EUROCRYPT 2025

Efficient Multiparty Private Simultaneous Messages for Symmetric Functions

May 6, 2025

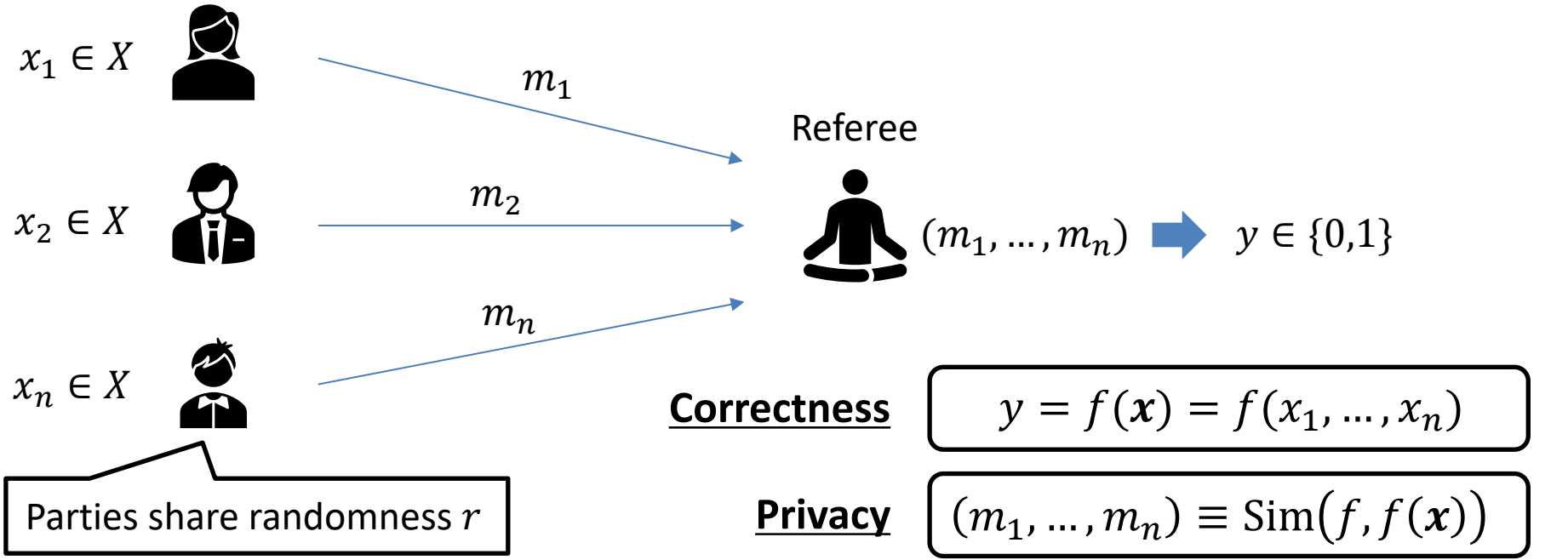
Reo Eriguchi,[1] Kazumasa Shinagawa[2,1]

1. AIST, Japan

2. University of Tsukuba, Japan

Private Simultaneous Messages (PSM) [FKN94]

- $f : X^n \to \{0,1\}$



Correctness $y = f(\boldsymbol{x}) = f(x_1, \dots, x_n)$

Privacy $(m_1, \dots, m_n) \equiv \mathrm{Sim}\big(f, f(\boldsymbol{x})\big)$

- Applications: Two-round MPC, CDS, general secret sharing

General Functions

- $f : X^n \to \{0,1\},\ X = \{1,2,\dots,d\}$
- Communication complexity := bit-length of $(m_1, \dots, m_n)$

Scheme	Communication (worst-case)
[FKN94] (truth-table), [IK97] (branching program), [AIK11] (circuit)	$d^n \cdot \mathrm{poly}(n,d)$
[BKN18]	$d^{n/2} \cdot n^3$
[AL21]	$d^{(n-1)/2} \cdot 2^{O(n)}$

Representation size: d^n bits

General Functions

- $f : X^n \to \{0,1\},\ X = \{1,2,\dots,d\}$
- Communication complexity := bit-length of $(m_1, \dots, m_n)$

Scheme	Communication (worst-case)
[FKN94] (truth-table), [IK97] (branching program), [AIK11] (circuit)	$d^n \cdot \mathrm{poly}(n,d)$
[BKN18]	$d^{n/2} \cdot n^3$
[AL21]	$d^{(n-1)/2} \cdot 2^{O(n)}$

Representation size: d^n bits

Breaking representation-size barrier

General Functions

- $f : X^n \to \{0,1\},\ X = \{1,2,\dots,d\}$
- Communication complexity := bit-length of $(m_1, \dots, m_n)$

Scheme	Communication (worst-case)
[FKN94] (truth-table), [IK97] (branching program), [AIK11] (circuit)	$d^n \cdot \mathrm{poly}(n,d)$
[BKN18]	$d^{n/2} \cdot n^3$
[AL21]	$d^{(n-1)/2} \cdot 2^{O(n)}$

Representation size: d^n bits

Breaking representation-size barrier

However, communication is still exponential in n.

Can we construct efficient protocols by focusing on special functions of practical use?

Symmetric Functions

- $f : X^n \to \{0,1\}$ is *symmetric* if $f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right) = f(x_1, \dots, x_n)$ for all permutation σ.

Example statistics, threshold functions

Scheme	Communication (worst-case)
[BKN18]	$d^{n/2} \cdot n^3$
[AL21]	$d^{(n-1)/2} \cdot 2^{O(n)}$
[BKR17]	$n^{d \log n} \cdot n^{O(1)}$
[BGI+14]	$O\left(n^{2d+1}\right)$
[EOYN21]	$O(n^d d^2 \log n)$

More efficient than general PSM if $n \gg d$

Symmetric Functions

- $f : X^n \to \{0,1\}$ is *symmetric* if $f\left(x_{\sigma(1)}, \dots, x_{\sigma(n)}\right) = f(x_1, \dots, x_n)$ for all permutation σ.

Example statistics, threshold functions

Representation size $\approx n^d$ bits

Scheme	Communication (worst-case)
[BKN18]	$d^{n/2} \cdot n^3$
[AL21]	$d^{(n-1)/2} \cdot 2^{O(n)}$
[BKR17]	$n^{d \log n} \cdot n^{O(1)}$
[BGI+14]	$O\left(n^{2d+1}\right)$
[EOYN21]	$O(n^d d^2 \log n)$
?	$O(n^{cd})$ for $c < 1$

More efficient than general PSM if $n \gg d$

Question Can we break the representation-size barrier for symmetric f?

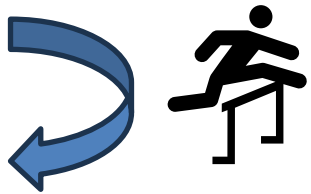
Our Results

Can we break the representation-size barrier for symmetric f?

Yes!

Representation size $\approx n^d$ bits

Scheme	Communication (worst-case)
[BKN18]	$d^{n/2} \cdot n^3$
[AL21]	$d^{(n-1)/2} \cdot 2^{O(n)}$
[BKR17]	$n^{d \log n + O(1)}$
[BGI+14]	$O(n^{2d+1})$
[EOYN21]	$O(n^d d^2 \log n)$
This work	$n^{2d/3+O(1)}$



- New decomposition techniques based on the symmetry of f
- Byproduct: PSM for symmetric f with *universal reconstruction*
- Extension to related models: *robust* PSM and *ad-hoc* PSM.

Our Techniques

- $f : [d]^n \to \{0,1\}$: symmetric function
- **New decomposition approach**

Referee cannot learn functions,
i.e., $(m_1, \dots, m_n) \equiv \mathrm{Sim}\big(n, d, f(\boldsymbol{x})\big)$

PSM for f → PSM for smaller symmetric functions with *universal reconstruction*

$g : [d/3]^n \to \{0,1\}$ $\times\, O(n^{d/3})$ $\quad$ $h : [2d/3]^n \to \{0,1\}$ $\times\, O(1)$

- Our approach is "orthogonal" to previous ones.

[BKN18, AL21]: PSM for f → PSM for smaller g's

$g : [d]^m \to \{0,1\}$ for $m < n$

Our Techniques

- **<u>New PSM with universal reconstruction</u>**

  If the domain is $[d_0]^n$, it has communication complexity of $O(n^{d_0})$.

  ✓ Improving existing PSM with universal reconstruction [BGI+14,EOYN21].

  ✓ Almost optimal: We show an almost matching lower bound $\Omega(n^{d_0-1})$.

- The total communication complexity is

$$O(n^{d/3}) \times O\left(n^{d/3}\right) + O(n^{2d/3}) \times O(1) = O(n^{2d/3}).$$

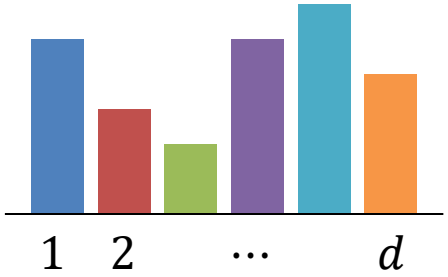
$g : [d/3]^n \to \{0,1\}$ $\times O(n^{d/3})$

$h : [2d/3]^n \to \{0,1\}$ $\times O(1)$

Technical Details

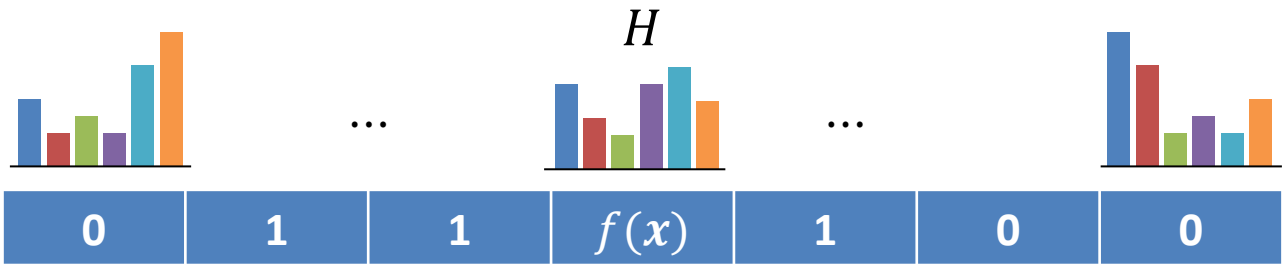
Representation

- $f : [d]^n \to \{0,1\}$: symmetric function
- $f(\boldsymbol{x})$ is determined by a *histogram*

$H =$ 

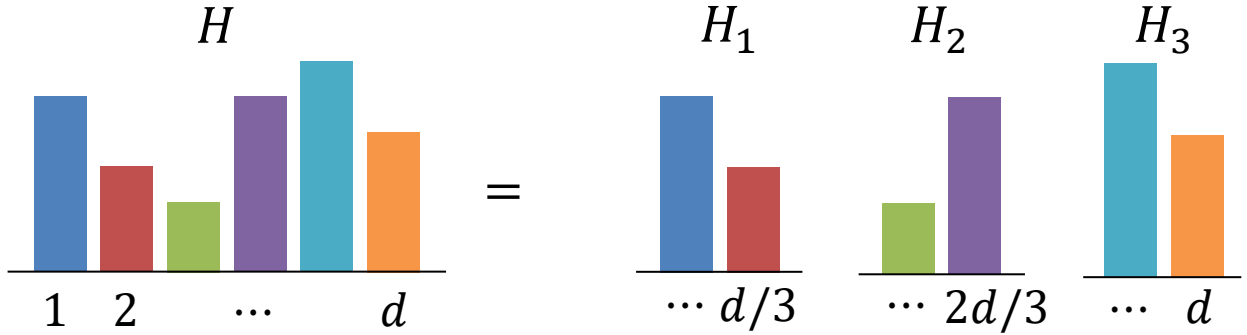
$$H(j) = \#\{i \in [n] : x_i = j\}$$

- f can be represented by one-dimensional array of length $\binom{n+d-1}{d-1} \lesssim n^d$

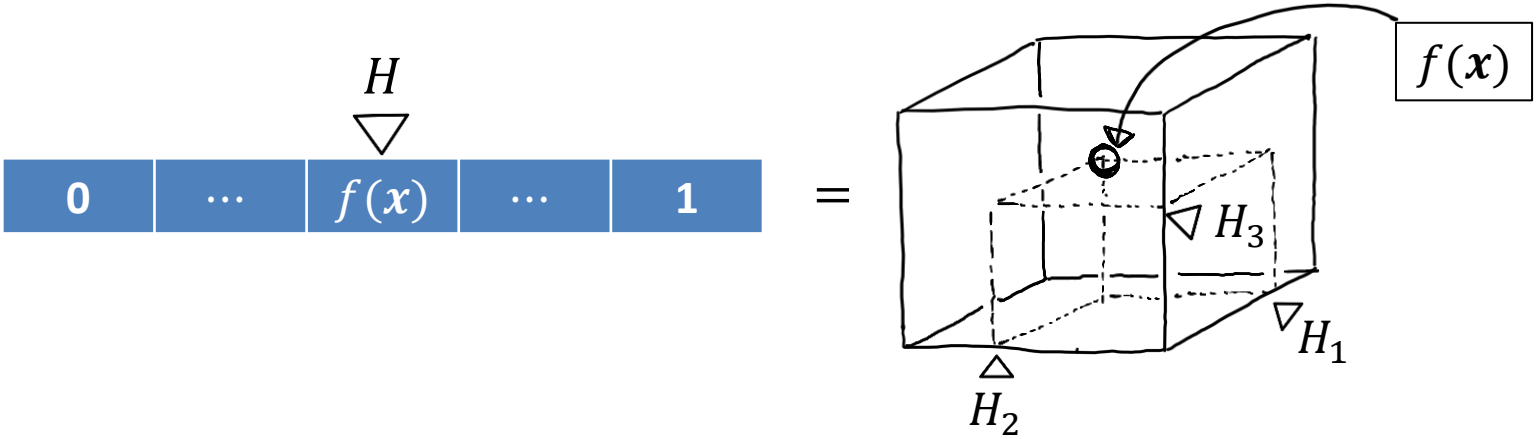


Decomposition

- Decompose H into three sub-histograms.



- f can be represented by a three-dimensional *cube*.



Decomposition

- Computing f can be reduced to computing a three-dimensional tensor T.

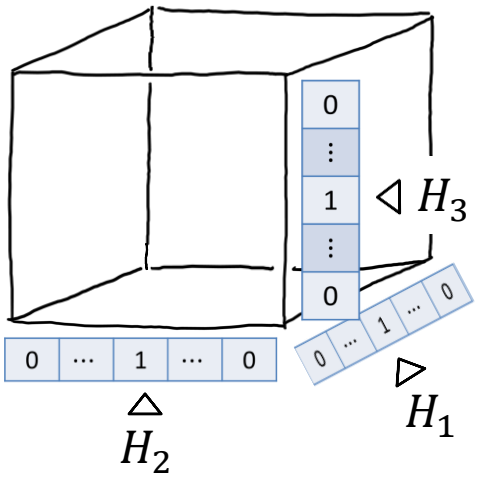
$$f(\boldsymbol{x}) =$$

0	⋯	$f(x)$	⋯	1

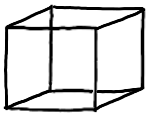
0
⋮
1
⋮
0

H

$=$



$= T(\boldsymbol{e}_{H_1}, \boldsymbol{e}_{H_2}, \boldsymbol{e}_{H_3})$

T : tensor corresponding to 

Our PSM

1. Parties send three vectors that mask $\boldsymbol{e}_{H_1}, \boldsymbol{e}_{H_2}$, and $\boldsymbol{e}_{H_3}$.

$$\boldsymbol{v}_i = \boldsymbol{e}_{H_i} + \boldsymbol{r}_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \begin{bmatrix} \$ \\ \vdots \\ \$ \\ \vdots \\ \$ \end{bmatrix} = \begin{bmatrix} v_i[1] \\ \vdots \\ \vdots \\ \vdots \\ v_i[O(n^{d/3})] \end{bmatrix}$$

Determined by H_i (and $\boldsymbol{r}_i$ hardwired to a function)
→ a symmetric function with domain $[d/3]^n$

Note
We need *universal reconstruction* to keep $\boldsymbol{r}_i$ hidden from Referee.

⇒ Requires $O(n^{d/3})$ executions of PSM w/ universal reconstruction for $g : [d/3]^n \to \{0,1\}$

Communication: $O(n^{d/3}) \cdot O(n^{d/3}) = O(n^{2d/3})$

Our PSM

2. As Referee knows T, he can compute

$$T(\boldsymbol{v}_1, \boldsymbol{v}_2, \boldsymbol{v}_3) = \underbrace{T\left(\boldsymbol{e}_{H_1}, \boldsymbol{e}_{H_2}, \boldsymbol{e}_{H_3}\right)}_{= f(\boldsymbol{x})} + \sum T\left(\boldsymbol{e}_{H_1}, \boldsymbol{e}_{H_2}, \boldsymbol{r}_3\right) + \sum T\left(\boldsymbol{e}_{H_1}, \boldsymbol{r}_2, \boldsymbol{r}_3\right)$$

$T\left(\boldsymbol{e}_{H_1}, \boldsymbol{e}_{H_2}, \boldsymbol{r}_3\right)$ is determined by H_1, H_2 (and common $\boldsymbol{r}_3$)

→ a symmetric function with domain $[2d/3]^n$

$T\left(\boldsymbol{e}_{H_1}, \boldsymbol{r}_2, \boldsymbol{r}_3\right)$ is determined by H_1 (and common $\boldsymbol{r}_2, \boldsymbol{r}_3$)

→ a symmetric function with domain $[d/3]^n$

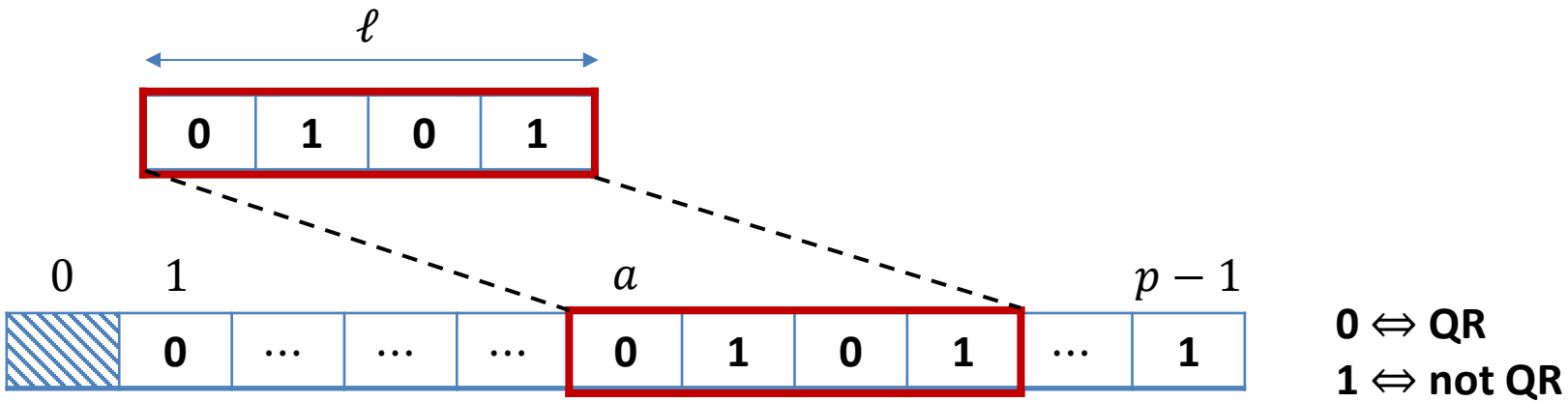
⇨ Requires $O(1)$ executions of PSM w/ universal reconstruction for $h : [2d/3]^n \to \{0,1\}$

Communication: $O(1) \cdot O\left(n^{2d/3}\right) = O\left(n^{2d/3}\right)$

Our PSM w/ Universal Reconstruction

- Inspired by the constructions using the sequence of quadratic characters [Ishai13, SESN23]
- **Fact**

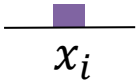
  For any $\ell \in \mathbb{N}$, there exists a prime $p = 2^{O(\ell)}$ such that
  the sequence of quadratic characters modulo p "contains" any sequence of length ℓ.



Our PSM w/ Universal Reconstruction

- Encode the histogram H of an input $\boldsymbol{x}$ into an integer $\widehat{H}$.

$$H = (h_1, \dots, h_d) \longrightarrow \widehat{H} = \sum_j h_j \cdot (n+1)^{j-1}$$

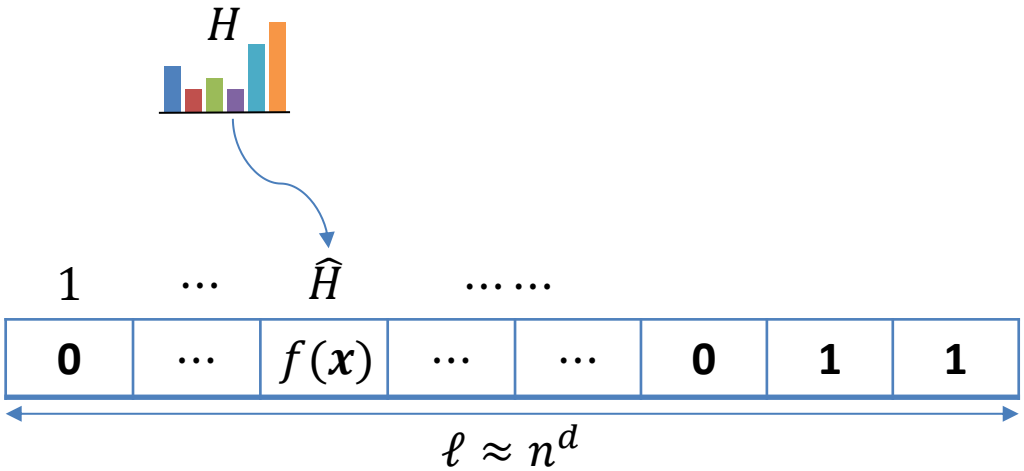


$$\longrightarrow \hat{x}_i = (n+1)^{x_i - 1}$$

"decomposable"

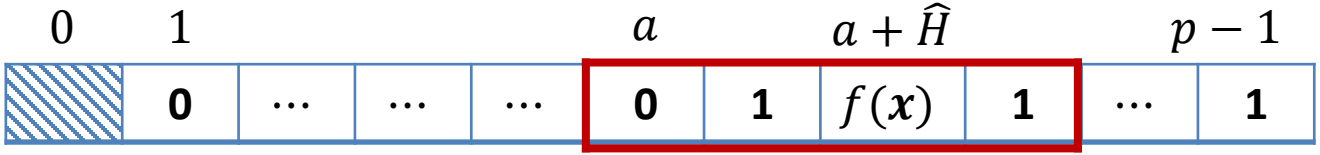
$$\widehat{H} = \hat{x}_1 + \cdots + \hat{x}_n$$

- Encode f into a sequence of length $\ell \approx n^d$.



Our PSM w/ Universal Reconstruction

- Set $p = 2^{O(n^d)}$.
- Find a subsequence containing the truth-table of f.



- Protocol

P_1 : $m_1 = q(a + \hat{x}_1) + r_i$

P_2 ⋮ P_n : $m_i = q\,\hat{x}_i + r_i$

Referee

Checks if $\sum_i m_i = q(a + \hat{H})$ is QR or not

Universal reconstruction

Referee learns p and $f(\boldsymbol{x})$ only.

q : random quadratic residues

$(r_1, \ldots, r_n)$: random shares of zero

Communication

$n \log p = O(n^{d+1})$

Can be reduced to $O(n^d)$ with some optimization

Summary

- Breaking the representation-size barrier in PSM for symmetric f.
  - New decomposition techniques based on the symmetry of f
  - Byproduct: Almost-optimal PSM for symmetric f with *universal reconstruction*
  - Extension to related models: *robust* PSM and *ad-hoc* PSM.

Scheme	Communication (worst-case)
[BKN18]	$d^{n/2} \cdot n^3$
[AL21]	$d^{(n-1)/2} \cdot 2^{O(n)}$
[BKR17]	$n^{d \log n + O(1)}$
[BGI+14]	$O(n^{2d+1})$
[EOYN21]	$O(n^d d^2 \log n)$
This work	$n^{2d/3+O(1)}$

Future work

- More efficient scheme, e.g., n^{cd} for $c < 2/3$
- Other related primitives, e.g., CDS and secret sharing

Thank you!