Authenticated Garbling From Simple Correlations

Eurocrypt 2022 Submission

Anonymous Submission

January 30, 2022· Presented by Hongrui Cui

* Some acknowledgments?

Introduction

- Authenticated Garbling with simple correlations: (s)VOLE, OLE, MT
- Goal: Malicious 2PC for Boolean circuits
- Techniques: PCG, LPZK, **Compression**, CDS
- Improvements (semi-honest as a baseline)

Protocol	Correlated randomness	Cost in garbled circuits	
		Dep. + online	Total
WRK [20]	OT	2.5	11.0
KRRW [14] v1	OT	1.5	7.75
KRRW [14] v2	OT	1	9.7
KRRW [14] with VOLE	$\mathcal{F}_{\mathsf{VOLE}}$	1	2.5
KRRW [14] with SPDZ	MT	1	7
KRRW [14] with SPDZ and certified VOLE	MT-$\mathcal{F}_{\mathsf{VOLE}} - \mathcal{F}_{\mathsf{subVOLE}}$	1	2.9
Ours, v1 (KRRW with $\mathcal{F}_{\mathsf{DAMT}}$ compiler to $\mathcal{F}_{\mathsf{pre}(\kappa)}$)	$\mathcal{F}_{\mathsf{DAMT}} - \mathcal{F}_{\mathsf{subVOLE}} - \mathcal{F}_{\mathsf{VOLE}}$	**1**	**1.31**
Ours, v2	$\mathcal{F}_{\mathsf{bVOLE}} - \mathcal{F}_{\mathsf{subVOLE}} - \mathcal{F}_{\mathsf{VOLE}}$	**1.47**	**2.25**
NISC in the single-execution setting			
Ours, v3	$\mathcal{F}_{\mathsf{OLE}}$	**7.47**	**7.47**
AMPR14 [1]	CRS	40	40

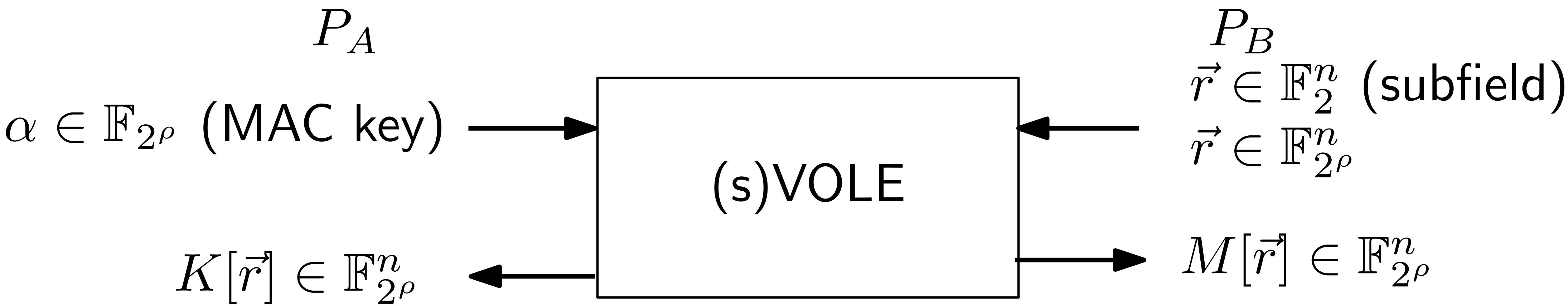
Main Contrinbutions In Details

$\mathcal{F}$-models	Online / Dep.	Total	Comp.
RO, **DAMT**, VOLE, sVOLE	$O(\kappa(\lvert\mathcal{I}\rvert + \lvert\mathcal{O}\rvert))$ / $(2\kappa+2)n$	$(2\kappa+4\rho+2)n$	$O(\kappa n)$
RO, VOLE, sVOLE, bVOLE	$O(\kappa(\lvert\mathcal{I}\rvert + \lvert\mathcal{O}\rvert))$ / $(2\kappa+3\rho)n$	$(5\rho+1)n+(2\kappa+3\rho)n$	$O(\kappa n)$
RO, OLE	$O(\kappa(\lvert\mathcal{I}\rvert + \lvert\mathcal{O}\rvert))$ / $(2\kappa+3\rho)n$	$(16\kappa+3\rho)n+o(1)$	$O(\kappa n)$

Ours, v1 (KRRW with $\mathcal{F}_{\mathsf{DAMT}}$ compiler to $\mathcal{F}_{\mathsf{pre}(\kappa)}$)	$\mathcal{F}_{\mathsf{DAMT}} - \mathcal{F}_{\mathsf{subVOLE}} - \mathcal{F}_{\mathsf{VOLE}}$	**1**	**1.31**
Ours, v2	$\mathcal{F}_{\mathsf{bVOLE}} - \mathcal{F}_{\mathsf{subVOLE}} - \mathcal{F}_{\mathsf{VOLE}}$	**1.47**	**2.25**
NISC in the single-execution setting			
Ours, v3	$\mathcal{F}_{\mathsf{OLE}}$	**7.47**	**7.47**

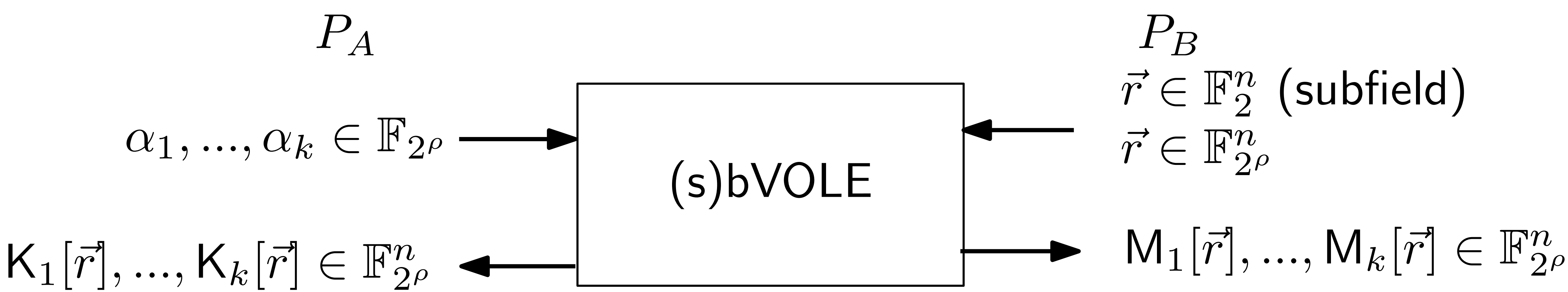
Preliminaries

- (subfield) Vector Oblivious Linear Evaluation



Constraint: $M[\vec{r}] = K[\vec{r}] + \alpha \cdot \vec{r}$

- (subfield) Block Vector Oblivious Linear Evaluation



Constraint: $\mathsf{M}_1[\vec{r}] = \mathsf{K}_1[\vec{r}] + \alpha_1 \cdot \vec{r}, \ldots, \mathsf{M}_k[\vec{r}] = \mathsf{K}_k[\vec{r}] + \alpha_k \cdot \vec{r}$

Preliminaries (Continued)

- Oblivious Linear Evaluations

P_A | | P_B
$\alpha \in \mathbb{F}_{2^\rho}$ $\rightarrow$ **OLE** $\leftarrow$ $b \in \mathbb{F}_{2^\rho}$

$c_A \in \mathbb{F}_{2^\rho}$ $\leftarrow$ **OLE** $\rightarrow$ $c_B \in \mathbb{F}_{2^\rho}$

Constraint: $c_A + c_B = \alpha \cdot b$

- Double Authenticated Multiplication Triples

P_A:

$\alpha \in \mathbb{F}_{2^\rho}$

$x_{A,1}, y_{A,1}, z_{A,1} \in \mathbb{F}_{2^\rho}^n$

$x_{A,2}, y_{A,2}, z_{A,2} \in \mathbb{F}_{2^\rho}^n$

$x_{A,3}, y_{A,3}, z_{A,3} \in \mathbb{F}_{2^\rho}^n$

$\leftarrow$ **DAMT** $\rightarrow$

P_B:

$\beta \in \mathbb{F}_{2^\rho}$

$x_{B,1}, y_{B,1}, z_{B,1} \in \mathbb{F}_{2^\rho}^n$

$x_{B,2}, y_{B,2}, z_{B,2} \in \mathbb{F}_{2^\rho}^n$

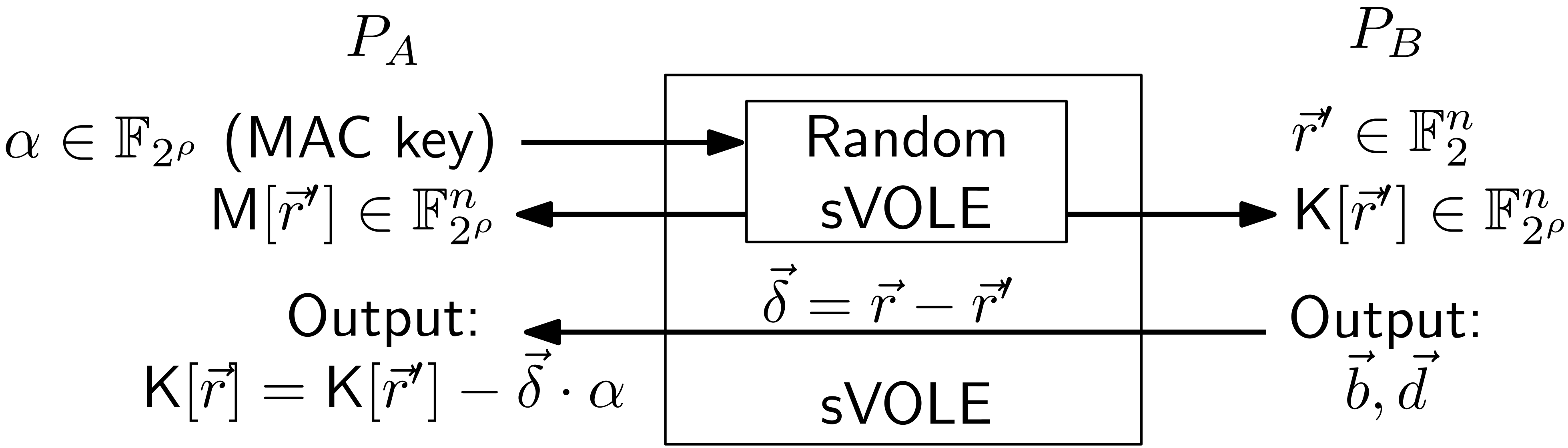
$x_{B,3}, y_{B,3}, z_{B,3} \in \mathbb{F}_{2^\rho}^n$

Constraint: $(x_{A,1} + x_{B,1}) \cdot (y_{A,1} + y_{B,1}) = (z_{A,1} + z_{B,1})$

$a_{A,2} + a_{B,2} = \alpha \cdot (a_{A,1} + a_{B,1})$, $a_{A,3} + a_{B,3} = \beta \cdot (a_{A,1} + a_{B,1})$

Preliminaries (Continued)

- State of the art for random VOLE: Wolverine (LPN)
- VOLE sender can prove low degree relation on inputs



- P_B prove deg-d poly on $\vec{r}$ using $O((\underbrace{n}_{\text{input}} + \underbrace{\rho d}_{\text{proof}}) \log p)$ bits

- State of the art for OLE: BCG+20 (Ring-LPN)
- Can realize DAMT over $\mathbb{F}_{2^\rho}$, not over $\mathbb{F}_2$

Starting Point: KRRW18 (Previous state of the art)

- Boolean circuit C: input $\mathcal{I}_A \cup \mathcal{I}_B$, intermediate gates $\mathcal{G}$, output $\mathcal{O}$
- $m = \#\text{Mult}$, $n = |\mathcal{I}| + m$
- Preprocessing + Online

P_A		P_B
$\Delta_A \in \mathbb{F}_{2^\kappa}$ $s_i, \mathsf{M}[s_i], \mathsf{K}[r_i]$ for $i \in [n]$ $\hat{s}_k, \mathsf{M}[\hat{s}_k], \mathsf{K}[\hat{r}_k]$ for $k \in [m]$	$\leftarrow$ $\boxed{\mathcal{F}_{\mathsf{pre}}^{C,\kappa,\rho}}$ $\rightarrow$	$\beta \in \mathbb{F}_{2^\rho}$ $r_i, \mathsf{M}[r_i], \mathsf{K}[s_i]$ for $i \in [n]$ $\hat{r}_k, \mathsf{M}[\hat{r}_k], \mathsf{K}[\hat{s}_k]$ for $k \in [m]$

- Wire mask $\lambda_i = (s_i + r_i)$
- Constraint1: $\forall$ $i, j \to \boxed{\wedge} \to k$ $\quad (\hat{s}_k + \hat{r}_k) = (s_i + r_i) \cdot (s_j + r_j)$
- Constraint2: $\mathsf{M}[\vec{s}] = \mathsf{K}[\vec{s}] + \beta \cdot \vec{s}, \mathsf{M}[\vec{\hat{s}}] = \mathsf{K}[\vec{\hat{c}}] + \beta \cdot \vec{\hat{s}}$ (over $\mathbb{F}_{2^\rho}$)
- Constraint3: $\mathsf{M}[\vec{r}] = \mathsf{K}[\vec{r}] + \Delta_A \cdot \vec{r}, \mathsf{M}[\vec{\hat{r}}] = \mathsf{K}[\vec{\hat{r}}] + \Delta_A \cdot \vec{\hat{r}}$ (over $\mathbb{F}_{2^\kappa}$)

Starting Point: KRRW18 (Online)

$\Delta_A \in \mathbb{F}_{2^\kappa}$

$s_i, \mathsf{M}[s_i], \mathsf{K}[r_i]$ for $i \in [n]$

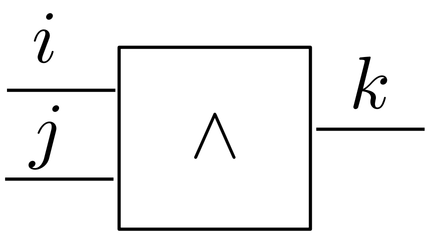
$\hat{s}_k, \mathsf{M}[\hat{s}_k], \mathsf{K}[\hat{r}_k]$ for $k \in [m]$

$\beta \in \mathbb{F}_{2^\rho}$

$r_i, \mathsf{M}[r_i], \mathsf{K}[s_i]$ for $i \in [n]$

$\hat{r}_k, \mathsf{M}[\hat{r}_k], \mathsf{K}[\hat{s}_k]$ for $k \in [m]$

P_A samples $L_{i,0} \leftarrow \mathbb{F}_{2^\kappa}$ for $i \in [n]$ and sets $L_{i,1} = L_{i,0} + \Delta_A$



$$G_0 = H(L_{i,0}) + H(L_{i,1}) + \underbrace{s_j \cdot \Delta_A + \mathsf{K}[r_j]}_{\lambda_j \cdot \Delta_A - \mathsf{M}[r_j]}$$

$$G_1 = H(L_{j,0}) + H(L_{j,1}) + \underbrace{s_i \cdot \Delta_A + \mathsf{K}[r_i] + L_{i,0}}_{\lambda_i \cdot \Delta_A + L_{i,0} - \mathsf{M}[r_i]}$$

$$L_{k,0} = H(L_{i,0}) + H(L_{j,0}) + \underbrace{(s_k + \hat{s}_k) \cdot \Delta_A + \mathsf{K}[r_k] + \mathsf{K}[\hat{r}_k]}_{(\lambda_i \cdot \lambda_j + \lambda_k) \cdot \Delta_A - \mathsf{M}[r_k] - \mathsf{M}[\hat{r}_k]}$$

$\mathsf{lsb}(L_{k,0})$ (Constraint: $\mathsf{lsb}(\Delta) = 1$)

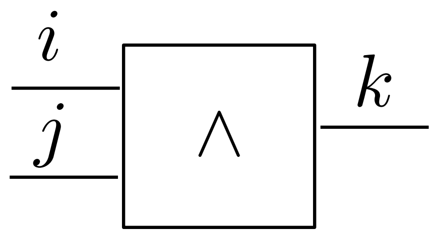
Starting Point: KRRW18 (Online)

Evaluate (GC):

$$
\begin{aligned}
L_{k,z_k} =& H(L_{i,z_i}) + H(L_{j,z_j}) + z_i \cdot (G_0 + \mathsf{M}[r_j]) \\
& + z_j \cdot (G_1 + \mathsf{M}[r_i] + L_{i,z_i}) + \mathsf{M}[r_k] + \mathsf{M}[\hat{r}_k] \\
=& H(L_{i,0}) + H(L_{j,0}) + (z_i\lambda_j + z_j\lambda_i + z_j z_i) \cdot \Delta_A + \mathsf{M}[r_k] + \mathsf{M}[\hat{r}_k] \\
=& L_{k,0} + ((z_i + \lambda_i) \cdot (z_j + \lambda_j) + \lambda_k)\Delta_A = L_{k,z_k}
\end{aligned}
$$

$$
z_k = \mathsf{lsb}(L_{k,z_k}) + \mathsf{lsb}(L_{k,0})
$$

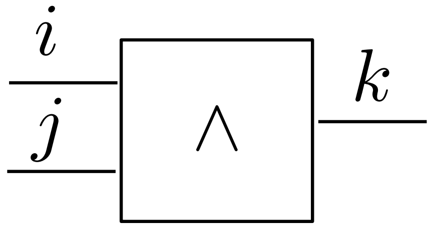
Starting Point: KRRW18 (Online)

- Evaluate (AuthGC)
- For each 

, checks $(z_i + \lambda_i) \cdot (z_j + \lambda_j) = (z_k + \lambda_k)$
- P_B sends all z_w to P_A

$$z_i z_j + z_i(s_j + r_j) + z_j(s_i + r_i) + (\hat{s}_k + \hat{r}_k) - z_k - (s_k + r_k) = 0$$
$$\underbrace{z_i z_j + z_i r_j + z_j r_i + \hat{r}_k + z_k + r_k}_{c_B} = \underbrace{z_i s_j + z_j s_i + \hat{s}_k + s_k}_{c_A}$$

Starting Point: KRRW18 (Online)

- Evaluate (AuthGC)
- For each 

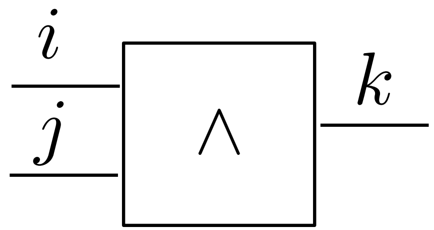
, checks $(z_i + \lambda_i) \cdot (z_j + \lambda_j) = (z_k + \lambda_k)$
- P_B sends all z_w to P_A

$$z_i z_j + z_i(s_j + r_j) + z_j(s_i + r_i) + (\hat{s}_k + \hat{r}_k) - z_k - (s_k + r_k) = 0$$

$$\underbrace{z_i z_j + z_i r_j + z_j r_i + \hat{r}_k + z_k + r_k}_{c_B} = \underbrace{z_i s_j + z_j s_i + \hat{s}_k + s_k}_{c_A}$$

- P_A sends $h = H(..., z_i \mathsf{M}[s_j] + z_j \mathsf{M}[s_i] + \mathsf{M}[\hat{s}_k] + \mathsf{M}[s_k], ...)$
- P_B checks $h = H(..., z_i \mathsf{K}[s_j] + z_j \mathsf{K}[s_i] + \mathsf{K}[\hat{s}_k] + \mathsf{K}[s_k] - c_A \cdot \beta, ...)$

Starting Point: KRRW18 (Online)

- Evaluate (AuthGC)
- For each 

, checks $(z_i + \lambda_i) \cdot (z_j + \lambda_j) = (z_k + \lambda_k)$
- P_B sends all z_w to P_A

$$z_i z_j + z_i(s_j + r_j) + z_j(s_i + r_i) + (\hat{s}_k + \hat{r}_k) - z_k - (s_k + r_k) = 0$$

$$\underbrace{z_i z_j + z_i r_j + z_j r_i + \hat{r}_k + z_k + r_k}_{c_B} = \underbrace{z_i s_j + z_j s_i + \hat{s}_k + s_k}_{c_A}$$

- P_A sends $h = H(..., z_i \mathsf{M}[s_j] + z_j \mathsf{M}[s_i] + \mathsf{M}[\hat{s}_k] + \mathsf{M}[s_k], ...)$
- P_B checks $h = H(..., z_i \mathsf{K}[s_j] + z_j \mathsf{K}[s_i] + \mathsf{K}[\hat{s}_k] + \mathsf{K}[s_k] - c_A \cdot \beta, ...)$

- Theorem 4 [KRRW]: Any boolean circuit C can be evaluated in the $\mathcal{F}_{\mathsf{pre}}^{C,\kappa,\rho}$-hybrid model using $O((2\kappa + 2)n)$ bits and 4 passes

1st Construction

$$\begin{tikzcd}
\boxed{\mathcal{F}_{\mathsf{DAMT}}} \arrow[r, "\text{Lemma 3}", "\text{Beaver-like}"'] & \boxed{\mathcal{F}_{\mathsf{pre}}^{\mathsf{PAnd},\rho,\rho}} \arrow[r, "\text{Lemma 2}", "\text{LPZK-like}"'] & \boxed{\mathcal{F}_{\mathsf{pre}}^{\mathsf{PAnd},\kappa,\rho}} \arrow[r, "\text{Lemma 1}", "\text{Beaver-like}"'] & \boxed{\mathcal{F}_{\mathsf{pre}}^{C,\kappa,\rho}} \arrow[d, "\text{Theorem 4}"'] \\
& & & \boxed{\mathcal{F}_C}
\end{tikzcd}$$

1st Construction

$$\begin{tikzcd}
\mathcal{F}_{\mathsf{DAMT}} \arrow[r, "\text{Lemma 3}", "\text{Beaver-like}"'] & \mathcal{F}_{\mathsf{pre}}^{\mathsf{PAnd},\rho,\rho} \arrow[r, "\text{Lemma 2}", "\text{LPZK-like}"'] & \mathcal{F}_{\mathsf{pre}}^{\mathsf{PAnd},\kappa,\rho} \arrow[r, "\text{Lemma 1}", "\text{Beaver-like}"'] & \mathcal{F}_{\mathsf{pre}}^{C,\kappa,\rho} \arrow[d, "\text{Theorem 4}"'] \\
 & & & \mathcal{F}_C
\end{tikzcd}$$

- Lemma 3: $\mathcal{F}_{\mathsf{DAMT}} \mapsto \mathcal{F}_{\mathsf{pre}}^{\mathsf{PAnd},\rho,\rho}$ with 4ρ bits per AND gate.

1st Construction

$$
\begin{tikzcd}[column sep=huge]
\mathcal{F}_{\mathsf{DAMT}} \arrow[r, "\text{Lemma 3}", "\text{Beaver-like}"'] & \mathcal{F}_{\mathsf{pre}}^{\mathsf{PAnd},\rho,\rho} \arrow[r, "\text{Lemma 2}", "\text{LPZK-like}"'] & \mathcal{F}_{\mathsf{pre}}^{\mathsf{PAnd},\kappa,\rho} \arrow[r, "\text{Lemma 1}", "\text{Beaver-like}"'] & \mathcal{F}_{\mathsf{pre}}^{C,\kappa,\rho} \arrow[d, "\text{Theorem 4}"'] \\
 & & & \mathcal{F}_C
\end{tikzcd}
$$

- Lemma 3: $\mathcal{F}_{\mathsf{DAMT}} \mapsto \mathcal{F}_{\mathsf{pre}}^{\mathsf{PAnd},\rho,\rho}$ with 4ρ bits per AND gate.

$$
\begin{tikzcd}
\begin{array}{c} P_A \\ x_{A,\ell}, y_{A,\ell}, z_{A,\ell} \\ \alpha \in \mathbb{F}_{2^\rho} \end{array} & \mathcal{F}_{\mathsf{DAMT}} \arrow[l] \arrow[r] & \begin{array}{c} P_B \\ x_{B,\ell}, y_{B,\ell}, z_{B,\ell} \\ \beta \in \mathbb{F}_{2^\rho} \end{array} \\
s_i, \mathsf{M}[s_i], \mathsf{K}[r_i] & \mathcal{F}_{\mathsf{sVOLE}} \arrow[l] \arrow[r] & r_i, \mathsf{M}[r_i], \mathsf{K}[s_i]
\end{tikzcd}
$$

1st Construction

$$\boxed{\mathcal{F}_{\mathsf{DAMT}}} \xrightarrow[\text{Beaver-like}]{\text{Lemma 3}} \boxed{\mathcal{F}^{\mathsf{PAnd},\rho,\rho}_{\mathsf{pre}}} \xrightarrow[\text{LPZK-like}]{\text{Lemma 2}} \boxed{\mathcal{F}^{\mathsf{PAnd},\kappa,\rho}_{\mathsf{pre}}} \xrightarrow[\text{Beaver-like}]{\text{Lemma 1}} \boxed{\mathcal{F}^{C,\kappa,\rho}_{\mathsf{pre}}} \xrightarrow{\text{Theorem 4}} \boxed{\mathcal{F}_C}$$

- Lemma 3: $\mathcal{F}_{\mathsf{DAMT}} \mapsto \mathcal{F}^{\mathsf{PAnd},\rho,\rho}_{\mathsf{pre}}$ with 4ρ bits per AND gate.

P_A		P_B
$x_{A,\ell}, y_{A,\ell}, z_{A,\ell}$ $\alpha \in \mathbb{F}_{2^\rho}$	$\longleftarrow \boxed{\mathcal{F}_{\mathsf{DAMT}}} \longrightarrow$	$x_{B,\ell}, y_{B,\ell}, z_{B,\ell}$ $\beta \in \mathbb{F}_{2^\rho}$
$s_i, \mathsf{M}[s_i], \mathsf{K}[r_i]$	$\longleftarrow \boxed{\mathcal{F}_{\mathsf{sVOLE}}} \longrightarrow$	$r_i, \mathsf{M}[r_i], \mathsf{K}[s_i]$
	$\xleftarrow{\mathsf{Open}(x_{B,1} - r_i,\ y_{B,1} - r_j)}$	
	$\xrightarrow{\mathsf{Open}(x_{A,1} - s_i,\ x_{A,1} - s_j)}$	

$$\begin{aligned} \hat{s}_k + \hat{r}_k &= (s_i + r_i) \cdot (s_j + r_j) \\ &= ef + e(y_{A,1} + y_{B,1}) + f(x_{A,1} + x_{B,1}) + z_{A,1} + z_{B,1} \end{aligned}$$

1st Construction

- $\mathsf{M}[\hat{r}_k], \mathsf{M}[\hat{s}_k], \mathsf{K}[\hat{r}_k], \mathsf{K}[\hat{s}_k]$ can also be linearly computed.
- Final step is to reduce $\hat{a}_k, \hat{b}_k$ to $\mathbb{F}_2$

$$\hat{s}_k + \hat{r}_k \in \{0, 1\}$$
$$\mathsf{lsb}(\hat{s}_k) + \hat{s}_k = \mathsf{lsb}(\hat{r}_k) + \hat{r}_k$$

1st Construction

- $\mathsf{M}[\hat{r}_k], \mathsf{M}[\hat{s}_k], \mathsf{K}[\hat{r}_k], \mathsf{K}[\hat{s}_k]$ can also be linearly computed.
- Final step is to reduce $\hat{a}_k, \hat{b}_k$ to $\mathbb{F}_2$

$$\hat{s}_k + \hat{r}_k \in \{0, 1\}$$
$$\mathsf{lsb}(\hat{s}_k) + \hat{s}_k = \mathsf{lsb}(\hat{r}_k) + \hat{r}_k$$

$$\mathsf{K}[\hat{s}_k] = \mathsf{M}[\hat{s}_k] + \hat{s}_k \cdot \beta$$
$$\mathsf{K}[\hat{s}_k] + (\hat{s}_k + \mathsf{lsb}(\hat{s}_k)) \cdot \beta = \mathsf{M}[\hat{s}_k] + (\hat{s}_k + \mathsf{lsb}(\hat{s}_k) + \mathsf{lsb}(\hat{s}_k)) \cdot \beta$$
$$\mathsf{K}[\hat{s}_k] + (\hat{r}_k + \mathsf{lsb}(\hat{r}_k)) \cdot \beta = \mathsf{M}[\hat{s}_k] + \mathsf{lsb}(\hat{s}_k) \cdot \beta$$

1st Construction

- Lemma 2: $\mathcal{F}_{\text{pre}}^{\text{PAnd},\rho,\rho} \mapsto \mathcal{F}_{\text{pre}}^{\text{PAnd},\kappa,\rho}$ with 2 bits per AND gate.

Mac Key	α	Δ_A
Wire Mask	$\mathsf{M}[r] = r \cdot \alpha + \mathsf{K}[r]$	$\mathsf{M}[r'] = r' \cdot \Delta_A + \mathsf{K}[r']$
Deg-2 Mask	$\mathsf{M}[\hat{r}] = \hat{r} \cdot \alpha + \mathsf{K}[\hat{r}]$	$\mathsf{M}[\hat{r}'] = \hat{r}' \cdot \Delta_A + \mathsf{K}[\hat{r}']$

Then use LPZK-like technique to check $b = b', \hat{b} = \hat{b}'$

- Lemma 1: $\mathcal{F}_{\text{pre}}^{\text{PAnd},\kappa,\rho} \mapsto \mathcal{F}_{\text{pre}}^{C,\kappa,\rho}$ with 4 bits per gate.

- Generate $\mathsf{M}[\vec{r}] = \Delta_A \cdot \vec{r} + \mathsf{K}[\vec{r}], \mathsf{M}[\vec{s}] = \beta \cdot \vec{s} + \mathsf{K}[\vec{s}]$ using sVOLE
- Open$(r_i - r_i', r_j - r_j', s_i - s_i', s_j - s_j')$

2nd Construction: block VOLE and compressed randomness

- High-level idea: generate triples by **reusing** input of VOLE and **hiding** z-values using non-interactive authentication/mac opening

$$\boxed{\mathcal{F}_{\mathsf{bVOLE}}} \xrightarrow[\text{Input reuse}]{\text{Lemma 5}} \boxed{\mathcal{F}_{\mathsf{cp}}^{C,\rho,\rho}} \xrightarrow[\text{LPZK}]{\text{Lemma 1*}} \boxed{\mathcal{F}_{\mathsf{cp}}^{C,\kappa,\rho}} \xrightarrow[\text{Compression}]{\text{Lemma 4}} \boxed{\mathcal{F}_{C}}$$

2nd Construction: block VOLE and compressed randomness

- High-level idea: generate triples by **reusing** input of VOLE and **hiding** z-values using non-interactive authentication/mac opening

$$\boxed{\mathcal{F}_{\text{bVOLE}}} \xrightarrow[\text{Input reuse}]{\text{Lemma 5}} \boxed{\mathcal{F}_{\text{cp}}^{C,\rho,\rho}} \xrightarrow[\text{LPZK}]{\text{Lemma 1*}} \boxed{\mathcal{F}_{\text{cp}}^{C,\kappa,\rho}} \xrightarrow[\text{Compression}]{\text{Lemma 4}} \boxed{\mathcal{F}_C}$$

- Lemma 5: From bVOLE to $\mathcal{F}_{\text{cp}}^{C,\rho,\rho}$: $5\rho + 2 + o(1)$ bits per gate

P_A $\longleftarrow$ $\boxed{\mathcal{F}_{\text{cp}}^{C,\rho,\rho}}$ $\longrightarrow$ P_B

P_A:

Mac Key: $\alpha \in \mathbb{F}_{2^\rho}$

$s_i, \mathsf{M}[s_i], \mathsf{K}[r_i]$ for $i \in \mathcal{I}$

$s_i, \mathsf{M}[s_i], \mathsf{K}[r_i']$ for $i \in [m]$

$\hat{s}_k, \mathsf{M}[\hat{s}_k], \mathsf{K}[\hat{r}_k]$ for $k \in [m]$

P_B:

Mac Key: $\beta \in \mathbb{F}_{2^\rho}$

$r_i, \mathsf{M}[r_i], \mathsf{K}[s_i]$ for $i \in \mathcal{I}$

$r_i', \mathsf{M}[r_i'], \mathsf{K}[s_i]$ for $i \in [m]$

$\hat{r}_k, \mathsf{M}[\hat{r}_k], \mathsf{K}[\hat{s}_k]$ for $k \in [m]$

$$L = \rho \cdot \log(8n/\rho)$$

$$\vec{b'} = M_H \cdot \vec{\mathfrak{b}}, \vec{d'} = M_H \cdot \vec{\mathfrak{d}}, \vec{w'} = M_H \cdot \vec{\mathfrak{w}}$$

2nd Construction: block VOLE and compressed randomness

- High-level idea: generate triples by **reusing** input of VOLE and **hiding** z-values using non-interactive authentication/mac opening

$$\begin{tikzcd} \mathcal{F}_{\mathsf{bVOLE}} \arrow[r, "\text{Lemma 5}", "\text{Input reuse}"'] & \mathcal{F}_{\mathsf{cp}}^{C,\rho,\rho} \arrow[r, "\text{Lemma 1*}", "\text{LPZK}"'] & \mathcal{F}_{\mathsf{cp}}^{C,\kappa,\rho} \arrow[r, "\text{Lemma 4}", "\text{Compression}"'] & \mathcal{F}_C \end{tikzcd}$$

- Lemma 5: From bVOLE to $\mathcal{F}_{\mathsf{cp}}^{C,\rho,\rho}$: $5\rho + 2 + o(1)$ bits per gate

$$\begin{tikzcd} P_A & \mathcal{F}_{\mathsf{cp}}^{C,\rho,\rho} \arrow[l] \arrow[r] & P_B \end{tikzcd}$$

P_A	P_B
Mac Key: $\alpha \in \mathbb{F}_{2^\rho}$	Mac Key: $\beta \in \mathbb{F}_{2^\rho}$
$s_i, \mathsf{M}[s_i], \mathsf{K}[r_i]$ for $i \in \mathcal{I}$	$r_i, \mathsf{M}[r_i], \mathsf{K}[s_i]$ for $i \in \mathcal{I}$
$s_i, \mathsf{M}[s_i], \mathsf{K}[r'_i]$ for $i \in [m]$	$r'_i, \mathsf{M}[r'_i], \mathsf{K}[s_i]$ for $i \in [m]$
$\hat{s}_k, \mathsf{M}[\hat{s}_k], \mathsf{K}[\hat{r}_k]$ for $k \in [m]$	$\hat{r}_k, \mathsf{M}[\hat{r}_k], \mathsf{K}[\hat{s}_k]$ for $k \in [m]$

$$L = \rho \cdot \log(8n/\rho)$$

$$\vec{b'} = M_H \cdot \vec{\mathfrak{b}}, \vec{d'} = M_H \cdot \vec{\mathfrak{d}}, \vec{w'} = M_H \cdot \vec{\mathfrak{w}}$$

- Non-Linear 1: $(\hat{s}_k + \hat{s}_k) = (s_i + r_i) \cdot (s_j + r_j)$
- Non-Linear 2: $\mathsf{M}[\hat{r}_k] = \mathsf{K}[\hat{r}_k] + \alpha \cdot \hat{r}_k$, $\mathsf{M}[\hat{s}_k] = \mathsf{K}[\hat{s}_k] + \beta \cdot \hat{s}_k$

2nd Construction: block VOLE and compressed randomness

P_A

$\alpha, \mathsf{K}[r_i]$

$\mathsf{K}[\mathfrak{r}]$

$\mathsf{K}[\vec{r'}] = M_H \cdot \mathsf{K}[\mathfrak{r}]$

$\longleftarrow$ $\boxed{\mathcal{F}_{\mathsf{sVOLE}}}$ $\longrightarrow$

Extend $(r_i r_j,$
$\beta \cdot \mathfrak{r} + \gamma, \beta + \gamma, \gamma)$ $\longleftarrow$

P_B

$r_i, \mathsf{M}[r_i], i \in \mathcal{I}$

$\mathfrak{r}, \mathsf{M}[\mathfrak{r}]$

$\vec{r'} = M_H \cdot \mathfrak{r}$

$\mathsf{M}[\vec{r'}] = M_H \cdot \mathsf{M}[\mathfrak{r}]$

2nd Construction: block VOLE and compressed randomness

P_A		P_B
$\alpha, \mathsf{K}[r_i]$ $\mathsf{K}[\mathfrak{r}]$	$\longleftarrow \boxed{\mathcal{F}_{\mathsf{sVOLE}}} \longrightarrow$	$r_i, \mathsf{M}[r_i], i \in \mathcal{I}$ $\mathfrak{r}, \mathsf{M}[\mathfrak{r}]$
$\mathsf{K}[\vec{r'}] = M_H \cdot \mathsf{K}[\mathfrak{r}]$	$\xleftarrow{\text{Extend } (r_i r_j,}$ $\beta \cdot \mathfrak{r} + \gamma, \beta + \gamma, \gamma)$	$\vec{r'} = M_H \cdot \mathfrak{r}$ $\mathsf{M}[\vec{r'}] = M_H \cdot \mathsf{M}[\mathfrak{r}]$
$\vec{s}, \{s_i s_j\}, \vec{\hat{s}}$	$\longrightarrow \boxed{\mathcal{F}_{\mathsf{bsVOLE}}} \longleftarrow$	$(\beta \cdot \mathfrak{r} + \gamma, \beta + \gamma, \gamma)$
$\alpha \cdot \vec{s}, \{\alpha \cdot s_i \cdot s_j\},$ $\alpha \cdot \vec{\hat{s}}, \{\hat{s}_{k,2}\}, \alpha$	$\longrightarrow \boxed{\mathcal{F}_{\mathsf{bVOLE}}} \longleftarrow$	$(\beta \cdot \mathfrak{r} + \gamma, \beta + \gamma, \gamma)$

$$\mathsf{M}[\hat{s}_k] = \hat{s}_k \beta + \mathsf{K}[\hat{s}_k] \quad \mathsf{M}[s_{k,2}] = \hat{s}_{k,2}\beta + \mathsf{K}[s_{k,2}] \quad \mathsf{M}[s_{k,3}] = \hat{s}_k \alpha\beta + \mathsf{K}[s_{k,3}]$$
$$\mathsf{M}[s_{k,4}] = (s_i s_j + s_i r_j + r_i s_j)\beta + \mathsf{K}[s_{k,4}] \quad \mathsf{M}[s_{k,5}] = (s_i s_j + s_i r_j + r_i s_j)\alpha\beta + \mathsf{K}[s_{k,5}]$$

2nd Construction: block VOLE and compressed randomness

P_A | P_B

$\alpha, \mathsf{K}[r_i]$
$\mathsf{K}[\mathfrak{r}]$

$\longleftarrow \mathcal{F}_{\mathsf{sVOLE}} \longrightarrow$

$r_i, \mathsf{M}[r_i], i \in \mathcal{I}$
$\mathfrak{r}, \mathsf{M}[\mathfrak{r}]$

$\vec{r'} = M_H \cdot \mathfrak{r}$
$\mathsf{M}[\vec{r'}] = M_H \cdot \mathsf{M}[\mathfrak{r}]$

$\mathsf{K}[\vec{r'}] = M_H \cdot \mathsf{K}[\mathfrak{r}]$

$\xleftarrow[\beta \cdot \mathfrak{r} + \gamma, \beta + \gamma, \gamma)]{\text{Extend } (r_i r_j,}$

$\vec{s}, \{s_i s_j\}, \vec{\hat{s}} \longrightarrow \mathcal{F}_{\mathsf{bsVOLE}} \longleftarrow (\beta \cdot \mathfrak{r} + \gamma, \beta + \gamma, \gamma)$

$\alpha \cdot \vec{s}, \{\alpha \cdot s_i \cdot s_j\},$
$\alpha \cdot \vec{\hat{s}}, \{\hat{s}_{k,2}\}, \alpha$

$\longrightarrow \mathcal{F}_{\mathsf{bVOLE}} \longleftarrow (\beta \cdot \mathfrak{r} + \gamma, \beta + \gamma, \gamma)$

$\mathsf{M}[\hat{s}_k] = \hat{s}_k \beta + \mathsf{K}[\hat{s}_k] \quad \mathsf{M}[s_{k,2}] = \hat{s}_{k,2}\beta + \mathsf{K}[s_{k,2}] \quad \mathsf{M}[s_{k,3}] = \hat{s}_k \alpha\beta + \mathsf{K}[s_{k,3}]$

$\mathsf{M}[s_{k,4}] = (s_i s_j + s_i r_j + r_i s_j)\beta + \mathsf{K}[s_{k,4}] \quad \mathsf{M}[s_{k,5}] = (s_i s_j + s_i r_j + r_i s_j)\alpha\beta + \mathsf{K}[s_{k,5}]$

$\mathsf{K}[\hat{r}_k] = \hat{s}_{k,2} + \mathsf{K}[r_{i,j}]$

$\xrightarrow[m_{k,2} = \mathsf{M}[s_{k,2} + s_{k,3} + s_{k,5}]]{m_{k,1} = \mathsf{M}[\hat{s}_k + s_{k,4}]}$

$\hat{r}_k = (\mathsf{K}[\hat{s}_k + s_{k,4}] + m_{k,1}) \cdot \beta^{-1}$
$\mathsf{M}[\hat{r}_k] = (\mathsf{K}[s_{k,2} + s_{k,3} + s_{k,5}] + m_{k,2}) \cdot \beta^{-1} + \mathsf{M}[r_{i,j}]$

2nd Construction: An Optimization

P_A

$\alpha, \mathsf{K}[r_i]$
$\mathsf{K}[\mathfrak{r}]$

$\mathsf{K}[\vec{r'}] = M_H \cdot \mathsf{K}[\mathfrak{r}]$

$\longleftarrow \boxed{\mathcal{F}_{\mathsf{sVOLE}}} \longrightarrow$

$\xleftarrow{\text{Extend } (r_i r_j)}$

P_B

$r_i, \mathsf{M}[r_i], i \in \mathcal{I}$
$\mathfrak{r}, \mathsf{M}[\mathfrak{r}]$
$\vec{r'} = M_H \cdot \mathfrak{r}$
$\mathsf{M}[\vec{r'}] = M_H \cdot \mathsf{M}[\mathfrak{r}]$

2nd Construction: An Optimization

P_A		P_B
$\alpha, \mathsf{K}[r_i]$ $\mathsf{K}[\mathfrak{r}]$	$\longleftarrow$ $\mathcal{F}_{\mathsf{sVOLE}}$ $\longrightarrow$	$r_i, \mathsf{M}[r_i], i \in \mathcal{I}$ $\mathfrak{r}, \mathsf{M}[\mathfrak{r}]$
$\mathsf{K}[\vec{r'}] = M_H \cdot \mathsf{K}[\mathfrak{r}]$	Extend $(r_i r_j)$ $\longleftarrow$	$\vec{r'} = M_H \cdot \mathfrak{r}$ $\mathsf{M}[\vec{r'}] = M_H \cdot \mathsf{M}[\mathfrak{r}]$
$\vec{s}, \{s_i s_j\}$	$\longrightarrow$ $\mathcal{F}_{\mathsf{bVOLE}}$ $\longleftarrow$	$\mathsf{M}[\mathfrak{r}], \mathfrak{r} + \gamma, \beta \cdot \mathfrak{r} + \gamma,$ $\beta + \gamma, \gamma$

- $\hat{s}_k + \hat{r}_k = (s_i + r_i) \cdot (s_j + r_j) = \underbrace{s_i s_j + s^{\times}_{i,j} + s^{\times}_{j,i}}_{\hat{s}_k} + \underbrace{r_i r_j + r^{\times}_{i,j} + r^{\times}_{j,i}}_{\hat{r}_k}$
- $\mathsf{M}[\hat{s}_k] + \mathsf{K}[\hat{s}_k] = \hat{s}_k \cdot \beta = s_i s_j \beta + s_i r_j \beta + s_j r_i \beta - r^{\times}_{i,j} \beta - r^{\times}_{j,i} \beta$
- $\mathsf{M}[\hat{r}_k] + \mathsf{K}[\hat{r}_k] = \hat{r}_k \cdot \alpha = r_i r_j \alpha + s_i r_j \alpha + s_j r_i \alpha - s^{\times}_{i,j} \alpha - s^{\times}_{j,i} \alpha$

2nd Construction: block VOLE and compressed randomness

- Lemma 4: Auth-GC from $\mathcal{F}_{\mathsf{cp}}^{C,\kappa,\rho}$ with $O((2\kappa + 3\rho)n)$ communication

2nd Construction: block VOLE and compressed randomness

- Lemma 4: Auth-GC from $\mathcal{F}_{\mathsf{cp}}^{C,\kappa,\rho}$ with $O((2\kappa+3\rho)n)$ communication

$\Delta_A \in \mathbb{F}_{2^\kappa}$

$s_i, \mathsf{M}[s_i], \mathsf{K}[r_i],\ i \in [n]$

$\hat{s}_k, \mathsf{M}[\hat{s}_k], \mathsf{K}[\hat{r}_k],\ k \in [m]$

$\beta \in \mathbb{F}_{2^\rho}$

$r_i, \mathsf{M}[r_i], \mathsf{K}[s_i],\ i \in [n]$

$\hat{r}_k, \mathsf{M}[\hat{r}_k], \mathsf{K}[\hat{s}_k],\ k \in [m]$

P_A samples $L_{i,0} \leftarrow \mathbb{F}_{2^\kappa}$ for $i \in [n]$ and sets $L_{i,1} = L_{i,0} + \Delta_A$

2nd Construction: block VOLE and compressed randomness

- Lemma 4: Auth-GC from $\mathcal{F}_{\mathsf{cp}}^{C,\kappa,\rho}$ with $O((2\kappa+3\rho)n)$ communication

$\Delta_A \in \mathbb{F}_{2^\kappa}$

$s_i, \mathsf{M}[s_i], \mathsf{K}[r_i],\ i \in [n]$

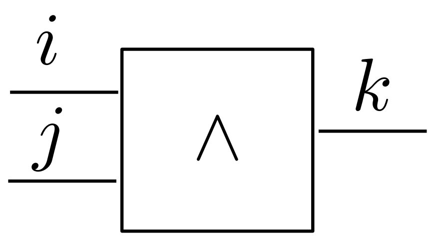
$\hat{s}_k, \mathsf{M}[\hat{s}_k], \mathsf{K}[\hat{r}_k],\ k \in [m]$

$\beta \in \mathbb{F}_{2^\rho}$

$r_i, \mathsf{M}[r_i], \mathsf{K}[s_i],\ i \in [n]$

$\hat{r}_k, \mathsf{M}[\hat{r}_k], \mathsf{K}[\hat{s}_k],\ k \in [m]$

P_A samples $L_{i,0} \leftarrow \mathbb{F}_{2^\kappa}$ for $i \in [n]$ and sets $L_{i,1} = L_{i,0} + \Delta_A$



$$G_0 = H(L_{i,0}) + H(L_{i,1}) + s_j \cdot \Delta_A + \mathsf{K}[r_j]$$
$$G_1 = H(L_{j,0}) + H(L_{j,1}) + s_i \cdot \Delta_A + \mathsf{K}[r_i] + L_{i,0}$$
$$L_{k,0} = H(L_{i,0}) + H(L_{j,0}) + (s_k + \hat{s}_k) \cdot \Delta_A + \mathsf{K}[r_k] + \mathsf{K}[\hat{r}_k]$$
$$G'_{k,0} = H'(L_{i,0}) + H'(L_{j,0}) + \mathsf{M}[s_k] + \mathsf{M}[\hat{s}_k]$$
$$G'_{k,1} = H'(L_{i,0}) + H'(L_{i,1}) + \mathsf{M}[s_j]$$
$$G'_{k,2} = H'(L_{j,0}) + H'(L_{j,1}) + \mathsf{M}[s_i]$$

2nd Construction: block VOLE and compressed randomness

- Lemma 4: Auth-GC from $\mathcal{F}_{\mathsf{cp}}^{C,\kappa,\rho}$ with $O((2\kappa+3\rho)n)$ communication

$\Delta_A \in \mathbb{F}_{2^\kappa}$

$s_i, \mathsf{M}[s_i], \mathsf{K}[r_i],\ i \in [n]$

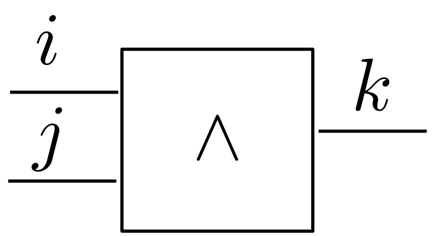
$\hat{s}_k, \mathsf{M}[\hat{s}_k], \mathsf{K}[\hat{r}_k],\ k \in [m]$

$\beta \in \mathbb{F}_{2^\rho}$

$r_i, \mathsf{M}[r_i], \mathsf{K}[s_i],\ i \in [n]$

$\hat{r}_k, \mathsf{M}[\hat{r}_k], \mathsf{K}[\hat{s}_k],\ k \in [m]$

P_A samples $L_{i,0} \leftarrow \mathbb{F}_{2^\kappa}$ for $i \in [n]$ and sets $L_{i,1} = L_{i,0} + \Delta_A$



$$
\begin{aligned}
G_0 &= H(L_{i,0}) + H(L_{i,1}) + s_j \cdot \Delta_A + \mathsf{K}[r_j] \\
G_1 &= H(L_{j,0}) + H(L_{j,1}) + s_i \cdot \Delta_A + \mathsf{K}[r_i] + L_{i,0} \\
L_{k,0} &= H(L_{i,0}) + H(L_{j,0}) + (s_k + \hat{s}_k) \cdot \Delta_A + \mathsf{K}[r_k] + \mathsf{K}[\hat{r}_k] \\
G'_{k,0} &= H'(L_{i,0}) + H'(L_{j,0}) + \mathsf{M}[s_k] + \mathsf{M}[\hat{s}_k] \\
G'_{k,1} &= H'(L_{i,0}) + H'(L_{i,1}) + \mathsf{M}[s_j] \\
G'_{k,2} &= H'(L_{j,0}) + H'(L_{j,1}) + \mathsf{M}[s_i]
\end{aligned}
$$

- $z_k = z_i z_j + z_i r_j + z_j r_i + (H'(L_{i,z_i}) + z_i G'_{k,1} + H'(L_{j,z_j}) + z_j G'_{k,2} + G'_{k,0} + z_i \mathsf{M}[r_j] + z_j \mathsf{M}[r_i] + \mathsf{M}[r_k] + \mathsf{M}[\hat{r}_k]) \cdot \beta^{-1}$
- $L_{k,z_k} = H(L_{i,z_i}) + z_i(G_0 + \mathsf{M}[r_j]) + H(L_{j,z_j}) + z_j(G_1 + \mathsf{M}[r_i] + L_{i,z_i})$

2nd Construction: block VOLE and compressed randomness

- Protocol is only one-pass, r_i is essentially hidden from P_A
- Only attack possibility: Selective-Failure Attack
- It is sufficient to use a $(\rho - 1, L)$-independent set as rows of M_H

$$b = M_H \cdot \mathfrak{b}$$

- $z_k = z_i z_j + z_i r_j + z_j r_i + (H'(L_{i,z_i}) + z_i G'_{k,1} + H'(L_{j,z_j}) + z_j G'_{k,2} + G'_{k,0} + z_i \mathsf{M}[r_j] + z_j \mathsf{M}[r_i] + \mathsf{M}[r_k] + \mathsf{M}[\hat{r}_k]) \cdot \beta^{-1}$
- $L_{k,z_k} = H(L_{i,z_i}) + z_i(G_0 + \mathsf{M}[r_j]) + H(L_{j,z_j}) + z_j(G_1 + \mathsf{M}[r_i] + L_{i,z_i})$
- Need to corrupt more than ρ gates to utilize linear dependency — Success probability $< 2^{-\rho}$

3rd Construction: NISC in $\mathcal{F}_{\mathsf{OLE}}$-hybrid model

- Dubious "Non-Interactive Secure Computation"

$$\mathcal{F}_{\mathsf{pOLE}} \xrightarrow[\text{CDS}]{\text{Lemma 6}} \mathcal{F}^{C,\rho,\rho}_{\mathsf{pre-wbc}} \xrightarrow[\text{Attachment}]{\text{Theorem 3}} \mathcal{F}_{C}$$

3rd Construction: NISC in $\mathcal{F}_{\mathsf{OLE}}$-hybrid model

- Dubious "Non-Interactive Secure Computation"

$$\begin{tikzcd}
\boxed{\mathcal{F}_{\mathsf{pOLE}}} \arrow[r, "\text{Lemma 6}", "\text{CDS}"'] & \boxed{\mathcal{F}^{C,\rho,\rho}_{\mathsf{pre-wbc}}} \arrow[r, "\text{Theorem 3}", "\text{Attachment}"'] & \boxed{\mathcal{F}_C}
\end{tikzcd}$$

- Theorem 3: assuming Lemma 6 (NISC $\mathcal{F}_{\mathsf{pOLE}} \mapsto \mathcal{F}^{C,\rho,\rho}_{\mathsf{pre-wbc}}$) exists, we can attach Lemma 4 ($\mathcal{F}^{C,\kappa,\rho}_{\mathsf{cp}} \mapsto \mathcal{F}_C$) messages to (m_B, m_A).

$$\begin{array}{ccc}
P_A & & P_B \\
 & \xleftarrow{\quad m_B \quad} & \\
 & \xrightarrow[G,\, G']{m_A,\, s_{\mathcal{I}},\, s_{\mathcal{O}}} &
\end{array}$$

- $s_{\mathcal{I}_A}, r_{\mathcal{I}_B}$ implicitly set to 0

3rd Construction: NISC in $\mathcal{F}_{\mathsf{OLE}}$-hybrid model

- Dubious "Non-Interactive Secure Computation"

$$\boxed{\mathcal{F}_{\mathsf{pOLE}}} \xrightarrow[\text{CDS}]{\text{Lemma 6}} \boxed{\mathcal{F}^{C,\rho,\rho}_{\mathsf{pre-wbc}}} \xrightarrow[\text{Attachment}]{\text{Theorem 3}} \boxed{\mathcal{F}_{C}}$$

- Lemma 6: **NISC** $\mathcal{F}_{\mathsf{pOLE}} \mapsto \mathcal{F}^{C,\rho,\rho}_{\mathsf{pre-wbc}}$.

3rd Construction: NISC in $\mathcal{F}_{\text{OLE}}$-hybrid model

- Dubious "Non-Interactive Secure Computation"

$$\boxed{\mathcal{F}_{\text{pOLE}}} \xrightarrow[\text{CDS}]{\text{Lemma 6}} \boxed{\mathcal{F}^{C,\rho,\rho}_{\text{pre}-\text{wbc}}} \xrightarrow[\text{Attachment}]{\text{Theorem 3}} \boxed{\mathcal{F}_C}$$

- Lemma 6: **NISC** $\mathcal{F}_{\text{pOLE}} \mapsto \mathcal{F}^{C,\rho,\rho}_{\text{pre}-\text{wbc}}$.

Primary Input Phase

$$\begin{array}{c} \Delta_A, s, \Delta_A s, \{s_i s_j\}, \\ \{\Delta_A s_i s_j\}, \hat{s}, \Delta_A \hat{s}, s_{i,2} \end{array} \longrightarrow \boxed{\mathcal{F}_{\text{pOLE}}} \longleftarrow \begin{array}{c} r+\gamma, r\beta+\gamma, \\ \{r_i r_j \beta + \gamma\}, \beta, \gamma \end{array}$$

3rd Construction: NISC in $\mathcal{F}_{\mathsf{OLE}}$-hybrid model

- Dubious "Non-Interactive Secure Computation"

$$\boxed{\mathcal{F}_{\mathsf{pOLE}}} \xrightarrow[\text{CDS}]{\text{Lemma 6}} \boxed{\mathcal{F}^{C,\rho,\rho}_{\mathsf{pre-wbc}}} \xrightarrow[\text{Attachment}]{\text{Theorem 3}} \boxed{\mathcal{F}_{C}}$$

- Lemma 6: **NISC** $\mathcal{F}_{\mathsf{pOLE}} \mapsto \mathcal{F}^{C,\rho,\rho}_{\mathsf{pre-wbc}}$.

Primary Input Phase