Collusion-Resistant Privacy-Preserving Data Mining

Bin Yang[1] Hiroshi Nakagawa[2] Issei Sato[1] Jun Sakuma[3]

[1]Graduate School of Information Science and Technology,
The University of Tokyo

[2]Information Technology Center, The University of Tokyo

[3]Department of Computer Science, University of Tsukuba

The 16th ACM SIGKDD Conference, July 25-28, 2010

Outline

Privacy-Preserving Data Mining (PPDM)

Bank 1

ID	Salary
1	XXX
:	:
10	XXX
Sum	100

Bank 2

ID	Salary
1	XXX
:	:
15	XXX
Sum	200

Bank 3

ID	Salary
1	XXX
:	:
5	XXX
Sum	100

Privacy-Preserving Data Mining (PPDM)

Bank 1

ID	Salary
1	XXX
:	:
10	XXX
Sum	100

$(100, 10)$

Bank 2

ID	Salary
1	XXX
:	:
15	XXX
Sum	200

$(200, 15)$

Bank 3

ID	Salary
1	XXX
:	:
5	XXX
Sum	100

$(100, 5)$

Privacy-Preserving Data Mining (PPDM)

Bank 1

ID	Salary
1	XXX
:	:
10	XXX
Sum	100

Bank 2

ID	Salary
1	XXX
:	:
15	XXX
Sum	200

Bank 3

ID	Salary
1	XXX
:	:
5	XXX
Sum	100

$(100, 10)$ $(200, 15)$ $(100, 5)$

$$\textbf{Average Salary} = \frac{100 + 200 + 100}{10 + 15 + 5}$$

Related Works

Works	Methods	Party	Hori./Vert.	Collusion
S. Jha 2005	K-Means	2	Horizontal	-
M. Ozarar 2007	K-Means	Multi	Horizontal	×
J. Vaidya 2004	Naive Bayes	Multi	Horizontal	×
J. Vaidya 2003	K-Means	Multi	Vertical	×

Collusion Problem

Bank 1	Bank 2	Bank 3
$(100, 10)$	$(200, 15)$	$(100, 5)$

Collusion Problem

Bank 1	Bank 2	Bank 3
$(100, 10)$	$(200, 15)$	$(100, 5)$

Secure Summation Protocol:

$$p_1 = 100 + 200 + 100$$
$$p_2 = 10 + 15 + 5$$

Collusion Problem

Bank 1	Bank 2	Bank 3
$(100, 10)$	$(200, 15)$	$(100, 5)$

Secure Summation Protocol:

$$p_1 = 100 + 200 + 100$$
$$p_2 = 10 + 15 + 5$$

$$\Rightarrow \text{Average Salary} = \frac{p_1}{p_2}$$

Collusion Problem

Bank 1

$(100, 10)$

Bank 2

$(200, 15)$

Bank 3

$(100, 5)$

Secure Summation Protocol:

$$p_1 = 100 + 200 + 100$$
$$p_2 = 10 + 15 + 5$$

$$\Rightarrow \text{Average Salary} = \frac{p_1}{p_2}$$

Collusion of Bank 2 and 3

$(200, 15, 100, 5, p_1, p_2)$

Collusion Problem

Bank 1

$(100, 10)$

Bank 2

$(200, 15)$

Bank 3

$(100, 5)$

Secure Summation Protocol:

$$p_1 = 100 + 200 + 100$$
$$p_2 = 10 + 15 + 5$$

$$\Rightarrow \text{Average Salary} = \frac{p_1}{p_2}$$

Collusion of Bank 2 and 3

$$(200, 15, 100, 5, p_1, p_2)$$
$$100 = p_1 - 200 - 100$$
$$10 = p_2 - 15 - 5$$

The Whole Layout

Clustering, K-means, EM, Categorization, etc.

Secure Ratio of Summations (SRoS)

Secure Comparison of Summations (SCoS)

Secure Product of Summations (SPoS)

Random Shares

Secure Linear Function Evaluation (SLFE)

Homomorphic Encryption

Secure Product of Summations (SPoS)

Input:

Party 1: $0 < {}^{1}\chi < 1$, $0 < {}^{1}\gamma < 1$
Party 2: $0 < {}^{2}\chi < 1$, $0 < {}^{2}\gamma < 1$
Party 3: $0 < {}^{3}\chi < 1$, $0 < {}^{3}\gamma < 1$

Output:

$$\mathbf{p} = \chi \cdot \gamma = ({}^{1}\chi + {}^{2}\chi + {}^{3}\chi) \cdot ({}^{1}\gamma + {}^{2}\gamma + {}^{3}\gamma)$$

Conditions (Collusion-Resistant):

Even though party 2 and 3 collude:

- ${}^{1}\chi$ and ${}^{1}\gamma$ are not revealed to party 2 and 3;
- χ and γ are not revealed to any party.

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)

γ

$\delta - \beta\gamma$

Bob (Party 2)

β, δ

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)

γ

Generates **pk** and **sk**

Bob (Party 2)

β, δ

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)

γ

Generates **pk** and **sk**

$\rightarrow$

Bob (Party 2)

β, δ

pk

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)

γ

Generates **pk** and **sk**

Encryptes $\mathbf{C} \leftarrow \mathbf{Enc_{pk}}(-\gamma)$

$\rightarrow$

Bob (Party 2)

β, δ

pk

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)

γ

Generates **pk** and **sk**

Encryptes **C** $\leftarrow$ **Enc**$_{\mathbf{pk}}$(-γ)

$\rightarrow$

$\rightarrow$

Bob (Party 2)

β, δ

pk

C

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)

γ

Generates **pk** and **sk**

Encryptes **C** $\leftarrow$ **Enc**$_{\mathbf{pk}}$(-γ)

$\rightarrow$ β,δ

$\rightarrow$ **pk**

C

Bob (Party 2)

Encryptes **D** $\leftarrow$ **Enc**$_{\mathbf{pk}}$(δ)

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)

γ

Generates **pk** and **sk**

Encryptes $\mathbf{C} \leftarrow \mathbf{Enc_{pk}}(-\gamma)$

$\rightarrow$ β, δ

$\rightarrow$ **pk**

C

Bob (Party 2)

Encryptes $\mathbf{D} \leftarrow \mathbf{Enc_{pk}}(\delta)$

Computes $\mathbf{E} \leftarrow \mathbf{D} \cdot \mathbf{C}^{\beta}$

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)		Bob (Party 2)
γ		β, δ
Generates **pk** and **sk**	$\rightarrow$	**pk**
Encryptes $\mathbf{C} \leftarrow \mathbf{Enc_{pk}}(-\gamma)$	$\rightarrow$	**C**
		Encryptes $\mathbf{D} \leftarrow \mathbf{Enc_{pk}}(\delta)$
E	$\leftarrow$	Computes $\mathbf{E} \leftarrow \mathbf{D} \cdot \mathbf{C}^{\beta}$

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)

γ

Generates **pk** and **sk**

Encryptes $\mathbf{C} \leftarrow \mathbf{Enc_{pk}}(-\gamma)$

$\mathbf{E}$

Decryptes $\epsilon \leftarrow \mathbf{Dec_{sk}}(\mathbf{E})$

$\rightarrow$ β, δ

$\rightarrow$ **pk**

$\rightarrow$ **C**

$\leftarrow$ Encryptes $\mathbf{D} \leftarrow \mathbf{Enc_{pk}}(\delta)$

Computes $\mathbf{E} \leftarrow \mathbf{D} \cdot \mathbf{C}^{\beta}$

Bob (Party 2)

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)		Bob (Party 2)
γ		β, δ
Generates **pk** and **sk**	$\rightarrow$	**pk**
Encryptes $\mathbf{C} \leftarrow \mathbf{Enc_{pk}}(-\gamma)$	$\rightarrow$	**C**
		Encryptes $\mathbf{D} \leftarrow \mathbf{Enc_{pk}}(\delta)$
E	$\leftarrow$	Computes $\mathbf{E} \leftarrow \mathbf{D} \cdot \mathbf{C}^{\beta}$
Decryptes $\epsilon \leftarrow \mathbf{Dec_{sk}}(\mathbf{E})$		
ϵ		

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)

γ

Generates **pk** and **sk**

Encryptes $\mathbf{C} \leftarrow \mathbf{Enc_{pk}}(-\gamma)$

$\mathbf{E}$

Decryptes $\epsilon \leftarrow \mathbf{Dec_{sk}}(\mathbf{E})$

ϵ

$\rightarrow$ β, δ

$\rightarrow$ **pk**

$\rightarrow$ **C**

$\leftarrow$ Encryptes $\mathbf{D} \leftarrow \mathbf{Enc_{pk}}(\delta)$

Computes $\mathbf{E} \leftarrow \mathbf{D} \cdot \mathbf{C}^{\beta}$

Bob (Party 2)

Homomorphic Encryption

$$\mathbf{Enc}(m_1 + m_2) = \mathbf{Enc}(m_1) \cdot \mathbf{Enc}(m_2)$$
$$\mathbf{Enc}(m \cdot k) = \mathbf{Enc}(m)^k$$

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)

γ

Generates **pk** and **sk**

Encryptes $\mathbf{C} \leftarrow \mathbf{Enc_{pk}}(-\gamma)$

$\mathbf{E}$

Decryptes $\epsilon \leftarrow \mathbf{Dec_{sk}}(\mathbf{E})$

$\epsilon (= \delta - \beta\gamma)$

$\rightarrow$ β, δ

$\rightarrow$ **pk**

$\leftarrow$ **C**

Bob (Party 2)

Encryptes $\mathbf{D} \leftarrow \mathbf{Enc_{pk}}(\delta)$

Computes $\mathbf{E} \leftarrow \mathbf{D} \cdot \mathbf{C}^{\beta}$

Homomorphic Encryption

$$\mathbf{Enc}(m_1 + m_2) = \mathbf{Enc}(m_1) \cdot \mathbf{Enc}(m_2)$$

$$\mathbf{Enc}(m \cdot k) = \mathbf{Enc}(m)^k$$

Secure Linear Function Evaluation (SLFE)

Alice (Party 1)		Bob (Party 2)
γ		β, δ
Generates **pk** and **sk**	$\rightarrow$	**pk**
Encryptes $\mathbf{C} \leftarrow \mathbf{Enc_{pk}}(-\gamma)$	$\rightarrow$	**C**
		Encryptes $\mathbf{D} \leftarrow \mathbf{Enc_{pk}}(\delta)$
E	$\leftarrow$	Computes $\mathbf{E} \leftarrow \mathbf{D} \cdot \mathbf{C}^{\beta}$
Decryptes $\epsilon \leftarrow \mathbf{Dec_{sk}}(\mathbf{E})$		
$\epsilon (= \delta - \beta\gamma)$		**nothing**

Homomorphic Encryption

$$\mathbf{Enc}(m_1 + m_2) = \mathbf{Enc}(m_1) \cdot \mathbf{Enc}(m_2)$$
$$\mathbf{Enc}(m \cdot k) = \mathbf{Enc}(m)^k$$

Secure Product of Summations (1/2)

Party 1:
Party 2:
Party 3:

Party 1:
Party 2:
Party 3:

Secure Product of Summations (1/2)

Party 1: ${}^{1}\beta_1$ ${}^{1}\beta_2$ ${}^{1}\beta_3$
Party 2:
Party 3:

Party 1:
Party 2:
Party 3:

Secure Product of Summations (1/2)

Party 1: ${}^{1}\chi + {}^{1}\beta_1$ ${}^{1}\chi + {}^{1}\beta_2$ ${}^{1}\chi + {}^{1}\beta_3$
Party 2:
Party 3:

Party 1:
Party 2:
Party 3:

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2:
Party 3:

Party 1:
Party 2:
Party 3:

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2:
Party 3:

Party 1: ${}^1\alpha_1$
Party 2: ${}^1\alpha_2$
Party 3: ${}^1\alpha_3$

Secure Product of Summations (1/2)

Party 1: ${}^{1}\chi + {}^{1}\beta_1 \rightarrow {}^{1}\alpha_1, {}^{1}\chi + {}^{1}\beta_2 \rightarrow {}^{1}\alpha_2, {}^{1}\chi + {}^{1}\beta_3 \rightarrow {}^{1}\alpha_3$
Party 2: ${}^{2}\beta_1$ ${}^{2}\beta_2$ ${}^{2}\beta_3$
Party 3:

Party 1: ${}^{1}\alpha_1$
Party 2: ${}^{1}\alpha_2$
Party 3: ${}^{1}\alpha_3$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1$ ${}^2\chi + {}^2\beta_2$ ${}^2\chi + {}^2\beta_3$
Party 3:

Party 1: ${}^1\alpha_1$
Party 2: ${}^1\alpha_2$
Party 3: ${}^1\alpha_3$

Secure Product of Summations (1/2)

Party 1: ${}^{1}\chi + {}^{1}\beta_1 \rightarrow {}^{1}\alpha_1, {}^{1}\chi + {}^{1}\beta_2 \rightarrow {}^{1}\alpha_2, {}^{1}\chi + {}^{1}\beta_3 \rightarrow {}^{1}\alpha_3$
Party 2: ${}^{2}\chi + {}^{2}\beta_1 \rightarrow {}^{2}\alpha_1, {}^{2}\chi + {}^{2}\beta_2 \rightarrow {}^{2}\alpha_2, {}^{2}\chi + {}^{2}\beta_3 \rightarrow {}^{2}\alpha_3$
Party 3:

Party 1: ${}^{1}\alpha_1$
Party 2: ${}^{1}\alpha_2$
Party 3: ${}^{1}\alpha_3$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3:

Party 1: ${}^1\alpha_1$ ${}^2\alpha_1$
Party 2: ${}^1\alpha_2$ ${}^2\alpha_2$
Party 3: ${}^1\alpha_3$ ${}^2\alpha_3$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\beta_1$ ${}^3\beta_2$ ${}^3\beta_3$

Party 1: ${}^1\alpha_1$ ${}^2\alpha_1$
Party 2: ${}^1\alpha_2$ ${}^2\alpha_2$
Party 3: ${}^1\alpha_3$ ${}^2\alpha_3$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \qquad {}^3\chi + {}^3\beta_2 \qquad {}^3\chi + {}^3\beta_3$

Party 1: ${}^1\alpha_1 \quad {}^2\alpha_1$
Party 2: ${}^1\alpha_2 \quad {}^2\alpha_2$
Party 3: ${}^1\alpha_3 \quad {}^2\alpha_3$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: ${}^1\alpha_1$ ${}^2\alpha_1$
Party 2: ${}^1\alpha_2$ ${}^2\alpha_2$
Party 3: ${}^1\alpha_3$ ${}^2\alpha_3$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1:	${}^1\alpha_1$	${}^2\alpha_1$	${}^3\alpha_1$
Party 2:	${}^1\alpha_2$	${}^2\alpha_2$	${}^3\alpha_2$
Party 3:	${}^1\alpha_3$	${}^2\alpha_3$	${}^3\alpha_3$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1:	${}^1\alpha_1$	${}^2\alpha_1$	${}^3\alpha_1$	${}^1\gamma$
Party 2:	${}^1\alpha_2$	${}^2\alpha_2$	${}^3\alpha_2$	${}^2\gamma$
Party 3:	${}^1\alpha_3$	${}^2\alpha_3$	${}^3\alpha_3$	${}^3\gamma$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathbf{p},$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathbf{p},$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathbf{p},$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathbf{p}, \quad {}^1\mathbf{p} \quad {}^2\mathbf{p} \quad {}^3\mathbf{p}$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathbf{p}, \quad {}^1\mathbf{p} \quad {}^2\mathbf{p} \quad {}^3\mathbf{p}$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathbf{p}, \quad {}^1\mathbf{p} \quad {}^2\mathbf{p} \quad {}^3\mathbf{p}$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathbf{p}, \quad {}^1\mathbf{p} + {}^2\mathbf{p} + {}^3\mathbf{p} \rightarrow \mathbf{p}$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathbf{p}, \quad {}^1\mathbf{p} + {}^2\mathbf{p} + {}^3\mathbf{p} \rightarrow \mathbf{p}$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathbf{p}, \quad {}^1\mathbf{p} + {}^2\mathbf{p} + {}^3\mathbf{p} \rightarrow \mathbf{p}$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathbf{p}, \quad {}^1\mathbf{p} + {}^2\mathbf{p} + {}^3\mathbf{p} \rightarrow \mathbf{p}$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathbf{p}, \quad {}^1\mathbf{p} + {}^2\mathbf{p} + {}^3\mathbf{p} \rightarrow \mathbf{p}$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathbf{p}, \quad {}^1\mathbf{p} + {}^2\mathbf{p} + {}^3\mathbf{p} \rightarrow \mathbf{p}$

Party 1: ${}^1\mathbf{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^1\gamma + ({}^1\beta_1 + {}^2\beta_1 + {}^3\beta_1){}^1\gamma$
Party 2: ${}^2\mathbf{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^2\gamma + ({}^1\beta_2 + {}^2\beta_2 + {}^3\beta_2){}^2\gamma$
Party 3: ${}^3\mathbf{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^3\gamma + ({}^1\beta_3 + {}^2\beta_3 + {}^3\beta_3){}^3\gamma$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$

Party 1: ${}^1\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^1\gamma \quad ({}^1\beta_1 + {}^2\beta_1 + {}^3\beta_1){}^1\gamma$
Party 2: ${}^2\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^2\gamma \quad ({}^1\beta_2 + {}^2\beta_2 + {}^3\beta_2){}^2\gamma$
Party 3: ${}^3\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^3\gamma \quad ({}^1\beta_3 + {}^2\beta_3 + {}^3\beta_3){}^3\gamma$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$

Party 1: ${}^1\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^1\gamma \quad ({}^1\beta_1 + {}^2\beta_1 + {}^3\beta_1){}^1\gamma$
Party 2: ${}^2\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^2\gamma \quad ({}^1\beta_2 + {}^2\beta_2 + {}^3\beta_2){}^2\gamma$
Party 3: ${}^3\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^3\gamma \quad ({}^1\beta_3 + {}^2\beta_3 + {}^3\beta_3){}^3\gamma$

$$||$$

$$\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi)({}^1\gamma + {}^2\gamma + {}^3\gamma)$$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$

Party 1: ${}^1\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^1\gamma \quad ({}^1\beta_1 + {}^2\beta_1 + {}^3\beta_1){}^1\gamma$
Party 2: ${}^2\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^2\gamma \quad ({}^1\beta_2 + {}^2\beta_2 + {}^3\beta_2){}^2\gamma$
Party 3: ${}^3\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^3\gamma \quad ({}^1\beta_3 + {}^2\beta_3 + {}^3\beta_3){}^3\gamma$

$$||$$

$$\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi)({}^1\gamma + {}^2\gamma + {}^3\gamma)$$

Secure Product of Summations (1/2)

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathbf{p}, \quad {}^1\mathbf{p} + {}^2\mathbf{p} + {}^3\mathbf{p} \rightarrow \mathbf{p}$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathbf{p}, \quad {}^1\mathbf{p} + {}^2\mathbf{p} + {}^3\mathbf{p} \rightarrow \mathbf{p}$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathbf{p}, \quad {}^1\mathbf{p} + {}^2\mathbf{p} + {}^3\mathbf{p} \rightarrow \mathbf{p}$

Party 1: ${}^1\mathbf{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^1\gamma \quad ({}^1\beta_1 + {}^2\beta_1 + {}^3\beta_1){}^1\gamma$
Party 2: ${}^2\mathbf{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^2\gamma \quad ({}^1\beta_2 + {}^2\beta_2 + {}^3\beta_2){}^2\gamma$
Party 3: ${}^3\mathbf{p} = ({}^1\chi + {}^2\chi + {}^3\chi){}^3\gamma \quad ({}^1\beta_3 + {}^2\beta_3 + {}^3\beta_3){}^3\gamma$

$$\| \qquad\qquad \|?$$

$$\mathbf{p} = ({}^1\chi + {}^2\chi + {}^3\chi)({}^1\gamma + {}^2\gamma + {}^3\gamma) \qquad 0$$

Secure Product of Summations (2/2)

Party 1: $({}^{1}\beta_1 + {}^{2}\beta_1 + {}^{3}\beta_1){}^{1}\gamma$

Party 2: $({}^{1}\beta_2 + {}^{2}\beta_2 + {}^{3}\beta_2){}^{2}\gamma$

Party 3: $({}^{1}\beta_3 + {}^{2}\beta_3 + {}^{3}\beta_3){}^{3}\gamma$

Secure Product of Summations (2/2)

Party 1: ${}^{1}\delta_1 + {}^{1}\delta_2 + {}^{1}\delta_3 = 0$
Party 2: ${}^{2}\delta_1 + {}^{2}\delta_2 + {}^{2}\delta_3 = 0$
Party 3: ${}^{3}\delta_1 + {}^{3}\delta_2 + {}^{3}\delta_3 = 0$

Party 1: $({}^{1}\beta_1 + {}^{2}\beta_1 + {}^{3}\beta_1){}^{1}\gamma$
Party 2: $({}^{1}\beta_2 + {}^{2}\beta_2 + {}^{3}\beta_2){}^{2}\gamma$
Party 3: $({}^{1}\beta_3 + {}^{2}\beta_3 + {}^{3}\beta_3){}^{3}\gamma$

Secure Product of Summations (2/2)

Party 1: ${}^1\delta_1 + {}^1\delta_2 + {}^1\delta_3 = 0$
Party 2: ${}^2\delta_1 + {}^2\delta_2 + {}^2\delta_3 = 0$
Party 3: ${}^3\delta_1 + {}^3\delta_2 + {}^3\delta_3 = 0$

Party 1: $({}^1\beta_1 + {}^2\beta_1 + {}^3\beta_1){}^1\gamma = {}^1\delta_1 + {}^2\delta_1 + {}^3\delta_1$
Party 2: $({}^1\beta_2 + {}^2\beta_2 + {}^3\beta_2){}^2\gamma = {}^1\delta_2 + {}^2\delta_2 + {}^3\delta_2$
Party 3: $({}^1\beta_3 + {}^2\beta_3 + {}^3\beta_3){}^3\gamma = {}^1\delta_3 + {}^2\delta_3 + {}^3\delta_3$

Secure Product of Summations (2/2)

Party 1: ${}^1\delta_1 + {}^1\delta_2 + {}^1\delta_3 = 0$
Party 2: ${}^2\delta_1 + {}^2\delta_2 + {}^2\delta_3 = 0$
Party 3: ${}^3\delta_1 + {}^3\delta_2 + {}^3\delta_3 = 0$

Party 1: $({}^1\beta_1 + {}^2\beta_1 + {}^3\beta_1){}^1\gamma = {}^1\delta_1 + {}^2\delta_1 + {}^3\delta_1$
Party 2: $({}^1\beta_2 + {}^2\beta_2 + {}^3\beta_2){}^2\gamma = {}^1\delta_2 + {}^2\delta_2 + {}^3\delta_2$
Party 3: $({}^1\beta_3 + {}^2\beta_3 + {}^3\beta_3){}^3\gamma = {}^1\delta_3 + {}^2\delta_3 + {}^3\delta_3$

$$\| \; 0$$

Secure Product of Summations (2/2)

Party 1: ${}^1\delta_1 + {}^1\delta_2 + {}^1\delta_3 = 0$
Party 2: ${}^2\delta_1 + {}^2\delta_2 + {}^2\delta_3 = 0$
Party 3: ${}^3\delta_1 + {}^3\delta_2 + {}^3\delta_3 = 0$

Party 1: $({}^1\beta_1 + {}^2\beta_1 + {}^3\beta_1){}^1\gamma = {}^1\delta_1 + {}^2\delta_1 + {}^3\delta_1$
Party 2: $({}^1\beta_2 + {}^2\beta_2 + {}^3\beta_2){}^2\gamma = {}^1\delta_2 + {}^2\delta_2 + {}^3\delta_2$
Party 3: $({}^1\beta_3 + {}^2\beta_3 + {}^3\beta_3){}^3\gamma = {}^1\delta_3 + {}^2\delta_3 + {}^3\delta_3$

$$\| \quad 0$$

Secure Product of Summations (2/2)

Party 1: $^{1}\delta_1 + {}^{1}\delta_2 + {}^{1}\delta_3 = 0$

Party 2: $^{2}\delta_1 + {}^{2}\delta_2 + {}^{2}\delta_3 = 0$

Party 3: $^{3}\delta_1 + {}^{3}\delta_2 + {}^{3}\delta_3 = 0$

Party 1: $({}^{1}\beta_1 + {}^{2}\beta_1 + {}^{3}\beta_1){}^{1}\gamma = {}^{1}\delta_1 + {}^{2}\delta_1 + {}^{3}\delta_1$

Secure Product of Summations (2/2)

Party 1: $^{1}\delta_1 + {}^{1}\delta_2 + {}^{1}\delta_3 = 0$

Party 2: $^{2}\delta_1 + {}^{2}\delta_2 + {}^{2}\delta_3 = 0$

Party 3: $^{3}\delta_1 + {}^{3}\delta_2 + {}^{3}\delta_3 = 0$

Party 1: $({}^{1}\beta_1 + {}^{2}\beta_1 + {}^{3}\beta_1){}^{1}\gamma = {}^{1}\delta_1 + {}^{2}\delta_1 + {}^{3}\delta_1$

$${}^{1}\beta_1{}^{1}\gamma = {}^{1}\delta_1 + \quad ({}^{2}\delta_1 - {}^{2}\beta_1{}^{1}\gamma) \quad + \quad ({}^{3}\delta_1 - {}^{3}\beta_1{}^{1}\gamma)$$

Secure Product of Summations (2/2)

Party 1: ${}^{1}\delta_1 + {}^{1}\delta_2 + {}^{1}\delta_3 = 0$

Party 2: ${}^{2}\delta_1 + {}^{2}\delta_2 + {}^{2}\delta_3 = 0$

Party 3: ${}^{3}\delta_1 + {}^{3}\delta_2 + {}^{3}\delta_3 = 0$

Party 1: $({}^{1}\beta_1 + {}^{2}\beta_1 + {}^{3}\beta_1){}^{1}\gamma = {}^{1}\delta_1 + {}^{2}\delta_1 + {}^{3}\delta_1$

$${}^{1}\beta_1{}^{1}\gamma = {}^{1}\delta_1 + \underbrace{({}^{2}\delta_1 - {}^{2}\beta_1{}^{1}\gamma)}_{= {}^{1}\epsilon_2} + \underbrace{({}^{3}\delta_1 - {}^{3}\beta_1{}^{1}\gamma)}_{= {}^{1}\epsilon_3}$$

Secure Product of Summations (2/2)

Party 1: ${}^{1}\delta_1 + {}^{1}\delta_2 + {}^{1}\delta_3 = 0$

Party 2: ${}^{2}\delta_1 + {}^{2}\delta_2 + {}^{2}\delta_3 = 0$

Party 3: ${}^{3}\delta_1 + {}^{3}\delta_2 + {}^{3}\delta_3 = 0$

Party 1: $({}^{1}\beta_1 + {}^{2}\beta_1 + {}^{3}\beta_1){}^{1}\gamma = {}^{1}\delta_1 + {}^{2}\delta_1 + {}^{3}\delta_1$

$$
\begin{array}{ccccccc}
{}^{1}\beta_1{}^{1}\gamma = {}^{1}\delta_1 + & ({}^{2}\delta_1 - {}^{2}\beta_1{}^{1}\gamma) & + & ({}^{3}\delta_1 - {}^{3}\beta_1{}^{1}\gamma) \\
 & \| & & \| \\
{}^{1}\beta_1{}^{1}\gamma = {}^{1}\delta_1 + & {}^{1}\epsilon_2 & + & {}^{1}\epsilon_3
\end{array}
$$

Secure Product of Summations (2/2)

Party 1: ${}^{1}\delta_1 + {}^{1}\delta_2 + {}^{1}\delta_3 = 0$

Party 2: ${}^{2}\delta_1 + {}^{2}\delta_2 + {}^{2}\delta_3 = 0$

Party 3: ${}^{3}\delta_1 + {}^{3}\delta_2 + {}^{3}\delta_3 = 0$

Party 1: $({}^{1}\beta_1 + {}^{2}\beta_1 + {}^{3}\beta_1){}^{1}\gamma = {}^{1}\delta_1 + {}^{2}\delta_1 + {}^{3}\delta_1$

$${}^{1}\beta_1{}^{1}\gamma = {}^{1}\delta_1 + \underbrace{({}^{2}\delta_1 - {}^{2}\beta_1{}^{1}\gamma)}_{= {}^{1}\epsilon_2} + \underbrace{({}^{3}\delta_1 - {}^{3}\beta_1{}^{1}\gamma)}_{= {}^{1}\epsilon_3}$$

$${}^{1}\beta_1{}^{1}\gamma = {}^{1}\delta_1 + {}^{1}\epsilon_2 + {}^{1}\epsilon_3$$

SLFE

${}^{2}\beta_1, {}^{1}\gamma, {}^{2}\delta_1$

SLFE

${}^{3}\beta_1, {}^{1}\gamma, {}^{3}\delta_1$

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma$
Party 2: ${}^{2}\gamma$
Party 3: ${}^{3}\gamma$

Party 1:
Party 2:
Party 3:

Party 1:
Party 2:
Party 3:

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma, \quad , {}^{1}\beta_2, {}^{1}\beta_3, {}^{1}\delta_1, {}^{1}\delta_2, {}^{1}\delta_3$
Party 2: ${}^{2}\gamma, {}^{2}\beta_1, \quad , {}^{2}\beta_3, {}^{2}\delta_1, {}^{2}\delta_2, {}^{2}\delta_3$
Party 3: ${}^{3}\gamma, {}^{3}\beta_1, {}^{3}\beta_2, \quad , {}^{3}\delta_1, {}^{3}\delta_2, {}^{3}\delta_3$

Party 1:
Party 2:
Party 3:

Party 1:
Party 2:
Party 3:

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma, {}^{1}\beta_1, {}^{1}\beta_2, {}^{1}\beta_3, {}^{1}\delta_1, {}^{1}\delta_2, {}^{1}\delta_3$
Party 2: ${}^{2}\gamma, {}^{2}\beta_1, {}^{2}\beta_2, {}^{2}\beta_3, {}^{2}\delta_1, {}^{2}\delta_2, {}^{2}\delta_3$
Party 3: ${}^{3}\gamma, {}^{3}\beta_1, {}^{3}\beta_2, {}^{3}\beta_3, {}^{3}\delta_1, {}^{3}\delta_2, {}^{3}\delta_3$

Party 1:
Party 2:
Party 3:

Party 1:
Party 2:
Party 3:

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma, {}^{1}\beta_1, {}^{1}\beta_2, {}^{1}\beta_3, {}^{1}\delta_1, {}^{1}\delta_2, {}^{1}\delta_3$
Party 2: ${}^{2}\gamma, {}^{2}\beta_1, {}^{2}\beta_2, {}^{2}\beta_3, {}^{2}\delta_1, {}^{2}\delta_2, {}^{2}\delta_3$
Party 3: ${}^{3}\gamma, {}^{3}\beta_1, {}^{3}\beta_2, {}^{3}\beta_3, {}^{3}\delta_1, {}^{3}\delta_2, {}^{3}\delta_3$

Party 1: ${}^{1}\chi + {}^{1}\beta_1 \rightarrow {}^{1}\alpha_1, {}^{1}\chi + {}^{1}\beta_2 \rightarrow {}^{1}\alpha_2, {}^{1}\chi + {}^{1}\beta_3 \rightarrow {}^{1}\alpha_3$
Party 2:
Party 3:

Party 1:
Party 2:
Party 3:

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma, {}^{1}\beta_1, {}^{1}\beta_2, {}^{1}\beta_3, {}^{1}\delta_1, {}^{1}\delta_2, {}^{1}\delta_3$
Party 2: ${}^{2}\gamma, {}^{2}\beta_1, {}^{2}\beta_2, {}^{2}\beta_3, {}^{2}\delta_1, {}^{2}\delta_2, {}^{2}\delta_3$
Party 3: ${}^{3}\gamma, {}^{3}\beta_1, {}^{3}\beta_2, {}^{3}\beta_3, {}^{3}\delta_1, {}^{3}\delta_2, {}^{3}\delta_3$

Party 1: ${}^{1}\chi + {}^{1}\beta_1 \rightarrow {}^{1}\alpha_1, {}^{1}\chi + {}^{1}\beta_2 \rightarrow {}^{1}\alpha_2, {}^{1}\chi + {}^{1}\beta_3 \rightarrow {}^{1}\alpha_3$
Party 2:
Party 3:

Party 1: ${}^{1}\alpha_1$
Party 2: ${}^{1}\alpha_2$
Party 3: ${}^{1}\alpha_3$

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma, {}^{1}\beta_1, {}^{1}\beta_2, {}^{1}\beta_3, {}^{1}\delta_1, {}^{1}\delta_2, {}^{1}\delta_3$
Party 2: ${}^{2}\gamma, {}^{2}\beta_1, {}^{2}\beta_2, {}^{2}\beta_3, {}^{2}\delta_1, {}^{2}\delta_2, {}^{2}\delta_3$
Party 3: ${}^{3}\gamma, {}^{3}\beta_1, {}^{3}\beta_2, {}^{3}\beta_3, {}^{3}\delta_1, {}^{3}\delta_2, {}^{3}\delta_3$

Party 1: ${}^{1}\chi + {}^{1}\beta_1 \rightarrow {}^{1}\alpha_1, {}^{1}\chi + {}^{1}\beta_2 \rightarrow {}^{1}\alpha_2, {}^{1}\chi + {}^{1}\beta_3 \rightarrow {}^{1}\alpha_3$
Party 2: ${}^{2}\chi + {}^{2}\beta_1 \rightarrow {}^{2}\alpha_1, {}^{2}\chi + {}^{2}\beta_2 \rightarrow {}^{2}\alpha_2, {}^{2}\chi + {}^{2}\beta_3 \rightarrow {}^{2}\alpha_3$
Party 3:

Party 1: ${}^{1}\alpha_1$
Party 2: ${}^{1}\alpha_2$
Party 3: ${}^{1}\alpha_3$

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma, {}^{1}\beta_1, {}^{1}\beta_2, {}^{1}\beta_3, {}^{1}\delta_1, {}^{1}\delta_2, {}^{1}\delta_3$
Party 2: ${}^{2}\gamma, {}^{2}\beta_1, {}^{2}\beta_2, {}^{2}\beta_3, {}^{2}\delta_1, {}^{2}\delta_2, {}^{2}\delta_3$
Party 3: ${}^{3}\gamma, {}^{3}\beta_1, {}^{3}\beta_2, {}^{3}\beta_3, {}^{3}\delta_1, {}^{3}\delta_2, {}^{3}\delta_3$

Party 1: ${}^{1}\chi+{}^{1}\beta_1\rightarrow {}^{1}\alpha_1, {}^{1}\chi+{}^{1}\beta_2\rightarrow {}^{1}\alpha_2, {}^{1}\chi+{}^{1}\beta_3\rightarrow {}^{1}\alpha_3$
Party 2: ${}^{2}\chi+{}^{2}\beta_1\rightarrow {}^{2}\alpha_1, {}^{2}\chi+{}^{2}\beta_2\rightarrow {}^{2}\alpha_2, {}^{2}\chi+{}^{2}\beta_3\rightarrow {}^{2}\alpha_3$
Party 3:

Party 1: ${}^{1}\alpha_1$ ${}^{2}\alpha_1$
Party 2: ${}^{1}\alpha_2$ ${}^{2}\alpha_2$
Party 3: ${}^{1}\alpha_3$ ${}^{2}\alpha_3$

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma, {}^{1}\beta_1, {}^{1}\beta_2, {}^{1}\beta_3, {}^{1}\delta_1, {}^{1}\delta_2, {}^{1}\delta_3$
Party 2: ${}^{2}\gamma, {}^{2}\beta_1, {}^{2}\beta_2, {}^{2}\beta_3, {}^{2}\delta_1, {}^{2}\delta_2, {}^{2}\delta_3$
Party 3: ${}^{3}\gamma, {}^{3}\beta_1, {}^{3}\beta_2, {}^{3}\beta_3, {}^{3}\delta_1, {}^{3}\delta_2, {}^{3}\delta_3$

Party 1: ${}^{1}\chi+{}^{1}\beta_1\rightarrow {}^{1}\alpha_1, {}^{1}\chi+{}^{1}\beta_2\rightarrow {}^{1}\alpha_2, {}^{1}\chi+{}^{1}\beta_3\rightarrow {}^{1}\alpha_3$
Party 2: ${}^{2}\chi+{}^{2}\beta_1\rightarrow {}^{2}\alpha_1, {}^{2}\chi+{}^{2}\beta_2\rightarrow {}^{2}\alpha_2, {}^{2}\chi+{}^{2}\beta_3\rightarrow {}^{2}\alpha_3$
Party 3: ${}^{3}\chi+{}^{3}\beta_1\rightarrow {}^{3}\alpha_1, {}^{3}\chi+{}^{3}\beta_2\rightarrow {}^{3}\alpha_2, {}^{3}\chi+{}^{3}\beta_3\rightarrow {}^{3}\alpha_3$

Party 1: ${}^{1}\alpha_1 \quad {}^{2}\alpha_1$
Party 2: ${}^{1}\alpha_2 \quad {}^{2}\alpha_2$
Party 3: ${}^{1}\alpha_3 \quad {}^{2}\alpha_3$

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma, {}^{1}\beta_1, {}^{1}\beta_2, {}^{1}\beta_3, {}^{1}\delta_1, {}^{1}\delta_2, {}^{1}\delta_3$
Party 2: ${}^{2}\gamma, {}^{2}\beta_1, {}^{2}\beta_2, {}^{2}\beta_3, {}^{2}\delta_1, {}^{2}\delta_2, {}^{2}\delta_3$
Party 3: ${}^{3}\gamma, {}^{3}\beta_1, {}^{3}\beta_2, {}^{3}\beta_3, {}^{3}\delta_1, {}^{3}\delta_2, {}^{3}\delta_3$

Party 1: ${}^{1}\chi+{}^{1}\beta_1\rightarrow {}^{1}\alpha_1, {}^{1}\chi+{}^{1}\beta_2\rightarrow {}^{1}\alpha_2, {}^{1}\chi+{}^{1}\beta_3\rightarrow {}^{1}\alpha_3$
Party 2: ${}^{2}\chi+{}^{2}\beta_1\rightarrow {}^{2}\alpha_1, {}^{2}\chi+{}^{2}\beta_2\rightarrow {}^{2}\alpha_2, {}^{2}\chi+{}^{2}\beta_3\rightarrow {}^{2}\alpha_3$
Party 3: ${}^{3}\chi+{}^{3}\beta_1\rightarrow {}^{3}\alpha_1, {}^{3}\chi+{}^{3}\beta_2\rightarrow {}^{3}\alpha_2, {}^{3}\chi+{}^{3}\beta_3\rightarrow {}^{3}\alpha_3$

Party 1:	${}^{1}\alpha_1$	${}^{2}\alpha_1$	${}^{3}\alpha_1$
Party 2:	${}^{1}\alpha_2$	${}^{2}\alpha_2$	${}^{3}\alpha_2$
Party 3:	${}^{1}\alpha_3$	${}^{2}\alpha_3$	${}^{3}\alpha_3$

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma, {}^{1}\beta_1, {}^{1}\beta_2, {}^{1}\beta_3, {}^{1}\delta_1, {}^{1}\delta_2, {}^{1}\delta_3$
Party 2: ${}^{2}\gamma, {}^{2}\beta_1, {}^{2}\beta_2, {}^{2}\beta_3, {}^{2}\delta_1, {}^{2}\delta_2, {}^{2}\delta_3$
Party 3: ${}^{3}\gamma, {}^{3}\beta_1, {}^{3}\beta_2, {}^{3}\beta_3, {}^{3}\delta_1, {}^{3}\delta_2, {}^{3}\delta_3$

Party 1: ${}^{1}\chi+{}^{1}\beta_1\rightarrow {}^{1}\alpha_1, {}^{1}\chi+{}^{1}\beta_2\rightarrow {}^{1}\alpha_2, {}^{1}\chi+{}^{1}\beta_3\rightarrow {}^{1}\alpha_3$
Party 2: ${}^{2}\chi+{}^{2}\beta_1\rightarrow {}^{2}\alpha_1, {}^{2}\chi+{}^{2}\beta_2\rightarrow {}^{2}\alpha_2, {}^{2}\chi+{}^{2}\beta_3\rightarrow {}^{2}\alpha_3$
Party 3: ${}^{3}\chi+{}^{3}\beta_1\rightarrow {}^{3}\alpha_1, {}^{3}\chi+{}^{3}\beta_2\rightarrow {}^{3}\alpha_2, {}^{3}\chi+{}^{3}\beta_3\rightarrow {}^{3}\alpha_3$

Party 1:	${}^{1}\alpha_1$	${}^{2}\alpha_1$	${}^{3}\alpha_1$	${}^{1}\gamma$
Party 2:	${}^{1}\alpha_2$	${}^{2}\alpha_2$	${}^{3}\alpha_2$	${}^{2}\gamma$
Party 3:	${}^{1}\alpha_3$	${}^{2}\alpha_3$	${}^{3}\alpha_3$	${}^{3}\gamma$

Secure Product of Summations (the Whole Layout)

Party 1: ${}^1\gamma, {}^1\beta_1, {}^1\beta_2, {}^1\beta_3, {}^1\delta_1, {}^1\delta_2, {}^1\delta_3$
Party 2: ${}^2\gamma, {}^2\beta_1, {}^2\beta_2, {}^2\beta_3, {}^2\delta_1, {}^2\delta_2, {}^2\delta_3$
Party 3: ${}^3\gamma, {}^3\beta_1, {}^3\beta_2, {}^3\beta_3, {}^3\delta_1, {}^3\delta_2, {}^3\delta_3$

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathbf{p},$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathbf{p},$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathbf{p},$

Secure Product of Summations (the Whole Layout)

Party 1: ${}^{1}\gamma, {}^{1}\beta_1, {}^{1}\beta_2, {}^{1}\beta_3, {}^{1}\delta_1, {}^{1}\delta_2, {}^{1}\delta_3$
Party 2: ${}^{2}\gamma, {}^{2}\beta_1, {}^{2}\beta_2, {}^{2}\beta_3, {}^{2}\delta_1, {}^{2}\delta_2, {}^{2}\delta_3$
Party 3: ${}^{3}\gamma, {}^{3}\beta_1, {}^{3}\beta_2, {}^{3}\beta_3, {}^{3}\delta_1, {}^{3}\delta_2, {}^{3}\delta_3$

Party 1: ${}^{1}\chi + {}^{1}\beta_1 \rightarrow {}^{1}\alpha_1, {}^{1}\chi + {}^{1}\beta_2 \rightarrow {}^{1}\alpha_2, {}^{1}\chi + {}^{1}\beta_3 \rightarrow {}^{1}\alpha_3$
Party 2: ${}^{2}\chi + {}^{2}\beta_1 \rightarrow {}^{2}\alpha_1, {}^{2}\chi + {}^{2}\beta_2 \rightarrow {}^{2}\alpha_2, {}^{2}\chi + {}^{2}\beta_3 \rightarrow {}^{2}\alpha_3$
Party 3: ${}^{3}\chi + {}^{3}\beta_1 \rightarrow {}^{3}\alpha_1, {}^{3}\chi + {}^{3}\beta_2 \rightarrow {}^{3}\alpha_2, {}^{3}\chi + {}^{3}\beta_3 \rightarrow {}^{3}\alpha_3$

Party 1: $({}^{1}\alpha_1 + {}^{2}\alpha_1 + {}^{3}\alpha_1){}^{1}\gamma \rightarrow {}^{1}\mathbf{p}, \quad {}^{1}\mathbf{p} \quad {}^{2}\mathbf{p} \quad {}^{3}\mathbf{p}$
Party 2: $({}^{1}\alpha_2 + {}^{2}\alpha_2 + {}^{3}\alpha_2){}^{2}\gamma \rightarrow {}^{2}\mathbf{p}, \quad {}^{1}\mathbf{p} \quad {}^{2}\mathbf{p} \quad {}^{3}\mathbf{p}$
Party 3: $({}^{1}\alpha_3 + {}^{2}\alpha_3 + {}^{3}\alpha_3){}^{3}\gamma \rightarrow {}^{3}\mathbf{p}, \quad {}^{1}\mathbf{p} \quad {}^{2}\mathbf{p} \quad {}^{3}\mathbf{p}$

Secure Product of Summations (the Whole Layout)

Party 1: ${}^1\gamma, {}^1\beta_1, {}^1\beta_2, {}^1\beta_3, {}^1\delta_1, {}^1\delta_2, {}^1\delta_3$
Party 2: ${}^2\gamma, {}^2\beta_1, {}^2\beta_2, {}^2\beta_3, {}^2\delta_1, {}^2\delta_2, {}^2\delta_3$
Party 3: ${}^3\gamma, {}^3\beta_1, {}^3\beta_2, {}^3\beta_3, {}^3\delta_1, {}^3\delta_2, {}^3\delta_3$

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$

Secure Product of Summations (the Whole Layout)

Party 1: ${}^1\gamma, {}^1\beta_1, {}^1\beta_2, {}^1\beta_3, {}^1\delta_1, {}^1\delta_2, {}^1\delta_3$
Party 2: ${}^2\gamma, {}^2\beta_1, {}^2\beta_2, {}^2\beta_3, {}^2\delta_1, {}^2\delta_2, {}^2\delta_3$
Party 3: ${}^3\gamma, {}^3\beta_1, {}^3\beta_2, {}^3\beta_3, {}^3\delta_1, {}^3\delta_2, {}^3\delta_3$

Party 1: ${}^1\chi + {}^1\beta_1 \rightarrow {}^1\alpha_1, {}^1\chi + {}^1\beta_2 \rightarrow {}^1\alpha_2, {}^1\chi + {}^1\beta_3 \rightarrow {}^1\alpha_3$
Party 2: ${}^2\chi + {}^2\beta_1 \rightarrow {}^2\alpha_1, {}^2\chi + {}^2\beta_2 \rightarrow {}^2\alpha_2, {}^2\chi + {}^2\beta_3 \rightarrow {}^2\alpha_3$
Party 3: ${}^3\chi + {}^3\beta_1 \rightarrow {}^3\alpha_1, {}^3\chi + {}^3\beta_2 \rightarrow {}^3\alpha_2, {}^3\chi + {}^3\beta_3 \rightarrow {}^3\alpha_3$

Party 1: $({}^1\alpha_1 + {}^2\alpha_1 + {}^3\alpha_1){}^1\gamma \rightarrow {}^1\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$
Party 2: $({}^1\alpha_2 + {}^2\alpha_2 + {}^3\alpha_2){}^2\gamma \rightarrow {}^2\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$
Party 3: $({}^1\alpha_3 + {}^2\alpha_3 + {}^3\alpha_3){}^3\gamma \rightarrow {}^3\mathrm{p}, \quad {}^1\mathrm{p} + {}^2\mathrm{p} + {}^3\mathrm{p} \rightarrow \mathrm{p}$

$$\mathrm{p} = ({}^1\chi + {}^2\chi + {}^3\chi)({}^1\gamma + {}^2\gamma + {}^3\gamma)$$

Security & Efficiency

Definition (t-Private)

A protocol is called **t-private** *if no coalition containing at most t parties can get any additional information from its execution. We call (m-1)-private* **fully-private**, *where m is the number of parties.*

Theorem (Security of SPoS)

SPoS protocol is fully private ((m-1)-private).

Theorem (Efficiency of SPoS)

The running time of SPoS protocol is O(m).

Security & Efficiency

Definition (t-Private)

A protocol is called **t-private** *if no coalition containing at most t parties can get any additional information from its execution. We call (m-1)-private* **fully-private**, *where m is the number of parties.*

Theorem (Security of SPoS)

SPoS protocol is fully private ((m-1)-private).

Theorem (Efficiency of SPoS)

The running time of SPoS protocol is O(m).

Security & Efficiency

Definition (t-Private)

A protocol is called **t-private** *if no coalition containing at most t parties can get any additional information from its execution. We call (m-1)-private* **fully-private**, *where m is the number of parties.*

Theorem (Security of SPoS)

SPoS protocol is fully private ((m-1)-private).

Theorem (Efficiency of SPoS)

The running time of SPoS protocol is O(m).

Secure Ratio of Summations (SRoS)

Input:

Party 1: $0 < {}^{1}x < 1$, $0 < {}^{1}y < 1$
Party 2: $0 < {}^{2}x < 1$, $0 < {}^{2}y < 1$
Party 3: $0 < {}^{3}x < 1$, $0 < {}^{3}y < 1$

Output:

$$r = \frac{x}{y} = \frac{{}^{1}x + {}^{2}x + {}^{3}x}{{}^{1}y + {}^{2}y + {}^{3}y}$$

Conditions:

Collusion-Resistant

Secure Ratio of Summations (SRoS)

Party 1: ${}^{1}x$, ${}^{1}y$
Party 2: ${}^{2}x$, ${}^{2}y$
Party 3: ${}^{3}x$, ${}^{3}y$

Secure Ratio of Summations (SRoS)

Party 1: ${}^{1}x$, ${}^{1}y$, ${}^{1}c$
Party 2: ${}^{2}x$, ${}^{2}y$, ${}^{2}c$
Party 3: ${}^{3}x$, ${}^{3}y$, ${}^{3}c$

Secure Ratio of Summations (SRoS)

Party 1: ${}^{1}x$, ${}^{1}y$, ${}^{1}c$
Party 2: ${}^{2}x$, ${}^{2}y$, ${}^{2}c$
Party 3: ${}^{3}x$, ${}^{3}y$, ${}^{3}c$

Secure Ratio of Summations (SRoS)

Party 1: ${}^{1}x$, ${}^{1}y$, ${}^{1}c$
Party 2: ${}^{2}x$, ${}^{2}y$, ${}^{2}c$
Party 3: ${}^{3}x$, ${}^{3}y$, ${}^{3}c$

$$p_x = \mathrm{SPoS}(x, c) = ({}^{1}x + {}^{2}x + {}^{3}x) \cdot ({}^{1}c + {}^{2}c + {}^{3}c)$$

Secure Ratio of Summations (SRoS)

Party 1: ${}^{1}x$, ${}^{1}y$, ${}^{1}c$
Party 2: ${}^{2}x$, ${}^{2}y$, ${}^{2}c$
Party 3: ${}^{3}x$, ${}^{3}y$, ${}^{3}c$

$$p_x = \mathrm{SPoS}(x, c) = ({}^{1}x + {}^{2}x + {}^{3}x) \cdot ({}^{1}c + {}^{2}c + {}^{3}c)$$

Secure Ratio of Summations (SRoS)

Party 1: ${}^{1}x$, ${}^{1}y$, ${}^{1}c$
Party 2: ${}^{2}x$, ${}^{2}y$, ${}^{2}c$
Party 3: ${}^{3}x$, ${}^{3}y$, ${}^{3}c$

$$p_x = \mathrm{SPoS}(x, c) = ({}^{1}x + {}^{2}x + {}^{3}x) \cdot ({}^{1}c + {}^{2}c + {}^{3}c)$$
$$p_y = \mathrm{SPoS}(y, c) = ({}^{1}y + {}^{2}y + {}^{3}y) \cdot ({}^{1}c + {}^{2}c + {}^{3}c)$$

Secure Ratio of Summations (SRoS)

Party 1: ${}^1x$, ${}^1y$, ${}^1c$
Party 2: ${}^2x$, ${}^2y$, ${}^2c$
Party 3: ${}^3x$, ${}^3y$, ${}^3c$

$$p_x = \mathrm{SPoS}(x, c) = ({}^1x + {}^2x + {}^3x) \cdot ({}^1c + {}^2c + {}^3c)$$
$$p_y = \mathrm{SPoS}(y, c) = ({}^1y + {}^2y + {}^3y) \cdot ({}^1c + {}^2c + {}^3c)$$

$$r = \frac{p_x}{p_y} = \frac{{}^1x + {}^2x + {}^3x}{{}^1y + {}^2y + {}^3y}$$

Secure Comparison of Summations (SCoS)

Input:

Party 1: $0 < {}^{1}x_1 < 1$, $0 < {}^{1}x_2 < 1$
Party 2: $0 < {}^{2}x_1 < 1$, $0 < {}^{2}x_2 < 1$
Party 3: $0 < {}^{3}x_1 < 1$, $0 < {}^{3}x_2 < 1$

Output:

$$c = \text{argmax}(x_1, x_2) = \text{argmax}({}^{1}x_1 + {}^{2}x_1 + {}^{3}x_1, {}^{1}x_2 + {}^{2}x_2 + {}^{3}x_2)$$

Conditions:

Collusion-Resistant

Secure Comparison of Summations (SCoS)

Party 1:
Party 2:
Party 3:

Secure Comparison of Summations (SCoS)

Party 1: ${}^{1}u$,
Party 2: ${}^{2}u$,
Party 3: ${}^{3}u$,

Secure Comparison of Summations (SCoS)

Party 1: ${}^{1}u$, ${}^{1}y_1 = {}^{1}x_1/P + {}^{1}u$,
Party 2: ${}^{2}u$, ${}^{2}y_1 = {}^{2}x_1/P + {}^{2}u$,
Party 3: ${}^{3}u$, ${}^{3}y_1 = {}^{3}x_1/P + {}^{3}u$,

Secure Comparison of Summations (SCoS)

Party 1: ${}^1u$, ${}^1y_1 = {}^1x_1/P + {}^1u$, ${}^1y_2 = {}^1x_2/P + {}^1u$,
Party 2: ${}^2u$, ${}^2y_1 = {}^2x_1/P + {}^2u$, ${}^2y_2 = {}^2x_2/P + {}^2u$,
Party 3: ${}^3u$, ${}^3y_1 = {}^3x_1/P + {}^3u$, ${}^3y_2 = {}^3x_2/P + {}^3u$,

Secure Comparison of Summations (SCoS)

Party 1: ${}^1u$, ${}^1y_1 = {}^1x_1/P + {}^1u$, ${}^1y_2 = {}^1x_2/P + {}^1u$, ${}^1c$
Party 2: ${}^2u$, ${}^2y_1 = {}^2x_1/P + {}^2u$, ${}^2y_2 = {}^2x_2/P + {}^2u$, ${}^2c$
Party 3: ${}^3u$, ${}^3y_1 = {}^3x_1/P + {}^3u$, ${}^3y_2 = {}^3x_2/P + {}^3u$, ${}^3c$

Secure Comparison of Summations (SCoS)

Party 1: ${}^{1}u$, ${}^{1}y_1 = {}^{1}x_1/P + {}^{1}u$, ${}^{1}y_2 = {}^{1}x_2/P + {}^{1}u$, ${}^{1}c$
Party 2: ${}^{2}u$, ${}^{2}y_1 = {}^{2}x_1/P + {}^{2}u$, ${}^{2}y_2 = {}^{2}x_2/P + {}^{2}u$, ${}^{2}c$
Party 3: ${}^{3}u$, ${}^{3}y_1 = {}^{3}x_1/P + {}^{3}u$, ${}^{3}y_2 = {}^{3}x_2/P + {}^{3}u$, ${}^{3}c$

Secure Comparison of Summations (SCoS)

Party 1: ${}^{1}u$, ${}^{1}y_1 = {}^{1}x_1/P + {}^{1}u$, ${}^{1}y_2 = {}^{1}x_2/P + {}^{1}u$, ${}^{1}c$
Party 2: ${}^{2}u$, ${}^{2}y_1 = {}^{2}x_1/P + {}^{2}u$, ${}^{2}y_2 = {}^{2}x_2/P + {}^{2}u$, ${}^{2}c$
Party 3: ${}^{3}u$, ${}^{3}y_1 = {}^{3}x_1/P + {}^{3}u$, ${}^{3}y_2 = {}^{3}x_2/P + {}^{3}u$, ${}^{3}c$

$$p_1 = \mathrm{SPoS}(y_1, c) = ({}^{1}y_1 + {}^{2}y_1 + {}^{3}y_1) \cdot ({}^{1}c + {}^{2}c + {}^{3}c)$$

Secure Comparison of Summations (SCoS)

Party 1: ${}^1u$, ${}^1y_1 = {}^1x_1/P + {}^1u$, ${}^1y_2 = {}^1x_2/P + {}^1u$, ${}^1c$
Party 2: ${}^2u$, ${}^2y_1 = {}^2x_1/P + {}^2u$, ${}^2y_2 = {}^2x_2/P + {}^2u$, ${}^2c$
Party 3: ${}^3u$, ${}^3y_1 = {}^3x_1/P + {}^3u$, ${}^3y_2 = {}^3x_2/P + {}^3u$, ${}^3c$

$$p_1 = \mathrm{SPoS}(y_1, c) = ({}^1y_1 + {}^2y_1 + {}^3y_1) \cdot ({}^1c + {}^2c + {}^3c)$$

Secure Comparison of Summations (SCoS)

Party 1: ${}^1u$, ${}^1y_1 = {}^1x_1/P + {}^1u$, ${}^1y_2 = {}^1x_2/P + {}^1u$, ${}^1c$
Party 2: ${}^2u$, ${}^2y_1 = {}^2x_1/P + {}^2u$, ${}^2y_2 = {}^2x_2/P + {}^2u$, ${}^2c$
Party 3: ${}^3u$, ${}^3y_1 = {}^3x_1/P + {}^3u$, ${}^3y_2 = {}^3x_2/P + {}^3u$, ${}^3c$

$$p_1 = \mathrm{SPoS}(y_1, c) = ({}^1y_1 + {}^2y_1 + {}^3y_1) \cdot ({}^1c + {}^2c + {}^3c)$$
$$p_2 = \mathrm{SPoS}(y_2, c) = ({}^1y_2 + {}^2y_2 + {}^3y_2) \cdot ({}^1c + {}^2c + {}^3c)$$

Secure Comparison of Summations (SCoS)

Party 1: ${}^1u$, ${}^1y_1 = {}^1x_1/P + {}^1u$, ${}^1y_2 = {}^1x_2/P + {}^1u$, ${}^1c$
Party 2: ${}^2u$, ${}^2y_1 = {}^2x_1/P + {}^2u$, ${}^2y_2 = {}^2x_2/P + {}^2u$, ${}^2c$
Party 3: ${}^3u$, ${}^3y_1 = {}^3x_1/P + {}^3u$, ${}^3y_2 = {}^3x_2/P + {}^3u$, ${}^3c$

$$p_1 = \mathrm{SPoS}(y_1, c) = ({}^1y_1 + {}^2y_1 + {}^3y_1) \cdot ({}^1c + {}^2c + {}^3c)$$
$$p_2 = \mathrm{SPoS}(y_2, c) = ({}^1y_2 + {}^2y_2 + {}^3y_2) \cdot ({}^1c + {}^2c + {}^3c)$$

Secure Comparison of Summations (SCoS)

Party 1: ${}^1u$, ${}^1y_1 = {}^1x_1/P + {}^1u$, ${}^1y_2 = {}^1x_2/P + {}^1u$, ${}^1c$
Party 2: ${}^2u$, ${}^2y_1 = {}^2x_1/P + {}^2u$, ${}^2y_2 = {}^2x_2/P + {}^2u$, ${}^2c$
Party 3: ${}^3u$, ${}^3y_1 = {}^3x_1/P + {}^3u$, ${}^3y_2 = {}^3x_2/P + {}^3u$, ${}^3c$

$$p_1 = \mathrm{SPoS}(y_1, c) = ({}^1y_1 + {}^2y_1 + {}^3y_1) \cdot ({}^1c + {}^2c + {}^3c)$$
$$p_2 = \mathrm{SPoS}(y_2, c) = ({}^1y_2 + {}^2y_2 + {}^3y_2) \cdot ({}^1c + {}^2c + {}^3c)$$

$$p_1 = ({}^1x_1 + {}^2x_1 + {}^3x_1)V + U$$
$$p_2 = ({}^1x_2 + {}^2x_2 + {}^3x_2)V + U$$
$$V = ({}^1c + {}^2c + {}^3c)/P > 0$$
$$U = ({}^1u + {}^2u + {}^3u)({}^1c + {}^2c + {}^3c) > 0$$

Secure Comparison of Summations (SCoS)

Party 1: ${}^1u$, ${}^1y_1 = {}^1x_1/P + {}^1u$, ${}^1y_2 = {}^1x_2/P + {}^1u$, ${}^1c$
Party 2: ${}^2u$, ${}^2y_1 = {}^2x_1/P + {}^2u$, ${}^2y_2 = {}^2x_2/P + {}^2u$, ${}^2c$
Party 3: ${}^3u$, ${}^3y_1 = {}^3x_1/P + {}^3u$, ${}^3y_2 = {}^3x_2/P + {}^3u$, ${}^3c$

$$p_1 = \mathrm{SPoS}(y_1, c) = ({}^1y_1 + {}^2y_1 + {}^3y_1) \cdot ({}^1c + {}^2c + {}^3c)$$
$$p_2 = \mathrm{SPoS}(y_2, c) = ({}^1y_2 + {}^2y_2 + {}^3y_2) \cdot ({}^1c + {}^2c + {}^3c)$$

$$p_1 = ({}^1x_1 + {}^2x_1 + {}^3x_1)V + U$$
$$p_2 = ({}^1x_2 + {}^2x_2 + {}^3x_2)V + U$$
$$V = ({}^1c + {}^2c + {}^3c)/P > 0$$
$$U = ({}^1u + {}^2u + {}^3u)({}^1c + {}^2c + {}^3c) > 0$$

$$p_1 > p_2 \Leftrightarrow {}^1x_1 + {}^2x_1 + {}^3x_1 > {}^1x_2 + {}^2x_2 + {}^3x_2$$

Conclusion

Security of SPoS

Fully private ((m-1)-private).

Efficiency of SPoS

The running time of SPoS protocol is O(m).

Methods	Hori./Vert.	Protocol	Collusion
K-Means	Horizontal	**SRoS**	o
Naive Bayes	Horizontal	**SRoS**	o
K-Means	Vertical	**SCoS**	o
Secure Sorting	Vertical	**SCoS**	o