Optimal Communication Unbalanced Private Set Union

Alexis GALAN

March 6, 2024

Cybersecurity Institute
Université Grenoble Alpes

In collaboration with:
Jean-Guillaume DUMAS, Bruno GRENET, Aude MAIGNAN, Daniel S. ROCHE

Table of Contents

Table of Contents

Concrete situation : whistleblower

Concrete situation : whistleblower

Concrete situation : whistleblower

Concrete situation : whistleblower

Concrete situation : whistleblower

Concrete situation : whistleblower

Table of Contents

Linearly Homomorphic Encryption

Definition

Linearly Homomorphic Encryption scheme (LHE):

- $L.D_{sk}(L.E_{pk}(m)) = m$

Linearly Homomorphic Encryption

Definition

Linearly Homomorphic Encryption scheme (LHE):

- $L.D_{sk}(L.E_{pk}(m)) = m$
- $L.D_{sk}(L.E_{pk}(m_1) +_L L.E_{pk}(m_2)) = m_1 + m_2$

Linearly Homomorphic Encryption

Definition

Linearly Homomorphic Encryption scheme (LHE):

- $L.D_{sk}(L.E_{pk}(m)) = m$
- $L.D_{sk}(L.E_{pk}(m_1) +_L L.E_{pk}(m_2)) = m_1 + m_2$
- $L.D_{sk}(m_2 \ltimes_L L.E_{pk}(m_1)) = m_1 m_2$

Linearly Homomorphic Encryption

Definition

Linearly Homomorphic Encryption scheme (LHE):

- $L.D_{sk}(L.E_{pk}(m)) = m$
- $L.D_{sk}(L.E_{pk}(m_1) +_L L.E_{pk}(m_2)) = m_1 + m_2$
- $L.D_{sk}(m_2 \ltimes_L L.E_{pk}(m_1)) = m_1 m_2$

Notation: $\hat{m} \leftarrow L.E_{pk}(m)$.

Linearly Homomorphic Encryption

Definition

Linearly Homomorphic Encryption scheme (LHE):

- $L.D_{sk}(L.E_{pk}(m)) = m$
- $L.D_{sk}(L.E_{pk}(m_1) +_L L.E_{pk}(m_2)) = m_1 + m_2$
- $L.D_{sk}(m_2 \ltimes_L L.E_{pk}(m_1)) = m_1 m_2$

Notation: $\hat{m} \leftarrow L.E_{pk}(m)$.

Constraints

Linearly Homomorphic Encryption

Definition

Linearly Homomorphic Encryption scheme (LHE):

- $L.D_{sk}(L.E_{pk}(m)) = m$
- $L.D_{sk}(L.E_{pk}(m_1) +_L L.E_{pk}(m_2)) = m_1 + m_2$
- $L.D_{sk}(m_2 \ltimes_L L.E_{pk}(m_1)) = m_1 m_2$

Notation: $\hat{m} \leftarrow L.E_{pk}(m)$.

Constraints

- No test (Straight-line programs).

Linearly Homomorphic Encryption

Definition

Linearly Homomorphic Encryption scheme (LHE):

- $L.D_{sk}(L.E_{pk}(m)) = m$
- $L.D_{sk}(L.E_{pk}(m_1) +_L L.E_{pk}(m_2)) = m_1 + m_2$
- $L.D_{sk}(m_2 \ltimes_L L.E_{pk}(m_1)) = m_1 m_2$

Notation: $\hat{m} \leftarrow L.E_{pk}(m)$.

Constraints

- No test (Straight-line programs).
- No division, no inversion.

Linearly Homomorphic Encryption

Definition

Linearly Homomorphic Encryption scheme (LHE):

- $L.D_{sk}(L.E_{pk}(m)) = m$
- $L.D_{sk}(L.E_{pk}(m_1) +_L L.E_{pk}(m_2)) = m_1 + m_2$
- $L.D_{sk}(m_2 \ltimes_L L.E_{pk}(m_1)) = m_1 m_2$

Notation: $\hat{m} \leftarrow L.E_{pk}(m)$.

Constraints

- No test (Straight-line programs).
- No division, no inversion.
- No ciphertext multiplication.

Linearly homomorphic multi-point evaluation

Construction

1. $$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ & \cdots & \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \ltimes_L \begin{pmatrix} \widehat{b_1} \\ \cdots \\ \widehat{b_m} \end{pmatrix} = \begin{pmatrix} a_{11} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{1m} \ltimes_L \widehat{b_m} \\ \cdots \\ a_{n1} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{nm} \ltimes_L \widehat{b_m} \end{pmatrix}$$

Linearly homomorphic multi-point evaluation

Construction

1. $$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ & \cdots & \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \ltimes_L \begin{pmatrix} \widehat{b_1} \\ \cdots \\ \widehat{b_m} \end{pmatrix} = \begin{pmatrix} a_{11} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{1m} \ltimes_L \widehat{b_m} \\ \cdots \\ a_{n1} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{nm} \ltimes_L \widehat{b_m} \end{pmatrix}$$
2. Clear-cipher polynomial product and middle product.
$$\widehat{B} \longmapsto A \ltimes_L \widehat{B} \; ; \; \widehat{C} \longmapsto A \ltimes_L^t \widehat{C}$$

Linearly homomorphic multi-point evaluation

Construction

1. $$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ & \cdots & \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \ltimes_L \begin{pmatrix} \widehat{b_1} \\ \cdots \\ \widehat{b_m} \end{pmatrix} = \begin{pmatrix} a_{11} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{1m} \ltimes_L \widehat{b_m} \\ \cdots \\ a_{n1} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{nm} \ltimes_L \widehat{b_m} \end{pmatrix}$$
2. Clear-cipher polynomial product and middle product.
$$\widehat{B} \longmapsto A \ltimes_L \widehat{B} \; ; \; \widehat{C} \longmapsto A \ltimes_L^t \widehat{C}$$

Linearly homomorphic multi-point evaluation

Construction

1. $$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ & \cdots & \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \ltimes_L \begin{pmatrix} \widehat{b_1} \\ \cdots \\ \widehat{b_m} \end{pmatrix} = \begin{pmatrix} a_{11} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{1m} \ltimes_L \widehat{b_m} \\ \cdots \\ a_{n1} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{nm} \ltimes_L \widehat{b_m} \end{pmatrix}$$
2. Clear-cipher polynomial product and middle product.
$$\widehat{B} \longmapsto A \ltimes_L \widehat{B} \; ; \; \widehat{C} \longmapsto A \ltimes_L^t \widehat{C}$$
3. **[Bostan et al., 2003]** Tellegen's principle $\Rightarrow$ Multi-point eval. via 2.

Linearly homomorphic multi-point evaluation

Construction

1. $$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ & \cdots & \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \ltimes_L \begin{pmatrix} \widehat{b_1} \\ \cdots \\ \widehat{b_m} \end{pmatrix} = \begin{pmatrix} a_{11} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{1m} \ltimes_L \widehat{b_m} \\ \cdots \\ a_{n1} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{nm} \ltimes_L \widehat{b_m} \end{pmatrix}$$
2. Clear-cipher polynomial product and middle product.
$$\widehat{B} \longmapsto A \ltimes_L \widehat{B} \; ; \; \widehat{C} \longmapsto A \ltimes_L^t \widehat{C}$$
3. **[Bostan et al., 2003]** Tellegen's principle $\Rightarrow$ Multi-point eval. via 2.

$$\Rightarrow MEv_L : \widehat{A}, \{y_1, ..., y_m\} \longmapsto \{\widehat{A}(y_1), ..., \widehat{A}(y_m)\}$$

Linearly homomorphic multi-point evaluation

Construction

1. $$\begin{pmatrix} a_{11} & \cdots & a_{1m} \\ & \cdots & \\ a_{n1} & \cdots & a_{nm} \end{pmatrix} \ltimes_L \begin{pmatrix} \widehat{b_1} \\ \cdots \\ \widehat{b_m} \end{pmatrix} = \begin{pmatrix} a_{11} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{1m} \ltimes_L \widehat{b_m} \\ \cdots \\ a_{n1} \ltimes_L \widehat{b_1} +_L \cdots +_L a_{nm} \ltimes_L \widehat{b_m} \end{pmatrix}$$
2. Clear-cipher polynomial product and middle product.
$$\widehat{B} \longmapsto A \ltimes_L \widehat{B} \; ; \; \widehat{C} \longmapsto A \ltimes_L^t \widehat{C}$$
3. **[Bostan et al., 2003]** Tellegen's principle $\Rightarrow$ Multi-point eval. via 2.

$$\Rightarrow MEv_L : \widehat{A}, \{y_1, ..., y_m\} \longmapsto \{\widehat{A}(y_1), ..., \widehat{A}(y_m)\}$$

Lemma

There is an algorithm computing MEv_L in $\mathscr{M}_L(m) \log m + \tilde{O}(m)$ such that:

$$L.D_{sk}\left(MEv_L\left(L.E_{pk}(A), \{y_1, ..., y_m\}\right)\right) = \{A(y_1), ..., A(y_m)\}$$

Notation: $\mathscr{M}_L(d)$ is arith. cost of LHE poly. mult. of degree $\leq d$.

Fully Homomorphic Encryption

Definition

Fully Homomorphic Encryption scheme (FHE)

Fully Homomorphic Encryption

Definition

Fully Homomorphic Encryption scheme (FHE)

- $F.D_{sk}(F.E_{pk}(m)) = m$

Fully Homomorphic Encryption

Definition

Fully Homomorphic Encryption scheme (FHE)

- $F.D_{sk}(F.E_{pk}(m)) = m$
- $F.D_{sk}(F.E_{pk}(m_1) +_F F.E_{pk}(m_2)) = m_1 + m_2$

Fully Homomorphic Encryption

Definition

Fully Homomorphic Encryption scheme (FHE)

- $F.D_{sk}(F.E_{pk}(m)) = m$
- $F.D_{sk}(F.E_{pk}(m_1) +_F F.E_{pk}(m_2)) = m_1 + m_2$
- $F.D_{sk}(F.E_{pk}(m_1) \times_F F.E_{pk}(m_1)) = m_1 m_2$

Fully Homomorphic Encryption

Definition

Fully Homomorphic Encryption scheme (FHE)

- $F.D_{sk}(F.E_{pk}(m)) = m$
- $F.D_{sk}(F.E_{pk}(m_1) +_F F.E_{pk}(m_2)) = m_1 + m_2$
- $F.D_{sk}(F.E_{pk}(m_1) \times_F F.E_{pk}(m_1)) = m_1 m_2$

Notation: $\widetilde{m} \leftarrow F.E_{pk}(m)$.

Fully Homomorphic Encryption

Definition

Fully Homomorphic Encryption scheme (FHE)

- $F.D_{sk}(F.E_{pk}(m)) = m$
- $F.D_{sk}(F.E_{pk}(m_1) +_F F.E_{pk}(m_2)) = m_1 + m_2$
- $F.D_{sk}(F.E_{pk}(m_1) \times_F F.E_{pk}(m_1)) = m_1 m_2$

Notation: $\tilde{m} \leftarrow F.E_{pk}(m)$.

Constraints

Fully Homomorphic Encryption

Definition

Fully Homomorphic Encryption scheme (FHE)

- $F.D_{sk}(F.E_{pk}(m)) = m$
- $F.D_{sk}(F.E_{pk}(m_1) +_F F.E_{pk}(m_2)) = m_1 + m_2$
- $F.D_{sk}(F.E_{pk}(m_1) \times_F F.E_{pk}(m_1)) = m_1 m_2$

Notation: $\tilde{m} \leftarrow F.E_{pk}(m)$.

Constraints

- No test.

Fully Homomorphic Encryption

Definition

Fully Homomorphic Encryption scheme (FHE)

- $F.D_{sk}(F.E_{pk}(m)) = m$
- $F.D_{sk}(F.E_{pk}(m_1) +_F F.E_{pk}(m_2)) = m_1 + m_2$
- $F.D_{sk}(F.E_{pk}(m_1) \times_F F.E_{pk}(m_1)) = m_1 m_2$

Notation: $\tilde{m} \leftarrow F.E_{pk}(m)$.

Constraints

- No test.
- No division, no inversion.

Fully Homomorphic Encryption

Definition

Fully Homomorphic Encryption scheme (FHE)

- $F.D_{sk}(F.E_{pk}(m)) = m$
- $F.D_{sk}(F.E_{pk}(m_1) +_F F.E_{pk}(m_2)) = m_1 + m_2$
- $F.D_{sk}(F.E_{pk}(m_1) \times_F F.E_{pk}(m_1)) = m_1 m_2$

Notation: $\tilde{m} \leftarrow F.E_{pk}(m)$.

Constraints

- No test.
- No division, no inversion.
- Ciphertext multiplication ✓ (but ⚠ circuit depth).

Fully homomorphic euclidean remainder

Construction

1. $A(Z) = B(Z)Q(Z) + R(Z)$

Fully homomorphic euclidean remainder

Construction

1. $\overleftarrow{A}(Z) = \overleftarrow{B}(Z)\overleftarrow{Q}(Z) + \overleftarrow{R}(Z)Z^{n-m+1}$

Fully homomorphic euclidean remainder

Construction

1. $\overleftarrow{A}(Z) = \overleftarrow{B}(Z)\overleftarrow{Q}(Z) + \overleftarrow{R}(Z)Z^{n-m+1} \Rightarrow \overleftarrow{Q} = \overleftarrow{B}^{-1}\overleftarrow{A} \mod Z^{n-m+1}$

Fully homomorphic euclidean remainder

Construction

1. $\overleftarrow{A}(Z) = \overleftarrow{B}(Z)\overleftarrow{Q}(Z) + \overleftarrow{R}(Z)Z^{n-m+1} \Rightarrow \overleftarrow{Q} = \overleftarrow{B}^{-1}\overleftarrow{A} \mod Z^{n-m+1}$
2. Newton method: $U_l = \overleftarrow{B}^{-1} \mod Z^{2^l}$

$$(U) = \begin{cases} U_0 & = & 1 \\ U_{k+1} & = & U_k\left(2 - U_k\overleftarrow{B}\right) \mod Z^{2^{k+1}} \end{cases}$$

Fully homomorphic euclidean remainder

Construction

1. $\overleftarrow{A}(Z) = \overleftarrow{B}(Z)\overleftarrow{Q}(Z) + \overleftarrow{R}(Z)Z^{n-m+1} \Rightarrow \overleftarrow{Q} = \overleftarrow{B}^{-1}\overleftarrow{A} \mod Z^{n-m+1}$
2. Newton method: $U_l = \overleftarrow{B}^{-1} \mod Z^{2^l}$

$$(U) = \begin{cases} U_0 & = & 1 \\ U_{k+1} & = & U_k\left(2 - U_k\overleftarrow{B}\right) \mod Z^{2^{k+1}} \end{cases}$$

3. $\overleftarrow{Q} = U_l\overleftarrow{A} \mod Z^{n-m+1} \Rightarrow R = A - BQ \mod Z^m$.

Fully homomorphic euclidean remainder

Construction

1. $\overleftarrow{A}(Z) = \overleftarrow{B}(Z)\overleftarrow{Q}(Z) + \overleftarrow{R}(Z)Z^{n-m+1} \Rightarrow \overleftarrow{Q} = \overleftarrow{B}^{-1}\overleftarrow{A} \mod Z^{n-m+1}$
2. Homomorphic Newton method: $\widetilde{U}_l = \overleftarrow{\widetilde{B}}^{-1} \mod Z^{2^l}$

$$(\widetilde{U}) = \begin{cases} \widetilde{U}_0 & = & \widetilde{1} \\ \widetilde{U}_{k+1} & = & \widetilde{U}_k \times_F \left(\widetilde{2} -_F \widetilde{U}_k \times_F \overleftarrow{\widetilde{B}}\right) \end{cases} \mod Z^{2^{k+1}}$$

3. $\overleftarrow{\widetilde{Q}} = \widetilde{U}_l \times_F \overleftarrow{\widetilde{A}} \mod Z^{n-m+1} \Rightarrow \widetilde{R} = \widetilde{A} -_F \widetilde{B} \times_F \widetilde{Q} \mod Z^m.$

Fully homomorphic euclidean remainder

Construction

1. $\overleftarrow{A}(Z) = \overleftarrow{B}(Z)\overleftarrow{Q}(Z) + \overleftarrow{R}(Z)Z^{n-m+1} \Rightarrow \overleftarrow{Q} = \overleftarrow{B}^{-1}\overleftarrow{A} \mod Z^{n-m+1}$
2. Homomorphic Newton method: $\widetilde{U}_l = \overleftarrow{\widetilde{B}}^{-1} \mod Z^{2^l}$

$$(\widetilde{U}) = \begin{cases} \widetilde{U}_0 & = & \widetilde{1} \\ \widetilde{U}_{k+1} & = & \widetilde{U}_k \times_F \left(\widetilde{2} -_F \widetilde{U}_k \times_F \overleftarrow{\widetilde{B}}\right) \end{cases} \mod Z^{2^{k+1}}$$

3. $\overleftarrow{\widetilde{Q}} = \widetilde{U}_l \times_F \overleftarrow{\widetilde{A}} \mod Z^{n-m+1} \Rightarrow \widetilde{R} = \widetilde{A} -_F \widetilde{B} \times_F \widetilde{Q} \mod Z^m$.

Lemma

There is an algorithm computing $\%_F$ in $\frac{9}{2}\mathscr{M}_F(n-m) + O(n)$ such that:

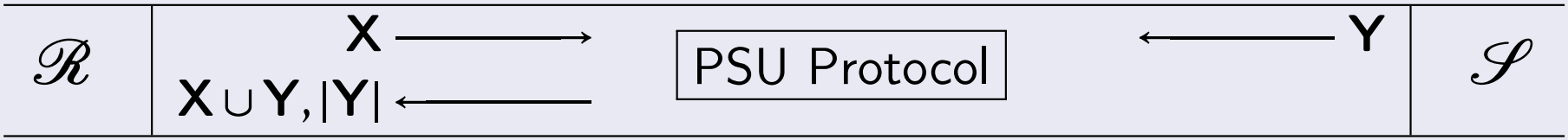
$$F.D_{sk}(F.E_{pk}(A)\%_F F.E_{pk}(B)) = R$$

Notation: $\mathscr{M}_F(d)$ is arith. cost of FHE poly. mult. of degree $\leq d$.

Table of Contents

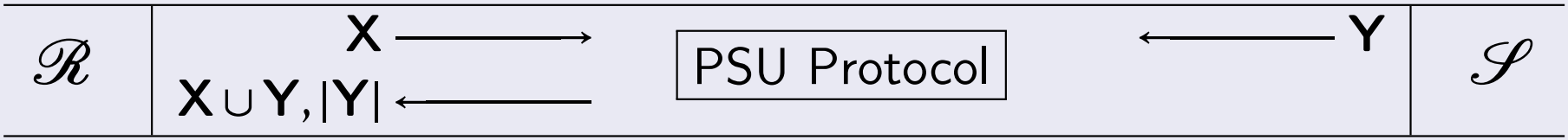
Unbalanced Private Set Union

Functionality



Unbalanced Private Set Union

Functionality

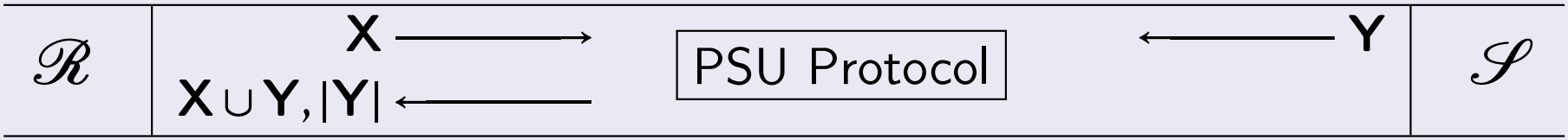


Security

In the honest-but-curious adversary model:

Unbalanced Private Set Union

Functionality



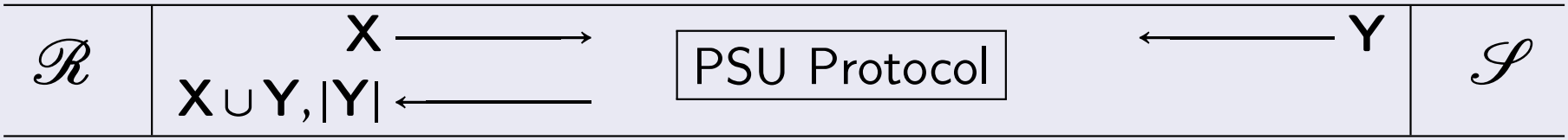
Security

In the honest-but-curious adversary model:

- $\mathscr{S}$ learns nothing about **X**.

Unbalanced Private Set Union

Functionality



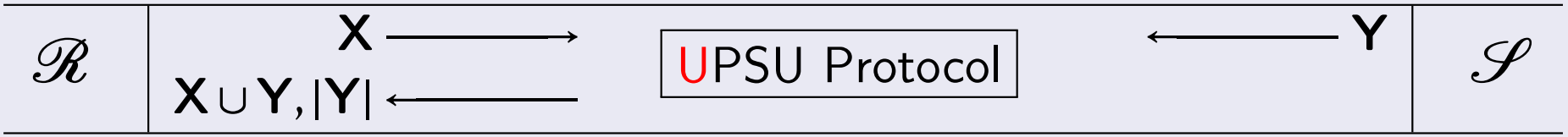
Security

In the honest-but-curious adversary model:

- $\mathscr{S}$ learns nothing about $\mathbf{X}$.
- $\mathscr{R}$ learns only $\mathbf{X} \cup \mathbf{Y}$ and $|\mathbf{Y}|$.

Unbalanced Private Set Union

Functionality



Security

In the honest-but-curious adversary model:

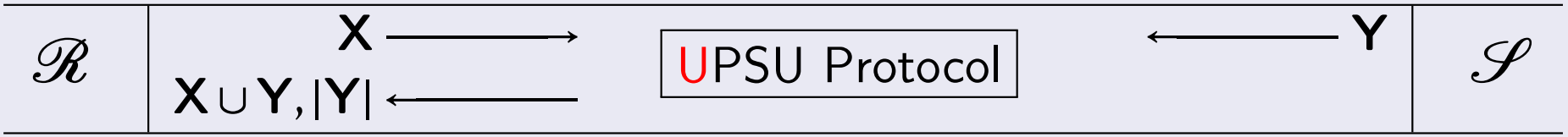
- $\mathscr{S}$ learns nothing about $\mathbf{X}$.
- $\mathscr{R}$ learns only $\mathbf{X} \cup \mathbf{Y}$ and $|\mathbf{Y}|$.

Unbalanced situation goals

$|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$ (possibly $n \gg m$)

Unbalanced Private Set Union

Functionality



Security

In the honest-but-curious adversary model:

- $\mathscr{S}$ learns nothing about $\mathbf{X}$.
- $\mathscr{R}$ learns only $\mathbf{X} \cup \mathbf{Y}$ and $|\mathbf{Y}|$.

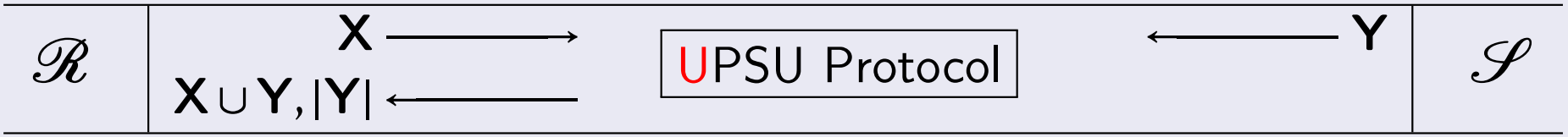
Unbalanced situation goals

$|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$ (possibly $n \gg m$)

- Communication volume proportional to m.

Unbalanced Private Set Union

Functionality



Security

In the honest-but-curious adversary model:

- $\mathscr{S}$ learns nothing about $\mathbf{X}$.
- $\mathscr{R}$ learns only $\mathbf{X} \cup \mathbf{Y}$ and $|\mathbf{Y}|$.

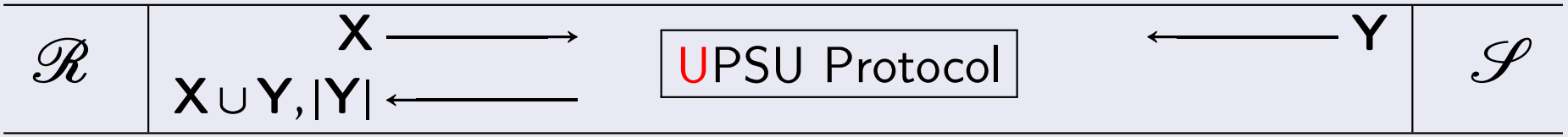
Unbalanced situation goals

$|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$ (possibly $n \gg m$)

- Communication volume proportional to m.
- Arithmetic cost for $\mathscr{S}$ independant from n.

Unbalanced Private Set Union

Functionality



Security

In the honest-but-curious adversary model:

- $\mathscr{S}$ learns nothing about $\mathbf{X}$.
- $\mathscr{R}$ learns only $\mathbf{X} \cup \mathbf{Y}$ and $|\mathbf{Y}|$.

Unbalanced situation goals

$|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$ (possibly $n \gg m$)

- Communication volume proportional to m.
- Arithmetic cost for $\mathscr{S}$ independant from n.
- Arithmetic cost for $\mathscr{R}$ reasonable.

State of the art

Notations

- $\mathscr{R}$ owns $\mathbf{X} \subset \mathbb{F}$, $|\mathbf{X}| = n$.
- $\mathscr{S}$ owns $\mathbf{Y} \subset \mathbb{F}$, $|\mathbf{Y}| = m$.
- $n \gg m$.
- Comm. Vol. : "number of field element sent".
- Arith. Cost : "number of field operations".

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.

$$\rightsquigarrow \mathbf{X} \longleftrightarrow P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x)$$

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.

$$\rightsquigarrow \mathbf{X} \longleftrightarrow P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x)$$

$$\rightsquigarrow \widehat{P_{\mathbf{X}}}(y) = \widehat{0} \Leftrightarrow y \in \mathbf{X}$$

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.

$$\rightsquigarrow \mathbf{X} \longleftrightarrow P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x)$$

$$\rightsquigarrow \widehat{P_{\mathbf{X}}}(y) = \widehat{0} \Leftrightarrow y \in \mathbf{X}$$

$$\rightsquigarrow \left(y \ltimes_L \widehat{P_{\mathbf{X}}}(y), \widehat{P_{\mathbf{X}}}(y) \right) \Rightarrow \begin{cases} y, \text{ if } y \notin \mathbf{X} \\ 0, \text{ if } y \in \mathbf{X} \end{cases}$$

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.

$$\rightsquigarrow \mathbf{X} \longleftrightarrow P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x)$$

$$\rightsquigarrow \widehat{P_{\mathbf{X}}}(y) = \widehat{0} \Leftrightarrow y \in \mathbf{X}$$

$$\rightsquigarrow \left(y \ltimes_L \widehat{P_{\mathbf{X}}}(y), \widehat{P_{\mathbf{X}}}(y) \right) \Rightarrow \begin{cases} y, \text{ if } y \notin \mathbf{X} \\ 0, \text{ if } y \in \mathbf{X} \end{cases}$$

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$
Frikken	$O(n)$	$O(nm)$	$O(n^{1+\epsilon})$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.
- **[Davidson and Cid, 2017]**: Bloom filter set representation and LHE sum.

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$
Frikken	$O(n)$	$O(nm)$	$O(n^{1+\epsilon})$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.
- **[Davidson and Cid, 2017]**: Bloom filter set representation and LHE sum.

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$
Frikken	$O(n)$	$O(nm)$	$O(n^{1+\epsilon})$
Dav. & Cid	$O(n)$	$O(m)$	$O(n)$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.
- **[Davidson and Cid, 2017]**: Bloom filter set representation and LHE sum.
- **[Zhang et al., 2023]**: Indexing intersection and oblivious transfer.

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$
Frikken	$O(n)$	$O(nm)$	$O(n^{1+\epsilon})$
Dav. & Cid	$O(n)$	$O(m)$	$O(n)$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.
- **[Davidson and Cid, 2017]**: Bloom filter set representation and LHE sum.
- **[Zhang et al., 2023]**: Indexing intersection and oblivious transfer.

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$
Frikken	$O(n)$	$O(nm)$	$O(n^{1+\epsilon})$
Dav. & Cid	$O(n)$	$O(m)$	$O(n)$
Zhang et al.	$O(n)$	$O(m \log n)$	$O(n)$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.
- **[Davidson and Cid, 2017]**: Bloom filter set representation and LHE sum.
- **[Zhang et al., 2023]**: Indexing intersection and oblivious transfer.
- **[Tu et al., 2023]**: Partitioned FHE polynomial evaluation and oblivious transfer.

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$
Frikken	$O(n)$	$O(nm)$	$O(n^{1+\epsilon})$
Dav. & Cid	$O(n)$	$O(m)$	$O(n)$
Zhang et al.	$O(n)$	$O(m \log n)$	$O(n)$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.
- **[Davidson and Cid, 2017]**: Bloom filter set representation and LHE sum.
- **[Zhang et al., 2023]**: Indexing intersection and oblivious transfer.
- **[Tu et al., 2023]**: Partitioned FHE polynomial evaluation and oblivious transfer.

⚠Partitioning ⇒ leaky protocol...

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$
Frikken	$O(n)$	$O(nm)$	$O(n^{1+\epsilon})$
Dav. & Cid	$O(n)$	$O(m)$	$O(n)$
Zhang et al.	$O(n)$	$O(m \log n)$	$O(n)$

State of the art

Main ideas in different protocols

- **[Frikken, 2007]**: Polynomial set representation and LHE evaluation.
- **[Davidson and Cid, 2017]**: Bloom filter set representation and LHE sum.
- **[Zhang et al., 2023]**: Indexing intersection and oblivious transfer.
- **[Tu et al., 2023]**: Partitioned FHE polynomial evaluation and oblivious transfer.

⚠Partitioning ⇒ leaky protocol...

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$
Frikken	$O(n)$	$O(nm)$	$O(n^{1+\epsilon})$
Dav. & Cid	$O(n)$	$O(m)$	$O(n)$
Zhang et al.	$O(n)$	$O(m \log n)$	$O(n)$
Tu et al.	$O(m \log n)$	$O(m^{1+\epsilon})$	$O(n^{1+\epsilon})$

Table of Contents

Construction of our protocol

Notations

- $\mathscr{R}$ owns $\mathbf{X} \subset \mathbb{F}$, $\mathscr{S}$ owns $\mathbf{Y} \subset \mathbb{F}$.
- $|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$.

Construction of our protocol

Notations

- $\mathscr{R}$ owns $\mathbf{X} \subset \mathbb{F}$, $\mathscr{S}$ owns $\mathbf{Y} \subset \mathbb{F}$.
- $|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$.

4 main ideas

- Polynomial set representation.

Construction of our protocol

Notations

- $\mathscr{R}$ owns $\mathbf{X} \subset \mathbb{F}$, $\mathscr{S}$ owns $\mathbf{Y} \subset \mathbb{F}$.
- $|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$.

4 main ideas

- Polynomial set representation.

$$P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x); \; P_{\mathbf{Y}}(Z) = \prod_{y \in \mathbf{Y}} (Z - y);$$

Construction of our protocol

Notations

- $\mathscr{R}$ owns $\mathbf{X} \subset \mathbb{F}$, $\mathscr{S}$ owns $\mathbf{Y} \subset \mathbb{F}$.
- $|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$.

4 main ideas

- Polynomial set representation.

$$P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x); \; P_{\mathbf{Y}}(Z) = \prod_{y \in \mathbf{Y}} (Z - y);$$

- Degree reduction : FHE remainder.

Construction of our protocol

Notations

- $\mathscr{R}$ owns $\mathbf{X} \subset \mathbb{F}$, $\mathscr{S}$ owns $\mathbf{Y} \subset \mathbb{F}$.
- $|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$.

4 main ideas

- Polynomial set representation.

$$P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x); \; P_{\mathbf{Y}}(Z) = \prod_{y \in \mathbf{Y}} (Z - y);$$

- Degree reduction : FHE remainder.

$$\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}; \; (\deg(R) < m)$$

Construction of our protocol

Notations

- $\mathscr{R}$ owns $\mathbf{X} \subset \mathbb{F}$, $\mathscr{S}$ owns $\mathbf{Y} \subset \mathbb{F}$.
- $|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$.

4 main ideas

- Polynomial set representation.

$$P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x); \; P_{\mathbf{Y}}(Z) = \prod_{y \in \mathbf{Y}} (Z - y);$$

- Degree reduction : FHE remainder.

$$\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}; \; (\deg(R) < m)$$

- Security and bridge between FHE and LHE : random masking.

Construction of our protocol

Notations

- $\mathscr{R}$ owns $\mathbf{X} \subset \mathbb{F}$, $\mathscr{S}$ owns $\mathbf{Y} \subset \mathbb{F}$.
- $|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$.

4 main ideas

- Polynomial set representation.

$$P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x); \; P_{\mathbf{Y}}(Z) = \prod_{y \in \mathbf{Y}} (Z - y);$$

- Degree reduction : FHE remainder.

$$\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}; \; (\deg(R) < m)$$

- Security and bridge between FHE and LHE : random masking.

$$\widetilde{H} \leftarrow \widetilde{R} +_F \widetilde{M}; \; \widehat{M}; \; (\deg(M) = m - 1)$$

Construction of our protocol

Notations

- $\mathscr{R}$ owns $\mathbf{X} \subset \mathbb{F}$, $\mathscr{S}$ owns $\mathbf{Y} \subset \mathbb{F}$.
- $|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$.

4 main ideas

- Polynomial set representation.

$$P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x); \; P_{\mathbf{Y}}(Z) = \prod_{y \in \mathbf{Y}} (Z - y);$$

- Degree reduction : FHE remainder.

$$\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}; \; (\deg(R) < m)$$

- Security and bridge between FHE and LHE : random masking.

$$\widetilde{H} \leftarrow \widetilde{R} +_F \widetilde{M}; \; \widehat{M}; \; (\deg(M) = m - 1)$$

- LHE multi-point evaluation.

Construction of our protocol

Notations

- $\mathscr{R}$ owns $\mathbf{X} \subset \mathbb{F}$, $\mathscr{S}$ owns $\mathbf{Y} \subset \mathbb{F}$.
- $|\mathbf{X}| = n$, $|\mathbf{Y}| = m$, $n \geq m$.

4 main ideas

- Polynomial set representation.

$$P_{\mathbf{X}}(Z) = \prod_{x \in \mathbf{X}} (Z - x); \; P_{\mathbf{Y}}(Z) = \prod_{y \in \mathbf{Y}} (Z - y);$$

- Degree reduction : FHE remainder.

$$\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}; \; (\deg(R) < m)$$

- Security and bridge between FHE and LHE : random masking.

$$\widetilde{H} \leftarrow \widetilde{R} +_F \widetilde{M}; \; \widehat{M}; \; (\deg(M) = m - 1)$$

- LHE multi-point evaluation.

$$\widehat{R}(y) = \widehat{0} \Leftrightarrow y \in \mathbf{X};$$

Optimal communication UPSU protocol

$\mathscr{R}$ $(\mathbf{X} = \{x_1, ..., x_n\}, pk_F, sk_L, pk_L)$

$P_{\mathbf{X}} = \prod(Z - x_i)$

$\mathscr{S}$ $(\mathbf{Y} = \{y_1, ..., y_m\}, pk_L, sk_F, pk_F)$

$P_{\mathbf{Y}} = \prod(Z - y_i)$

Optimal communication UPSU protocol

$\mathscr{R}$ $(\mathbf{X} = \{x_1, ..., x_n\}, pk_F, sk_L, pk_L)$		$\mathscr{S}$ $(\mathbf{Y} = \{y_1, ..., y_m\}, pk_L, sk_F, pk_F)$
$P_{\mathbf{X}} = \prod(Z - x_i)$		$P_{\mathbf{Y}} = \prod(Z - y_i)$
	$\xleftarrow{\widetilde{P_{\mathbf{Y}}}}$	$\widetilde{P_{\mathbf{Y}}} \leftarrow F.E_{pk_F}(P_{\mathbf{Y}})$

Optimal communication UPSU protocol

$\mathscr{R}$ $(\mathbf{X} = \{x_1, ..., x_n\}, pk_F, sk_L, pk_L)$

$P_{\mathbf{X}} = \prod(Z - x_i)$

$\mathscr{S}$ $(\mathbf{Y} = \{y_1, ..., y_m\}, pk_L, sk_F, pk_F)$

$P_{\mathbf{Y}} = \prod(Z - y_i)$

$\widetilde{P_{\mathbf{Y}}} \leftarrow F.E_{pk_F}(P_{\mathbf{Y}})$

$\widetilde{P_{\mathbf{Y}}}$ ⟵

$\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}$

Optimal communication UPSU protocol

$\mathscr{R}$ $(\mathbf{X} = \{x_1, ..., x_n\}, pk_F, sk_L, pk_L)$		$\mathscr{S}$ $(\mathbf{Y} = \{y_1, ..., y_m\}, pk_L, sk_F, pk_F)$
$P_{\mathbf{X}} = \prod(Z - x_i)$		$P_{\mathbf{Y}} = \prod(Z - y_i)$
M random mask	$\xleftarrow{\widetilde{P_{\mathbf{Y}}}}$	$\widetilde{P_{\mathbf{Y}}} \leftarrow F.E_{pk_F}(P_{\mathbf{Y}})$
$\widehat{M} \leftarrow L.E_{pk_L}(M)$		
$\widetilde{M} \leftarrow F.E_{pk_F}(M)$		
$\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}$		
$\widetilde{H} \leftarrow \widetilde{R} +_F \widetilde{M}$	$\xrightarrow{\widetilde{H}, \widehat{M}}$	

Optimal communication UPSU protocol

$\mathscr{R}$ $(\mathbf{X} = \{x_1, ..., x_n\}, pk_F, sk_L, pk_L)$		$\mathscr{S}$ $(\mathbf{Y} = \{y_1, ..., y_m\}, pk_L, sk_F, pk_F)$
$P_{\mathbf{X}} = \prod(Z - x_i)$		$P_{\mathbf{Y}} = \prod(Z - y_i)$
M random mask	$\xleftarrow{\widetilde{P_{\mathbf{Y}}}}$	$\widetilde{P_{\mathbf{Y}}} \leftarrow F.E_{pk_F}(P_{\mathbf{Y}})$
$\widehat{M} \leftarrow L.E_{pk_L}(M)$ $\widetilde{M} \leftarrow F.E_{pk_F}(M)$ $\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}$		
$\widetilde{H} \leftarrow \widetilde{R} +_F \widetilde{M}$	$\xrightarrow{\widetilde{H}, \widehat{M}}$	$H = R + M \leftarrow F.D_{sk_F}(\widetilde{H})$ $\{h_i\} \leftarrow MEv(H, \mathbf{Y})$ $\{\widehat{m_i}\} \leftarrow MEv_L(\widehat{M}, \mathbf{Y})$

Optimal communication UPSU protocol

$\mathscr{R}$ $(\mathbf{X} = \{x_1, ..., x_n\}, pk_F, sk_L, pk_L)$		$\mathscr{S}$ $(\mathbf{Y} = \{y_1, ..., y_m\}, pk_L, sk_F, pk_F)$
$P_{\mathbf{X}} = \prod(Z - x_i)$		$P_{\mathbf{Y}} = \prod(Z - y_i)$
M random mask	$\xleftarrow{\widetilde{P_{\mathbf{Y}}}}$	$\widetilde{P_{\mathbf{Y}}} \leftarrow F.E_{pk_F}(P_{\mathbf{Y}})$
$\widehat{M} \leftarrow L.E_{pk_L}(M)$ $\widetilde{M} \leftarrow F.E_{pk_F}(M)$ $\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}$		
$\widetilde{H} \leftarrow \widetilde{R} +_F \widetilde{M}$	$\xrightarrow{\widetilde{H}, \widehat{M}}$	$H = R + M \leftarrow F.D_{sk_F}(\widetilde{H})$ $\{h_i\} \leftarrow MEv(H, \mathbf{Y})$ $\{\widehat{m_i}\} \leftarrow MEv_L(\widehat{M}, \mathbf{Y})$ $\{\widehat{r_i}\} \leftarrow \{\widehat{h_i} -_L \widehat{m_i}\}$

Optimal communication UPSU protocol

$\mathscr{R}$ $(\mathbf{X}=\{x_1,...,x_n\}, pk_F, sk_L, pk_L)$		$\mathscr{S}$ $(\mathbf{Y}=\{y_1,...,y_m\}, pk_L, sk_F, pk_F)$
$P_{\mathbf{X}} = \prod(Z - x_i)$		$P_{\mathbf{Y}} = \prod(Z - y_i)$
M random mask	$\xleftarrow{\widetilde{P_{\mathbf{Y}}}}$	$\widetilde{P_{\mathbf{Y}}} \leftarrow F.E_{pk_F}(P_{\mathbf{Y}})$
$\widehat{M} \leftarrow L.E_{pk_L}(M)$ $\widetilde{M} \leftarrow F.E_{pk_F}(M)$ $\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}$		
$\widetilde{H} \leftarrow \widetilde{R} +_F \widetilde{M}$	$\xrightarrow{\widetilde{H}, \widehat{M}}$	$H = R + M \leftarrow F.D_{sk_F}(\widetilde{H})$
		$\{h_i\} \leftarrow MEv(H, \mathbf{Y})$
		$\{\widehat{m_i}\} \leftarrow MEv_L(\widehat{M}, \mathbf{Y})$
		$\{\widehat{r_i}\} \leftarrow \{\widehat{h_i} -_L \widehat{m_i}\}$
		$\{\widehat{\rho_i}\} \leftarrow \{y_i \ltimes_L \widehat{r_i}\}$

Optimal communication UPSU protocol

$\mathscr{R}$ $(\mathbf{X}=\{x_1,...,x_n\}, pk_F, sk_L, pk_L)$		$\mathscr{S}$ $(\mathbf{Y}=\{y_1,...,y_m\}, pk_L, sk_F, pk_F)$
$P_{\mathbf{X}} = \prod(Z - x_i)$		$P_{\mathbf{Y}} = \prod(Z - y_i)$
M random mask	$\xleftarrow{\widetilde{P_{\mathbf{Y}}}}$	$\widetilde{P_{\mathbf{Y}}} \leftarrow F.E_{pk_F}(P_{\mathbf{Y}})$
$\widehat{M} \leftarrow L.E_{pk_L}(M)$ $\widetilde{M} \leftarrow F.E_{pk_F}(M)$ $\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}$		
$\widetilde{H} \leftarrow \widetilde{R} +_F \widetilde{M}$	$\xrightarrow{\widetilde{H}, \widehat{M}}$	$H = R + M \leftarrow F.D_{sk_F}(\widetilde{H})$
		$\{h_i\} \leftarrow MEv(H, \mathbf{Y})$
		$\{\widehat{m_i}\} \leftarrow MEv_L(\widehat{M}, \mathbf{Y})$
		$\{\widehat{r_i}\} \leftarrow \{\widehat{h_i} -_L \widehat{m_i}\}$
	$\xleftarrow{\{(\widehat{r_i}, \widehat{\rho_i})\}}$	$\{\widehat{\rho_i}\} \leftarrow \{y_i \ltimes_L \widehat{r_i}\}$

Optimal communication UPSU protocol

$\mathscr{R}$ $(\mathbf{X}=\{x_1,...,x_n\}, pk_F, sk_L, pk_L)$		$\mathscr{S}$ $(\mathbf{Y}=\{y_1,...,y_m\}, pk_L, sk_F, pk_F)$
$P_{\mathbf{X}} = \prod(Z - x_i)$		$P_{\mathbf{Y}} = \prod(Z - y_i)$
M random mask	$\xleftarrow{\widetilde{P_{\mathbf{Y}}}}$	$\widetilde{P_{\mathbf{Y}}} \leftarrow F.E_{pk_F}(P_{\mathbf{Y}})$
$\widehat{M} \leftarrow L.E_{pk_L}(M)$ $\widetilde{M} \leftarrow F.E_{pk_F}(M)$ $\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}$		
$\widetilde{H} \leftarrow \widetilde{R} +_F \widetilde{M}$	$\xrightarrow{\widetilde{H}, \widehat{M}}$	$H = R + M \leftarrow F.D_{sk_F}(\widetilde{H})$
		$\{h_i\} \leftarrow MEv(H, \mathbf{Y})$ $\{\widehat{m_i}\} \leftarrow MEv_L(\widehat{M}, \mathbf{Y})$ $\{\widehat{r_i}\} \leftarrow \{\widehat{h_i} -_L \widehat{m_i}\}$
$\{(r_i, \rho_i)\} \leftarrow \{L.D_{sk_L}(\widehat{r_i}, \widehat{\rho_i})\}$	$\xleftarrow{\{(\widehat{r_i}, \widehat{\rho_i})\}}$	$\{\widehat{\rho_i}\} \leftarrow \{y_i \ltimes_L \widehat{r_i}\}$

Optimal communication UPSU protocol

$\mathscr{R}$ $(\mathbf{X}=\{x_1,...,x_n\}, pk_F, sk_L, pk_L)$		$\mathscr{S}$ $(\mathbf{Y}=\{y_1,...,y_m\}, pk_L, sk_F, pk_F)$
$P_{\mathbf{X}} = \prod(Z - x_i)$		$P_{\mathbf{Y}} = \prod(Z - y_i)$
M random mask	$\xleftarrow{\widetilde{P_{\mathbf{Y}}}}$	$\widetilde{P_{\mathbf{Y}}} \leftarrow F.E_{pk_F}(P_{\mathbf{Y}})$
$\widehat{M} \leftarrow L.E_{pk_L}(M)$ $\widetilde{M} \leftarrow F.E_{pk_F}(M)$ $\widetilde{R} \leftarrow \widetilde{P_{\mathbf{X}}} \%_F \widetilde{P_{\mathbf{Y}}}$		
$\widetilde{H} \leftarrow \widetilde{R} +_F \widetilde{M}$	$\xrightarrow{\widetilde{H}, \widehat{M}}$	$H = R + M \leftarrow F.D_{sk_F}(\widetilde{H})$
		$\{h_i\} \leftarrow MEv(H, \mathbf{Y})$ $\{\widehat{m_i}\} \leftarrow MEv_L(\widehat{M}, \mathbf{Y})$ $\{\widehat{r_i}\} \leftarrow \{\widehat{h_i} -_L \widehat{m_i}\}$
$\{(r_i, \rho_i)\} \leftarrow \{L.D_{sk_L}(\widehat{r_i}, \widehat{\rho_i})\}$	$\xleftarrow{\{(\widehat{r_i}, \widehat{\rho_i})\}}$	$\{\widehat{\rho_i}\} \leftarrow \{y_i \ltimes_L \widehat{r_i}\}$
$\begin{cases} r_i = 0 & \Rightarrow \perp \\ r_i \neq 0 & \Rightarrow y_i = \rho_i r_i^{-1} \end{cases}$		

Table of Contents

Comparison to the state of the art

Our protocol Asymptotic

- Communication volume : $O(m)$.
- Arithmetic cost for $\mathscr{S}$: $\mathscr{M}_L(m)\log m + \tilde{O}(m) \in O(m^{1+\epsilon})$.
- Arithmetic cost for $\mathscr{R}$: $\frac{9}{2}\mathscr{M}_F(n-m) + O(n) \in O(n^{1+\epsilon})$.

Comparison to the state of the art

Our protocol Asymptotic

- Communication volume : $O(m)$.
- Arithmetic cost for $\mathscr{S}$: $\mathscr{M}_L(m)\log m + \tilde{O}(m) \in O(m^{1+\epsilon})$.
- Arithmetic cost for $\mathscr{R}$: $\frac{9}{2}\mathscr{M}_F(n-m) + O(n) \in O(n^{1+\epsilon})$.

	Comm. Vol.	Arith. Cost $\mathscr{S}$	Arith. Cost $\mathscr{R}$	Security
Frikken	$O(n)$	$O(nm)$	$O(n^{1+\epsilon})$	✓
Dav. & Cid	$O(n)$	$O(m)$	$O(n)$	✓
Zhang et al.	$O(n)$	$O(m\log n)$	$O(n)$	✓
Tu et al.	$O(m\log n)$	$O(m^{1+\epsilon})$	$O(n^{1+\epsilon})$	leaky
Ours	$O(m)$	$O(m^{1+\epsilon})$	$O(n^{1+\epsilon})$	✓

References

Bostan, A., Lecerf, G., and Schost, É. (2003).
Tellegen's principle into practice.
In *Symbolic and Algebraic Computation, International Symposium ISSAC 2003, Drexel University, Philadelphia, Pennsylvania, USA, August 3-6, 2003, Proceedings*.

Davidson, A. and Cid, C. (2017).
An efficient toolkit for computing private set operations.
In *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3-5, 2017, Proceedings, Part II*.

Frikken, K. B. (2007).
Privacy-preserving set union.
In *Applied Cryptography and Network Security, 5th International Conference, ACNS 2007, Zhuhai, China, June 5-8, 2007, Proceedings*.

Tu, B., Chen, Y., Liu, Q., and Zhang, C. (2023).
Fast unbalanced private set union from fully homomorphic encryption.
In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023, Copenhagen, Denmark, November 26-30, 2023*.

Zhang, C., Chen, Y., Liu, W., Zhang, M., and Lin, D. (2023).
Linear private set union from multi-query reverse private membership test.
In *32nd USENIX Security Symposium, USENIX Security 2023, Anaheim, CA, USA, August 9-11, 2023*.


Thank you for your attention !
Any question ?