Silent Circuit Relinearisation: Sublinear-Size (Boolean and Arithmetic) Garbled Circuits from DCR

Pierre Meyer , Claudio Orlandi , Lawrence Roy , Peter Scholl

Aarhus University, Denmark

Crypto 2025

AARHUS UNIVERSITY

Today

Prologue

Advanced Cryptographic Primitives
from Homomorphic Secret Sharing

A new HSS technique. . .
(silent re-linearisation)

ACT I

. . . & its application to garbling
(via circuit randomisation)

ACT II

Advanced Primitives from Distributed DLog

Non-interactively computing shares of $\Delta \cdot xy$

1 If Alice and Bob hold $\langle \Delta\ x\rangle, \langle \Delta\ y\rangle, \mathsf{Enc}_\Delta(y)$

C'16: Boyle, Gilboa, Ishai

HSS for NC^1

2 Only Bob needs $\mathsf{Enc}_\Delta(y)$
(Alice can now pre-process!)
for specific Enc

EC'23: Couteau, Meyer, Passelègue, Riahinia

CPRF for NC^1

3 $\mathsf{Enc}_\Delta(y)$ replaced with $\mathsf{Enc}_\Delta(\langle x\rangle_A)$, $\mathsf{Enc}_\Delta(\langle y\rangle_B)$
(enc can now be rate-1 & pre-proc!)

TCC'24: Meyer, Orlandi, Roy, Scholl

Rate-1 arithmetic garbling

??'25: Behera,M,O,R,S

Private puncturing

4 **Alice and Bob hold $\langle \Delta\ x\rangle, \langle \Delta\ y\rangle$**
(no gate-by-gate blowup!)

C'25: M,O,R,S
FOCS'25: Ishai, Li, Lin

sublinear GC, P/poly CPRF

The Quest for Group-Based Succinct Garbling

1. (Boolean) polynomial overhead — FOCS'86: Yao
   - OWF
2. (Arithmetic) polynomial overhead — FOCS'11: Applebaum, Ishai, Kushilevitz
   - LWE
3. (Arithmetic & Boolean) fully succinct — EC'14: Boneh, Gentry, Gorbunov, Halevi, Nikolaenko, Segev, Vaikuntanathan, Vinayagamurthy
   - iO or FHE+ABE / LFE (LWE)
4. (Arithmetic) constant rate — EC'23: Ball, Li, Lin, Liu
   - LWE or DCR
5. (Arithmetic) rate-1 — TCC'24: Meyer, Orlandi, Roy, Scholl
   - DCR
6. (Boolean & Arithmetic) $o(\lambda)$ overhead — [E'25: Couteau, Hazay, Hegde, Kumar] and [C'25: Couteau, Hazay, Hegde, Kumar]
   - Power-DDH
7. (Boolean & Arithmetic) sublinear-size — [C'25: Meyer, Orlandi, Roy, Scholl] and [FOCS'25, C'25: Ishai, Li, Lin]
   - [DCR] and [P-DDH or P-RLWE or DCR]

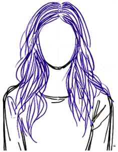
Advanced Cryptographic Primitives from Homomorphic Secret Sharing

Simplest example: Constrained PRFs

~~Advanced Cryptographic Primitives~~ from Homomorphic Secret Sharing

Later: garbling from HSS!

Constrained Pseudorandom Functions



1^λ

KeyGen

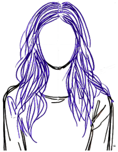
k

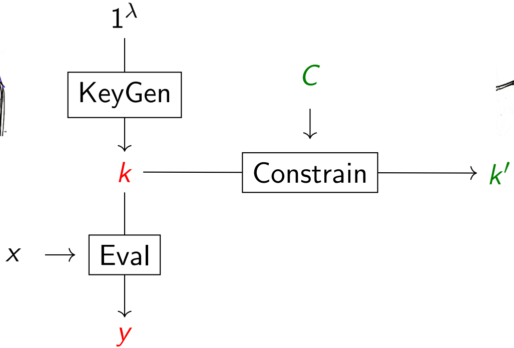
$x \longrightarrow$ Eval

y

Goal: Alice delegates to Bob the ability to evaluate her PRF on a subset of the domain

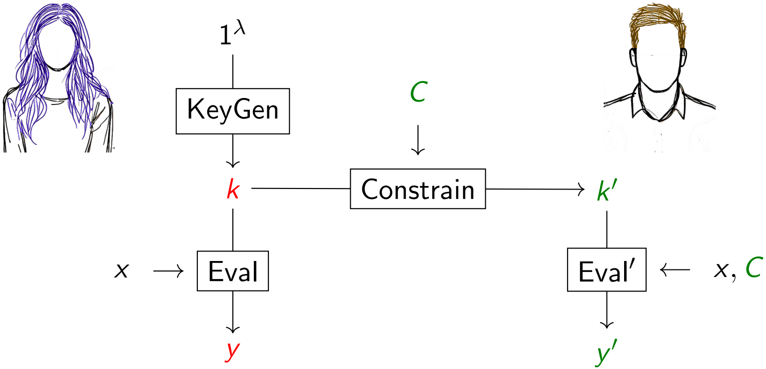
Constrained Pseudorandom Functions





Goal: Alice delegates to Bob the ability to evaluate her PRF on a subset of the domain

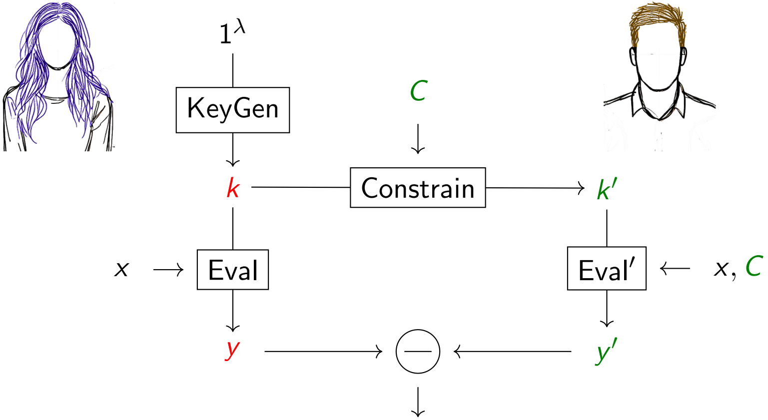
Constrained Pseudorandom Functions



$$y' = \begin{cases} y & \text{if } C(x) = 0 \\ \$ & \text{if } C(x) = 1 \end{cases}$$

Goal: Alice delegates to Bob the ability to evaluate her PRF on a subset of the domain

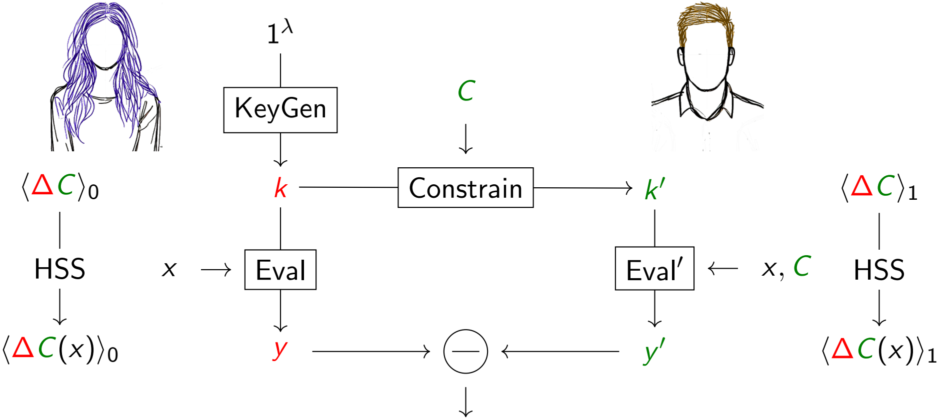
Constrained Pseudorandom Functions



$$\begin{cases} 0 & \text{if } C(x) = 0 \\ \$ & \text{if } C(x) = 1 \end{cases}$$

Goal: Alice delegates to Bob the ability to evaluate her PRF on a subset of the domain

Constrained Pseudorandom Functions from Homomorphic Secret Sharing

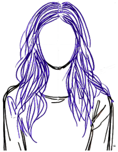


Authenticated shares of X:
$\Delta X = \langle \Delta X \rangle_1 - \langle \Delta X \rangle_0$

$$\begin{cases} 0 & \text{if } C(x) = 0 \\ \Delta & \text{if } C(x) = 1 \end{cases}$$

Goal: Alice delegates to Bob the ability to evaluate her PRF on a subset of the domain

Constrained Pseudorandom Functions from Homomorphic Secret Sharing



$$\begin{tikzcd}
 & & 1^\lambda \arrow[d, dash] & & & & \\
 & & \boxed{\mathsf{KeyGen}} \arrow[d] & C \arrow[d] & & & \\
\langle \Delta C \rangle_0 \arrow[d, dash] & & k \arrow[r, dash] \arrow[d, dash] & \boxed{\mathsf{Constrain}} \arrow[r] & k' \arrow[d, dash] & & \langle \Delta C \rangle_1 \arrow[d, dash] \\
\mathsf{HSS} \arrow[d] & x \arrow[r] & \boxed{\mathsf{Eval}} \arrow[d] & & \boxed{\mathsf{Eval}'} \arrow[d] & x, C \arrow[l] & \mathsf{HSS} \arrow[d] \\
\langle \Delta C(x) \rangle_0 & & H(y) \arrow[r] & \ominus \arrow[d] & H(y') \arrow[l] & & \langle \Delta C(x) \rangle_1 \\
 & & & \begin{cases} 0 & \text{if } C(x) = 0 \\ \$ & \text{if } C(x) = 1 \end{cases} & & &
\end{tikzcd}$$

Goal: Alice delegates to Bob the ability to evaluate her PRF on a subset of the domain

Technical HSS Challenge

Alice & Bob need to go from $\langle \Delta\ x \rangle$ to $\langle \Delta\ f(x) \rangle$ (for an arbitrary public f)

- Requirement: Alice's share must be independent of x (but she can know Δ)
- Relaxation: Bob can know x (but not Δ)

Technical HSS Challenge

Alice & Bob need to go from $\langle \Delta \; x \rangle$ to $\langle \Delta \; f(x) \rangle$ (for an arbitrary public f)

- Requirement: Alice's share must be independent of x (but she can know Δ)
- Relaxation: Bob can know x (but not Δ)

What does standard HSS give us?

DDLog over Damgård-Jurik [C'21: Roy and Singh]

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

Damgård-Jurik Cryptosystem
Public-key: RSA modulus N
Private-key: $\Delta = \lvert\mathbb{H}\rvert = \varphi(N)$
$\mathsf{DJ.Enc}_N(x) \rightarrow r^{N^2} \cdot \exp(x) \in \mathbb{Z}/N^3\mathbb{Z}$
$\mathsf{DJ.Dec}_\Delta(x) = \Delta^{-1} \cdot \mathsf{DLog}(x^\Delta)$

DDLog over Damgård-Jurik [C'21: Roy and Singh]

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

$$\mathbb{G} = \mathbb{Z}_{N^3}^{\times}$$

Damgård-Jurik Cryptosystem
Public-key: RSA modulus N
Private-key: $\Delta = \lvert\mathbb{H}\rvert = \varphi(N)$
$\mathsf{DJ.Enc}_N(x) \to r^{N^2} \cdot \exp(x) \in \mathbb{Z}/N^3\mathbb{Z}$
$\mathsf{DJ.Dec}_\Delta(x) = \Delta^{-1} \cdot \mathsf{DLog}(x^\Delta)$

DDLog over Damgård-Jurik [C'21: Roy and Singh]

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

Damgård-Jurik Cryptosystem
Public-key: RSA modulus N
Private-key: $\Delta = \lvert\mathbb{H}\rvert = \varphi(N)$
$\mathsf{DJ.Enc}_N(x) \to r^{N^2} \cdot \exp(x) \in \mathbb{Z}/N^3\mathbb{Z}$
$\mathsf{DJ.Dec}_\Delta(x) = \Delta^{-1} \cdot \mathsf{DLog}(x^\Delta)$

$$\mathbb{G} = \mathbb{Z}_{N^3}^\times$$

$$\mathbb{F} = (1 + N\mathbb{Z}_{N^3})^\times$$

DDLog over Damgård-Jurik [C'21: Roy and Singh]

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

Damgård-Jurik Cryptosystem
Public-key: RSA modulus N
Private-key: $\Delta = \lvert\mathbb{H}\rvert = \varphi(N)$
$\mathsf{DJ.Enc}_N(x) \to r^{N^2} \cdot \exp(x) \in \mathbb{Z}/N^3\mathbb{Z}$
$\mathsf{DJ.Dec}_\Delta(x) = \Delta^{-1} \cdot \mathsf{DLog}(x^\Delta)$

$$\mathbb{G} = \mathbb{Z}^\times_{N^3}$$

$$\mathbb{F} = (1 + N\mathbb{Z}_{N^3})^\times$$

$$\mathbb{H} = (\mathbb{Z}^\times_{N^3})^{N^2}$$

DDLog over Damgård-Jurik [C'21: Roy and Singh]

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

Damgård-Jurik Cryptosystem
Public-key: RSA modulus N
Private-key: $\Delta = \lvert\mathbb{H}\rvert = \varphi(N)$
$\mathsf{DJ.Enc}_N(x) \to \quad r^{N^2} \cdot \exp(x)$
$\in \mathbb{Z}/N^3\mathbb{Z}$
$\mathsf{DJ.Dec}_\Delta(x) = \Delta^{-1} \cdot \mathsf{DLog}(x^\Delta)$

$$\mathbb{G} = \mathbb{Z}_{N^3}^\times$$
$$\mathbb{F} = (1 + N\mathbb{Z}_{N^3})^\times$$
$$\mathbb{H} = (\mathbb{Z}_{N^3}^\times)^{N^2} \simeq \mathbb{Z}_N$$

DDLog over Damgård-Jurik [C'21: Roy and Singh]

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

Damgård-Jurik Cryptosystem	
Public-key: RSA modulus N	
Private-key: $\Delta = \lvert\mathbb{H}\rvert = \varphi(N)$	
$\mathsf{DJ.Enc}_N(x) \to$	$r^{N^2} \cdot \exp(x)$
	$\in \mathbb{Z}/N^3\mathbb{Z}$
$\mathsf{DJ.Dec}_\Delta(x) = \Delta^{-1} \cdot \mathsf{DLog}(x^\Delta)$	

$$\mathbb{G} = \mathbb{Z}_{N^3}^\times$$

$$\mathbb{F} = (1 + N\mathbb{Z}_{N^3})^\times$$

$$\mathbb{H} = (\mathbb{Z}_{N^3}^\times)^{N^2} \simeq \mathbb{Z}_N$$

Promise

$$g_1/g_0 = \exp(x) \in \mathbb{F}$$

DDLog over Damgård-Jurik [C'21: Roy and Singh]

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

Damgård-Jurik Cryptosystem
Public-key: RSA modulus N
Private-key: $\Delta = \lvert\mathbb{H}\rvert = \varphi(N)$
$\mathrm{DJ.Enc}_N(x) \to \quad r^{N^2} \cdot \exp(x)$
$\in \mathbb{Z}/N^3\mathbb{Z}$
$\mathrm{DJ.Dec}_\Delta(x) = \Delta^{-1} \cdot \mathrm{DLog}(x^\Delta)$

$$\mathbb{G} = \mathbb{Z}_{N^3}^\times$$

$$\mathbb{F} = (1 + N\mathbb{Z}_{N^3})^\times \simeq \mathbb{Z}_{N^2}^+$$

$$\mathbb{H} = (\mathbb{Z}_{N^3}^\times)^{N^2} \simeq \mathbb{Z}_N$$

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

$$\mathrm{DLog}(1 + Nx) = x - \frac{Nx^2}{2}$$

<u>Promise</u>

$$g_1/g_0 = \exp(x) \in \mathbb{F}$$

DDLog over Damgård-Jurik [C'21: Roy and Singh]

$$\underset{\text{easy DLog}\downarrow}{}\qquad\qquad \underset{\swarrow\text{hard DLog}}{}$$

$$\mathbb{G} \simeq \mathbb{F} \times \mathbb{H}$$

$$\mathbb{G} = \mathbb{Z}_{N^3}^\times$$

$$\mathbb{F} = (1 + N\mathbb{Z}_{N^3})^\times = \langle \exp(1) \rangle \simeq \mathbb{Z}_{N^2}^+$$

$$\mathbb{H} = (\mathbb{Z}_{N^3}^\times)^{N^2} \simeq \mathbb{Z}_N$$

Promise

$$g_1/g_0 = \exp(x) \in \mathbb{F}$$

Damgård-Jurik Cryptosystem
Public-key: RSA modulus N
Private-key: $\Delta = \lvert\mathbb{H}\rvert = \varphi(N)$
$\mathrm{DJ.Enc}_N(x) \to \quad r^{N^2} \cdot \exp(x)$
$\in \mathbb{Z}/N^3\mathbb{Z}$
$\mathrm{DJ.Dec}_\Delta(x) = \Delta^{-1} \cdot \mathrm{DLog}(x^\Delta)$

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

$$\mathrm{DLog}(1 + Nx) = x - \frac{Nx^2}{2}$$

DDLog over Damgård-Jurik [C'21: Roy and Singh]

Damgård-Jurik Cryptosystem
Public-key: RSA modulus N
Private-key: $\Delta = |\mathbb{H}| = \varphi(N)$
$\mathsf{DJ.Enc}_N(x) \rightarrow \quad r^{N^2} \cdot \exp(x) \in \mathbb{Z}/N^3\mathbb{Z}$
$\mathsf{DJ.Dec}_\Delta(x) = \Delta^{-1} \cdot \mathsf{DLog}(x^\Delta)$

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

$$\mathbb{G} = \mathbb{Z}_{N^3}^\times$$
$$\mathbb{F} = (1 + N\mathbb{Z}_{N^3})^\times = \langle \exp(1) \rangle \simeq \mathbb{Z}_{N^2}^+$$
$$\mathbb{H} = (\mathbb{Z}_{N^3}^\times)^{N^2} \simeq \mathbb{Z}_N$$

$$\exp(x) = 1 + Nx + \frac{(Nx)^2}{2}$$
$$\mathsf{DLog}(1 + Nx) = x - \frac{Nx^2}{2}$$

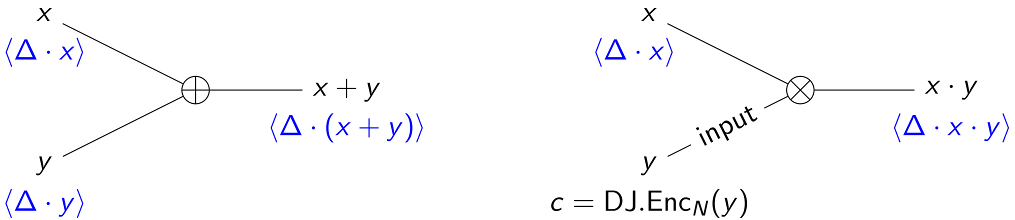
$$\mathsf{DDLog}(x) = \mathsf{DLog}\left(\frac{x}{x \bmod N}\right)$$

Promise

$$g_1/g_0 = \exp(x) \in \mathbb{F}$$

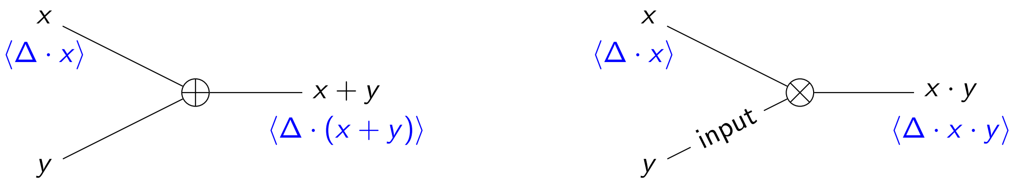
$$\mathsf{DDLog}(g_1) - \mathsf{DDLog}(g_0) \equiv x \pmod{N^2}$$

Homomorphic Secret Sharing from Damgård-Jurik



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

Homomorphic Secret Sharing from Damgård-Jurik



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

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

$$\frac{c^{\langle \Delta \cdot x \rangle_1}}{c^{\langle \Delta \cdot x \rangle_0}} = (r^{N^2} \exp(y))^{\Delta \cdot x} = \exp(\Delta \cdot x \cdot y)$$

Technical HSS Challenge

Alice & Bob need to go from $\langle \Delta\ x \rangle$ to $\langle \Delta\ f(x) \rangle$ (for an arbitrary public f)

- Requirement: Alice's share must be independent of x (but she can know Δ)
- Relaxation: Bob can know x (but not Δ)

What does standard HSS give us?

Technical HSS Challenge

Alice & Bob need to go from $\langle \Delta\ x \rangle$ to $\langle \Delta\ f(x) \rangle$ (for an arbitrary public f)

- Requirement: Alice's share must be independent of x (but she can know Δ)
- Relaxation: Bob can know x (but not Δ)

What does standard HSS give us?

Multiplication only by inputs.

Technical HSS Challenge

Alice & Bob need to go from $\langle \Delta \; x \rangle$ to $\langle \Delta \; f(x) \rangle$ (for an arbitrary public f)

- Requirement: Alice's share must be independent of x (but she can know Δ)
- Relaxation: Bob can know x (but not Δ)

What does standard HSS give us?

Multiplication only by inputs.

Our solution: **Silent Re-Linearisation**

Inspired by QuickSilver (CCS'21: Yang, Sarkar, Weng, and Wang) and (earlier) Line-Point Zero Knowledge (ITC'21: Dittmer, Ishai, Ostrovsky)

$$\begin{aligned}\langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 &= (\langle \Delta \cdot \alpha \rangle_1 - \Delta \cdot \alpha) \cdot (\langle \Delta \cdot \beta \rangle_1 - \Delta \cdot \beta) \\ &= \Delta^2 \cdot \alpha\beta + \Delta \cdot (-\alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1) + \langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1\end{aligned}$$

Inspired by QuickSilver (CCS'21: Yang, Sarkar, Weng, and Wang)
and (earlier) Line-Point Zero Knowledge (ITC'21: Dittmer, Ishai, Ostrovsky)

Proof:

$$\begin{aligned}\langle \Delta\cdot\alpha\rangle_0\cdot\langle \Delta\cdot\beta\rangle_0 &= (\langle \Delta\cdot\alpha\rangle_1-\Delta\cdot\alpha)\cdot(\langle \Delta\cdot\beta\rangle_1-\Delta\cdot\beta)\\ &= \Delta^2\cdot\alpha\beta+\Delta\cdot(-\alpha\cdot\langle \Delta\cdot\beta\rangle_1-\beta\cdot\langle \Delta\cdot\alpha\rangle_1)+\langle \Delta\cdot\alpha\rangle_1\cdot\langle \Delta\cdot\beta\rangle_1\end{aligned}$$

$$\boxed{\langle \Delta\cdot\alpha\rangle_1\cdot\langle \Delta\cdot\beta\rangle_1-\langle \Delta\cdot\alpha\rangle_0\cdot\langle \Delta\cdot\beta\rangle_0=\Delta\cdot(-\Delta\cdot\alpha\beta-\alpha\cdot\langle \Delta\cdot\beta\rangle_1-\beta\cdot\langle \Delta\cdot\alpha\rangle_1)}$$

Inspired by QuickSilver (CCS'21: Yang, Sarkar, Weng, and Wang)
and (earlier) Line-Point Zero Knowledge (ITC'21: Dittmer, Ishai, Ostrovsky)

Proof:

$$\begin{aligned}\langle \Delta\cdot\alpha\rangle_0 \cdot \langle \Delta\cdot\beta\rangle_0 &= (\langle \Delta\cdot\alpha\rangle_1 - \Delta\cdot\alpha)\cdot(\langle \Delta\cdot\beta\rangle_1 - \Delta\cdot\beta) \\ &= \Delta^2\cdot\alpha\beta + \Delta\cdot(-\alpha\cdot\langle \Delta\cdot\beta\rangle_1 - \beta\cdot\langle \Delta\cdot\alpha\rangle_1) + \langle \Delta\cdot\alpha\rangle_1\cdot\langle \Delta\cdot\beta\rangle_1\end{aligned}$$

$$\boxed{\langle \Delta\cdot\alpha\rangle_1 \cdot \langle \Delta\cdot\beta\rangle_1 - \langle \Delta\cdot\alpha\rangle_0 \cdot \langle \Delta\cdot\beta\rangle_0 = \Delta\cdot(-\Delta\cdot\alpha\beta - \alpha\cdot\langle \Delta\cdot\beta\rangle_1 - \beta\cdot\langle \Delta\cdot\alpha\rangle_1)}$$

Authenticated shares of α and β $\xrightarrow{\text{Homomorphism}}$ **Authenticated shares of $\alpha\cdot\beta$**

Inspired by QuickSilver (CCS'21: Yang, Sarkar, Weng, and Wang)
and (earlier) Line-Point Zero Knowledge (ITC'21: Dittmer, Ishai, Ostrovsky)

Proof:

$$\begin{aligned}\langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 &= (\langle \Delta \cdot \alpha \rangle_1 - \Delta \cdot \alpha) \cdot (\langle \Delta \cdot \beta \rangle_1 - \Delta \cdot \beta) \\ &= \Delta^2 \cdot \alpha\beta + \Delta \cdot (-\alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1) + \langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1\end{aligned}$$

$$\boxed{\langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1 - \langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 = \Delta \cdot (-\Delta \cdot \alpha\beta - \alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1)}$$

Authenticated shares of α and β $\xrightarrow{\text{Homomorphism}}$ **Authenticated shares of $\alpha \cdot \beta$**

Encryption with
"Distributed Decryption"

$$\begin{cases} \mathsf{Enc}_\Delta(X) \\ \langle \Delta \cdot Y \rangle_\sigma \end{cases} \longmapsto \langle \Delta \cdot XY \rangle_\sigma$$

Inspired by QuickSilver (CCS'21: Yang, Sarkar, Weng, and Wang)
and (earlier) Line-Point Zero Knowledge (ITC'21: Dittmer, Ishai, Ostrovsky)

Proof:

$$\begin{aligned} \langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 &= (\langle \Delta \cdot \alpha \rangle_1 - \Delta \cdot \alpha) \cdot (\langle \Delta \cdot \beta \rangle_1 - \Delta \cdot \beta) \\ &= \Delta^2 \cdot \alpha\beta + \Delta \cdot (-\alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1) + \langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1 \end{aligned}$$

$$\boxed{\langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1 - \langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 = \Delta \cdot (-\Delta \cdot \alpha\beta - \alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1)}$$

$$\textbf{Authenticated shares of } \alpha \textbf{ and } \beta \xrightarrow{\text{Homomorphism}} \textbf{Authenticated shares of } \alpha \cdot \beta$$

Encryption with
"Distributed Decryption"

$$\begin{cases} \mathrm{Enc}_\Delta(\Delta^{-1}) \\ \langle \Delta \cdot Y \rangle_\sigma \end{cases} \longmapsto \langle \Delta \cdot \Delta^{-1} Y \rangle_\sigma$$

Inspired by QuickSilver (CCS'21: Yang, Sarkar, Weng, and Wang)
and (earlier) Line-Point Zero Knowledge (ITC'21: Dittmer, Ishai, Ostrovsky)

Proof:

$$\begin{aligned}\langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 &= (\langle \Delta \cdot \alpha \rangle_1 - \Delta \cdot \alpha) \cdot (\langle \Delta \cdot \beta \rangle_1 - \Delta \cdot \beta) \\ &= \Delta^2 \cdot \alpha\beta + \Delta \cdot (-\alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1) + \langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1\end{aligned}$$

$$\boxed{\langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1 - \langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 = \Delta \cdot (-\Delta \cdot \alpha\beta - \alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1)}$$

$$\textbf{Authenticated shares of } \boldsymbol{\alpha} \textbf{ and } \boldsymbol{\beta} \quad \xrightarrow{\text{Homomorphism}} \quad \textbf{Authenticated shares of } \boldsymbol{\alpha \cdot \beta}$$

Encryption with
"Distributed Decryption"

$$\begin{cases} \mathsf{Enc}_\Delta(\Delta^{-1}) \\ \langle \Delta \cdot Y \rangle_\sigma \end{cases} \longmapsto \langle Y \rangle_\sigma$$

Inspired by QuickSilver (CCS'21: Yang, Sarkar, Weng, and Wang)
and (earlier) Line-Point Zero Knowledge (ITC'21: Dittmer, Ishai, Ostrovsky)

Proof:

$$\begin{aligned}\langle \Delta \cdot \alpha\rangle_0 \cdot \langle \Delta \cdot \beta\rangle_0 &= (\langle \Delta \cdot \alpha\rangle_1 - \Delta \cdot \alpha) \cdot (\langle \Delta \cdot \beta\rangle_1 - \Delta \cdot \beta) \\ &= \Delta^2 \cdot \alpha\beta + \Delta \cdot (-\alpha \cdot \langle \Delta \cdot \beta\rangle_1 - \beta \cdot \langle \Delta \cdot \alpha\rangle_1) + \langle \Delta \cdot \alpha\rangle_1 \cdot \langle \Delta \cdot \beta\rangle_1\end{aligned}$$

$$\boxed{\langle \Delta \cdot \alpha\rangle_1 \cdot \langle \Delta \cdot \beta\rangle_1 - \langle \Delta \cdot \alpha\rangle_0 \cdot \langle \Delta \cdot \beta\rangle_0 = \Delta \cdot (-\Delta \cdot \alpha\beta - \alpha \cdot \langle \Delta \cdot \beta\rangle_1 - \beta \cdot \langle \Delta \cdot \alpha\rangle_1)}$$

Authenticated shares of α and β $\xrightarrow{\text{Homomorphism}}$ **Authenticated shares of $\alpha \cdot \beta$**

Both parties hold
$c = \mathrm{Enc}_\Delta(\Delta^{-1})$

Encryption with
"Distributed Decryption"

$$\begin{cases}\mathrm{Enc}_\Delta(\Delta^{-1}) \\ \langle \Delta \cdot Y\rangle_\sigma\end{cases} \longmapsto \langle Y\rangle_\sigma$$

Shares of
$$-\boldsymbol{\Delta} \cdot \boldsymbol{\alpha\beta} - \boldsymbol{\alpha} \cdot \langle \boldsymbol{\Delta} \cdot \boldsymbol{\beta}\rangle_1 - \boldsymbol{\beta} \cdot \langle \boldsymbol{\Delta} \cdot \boldsymbol{\alpha}\rangle_1$$

Inspired by QuickSilver (CCS'21: Yang, Sarkar, Weng, and Wang)
and (earlier) Line-Point Zero Knowledge (ITC'21: Dittmer, Ishai, Ostrovsky)

Proof:

$$\begin{aligned} \langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 &= (\langle \Delta \cdot \alpha \rangle_1 - \Delta \cdot \alpha) \cdot (\langle \Delta \cdot \beta \rangle_1 - \Delta \cdot \beta) \\ &= \Delta^2 \cdot \alpha\beta + \Delta \cdot (-\alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1) + \langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1 \end{aligned}$$

$$\boxed{\langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1 - \langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 = \Delta \cdot (-\Delta \cdot \alpha\beta - \alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1)}$$

Authenticated shares of α and β $\xrightarrow{\text{Homomorphism}}$ **Authenticated shares of $\alpha \cdot \beta$**

Both parties hold
$c = \mathsf{Enc}_\Delta(\Delta^{-1})$

Encryption with
"Distributed Decryption"

$$\begin{cases} \mathsf{Enc}_\Delta(\Delta^{-1}) \\ \langle \Delta \cdot Y \rangle_\sigma \end{cases} \longmapsto \langle Y \rangle_\sigma$$

Bob (holding $\langle \cdot \rangle_1$)
knows α, β (semi-privacy)

Shares of
$\boldsymbol{-\Delta \cdot \alpha\beta - \alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1}$

Inspired by QuickSilver (CCS'21: Yang, Sarkar, Weng, and Wang)
and (earlier) Line-Point Zero Knowledge (ITC'21: Dittmer, Ishai, Ostrovsky)

Proof:

$$\begin{aligned} \langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 &= (\langle \Delta \cdot \alpha \rangle_1 - \Delta \cdot \alpha) \cdot (\langle \Delta \cdot \beta \rangle_1 - \Delta \cdot \beta) \\ &= \Delta^2 \cdot \alpha\beta + \Delta \cdot (-\alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1) + \langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1 \end{aligned}$$

$$\boxed{\langle \Delta \cdot \alpha \rangle_1 \cdot \langle \Delta \cdot \beta \rangle_1 - \langle \Delta \cdot \alpha \rangle_0 \cdot \langle \Delta \cdot \beta \rangle_0 = \Delta \cdot (-\Delta \cdot \alpha\beta - \alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1)}$$

Authenticated shares of α and β $\xrightarrow{\text{Homomorphism}}$ **Authenticated shares of $\alpha \cdot \beta$**

Both parties hold
$c = \mathsf{Enc}_\Delta(\Delta^{-1})$

Encryption with
"Distributed Decryption"

$$\begin{cases} \mathsf{Enc}_\Delta(\Delta^{-1}) \\ \langle \Delta \cdot Y \rangle_\sigma \end{cases} \longmapsto \langle Y \rangle_\sigma$$

Bob (holding $\langle \cdot \rangle_1$)
knows α, β (semi-privacy)

Shares of
$\boldsymbol{-\Delta \cdot \alpha\beta - \alpha \cdot \langle \Delta \cdot \beta \rangle_1 - \beta \cdot \langle \Delta \cdot \alpha \rangle_1}$

Alice and Bob hold...

...auth shares of α and β	...auth shares of the ugly blue term	...shares of blue term	...auth shares of $\alpha\beta$

$\langle \Delta\ \alpha \rangle$

$\langle \Delta\ \beta \rangle$

$$\langle \Delta\ \alpha \rangle \otimes \langle \Delta\ \beta \rangle \longrightarrow \langle \Delta\ (-\Delta\ \alpha\beta - \alpha \cdot \langle \Delta\ \beta \rangle_1 - \beta \cdot \langle \Delta\ \alpha \rangle_1) \rangle$$

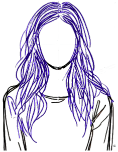
Distributed Decryption (a.k.a. DDLog)

$$\longrightarrow \langle -\Delta\ \alpha\beta - \alpha\ \langle \Delta\ \beta \rangle_1 - \beta \cdot \langle \Delta\ \alpha \rangle_1 \rangle \longrightarrow \langle \Delta\ \alpha\beta \rangle$$

$\mathsf{Enc}_\Delta(\Delta^{-1})$
(held by both parties)

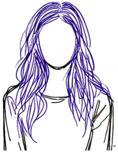
Bob locally adds
$\alpha\ \langle \Delta\ \beta \rangle_1 + \beta\ \langle \Delta\ \alpha \rangle_1$

Offline-Online Homomorphic Secret Sharing



$$
\begin{tikzcd}
& \langle \Delta \cdot x \rangle_0 \arrow[d, no head] & & (x,\ \langle \Delta \cdot x \rangle_1) \arrow[d, no head] & \\
C \arrow[r] & \boxed{\mathsf{Eval}} \arrow[d] & \mathsf{Enc}_{\Delta}(\Delta^{-1}) \arrow[l] \arrow[r] & \boxed{\mathsf{Eval}} \arrow[d] & C \arrow[l] \\
& \langle \Delta C(x) \rangle_0 & & \langle \Delta C(x) \rangle_1 &
\end{tikzcd}
$$

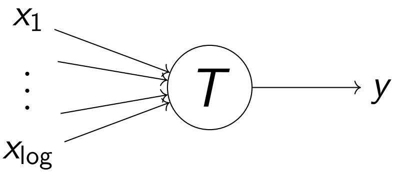
Offline-Online Homomorphic Secret Sharing



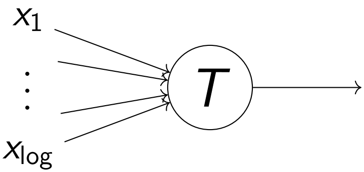
$$
\begin{tikzcd}
 & \langle \Delta \cdot x \rangle_0 \arrow[d, dash] & & (\mathrm{x},\ \langle \Delta \cdot x \rangle_1) \arrow[d, dash] & \\
C \arrow[r] & \boxed{\mathsf{Eval}} \arrow[d] & \mathsf{Enc}_\Delta(\Delta^{-1}) \arrow[l] \arrow[r] & \boxed{\mathsf{Eval}} \arrow[d] & C \arrow[l] \\
 & \langle \Delta C(x) \rangle_0 \arrow[d, dash] & & \langle \Delta C(x) \rangle_1 \arrow[d, dash] & \\
C' \arrow[r] & \boxed{\mathsf{Eval}'} \arrow[d] & \mathsf{Enc}_\Delta(y) \arrow[l] \arrow[r] & \boxed{\mathsf{Eval}'} \arrow[d] & C' \arrow[l] \\
 & \langle \Delta C(x) C'(y) \rangle_0 & & \langle \Delta C(x) C'(y) \rangle_1 &
\end{tikzcd}
$$

Sublinear-Size Boolean Garbling from Homomorphic Secret Sharing

Truth-Table Circuits

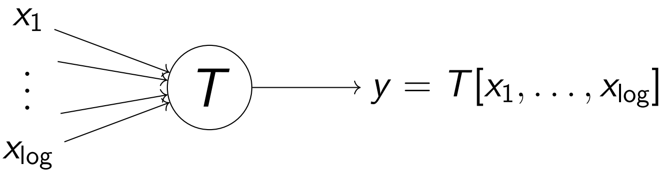


Truth-Table Circuits



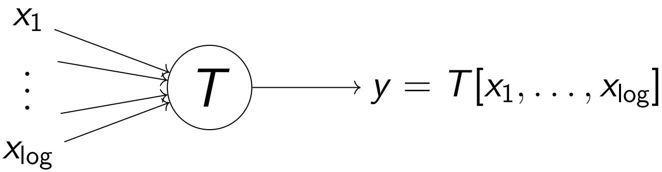
$$y = T[x_1, \ldots, x_{\log}]$$

Truth-Table Circuits



Fan-in 2 layered circuits $\rightarrow$ $\frac{1}{\log\log}$-sized truth-table circuits (EC'19: Couteau)

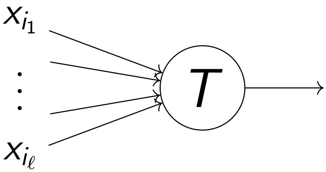
Truth-Table Circuits



Fan-in 2 layered circuits $\rightarrow$ $\frac{1}{\log\log}$-sized truth-table circuits (EC'19: Couteau)

Goal: Garble truth-table circuits with rate 1.

Garbling Invariants

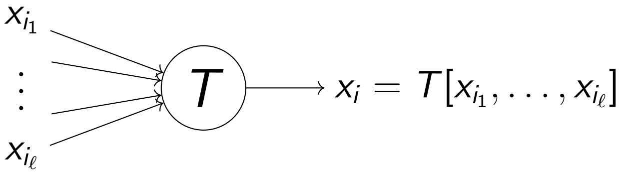


$$x_i = T[x_{i_1}, \ldots, x_{i_\ell}]$$

Garbling Invariants

For each wire x_j:

- Mask: $r_j := \mathsf{PRF}_k(i)$.
- Color Bit: $\bar{x}_j := x_j \oplus r_j$.
- Authenticator: $\langle \Delta \cdot \bar{x}_j \rangle$.
  I.e., $\langle \Delta \cdot \bar{x}_j \rangle_1 = \langle \Delta \cdot \bar{x}_j \rangle_0 + \Delta \cdot \bar{x}_j$

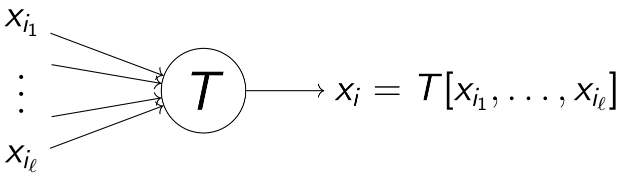


Garbling Invariants

For each wire x_j:

- Mask: $r_j := \mathsf{PRF}_k(i)$.
- Color Bit: $\bar{x}_j := x_j \oplus r_j$.
- Authenticator: $\langle \Delta \cdot \bar{x}_j \rangle$.
  I.e., $\langle \Delta \cdot \bar{x}_j \rangle_1 = \langle \Delta \cdot \bar{x}_j \rangle_0 + \Delta \cdot \bar{x}_j$

Wire label: $(\bar{x}_j, \langle \Delta \cdot \bar{x}_j \rangle_1)$.

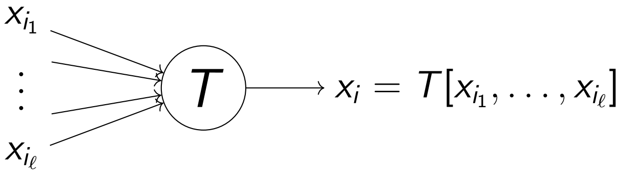


Garbling Invariants

For each wire x_j:

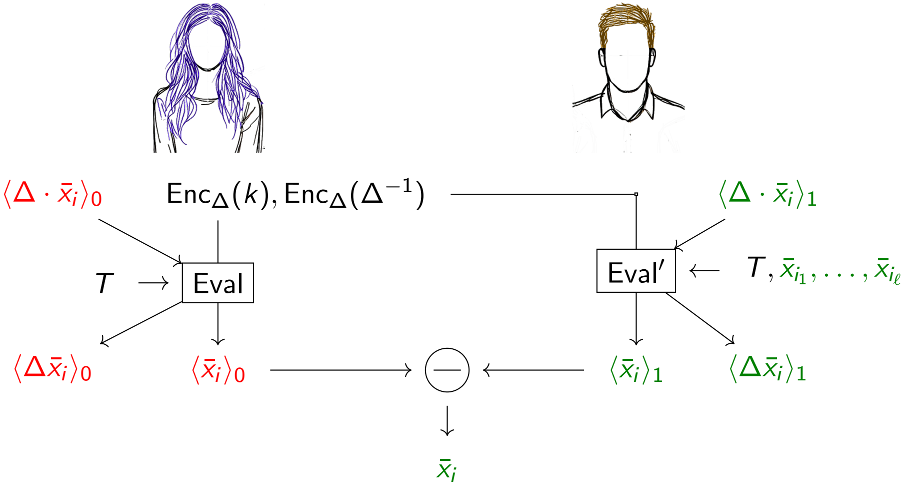
- Mask: $r_j := \mathsf{PRF}_k(i)$.
- Color Bit: $\bar{x}_j := x_j \oplus r_j$.
- Authenticator: $\langle \Delta \cdot \bar{x}_j \rangle$.
  I.e., $\langle \Delta \cdot \bar{x}_j \rangle_1 = \langle \Delta \cdot \bar{x}_j \rangle_0 + \Delta \cdot \bar{x}_j$

Wire label: $(\bar{x}_j, \langle \Delta \cdot \bar{x}_j \rangle_1)$.

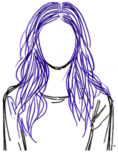


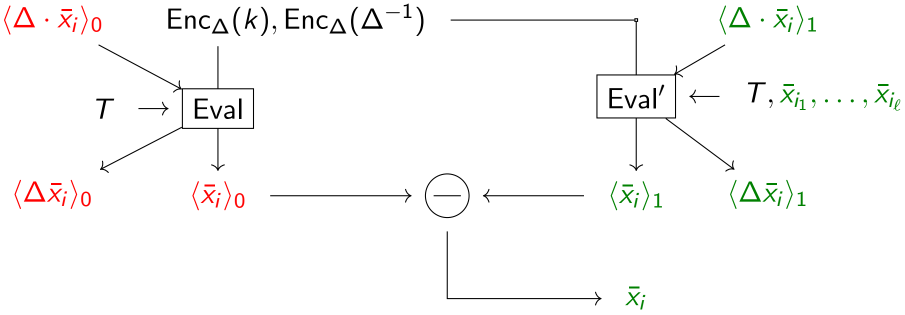
How to get the output wire label $(\bar{x}_i, \langle \Delta \cdot \bar{x}_i \rangle_1)$?

Garbling Protocol from Homomorphic Secret Sharing

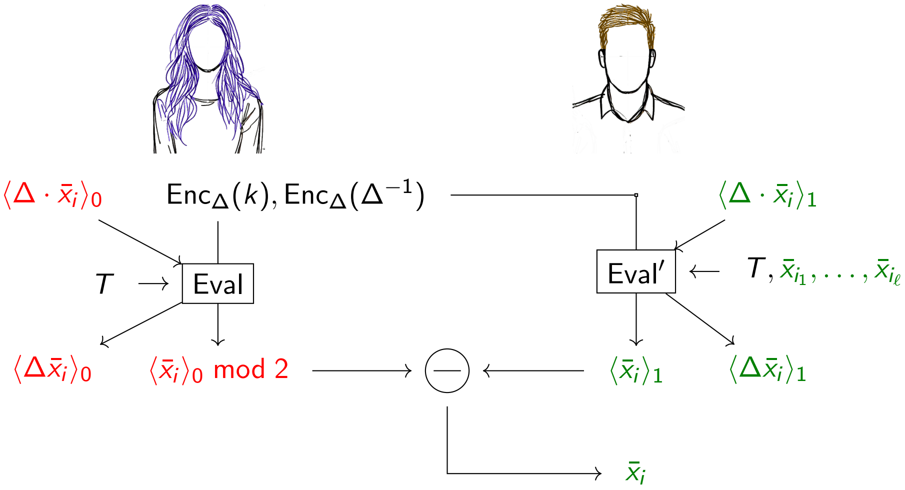


Garbling Protocol from Homomorphic Secret Sharing

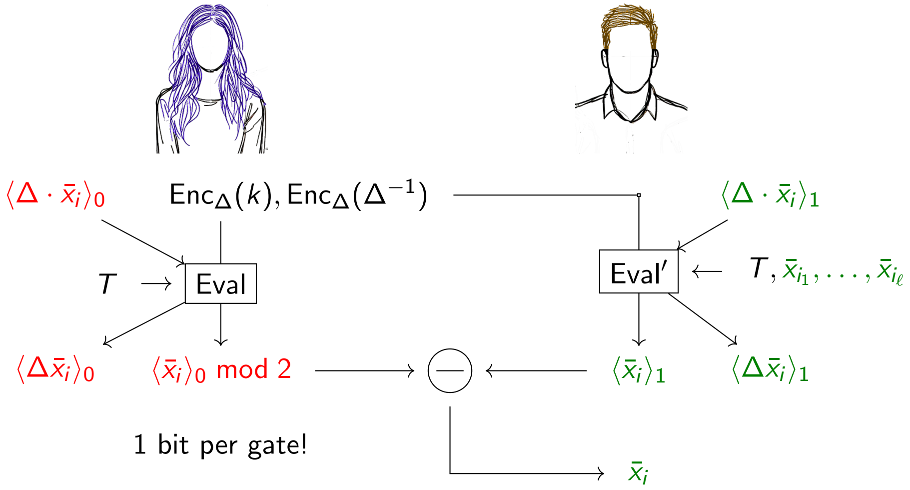




Garbling Protocol from Homomorphic Secret Sharing



Garbling Protocol from Homomorphic Secret Sharing



Representing Truth Tables

$$x_i = T[x_{i_1}, \ldots, x_{i_\ell}]$$

Representing Truth Tables

$$x_i = T[x_{i_1}, \ldots, x_{i_\ell}]$$

$$\bar{x}_i = r_i \oplus T[r_{i_1} \oplus \bar{x}_{i_1}, \ldots, r_{i_\ell} \oplus \bar{x}_{i_\ell}]$$

Representing Truth Tables

$$
\begin{aligned}
x_i &= T[x_{i_1}, \ldots, x_{i_\ell}] \\
\bar{x}_i &= r_i \oplus T[r_{i_1} \oplus \bar{x}_{i_1}, \ldots, r_{i_\ell} \oplus \bar{x}_{i_\ell}] \\
&= \sum_{u_1,\ldots,u_\ell \in \{0,1\}^\ell} (r_i \oplus T[r_{i_1} \oplus u_1, \ldots, r_{i_\ell} \oplus u_\ell]) \left(\begin{cases} 1 & \text{if } (u_1, \ldots, u_\ell) = (\bar{x}_{i_1}, \ldots, \bar{x}_{i_\ell}) \\ 0 & \text{otherwise} \end{cases} \right)
\end{aligned}
$$

Representing Truth Tables

$$
\begin{aligned}
x_i &= T[x_{i_1}, \ldots, x_{i_\ell}] \\
\bar{x}_i &= r_i \oplus T[r_{i_1} \oplus \bar{x}_{i_1}, \ldots, r_{i_\ell} \oplus \bar{x}_{i_\ell}] \\
&= \sum_{u_1,\ldots,u_\ell \in \{0,1\}^\ell} (r_i \oplus T[r_{i_1} \oplus u_1, \ldots, r_{i_\ell} \oplus u_\ell]) \left(\begin{cases} 1 & \text{if } (u_1, \ldots, u_\ell) = (\bar{x}_{i_1}, \ldots, \bar{x}_{i_\ell}) \\ 0 & \text{otherwise} \end{cases} \right)
\end{aligned}
$$

Representing Truth Tables

$$
\begin{aligned}
x_i &= T[x_{i_1}, \dots, x_{i_\ell}] \\
\bar{x}_i &= r_i \oplus T[r_{i_1} \oplus \bar{x}_{i_1}, \dots, r_{i_\ell} \oplus \bar{x}_{i_\ell}] \\
&= \sum_{u_1,\dots,u_\ell \in \{0,1\}^\ell} (r_i \oplus T[r_{i_1} \oplus u_1, \dots, r_{i_\ell} \oplus u_\ell]) \left(\begin{cases} 1 & \text{if } (u_1, \dots, u_\ell) = (\bar{x}_{i_1}, \dots, \bar{x}_{i_\ell}) \\ 0 & \text{otherwise} \end{cases} \right)
\end{aligned}
$$

Results

- Semi-private offline-online HSS for bounded-integer programs $\sum_i C_i(x)C_i'(y)$ where $C_i \in \mathsf{VP}$, $C_i' \in \mathsf{RMS}$, x is semi-private, and y is private and offline.
- Sublinear communication garbled circuits:

	Size
Boolean (DCR)	$O\big(s/\log\log(s)\big) + \big(D+1\big) \cdot \mathrm{poly}(\lambda)$
Boolean (KDM)	$O\big(s/\log\log(s)\big) + \mathrm{poly}(\lambda)\big)$
Arithmetic (DCR)	$O\big((s/\log\log(s))(\lambda + \log B)\big) + (D+1) \cdot \mathrm{poly}(\lambda, \log B)$
Arithmetic (KDM)	$O\big((s/\log\log(s))(\lambda + \log B)\big) + \mathrm{poly}(\lambda, \log B)$

for a fan-in 2 circuit with s gates and depth d, defined either over bits or B-bounded values.