller than C

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

Garbled Circuits

[Yao'86]

Garbler

Evaluator

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

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

$\xrightarrow{\widehat{C},\ \hat{x}}$ $\widehat{C}(\hat{x})$

Communication cost dominated by GC size

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

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

Public circuit $\Longrightarrow$ $\widehat{C}$ can be smaller than C

Rate: $\dfrac{\text{Number of gates in } C}{\text{Size of } \widehat{C} \text{ in bits}}$

Higher rate $\Longrightarrow$ smaller garbled circuits

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] [Koleshnikov-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] [Koleshnikov-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] [Koleshnikov-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] [Koleshnikov-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

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

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

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

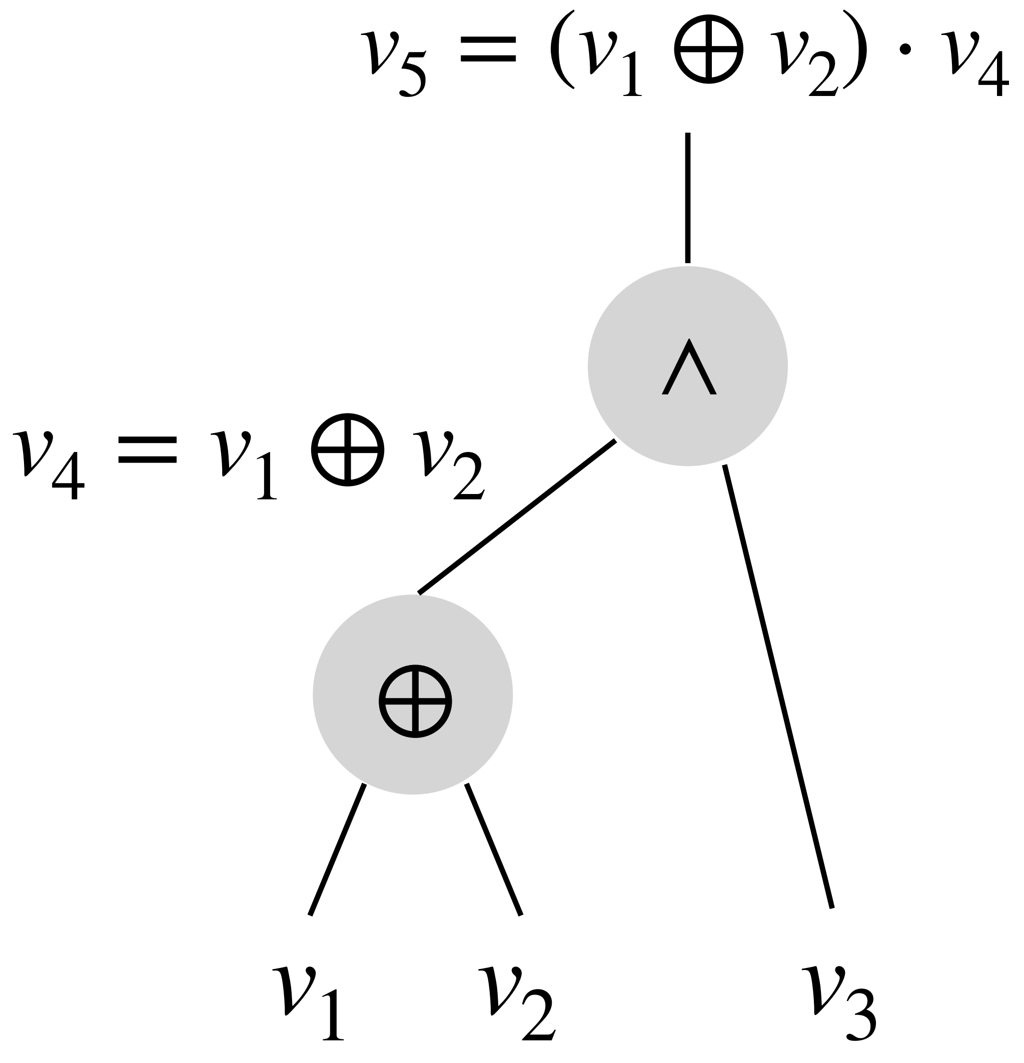
Assuming **Power-DDH** and a **Tweakable Correlation Robust Hash** function, there exists a garbling scheme that garbles a layered boolean circuit C into $\widehat{C}$ such that

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

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

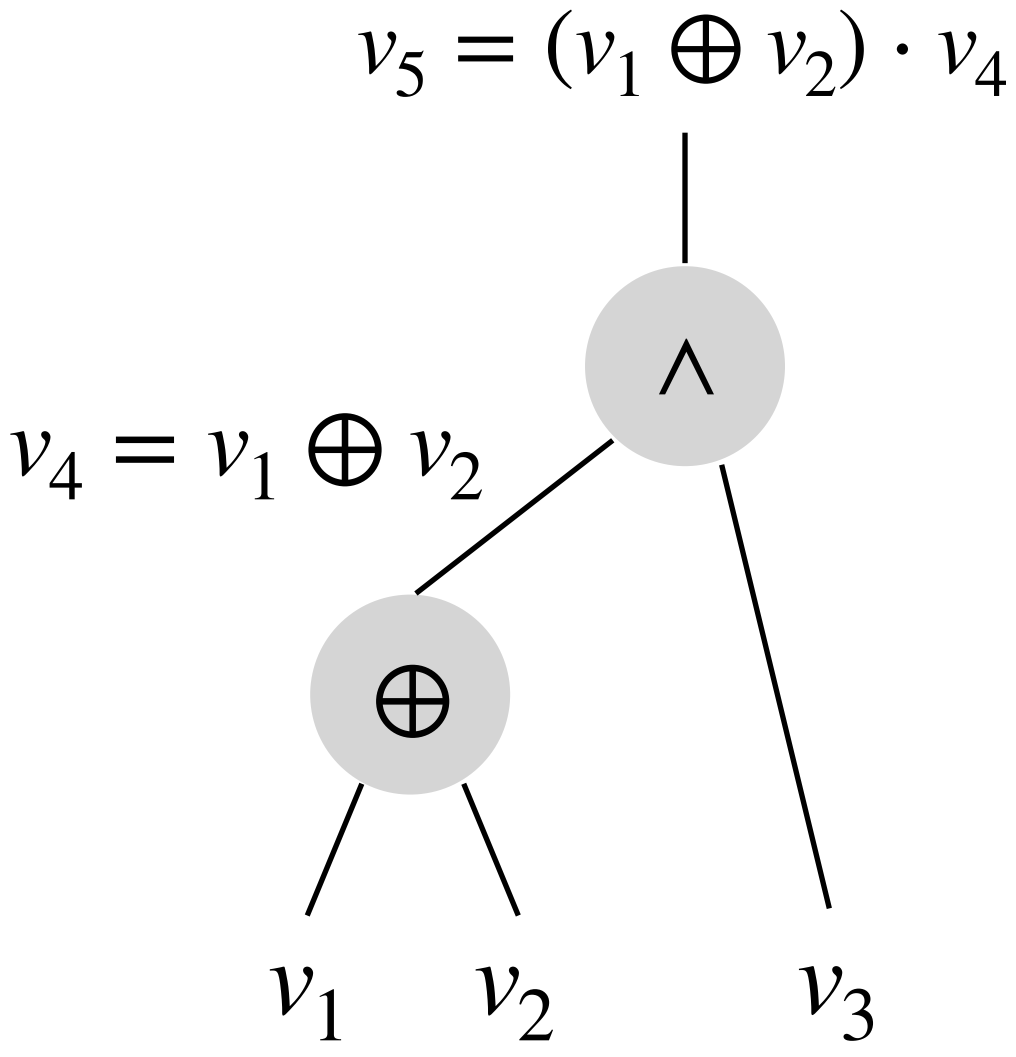
$o(\lambda)$-bits per gate scheme from assumptions not known to imply FHE

Template for Garbling Circuits

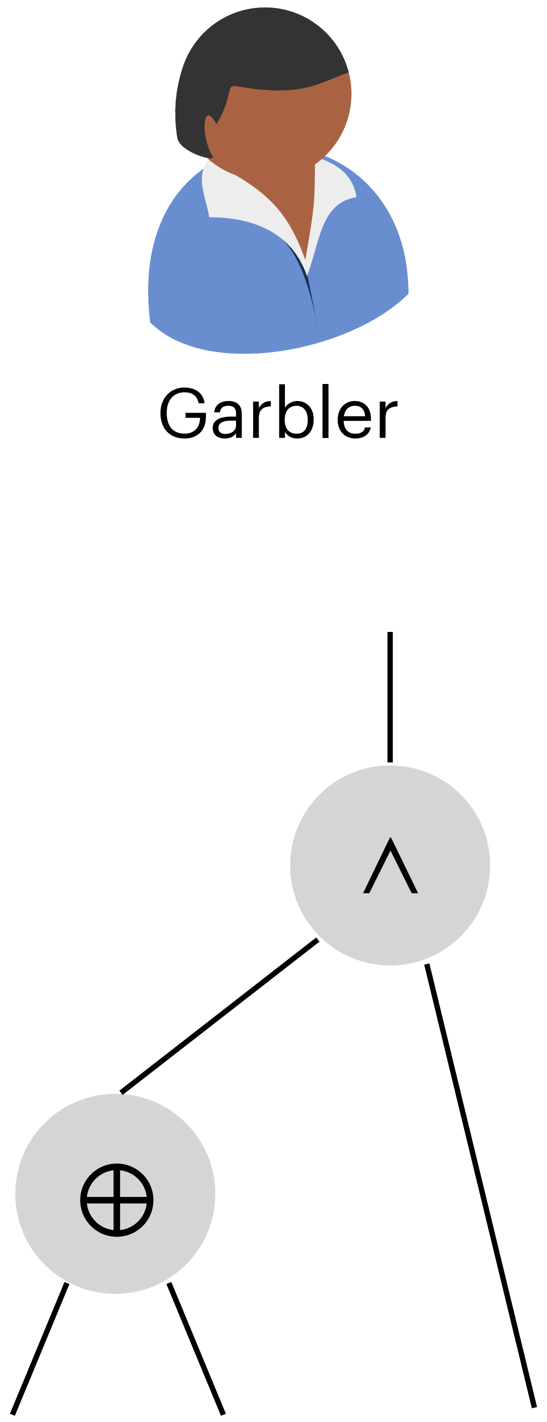


Boolean Circuit

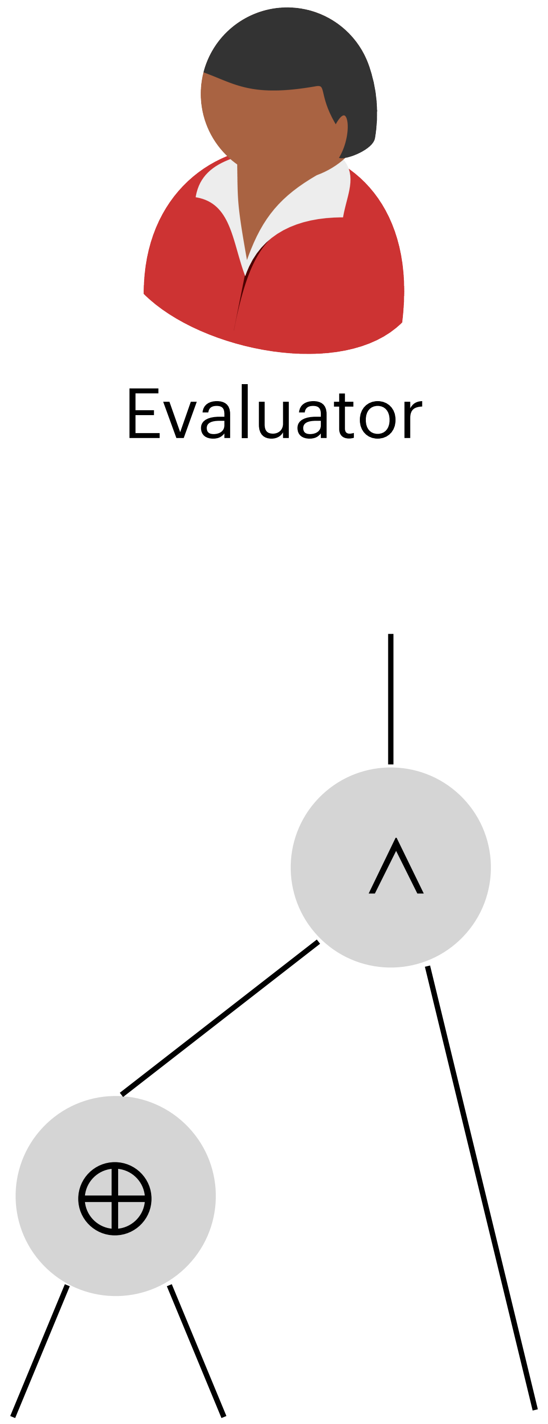
Template for Garbling Circuits



Boolean Circuit

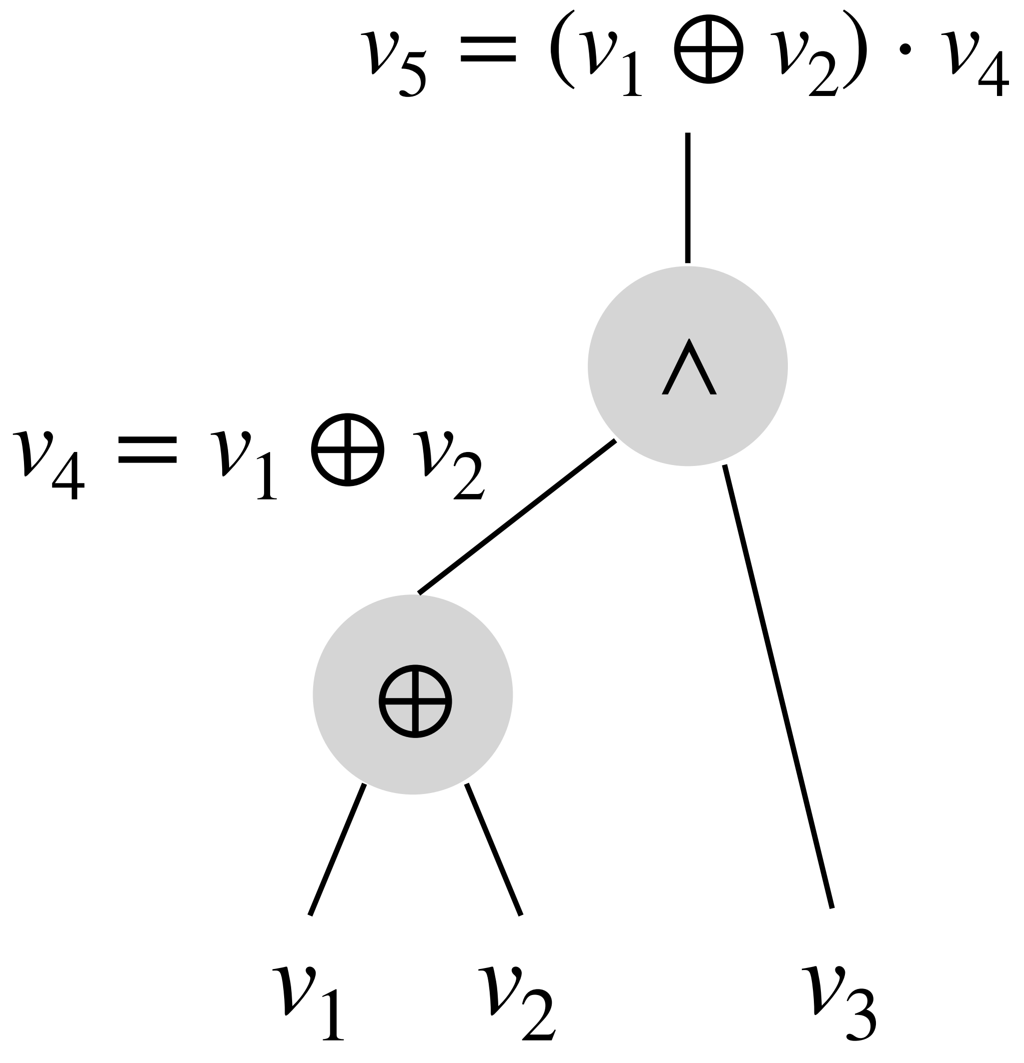


Garbler

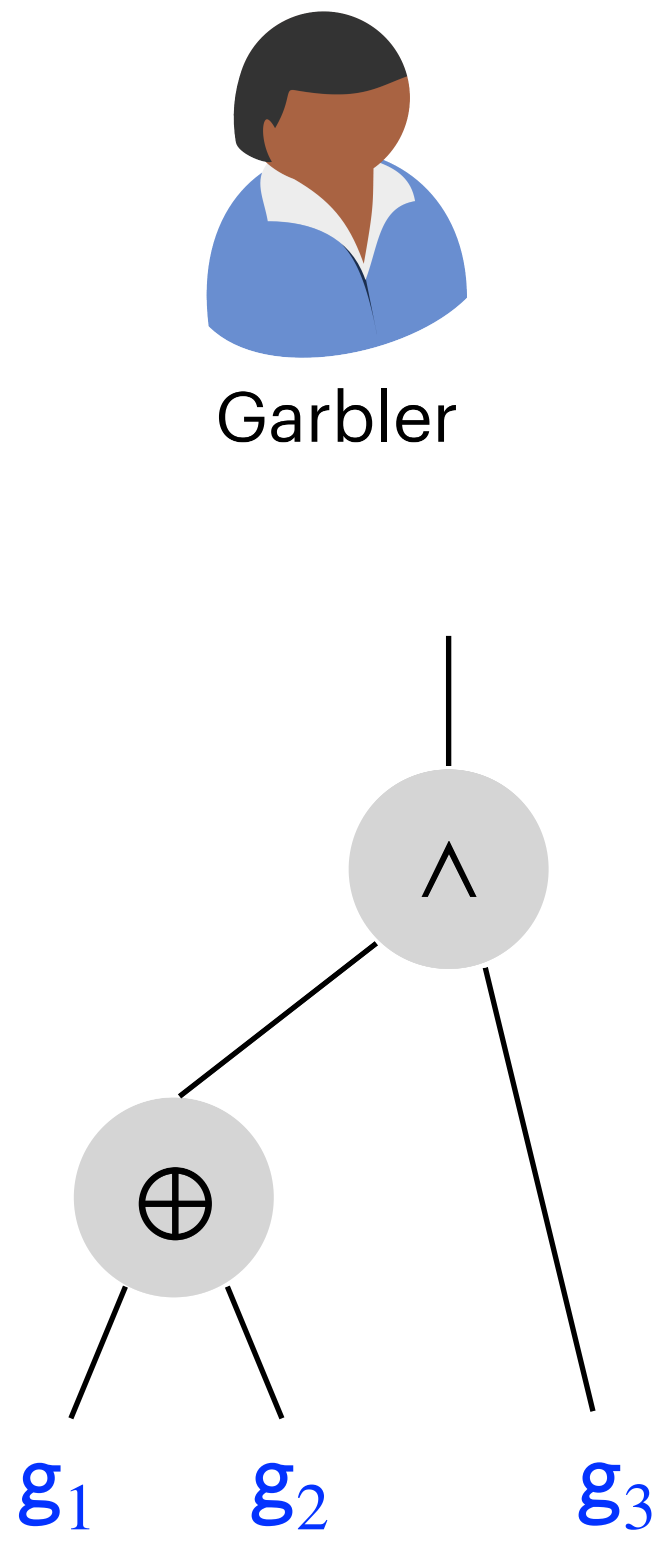


Evaluator

Template for Garbling Circuits

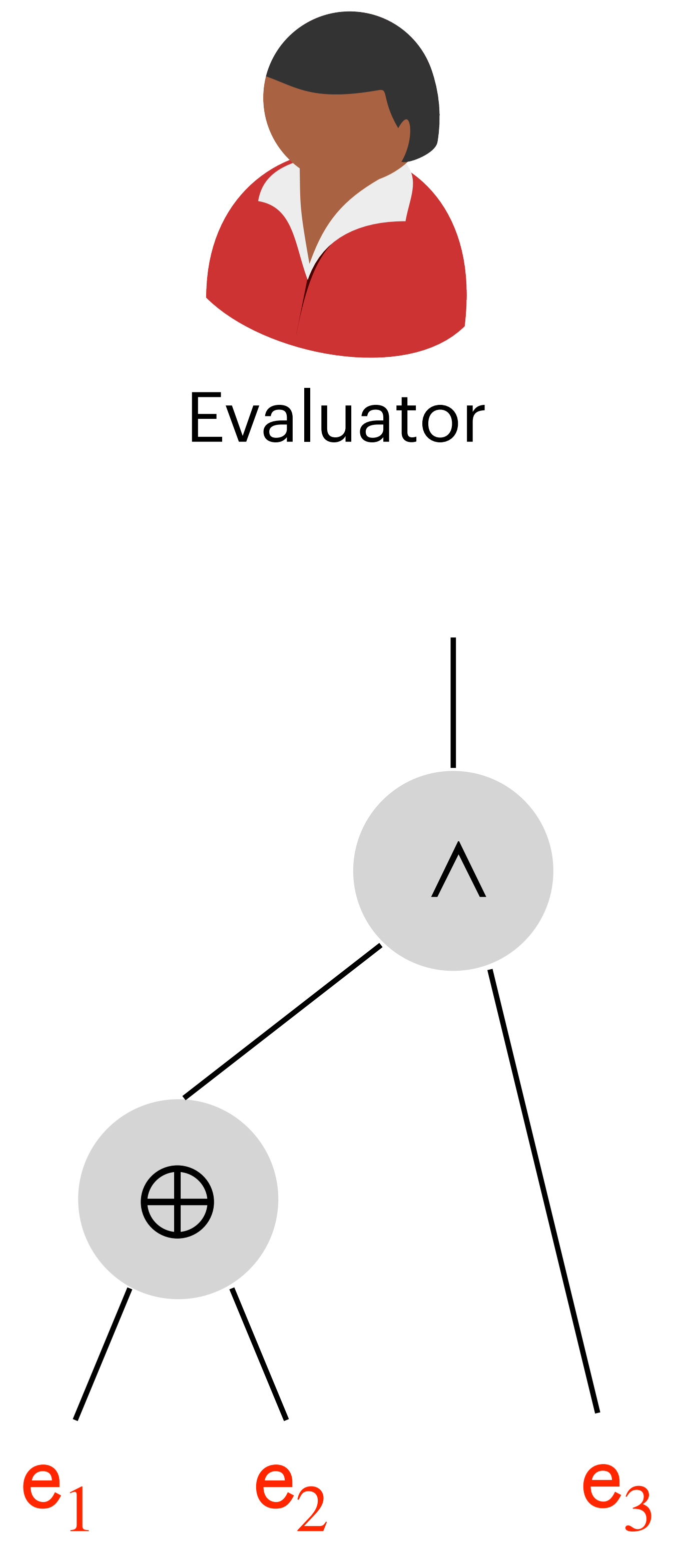


Boolean Circuit

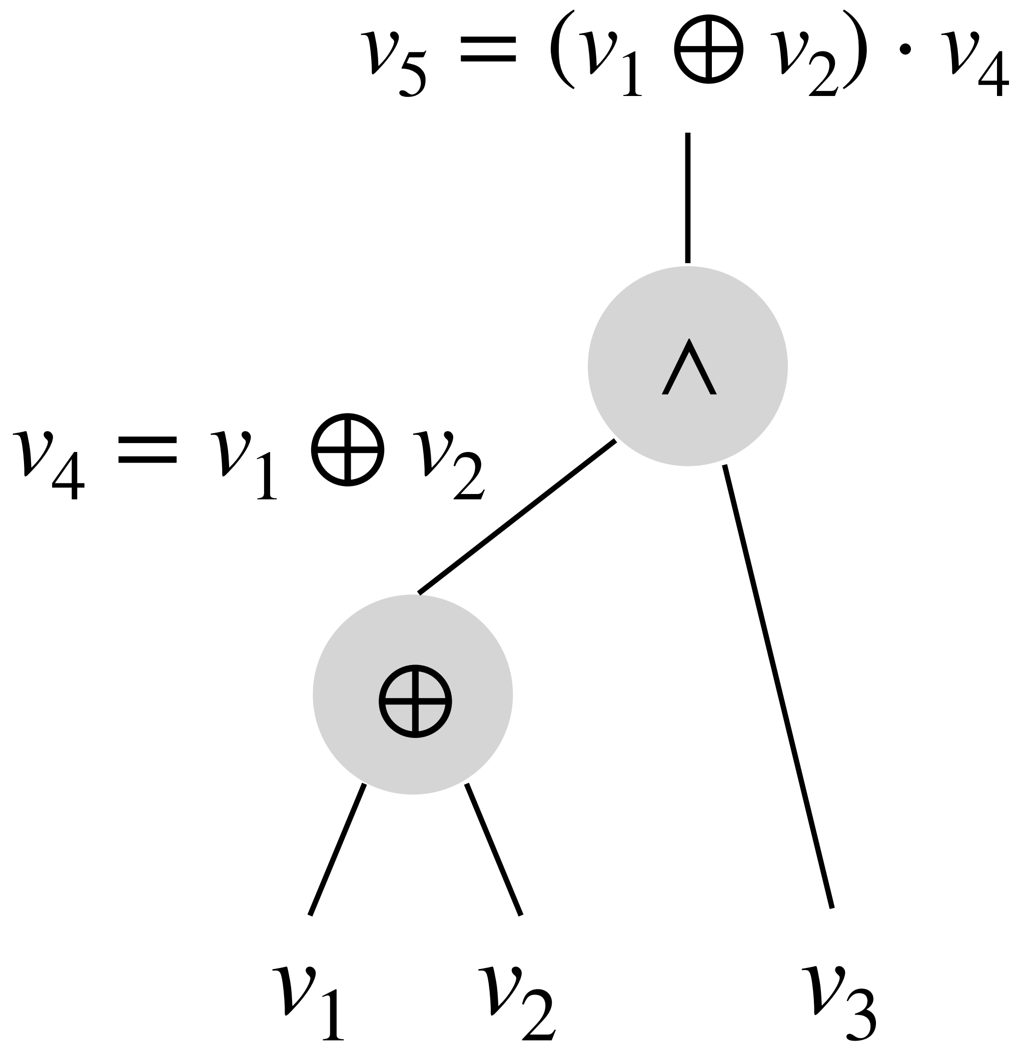


Invariant

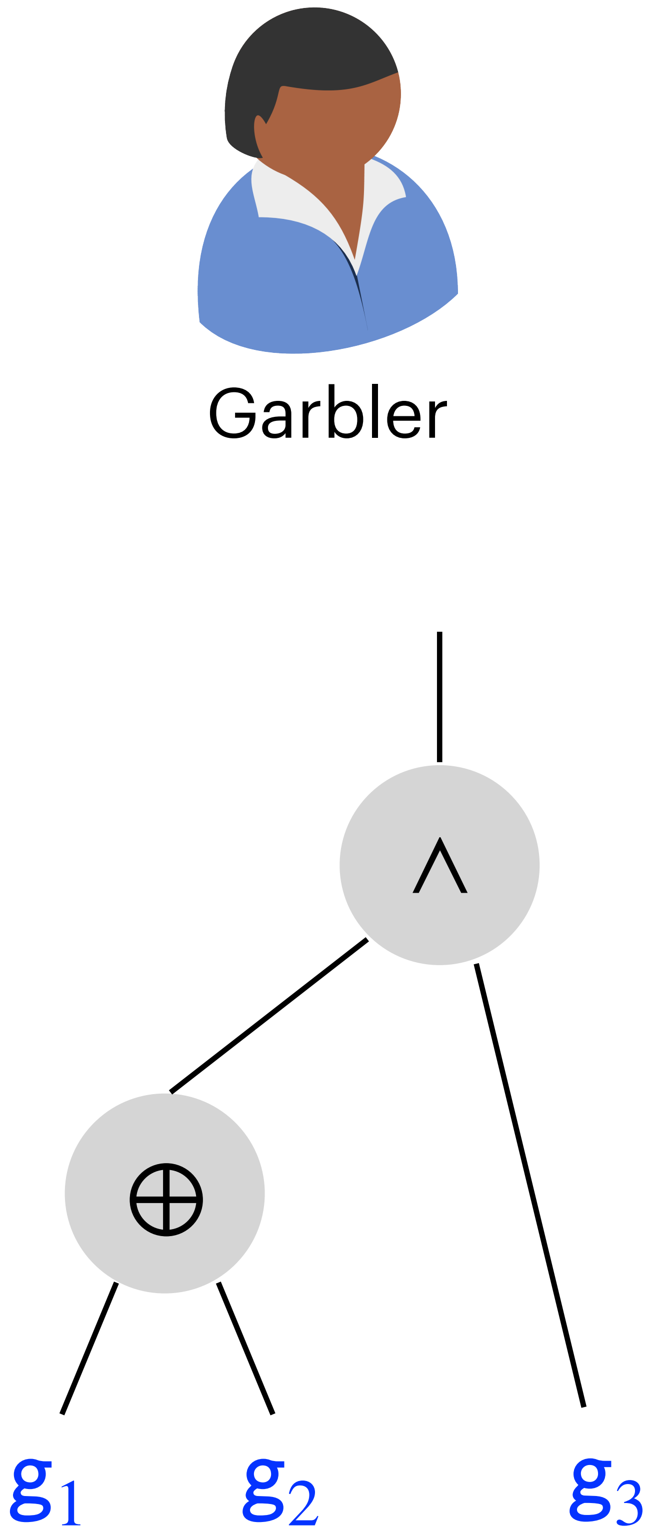
$g_i \oplus e_i = v_i$



Template for Garbling Circuits

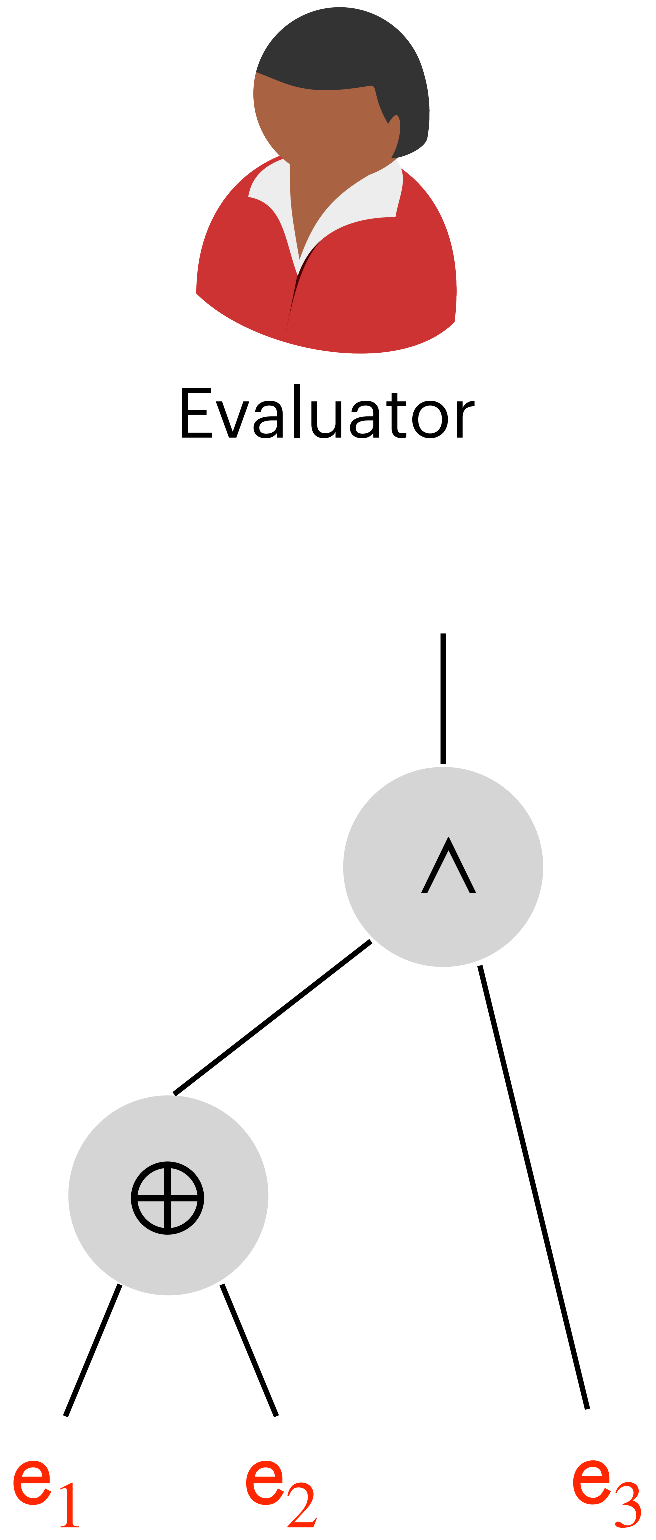


Boolean Circuit



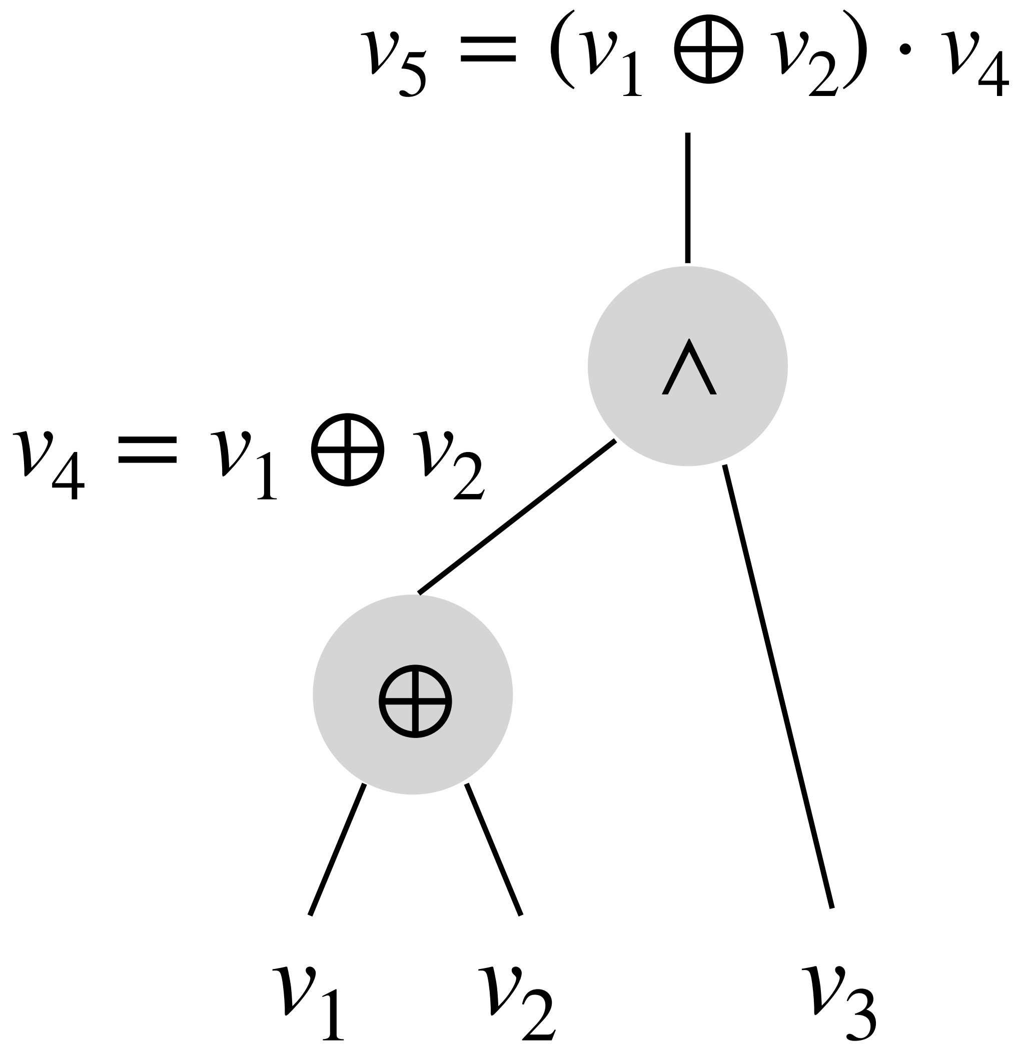
Invariant

$g_i \oplus e_i = v_i$



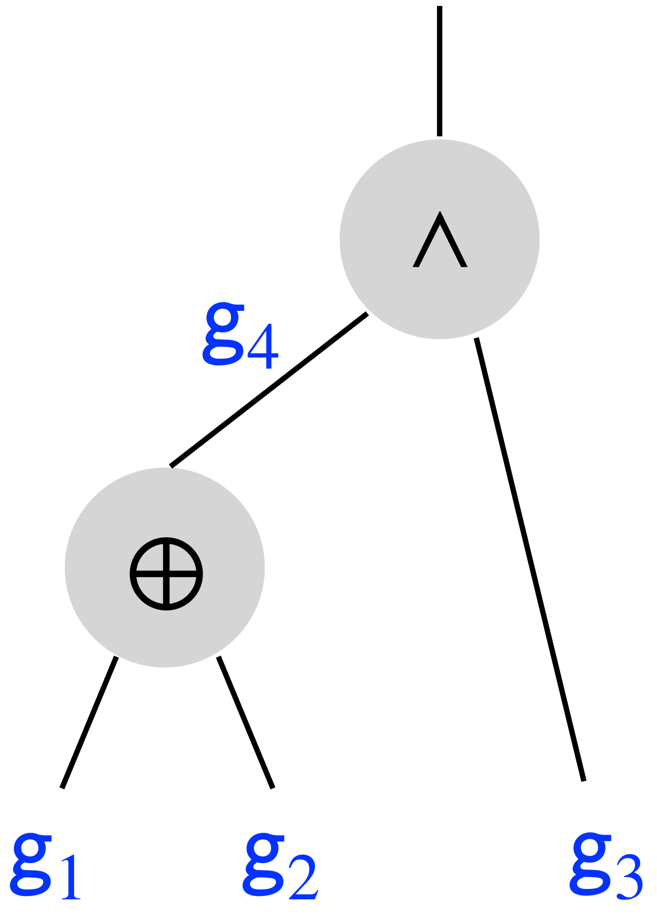
Garbled Circuit $\widehat{C}$

Template for Garbling Circuits



Boolean Circuit

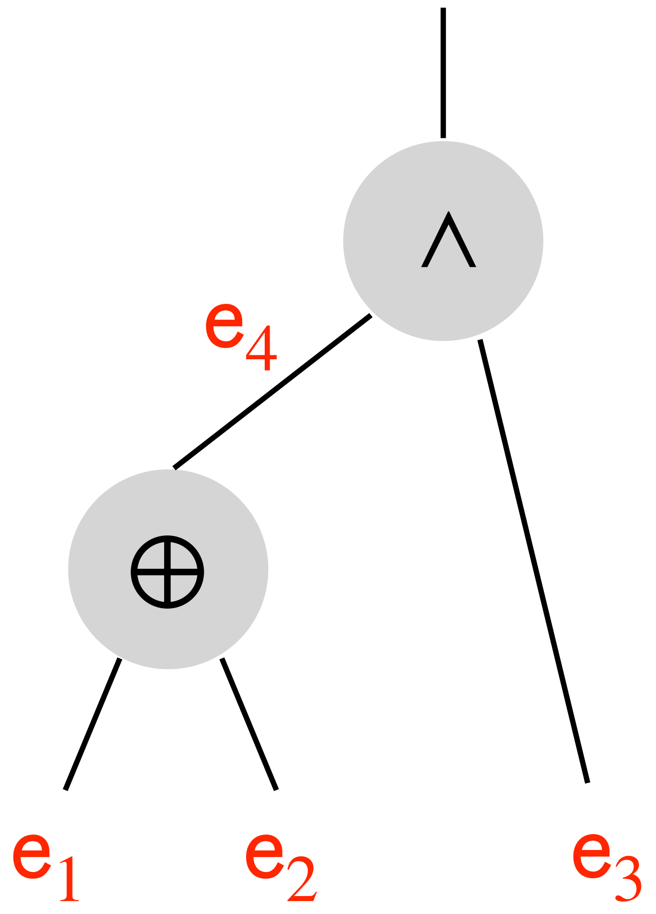
Garbler



Invariant

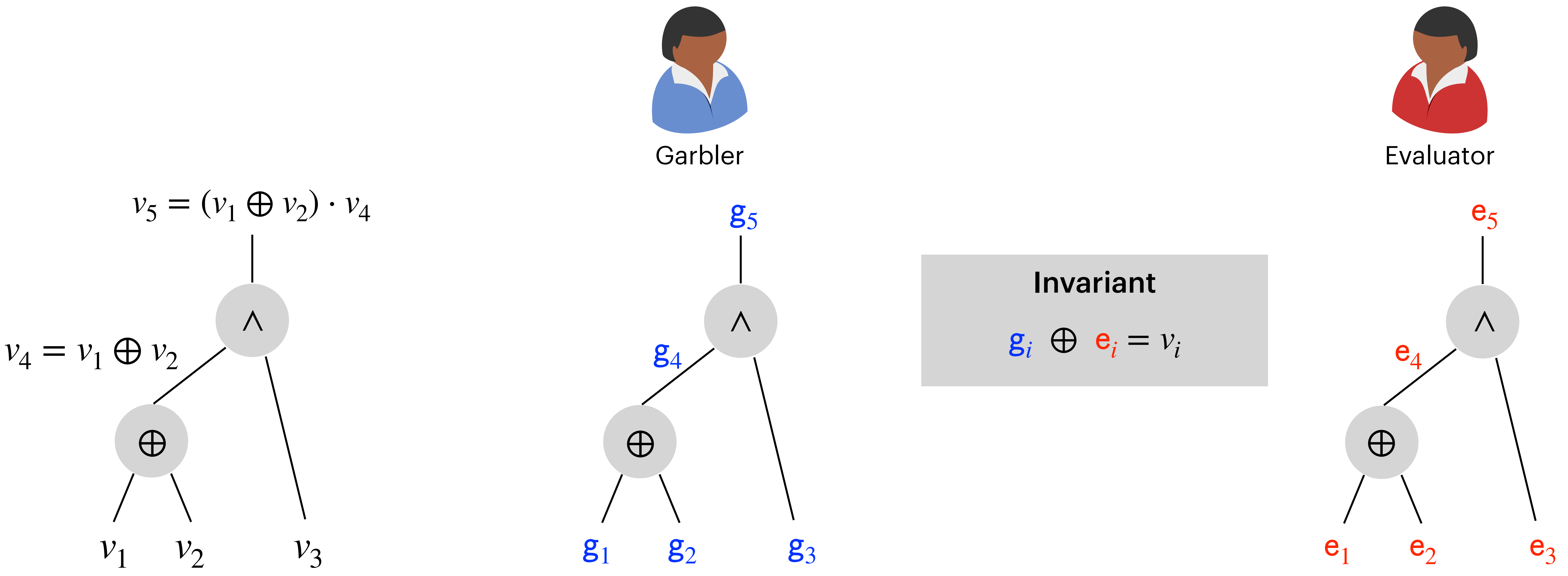
$g_i \oplus e_i = v_i$

Evaluator



Garbled Circuit $\widehat{C}$

Template for Garbling Circuits



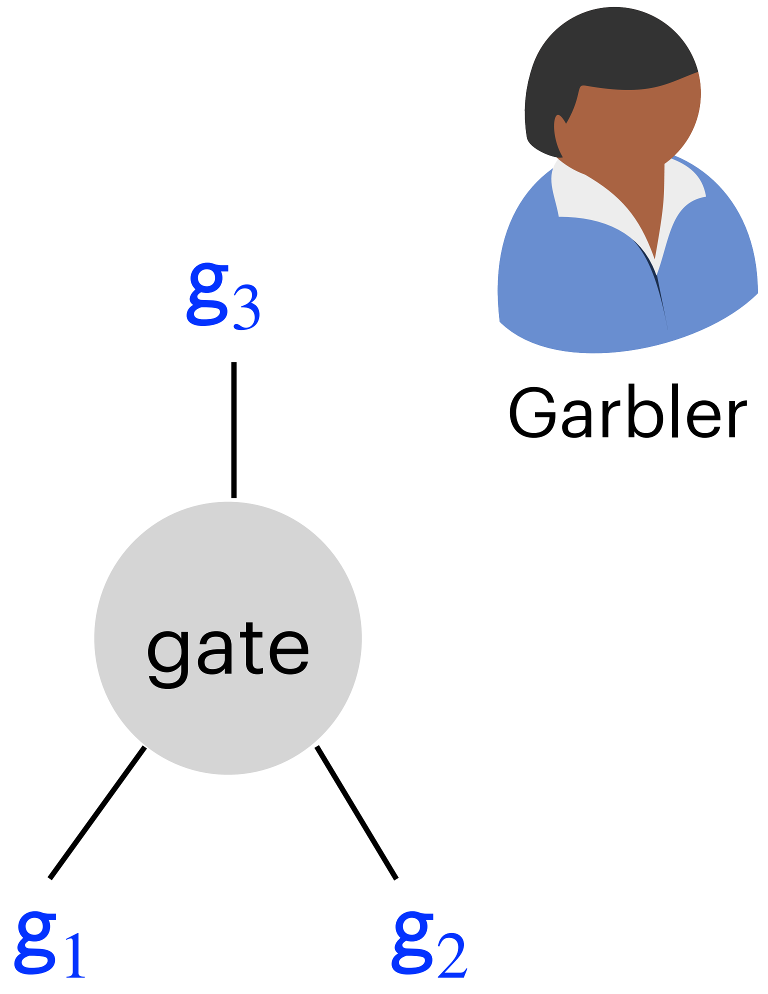
Invariant

$g_i \oplus e_i = v_i$

Boolean Circuit

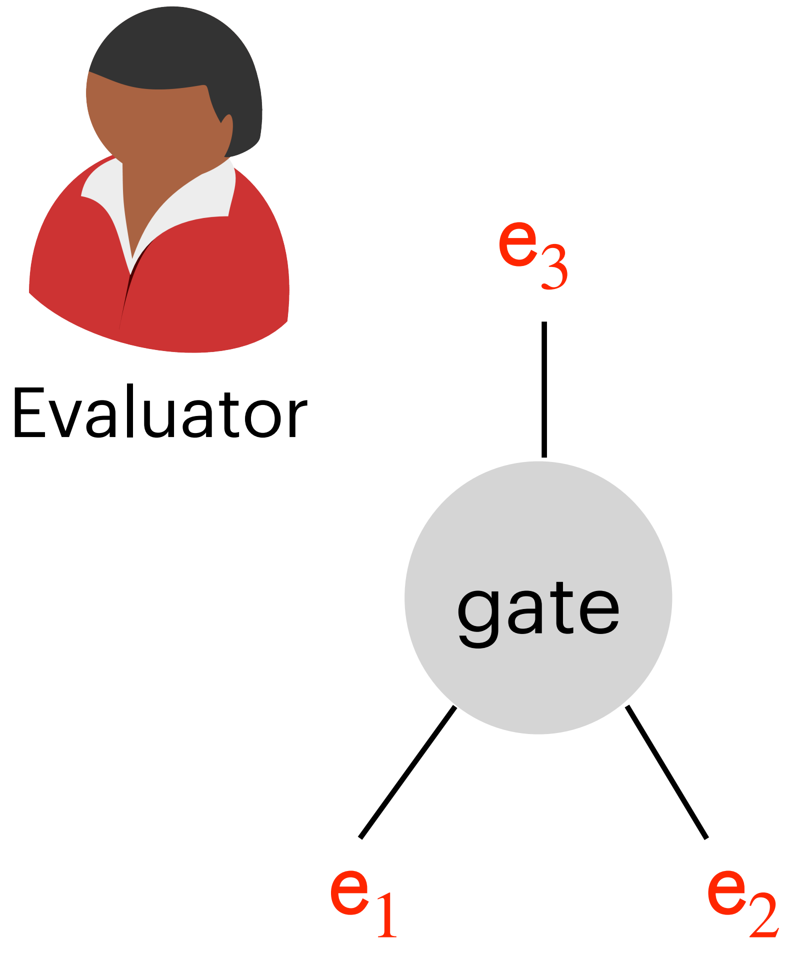
Garbled Circuit $\widehat{C}$

Template for Garbling Circuits

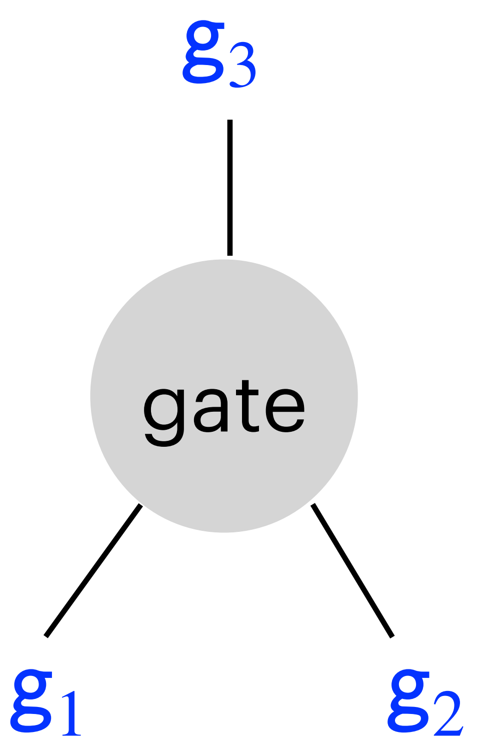


Invariant

$$g_i \oplus e_i = v_i$$



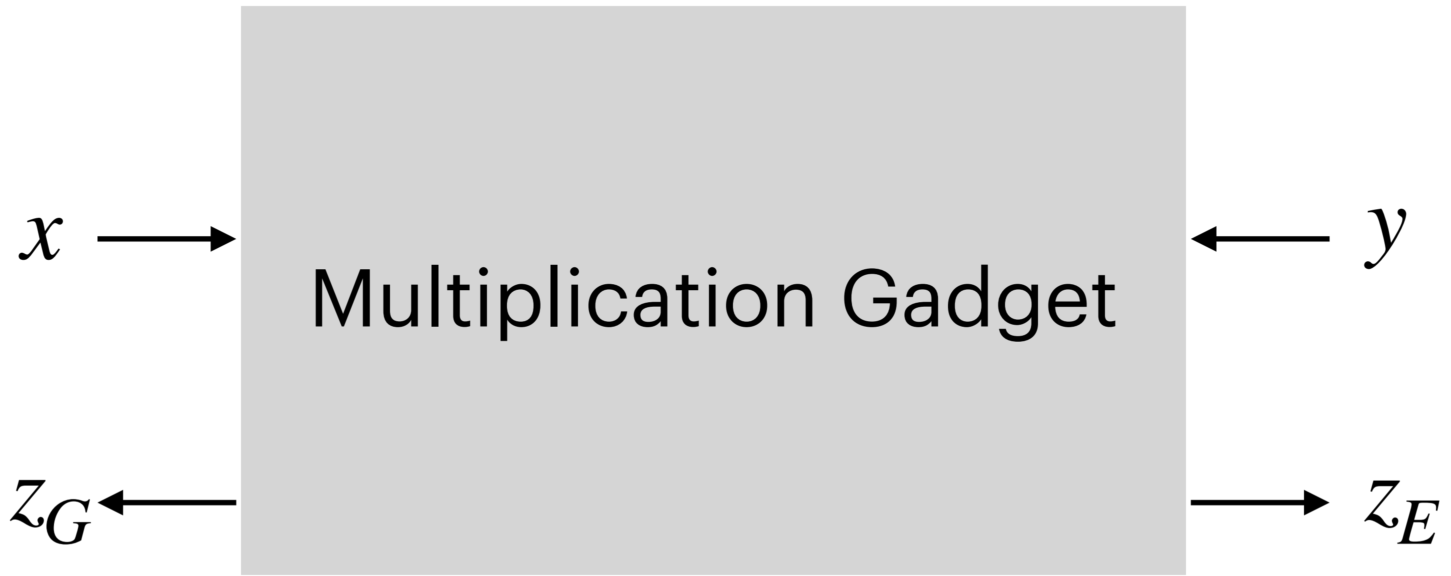
Template for Garbling Circuits



Garbler

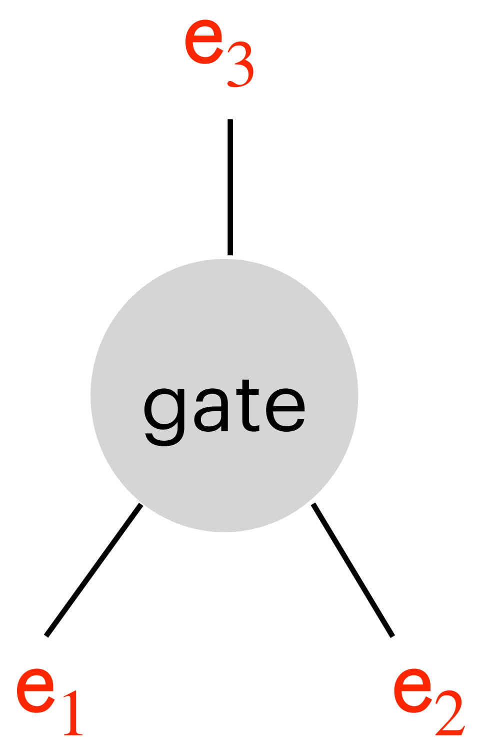
Invariant

$$g_i \oplus e_i = v_i$$

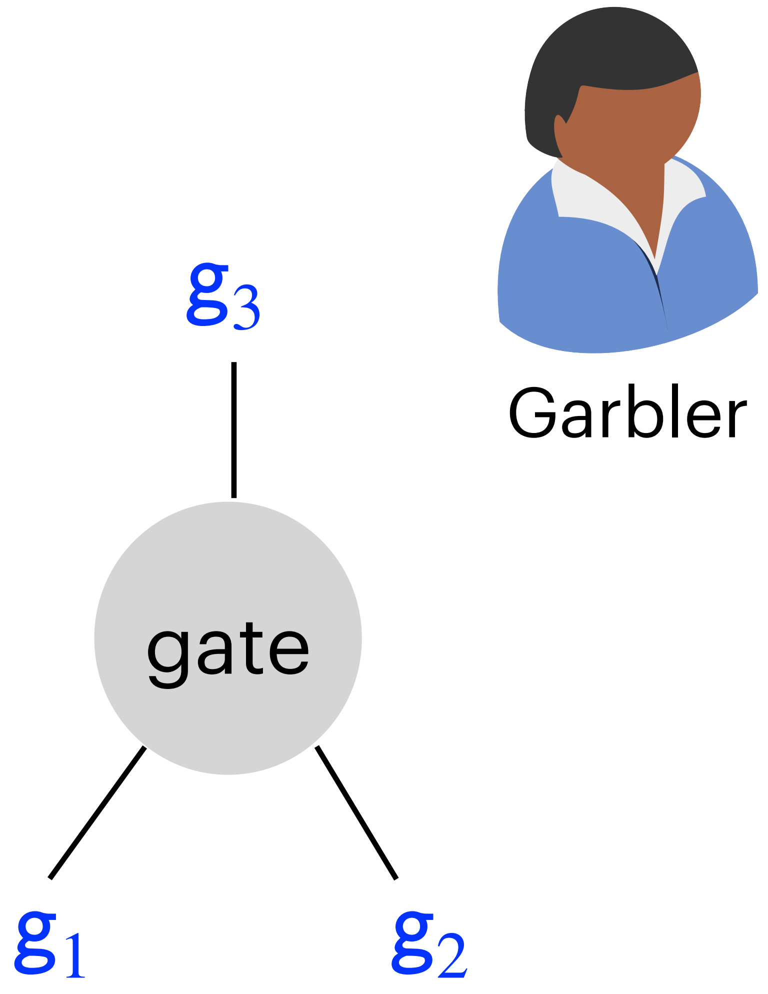


$$z_G \oplus z_E = xy$$

Evaluator

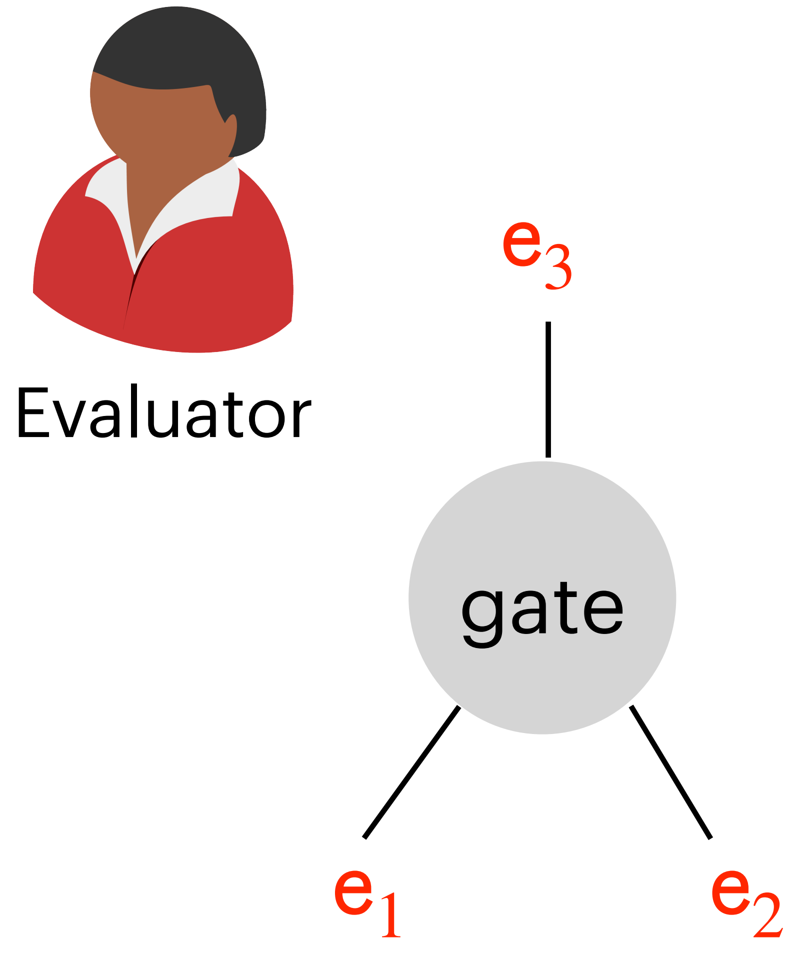


Template for Garbling Circuits



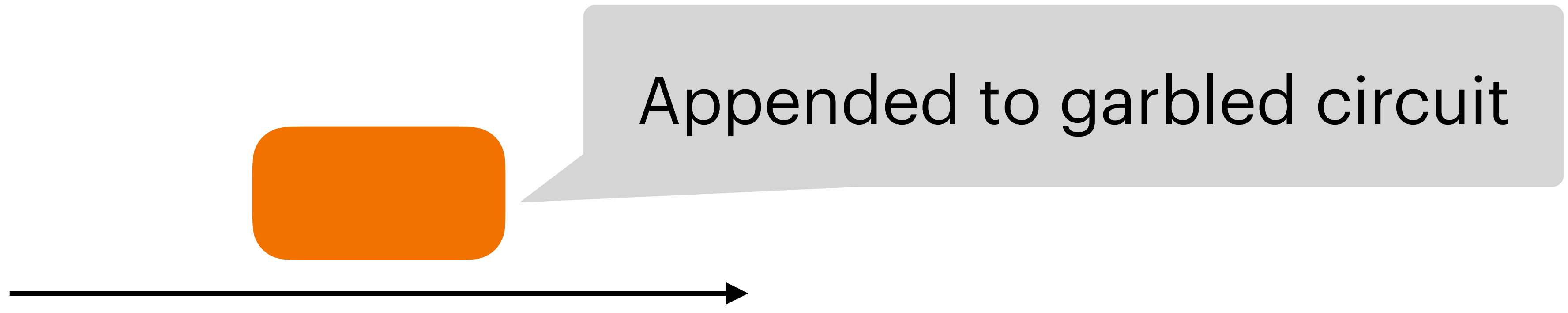
Invariant

$$g_i \oplus e_i = v_i$$



$$z_G \oplus z_E = xy$$

Instantiation:



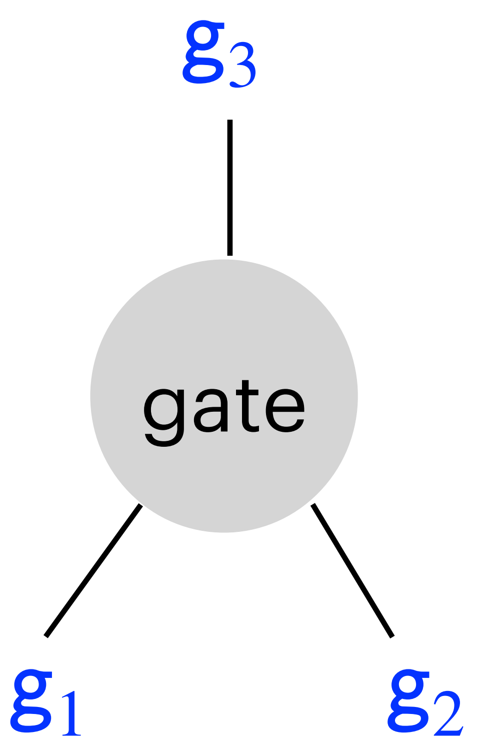
Appended to garbled circuit

Template for Garbling Circuits

Δ

Known to the Garbler

Garbler



g_3

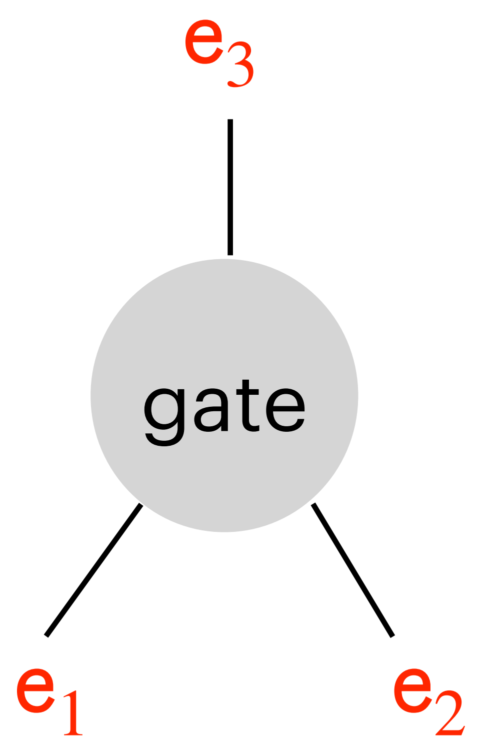
gate

g_1 g_2

Invariant

$g_i \oplus e_i = v_i$

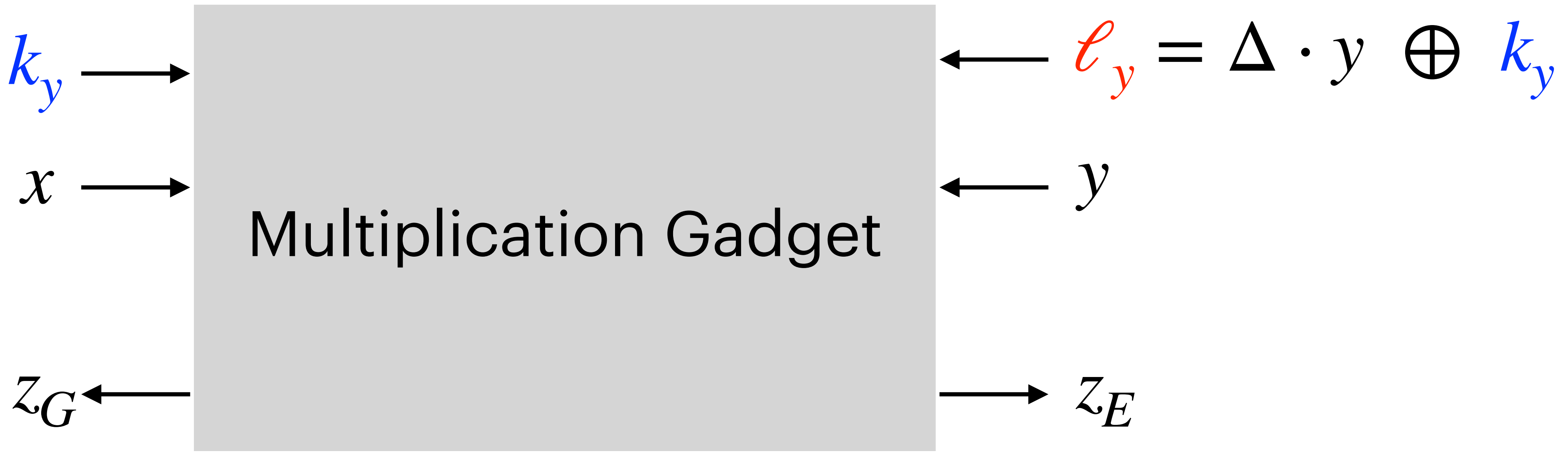
Evaluator



e_3

gate

e_1 e_2



k_y

x

z_G

Multiplication Gadget

$\ell_y = \Delta \cdot y \oplus k_y$

y

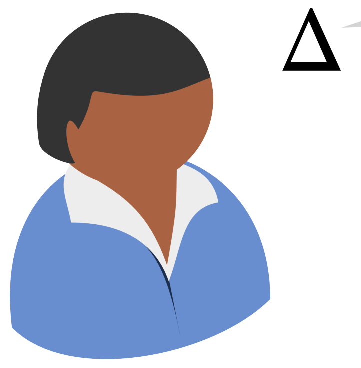
z_E

$z_G \oplus z_E = xy$

Instantiation:

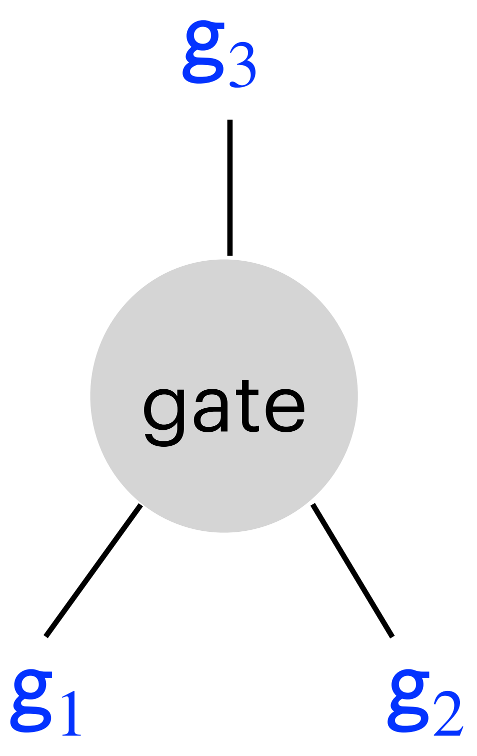
Appended to garbled circuit

Template for Garbling Circuits



Known to the Garbler

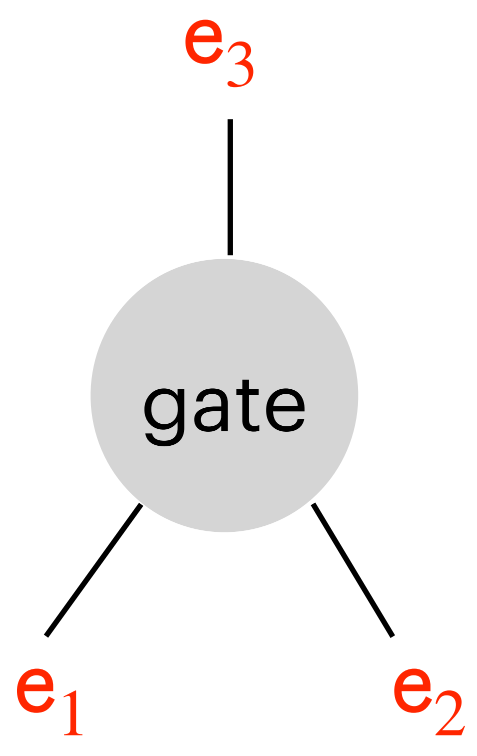
Garbler

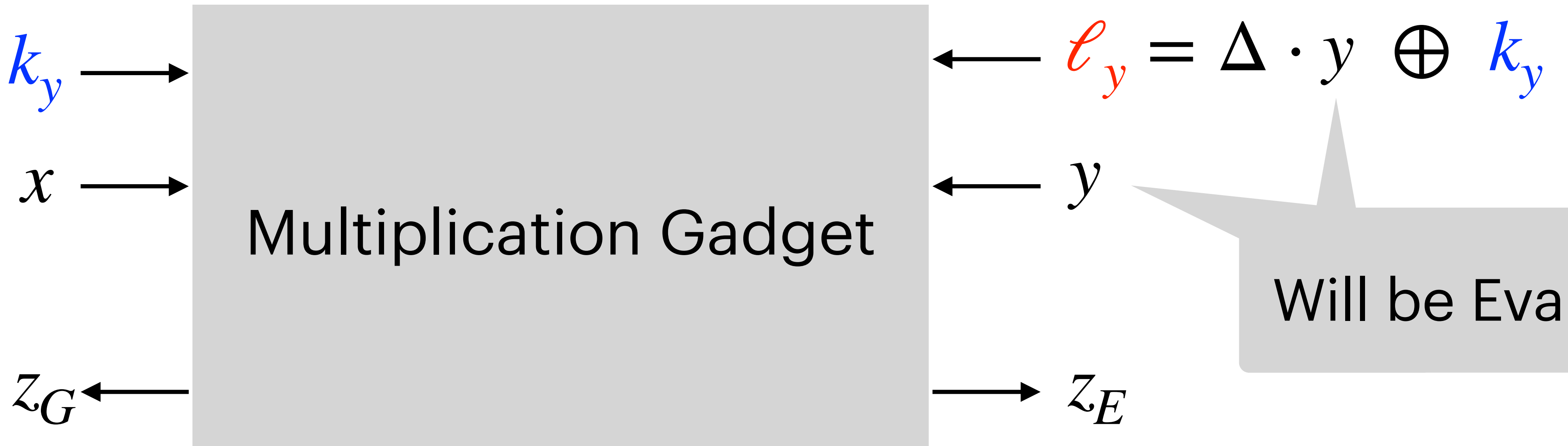


Invariant

$g_i \oplus e_i = v_i$

Evaluator





Will be Evaluator's share e

$z_G \oplus z_E = xy$

Instantiation:

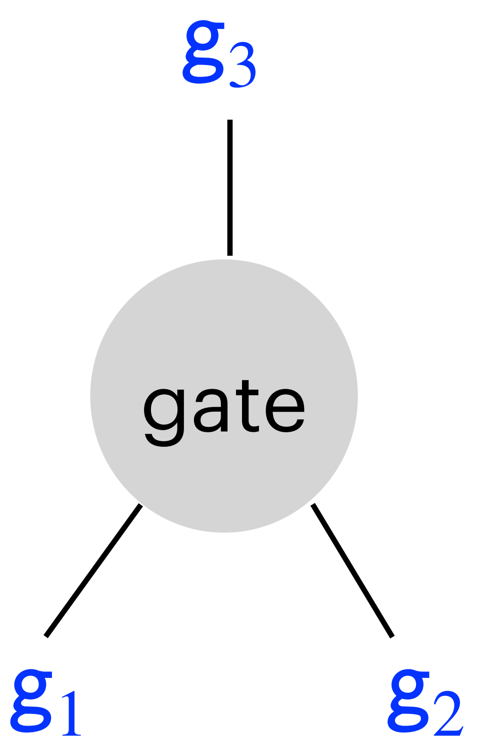
Appended to garbled circuit

Template for Garbling Circuits

Known to the Garbler

Δ

Garbler

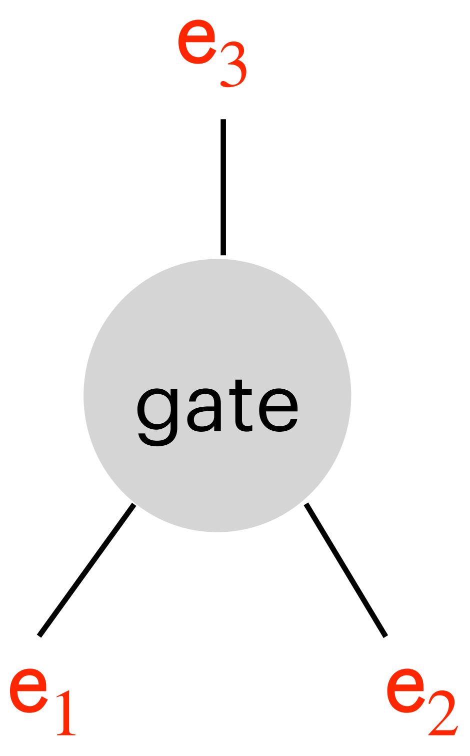


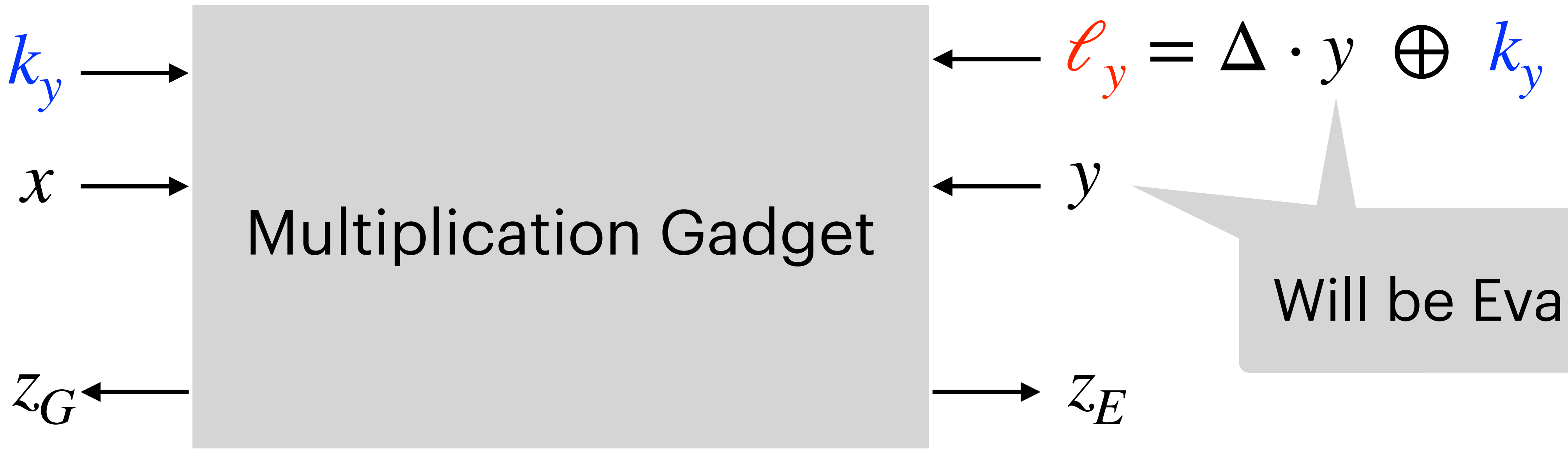
Invariant

$$g_i \oplus e_i = v_i$$

$$k_i \oplus \ell_i = \Delta \cdot e_i$$

Evaluator





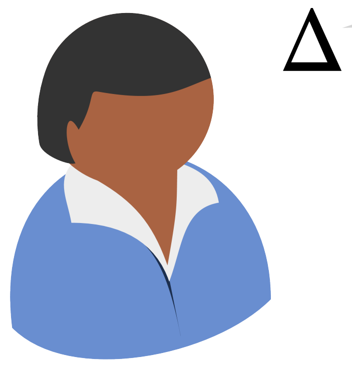
Will be Evaluator’s share e

$$z_G \oplus z_E = xy$$

Instantiation:

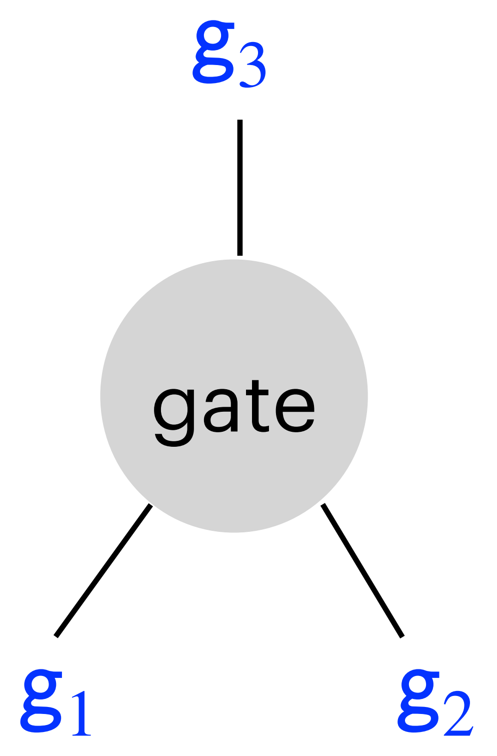
Appended to garbled circuit

Template for Garbling Circuits



Known to the Garbler

Garbler

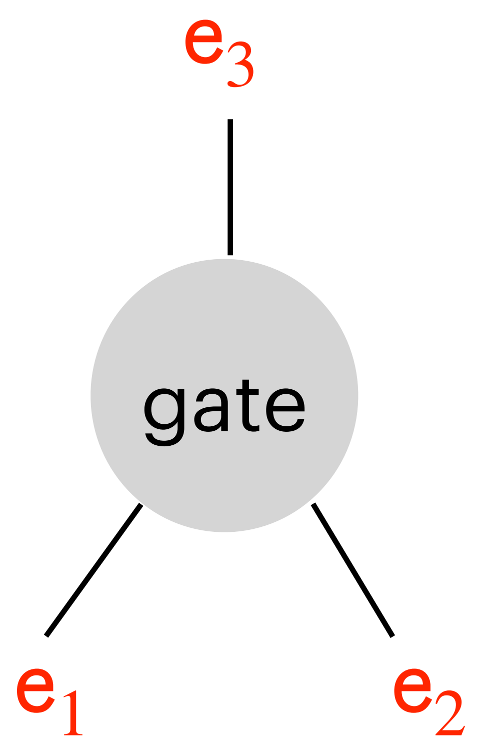


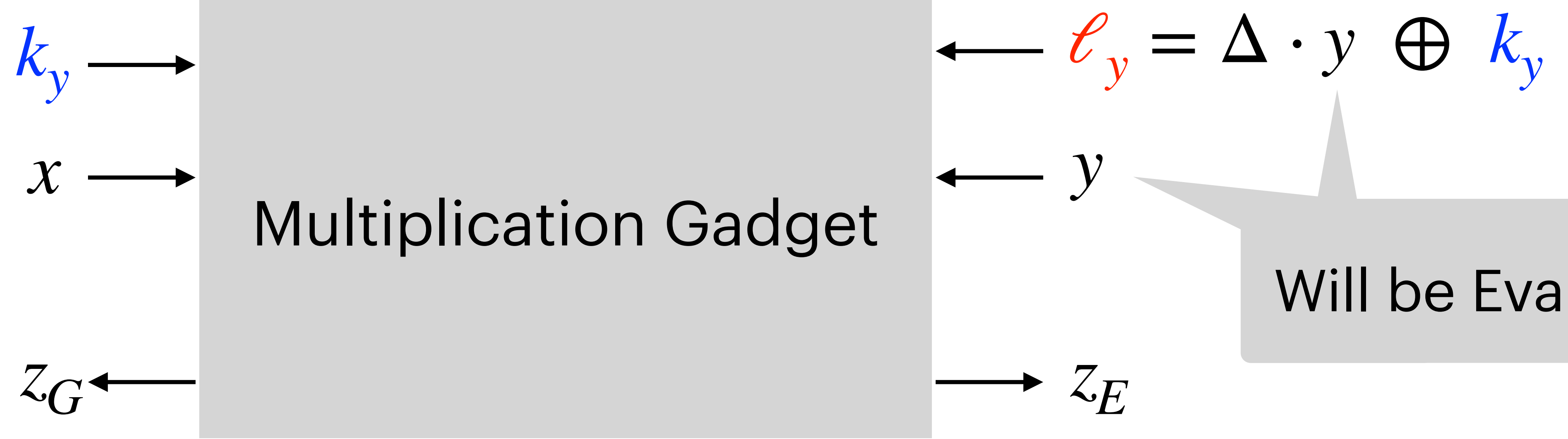
Invariant

$$g_i \oplus e_i = v_i$$

$$k_i \oplus \ell_i = \Delta \cdot e_i$$

Evaluator





Will be Evaluator's share e

$$z_G \oplus z_E = xy$$

Suffices for garbling,

$O(1)$ invocations per gate

Appended to garbled circuit

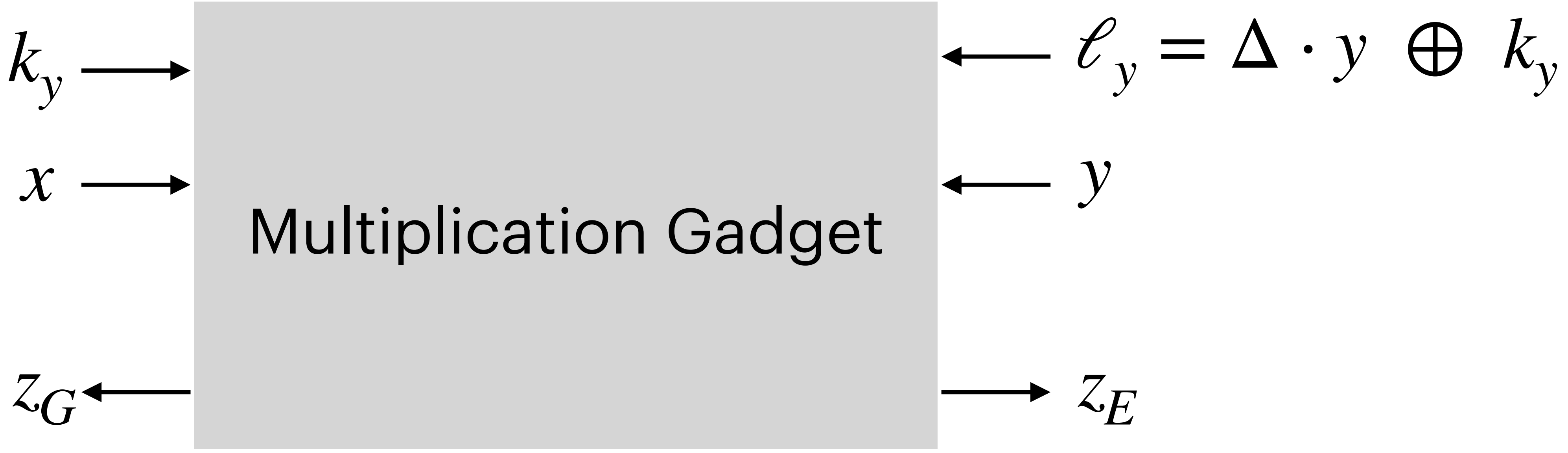
Instantiation:

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

Δ

Garbler

Evaluator



Multiplication Gadget

$k_y \rightarrow$

$x \rightarrow$

$z_G \leftarrow$

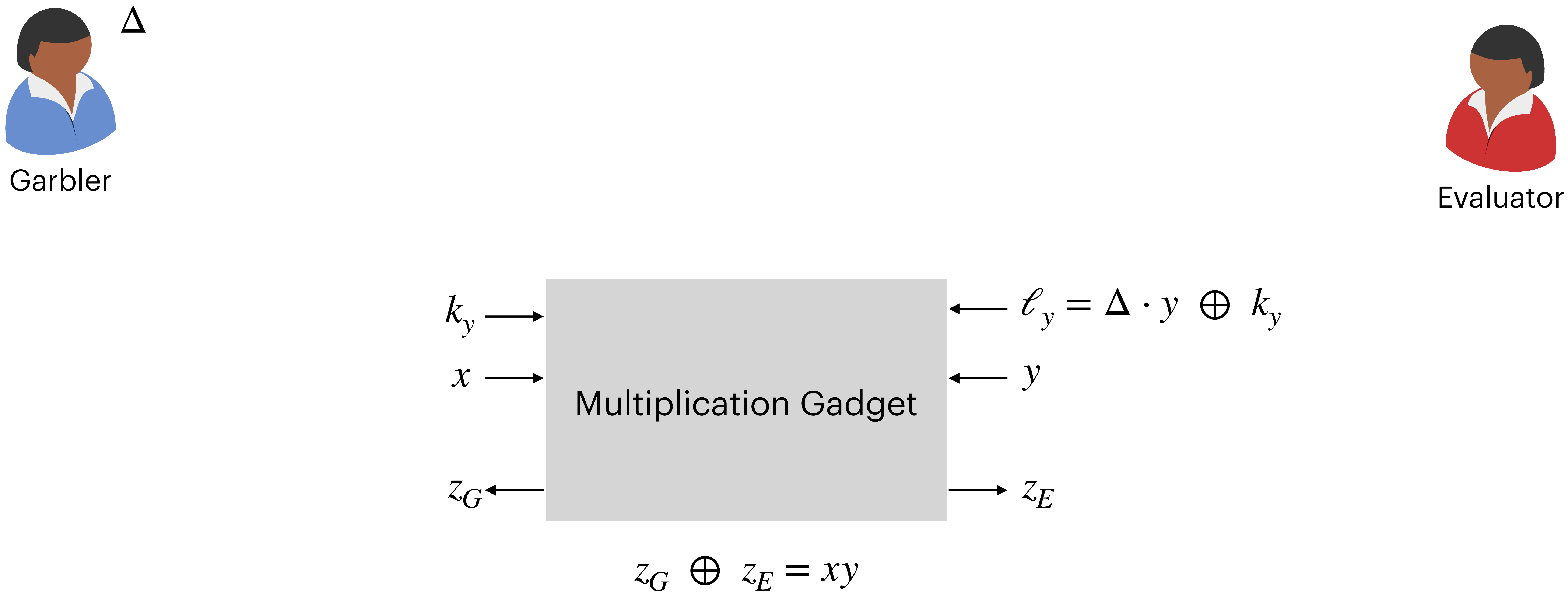
$\leftarrow \ell_y = \Delta \cdot y \oplus k_y$

$\leftarrow y$

$\rightarrow z_E$

$$z_G \oplus z_E = xy$$

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



Δ

Garbler

Evaluator

Multiplication Gadget

$k_y \rightarrow$

$x \rightarrow$

$z_G \leftarrow$

$\leftarrow \ell_y = \Delta \cdot y \oplus k_y$

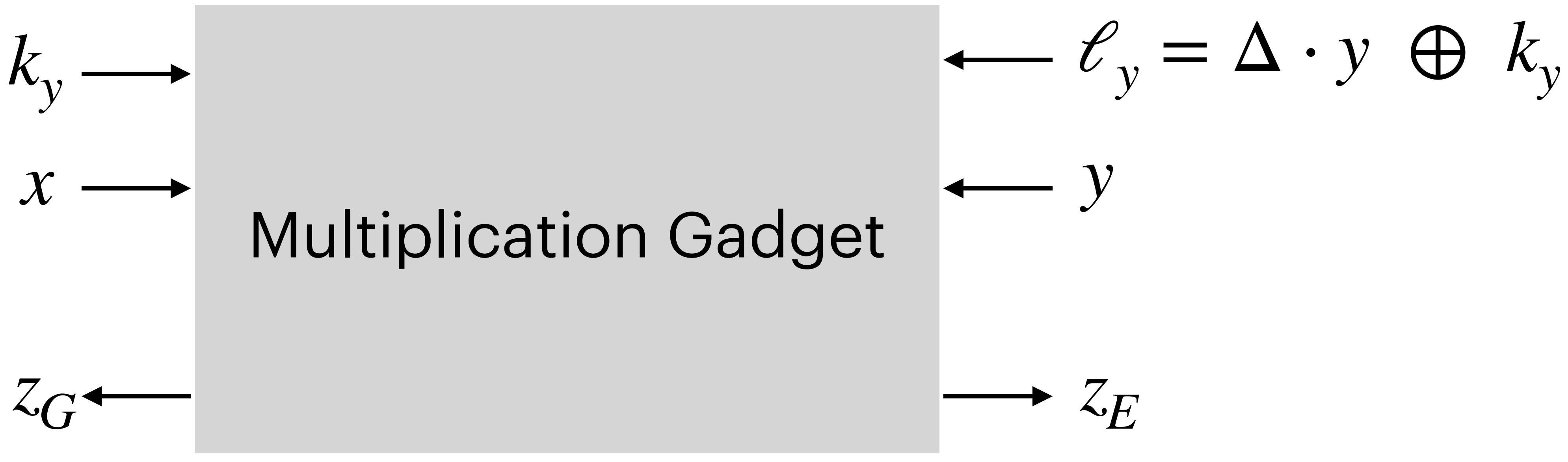
$\leftarrow y$

$\rightarrow z_E$

$z_G \oplus z_E = xy$

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

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



$$z_G \oplus z_E = xy$$

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

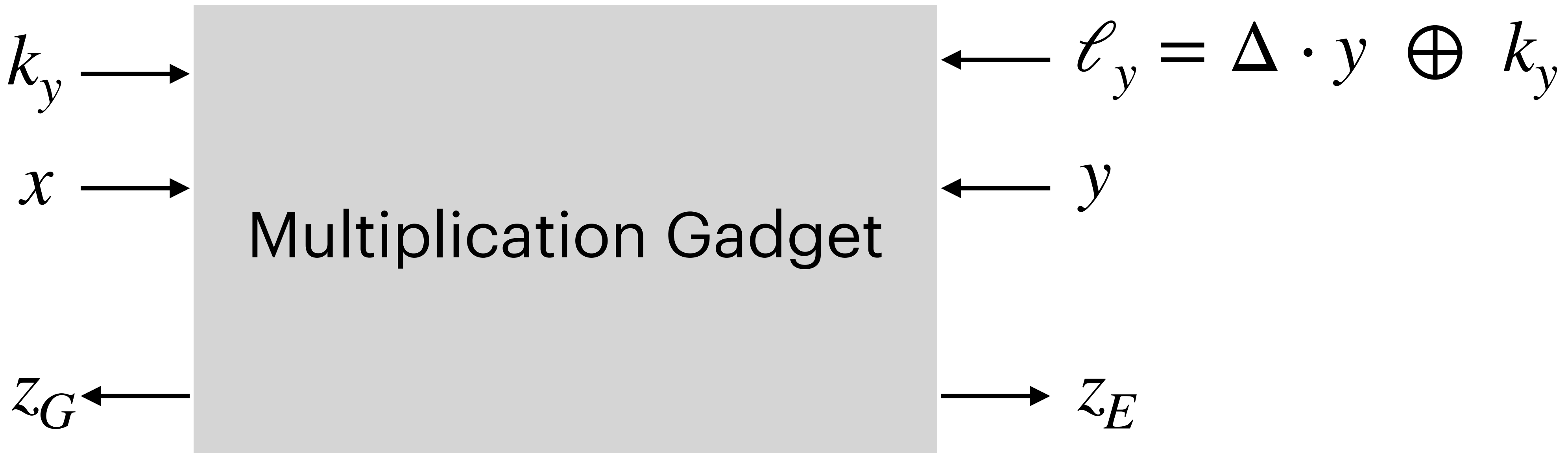
$\omega(1/\lambda)$**-Rate Garbling:** Requires instantiation with $o(\lambda)$-bit message

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

Δ

Garbler

Evaluator



$$z_G \oplus z_E = xy$$

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

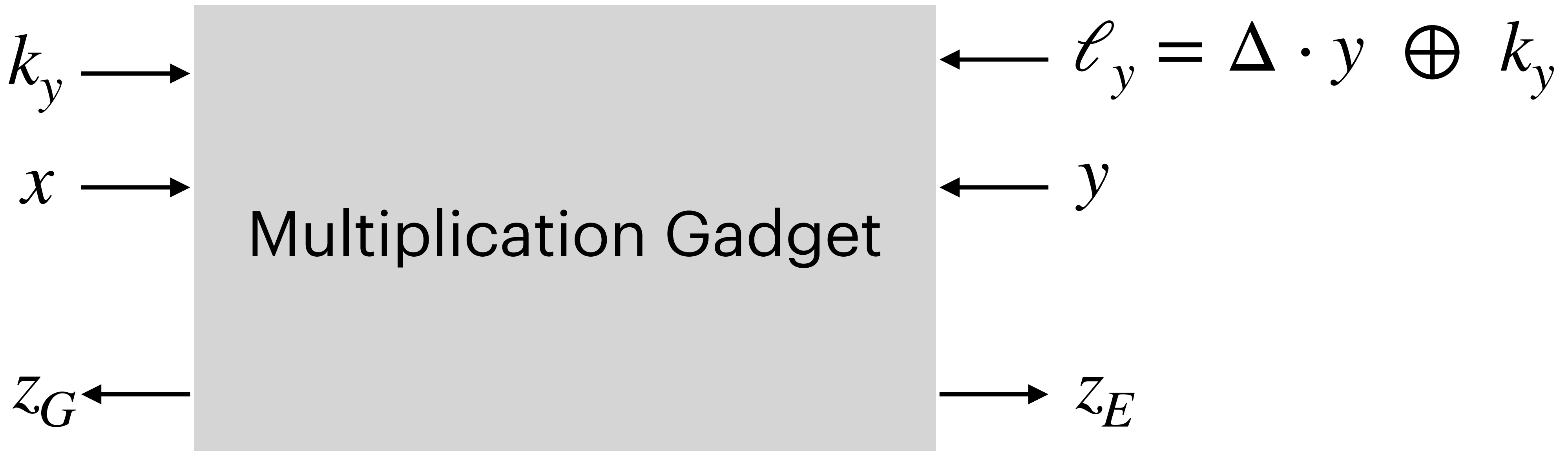
Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]

Δ

Garbler

Evaluator

Multiplication Gadget for Integers



$$z_G \oplus z_E = xy$$

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

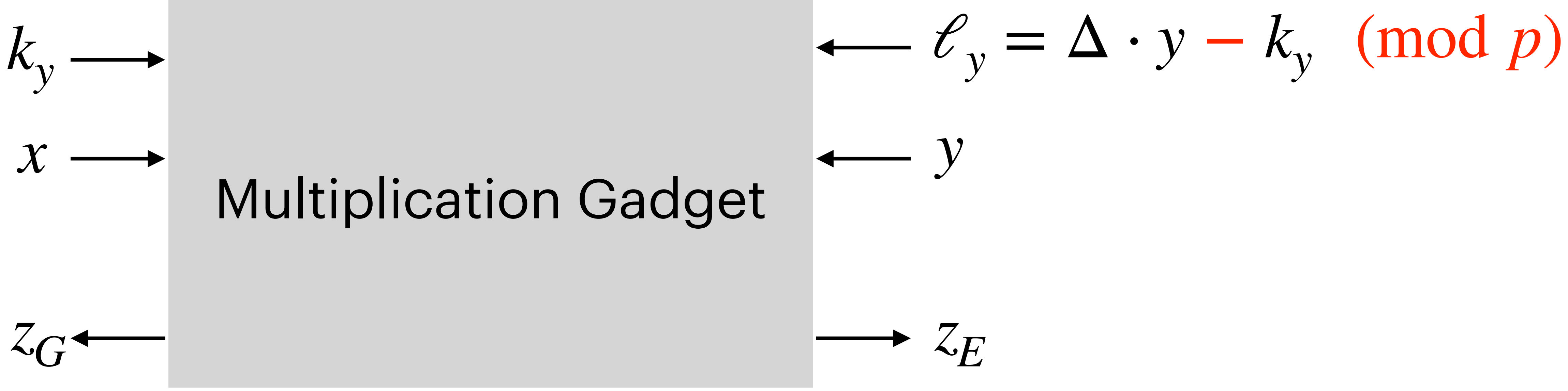
Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]

Δ

Garbler

Evaluator

Multiplication Gadget for Integers



k_y

x

z_G

Multiplication Gadget

$\ell_y = \Delta \cdot y - k_y \pmod{p}$

y

z_E

$$z_G \oplus z_E = xy$$

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

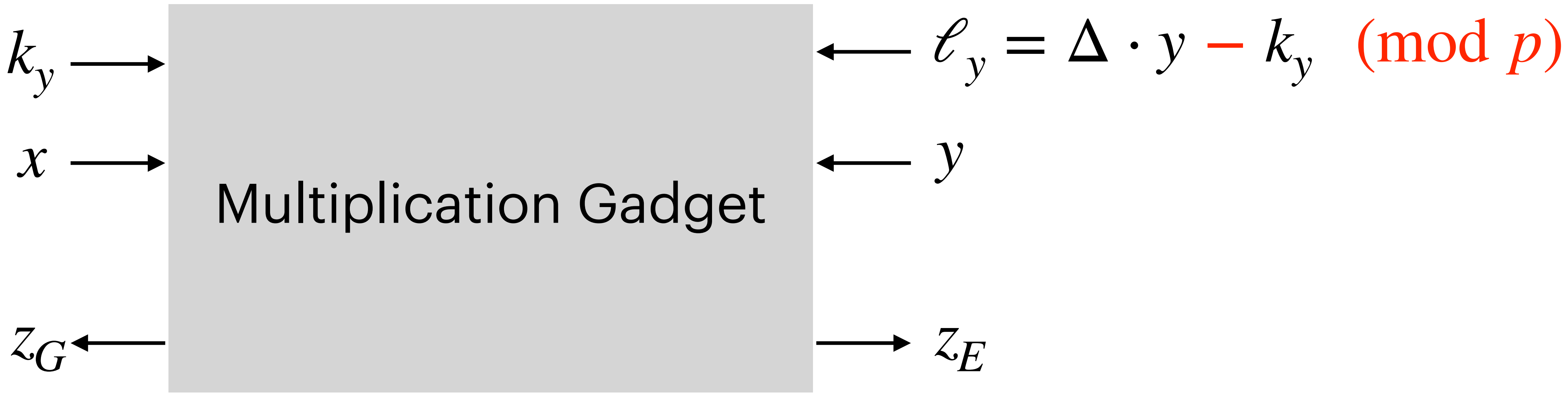
Multiplication Gadget from [Couteau-Hazay-H-Kumar’25]

Δ

Garbler

Evaluator

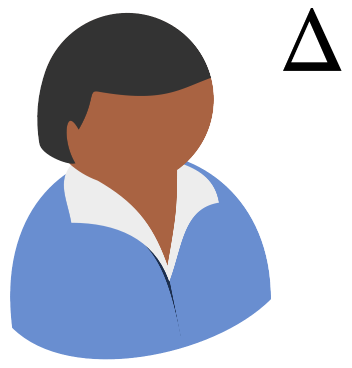
Multiplication Gadget for Integers



$$z_G + z_E = xy$$

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

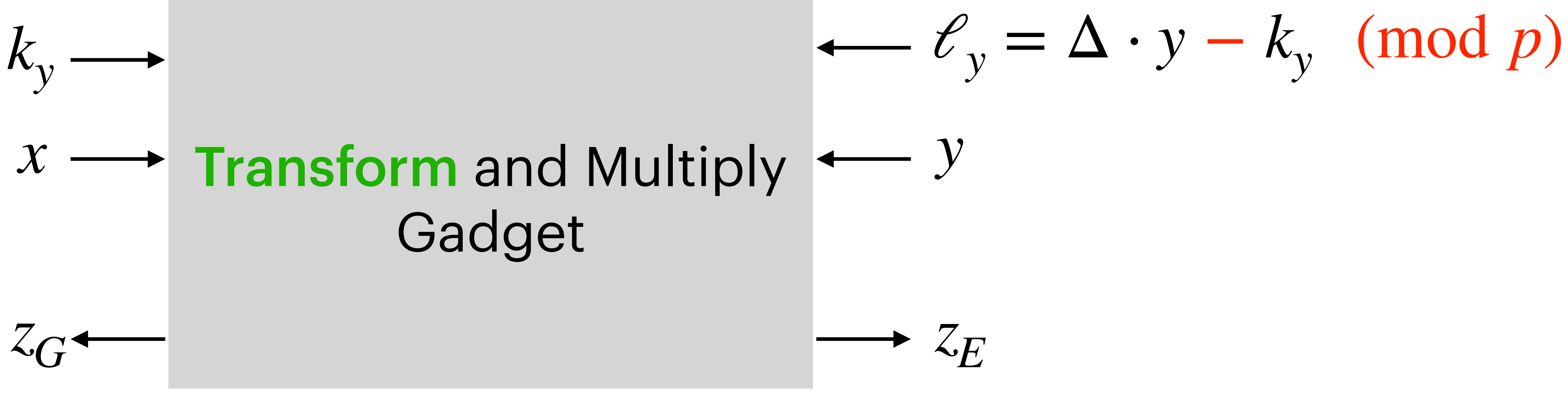
Multiplication Gadget from [Couteau-Hazay-H-Kumar’25]



Garbler

Evaluator

Multiplication Gadget for Integers



Transform and Multiply Gadget

k_y

x

z_G

$\ell_y = \Delta \cdot y - k_y \pmod{p}$

y

z_E

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

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

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

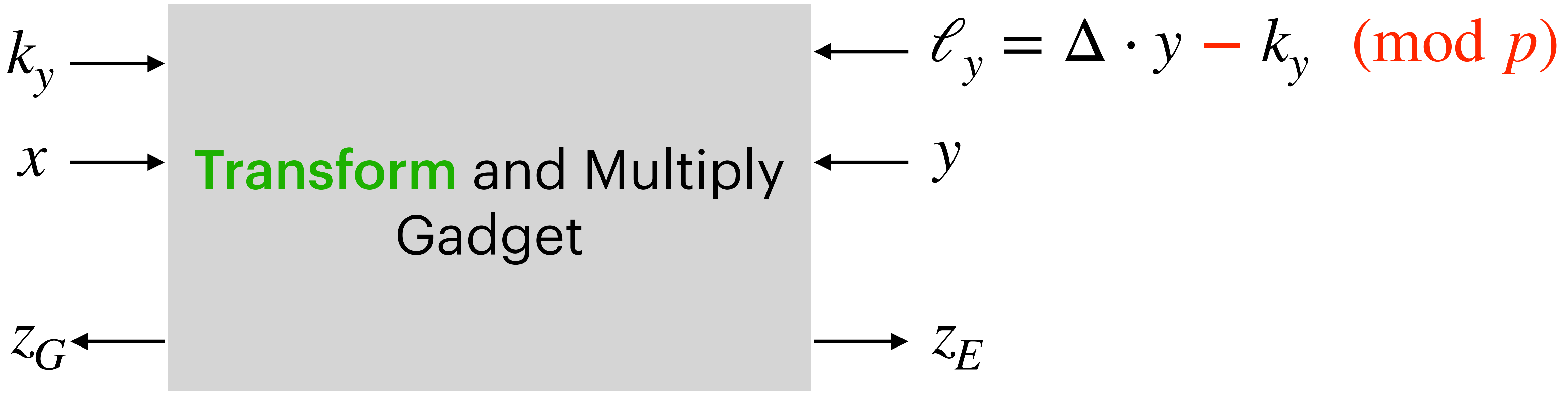
Δ

Garbler

Evaluator

Multiplication Gadget for Integers

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



$k_y \rightarrow$

$x \rightarrow$

$z_G \leftarrow$

Transform and Multiply Gadget

$\leftarrow \ell_y = \Delta \cdot y - k_y \pmod{p}$

$\leftarrow y$

$\rightarrow z_E$

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

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

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

Δ

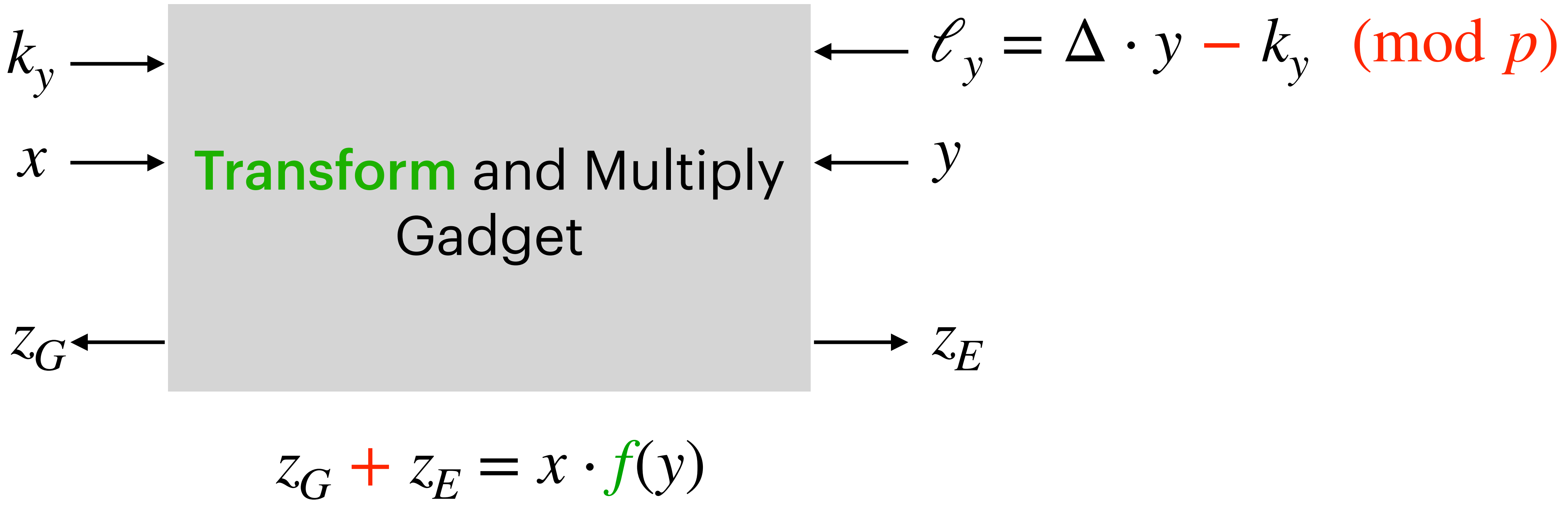
Garbler

Evaluator

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

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

Multiplication Gadget for Integers



$k_y \rightarrow$

$x \rightarrow$

Transform and Multiply Gadget

$\leftarrow \ell_y = \Delta \cdot y - k_y \pmod{p}$

$\leftarrow y$

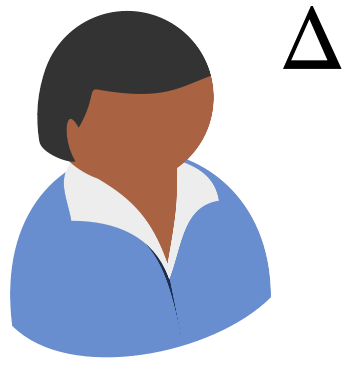
$z_G \leftarrow$

$\rightarrow z_E$

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

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

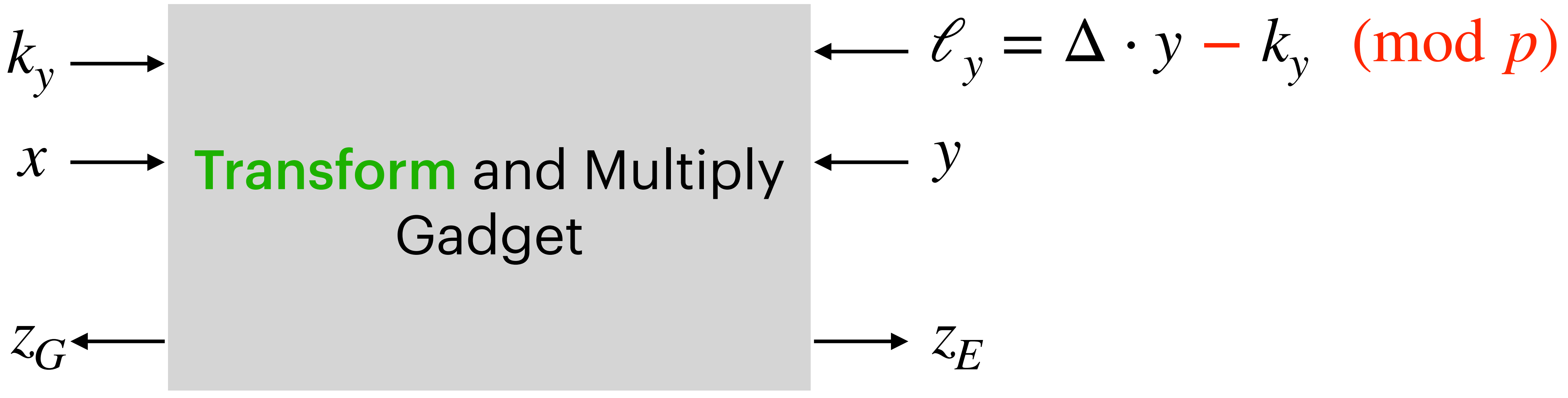
Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]



Garbler

Evaluator

Multiplication Gadget for Integers



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

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

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

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

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

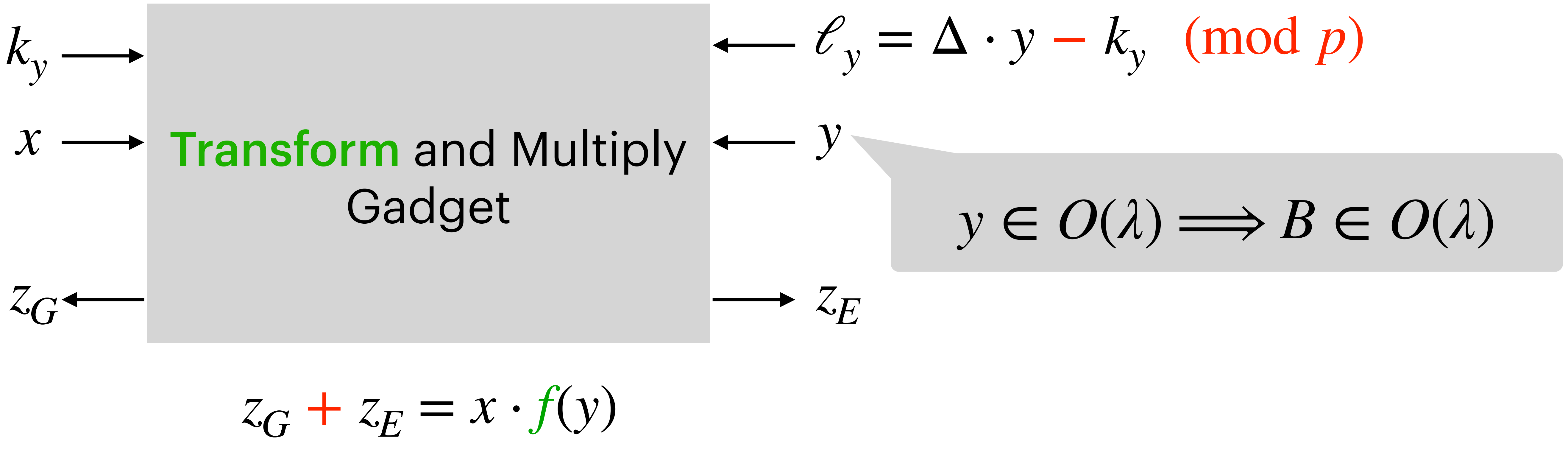
Multiplication Gadget from [Couteau-Hazay-H-Kumar’25]

Δ

Garbler

Evaluator

Multiplication Gadget for Integers



$k_y \rightarrow$

$x \rightarrow$

$z_G \leftarrow$

Transform and Multiply Gadget

$\leftarrow \ell_y = \Delta \cdot y - k_y \pmod{p}$

$\leftarrow y$

$\rightarrow z_E$

$y \in O(\lambda) \Longrightarrow B \in O(\lambda)$

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

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

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

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

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

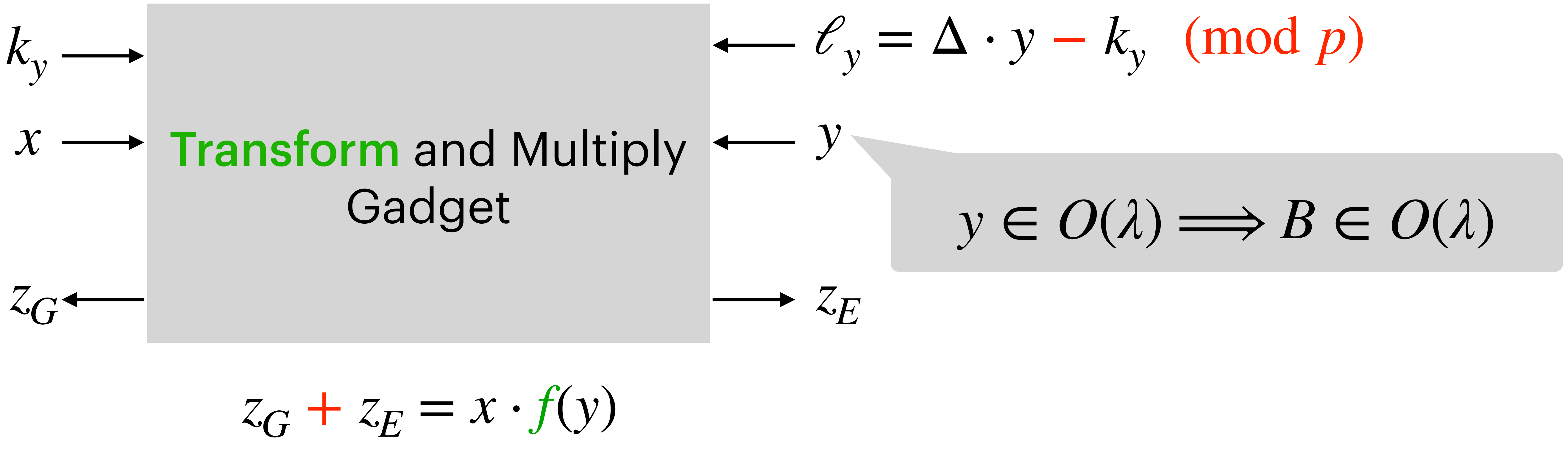
Multiplication Gadget from [Couteau-Hazay-H-Kumar’25]

Δ

Garbler

Evaluator

Multiplication Gadget for Integers



Transform and Multiply Gadget

$k_y \rightarrow$

$x \rightarrow$

$z_G \leftarrow$

$\leftarrow \ell_y = \Delta \cdot y - k_y \pmod{p}$

$\leftarrow y$

$\rightarrow z_E$

$y \in O(\lambda) \Longrightarrow B \in O(\lambda)$

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

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

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

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

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

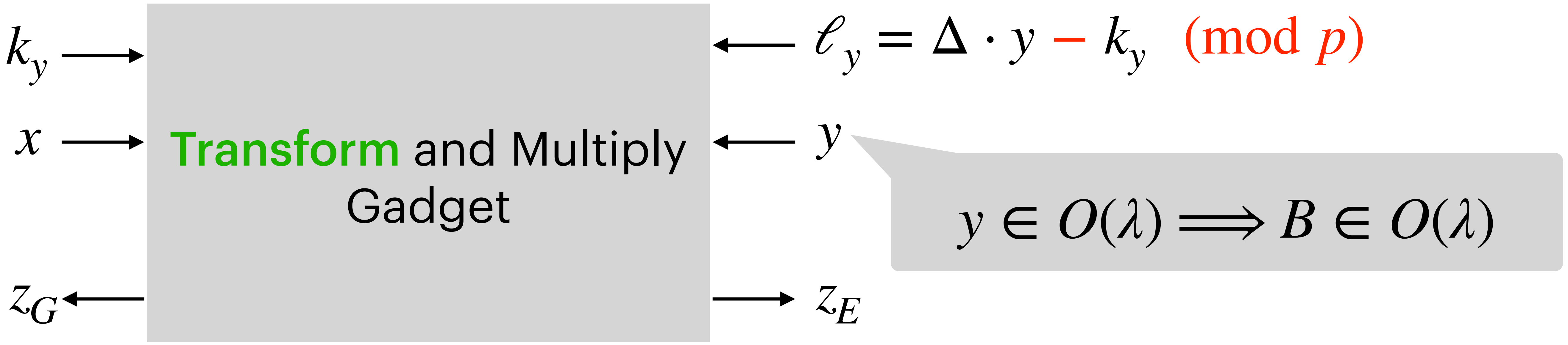
Multiplication Gadget from [Couteau-Hazay-H-Kumar'25]

Δ

Garbler

Evaluator

Multiplication Gadget for Integers



k_y

x

z_G

Transform and Multiply Gadget

$\ell_y = \Delta \cdot y - k_y \pmod{p}$

y

z_E

$y \in O(\lambda) \Longrightarrow B \in O(\lambda)$

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

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

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

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

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

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

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

Δ

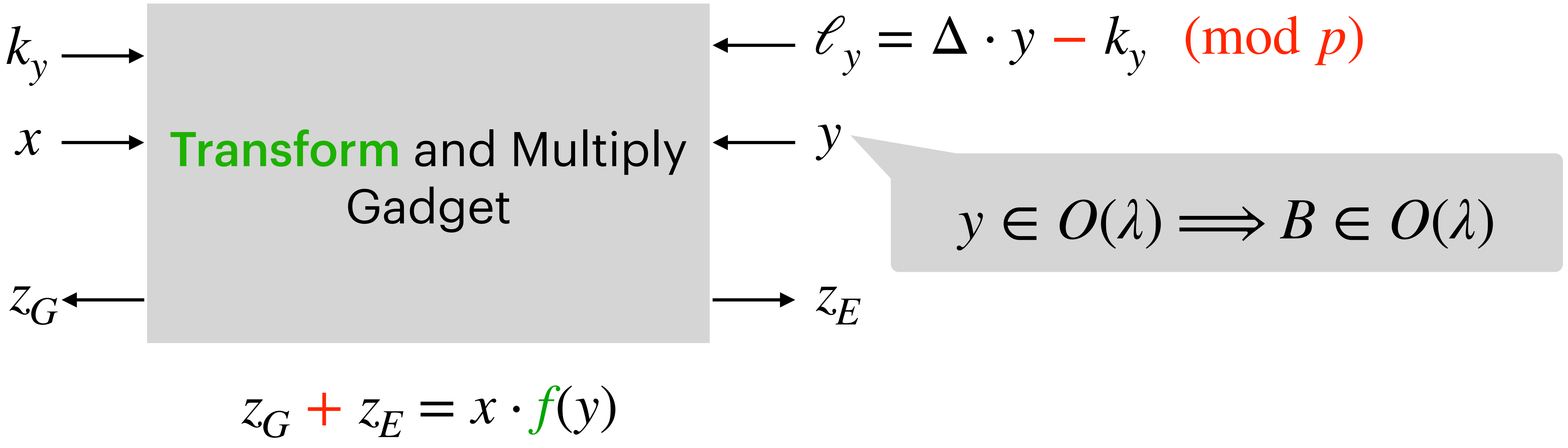
Garbler

Evaluator

Multiplication Gadget for Integers

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

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



$k_y \rightarrow$

$x \rightarrow$

$z_G \leftarrow$

Transform and Multiply Gadget

$\leftarrow \ell_y = \Delta \cdot y - k_y \pmod{p}$

$\leftarrow y$

$y \in O(\lambda) \implies B \in O(\lambda)$

$\rightarrow z_E$

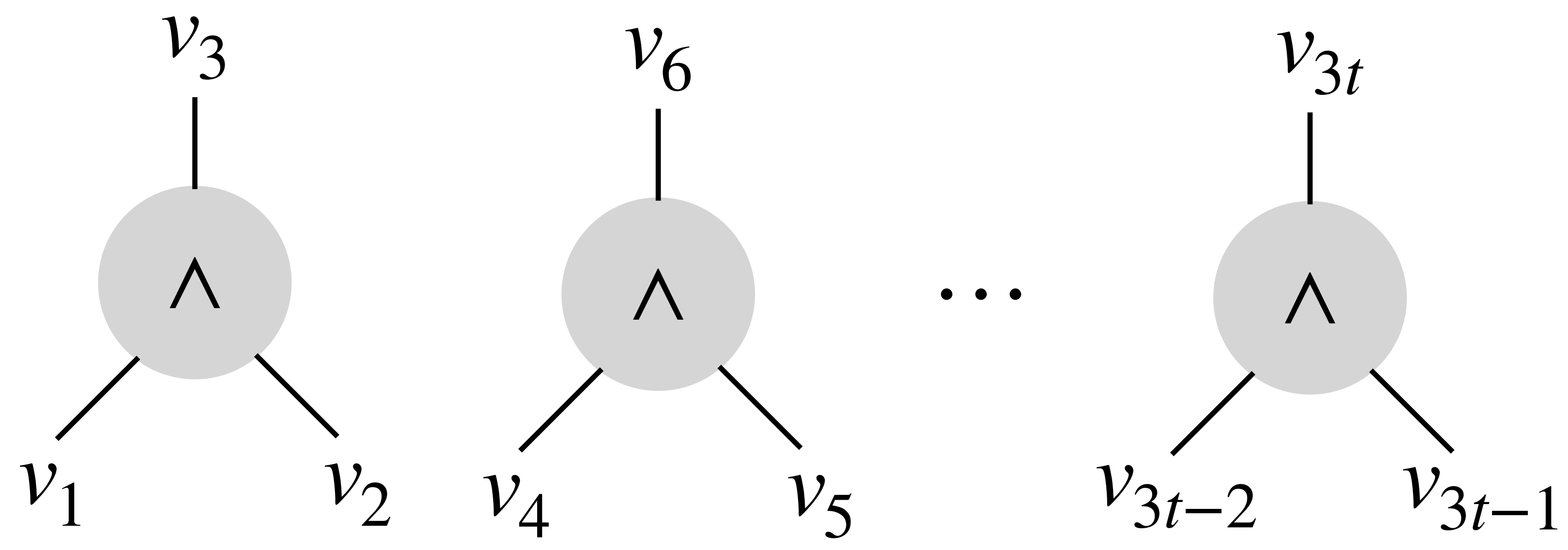
$z_G + z_E = x \cdot f(y)$

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

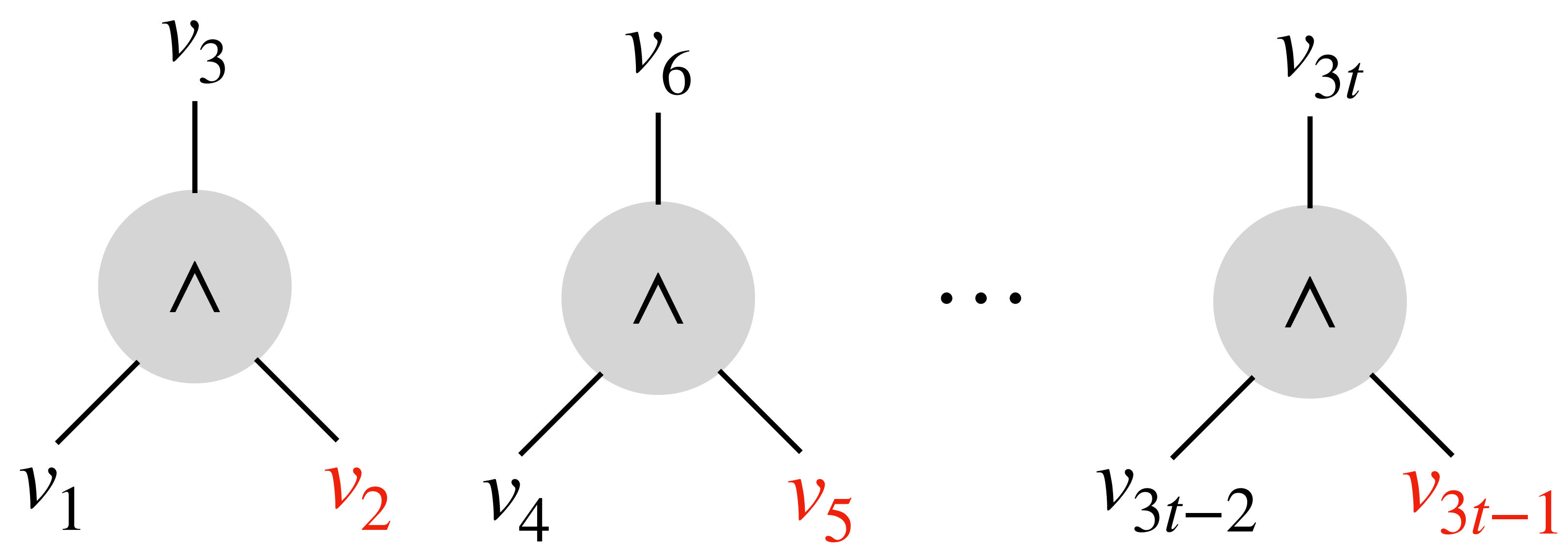
Rate of Boolean Garbling: $O\left(\dfrac{1}{\lambda}\right)$

Key Ingredient: A packing from $\mathbb{F}_2^t$ to $\log \lambda$-bit integers

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



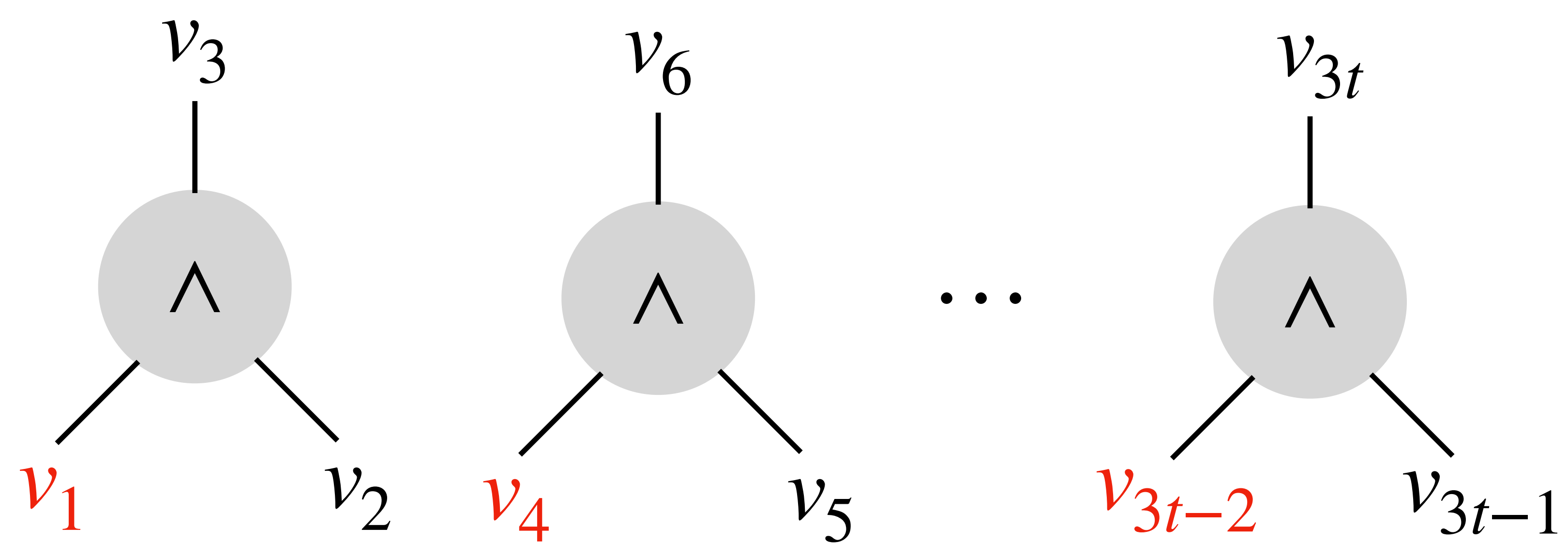
Template for $\omega(1/\lambda)$-Rate Garbling



1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

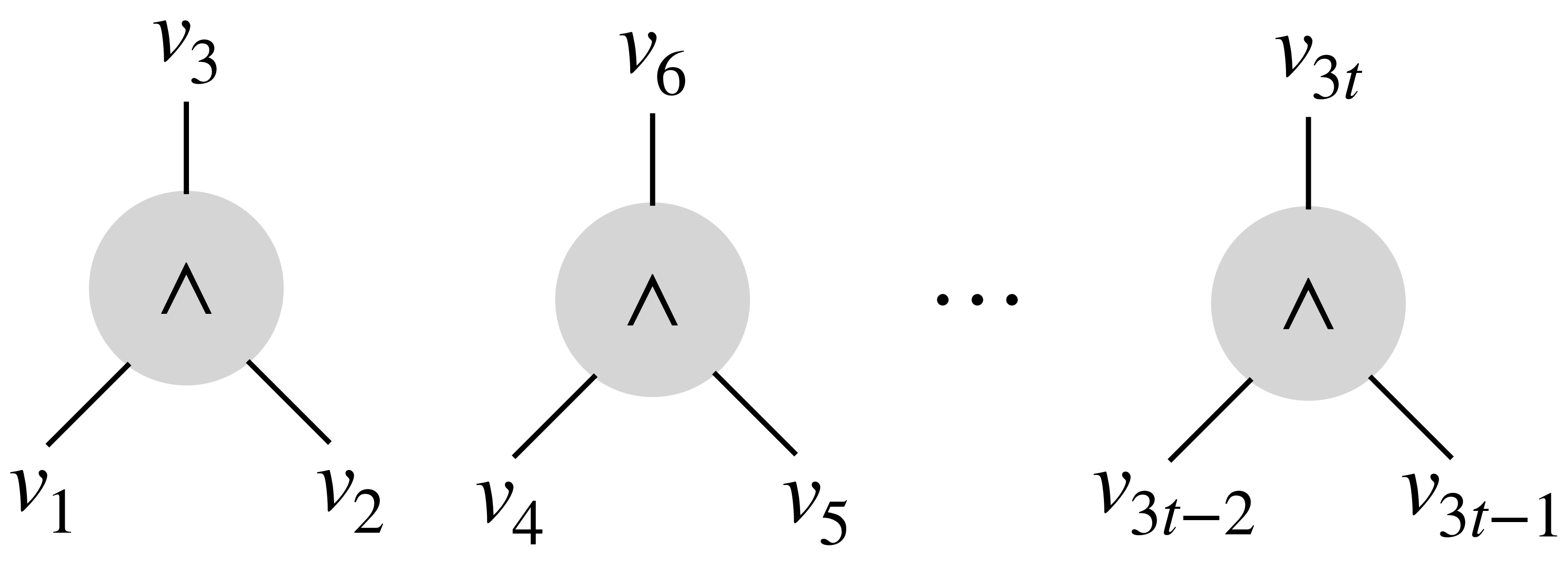
Template for $\omega(1/\lambda)$-Rate Garbling



1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

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



1. Packing

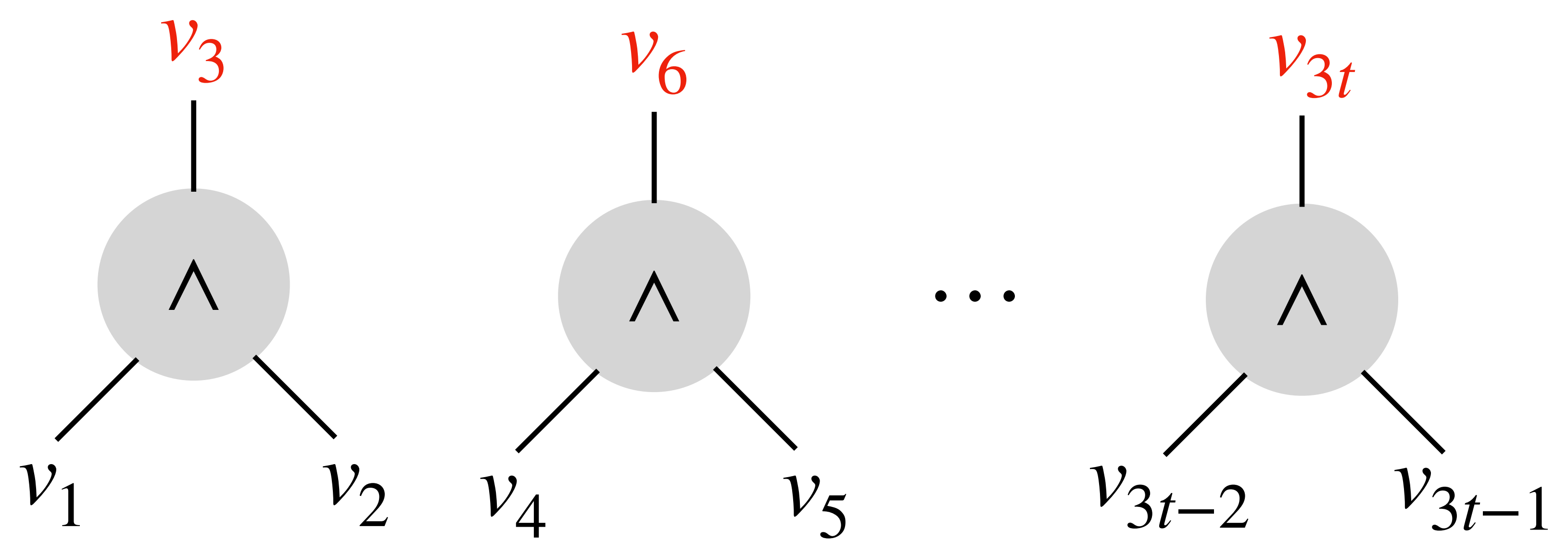
$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

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



1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

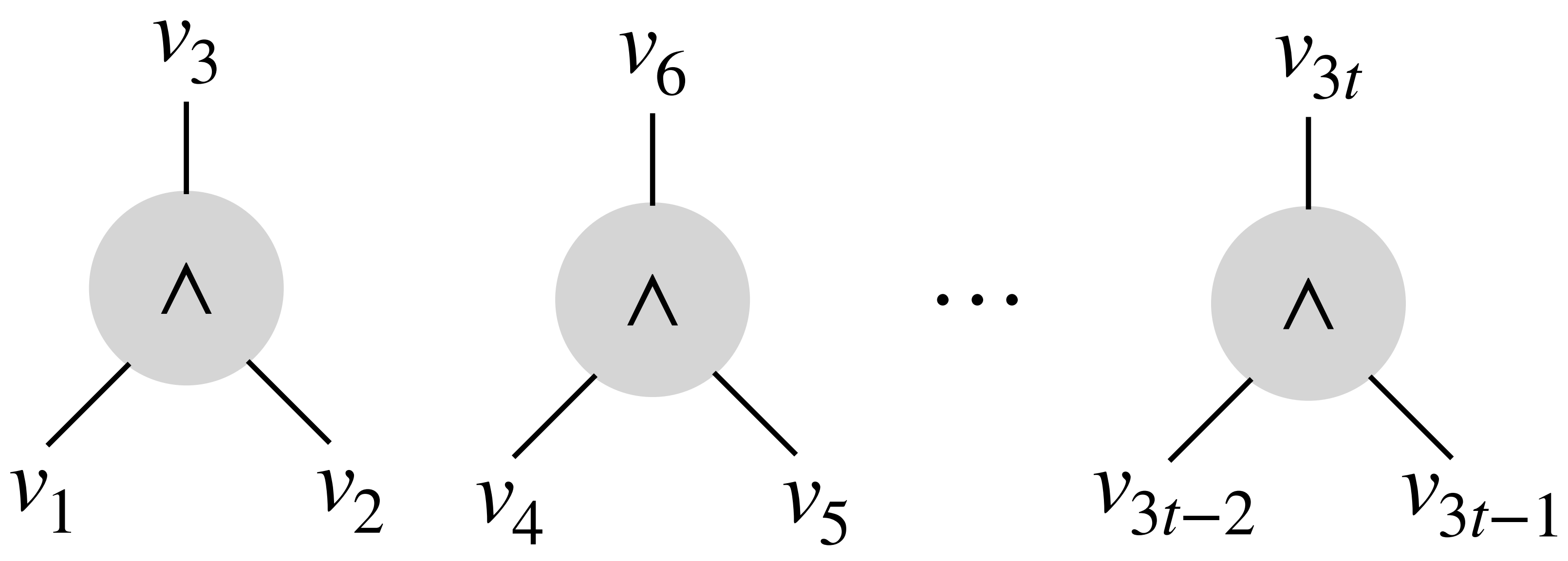
2. Gate Evaluation

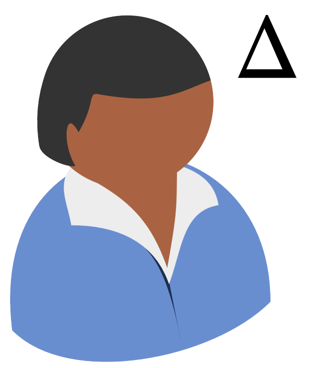
$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

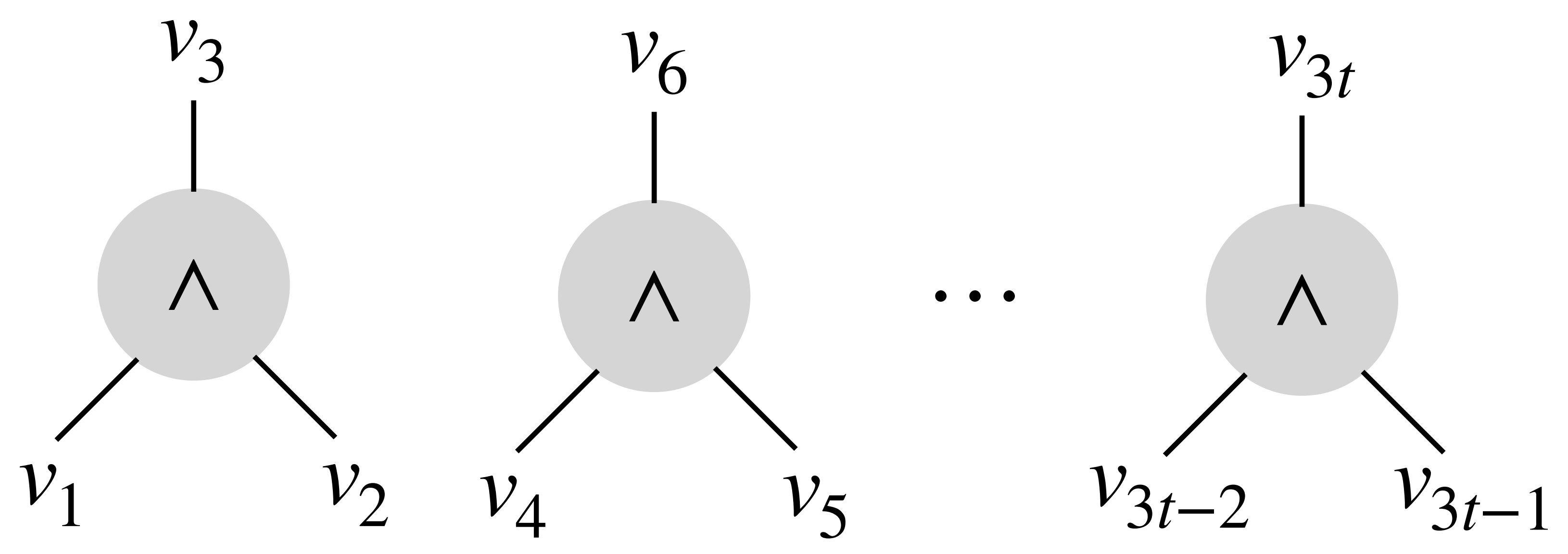
2. Gate Evaluation

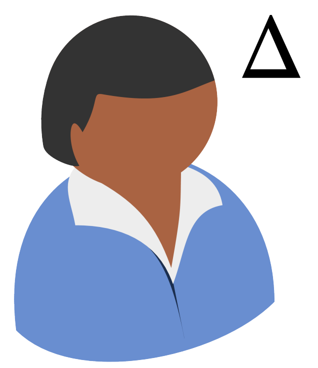
$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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





Garbler

Invariant

$$g_i \oplus e_i = v_i$$

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

Evaluator

1. Packing

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

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

2. Gate Evaluation

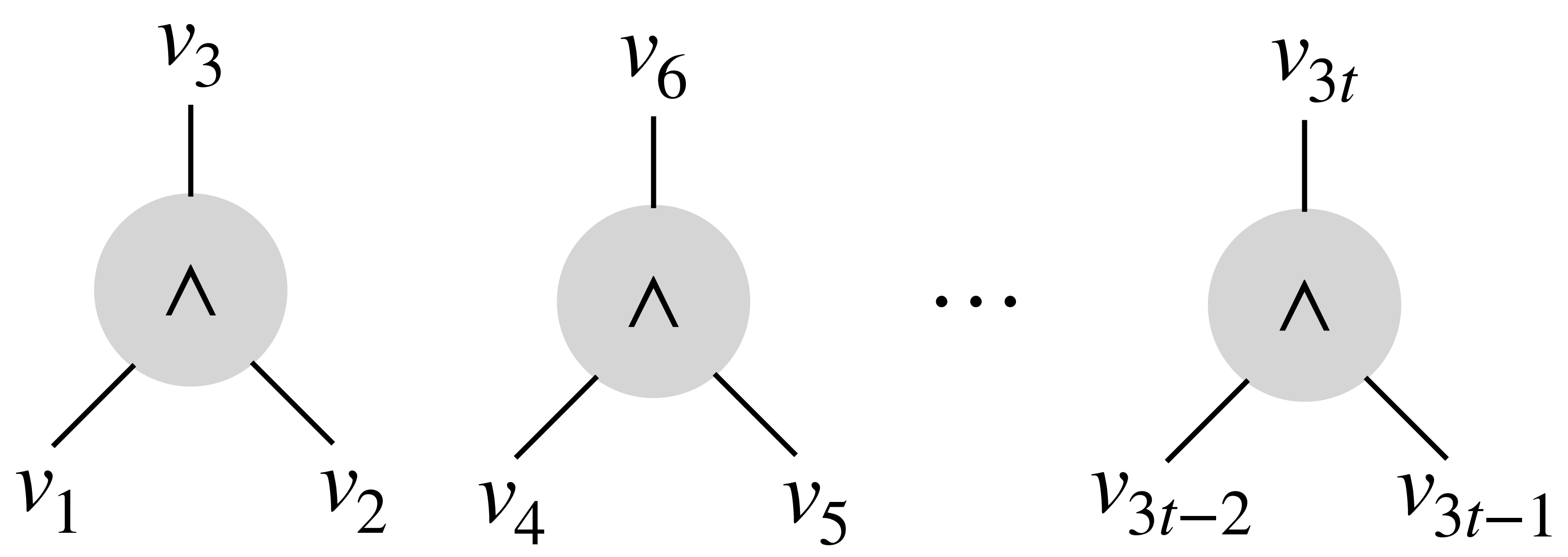
$$V = V_1 \cdot V_2$$

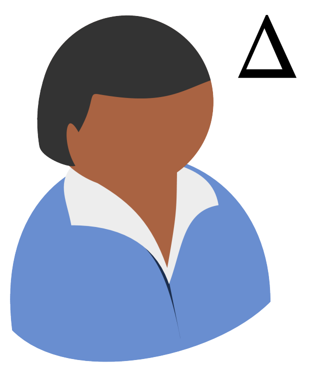
Evaluate over shares of packed encodings using multiplication gadget

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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





Garbler

Invariant

$$g_i \oplus e_i = v_i$$

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

Evaluator

1. Packing

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

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

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

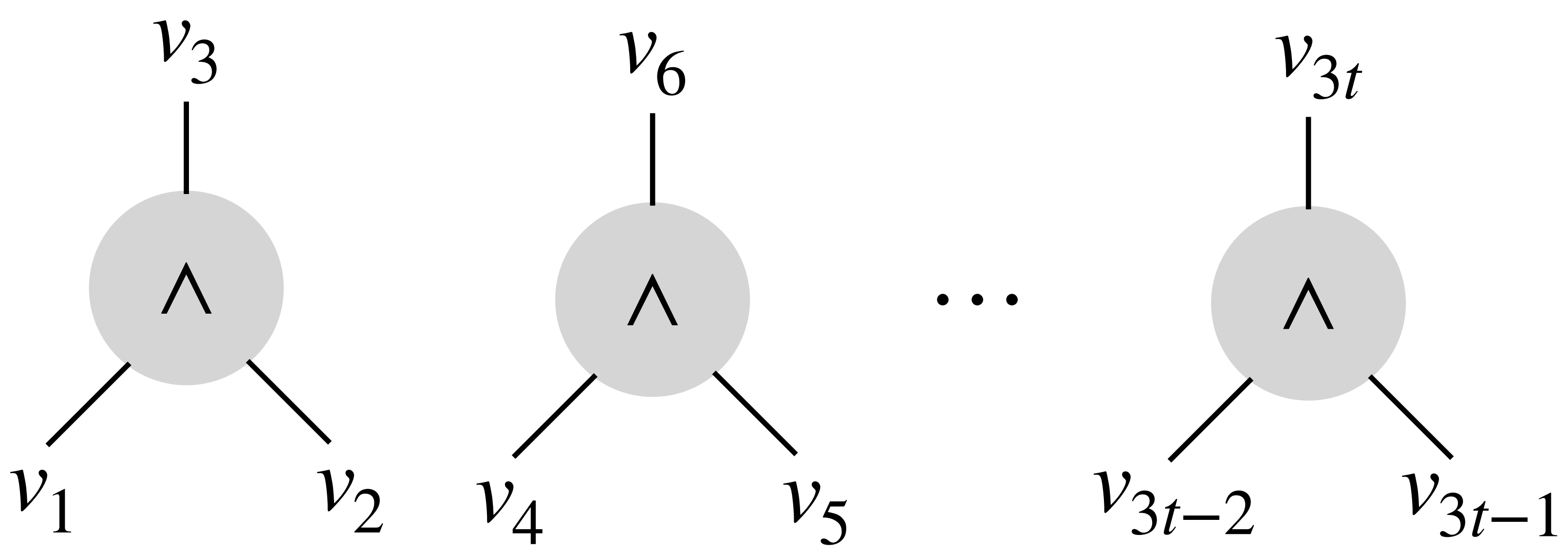
3. Unpacking

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

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

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

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



1. Packing

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

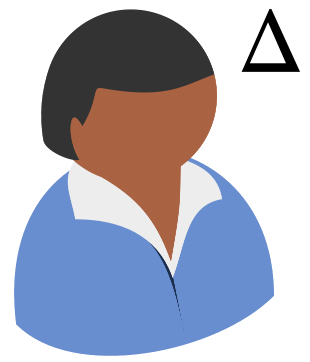
$$V_L = \text{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

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



Garbler

Invariant

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

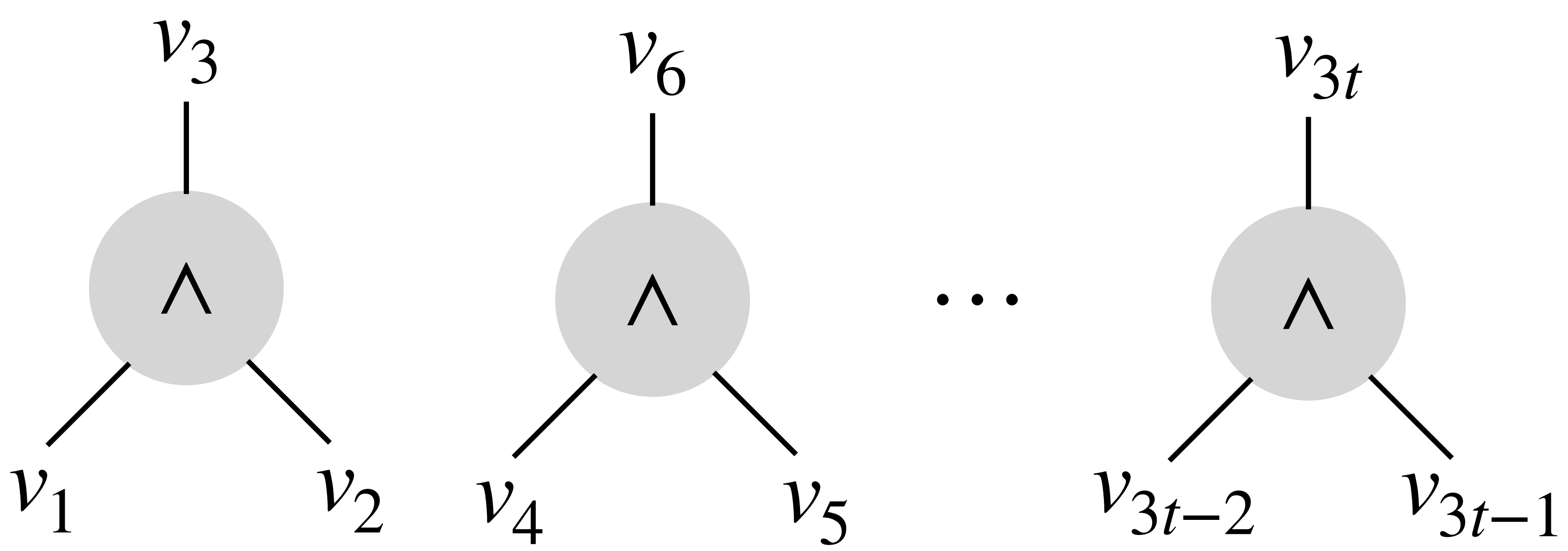
Evaluator

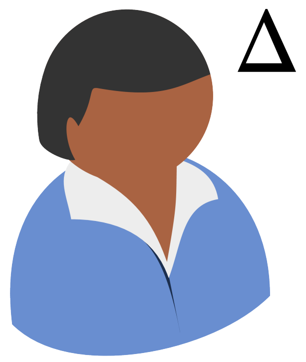
$G_R = \text{Pack}(g_2, g_5, \ldots, g_{3t-1})$

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

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

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$

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

$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$

We will need shares of $\Delta \cdot E_\mathsf{R}$ for evaluating the gate

K_R

$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod p$

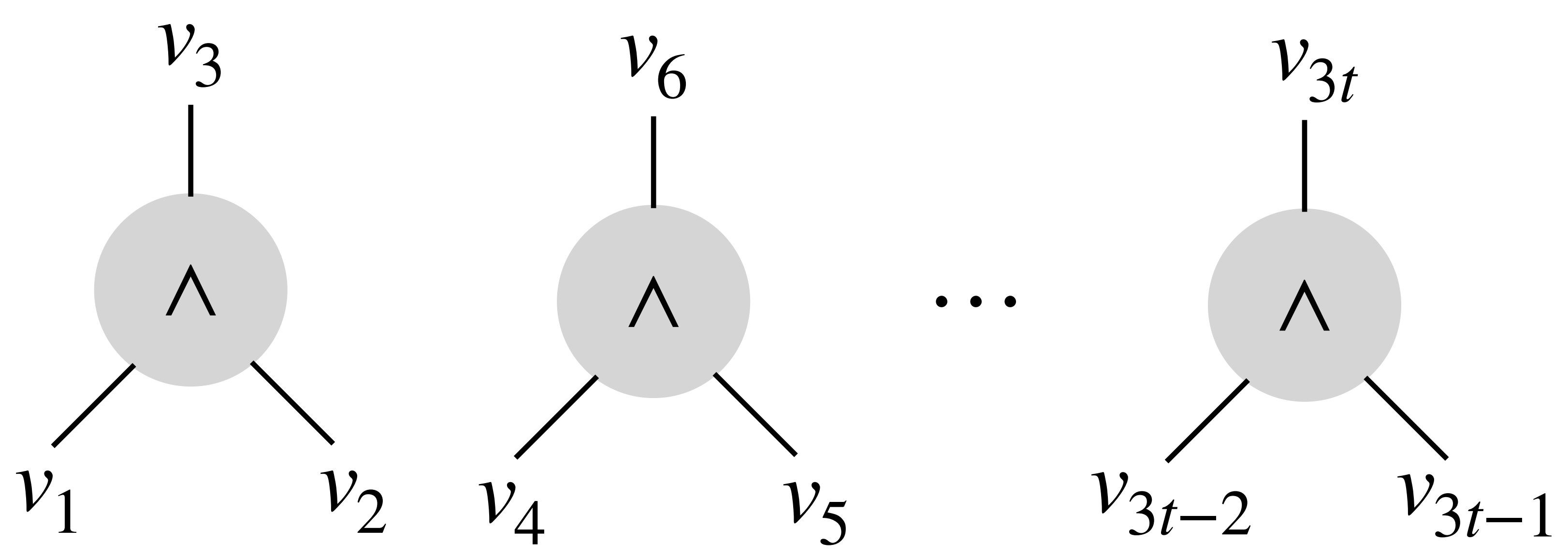
2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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



1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

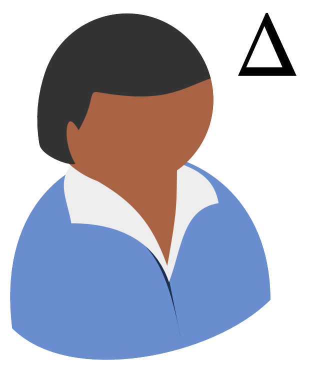
$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$



Garbler

Invariant

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

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

Evaluator

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

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

$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

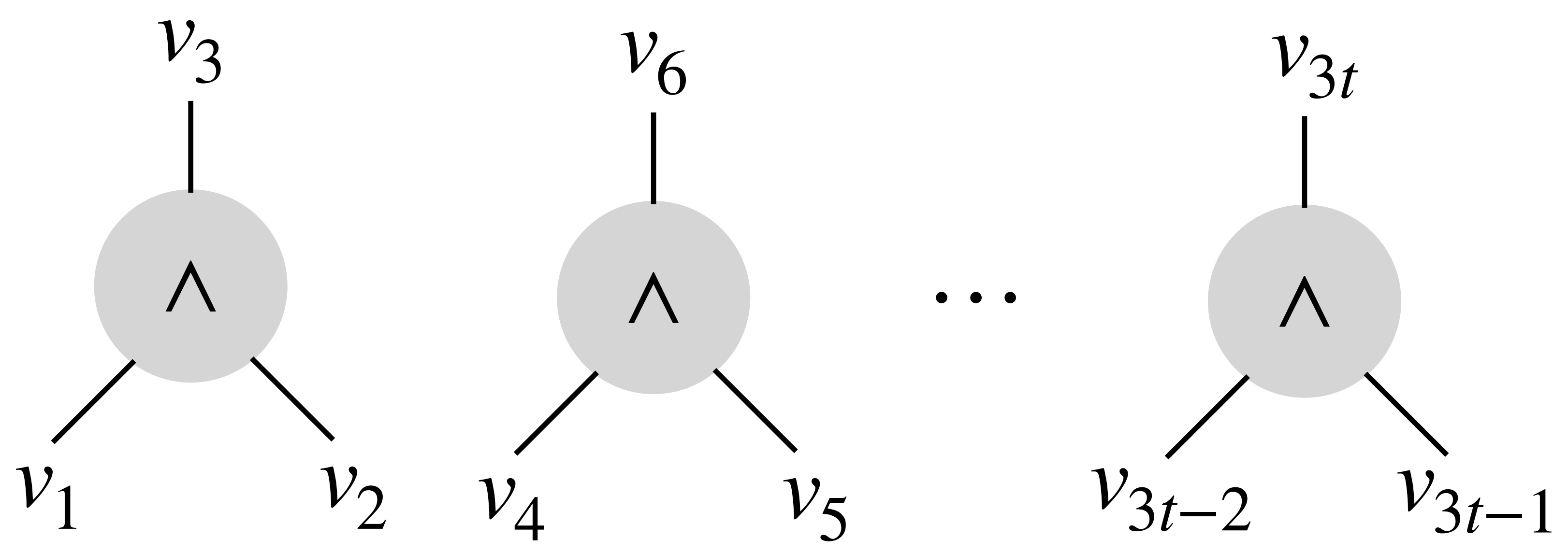
We will need shares of $\Delta \cdot E_\mathsf{R}$ for evaluating the gate

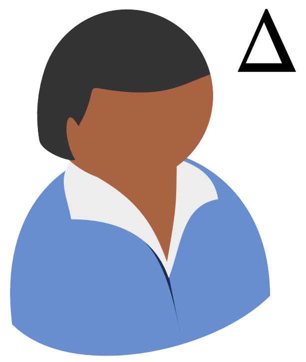
K_R

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod p$$

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

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

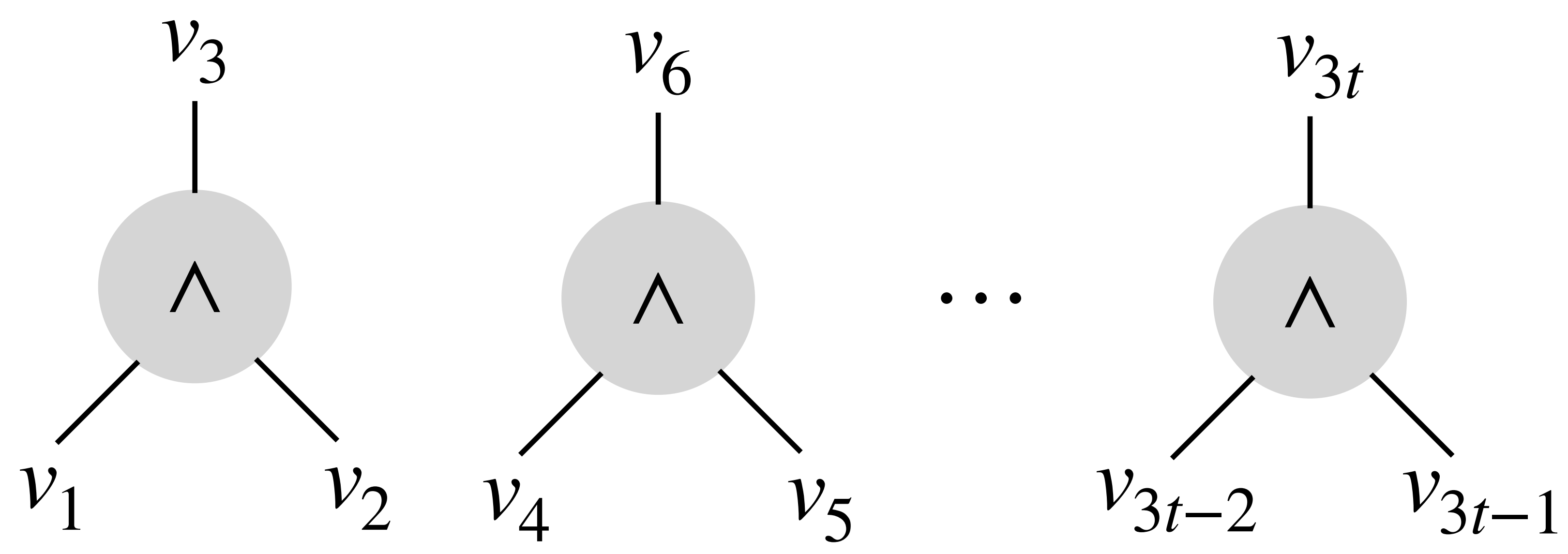
2. Gate Evaluation

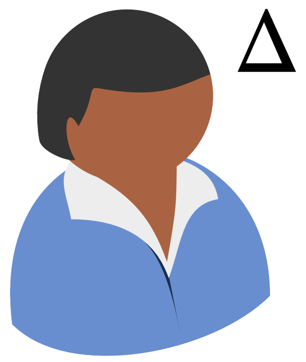
$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

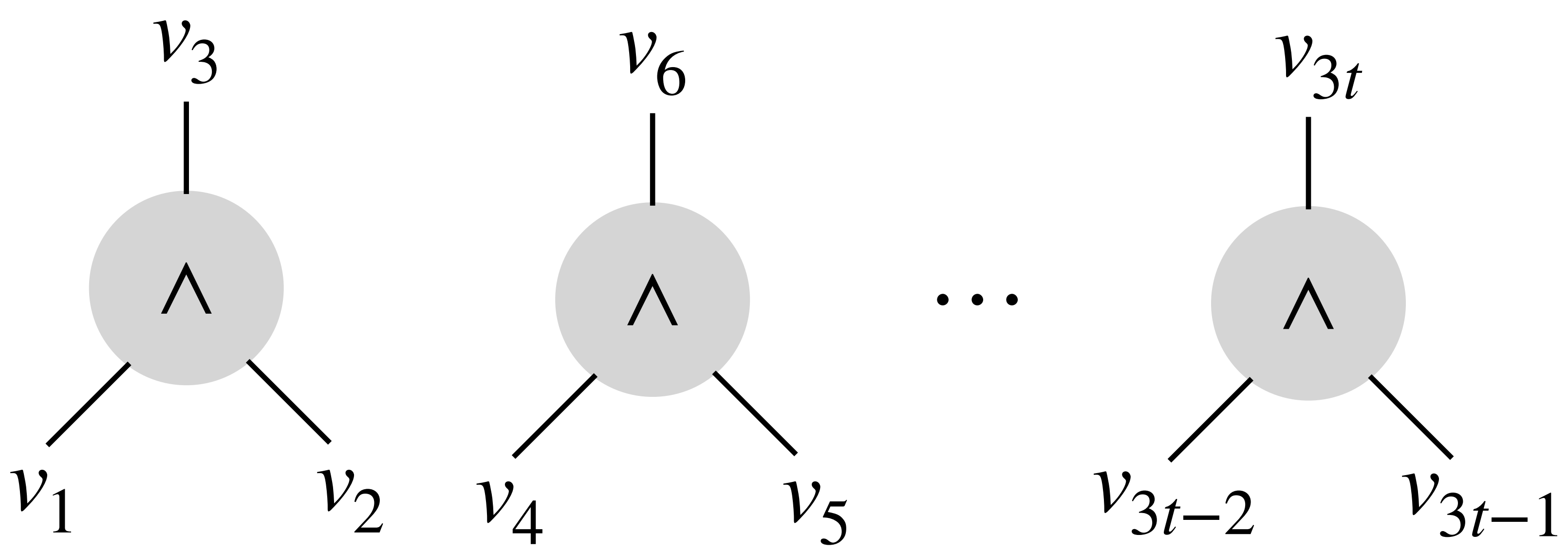
$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

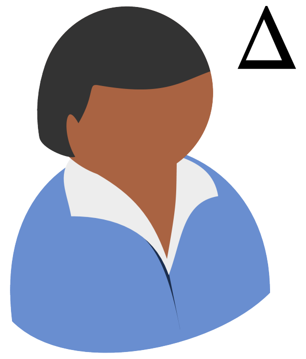
$$G_{\mathsf{R}} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$E_{\mathsf{R}} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

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

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





Δ

Garbler

Invariant

$$g_i \oplus e_i = v_i$$

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

Evaluator

1. Packing

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

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

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

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

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

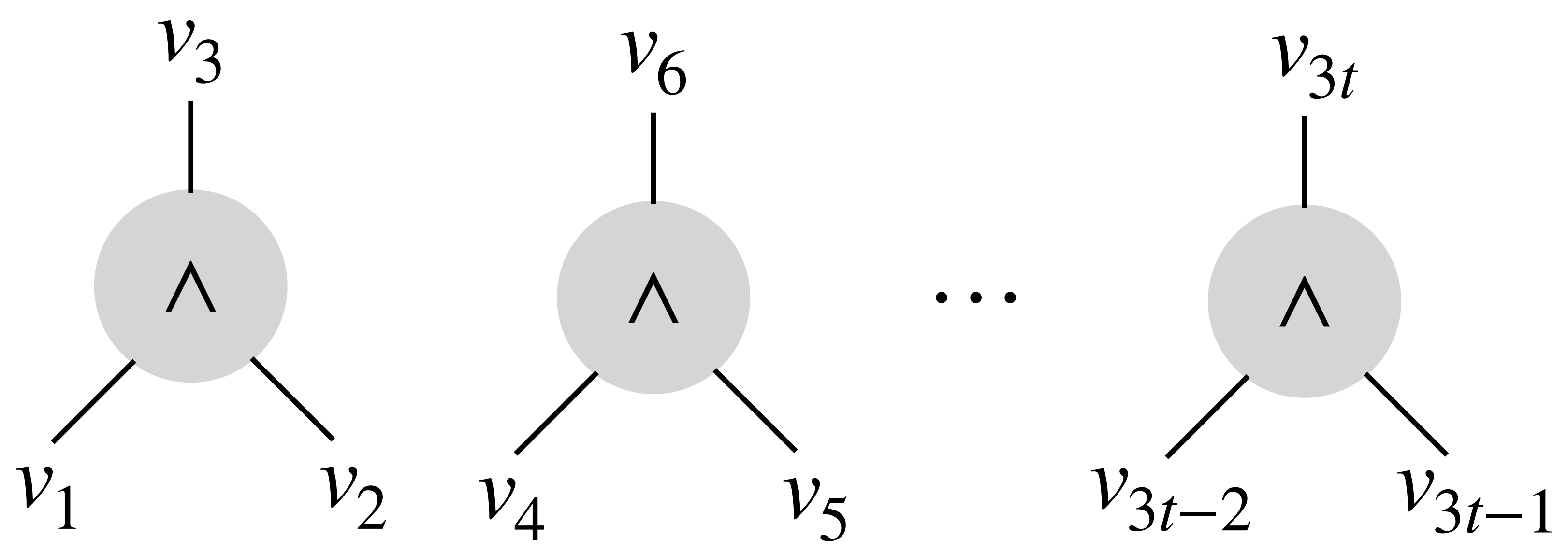
$$E_R = \text{Pack}(e_2, e_5, \ldots, e_{3t-1})$$

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

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

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

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



1. Packing

$$V_{\mathrm{R}} = \mathrm{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

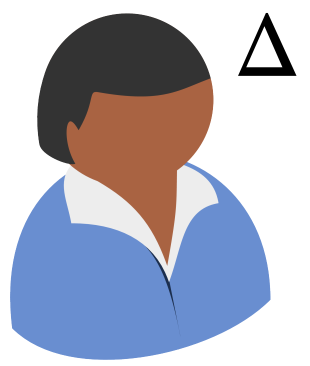
$$V_{\mathrm{L}} = \mathrm{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathrm{UnPack}(V)$$



Garbler

Invariant

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

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

Evaluator

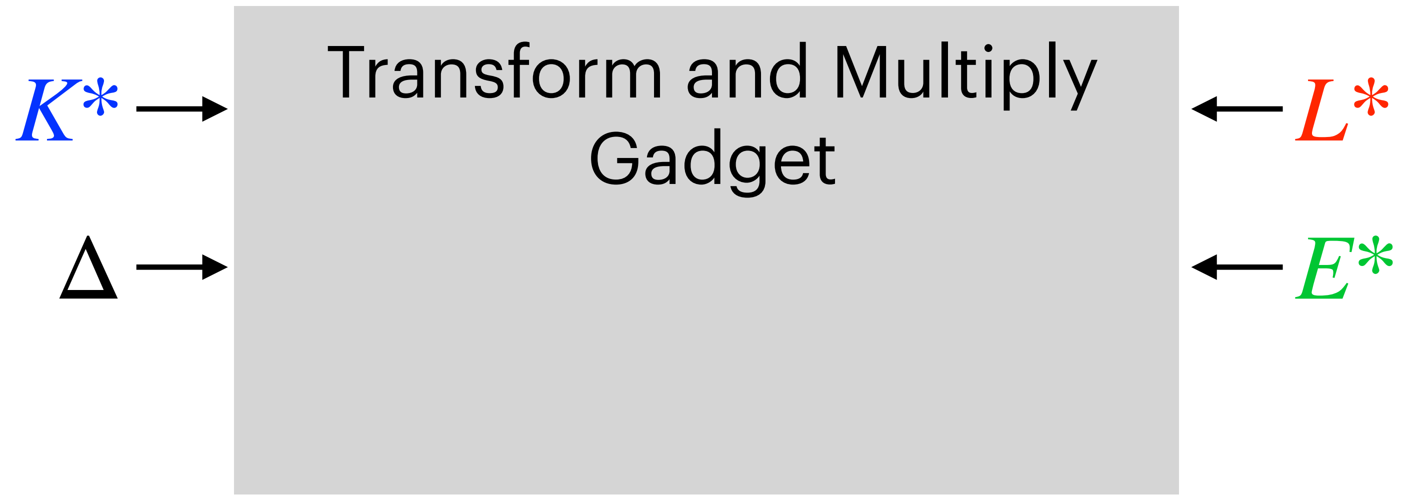
$$G_{\mathrm{R}} = \mathrm{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$E_{\mathrm{R}} = \mathrm{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

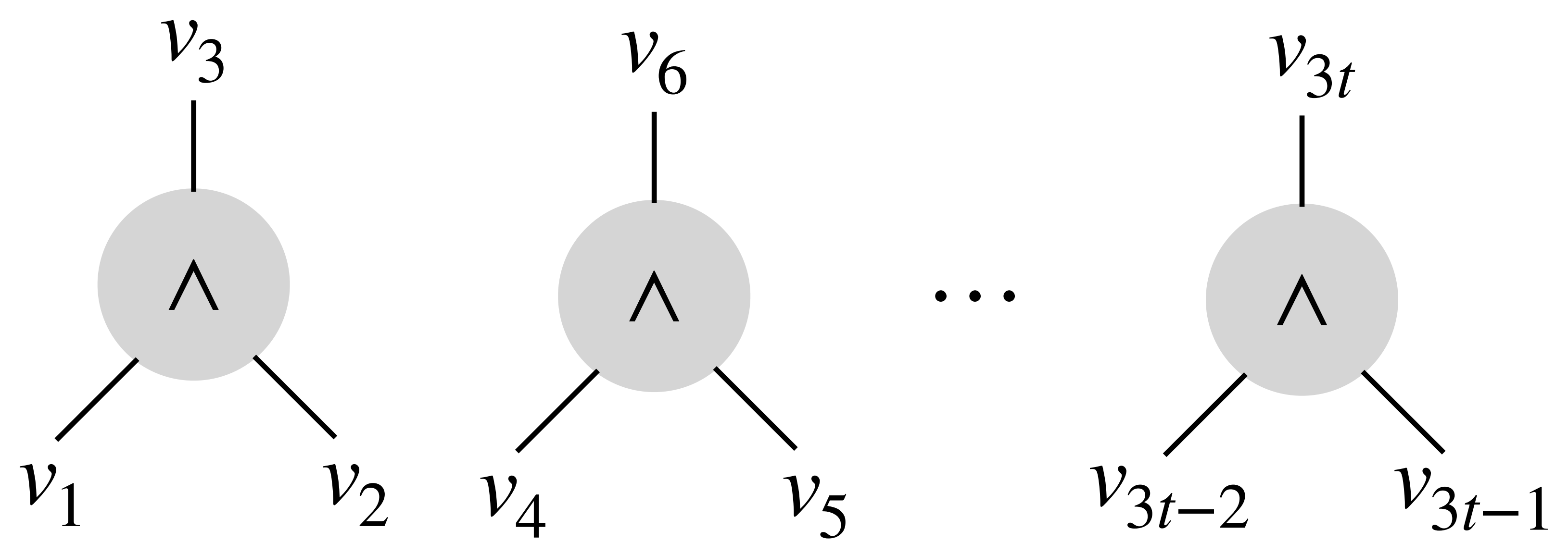
$$E^* = \sum_{i=1}^{t} \mathsf{e}_{3i-1} \cdot 2^i$$

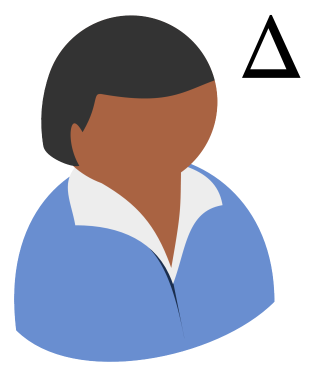
$$K^* = \sum_{i=1}^{t} k_{3i-1} \cdot 2^i \pmod p$$

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



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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

$$G_{\mathsf{R}} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$E_{\mathsf{R}} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

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

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

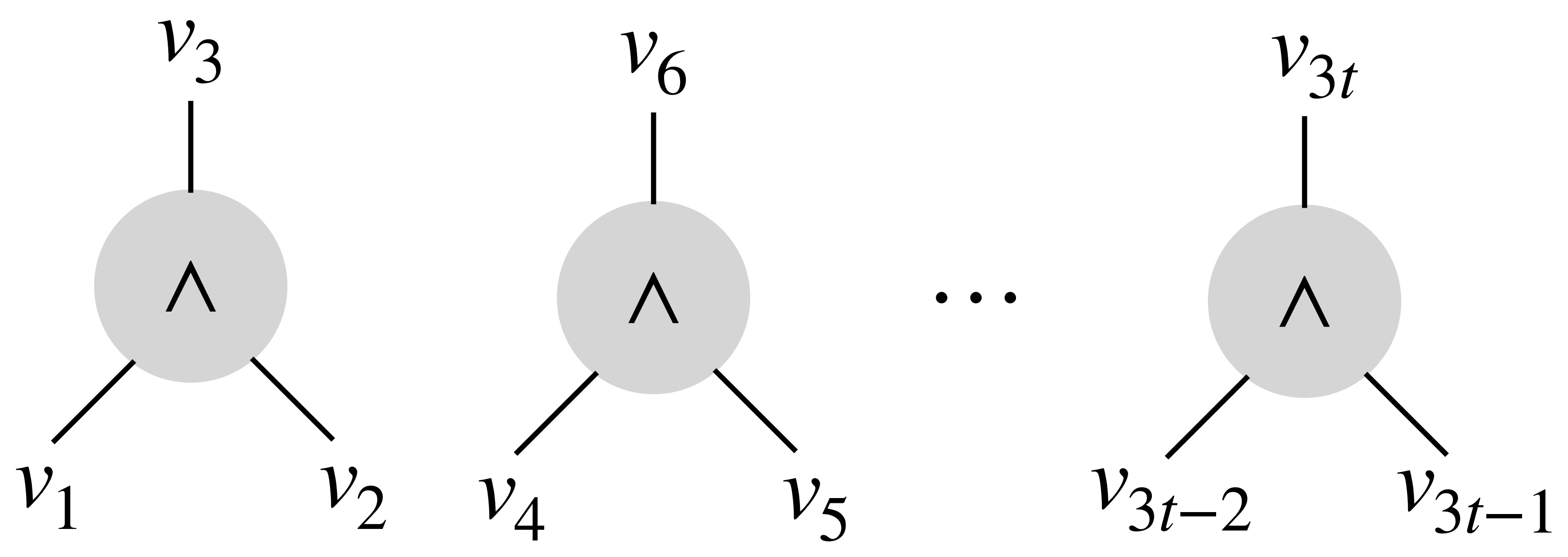
$$L^* = \sum_{i=1}^{t} \ell_{3i-1} \cdot 2^i \pmod{p}$$

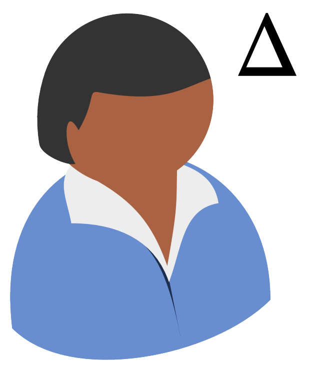
Transform and Multiply Gadget

$$K^* \rightarrow \qquad \leftarrow L^* = \Delta \cdot E^* - K^* \pmod{p}$$

$$\Delta \rightarrow \qquad \leftarrow E^*$$

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





Garbler

Invariant

$g_i \oplus e_i = v_i$

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

Evaluator

1. Packing

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

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

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

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

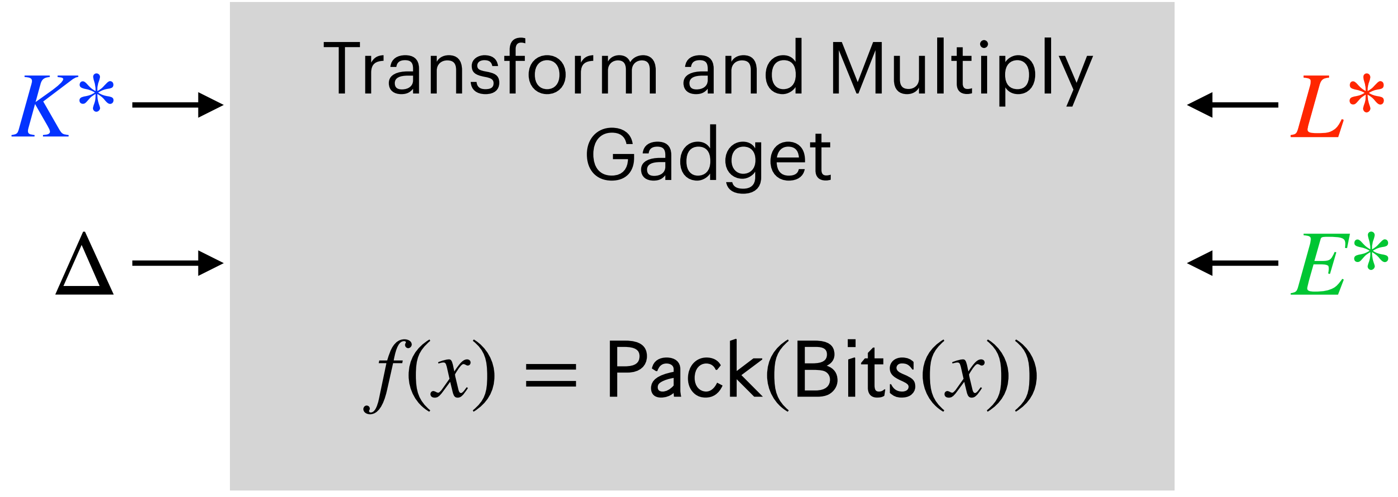
$$E^* = \sum_{i=1}^{t} e_{3i-1} \cdot 2^i$$

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

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

2. Gate Evaluation

$V = V_1 \cdot V_2$



Transform and Multiply Gadget

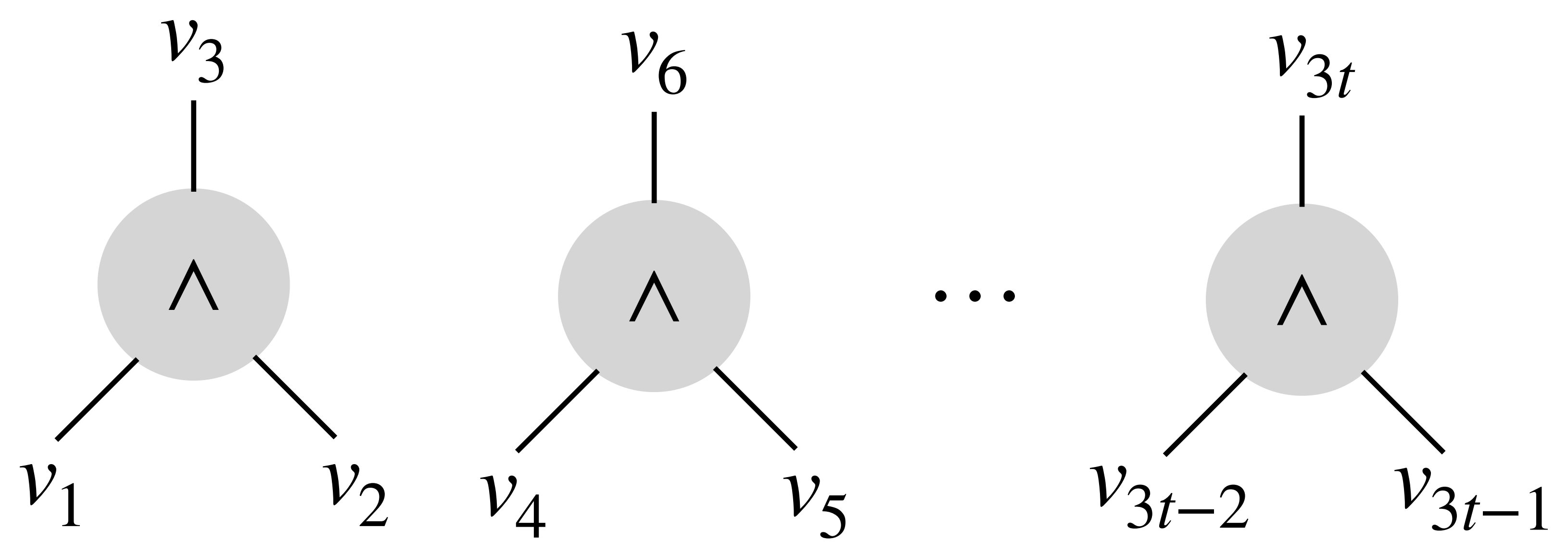
$f(x) = \text{Pack}(\text{Bits}(x))$

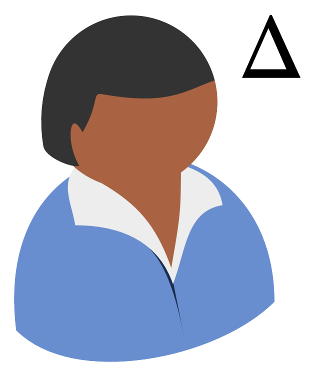
$L^* = \Delta \cdot E^* - K^* \pmod{p}$

3. Unpacking

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

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





Garbler

Invariant

$$g_i \oplus e_i = v_i$$

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

Evaluator

1. Packing

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

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

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

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

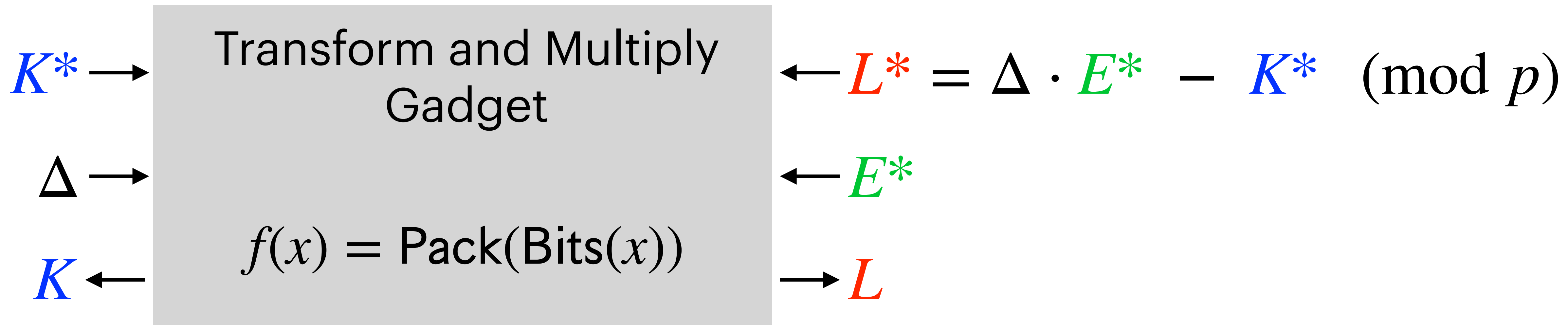
$$G_R = \text{Pack}(g_2, g_5, \ldots, g_{3t-1})$$

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

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

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

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



Transform and Multiply Gadget

$$f(x) = \text{Pack}(\text{Bits}(x))$$

$$K^* \rightarrow$$

$$\Delta \rightarrow$$

$$K \leftarrow$$

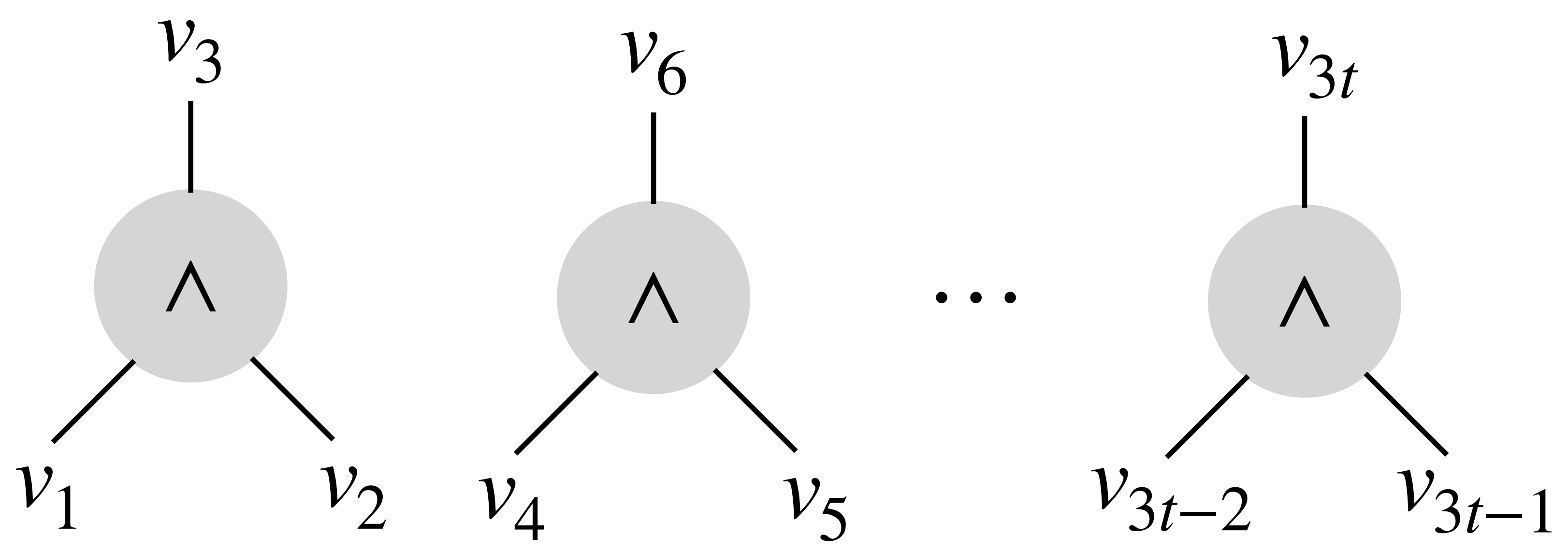
$$\leftarrow L^* = \Delta \cdot E^* - K^* \pmod{p}$$

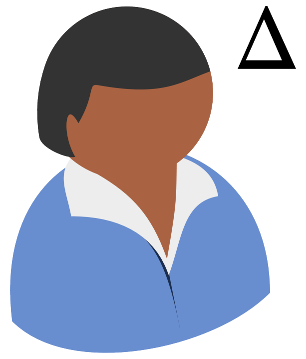
$$\leftarrow E^*$$

$$\rightarrow L$$

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

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




Δ

Garbler

Invariant

$$g_i \oplus e_i = v_i$$

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

Evaluator

1. Packing

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

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

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

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

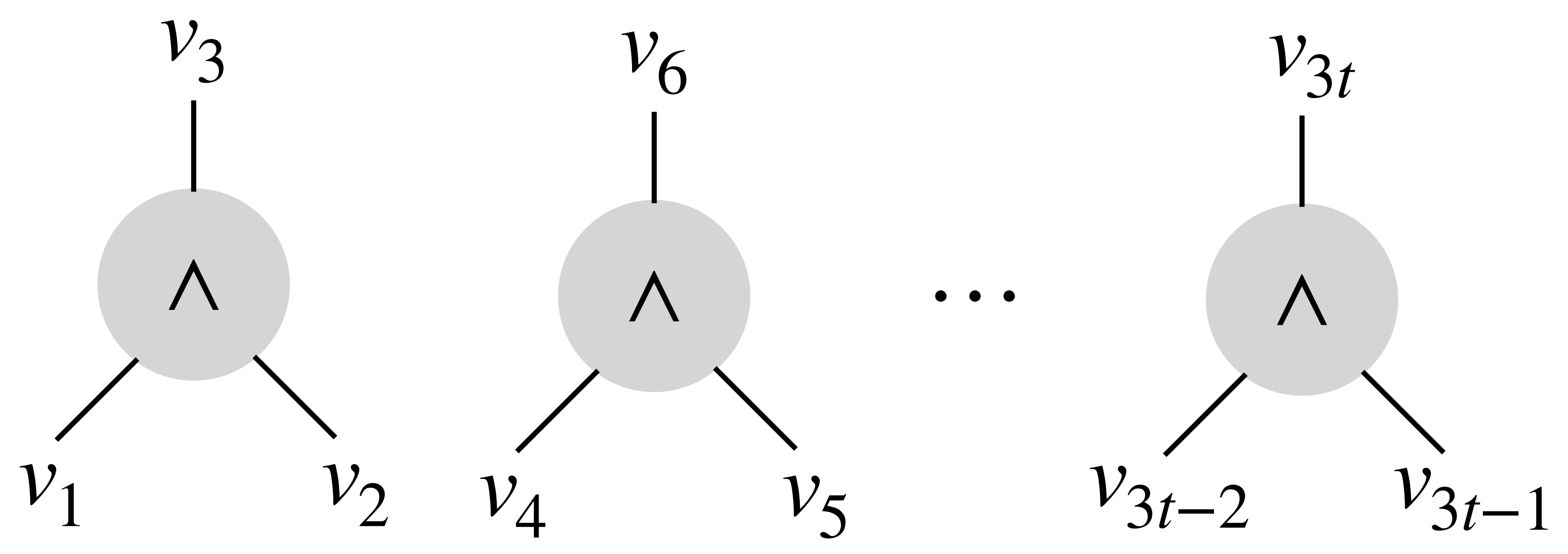
2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

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

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



1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

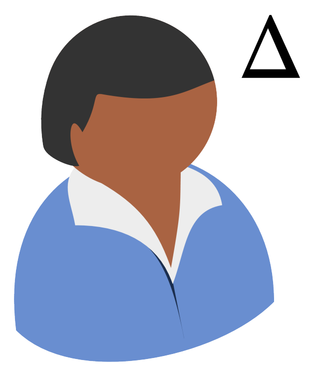
$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$



Garbler

Invariant

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

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

Evaluator

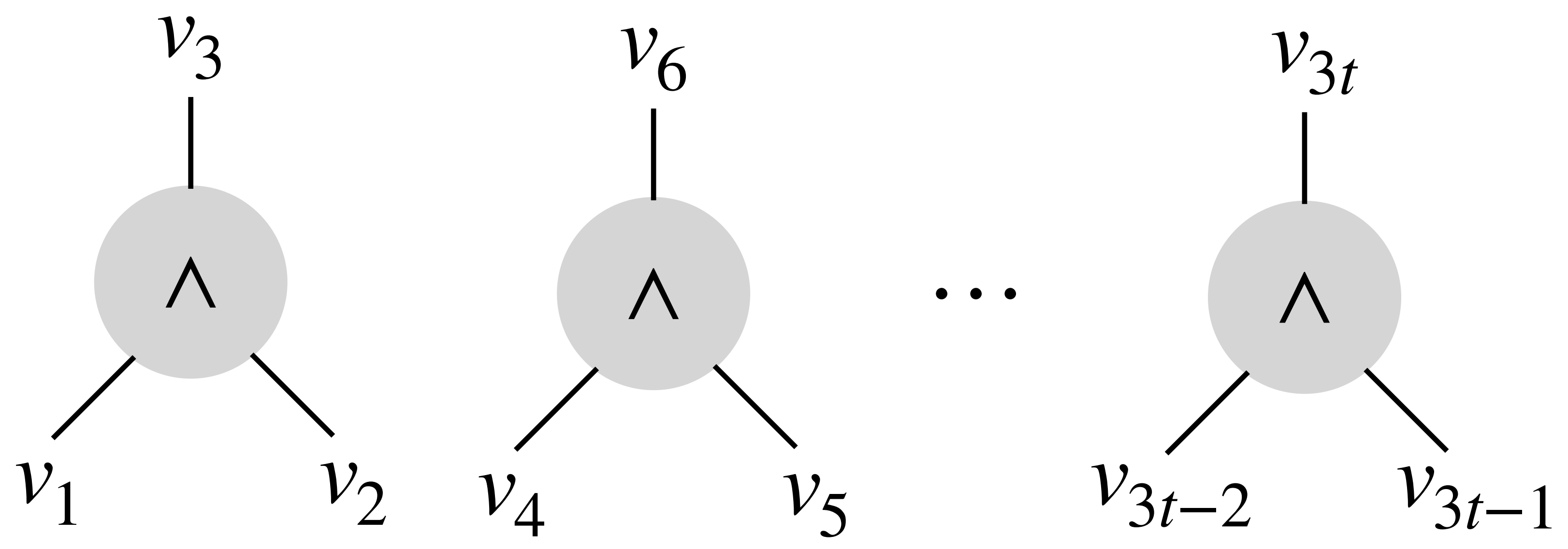
$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

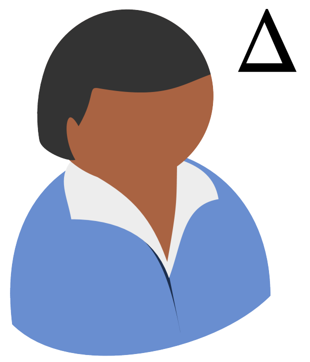
$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

$$K_\mathsf{R}$$

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod{p}$$

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





Garbler

Invariant

$$g_i \oplus e_i = v_i$$

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

Evaluator

1. Packing

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

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

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

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

K_L K_R

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

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

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

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

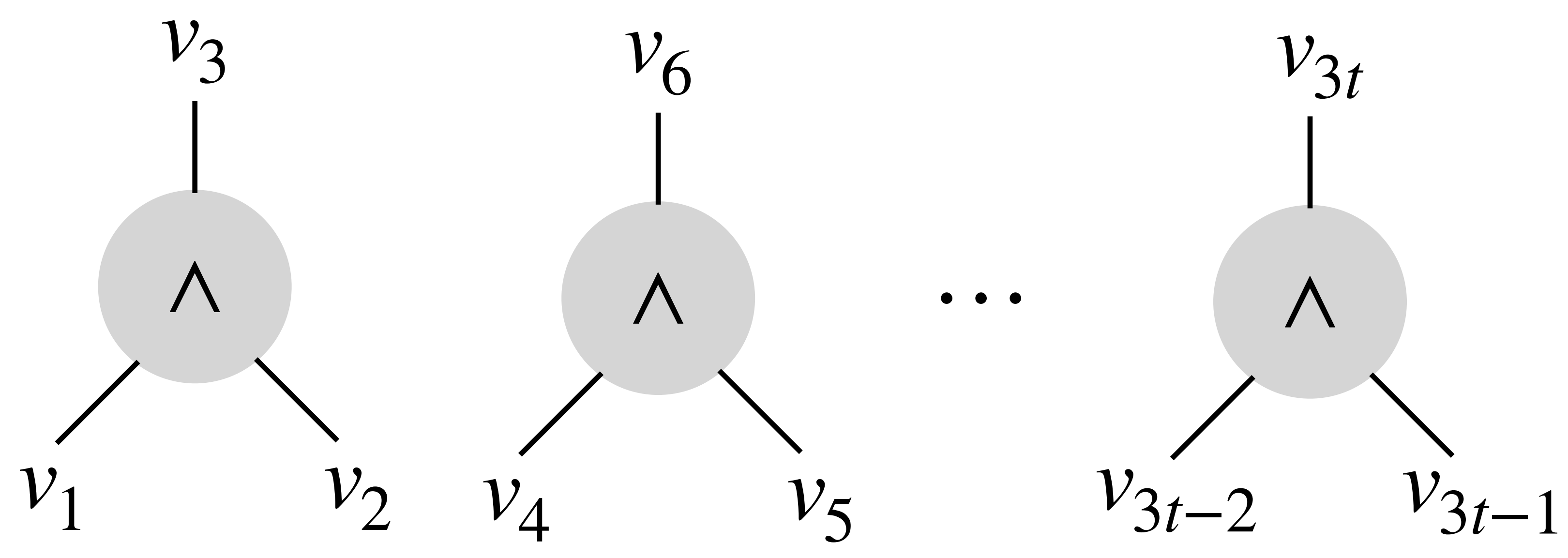
2. Gate Evaluation

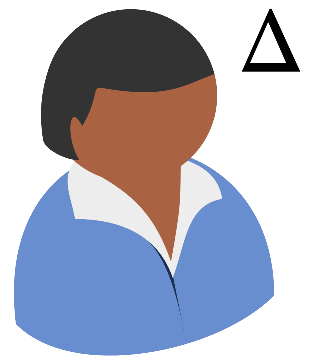
$$V = V_1 \cdot V_2$$

3. Unpacking

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

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$
$$G_\mathsf{L} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

K_L K_R

$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$
$$E_\mathsf{L} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod{p}$$
$$L_\mathsf{L} = \Delta \cdot E_\mathsf{L} - K_\mathsf{L} \pmod{p}$$

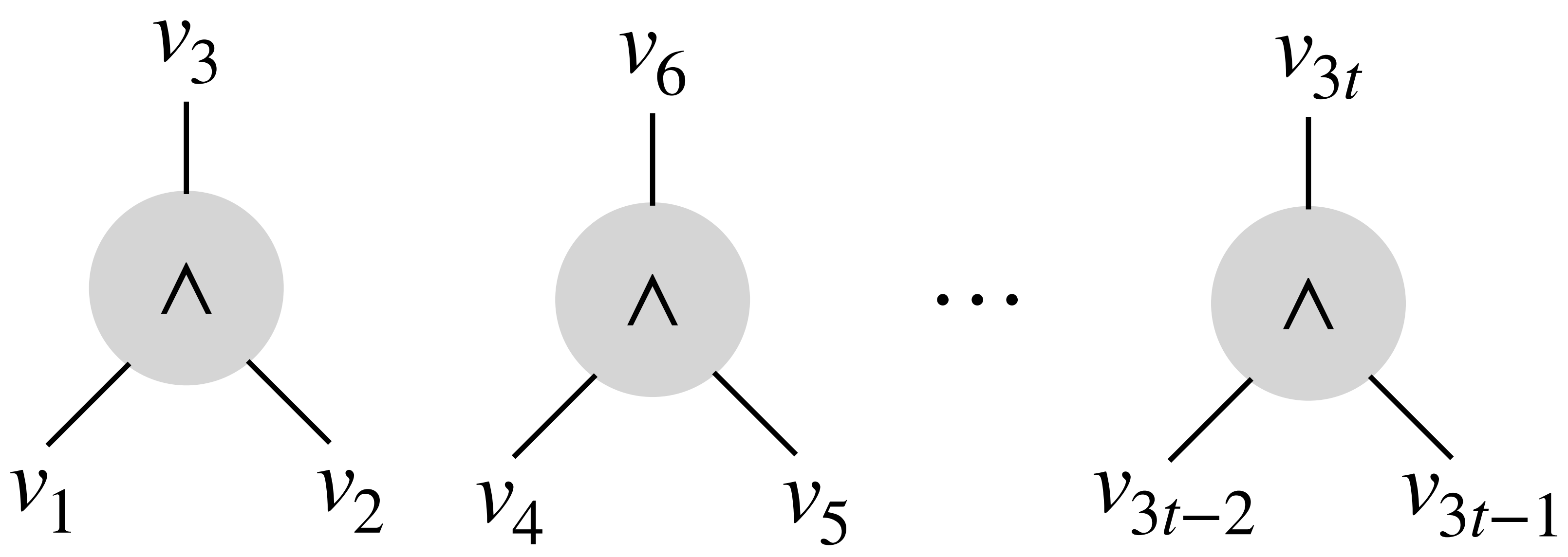
2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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



1. Packing

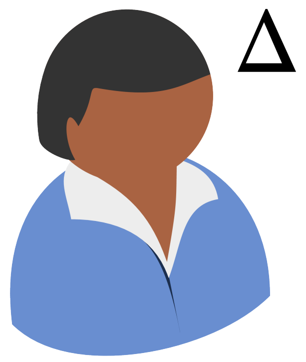
$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$



Garbler

Invariant

$$\mathsf{g}_i \oplus \mathsf{e}_i = v_i$$
$$k_i + \ell_i = \Delta \cdot \mathsf{e}_i \pmod{p}$$

Evaluator

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$
$$G_\mathsf{L} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

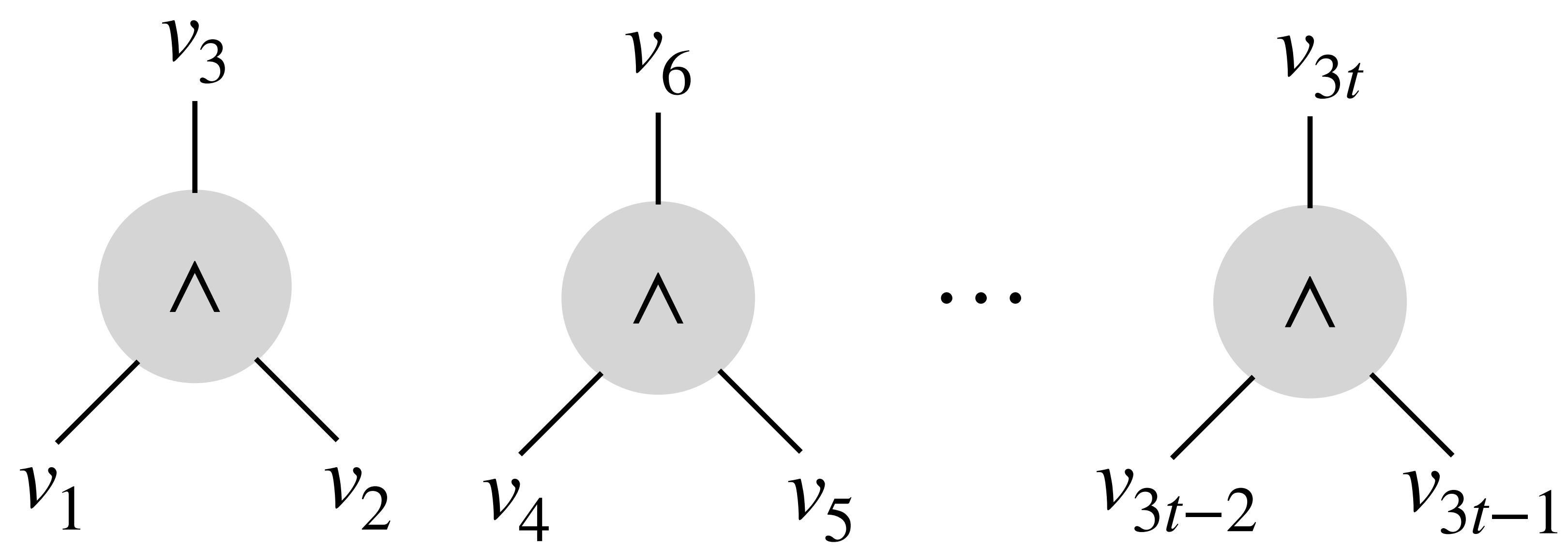
$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$
$$E_\mathsf{L} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

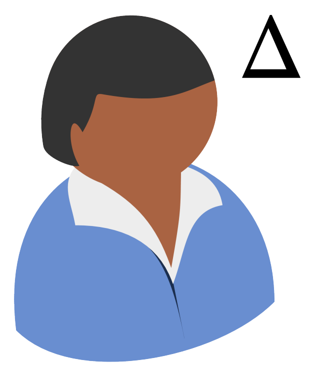
K_L K_R

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod{p}$$
$$L_\mathsf{L} = \Delta \cdot E_\mathsf{L} - K_\mathsf{L} \pmod{p}$$

$$V = V_1 \cdot V_2 = (G_\mathsf{L} + E_\mathsf{L}) \cdot (G_\mathsf{R} + E_\mathsf{R})$$

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





Garbler

Invariant

$$\mathsf{g}_i \oplus \mathsf{e}_i = v_i$$
$$k_i + \ell_i = \Delta \cdot \mathsf{e}_i \pmod{p}$$

Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$
$$G_\mathsf{L} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$
$$E_\mathsf{L} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

K_L K_R

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod{p}$$
$$L_\mathsf{L} = \Delta \cdot E_\mathsf{L} - K_\mathsf{L} \pmod{p}$$

2. Gate Evaluation

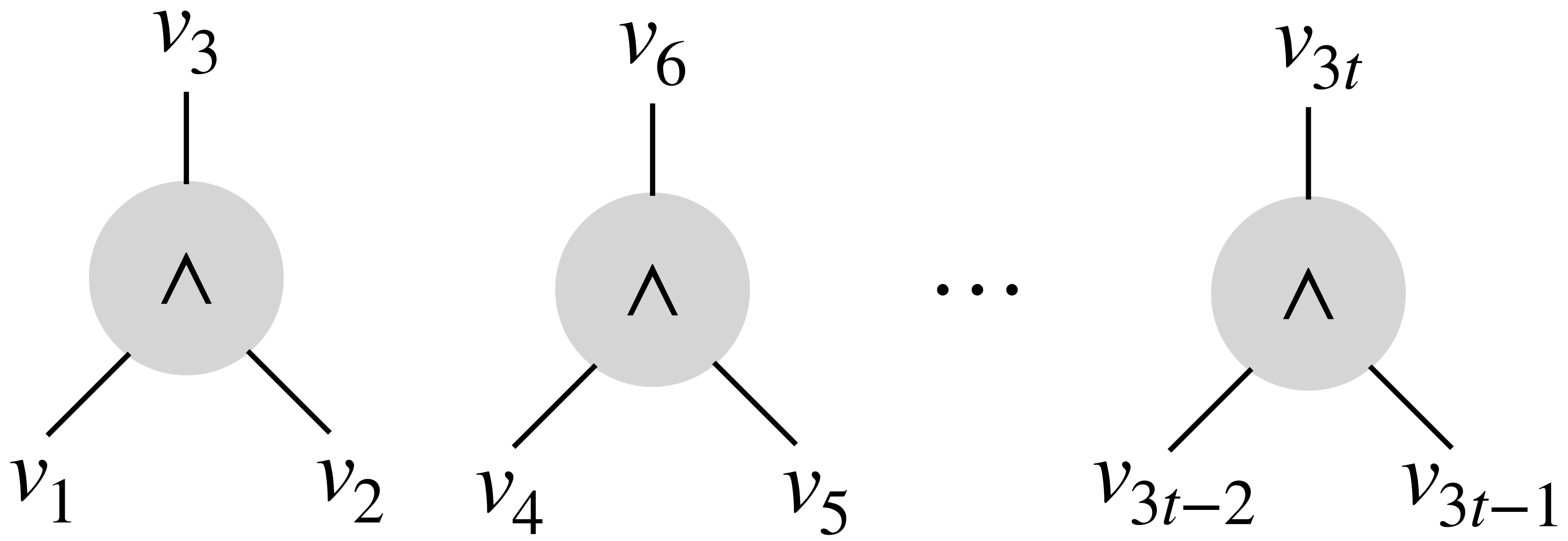
$$V = V_1 \cdot V_2$$

$$V = V_1 \cdot V_2 = (G_\mathsf{L} + E_\mathsf{L}) \cdot (G_\mathsf{R} + E_\mathsf{R})$$
$$= G_\mathsf{L} \cdot G_\mathsf{R} + G_\mathsf{L} \cdot E_\mathsf{R} + E_\mathsf{L} \cdot G_\mathsf{R} + E_\mathsf{L} \cdot E_\mathsf{R}$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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



1. Packing

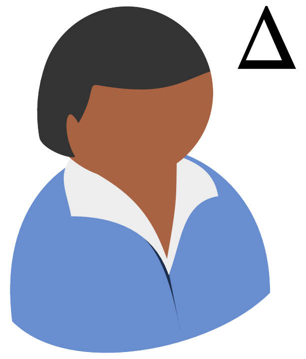
$$V_R = \text{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_L = \text{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

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



Δ

Garbler

Invariant

$$g_i \oplus e_i = v_i$$
$$k_i + \ell_i = \Delta \cdot e_i \pmod p$$

Evaluator

$$G_R = \text{Pack}(g_2, g_5, \ldots, g_{3t-1})$$
$$G_L = \text{Pack}(g_1, g_4, \ldots, g_{3t-2})$$

$K_L \quad K_R$

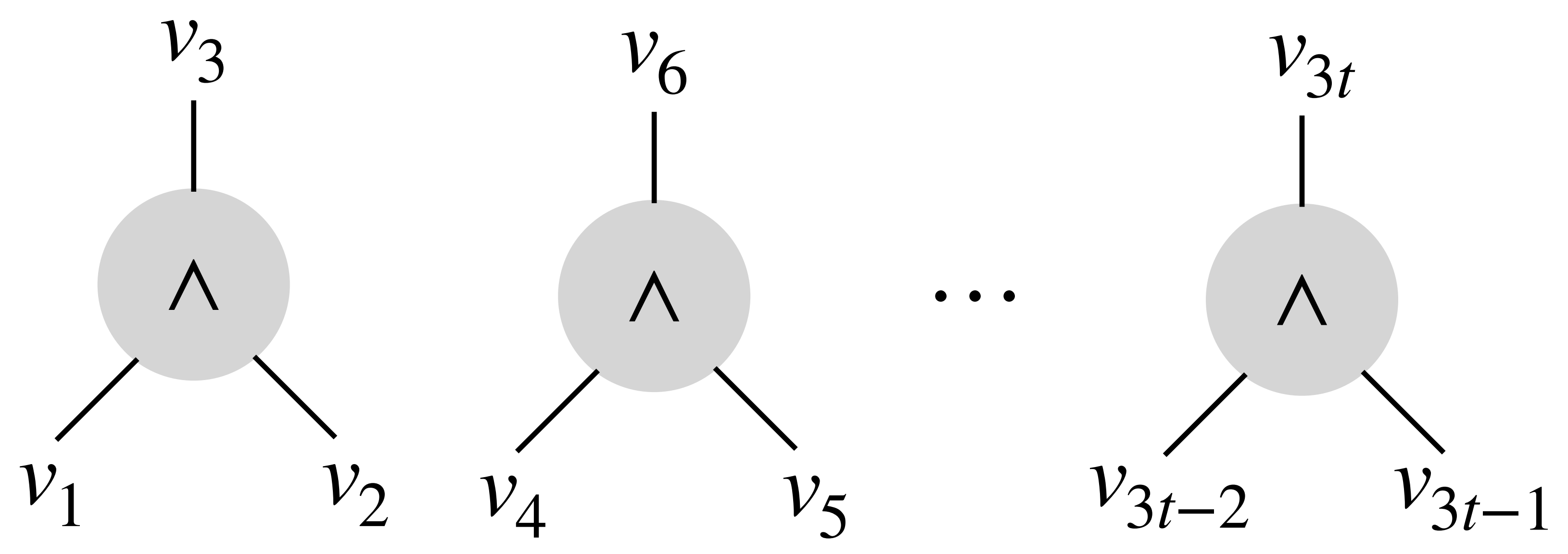
$$E_R = \text{Pack}(e_2, e_5, \ldots, e_{3t-1})$$
$$E_L = \text{Pack}(e_1, e_4, \ldots, e_{3t-2})$$

$$L_R = \Delta \cdot E_R - K_R \pmod p$$
$$L_L = \Delta \cdot E_L - K_L \pmod p$$

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

Packed encoding is homomorphic

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



Garbler Δ

Invariant

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

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

Evaluator

1. Packing

$$V_\mathsf{R} = \text{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_\mathsf{L} = \text{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_\mathsf{R} = \text{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$G_\mathsf{L} = \text{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$E_\mathsf{R} = \text{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

$$E_\mathsf{L} = \text{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

$$\xrightarrow{\quad}$$

K_L K_R

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod p$$

$$L_\mathsf{L} = \Delta \cdot E_\mathsf{L} - K_\mathsf{L} \pmod p$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

$$V = V_1 \cdot V_2 = (G_\mathsf{L} + E_\mathsf{L}) \cdot (G_\mathsf{R} + E_\mathsf{R})$$

Packed encoding is homomorphic

$$= G_\mathsf{L} \cdot G_\mathsf{R} + G_\mathsf{L} \cdot E_\mathsf{R} + E_\mathsf{L} \cdot G_\mathsf{R} + E_\mathsf{L} \cdot E_\mathsf{R}$$

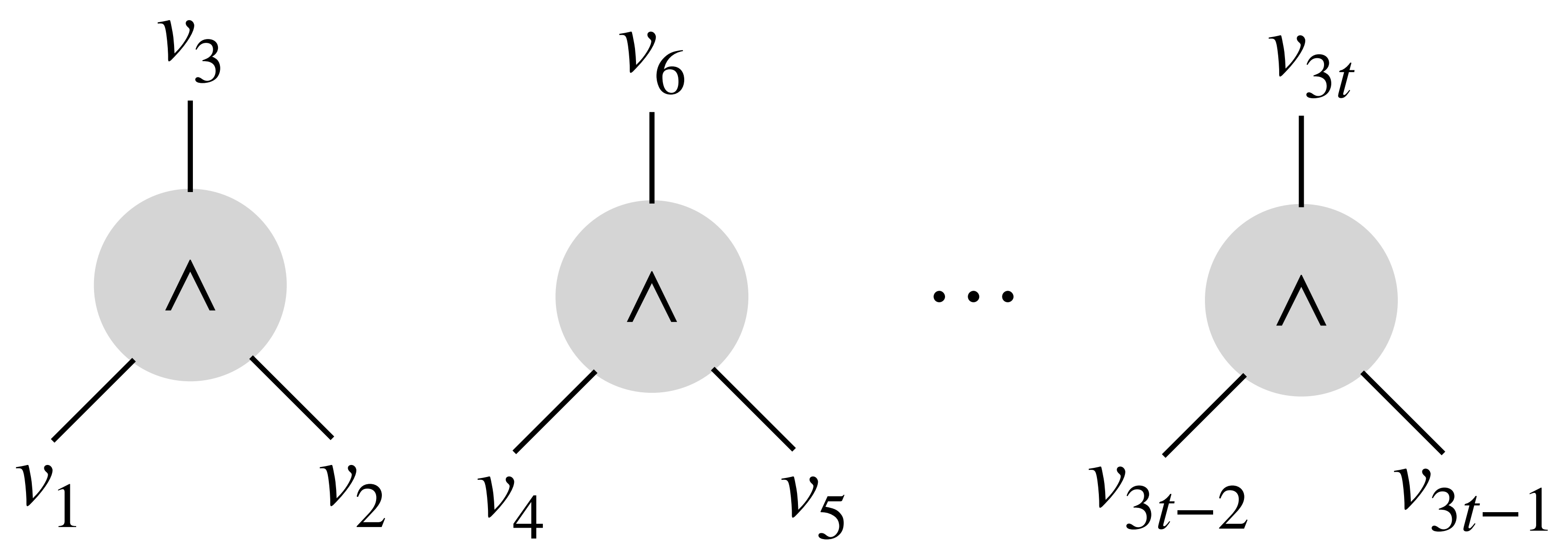
Locally computed by Garbler

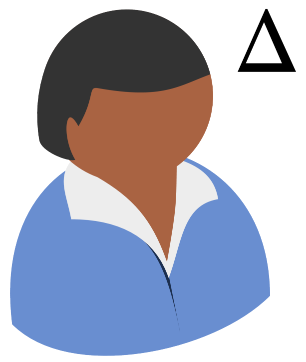
Locally computed by Evaluator

3. Unpacking

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

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





Garbler

Invariant

$$\mathsf{g}_i \oplus \mathsf{e}_i = v_i$$
$$k_i + \ell_i = \Delta \cdot \mathsf{e}_i \pmod{p}$$

Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$
$$G_\mathsf{L} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$
$$E_\mathsf{L} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

K_L K_R

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod{p}$$
$$L_\mathsf{L} = \Delta \cdot E_\mathsf{L} - K_\mathsf{L} \pmod{p}$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

$$V = V_1 \cdot V_2 = (G_\mathsf{L} + E_\mathsf{L}) \cdot (G_\mathsf{R} + E_\mathsf{R})$$

Packed encoding is homomorphic

$$= G_\mathsf{L} \cdot G_\mathsf{R} + G_\mathsf{L} \cdot E_\mathsf{R} + E_\mathsf{L} \cdot G_\mathsf{R} + E_\mathsf{L} \cdot E_\mathsf{R}$$

Locally computed by Garbler

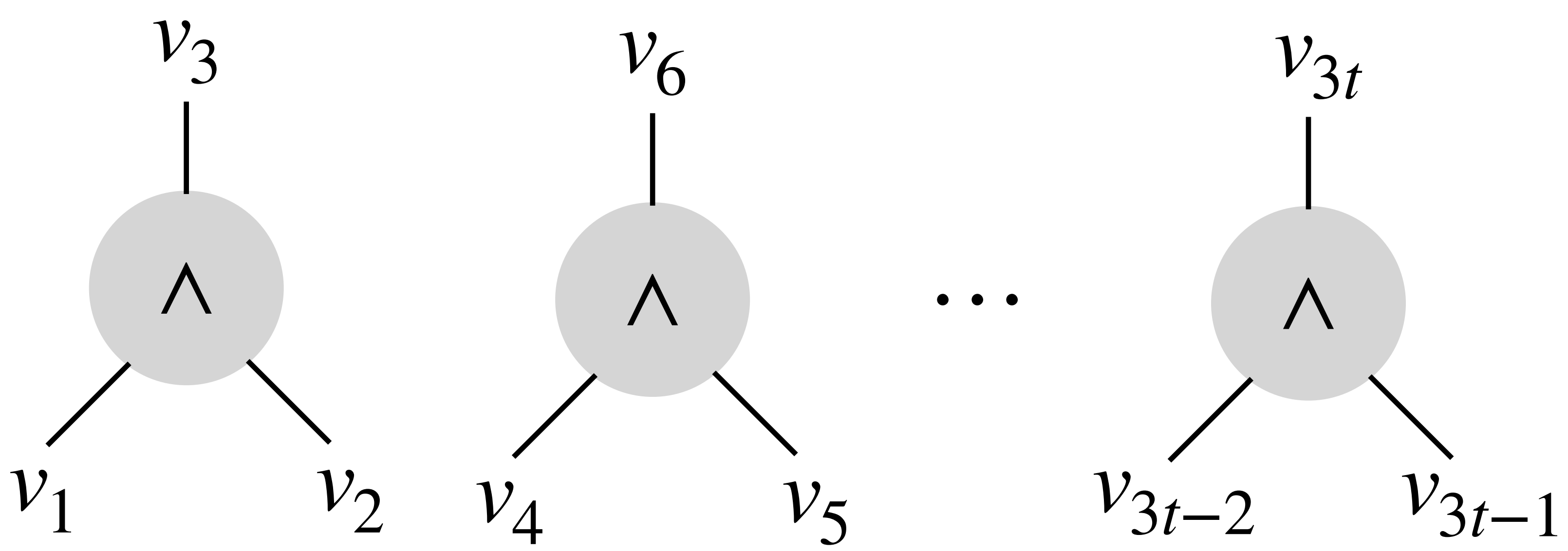
Use multiplication gadget

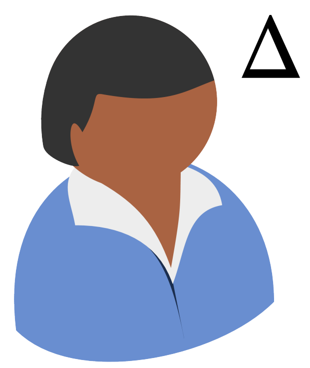
Locally computed by Evaluator

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_{\mathsf{R}} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$G_{\mathsf{L}} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$E_{\mathsf{R}} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

$$E_{\mathsf{L}} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

K_{L} K_{R}

$$L_{\mathsf{R}} = \Delta \cdot E_{\mathsf{R}} - K_{\mathsf{R}} \pmod{p}$$

$$L_{\mathsf{L}} = \Delta \cdot E_{\mathsf{L}} - K_{\mathsf{L}} \pmod{p}$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

$$V = V_1 \cdot V_2 = (G_{\mathsf{L}} + E_{\mathsf{L}}) \cdot (G_{\mathsf{R}} + E_{\mathsf{R}})$$

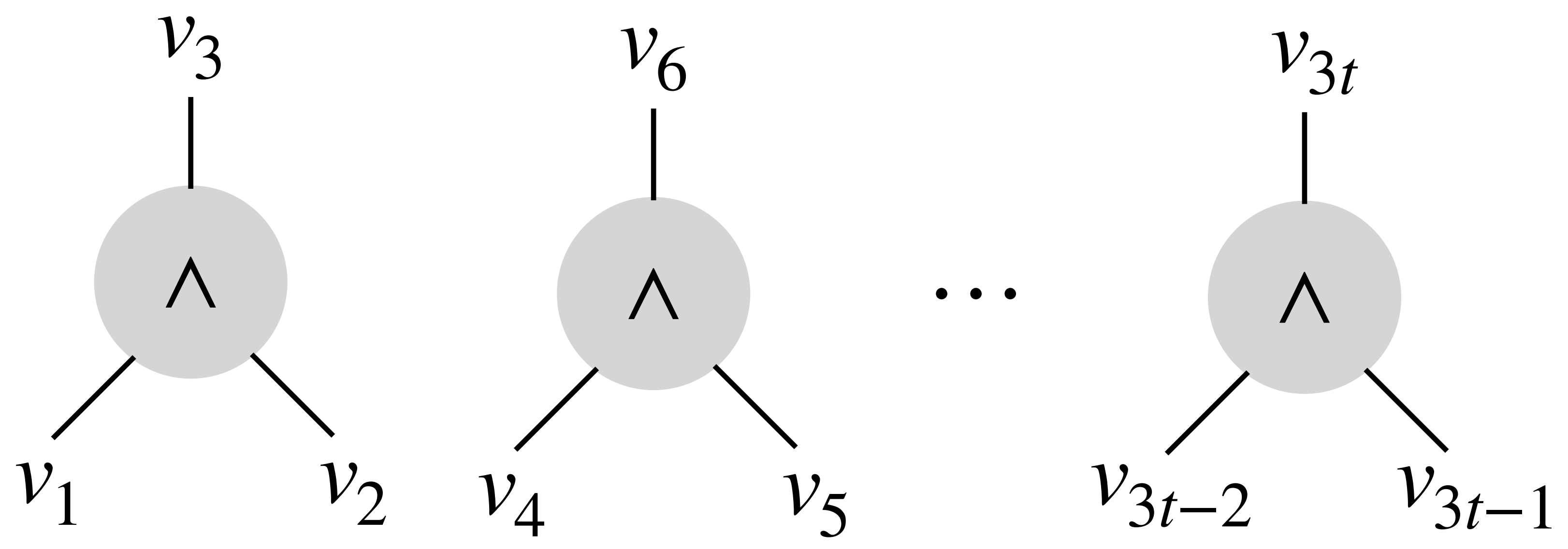
$$= G_{\mathsf{L}} \cdot G_{\mathsf{R}} + G_{\mathsf{L}} \cdot E_{\mathsf{R}} + E_{\mathsf{L}} \cdot G_{\mathsf{R}} + E_{\mathsf{L}} \cdot E_{\mathsf{R}}$$

Use multiplication gadget

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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



1. Packing

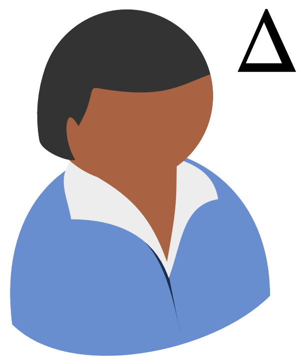
$$V_R = \text{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_L = \text{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

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



Δ

Garbler

Invariant

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

Evaluator

$$G_R = \text{Pack}(g_2, g_5, \ldots, g_{3t-1})$$
$$G_L = \text{Pack}(g_1, g_4, \ldots, g_{3t-2})$$

$K_L \quad K_R$

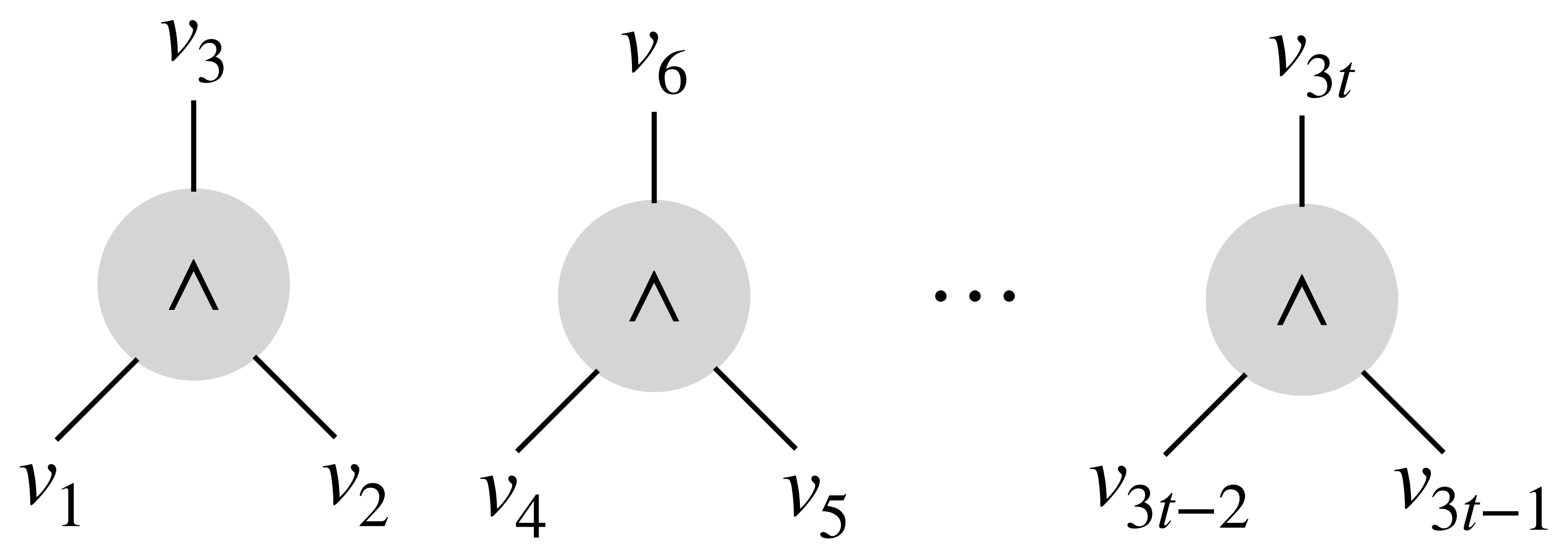
G

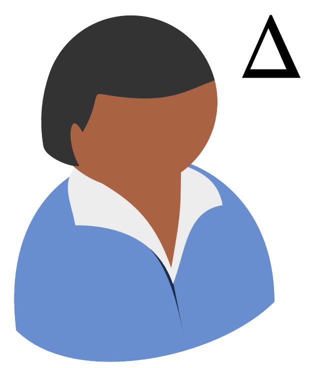
$$E_R = \text{Pack}(e_2, e_5, \ldots, e_{3t-1})$$
$$E_L = \text{Pack}(e_1, e_4, \ldots, e_{3t-2})$$

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

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

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





Invariant

$$\mathsf{g}_i \oplus \mathsf{e}_i = v_i$$
$$k_i + \ell_i = \Delta \cdot \mathsf{e}_i \pmod p$$

1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_{\mathsf{R}} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$
$$G_{\mathsf{L}} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$E_{\mathsf{R}} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$
$$E_{\mathsf{L}} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

K_{L} K_{R}

$$L_{\mathsf{R}} = \Delta \cdot E_{\mathsf{R}} - K_{\mathsf{R}} \pmod p$$
$$L_{\mathsf{L}} = \Delta \cdot E_{\mathsf{L}} - K_{\mathsf{L}} \pmod p$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

G

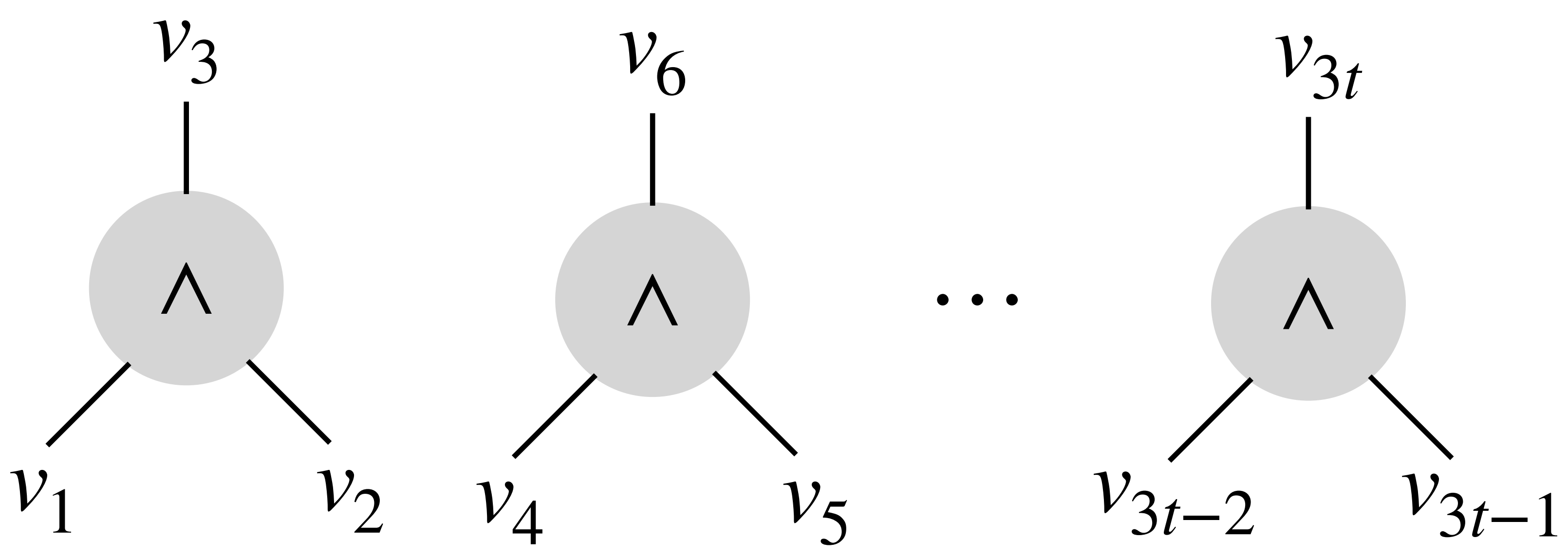
$$E = \mathsf{Pack}(v_3, \ldots, v_{3t}) - G$$

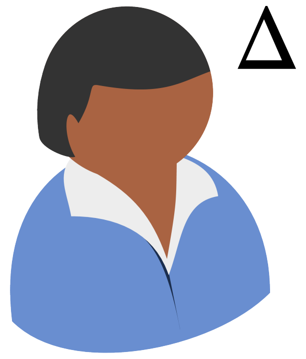
3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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

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





Δ

Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$G_\mathsf{L} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

$$E_\mathsf{L} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

K_L K_R

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod p$$

$$L_\mathsf{L} = \Delta \cdot E_\mathsf{L} - K_\mathsf{L} \pmod p$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

G

K

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

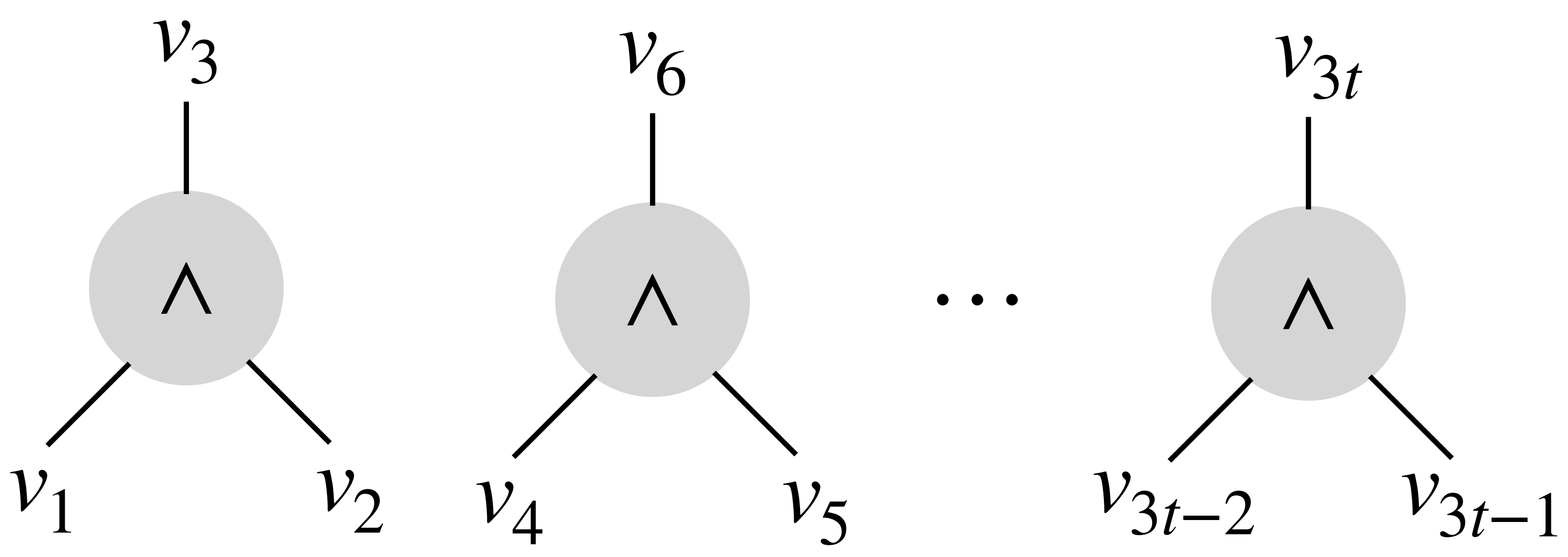
$$L = \Delta \cdot E - K \pmod p$$

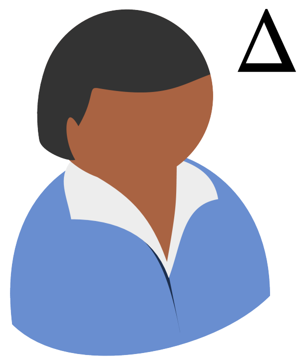
3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

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

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




Δ

Garbler

Invariant

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

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


Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \dots, v_{3t-1})$$

$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \dots, v_{3t-2})$$

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \dots, \mathsf{g}_{3t-1})$$

$$G_\mathsf{L} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \dots, \mathsf{g}_{3t-2})$$

$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \dots, \mathsf{e}_{3t-1})$$

$$E_\mathsf{L} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \dots, \mathsf{e}_{3t-2})$$

$$K_\mathsf{L} \quad K_\mathsf{R}$$

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod{p}$$

$$L_\mathsf{L} = \Delta \cdot E_\mathsf{L} - K_\mathsf{L} \pmod{p}$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

$$G$$

$$K$$

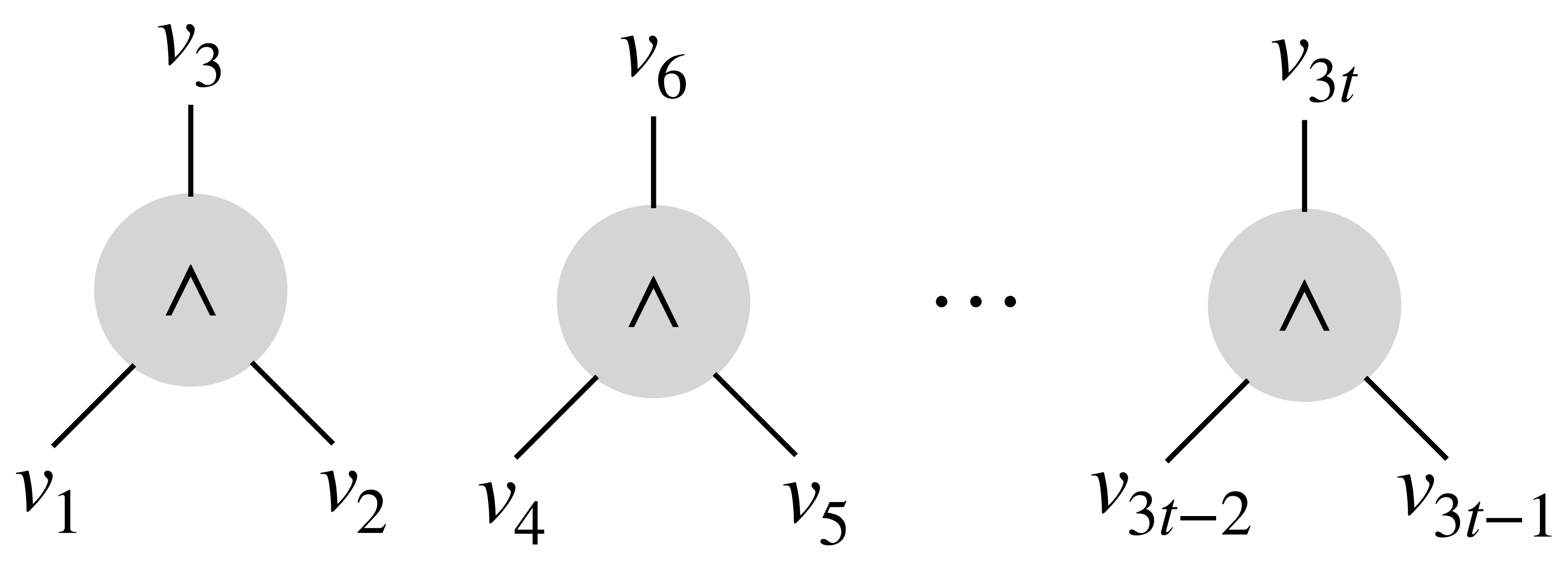
$$E = \mathsf{Pack}(v_3, \dots, v_{3t}) - G$$

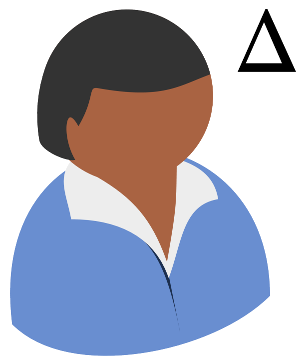
$$L = \Delta \cdot E - K \pmod{p}$$

3. Unpacking

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

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_{\mathsf{R}} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$G_{\mathsf{L}} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$E_{\mathsf{R}} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

$$E_{\mathsf{L}} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

K_{L} K_{R}

$$L_{\mathsf{R}} = \Delta \cdot E_{\mathsf{R}} - K_{\mathsf{R}} \pmod p$$

$$L_{\mathsf{L}} = \Delta \cdot E_{\mathsf{L}} - K_{\mathsf{L}} \pmod p$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

G

K

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

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

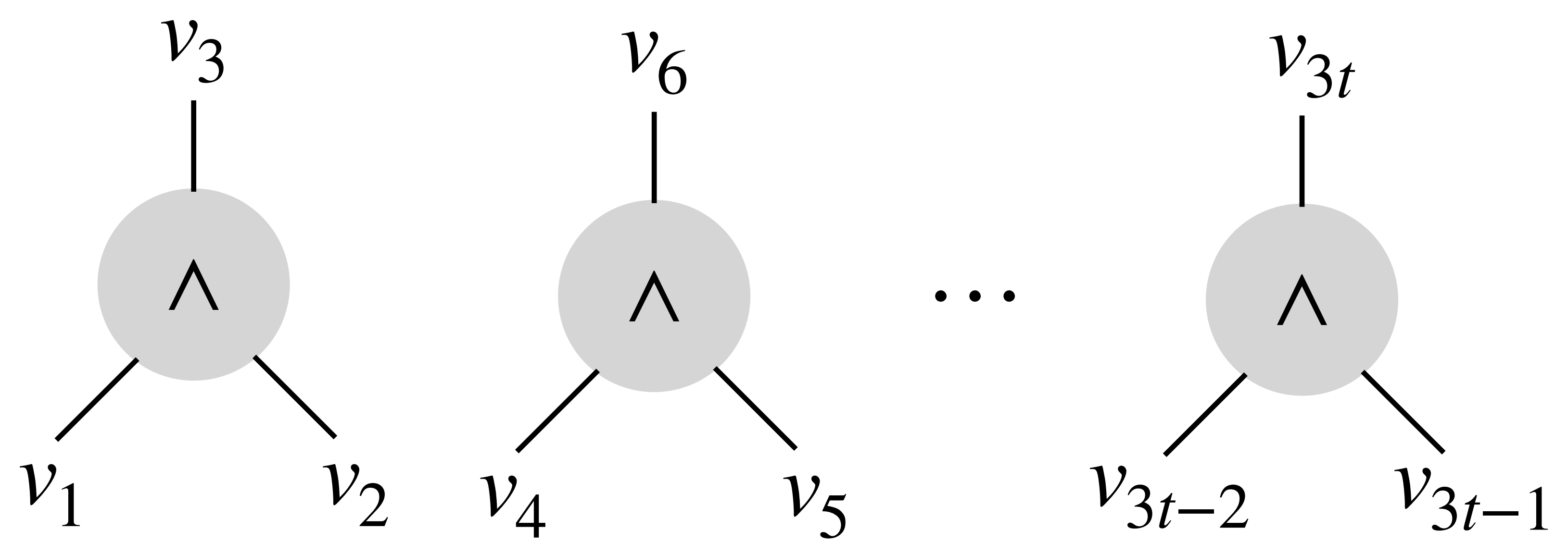
3. Unpacking

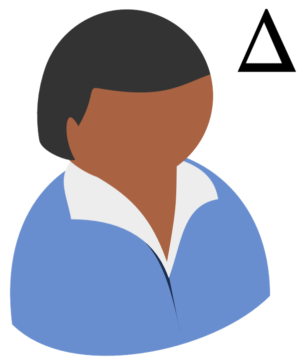
$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

$$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$$

$$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$$

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





Garbler

Invariant

$$g_i \oplus e_i = v_i$$

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

Evaluator

1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_{\mathsf{R}} = \mathsf{Pack}(g_2, g_5, \ldots, g_{3t-1})$$

$$G_{\mathsf{L}} = \mathsf{Pack}(g_1, g_4, \ldots, g_{3t-2})$$

$$E_{\mathsf{R}} = \mathsf{Pack}(e_2, e_5, \ldots, e_{3t-1})$$

$$E_{\mathsf{L}} = \mathsf{Pack}(e_1, e_4, \ldots, e_{3t-2})$$

K_{L} K_{R}

$$L_{\mathsf{R}} = \Delta \cdot E_{\mathsf{R}} - K_{\mathsf{R}} \pmod{p}$$

$$L_{\mathsf{L}} = \Delta \cdot E_{\mathsf{L}} - K_{\mathsf{L}} \pmod{p}$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

G

K

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

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

3. Unpacking

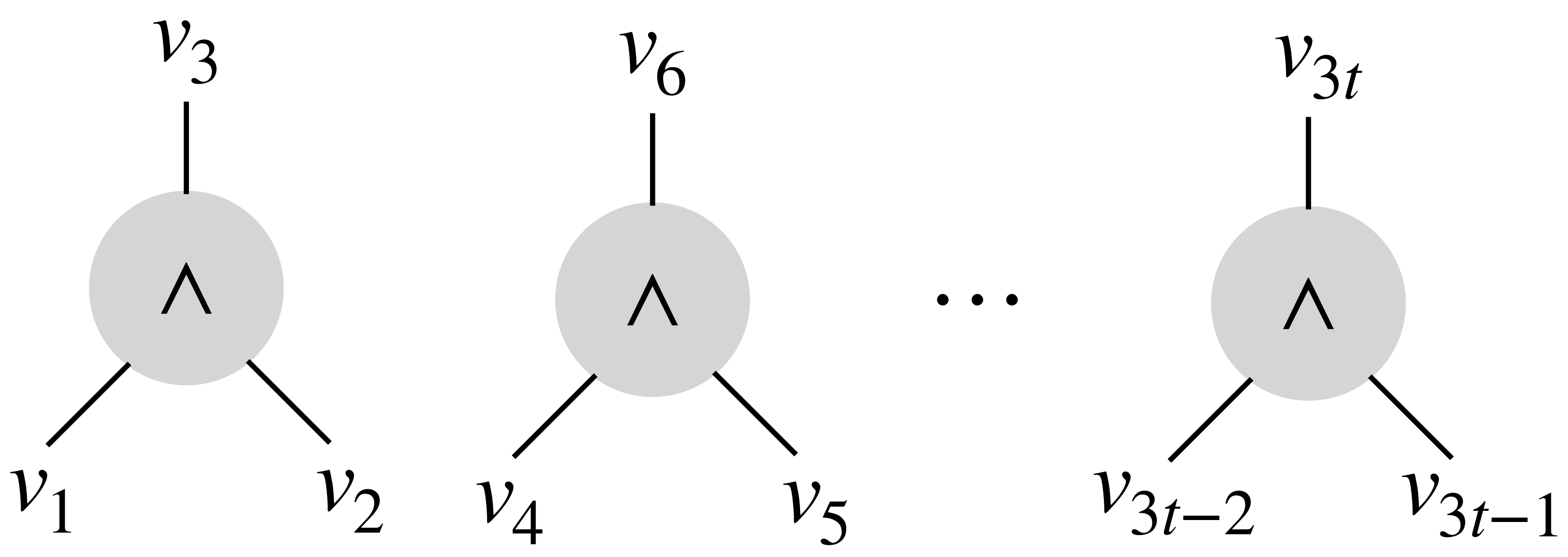
$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

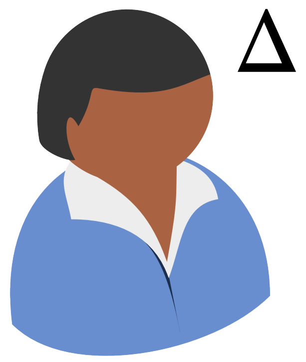
$$(g_3, g_6, \ldots, g_{3t}) = \mathsf{UnPack}(G)$$

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

$$(e_3, e_6, \ldots, e_{3t}) = \mathsf{UnPack}(E)$$

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

$G_{\mathsf{R}} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$

$G_{\mathsf{L}} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$

$E_{\mathsf{R}} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$

$E_{\mathsf{L}} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$

$K_{\mathsf{L}} \quad K_{\mathsf{R}}$

$L_{\mathsf{R}} = \Delta \cdot E_{\mathsf{R}} - K_{\mathsf{R}} \pmod p$

$L_{\mathsf{L}} = \Delta \cdot E_{\mathsf{L}} - K_{\mathsf{L}} \pmod p$

G

K

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

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

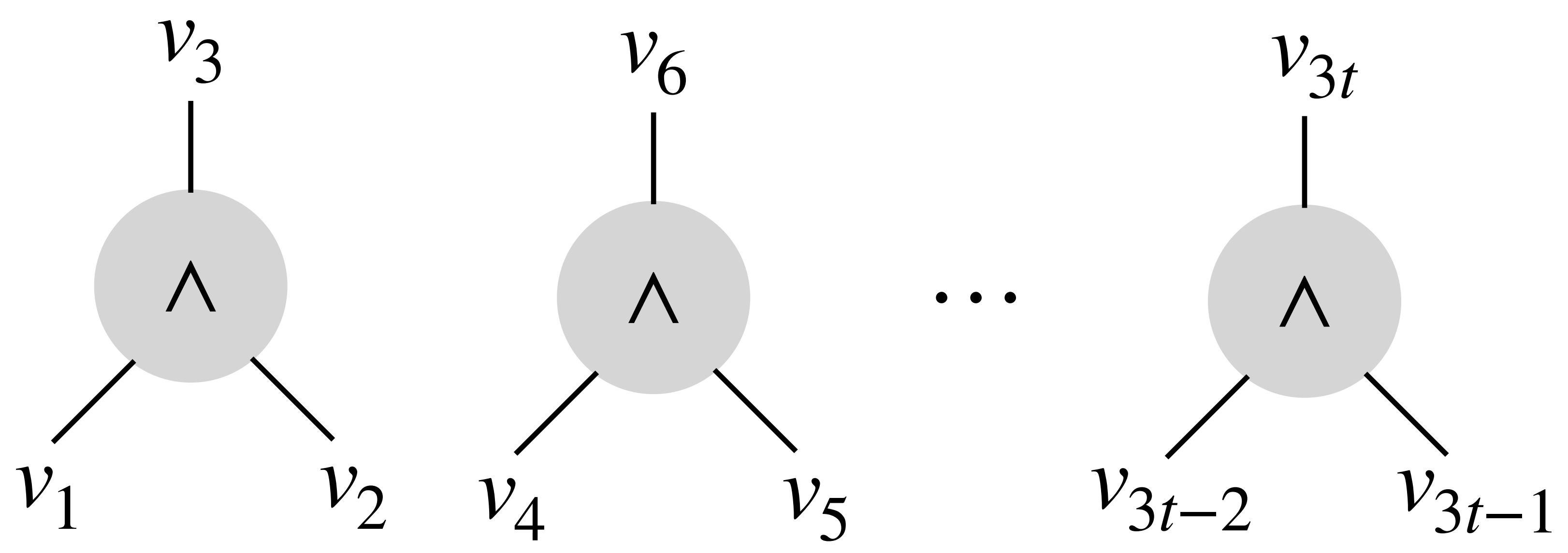
$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$

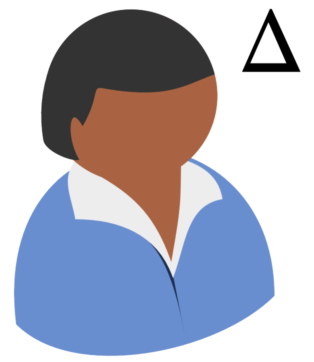
UnPack is $\mathbb{F}_2$-linear

$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$

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

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_\mathrm{R} = \mathrm{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_\mathrm{L} = \mathrm{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathrm{UnPack}(V)$$

G

K

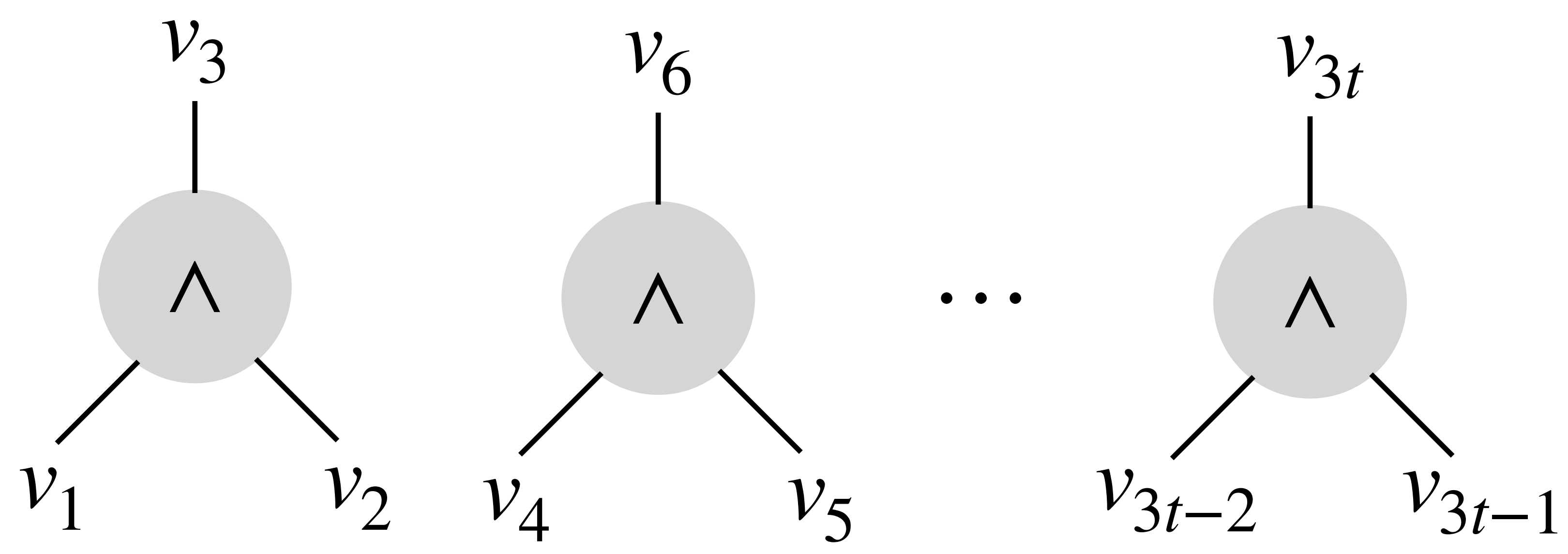
$$E = \mathrm{Pack}(v_3, \ldots, v_{3t}) - G$$

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

$$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathrm{UnPack}(G)$$

$$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathrm{UnPack}(E)$$

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



1. Packing

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

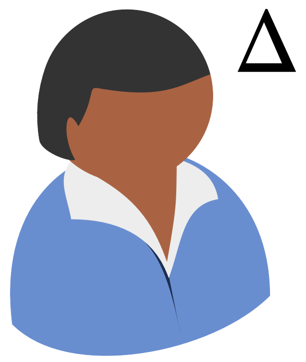
$$V_L = \text{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

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



Δ

Garbler

Invariant

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

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

Evaluator

G

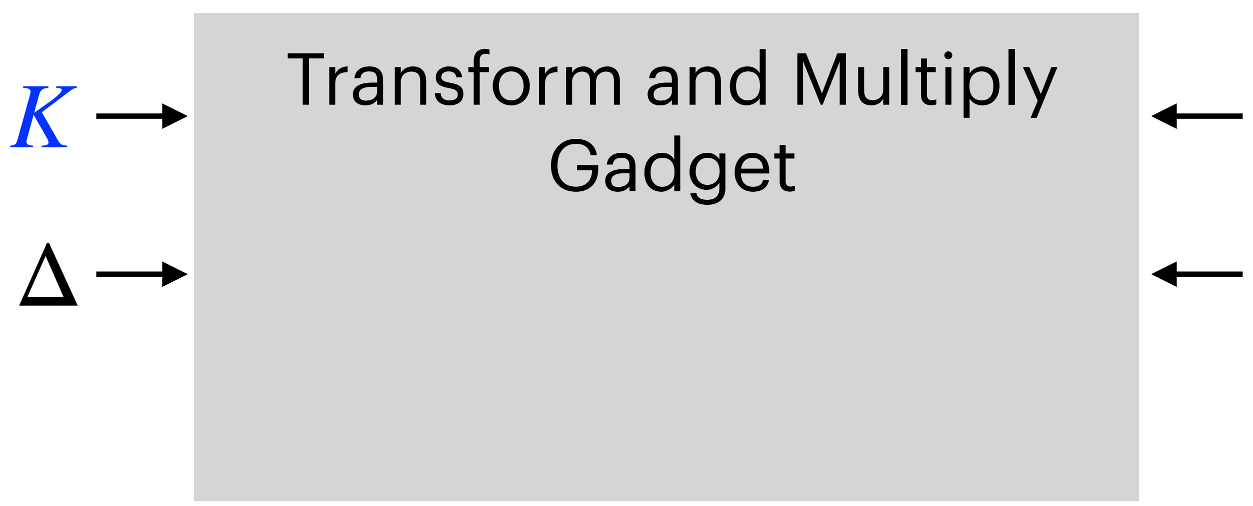
K

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

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

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

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



Transform and Multiply Gadget

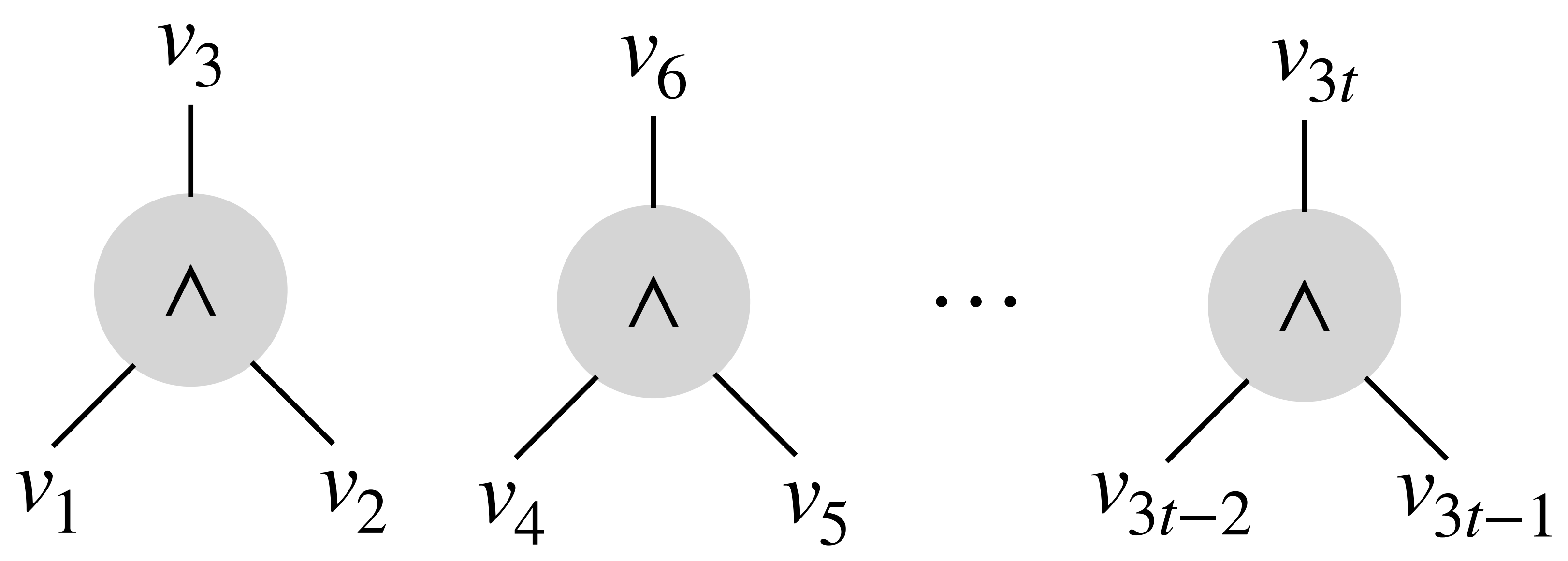
$K \rightarrow$

$\Delta \rightarrow$

$\leftarrow L = \Delta \cdot E - K \pmod p$

$\leftarrow E$

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



1. Packing

$$V_{\mathrm{R}} = \mathrm{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_{\mathrm{L}} = \mathrm{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathrm{UnPack}(V)$$

Garbler Δ

Invariant

$$\mathsf{g}_i \oplus \mathsf{e}_i = v_i$$
$$k_i + \ell_i = \Delta \cdot \mathsf{e}_i \pmod p$$

Evaluator

G

K

$$E = \mathrm{Pack}(v_3, \ldots, v_{3t}) - G$$
$$L = \Delta \cdot E - K \pmod p$$

$$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathrm{UnPack}(G)$$

$$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathrm{UnPack}(E)$$

$K \rightarrow$

$\Delta \rightarrow$

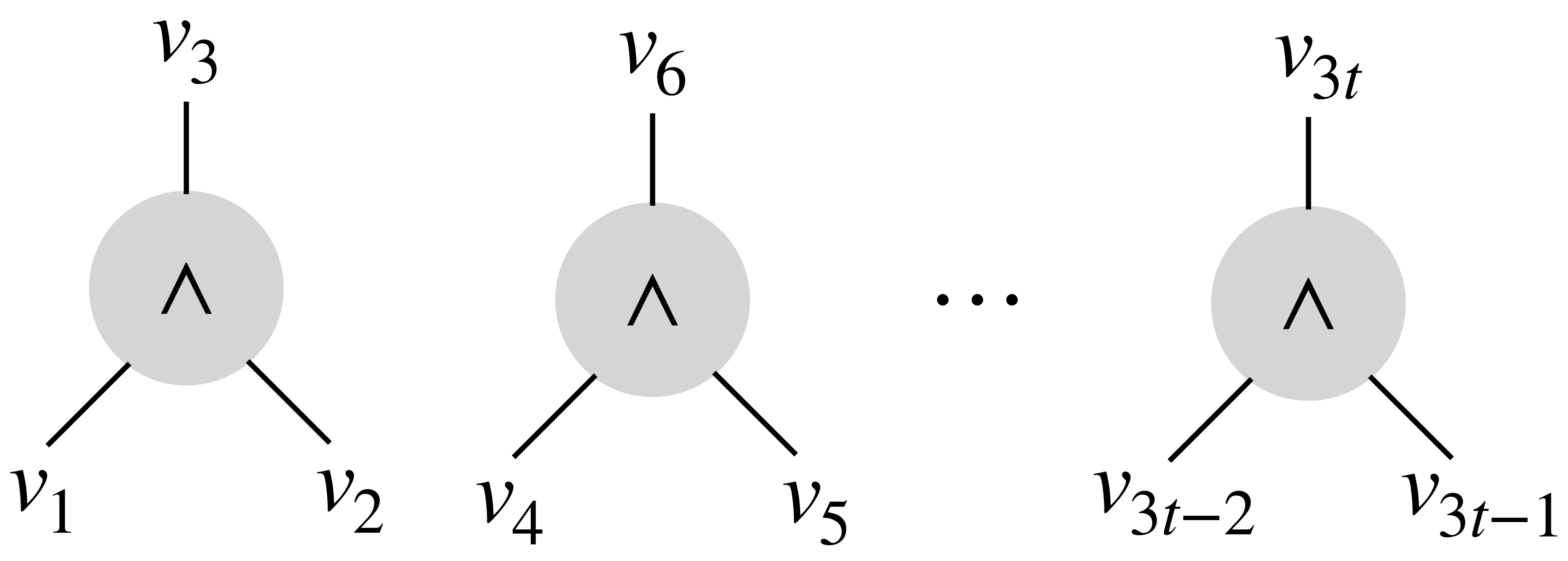
Transform and Multiply Gadget

$f_i(x) = \mathrm{Index}(i, \mathrm{UnPack}(x))$

$\leftarrow L = \Delta \cdot E - K \pmod p$

$\leftarrow E$

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



1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

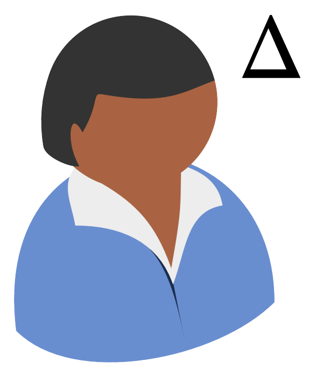
$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$



Garbler

Invariant

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

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

Evaluator

G

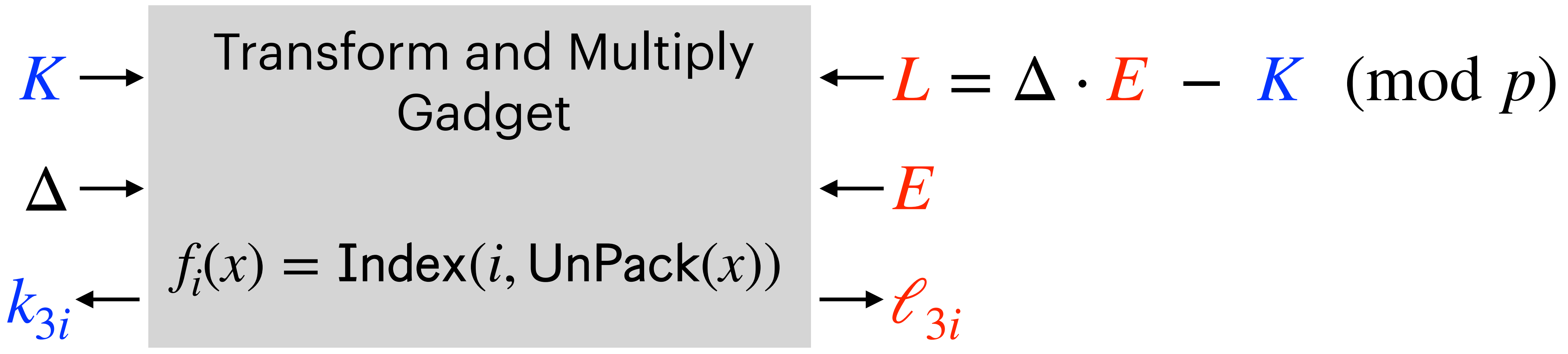
K

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

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

$$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$$

$$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$$



Transform and Multiply Gadget

$$f_i(x) = \mathsf{Index}(i, \mathsf{UnPack}(x))$$

$K \rightarrow$

$\Delta \rightarrow$

$k_{3i} \leftarrow$

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

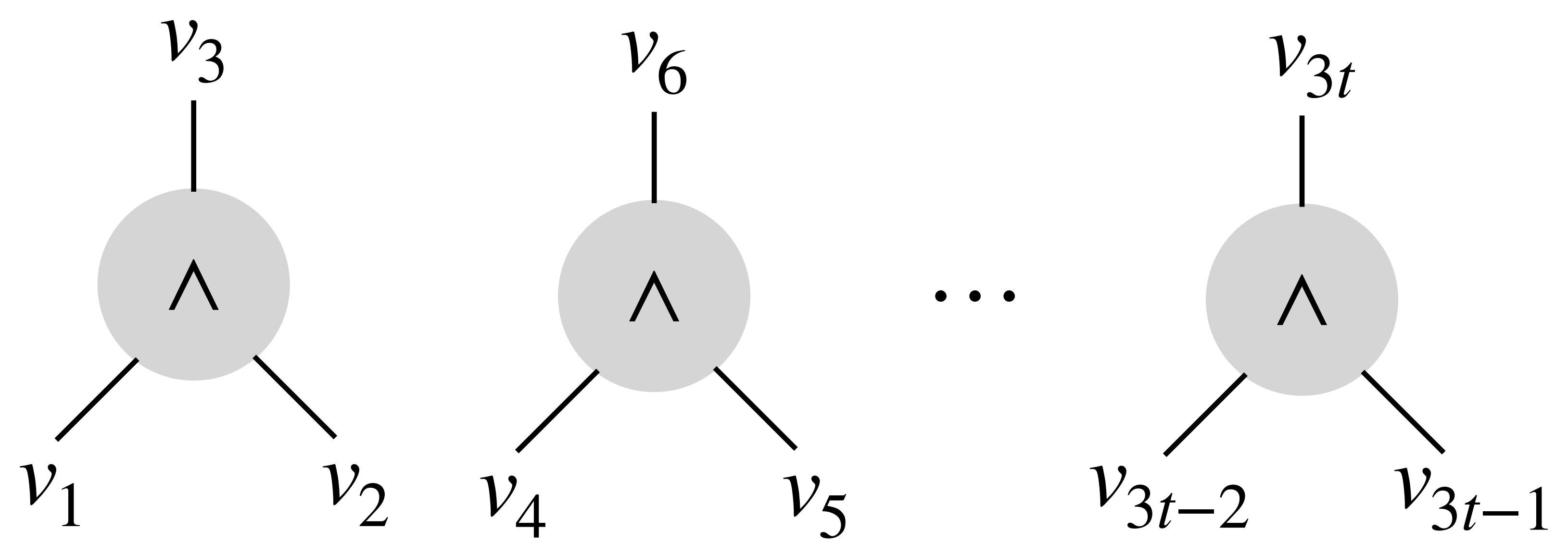
$\leftarrow E$

$\rightarrow \ell_{3i}$

$$k_{3i} + \ell_{3i} = \Delta \cdot f_i(E)$$

$$= \Delta \cdot \mathsf{e}_{3i}$$

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



1. Packing

$$V_R = \text{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_L = \text{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

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

Garbler Δ

Invariant

$$\mathsf{g}_i \oplus \mathsf{e}_i = v_i$$
$$k_i + \ell_i = \Delta \cdot \mathsf{e}_i \pmod p$$

Evaluator

G

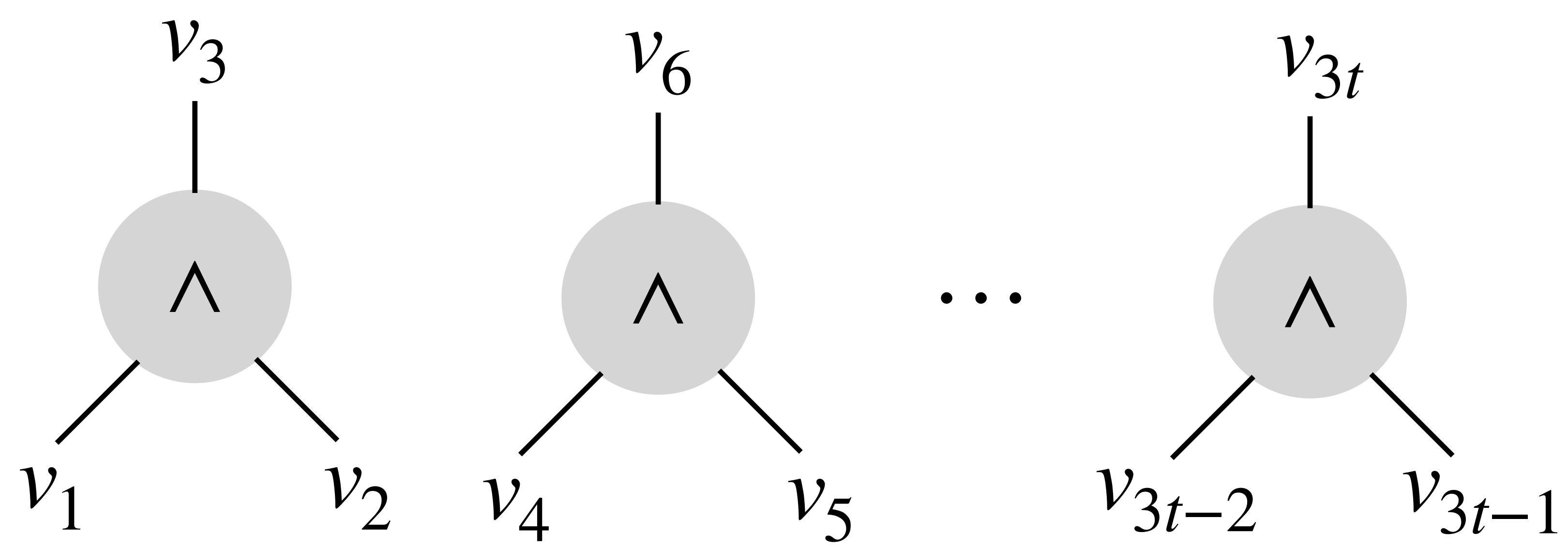
K

$$E = \text{Pack}(v_3, \ldots, v_{3t}) - G$$
$$L = \Delta \cdot E - K \pmod p$$

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

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

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



1. Packing

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

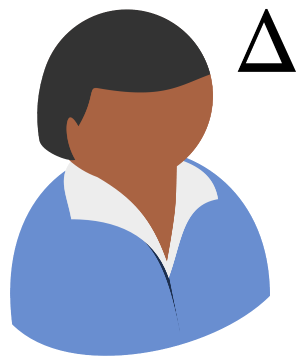
$$V_L = \text{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

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



Garbler

Invariant

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

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

Evaluator

G

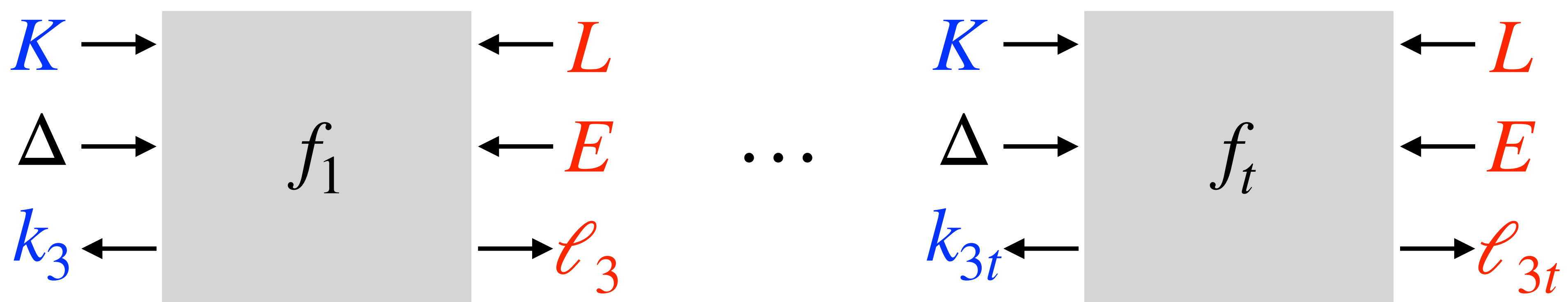
K

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

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

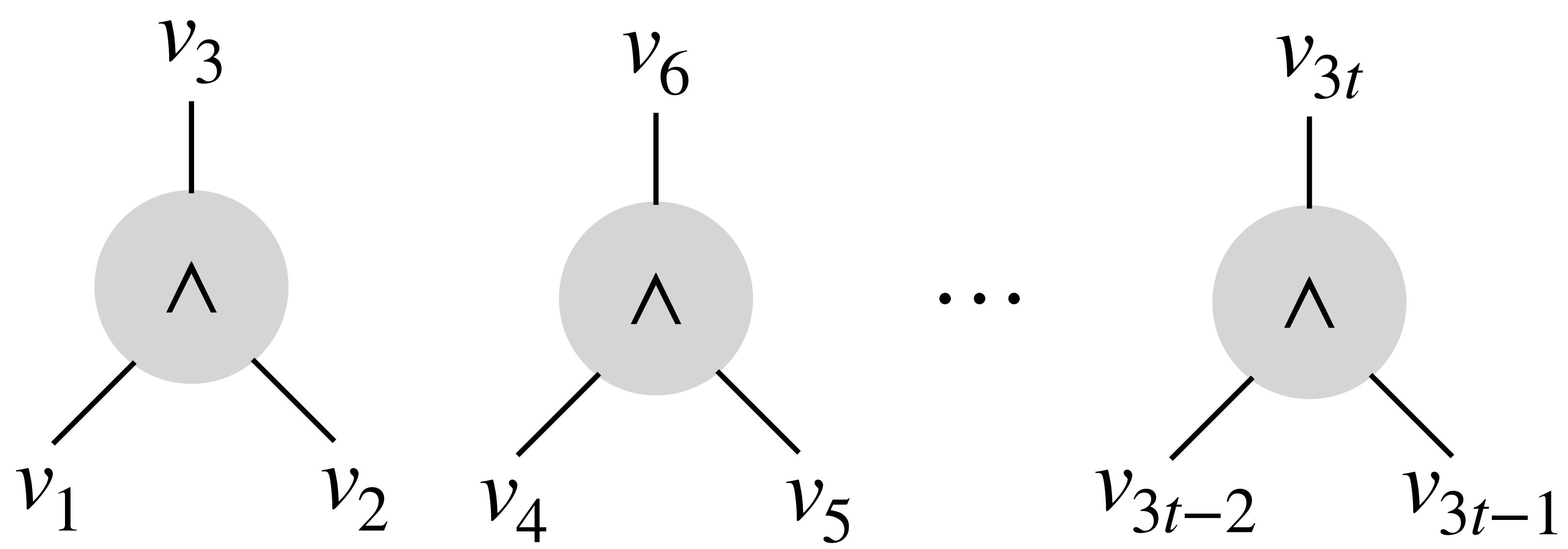
$$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \text{UnPack}(G)$$

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



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

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



1. Packing

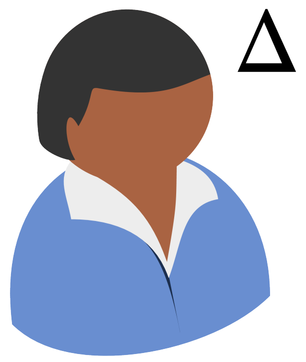
$$V_R = \text{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_L = \text{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

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



Garbler

Invariant

$$g_i \oplus e_i = v_i$$
$$k_i + \ell_i = \Delta \cdot e_i \pmod p$$

Evaluator

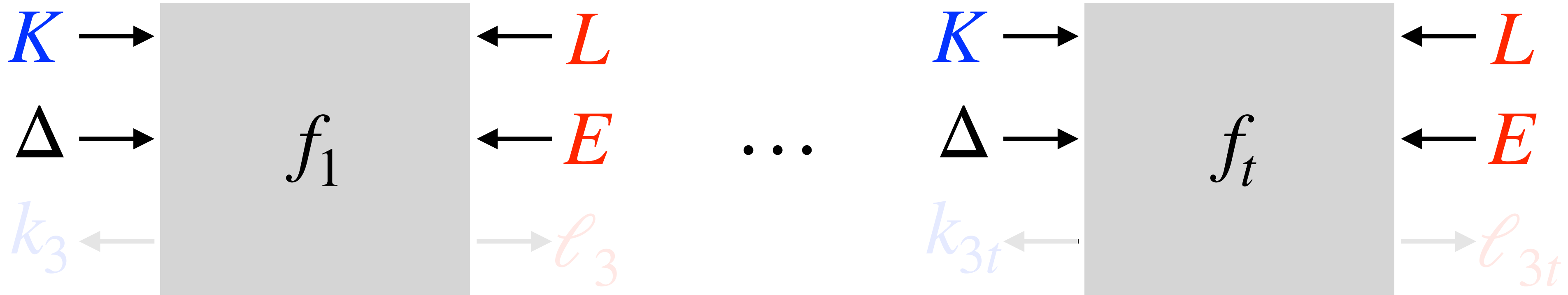
G

K

$$E = \text{Pack}(v_3, \ldots, v_{3t}) - G$$
$$L = \Delta \cdot E - K \pmod p$$

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

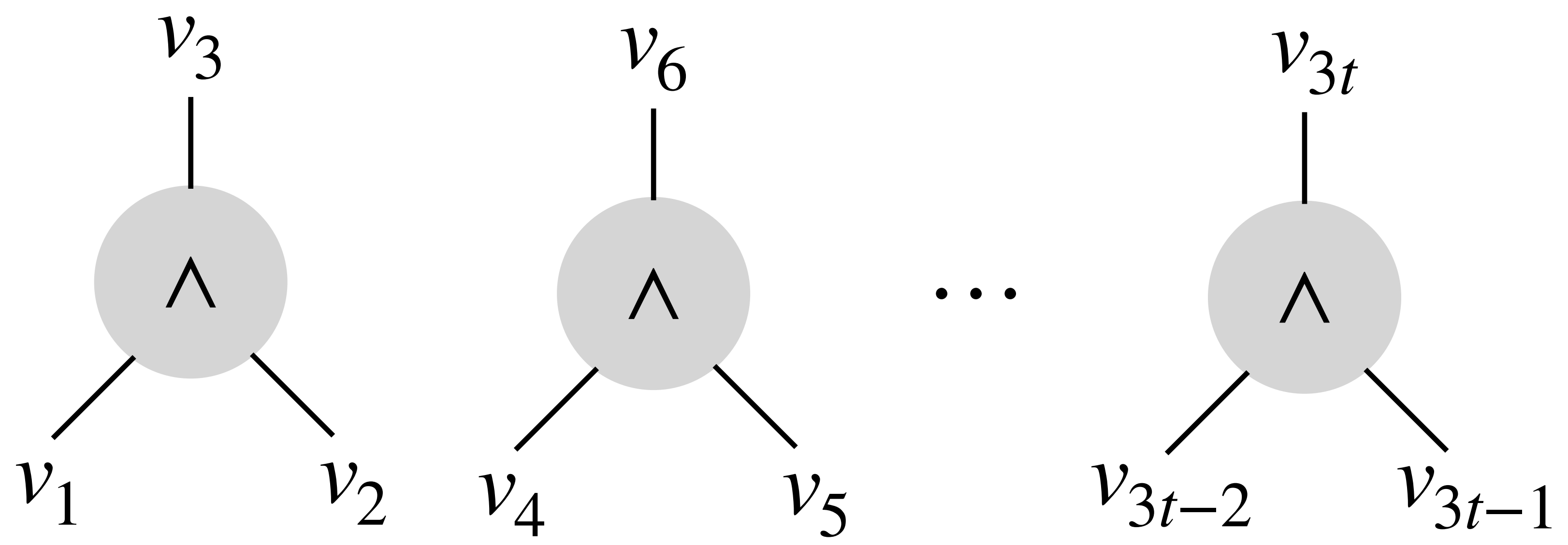
$$(e_3, e_6, \ldots, e_{3t}) = \text{UnPack}(E)$$

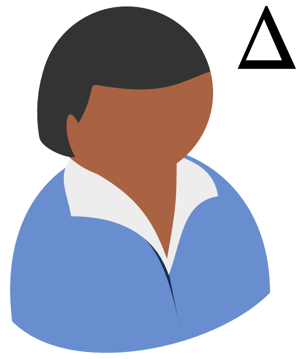


t invocations $\implies$ $O(\lambda)$-bit communication per gate

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

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$G_\mathsf{L} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$K_\mathsf{L} \quad K_\mathsf{R}$$

$$G$$

$$K$$

$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

$$E_\mathsf{L} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

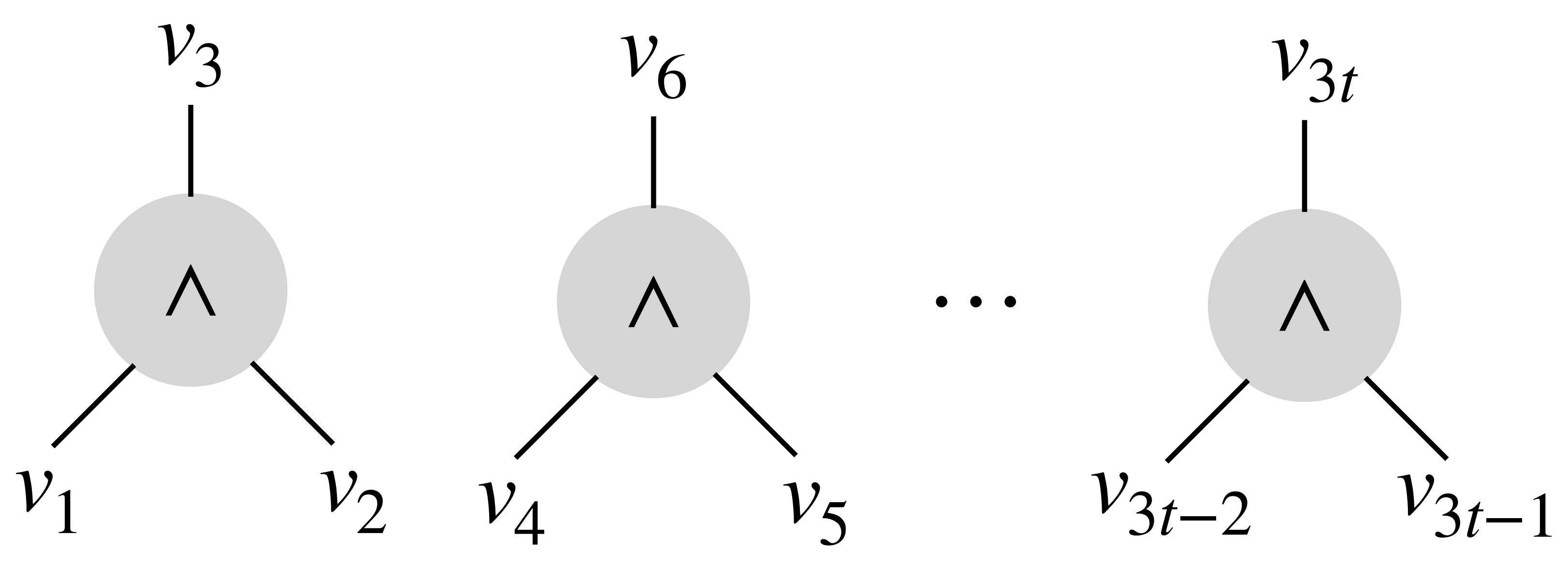
$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod{p}$$

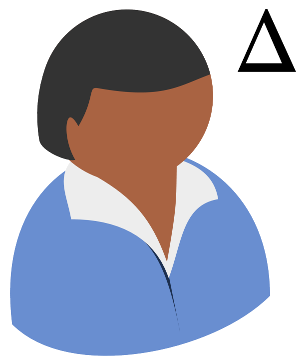
$$L_\mathsf{L} = \Delta \cdot E_\mathsf{L} - K_\mathsf{L} \pmod{p}$$

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

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

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




Δ

Garbler

Invariant

$$\mathsf{g}_i \oplus \mathsf{e}_i = v_i$$
$$k_i + \ell_i = \Delta \cdot \mathsf{e}_i \pmod p$$

Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$
$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$
$$G_\mathsf{L} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$
$$E_\mathsf{L} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

K_L K_R

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod p$$
$$L_\mathsf{L} = \Delta \cdot E_\mathsf{L} - K_\mathsf{L} \pmod p$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

G

K

$$E = \mathsf{Pack}(v_3, \ldots, v_{3t}) - G$$
$$L = \Delta \cdot E - K \pmod p$$

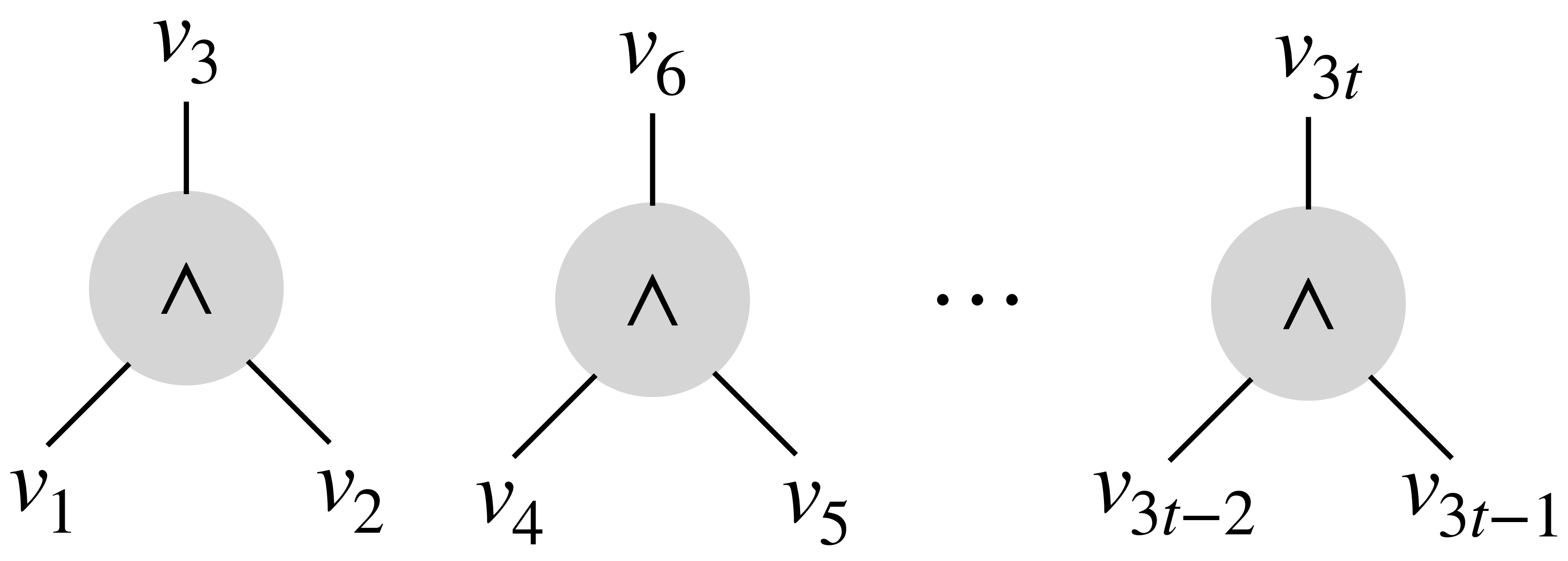
3. Unpacking

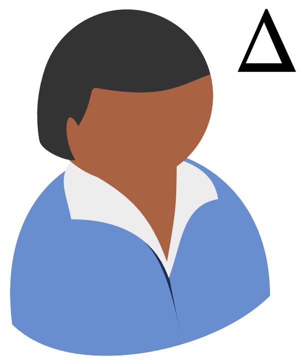
$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

$$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$$

$$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$$

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

$$G_{\mathsf{R}} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$G_{\mathsf{L}} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$E_{\mathsf{R}} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

$$E_{\mathsf{L}} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$

$$K_{\mathsf{L}} \quad K_{\mathsf{R}}$$

$$L_{\mathsf{R}} = \Delta \cdot E_{\mathsf{R}} - K_{\mathsf{R}} \pmod p$$

$$L_{\mathsf{L}} = \Delta \cdot E_{\mathsf{L}} - K_{\mathsf{L}} \pmod p$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

$$G$$

$$K$$

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

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

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

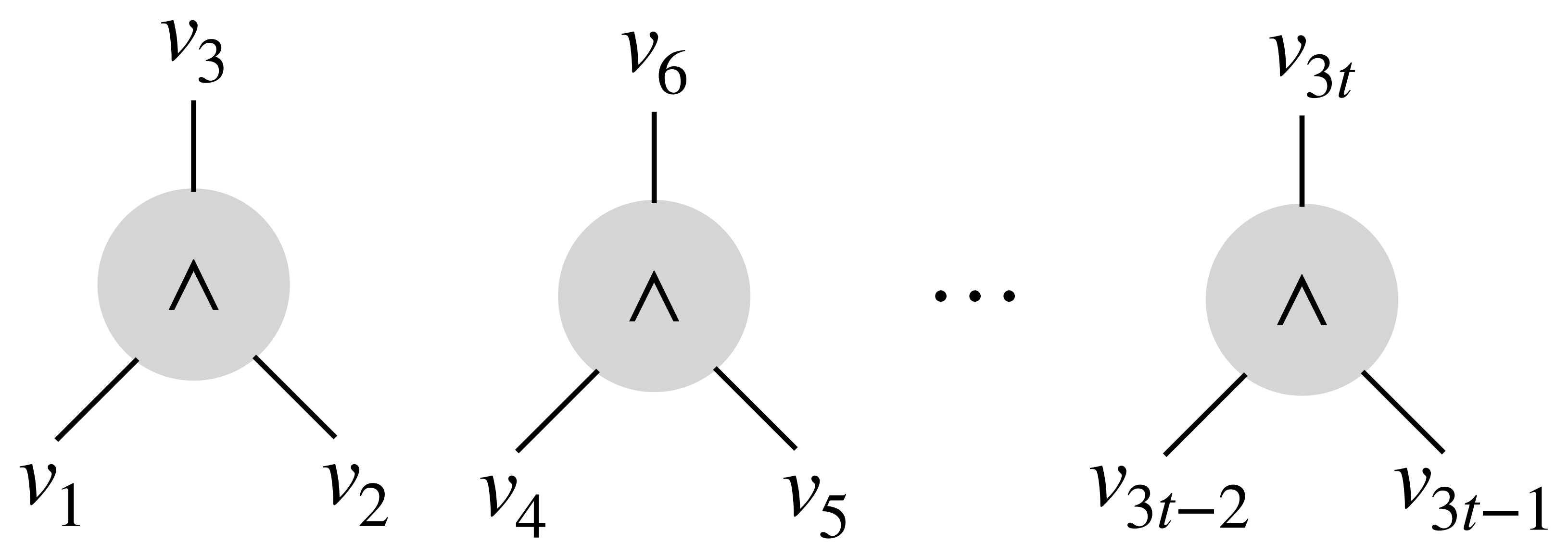
$$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$$

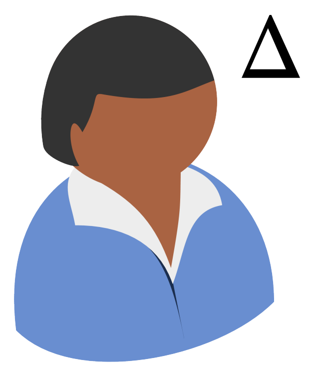
$$(k_3, \ldots, k_{3t})$$

$$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$$

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

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

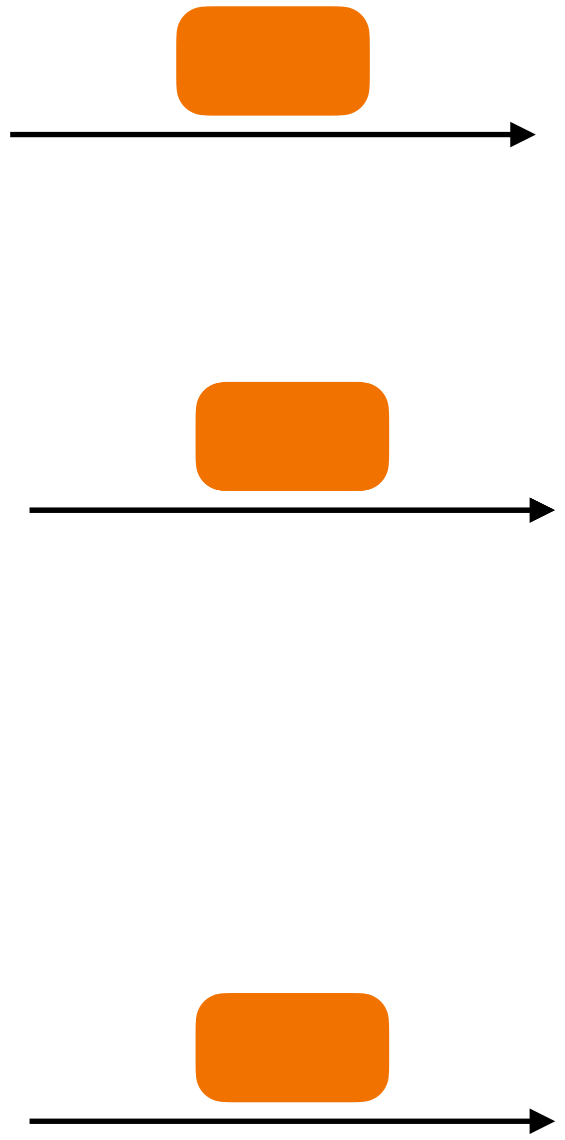
$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

$$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$$

$$G_\mathsf{L} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$$

$$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$$

$$E_\mathsf{L} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$$



K_L K_R

$$L_\mathsf{R} = \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod p$$

$$L_\mathsf{L} = \Delta \cdot E_\mathsf{L} - K_\mathsf{L} \pmod p$$

G

K

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

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

$$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$$

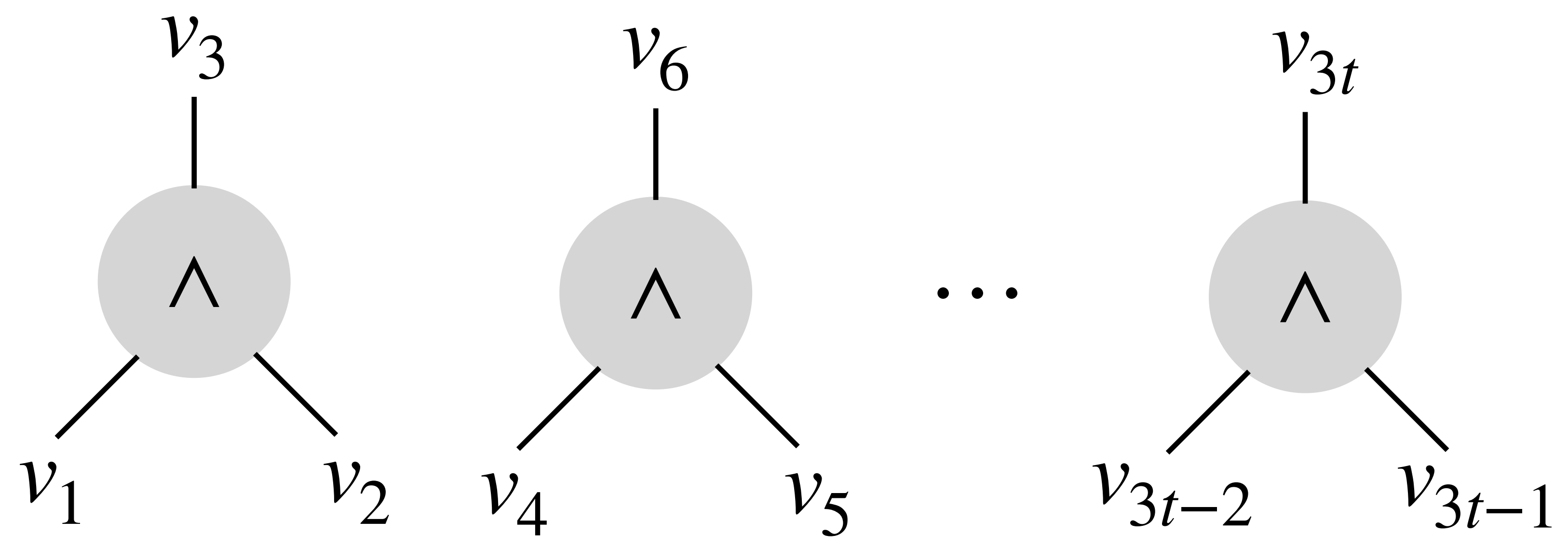
$$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$$

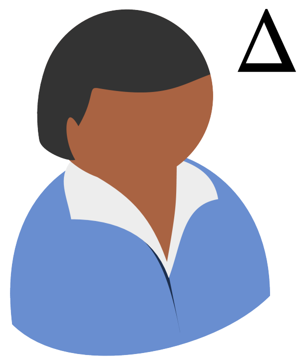
$$(k_3, \ldots, k_{3t})$$

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

Invariant maintained!

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





Garbler

Invariant

$$g_i \oplus e_i = v_i$$

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

Evaluator

1. Packing

$$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$$

$$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$$

2. Gate Evaluation

$$V = V_1 \cdot V_2$$

3. Unpacking

$$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$$

$$G_{\mathsf{R}} = \mathsf{Pack}(g_2, g_5, \ldots, g_{3t-1})$$

$$G_{\mathsf{L}} = \mathsf{Pack}(g_1, g_4, \ldots, g_{3t-2})$$

K_{L} K_{R}

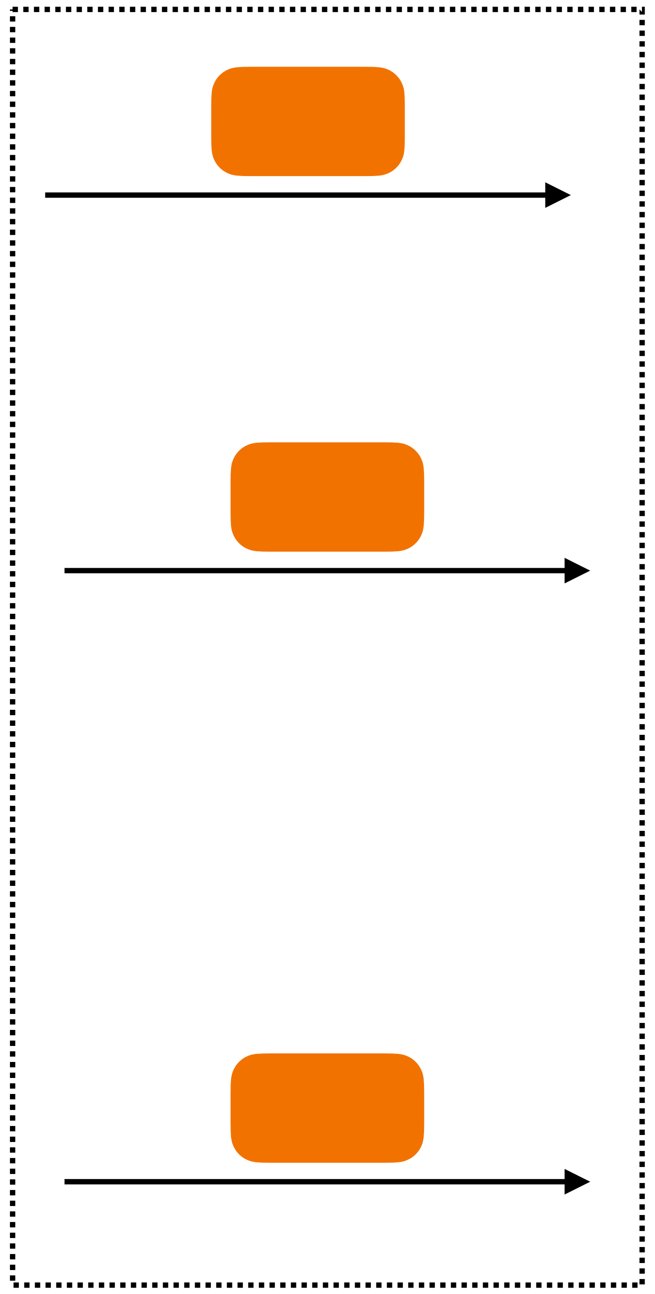
G

K

$$(g_3, g_6, \ldots, g_{3t}) = \mathsf{UnPack}(G)$$

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

$O(\lambda)$ bits



$$E_{\mathsf{R}} = \mathsf{Pack}(e_2, e_5, \ldots, e_{3t-1})$$

$$E_{\mathsf{L}} = \mathsf{Pack}(e_1, e_4, \ldots, e_{3t-2})$$

$$L_{\mathsf{R}} = \Delta \cdot E_{\mathsf{R}} - K_{\mathsf{R}} \pmod p$$

$$L_{\mathsf{L}} = \Delta \cdot E_{\mathsf{L}} - K_{\mathsf{L}} \pmod p$$

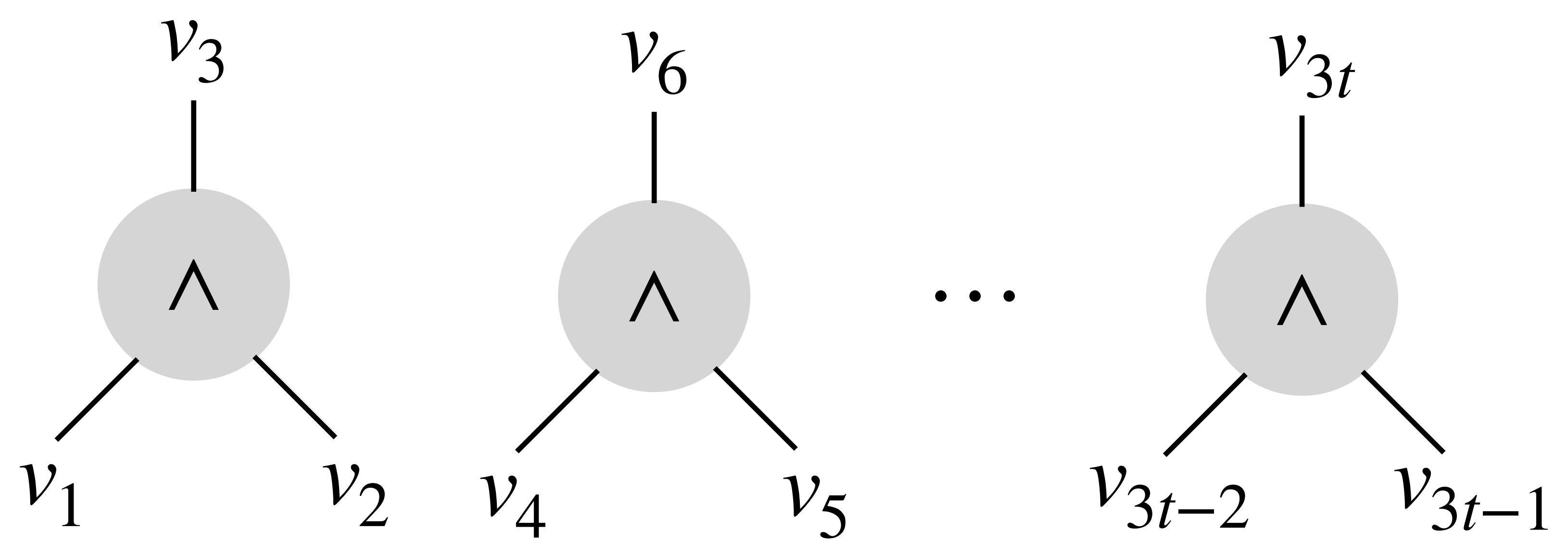
$$E = \mathsf{Pack}(v_3, \ldots, v_{3t}) - G$$

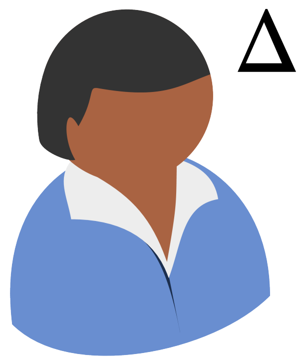
$$L = \Delta \cdot E - K \pmod p$$

$$(e_3, e_6, \ldots, e_{3t}) = \mathsf{UnPack}(E)$$

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

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





Garbler

Invariant

$$\mathsf{g}_i \oplus \mathsf{e}_i = v_i$$
$$k_i + \ell_i = \Delta \cdot \mathsf{e}_i \pmod p$$

Evaluator

1. Packing

Rate: $O\left(\frac{t}{\lambda}\right)$

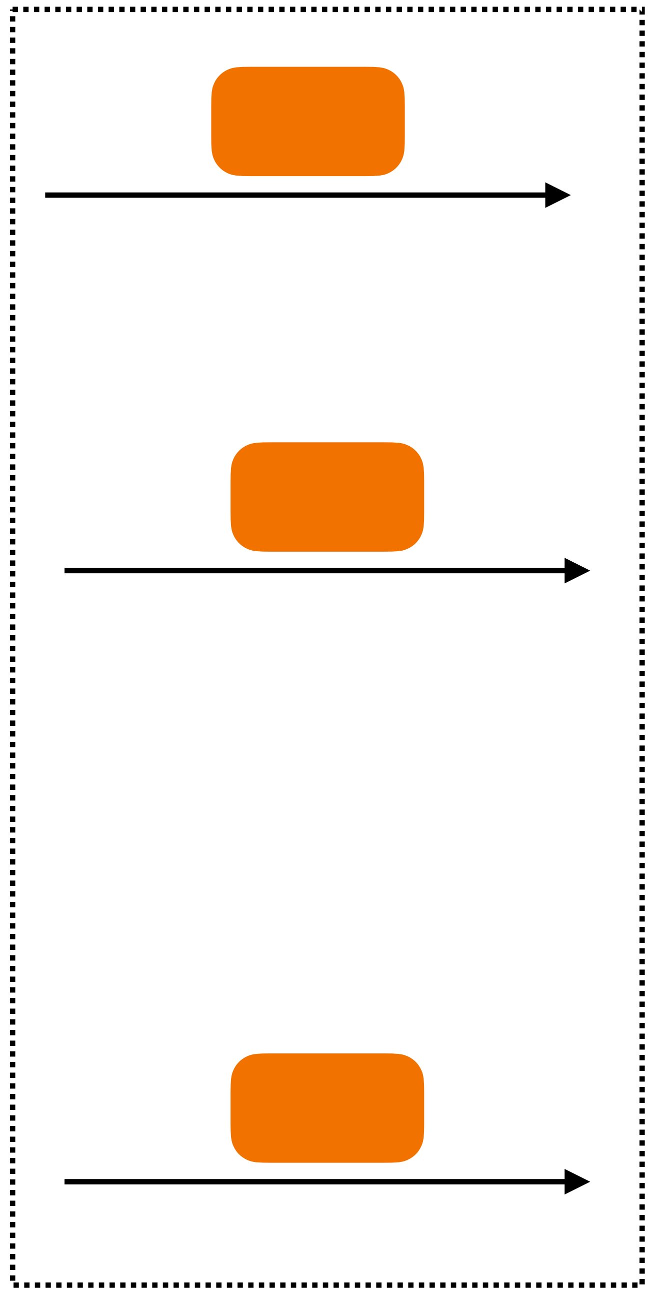
$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$

$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$

$G_{\mathsf{R}} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$

$G_{\mathsf{L}} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$

$O(\lambda)$ bits



$E_{\mathsf{R}} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$

$E_{\mathsf{L}} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$

$K_{\mathsf{L}} \quad K_{\mathsf{R}}$

$L_{\mathsf{R}} = \Delta \cdot E_{\mathsf{R}} - K_{\mathsf{R}} \pmod p$
$L_{\mathsf{L}} = \Delta \cdot E_{\mathsf{L}} - K_{\mathsf{L}} \pmod p$

2. Gate Evaluation

$V = V_1 \cdot V_2$

G

K

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

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

3. Unpacking

$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$

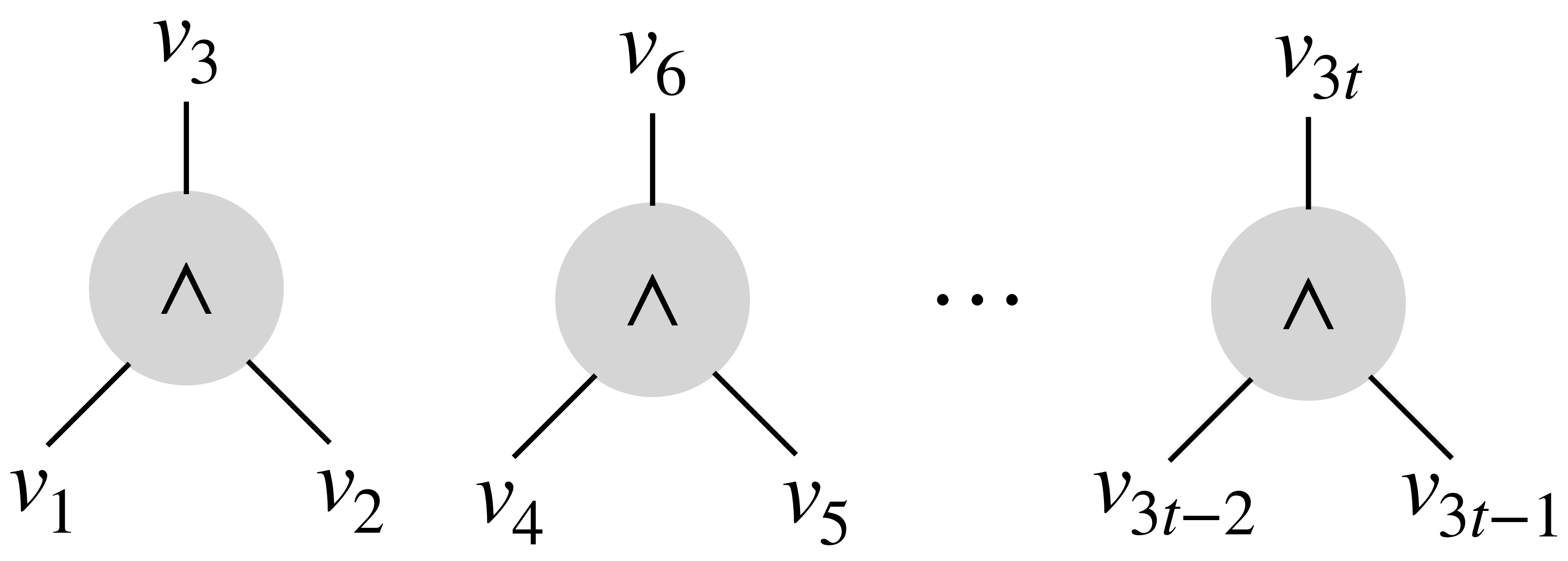
$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$

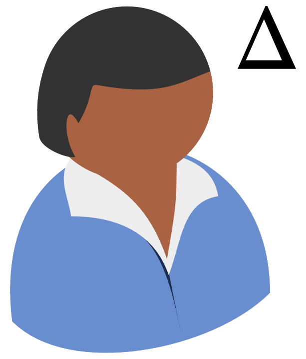
$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$

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

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

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





Garbler

Invariant

$$g_i \oplus e_i = v_i$$

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

Evaluator

1. Packing

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

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

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

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

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

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

Rate: $O\left(\frac{t}{\lambda}\right)$

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

$K_L \quad K_R$

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

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

2. Gate Evaluation

$V = V_1 \cdot V_2$

G

K

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

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

3. Unpacking

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

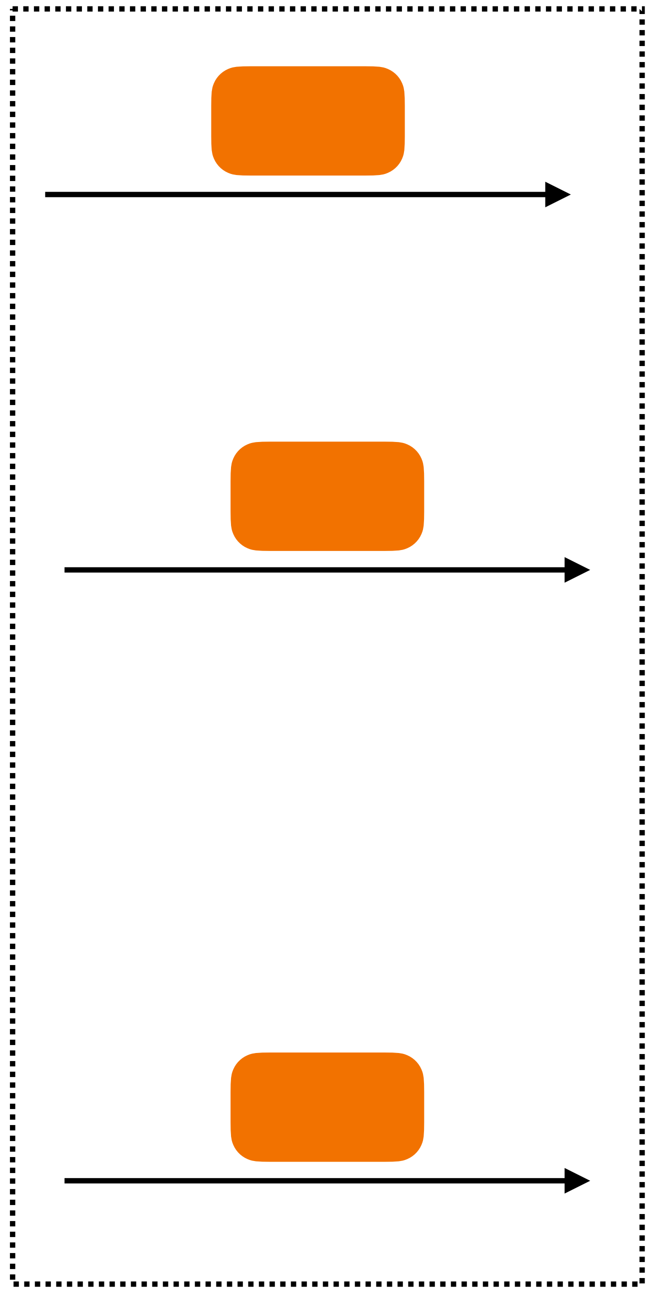
$(g_3, g_6, \ldots, g_{3t}) = \text{UnPack}(G)$

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

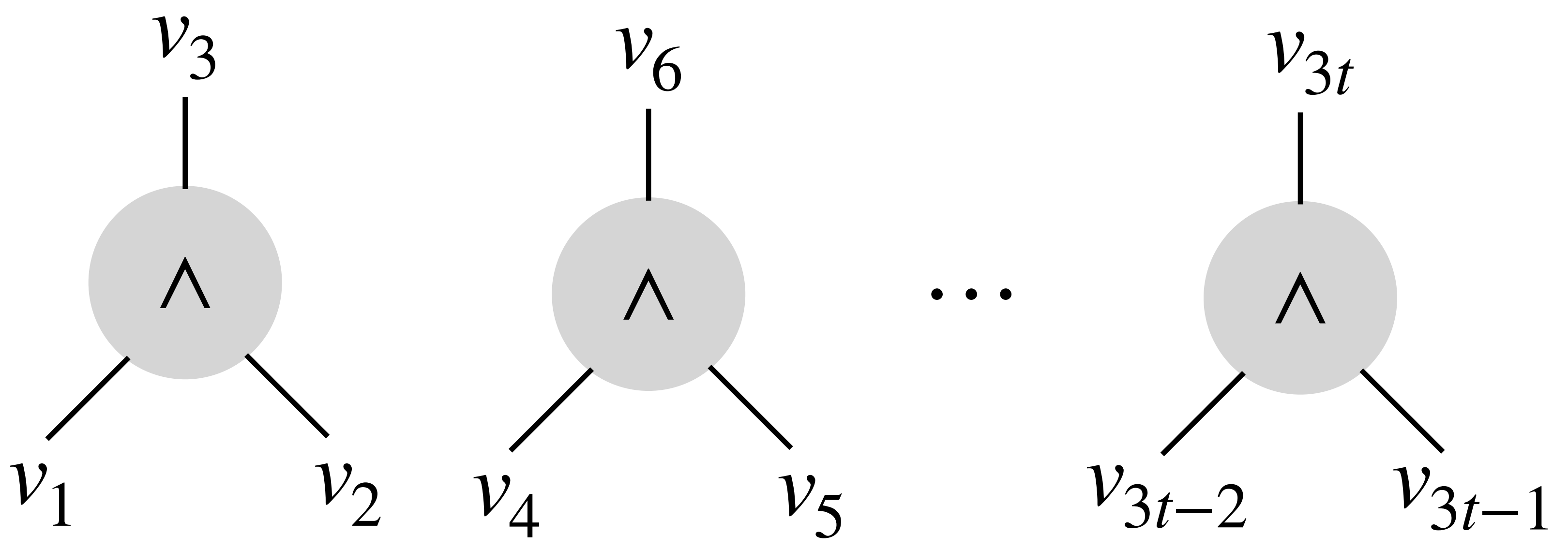
$(k_3, \ldots, k_{3t})$

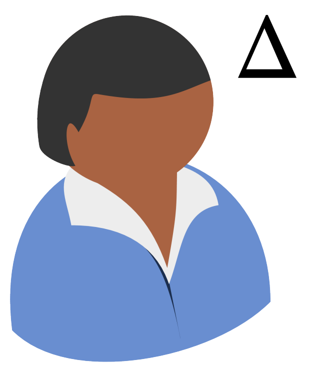
$\ell_i = \Delta \cdot e_i - k_i \pmod{p}$

$O(\lambda)$ bits



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





Garbler

Invariant

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

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

Evaluator

1. Packing

$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$

$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$

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

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

$G_{\mathsf{R}} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$

$G_{\mathsf{L}} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$

$E_{\mathsf{R}} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$

$E_{\mathsf{L}} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$

$K_{\mathsf{L}} \quad K_{\mathsf{R}}$

$L_{\mathsf{R}} = \Delta \cdot E_{\mathsf{R}} - K_{\mathsf{R}} \pmod{p}$

$L_{\mathsf{L}} = \Delta \cdot E_{\mathsf{L}} - K_{\mathsf{L}} \pmod{p}$

2. Gate Evaluation

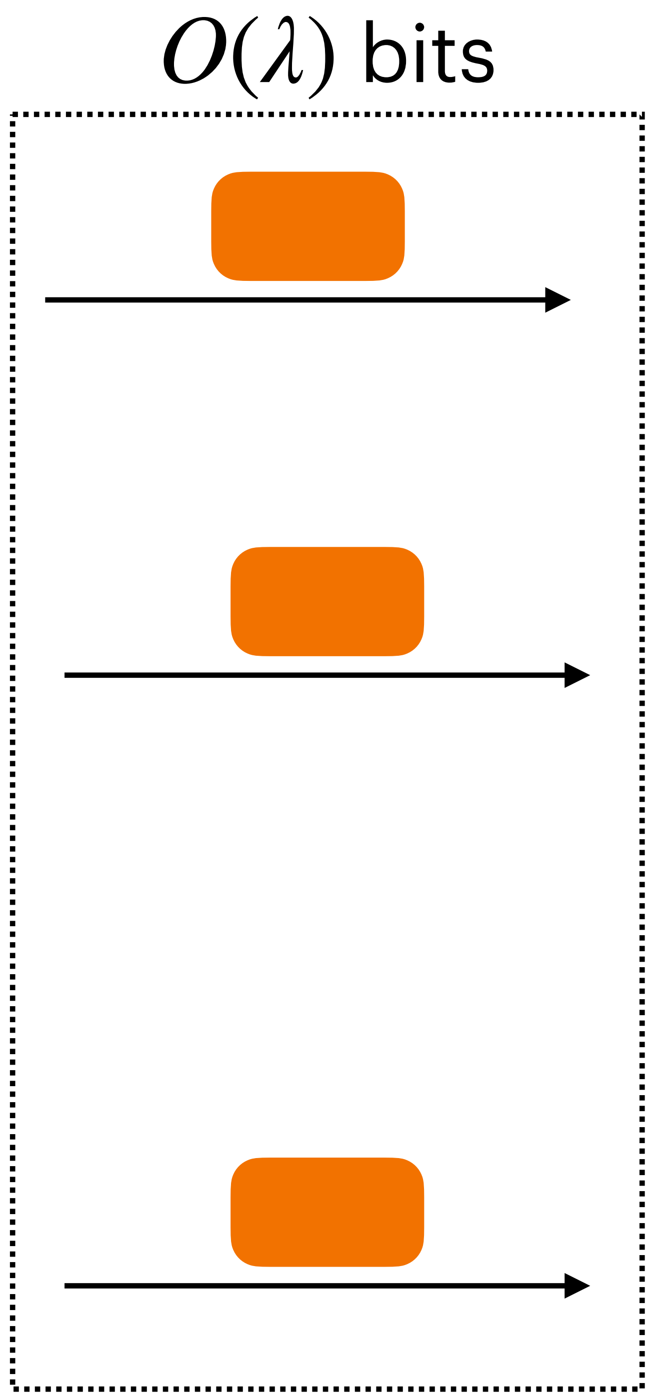
$V = V_1 \cdot V_2$

G

K

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

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



3. Unpacking

$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$

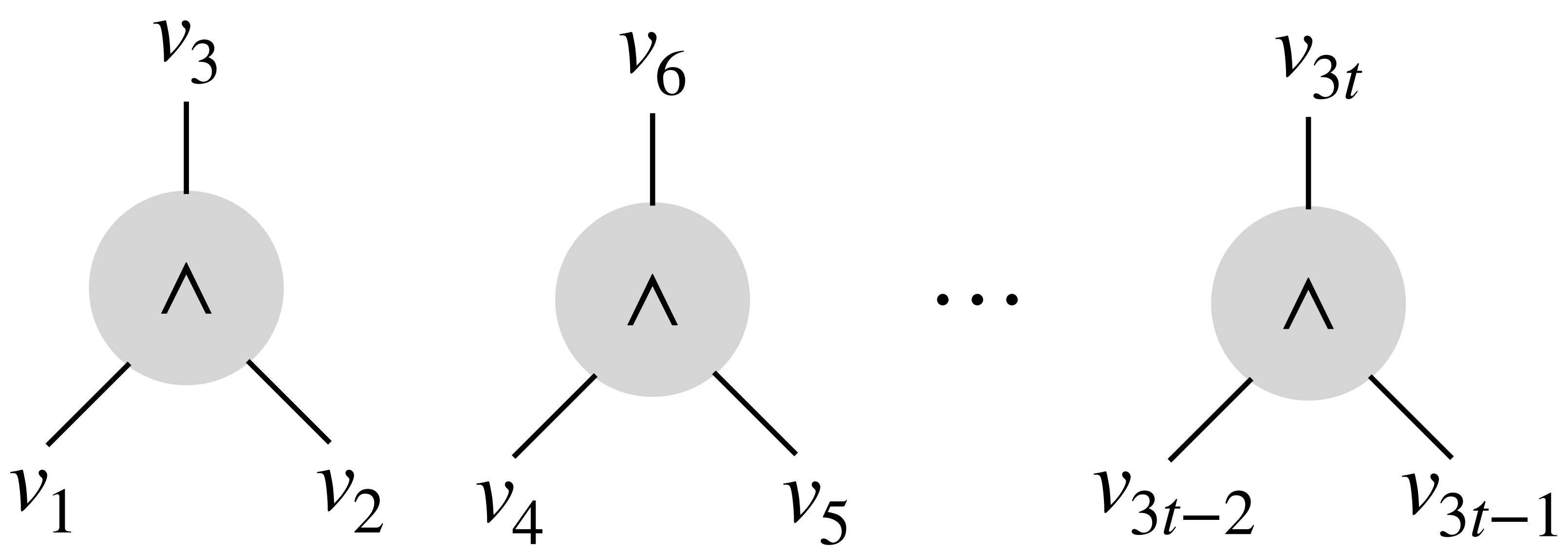
$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$

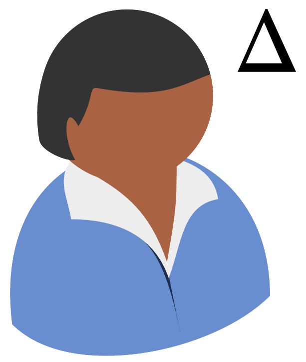
$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$

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

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

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





Garbler

Invariant

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

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

Evaluator

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

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

1. Packing

$V_{\mathsf{R}} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$

$V_{\mathsf{L}} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$

$G_{\mathsf{R}} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$

$G_{\mathsf{L}} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$

$E_{\mathsf{R}} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$

$E_{\mathsf{L}} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$

$K_{\mathsf{L}} \quad K_{\mathsf{R}}$

$L_{\mathsf{R}} = \Delta \cdot E_{\mathsf{R}} - K_{\mathsf{R}} \pmod p$

$L_{\mathsf{L}} = \Delta \cdot E_{\mathsf{L}} - K_{\mathsf{L}} \pmod p$

2. Gate Evaluation

$V = V_1 \cdot V_2$

G

K

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

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

3. Unpacking

$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$

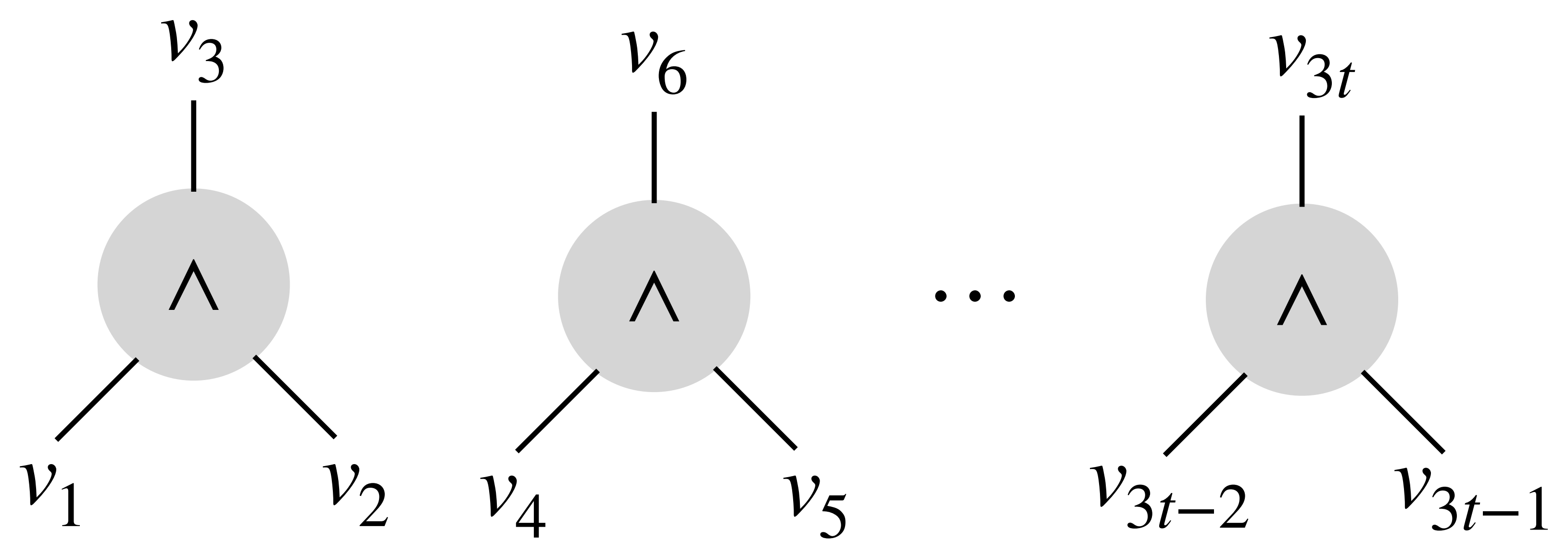
$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$

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

$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$

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

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



1. Packing

$V_\mathsf{R} = \mathsf{Pack}(v_2, v_5, \ldots, v_{3t-1})$

$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$

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

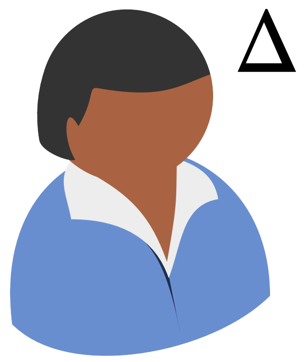
Why $t = O\left(\sqrt{\log \lambda}\right)$?

2. Gate Evaluation

$V = V_1 \cdot V_2$

3. Unpacking

$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$



Garbler

Invariant

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

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

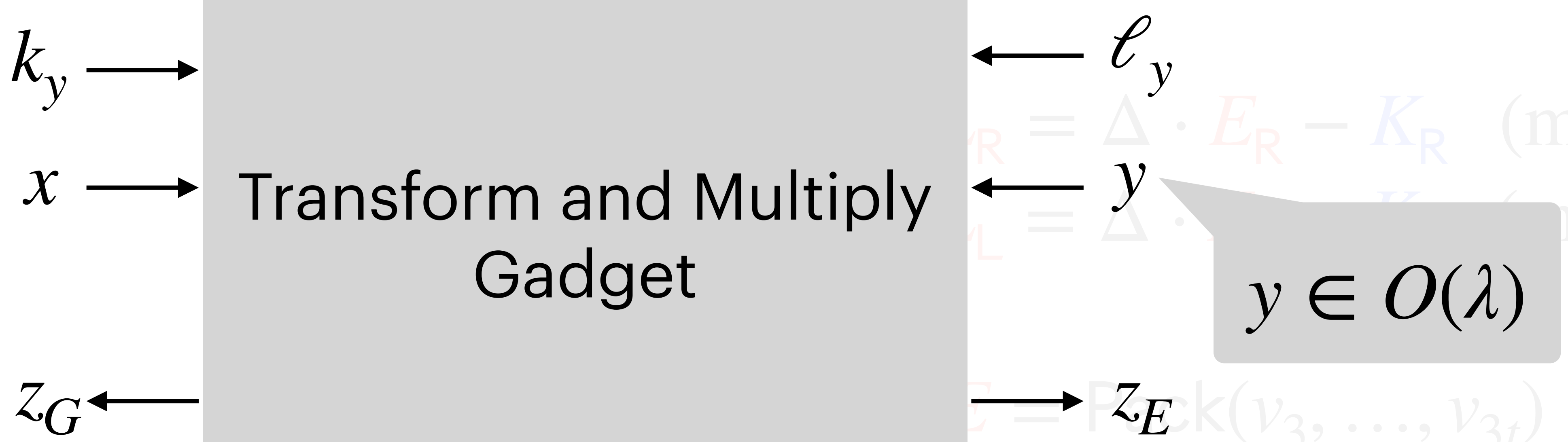
Evaluator

$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$

$G_\mathsf{L} = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$

$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$

$E_\mathsf{L} = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$



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

K_L K_R

$= \Delta \cdot E_\mathsf{R} - K_\mathsf{R} \pmod p$

$\pmod p$

G

K

$\mathsf{Pack}(v_3, \ldots, v_{3t}) - G$

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

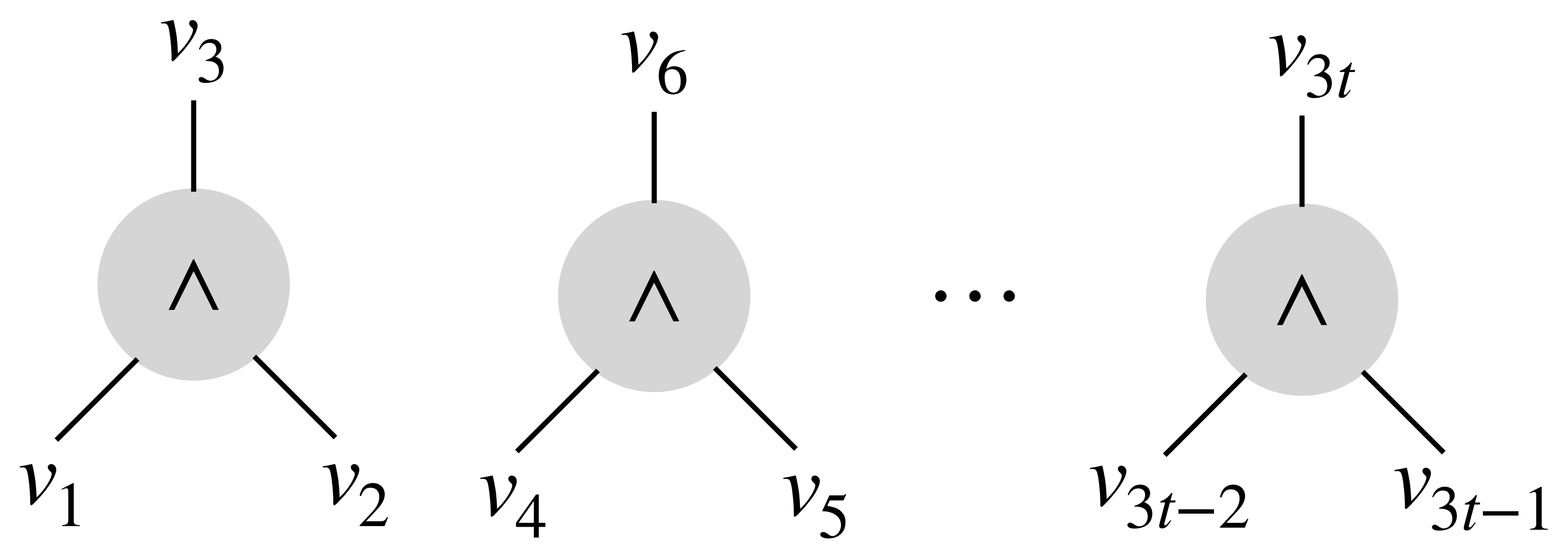
$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$

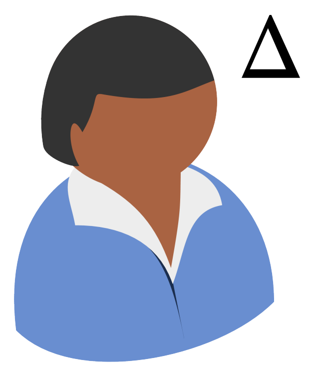
$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$

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

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

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




Δ

Garbler

Invariant

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

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


Evaluator

1. Packing

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

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

$G_R = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$

$G_L = \mathsf{Pack}(\mathsf{g}_1, \mathsf{g}_4, \ldots, \mathsf{g}_{3t-2})$

$E_R = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$

$E_L = \mathsf{Pack}(\mathsf{e}_1, \mathsf{e}_4, \ldots, \mathsf{e}_{3t-2})$

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

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

- $t \in O(\log \lambda)$

2. Gate Evaluation

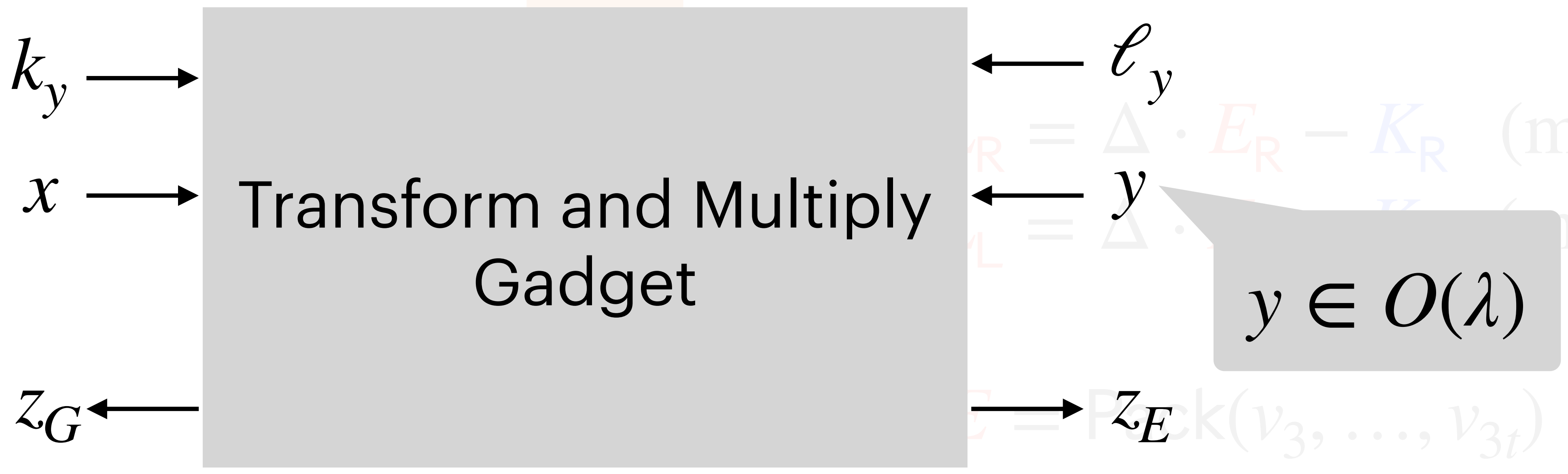
$K_L \quad K_R$

G

K

$= \Delta \cdot E_R - K_R \pmod p$

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



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

3. Unpacking

$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$

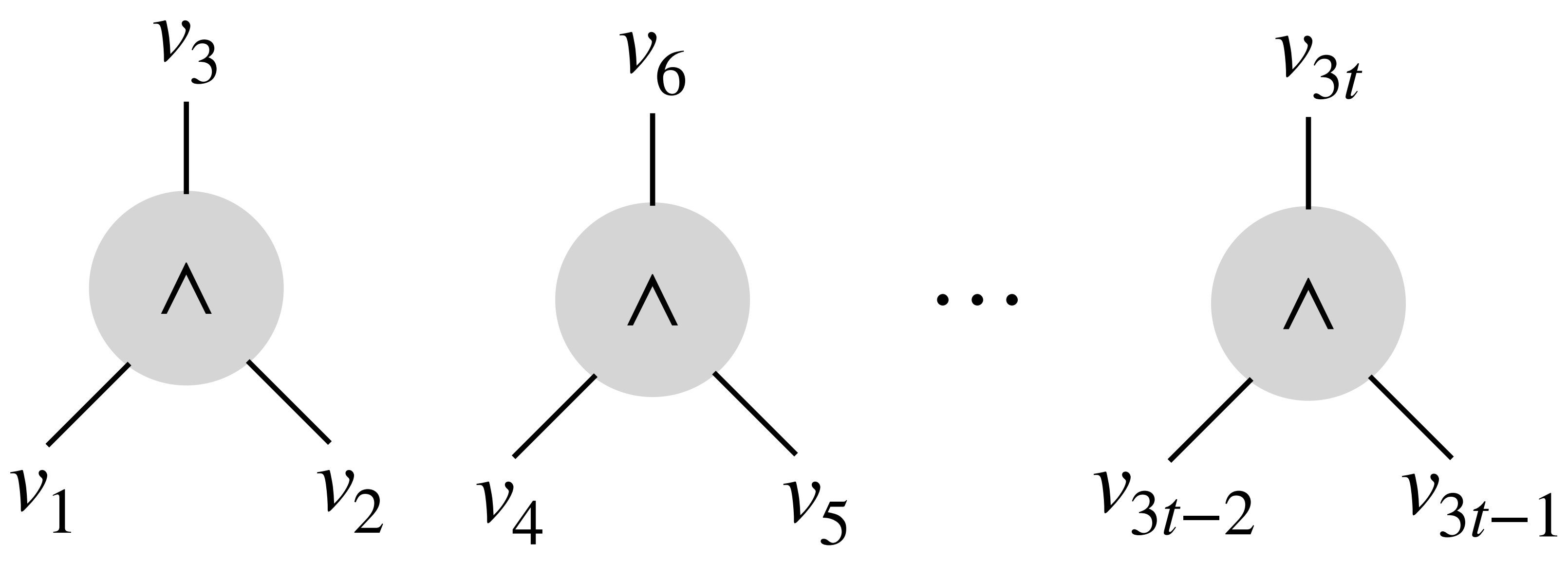
$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$

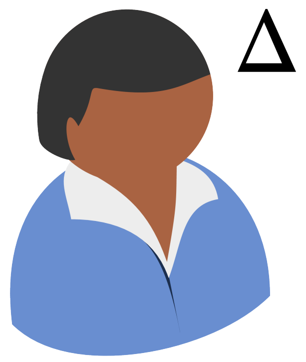
$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$

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

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

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





Garbler

Invariant

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

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

Evaluator

1. Packing

$G_\mathsf{R} = \mathsf{Pack}(\mathsf{g}_2, \mathsf{g}_5, \ldots, \mathsf{g}_{3t-1})$

$E_\mathsf{R} = \mathsf{Pack}(\mathsf{e}_2, \mathsf{e}_5, \ldots, \mathsf{e}_{3t-1})$

$V_\mathsf{L} = \mathsf{Pack}(v_1, v_4, \ldots, v_{3t-2})$

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

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

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

- $t \in O(\log \lambda)$

2. Gate Evaluation

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

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

$V = V_1 \cdot V_2 = (G_\mathsf{L} + E_\mathsf{L}) \cdot (G_\mathsf{R} + E_\mathsf{R})$

$= G_\mathsf{L} \cdot G_\mathsf{R} + G_\mathsf{L} \cdot E_\mathsf{R} + E_\mathsf{L} \cdot G_\mathsf{R} + E_\mathsf{L} \cdot E_\mathsf{R}$

Use multiplication gadget

3. Unpacking

$(\mathsf{g}_3, \mathsf{g}_6, \ldots, \mathsf{g}_{3t}) = \mathsf{UnPack}(G)$

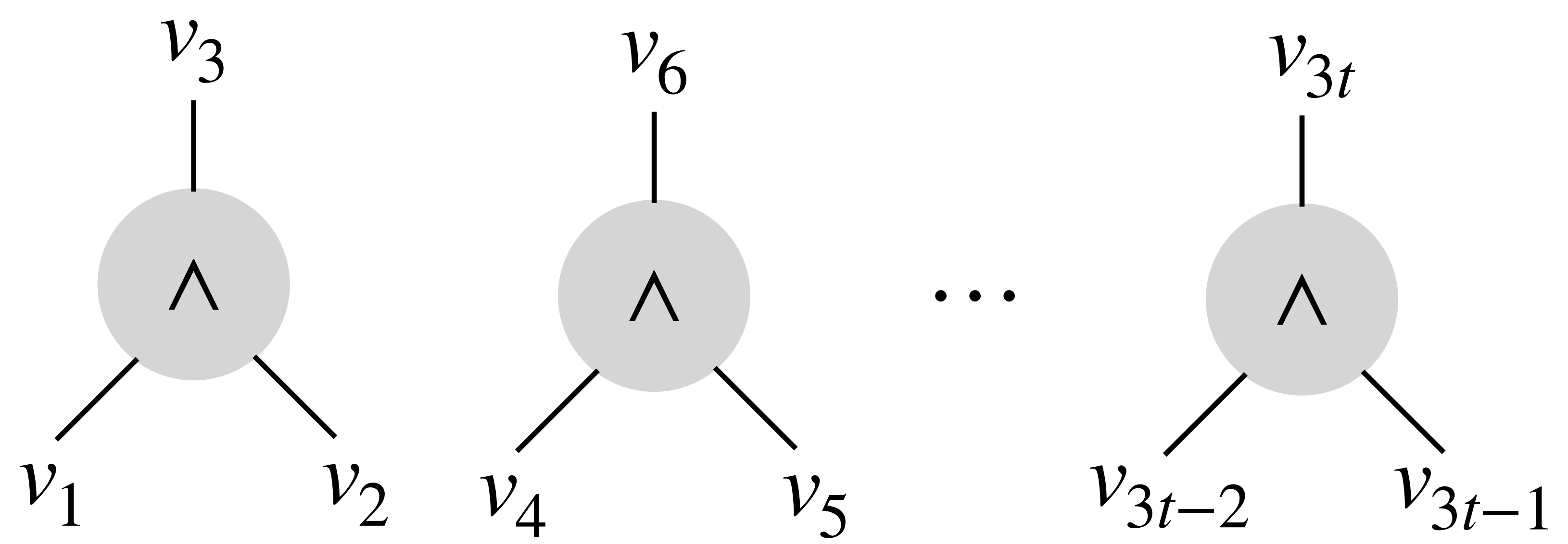
$(\mathsf{e}_3, \mathsf{e}_6, \ldots, \mathsf{e}_{3t}) = \mathsf{UnPack}(E)$

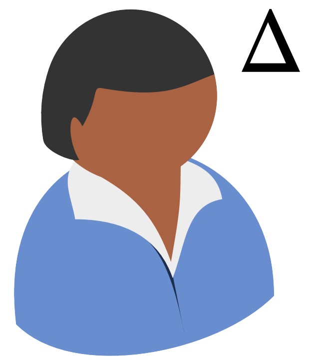
$(v_3, v_6, \ldots, v_{3t}) = \mathsf{UnPack}(V)$

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

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

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





Garbler

Invariant

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

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

Evaluator

1. Packing

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

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

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

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

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

2. Gate Evaluation

$V = V_1 \cdot V_2$

3. Unpacking

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

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

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

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

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

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

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

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

Use multiplication gadget

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

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

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

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

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

$$\begin{tikzcd}
\mathbb{F}_2^t \arrow[r, bend left, dotted] & \mathbb{F}_{2^m} \arrow[l, bend left, dotted] \arrow[r, bend left, dotted] & \mathbb{Z} \arrow[l, bend left, dotted]
\end{tikzcd}$$

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]

$$\begin{tikzcd}
\mathbb{F}_2^t \arrow[r, bend left, "\text{RMFE}"] & \mathbb{F}_{2^m} \arrow[l, bend left, "\text{RMFE}^{-1}"] \arrow[r, bend left] & \mathbb{Z} \arrow[l, bend left]
\end{tikzcd}$$

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]

$$\begin{tikzcd}
\mathbb{F}_2^t \arrow[r, bend left, dotted, "\text{RMFE}"] & \mathbb{F}_{2^m} \arrow[l, bend left, dotted, "\text{RMFE}^{-1}"] \arrow[r, bend left, dotted] & \mathbb{Z} \arrow[l, bend left, dotted]
\end{tikzcd}$$

RMFE and 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]

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

$$\begin{tikzcd}
\mathbb{F}_2^t \arrow[r, bend left, "\text{RMFE}"] & \mathbb{F}_{2^m} \arrow[l, bend left, "\text{RMFE}^{-1}"] \arrow[r, bend left] & \mathbb{Z} \arrow[l, bend left]
\end{tikzcd}$$

RMFE and 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]

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

$$\begin{tikzcd}
\mathbb{F}_2^t \arrow[r, bend left, dotted, "\mathsf{RMFE}"] & \mathbb{F}_{2^m} \arrow[l, bend left, dotted, "\mathsf{RMFE}^{-1}"] \arrow[r, bend left, dotted] & \mathbb{Z} \arrow[l, bend left, dotted]
\end{tikzcd}$$

ToPoly(x) :
1. N-ary decomposition $x = \sum_{i=1}^{m} x_i \cdot N^{i-1}$
2. Output $\sum_{i=1}^{m} x_i \cdot X^{i-1} \pmod 2 \in \mathbb{F}_{2^m}$

RMFE and 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]

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

$$\begin{tikzcd}
\mathbb{F}_2^t \arrow[r, bend left, dotted, "\text{RMFE}"] & \mathbb{F}_{2^m} \arrow[l, bend left, dotted, "\text{RMFE}^{-1}"] \arrow[r, bend left, dotted] & \mathbb{Z} \arrow[l, bend left, dotted]
\end{tikzcd}$$

ToPoly(x) :
1. N-ary decomposition $x = \sum_{i=1}^{m} x_i \cdot N^{i-1}$
2. Output $\sum_{i=1}^{m} x_i \cdot X^{i-1} \pmod 2 \in \mathbb{F}_{2^m}$

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

Homomorphic for sum of products

$m = \Theta(t)$

Eval and ToPoly are $\mathbb{F}_2$-linear

Homomorphic for sum of k products when $N > k \cdot m$

Conclusion

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

Symmetric-key crypto Black-box use of crypto

[Yao'86] [Lindell-Pinkas'07] [Koleshnikov-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] [Koleshnikov-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] [Koleshnikov-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] [Koleshnikov-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

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

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] [Koleshnikov-Schneider'08] [Zahur-Rosulek-Evans'15] [Rosulek-Roy'21]

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

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

Generic Group Model   Black-box use of crypto

This Work

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

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] [Koleshnikov-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]

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

Thank You