Rate-1 Arithmetic Garbling From Homomorphic Secret Sharing

Pierre Meyer Claudio Orlandi Lawrence Roy Peter Scholl

AARHUS UNIVERSITY

December 6
TCC 2024

Funded by the European Union
European Research Council
Established by the European Commission

Arithmetic Garbling

Arithmetic Garbling

Boolean GC

$$\begin{aligned} \mathsf{Garble}(C) &\rightarrow (\widetilde{C}, (L_{i,0}, L_{i,1})_{i\in[n]}) \\ (L_{i,1} &\leftarrow \mathsf{sk}_i + L_{i,0}) \\ \mathsf{Eval}(\widetilde{C}, (L_{i,x_i})_{i\in[n]}) &\rightarrow C(x_1, \ldots, x_n) \end{aligned}$$

Arithmetic Garbling

Boolean GC

$$\begin{aligned} \mathsf{Garble}(C) &\rightarrow (\widetilde{C}, (L_{i,0}, L_{i,1})_{i\in[n]}) \\ (L_{i,1} &\leftarrow \mathsf{sk}_i + L_{i,0}) \\ \mathsf{Eval}(\widetilde{C}, (L_{i,x_i})_{i\in[n]}) &\rightarrow C(x_1, \ldots, x_n) \end{aligned}$$

Arithmetic GC

$$\begin{aligned} \mathsf{Garble}(C) &\rightarrow (\widetilde{C}, (a_i, b_i)_{i\in[n]}) \\ (L_{x_i} &\leftarrow \mathsf{sk}_i \cdot x_i + K_i) \\ \mathsf{Eval}(\widetilde{C}, (L_{x_i})_{i\in[n]}) &\rightarrow C(x_1, \ldots, x_n) \end{aligned}$$

Arithmetic Garbling With Free Addition

Boolean GC

$$\mathsf{Garble}(C) \rightarrow (\widetilde{C}, (L_{i,0}, L_{i,1})_{i\in[n]})$$

$$(L_{i,1} \leftarrow \mathsf{sk} + L_{i,0})$$

$$\mathsf{Eval}(\widetilde{C}, (L_{i,x_i})_{i\in[n]}) \rightarrow C(x_1, \dots, x_n)$$

Arithmetic GC

$$\mathsf{Garble}(C) \rightarrow (\widetilde{C}, (a_i, b_i)_{i\in[n]})$$

$$(L_{x_i} \leftarrow \mathsf{sk} \cdot x_i + K_i)$$

$$\mathsf{Eval}(\widetilde{C}, (L_{x_i})_{i\in[n]}) \rightarrow C(x_1, \dots, x_n)$$

Arithmetic Garbling Over Bounded Integers

$$\text{rate} = \frac{(|C| + n)\ell}{\text{size}(\widetilde{C}) + \text{size}(\boldsymbol{L})} = \frac{\text{total size of all integers in circuit}}{\text{total size of garbled circuit}}$$

Arithmetic Garbling Over Bounded Integers

$$\text{rate} = \frac{(|C| + n)\ell}{\text{size}(\widetilde{C}) + \text{size}(\boldsymbol{L})} = \frac{\text{total size of all integers in circuit}}{\text{total size of garbled circuit}}$$

Construction	Security	Rate	Free addition
Yao	OWF	$\Theta(1/\lambda \log \ell)$	✗
BMR16	RO	$\Theta(\log \ell / \lambda \ell)$	✓
Heath24	CCR hash	$\Theta(1/\lambda)$	✗
AIK11	LWE	$\Theta(1/\lambda_{\mathsf{LWE}})$	✗
BLLL23	DCR	$1/12$	✗
This work	DCR + KDM	1	✓
This work	DCR	$1/2$	✓

Summary of bounded integer arithmetic garbling schemes for ℓ-bit integers, as $\ell \to \infty$.

Arithmetic Garbling Over Bounded Integers

$$\text{rate} = \frac{(|C| + n)\ell}{\text{size}(\widetilde{C}) + \text{size}(\boldsymbol{L})} = \frac{\text{total size of all integers in circuit}}{\text{total size of garbled circuit}}$$

Construction	Security	Rate	Free addition
Yao	OWF	$\Theta(1/\lambda \log \ell)$	✗
BMR16	RO	$\Theta(\log \ell / \lambda \ell)$	✓
Heath24	CCR hash	$\Theta(1/\lambda)$	✗
AIK11	LWE	$\Theta(1/\lambda_{\text{LWE}})$	✗
BLLL23	DCR	$1/12$	✗
This work	**DCR + KDM**	1	✓
This work	DCR	$1/2$	✓

Summary of bounded integer arithmetic garbling schemes for ℓ-bit integers, as $\ell \to \infty$.

Wire Labels as Subtractive Secret Shares

$$L_{x_i} = \mathsf{sk} \cdot x_i + K_i$$

Wire Labels as Subtractive Secret Shares

Given to Evaluator

Known to Garbler

$$L_{x_i} = \mathsf{sk} \cdot x_i + K_i$$

Wire Labels as Subtractive Secret Shares

Given to Evaluator

Known to Garbler

$$L_{x_i} = \mathsf{sk} \cdot x_i + K_i$$

$$\langle \mathsf{sk} \cdot x_i \rangle_1 = \mathsf{sk} \cdot x_i + \langle \mathsf{sk} \cdot x_i \rangle_0$$

Wire Labels as Subtractive Secret Shares

Given to Evaluator

Known to Garbler

$$\underbrace{L_{x_i}}_{} = \mathsf{sk} \cdot x_i + K_i$$

$$\langle \mathsf{sk} \cdot x_i \rangle_1 - \langle \mathsf{sk} \cdot x_i \rangle_0 = \mathsf{sk} \cdot x_i$$

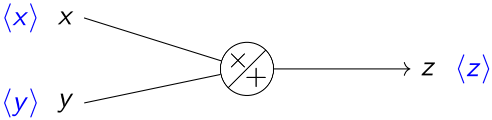
Wire Labels as Subtractive Secret Shares

Given to Evaluator

Known to Garbler

$$L_{x_i} = \mathsf{sk} \cdot x_i + K_i$$

$$\langle \mathsf{sk} \cdot x_i \rangle_1 - \langle \mathsf{sk} \cdot x_i \rangle_0 = \mathsf{sk} \cdot x_i$$



$$\mathbb{G} = \langle g \rangle$$

Subtractive shares

$$x = \langle x \rangle_1 - \langle x \rangle_0$$

$$g^{\langle x \rangle} \xmapsto{\quad ? \quad} \langle x \rangle$$

$$\mathbb{G} = \langle g \rangle$$

Subtractive shares

$$x = \langle x \rangle_1 - \langle x \rangle_0$$

$$g^{\langle x \rangle} \xmapsto{\text{DLog}} \langle x \rangle$$

$$\mathbb{G} = \langle g \rangle$$

Subtractive shares

$$x = \langle x \rangle_1 - \langle x \rangle_0$$

$$g^{\langle x \rangle} \xmapsto{\cancel{\text{DLog}}} \langle x \rangle$$

$$\mathbb{G} = \langle g \rangle$$

Subtractive shares

$$x = \langle x \rangle_1 - \langle x \rangle_0$$

$$\begin{tikzcd}
g^{\langle x \rangle} \arrow[rr, mapsto, "\cancel{\mathrm{DLog}}"] \arrow[rr, mapsto, bend right, "\mathrm{DDLog}"'] & & \langle x \rangle
\end{tikzcd}$$

$$\mathbb{G} = \langle g \rangle$$

Subtractive shares

$$x = \langle x \rangle_1 - \langle x \rangle_0$$

$$\begin{tikzcd} g^{\langle x \rangle} \arrow[r, mapsto, "\cancel{\mathrm{DLog}}"] \arrow[r, mapsto, bend right, "\mathrm{DDLog}"'] & \langle x \rangle' \end{tikzcd}$$

Arithmetic Garbling from DDLog

Thought Experiment

"g^x is an encryption of x"

$$x \cdot y = \langle x \rangle_1 \cdot \langle y \rangle_1 - x \cdot \langle y \rangle_0 - y \cdot \langle x \rangle_0 - \langle x \rangle_0 \cdot \langle y \rangle_0$$

Arithmetic Garbling from DDLog

Thought Experiment

"g^x is an encryption of x"

$$x \cdot y = \langle x \rangle_1 \cdot \langle y \rangle_1 - x \cdot \langle y \rangle_0 \underbrace{- y \cdot \langle x \rangle_0 - \langle x \rangle_0 \cdot \langle y \rangle_0}$$

$$\begin{aligned} &= -\langle x \rangle_0 \cdot (y + \langle y \rangle_0) \\ &= -\langle x \rangle_0 \cdot \langle y \rangle_1 \end{aligned}$$

Arithmetic Garbling from DDLog

Thought Experiment
"g^x is an encryption of x"

$$x \cdot y = \underbrace{\langle x\rangle_1 \cdot \langle y\rangle_1} - x \cdot \langle y\rangle_0 \underbrace{\underbrace{- y \cdot \langle x\rangle_0 - \langle x\rangle_0 \cdot \langle y\rangle_0}_{\begin{aligned} &= -\langle x\rangle_0 \cdot (y + \langle y\rangle_0) \\ &= -\langle x\rangle_0 \cdot \langle y\rangle_1 \end{aligned}}}$$

$$\begin{aligned} &= \langle y\rangle_1 \cdot (\langle x\rangle_1 - \langle x\rangle_0) \\ &= \langle y\rangle_1 \cdot x \end{aligned}$$

Arithmetic Garbling from DDLog

Thought Experiment
“g^x is an encryption of x”

$$x \cdot y = \langle x \rangle_1 \cdot \langle y \rangle_1 - x \cdot \langle y \rangle_0 - y \cdot \langle x \rangle_0 - \langle x \rangle_0 \cdot \langle y \rangle_0$$

$$\begin{aligned} &= -\langle x \rangle_0 \cdot (y + \langle y \rangle_0) \\ &= -\langle x \rangle_0 \cdot \langle y \rangle_1 \end{aligned}$$

$$\begin{aligned} &= \langle y \rangle_1 \cdot (\langle x \rangle_1 - \langle x \rangle_0) \\ &= \langle y \rangle_1 \cdot x \end{aligned}$$

$$\begin{aligned} &= x \cdot (\langle y \rangle_1 - \langle y \rangle_0) \\ &= x \cdot y \end{aligned}$$

Arithmetic Garbling from DDLog

Thought Experiment

“g^x is an encryption of x”

$$x \cdot y = \langle x \rangle_1 \cdot \langle y \rangle_1 - x \cdot \langle y \rangle_0 - y \cdot \langle x \rangle_0 - \langle x \rangle_0 \cdot \langle y \rangle_0$$

$$\langle x \rangle, g^{\langle y \rangle_0} \quad \longmapsto \quad \mathsf{DDLog}\left((g^{\langle y \rangle_0})^{\langle x \rangle} \right) \equiv \langle x \cdot \langle y \rangle_0 \rangle$$

$$\langle y \rangle, g^{\langle x \rangle_0} \quad \longmapsto \quad \mathsf{DDLog}\left((g^{\langle x \rangle_0})^{\langle y \rangle} \right) \equiv \langle y \cdot \langle x \rangle_0 \rangle$$

$$\langle x \cdot y \rangle \leftarrow \langle x \rangle \cdot \langle y \rangle - \langle x \cdot \langle y \rangle_0 \rangle - \langle y \cdot \langle x \rangle_0 \rangle$$

Arithmetic Garbling from DDLog

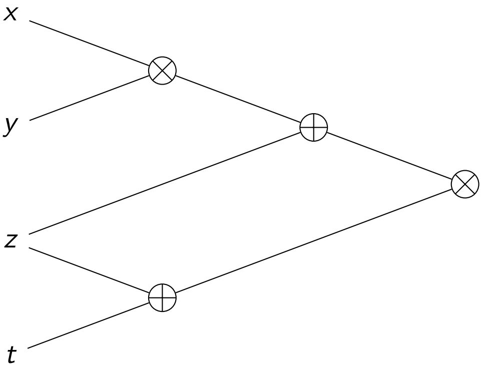
Thought Experiment

"g^x is an encryption of x"

At circuit-garbling time

At input-garbling time

At evaluation time



Arithmetic Garbling from DDLog

Thought Experiment

"g^x is an encryption of x"

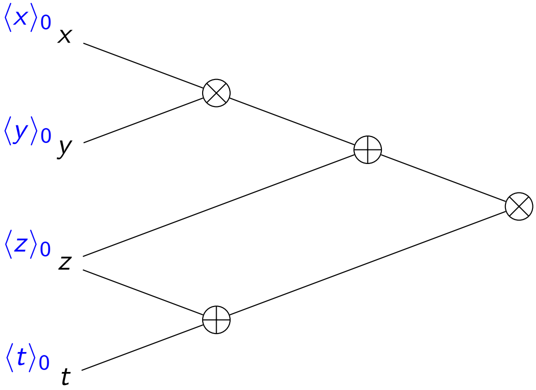
At circuit-garbling time

sample $\langle \text{in} \rangle_0$

for each input in

At input-garbling time

At evaluation time



Arithmetic Garbling from DDLog

Thought Experiment

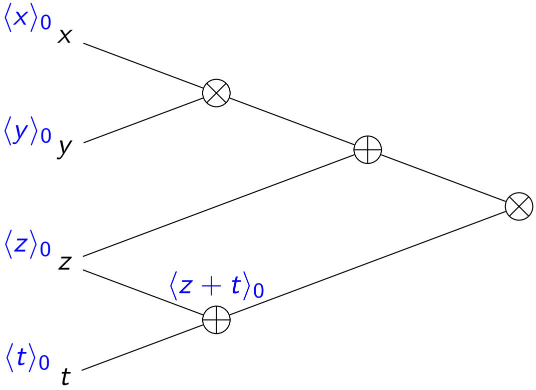
“g^x is an encryption of x”

At circuit-garbling time

sample $\langle \text{in} \rangle_0$
for each input in

At input-garbling time

At evaluation time



Arithmetic Garbling from DDLog

Thought Experiment

"g^x is an encryption of x"

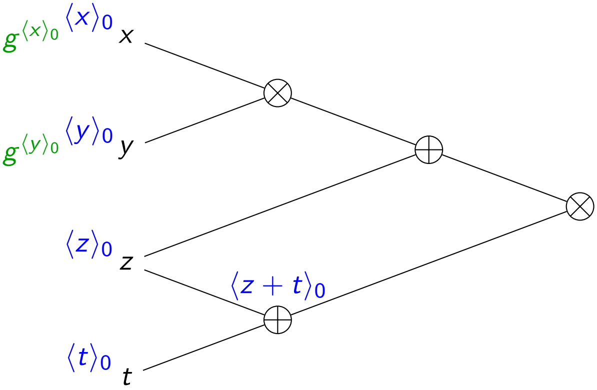
At circuit-garbling time

sample $\langle \text{in} \rangle_0$
for each input in

compute $g^{\langle w \rangle_0}$
for input to a mult w

At input-garbling time

At evaluation time



Arithmetic Garbling from DDLog

Thought Experiment

“g^x is an encryption of x”

At circuit-garbling time

sample $\langle \text{in} \rangle_0$

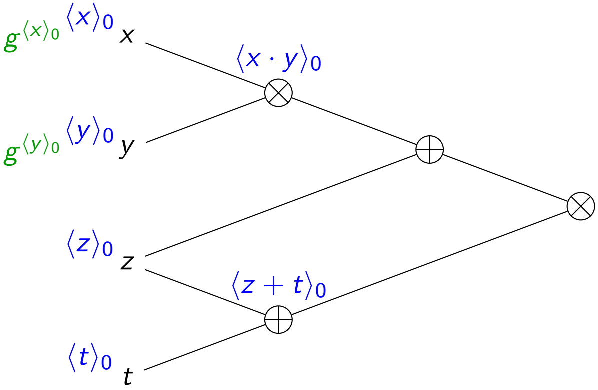
for each input in

compute $g^{\langle w \rangle_0}$

for input to a mult w

At input-garbling time

At evaluation time



Arithmetic Garbling from DDLog

Thought Experiment

"g^x is an encryption of x"

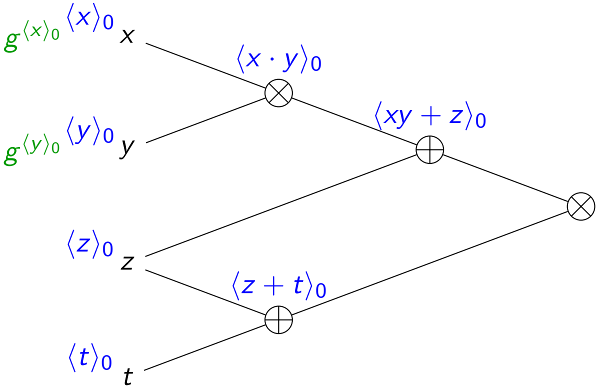
At circuit-garbling time

sample $\langle \mathrm{in} \rangle_0$
for each input in

compute $g^{\langle w \rangle_0}$
for input to a mult w

At input-garbling time

At evaluation time



Arithmetic Garbling from DDLog

Thought Experiment

"g^x is an encryption of x"

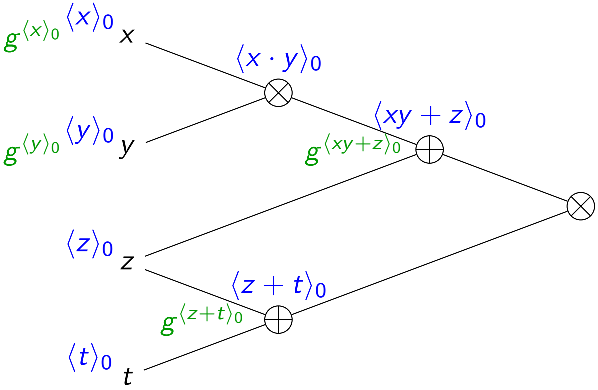
At circuit-garbling time

sample $\langle \text{in} \rangle_0$
for each input in

compute $g^{\langle w \rangle_0}$
for input to a mult w

At input-garbling time

At evaluation time



Arithmetic Garbling from DDLog

Thought Experiment

"g^x is an encryption of x"

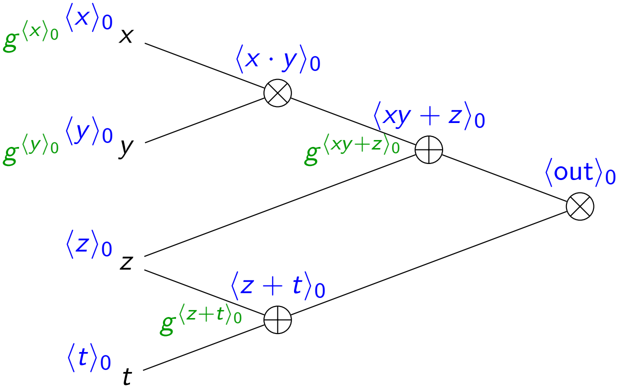
<u>At circuit-garbling time</u>

sample $\langle \text{in} \rangle_0$
for each input in

compute $g^{\langle w \rangle_0}$
for input to a mult w

<u>At input-garbling time</u>

<u>At evaluation time</u>



Arithmetic Garbling from DDLog

Thought Experiment

“g^x is an encryption of x”

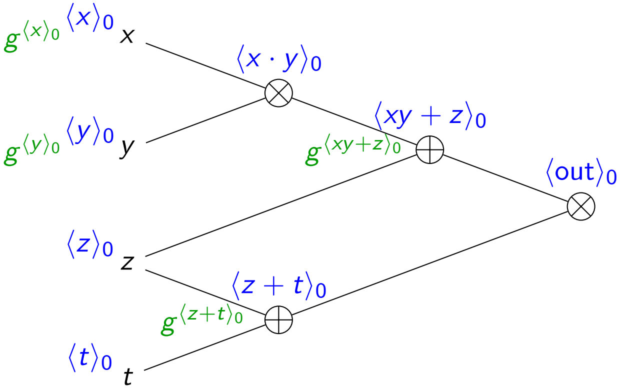
At circuit-garbling time

sample $\langle \text{in} \rangle_0$
for each input in

compute $g^{\langle w \rangle_0}$
for input to a mult w

At input-garbling time

At evaluation time



Garbled circuit: $g^{\langle L \rangle_0}, g^{\langle R \rangle_0}$
for each mult $L \times R$

Decoding info: $\langle \text{out} \rangle_0$
for each output out

Arithmetic Garbling from DDLog

Thought Experiment

"g^x is an encryption of x"

At circuit-garbling time

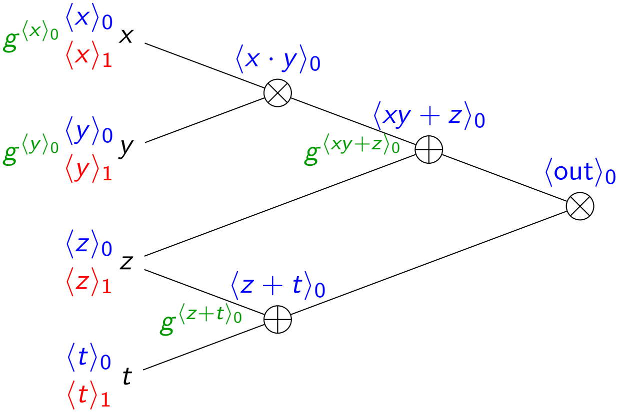
sample $\langle \text{in} \rangle_0$
for each input in

compute $g^{\langle w \rangle_0}$
for input to a mult w

At input-garbling time

$\langle \text{in} \rangle_1 \leftarrow \text{in} + \langle \text{in} \rangle_0$
for each input in

At evaluation time



Labels/Garbled inputs: $\langle \text{in} \rangle_1$
for each input in

Garbled circuit: $g^{\langle L \rangle_0}, g^{\langle R \rangle_0}$
for each mult $L \times R$

Decoding info: $\langle \text{out} \rangle_0$
for each output out

Arithmetic Garbling from DDLog

Thought Experiment

"g^x is an encryption of x"

At circuit-garbling time

sample $\langle \text{in} \rangle_0$
for each input in

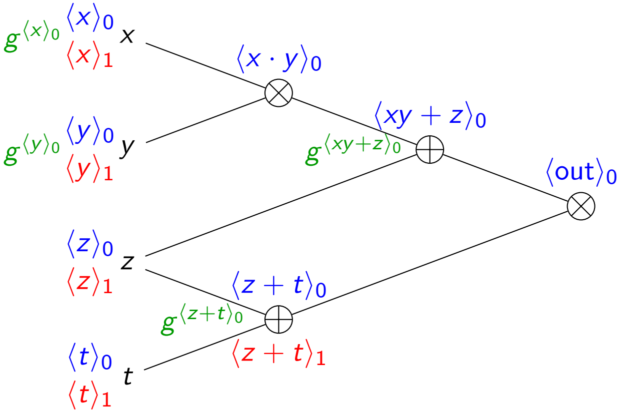
compute $g^{\langle w \rangle_0}$
for input to a mult w

At input-garbling time

$\langle \text{in} \rangle_1 \leftarrow \text{in} + \langle \text{in} \rangle_0$
for each input in

At evaluation time

compute $\langle \cdot \rangle_1$ gate-by-gate



Labels/Garbled inputs: $\langle \text{in} \rangle_1$
for each input in

Garbled circuit: $g^{\langle L \rangle_0}, g^{\langle R \rangle_0}$
for each mult $L \times R$

Decoding info: $\langle \text{out} \rangle_0$
for each output out

Arithmetic Garbling from DDLog

Thought Experiment

“g^x is an encryption of x”

At circuit-garbling time

sample $\langle \mathrm{in} \rangle_0$

for each input in

compute $g^{\langle w \rangle_0}$

for input to a mult w

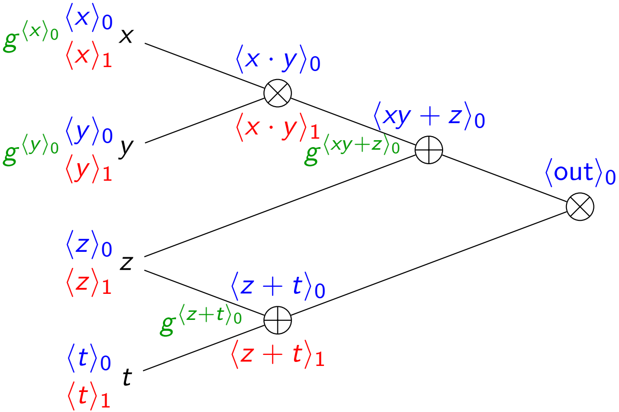
At input-garbling time

$\langle \mathrm{in} \rangle_1 \leftarrow \mathrm{in} + \langle \mathrm{in} \rangle_0$

for each input in

At evaluation time

compute $\langle \cdot \rangle_1$ gate-by-gate



Labels/Garbled inputs: $\langle \mathrm{in} \rangle_1$

for each input in

Garbled circuit: $g^{\langle L \rangle_0}, g^{\langle R \rangle_0}$

for each mult $L \times R$

Decoding info: $\langle \mathrm{out} \rangle_0$

for each output out

Arithmetic Garbling from DDLog

Thought Experiment

“g^x is an encryption of x”

At circuit-garbling time

sample $\langle \mathrm{in} \rangle_0$

for each input in

compute $g^{\langle w \rangle_0}$

for input to a mult w

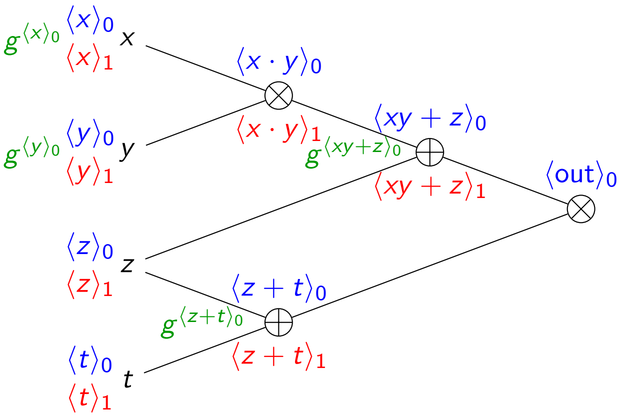
At input-garbling time

$\langle \mathrm{in} \rangle_1 \leftarrow \mathrm{in} + \langle \mathrm{in} \rangle_0$

for each input in

At evaluation time

compute $\langle \cdot \rangle_1$ gate-by-gate



Labels/Garbled inputs: $\langle \mathrm{in} \rangle_1$

for each input in

Garbled circuit: $g^{\langle L \rangle_0}, g^{\langle R \rangle_0}$

for each mult $L \times R$

Decoding info: $\langle \mathrm{out} \rangle_0$

for each output out

Arithmetic Garbling from DDLog

Thought Experiment

“g^x is an encryption of x”

At circuit-garbling time

sample $\langle \text{in} \rangle_0$
for each input in

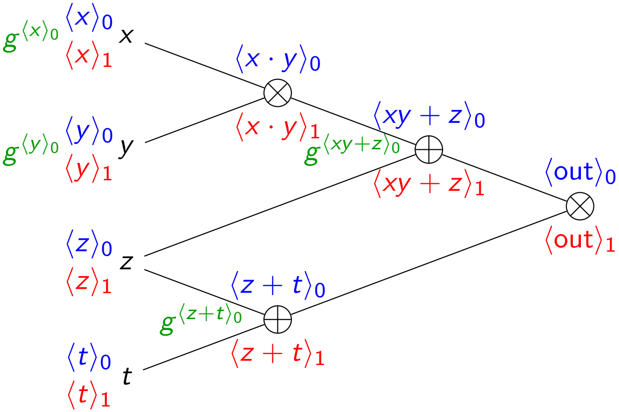
compute $g^{\langle w \rangle_0}$
for input to a mult w

At input-garbling time

$\langle \text{in} \rangle_1 \leftarrow \text{in} + \langle \text{in} \rangle_0$
for each input in

At evaluation time

compute $\langle \cdot \rangle_1$ gate-by-gate



Labels/Garbled inputs: $\langle \text{in} \rangle_1$
for each input in

Garbled circuit: $g^{\langle L \rangle_0}, g^{\langle R \rangle_0}$
for each mult $L \times R$

Decoding info: $\langle \text{out} \rangle_0$
for each output out

Arithmetic Garbling from DDLog

Thought Experiment

“g^x is an encryption of x”

At circuit-garbling time

sample $\langle \text{in} \rangle_0$
for each input in

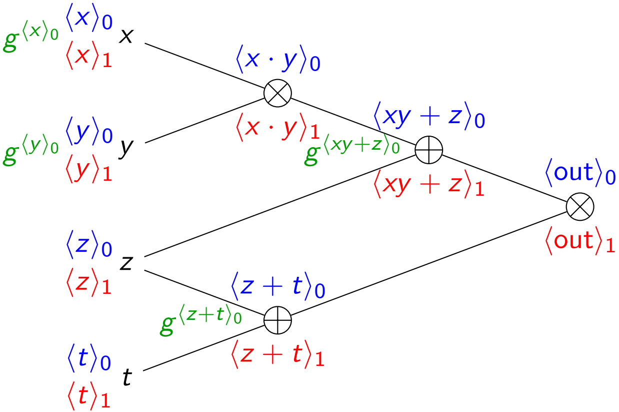
compute $g^{\langle w \rangle_0}$
for input to a mult w

At input-garbling time

$\langle \text{in} \rangle_1 \leftarrow \text{in} + \langle \text{in} \rangle_0$
for each input in

At evaluation time

compute $\langle \cdot \rangle_1$ gate-by-gate
output $\langle \text{out} \rangle_1 - \langle \text{out} \rangle_0$



Labels/Garbled inputs: $\langle \text{in} \rangle_1$
for each input in

Garbled circuit: $g^{\langle L \rangle_0}, g^{\langle R \rangle_0}$
for each mult $L \times R$

Decoding info: $\langle \text{out} \rangle_0$
for each output out

Arithmetic Garbling from DDLog

Thought Experiment
"g^x is an encryption of x"

At circuit-garbling time

sample $\langle \text{in} \rangle_0$
for each input in

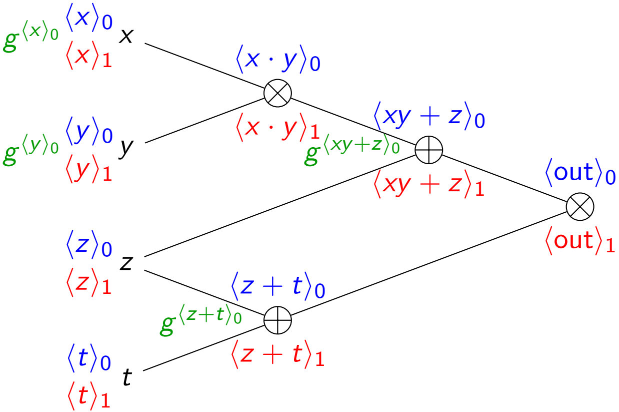
compute $g^{\langle w \rangle_0}$
for input to a mult w

At input-garbling time

$\langle \text{in} \rangle_1 \leftarrow \text{in} + \langle \text{in} \rangle_0$
for each input in

At evaluation time

compute $\langle \cdot \rangle_1$ gate-by-gate
output $\langle \text{out} \rangle_1 - \langle \text{out} \rangle_0$



Labels/Garbled inputs: $\langle \text{in} \rangle_1, g^{\langle \text{in} \rangle_0}$
for each input in

Garbled circuit: $g^{\langle L \cdot R \rangle_0}$
for each mult $L \times R$

Decoding info: $\langle \text{out} \rangle_0$
for each output out

DDLog in groups with a DDLog-easy cyclic subgroup

[OSY21, RS21, ADOS22]

$$\mathbb{G} \simeq \overset{\substack{\text{easy}\\ \text{DLog}\\ \downarrow}}{\mathbb{F}} \times \mathbb{H}^{\overset{\substack{\text{hard}\\ \text{DLog}}}{\swarrow}}$$

$$\mathbb{F} = \langle f \rangle;\ |\mathbb{F}| = q$$

<u>Promise</u>

$$g_1/g_0 = f^x$$

$$\mathrm{DDLog}(g_1) - \mathrm{DDLog}(g_0) \equiv x \pmod{q}$$

DDLog in groups with a DDLog-easy cyclic subgroup

[OSY21, RS21, ADOS22]

$$\mathbb{G} \simeq \overset{\substack{\text{easy}\\ \text{DLog}\\ \downarrow}}{\mathbb{F}} \times \mathbb{H}^{\swarrow\,\substack{\text{hard}\\ \text{DLog}}}$$

$$\mathbb{F} = \langle f \rangle;\ |\mathbb{F}| = N^2$$

Promise

$$g_1/g_0 = f^x$$

$$\mathrm{DDLog}(g_1) - \mathrm{DDLog}(g_0) \equiv x \pmod{N^2}$$

Damgård-Jurik Cryptosystem

Public-key: RSA modulus N

$$\mathrm{DJ.Enc}_N(x) \to \quad r^{N^2} \cdot \exp(x) \in \mathbb{Z}/N^3\mathbb{Z}$$

DDLog in groups with a DDLog-easy cyclic subgroup
[OSY21, RS21, ADOS22]

$$\mathbb{G} \simeq \overset{\substack{\text{easy}\\ \text{DLog}\\ \downarrow}}{\mathbb{F}} \times \mathbb{H}^{\overset{\substack{\text{hard}\\ \text{DLog}}}{\swarrow}}$$

$$\exp(X) = 1 + NX + \frac{(Nx)^2}{2}$$

$$\mathbb{F} = \langle f \rangle;\ |\mathbb{F}| = N^2$$

Damgård-Jurik Cryptosystem

Public-key: RSA modulus N

$$\mathrm{DJ.Enc}_N(x) \to \quad r^{N^2} \cdot \exp(x) \in \mathbb{Z}/N^3\mathbb{Z}$$

Promise

$$g_1/g_0 = f^x$$

$$\mathrm{DDLog}(g_1) - \mathrm{DDLog}(g_0) \equiv x \pmod{N^2}$$

DDLog in groups with a DDLog-easy cyclic subgroup

[OSY21, RS21, ADOS22]

$$\mathbb{G} \simeq \overset{\substack{\text{easy}\\ \text{DLog}\\ \downarrow}}{\mathbb{F}} \times \mathbb{H}^{\substack{\text{hard}\\ \text{DLog}\\ \swarrow}}$$

$$\exp(X) = 1 + NX + \frac{(Nx)^2}{2}$$

$$\mathbb{F} := \langle \exp(1) \rangle$$

$$\mathbb{F} = \langle f \rangle;\ |\mathbb{F}| = N^2$$

Damgård-Jurik Cryptosystem

Public-key: RSA modulus N

$$\mathsf{DJ.Enc}_N(x) \rightarrow \quad r^{N^2} \cdot \exp(x) \in \mathbb{Z}/N^3\mathbb{Z}$$

Promise

$$g_1/g_0 = f^x$$

$$\mathsf{DDLog}(g_1) - \mathsf{DDLog}(g_0) \equiv x \pmod{N^2}$$

DDLog in groups with a DDLog-easy cyclic subgroup

[OSY21, RS21, ADOS22]

$$\mathbb{G} \simeq \overset{\substack{\text{easy}\\ \text{DLog}\\ \downarrow}}{\mathbb{F}} \times \mathbb{H}^{\substack{\text{hard}\\ \text{DLog}\\ \swarrow}}$$

$$\mathbb{F} = \langle f \rangle;\ |\mathbb{F}| = N^2$$

Promise

$$g_1 / g_0 = f^x$$

$$\mathrm{DDLog}(g_1) - \mathrm{DDLog}(g_0) \equiv x \pmod{N^2}$$

$$\exp(X) = 1 + NX + \frac{(Nx)^2}{2}$$

$$\mathbb{F} := \langle \exp(1) \rangle$$

$$\forall h \in \mathbb{F}, \mathrm{DLog}(1 + Nx) = x - \frac{Nx^2}{2}$$

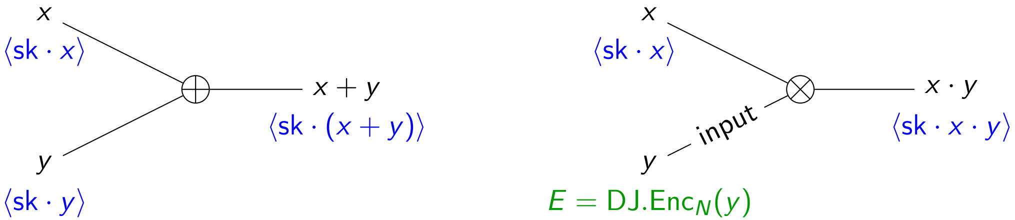
Damgård-Jurik Cryptosystem

Public-key: RSA modulus N

$$\mathrm{DJ.Enc}_N(x) \to \quad r^{N^2} \cdot \exp(x) \in \mathbb{Z}/N^3\mathbb{Z}$$

Homomorphic Secret Sharing from Damgård-Jurik

Set $\mathsf{sk} = \varphi(N)$.



x

$\langle \mathsf{sk} \cdot x \rangle$

$x + y$

$\langle \mathsf{sk} \cdot (x + y) \rangle$

y

$\langle \mathsf{sk} \cdot y \rangle$

x

$\langle \mathsf{sk} \cdot x \rangle$

input

$x \cdot y$

$\langle \mathsf{sk} \cdot x \cdot y \rangle$

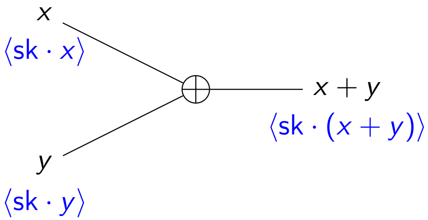
y

$E = \mathsf{DJ.Enc}_N(y)$

$$\mathsf{HSS.Mul}(C, \langle \mathsf{sk} \cdot x \rangle_\sigma) = \mathsf{DDLog}(C^{\langle \mathsf{sk} \cdot x \rangle_\sigma}) = \langle \mathsf{sk} \cdot x \cdot y \rangle_\sigma$$

Homomorphic Secret Sharing from Damgård-Jurik

Set $\mathsf{sk} = \varphi(N)$.



x

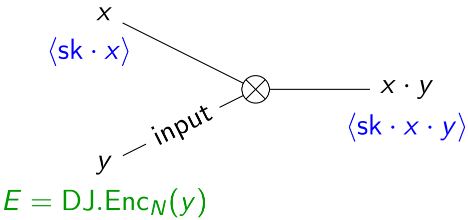
$\langle \mathsf{sk} \cdot x \rangle$

y

$\langle \mathsf{sk} \cdot y \rangle$

$x + y$

$\langle \mathsf{sk} \cdot (x + y) \rangle$



x

$\langle \mathsf{sk} \cdot x \rangle$

y

input

$E = \mathsf{DJ.Enc}_N(y)$

$x \cdot y$

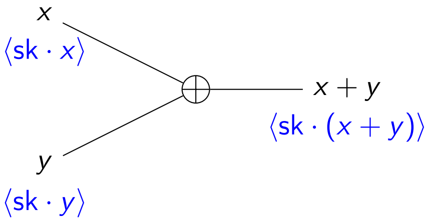
$\langle \mathsf{sk} \cdot x \cdot y \rangle$

$$\mathsf{HSS.Mul}(C, \langle \mathsf{sk} \cdot x \rangle_\sigma) = \mathsf{DDLog}(C^{\langle \mathsf{sk} \cdot x \rangle_\sigma}) = \langle \mathsf{sk} \cdot x \cdot y \rangle_\sigma$$

$$\frac{C^{\langle \mathsf{sk} \cdot x \rangle_1}}{C^{\langle \mathsf{sk} \cdot x \rangle_0}} = (r^{N^2} \exp(y))^{\mathsf{sk} \cdot x} = \exp(\mathsf{sk} \cdot x \cdot y)$$

Homomorphic Secret Sharing from Damgård-Jurik

Set $\mathsf{sk} = \varphi(N)$.



x

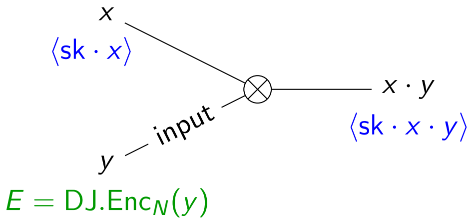
$\langle \mathsf{sk} \cdot x \rangle$

y

$\langle \mathsf{sk} \cdot y \rangle$

$x + y$

$\langle \mathsf{sk} \cdot (x + y) \rangle$



x

$\langle \mathsf{sk} \cdot x \rangle$

y

input

$E = \mathsf{DJ.Enc}_N(y)$

$x \cdot y$

$\langle \mathsf{sk} \cdot x \cdot y \rangle$

$$\mathsf{HSS.Mul}(C, \langle \mathsf{sk} \cdot x \rangle_\sigma) = \mathsf{DDLog}(C^{\langle \mathsf{sk} \cdot x \rangle_\sigma}) = \langle \mathsf{sk} \cdot x \cdot y \rangle_\sigma$$

$$\frac{C^{\langle \mathsf{sk} \cdot x \rangle_1}}{C^{\langle \mathsf{sk} \cdot x \rangle_0}} = (r^{N^2} \exp(y))^{\mathsf{sk} \cdot x} = \exp(\mathsf{sk} \cdot x \cdot y)$$

Can multiply with $\mathsf{DJ.Enc}_N(\mathsf{sk}^{-1} \bmod N^2)$ to remove sk from shares.

Arithmetic Garbling

$$\langle x \rangle_1 \cdot \langle y \rangle_1 = (x + \langle x \rangle_0)(y + \langle y \rangle_0)$$

Arithmetic Garbling

$$\begin{aligned}\langle x\rangle_1 \cdot \langle y\rangle_1 &= (x + \langle x\rangle_0)(y + \langle y\rangle_0) \\ &= x \cdot y + x \cdot \langle y\rangle_0 + \langle x\rangle_0 \cdot y + \langle x\rangle_0 \cdot \langle y\rangle_0\end{aligned}$$

Arithmetic Garbling

$$\begin{aligned}
\langle x \rangle_1 \cdot \langle y \rangle_1 &= (x + \langle x \rangle_0)(y + \langle y \rangle_0) \\
&= x \cdot y + x \cdot \langle y \rangle_0 + \langle x \rangle_0 \cdot y + \langle x \rangle_0 \cdot \langle y \rangle_0 \\
x \cdot y &= \langle x \rangle_1 \cdot \langle y \rangle_1 - x \cdot \langle y \rangle_0 - \langle x \rangle_0 \cdot y - \langle x \rangle_0 \cdot \langle y \rangle_0
\end{aligned}$$

Arithmetic Garbling

$$\begin{aligned}
\langle x \rangle_1 \cdot \langle y \rangle_1 &= (x + \langle x \rangle_0)(y + \langle y \rangle_0) \\
&= x \cdot y + x \cdot \langle y \rangle_0 + \langle x \rangle_0 \cdot y + \langle x \rangle_0 \cdot \langle y \rangle_0 \\
x \cdot y &= \underbrace{\langle x \rangle_1 \cdot \langle y \rangle_1}_{\text{Known to Evaluator}} - x \cdot \langle y \rangle_0 - \langle x \rangle_0 \cdot y - \underbrace{\langle x \rangle_0 \cdot \langle y \rangle_0}_{\text{Known to Garbler}}
\end{aligned}$$

Arithmetic Garbling

$$\begin{aligned} \langle x \rangle_1 \cdot \langle y \rangle_1 &= (x + \langle x \rangle_0)(y + \langle y \rangle_0) \\ &= x \cdot y + x \cdot \langle y \rangle_0 + \langle x \rangle_0 \cdot y + \langle x \rangle_0 \cdot \langle y \rangle_0 \\ x \cdot y = \quad & \underbrace{\langle x \rangle_1 \cdot \langle y \rangle_1}_{\text{Known to Evaluator}} \quad - \quad \underbrace{x \cdot \langle y \rangle_0}_{\mathsf{HSS.Mul}(C_{\langle y \rangle_0}, \langle \mathsf{sk} \cdot x \rangle)} \quad - \quad \underbrace{\langle x \rangle_0 \cdot y}_{\mathsf{HSS.Mul}(C_{\langle x \rangle_0}, \langle \mathsf{sk} \cdot y \rangle)} \quad - \quad \underbrace{\langle x \rangle_0 \cdot \langle y \rangle_0}_{\text{Known to Garbler}} \end{aligned}$$

G contains:

$$\begin{aligned} C_{\langle x \rangle_0} &= \mathsf{DJ.Enc}(\mathsf{sk}^{-1} \langle x \rangle_0) \\ C_{\langle y \rangle_0} &= \mathsf{DJ.Enc}(\mathsf{sk}^{-1} \langle y \rangle_0) \end{aligned}$$

Arithmetic Garbling

$$\begin{aligned}\langle x\rangle_1 \cdot \langle y\rangle_1 &= (x + \langle x\rangle_0)(y + \langle y\rangle_0)\\ &= x \cdot y + x \cdot \langle y\rangle_0 + \langle x\rangle_0 \cdot y + \langle x\rangle_0 \cdot \langle y\rangle_0\end{aligned}$$

$$x \cdot y = \underbrace{\langle x\rangle_1 \cdot \langle y\rangle_1}_{\text{Known to Evaluator}} - \underbrace{x \cdot \langle y\rangle_0}_{\mathsf{HSS.Mul}(C_{\langle y\rangle_0}, \langle \mathsf{sk}\cdot x\rangle)} - \underbrace{\langle x\rangle_0 \cdot y}_{\mathsf{HSS.Mul}(C_{\langle x\rangle_0}, \langle \mathsf{sk}\cdot y\rangle)} - \underbrace{\langle x\rangle_0 \cdot \langle y\rangle_0}_{\text{Known to Garbler}}$$

$$\mathsf{sk} \cdot x \cdot y = \underbrace{\langle x\rangle_1 \cdot \langle \mathsf{sk} \cdot y\rangle_1}_{\text{Known to Evaluator}} - \underbrace{x \cdot \langle \mathsf{sk} \cdot y\rangle_0}_{\mathsf{HSS.Mul}(C_{\langle \mathsf{sk}\cdot y\rangle_0}, \langle \mathsf{sk}\cdot x\rangle)} - \underbrace{\langle x\rangle_0 \cdot \mathsf{sk} \cdot y}_{\mathsf{HSS.Mul}(C'_{\langle x\rangle_0}, \langle \mathsf{sk}\cdot y\rangle)} - \underbrace{\langle x\rangle_0 \cdot \langle \mathsf{sk} \cdot y\rangle_0}_{\text{Known to Garbler}}$$

G contains:

$$\begin{aligned}C_{\langle x\rangle_0} &= \mathsf{DJ.Enc}(\mathsf{sk}^{-1}\langle x\rangle_0)\\ C_{\langle y\rangle_0} &= \mathsf{DJ.Enc}(\mathsf{sk}^{-1}\langle y\rangle_0)\\ C'_{\langle x\rangle_0} &= \mathsf{DJ.Enc}(\langle x\rangle_0)\\ C_{\langle \mathsf{sk}\cdot y\rangle_0} &= \mathsf{DJ.Enc}(\mathsf{sk}^{-1}\langle \mathsf{sk} \cdot y\rangle_0)\end{aligned}$$

Arithmetic Garbling

$$\begin{aligned}\langle x\rangle_1 \cdot \langle y\rangle_1 &= (x + \langle x\rangle_0)(y + \langle y\rangle_0)\\ &= x \cdot y + x \cdot \langle y\rangle_0 + \langle x\rangle_0 \cdot y + \langle x\rangle_0 \cdot \langle y\rangle_0\end{aligned}$$

$$x \cdot y = \underbrace{\langle x\rangle_1 \cdot \langle y\rangle_1}_{\text{Known to Evaluator}} - \underbrace{x \cdot \langle y\rangle_0}_{\mathsf{HSS.Mul}(C_{\langle y\rangle_0}, \langle \mathsf{sk} \cdot x\rangle)} - \underbrace{\langle x\rangle_0 \cdot y}_{\mathsf{HSS.Mul}(C_{\langle x\rangle_0}, \langle \mathsf{sk} \cdot y\rangle)} - \underbrace{\langle x\rangle_0 \cdot \langle y\rangle_0}_{\text{Known to Garbler}}$$

$$\mathsf{sk} \cdot x \cdot y = \underbrace{\langle x\rangle_1 \cdot \langle \mathsf{sk} \cdot y\rangle_1}_{\text{Known to Evaluator}} - \underbrace{x \cdot \langle \mathsf{sk} \cdot y\rangle_0}_{\mathsf{HSS.Mul}(C_{\langle \mathsf{sk} \cdot y\rangle_0}, \langle \mathsf{sk} \cdot x\rangle)} - \underbrace{\langle x\rangle_0 \cdot \mathsf{sk} \cdot y}_{\mathsf{HSS.Mul}(C'_{\langle x\rangle_0}, \langle \mathsf{sk} \cdot y\rangle)} - \underbrace{\langle x\rangle_0 \cdot \langle \mathsf{sk} \cdot y\rangle_0}_{\text{Known to Garbler}}$$

G contains:

$$\begin{aligned}C_{\langle x\rangle_0} &= \mathsf{DJ.Enc}(\mathsf{sk}^{-1}\langle x\rangle_0)\\ C_{\langle y\rangle_0} &= \mathsf{DJ.Enc}(\mathsf{sk}^{-1}\langle y\rangle_0)\\ C'_{\langle x\rangle_0} &= \mathsf{DJ.Enc}(\langle x\rangle_0)\\ C_{\langle \mathsf{sk} \cdot y\rangle_0} &= \mathsf{DJ.Enc}(\mathsf{sk}^{-1}\langle \mathsf{sk} \cdot y\rangle_0)\end{aligned}$$

Rate: $\frac{1}{4}$?

Arithmetic Garbling

$$\begin{aligned}\langle x\rangle_1 \cdot \langle y\rangle_1 &= (x + \langle x\rangle_0)(y + \langle y\rangle_0)\\ &= x \cdot y + x \cdot \langle y\rangle_0 + \langle x\rangle_0 \cdot y + \langle x\rangle_0 \cdot \langle y\rangle_0\end{aligned}$$

$$x \cdot y = \underbrace{\langle x\rangle_1 \cdot \langle y\rangle_1}_{\text{Known to Evaluator}} - \underbrace{x \cdot \langle y\rangle_0}_{\text{HSS.Mul}(C_{\langle y\rangle_0}, \langle \text{sk} \cdot x\rangle)} - \underbrace{\langle x\rangle_0 \cdot y}_{\text{HSS.Mul}(C_{\langle x\rangle_0}, \langle \text{sk} \cdot y\rangle)} - \underbrace{\langle x\rangle_0 \cdot \langle y\rangle_0}_{\text{Known to Garbler}}$$

$$\text{sk} \cdot x \cdot y = \underbrace{\langle x\rangle_1 \cdot \langle \text{sk} \cdot y\rangle_1}_{\text{Known to Evaluator}} - \underbrace{x \cdot \langle \text{sk} \cdot y\rangle_0}_{\text{HSS.Mul}(C_{\langle \text{sk} \cdot y\rangle_0}, \langle \text{sk} \cdot x\rangle)} - \underbrace{\langle x\rangle_0 \cdot \text{sk} \cdot y}_{\text{HSS.Mul}(C'_{\langle x\rangle_0}, \langle \text{sk} \cdot y\rangle)} - \underbrace{\langle x\rangle_0 \cdot \langle \text{sk} \cdot y\rangle_0}_{\text{Known to Garbler}}$$

G contains:

$$\begin{aligned}C_{\langle x\rangle_0} &= \text{DJ.Enc}(\text{sk}^{-1}\langle x\rangle_0)\\ C_{\langle y\rangle_0} &= \text{DJ.Enc}(\text{sk}^{-1}\langle y\rangle_0)\\ C'_{\langle x\rangle_0} &= \text{DJ.Enc}(\langle x\rangle_0)\\ C_{\langle \text{sk} \cdot y\rangle_0} &= \text{DJ.Enc}(\text{sk}^{-1}\langle \text{sk} \cdot y\rangle_0)\end{aligned}$$

Rate: $\frac{1}{3}$

Rate-1 Arithmetic Garbling

$$\mathsf{sk}\cdot x\cdot \mathsf{sk}\cdot y = \underbrace{\langle \mathsf{sk}\cdot x\rangle_1 \cdot \langle \mathsf{sk}\cdot y\rangle_1}_{\text{Known to Evaluator}} - \underbrace{\mathsf{sk}\cdot x\cdot \langle \mathsf{sk}\cdot y\rangle_0}_{\mathsf{HSS.Mul}(C_{\langle \mathsf{sk}\cdot y\rangle_0}, \langle \mathsf{sk}\cdot x\rangle)} - \underbrace{\langle \mathsf{sk}\cdot x\rangle_0 \cdot \mathsf{sk}\cdot y}_{\mathsf{HSS.Mul}(C_{\langle \mathsf{sk}\cdot x\rangle_0}, \langle \mathsf{sk}\cdot y\rangle)} - \underbrace{\langle \mathsf{sk}\cdot x\rangle_0 \cdot \langle \mathsf{sk}\cdot y\rangle_0}_{\text{Known to Garbler}}$$

Rate-1 Arithmetic Garbling

$$\mathsf{sk} \cdot x \cdot \mathsf{sk} \cdot y = \underbrace{\langle \mathsf{sk} \cdot x \rangle_1 \cdot \langle \mathsf{sk} \cdot y \rangle_1}_{\text{Known to Evaluator}} - \underbrace{\mathsf{sk} \cdot x \cdot \langle \mathsf{sk} \cdot y \rangle_0}_{\mathsf{HSS.Mul}(C_{\langle \mathsf{sk} \cdot y \rangle_0}, \langle \mathsf{sk} \cdot x \rangle)} - \underbrace{\langle \mathsf{sk} \cdot x \rangle_0 \cdot \mathsf{sk} \cdot y}_{\mathsf{HSS.Mul}(C_{\langle \mathsf{sk} \cdot x \rangle_0}, \langle \mathsf{sk} \cdot y \rangle)} - \underbrace{\langle \mathsf{sk} \cdot x \rangle_0 \cdot \langle \mathsf{sk} \cdot y \rangle_0}_{\text{Known to Garbler}}$$

G contains:

$$C_{\langle \mathsf{sk} \cdot x \rangle_0} = \mathsf{DJ.Enc}_N(\langle \mathsf{sk} \cdot x \rangle_0)$$
$$C_{\langle \mathsf{sk} \cdot y \rangle_0} = \mathsf{DJ.Enc}_N(\langle \mathsf{sk} \cdot y \rangle_0)$$

Rate-1 Arithmetic Garbling

$$\mathsf{sk} \cdot x \cdot \mathsf{sk} \cdot y = \underbrace{\langle \mathsf{sk} \cdot x \rangle_1 \cdot \langle \mathsf{sk} \cdot y \rangle_1}_{\text{Known to Evaluator}} - \underbrace{\mathsf{sk} \cdot x \cdot \langle \mathsf{sk} \cdot y \rangle_0}_{\mathsf{HSS.Mul}(C_{\langle \mathsf{sk} \cdot y \rangle_0}, \langle \mathsf{sk} \cdot x \rangle)} - \underbrace{\langle \mathsf{sk} \cdot x \rangle_0 \cdot \mathsf{sk} \cdot y}_{\mathsf{HSS.Mul}(C_{\langle \mathsf{sk} \cdot x \rangle_0}, \langle \mathsf{sk} \cdot y \rangle)} - \underbrace{\langle \mathsf{sk} \cdot x \rangle_0 \cdot \langle \mathsf{sk} \cdot y \rangle_0}_{\text{Known to Garbler}}$$

G contains:

$$C_{\langle \mathsf{sk} \cdot x \rangle_0} = \mathsf{DJ.Enc}_N(\langle \mathsf{sk} \cdot x \rangle_0)$$
$$C_{\langle \mathsf{sk} \cdot y \rangle_0} = \mathsf{DJ.Enc}_N(\langle \mathsf{sk} \cdot y \rangle_0)$$

Multiply with $\mathsf{DJ.Enc}_N(\mathsf{sk}^{-1} \bmod N^2)$ to get $\langle \mathsf{sk} \cdot x \cdot y \rangle$.

Rate-1 Arithmetic Garbling

$$\mathsf{sk}\cdot x\cdot \mathsf{sk}\cdot y = \underbrace{\langle \mathsf{sk}\cdot x\rangle_1 \cdot \langle \mathsf{sk}\cdot y\rangle_1}_{\text{Known to Evaluator}} - \underbrace{\mathsf{sk}\cdot x\cdot \langle \mathsf{sk}\cdot y\rangle_0}_{\mathsf{HSS.Mul}(C_{\langle \mathsf{sk}\cdot y\rangle_0}, \langle \mathsf{sk}\cdot x\rangle)} - \underbrace{\langle \mathsf{sk}\cdot x\rangle_0 \cdot \mathsf{sk}\cdot y}_{\mathsf{HSS.Mul}(C_{\langle \mathsf{sk}\cdot x\rangle_0}, \langle \mathsf{sk}\cdot y\rangle)} - \underbrace{\langle \mathsf{sk}\cdot x\rangle_0 \cdot \langle \mathsf{sk}\cdot y\rangle_0}_{\text{Known to Garbler}}$$

G contains:

$$C_{\langle \mathsf{sk}\cdot x\rangle_0} = \mathsf{DJ.Enc}_N(\langle \mathsf{sk}\cdot x\rangle_0)$$
$$C_{\langle \mathsf{sk}\cdot y\rangle_0} = \mathsf{DJ.Enc}_N(\langle \mathsf{sk}\cdot y\rangle_0)$$

Multiply with $\mathsf{DJ.Enc}_N(\mathsf{sk}^{-1} \bmod N^2)$ to get $\langle \mathsf{sk}\cdot x\cdot y\rangle$.

Rate: $\frac{1}{2}$?

Rate-1 Arithmetic Garbling

$$\mathsf{sk}\cdot x\cdot\mathsf{sk}\cdot y=\underbrace{\langle\mathsf{sk}\cdot x\rangle_1\cdot\langle\mathsf{sk}\cdot y\rangle_1}_{\text{Known to Evaluator}}-\underbrace{\mathsf{sk}\cdot x\cdot\langle\mathsf{sk}\cdot y\rangle_0}_{\mathsf{HSS.Mul}(C_{\langle\mathsf{sk}\cdot y\rangle_0},\langle\mathsf{sk}\cdot x\rangle)}-\underbrace{\langle\mathsf{sk}\cdot x\rangle_0\cdot\mathsf{sk}\cdot y}_{\mathsf{HSS.Mul}(C_{\langle\mathsf{sk}\cdot x\rangle_0},\langle\mathsf{sk}\cdot y\rangle)}-\underbrace{\langle\mathsf{sk}\cdot x\rangle_0\cdot\langle\mathsf{sk}\cdot y\rangle_0}_{\text{Known to Garbler}}$$

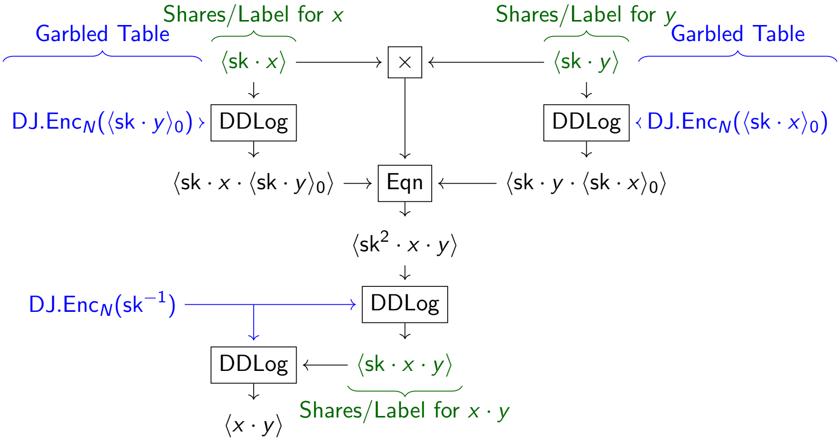
G contains:

$$C_{\langle\mathsf{sk}\cdot x\rangle_0}=\mathsf{DJ.Enc}_N(\langle\mathsf{sk}\cdot x\rangle_0)$$
$$C_{\langle\mathsf{sk}\cdot y\rangle_0}=\mathsf{DJ.Enc}_N(\langle\mathsf{sk}\cdot y\rangle_0)$$

Multiply with $\mathsf{DJ.Enc}_N(\mathsf{sk}^{-1} \bmod N^2)$ to get $\langle\mathsf{sk}\cdot x\cdot y\rangle$.

Rate: 1

Damgård-Jurik Arithmetic Garbling: Pipeline



Shares/Label for x

Shares/Label for y

Garbled Table

Garbled Table

$\langle \mathsf{sk} \cdot x \rangle$

$\times$

$\langle \mathsf{sk} \cdot y \rangle$

$\mathsf{DJ.Enc}_N(\langle \mathsf{sk} \cdot y \rangle_0)$

DDLog

DDLog

$\mathsf{DJ.Enc}_N(\langle \mathsf{sk} \cdot x \rangle_0)$

$\langle \mathsf{sk} \cdot x \cdot \langle \mathsf{sk} \cdot y \rangle_0 \rangle$

Eqn

$\langle \mathsf{sk} \cdot y \cdot \langle \mathsf{sk} \cdot x \rangle_0 \rangle$

$\langle \mathsf{sk}^2 \cdot x \cdot y \rangle$

$\mathsf{DJ.Enc}_N(\mathsf{sk}^{-1})$

DDLog

DDLog

$\langle \mathsf{sk} \cdot x \cdot y \rangle$

$\langle x \cdot y \rangle$

Shares/Label for $x \cdot y$