Improved Private Simultaneous Messages Protocols for Symmetric Functions with Universal Reconstruction

Koji Nuida
IMI, Kyushu University / AIST

IWSEC 2025 @Fukuoka, Japan
November 26, 2025

Summary

- Private Simultaneous Messages (PSM) protocols for symmetric functions $f:\{0,1,\dots,d-1\}^n \to \{0,1\}$ w/ and w/o universal reconstruction property
  - exponentially (in d) better than the SOTA protocols by [Eriguchi and Shinagawa, EUROCRYPT 2025]
- Main ingredient: Exponentially more efficient (linear and injective) encoding of histograms for inputs

Contents

- Background
- [Eriguchi & Shinagawa, EC' 25]
- Our Results

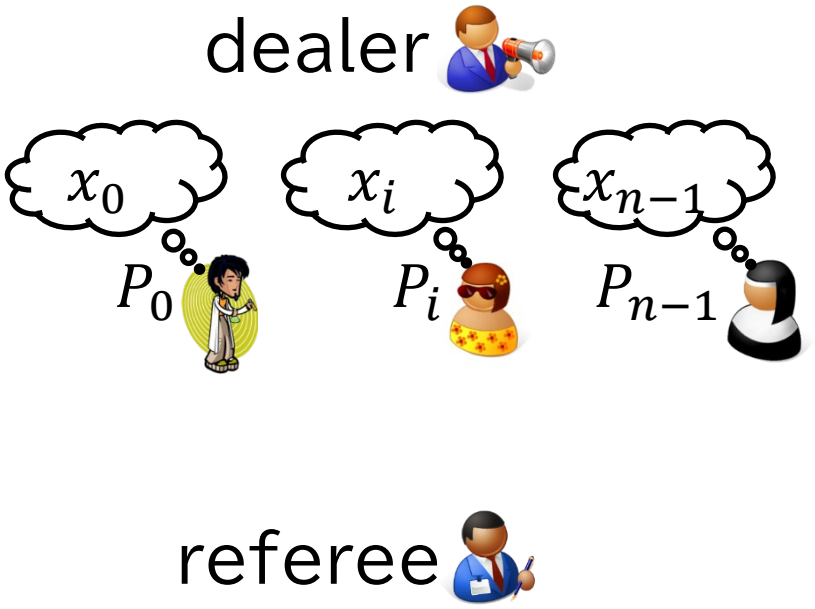
Contents

- Background
- [Eriguchi & Shinagawa, EC' 25]
- Our Results

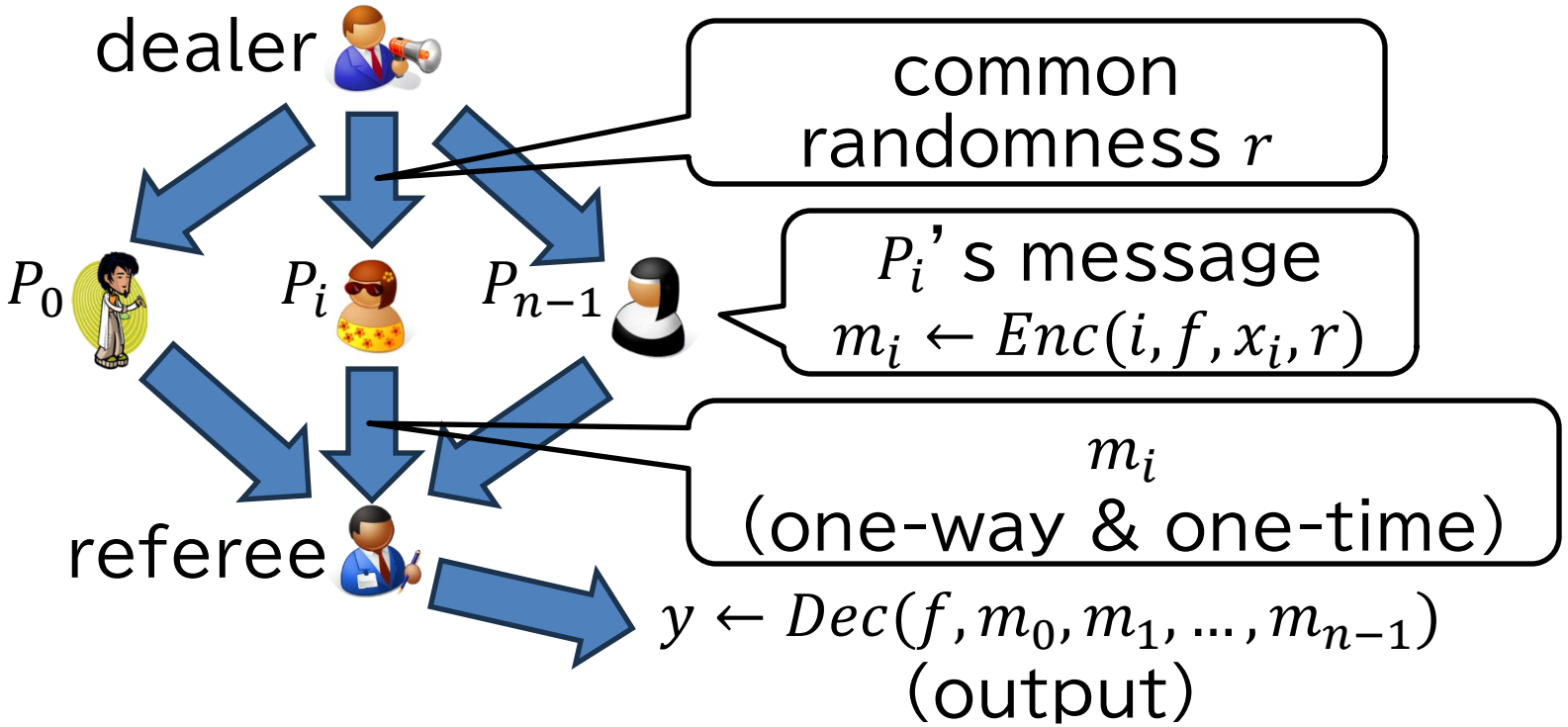
Private Simultaneous Messages (PSM)

- A “minimal” model for secure multiparty computation
  - to compute a function f
- Players:
  - n input parties $P_0, P_1, \ldots, P_{n-1}$ (honest)
    - with inputs $x_0, x_1, \ldots, x_{n-1}$
  - Referee (output party; semi-honest)
  - Dealer (honest)

Private Simultaneous Messages (PSM)

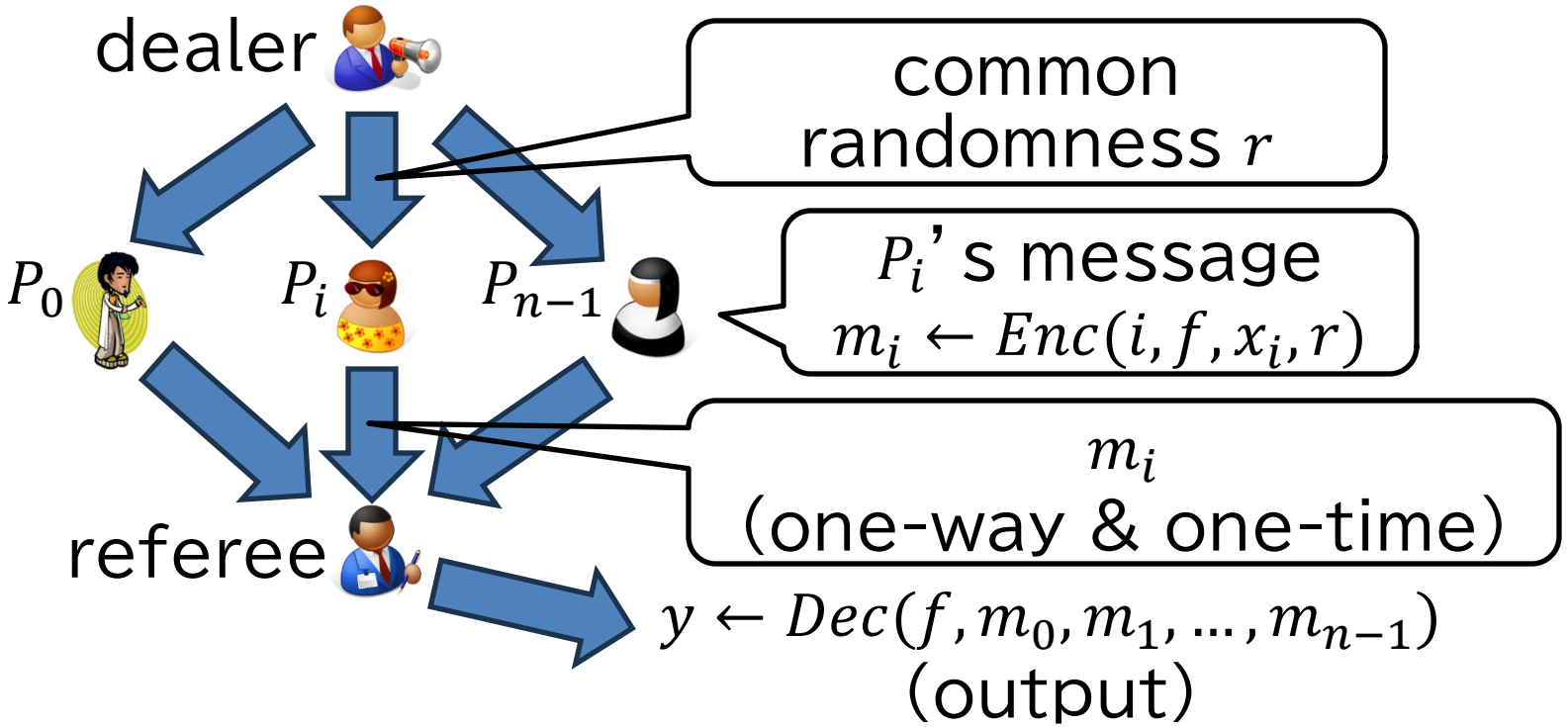


Private Simultaneous Messages (PSM)



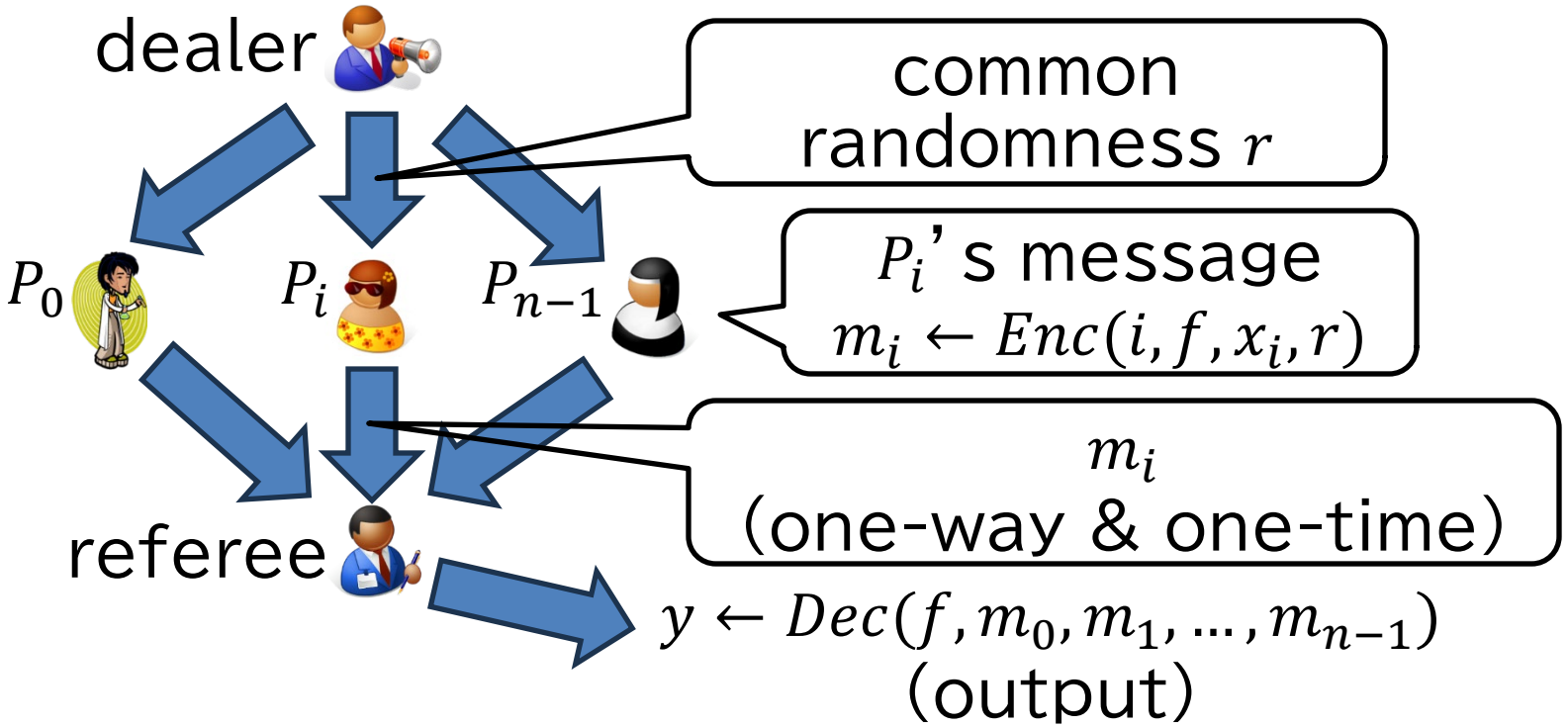
- Correctness:
  $y = f(x_0, x_1, \ldots, x_{n-1})$ for any r

Private Simultaneous Messages (PSM)



- Security:
  $(m_0, m_1, \ldots, m_{n-1}) \equiv S(f, y)$ for a simulator S

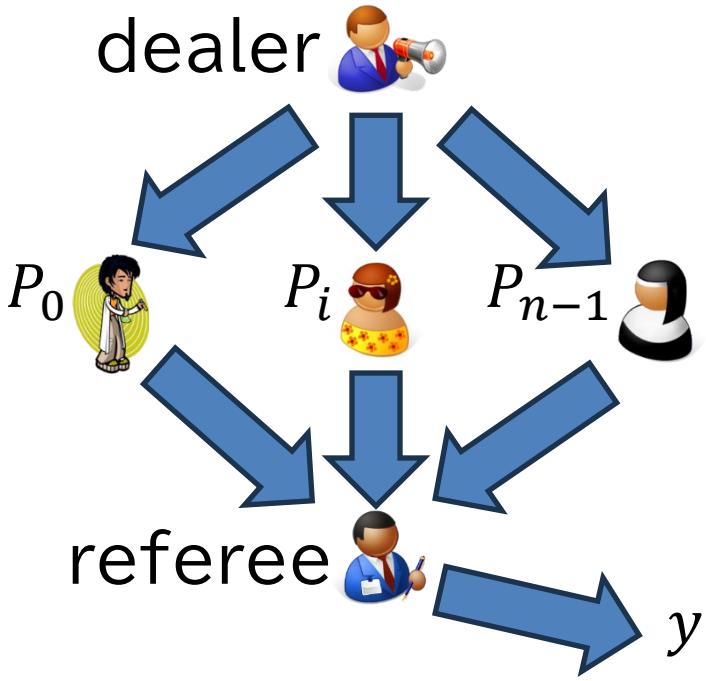
Private Simultaneous Messages (PSM)



- Main efficiency measures:
  $Comm(\Pi) := |m_0| + \cdots + |m_{n-1}|$, $Rand(\Pi) := |r|$

PSM with Universal Reconstruction

(Beimel et al., TCC 2014)



$\Leftrightarrow$ Dec and S do not use f

$y \leftarrow Dec(f, m_0, m_1, \ldots, m_{n-1})$
(output)

- Security:
  $(m_0, m_1, \ldots, m_{n-1}) \equiv S(f, y)$ for a simulator S

[Eriguchi & Shinagawa, EUROCRYPT 2025]

- PSM for symmetric func. from PSM w/ univ. reconst. for symmetric func.
- Efficient PSM w/ u.r. for symm. func.

- State-of-the-art PSM for symm. func.
  - For symmetric $f: \{0,1,\dots,d-1\}^n \to \{0,1\}$, $Comm(\Pi) = O(n^{\approx 2d/3})$, $Rand(\Pi) = O(n^{\approx 2d/3})$

Contents

- Background
- [Eriguchi & Shinagawa, EC' 25]
- Our Results

Quadratic Character Sequence

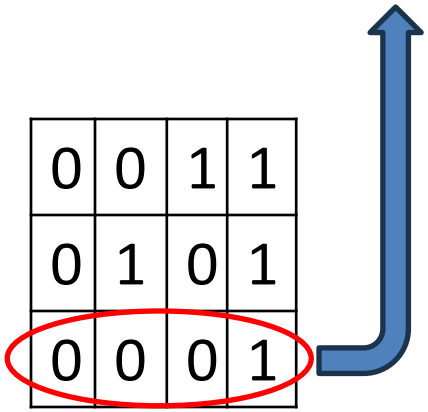
- For prime p, $Q_p(a) :=$
  $\begin{cases} 0, \text{ if } \exists b \text{ s.t. } a = b^2 \ mod \ p \\ 1, \text{ otherwise} \end{cases}$
- E.g., $Q_{11} = 0100011101$

$\nexists \sqrt{2} \ (mod \ 11)$

$\sqrt{5} = 4 \ (mod \ 11)$

Embedding of Function

- E.g., $Q_{11} = 0100011101$
- AND:



- Fact: $\exists p_L = 2^{O(L)}$ s.t. **any** L-bit sequence can be embedded in Q_{p_L}

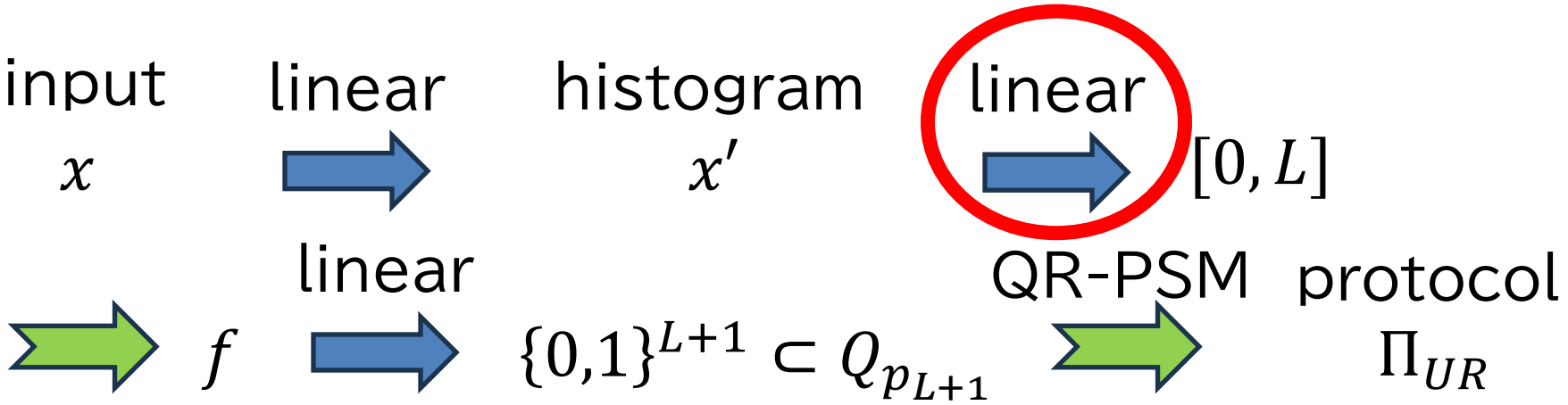
QR-PSM (w/ u.r.)

- Fact: $\exists p_L = 2^{O(L)}$ s.t. **any** L-bit sequence can be embedded in Q_{p_L}
- Once the function is "linearly" embedded in Q_{p_L}, a PSM protocol is obtained via a technique of [Shinagawa et al., DCC 2023]
  - Univ. reconst., because p_L is common to any function

Histogram of Inputs

- $f:\{0,1,\ldots,d-1\}^n \to \{0,1\}$ is symmetric, so **$f(x)$ is determined by histograms**
  $x'_k := \#\{i : x_i = k\}$ for $k = 0,1,\ldots,d-2$
  – x'_{d-1} is recovered from n and $x'_0,\ldots,x'_{d-2}$
- By putting $x'_{i,k} := 1$ if $x_i = k$ and $x'_{i,k} := 0$ if $x_i \neq k$, we have $x'_k = x'_{0,k} + x'_{1,k} + \cdots + x'_{n-1,k}$

Strategy



- We need linear and injective encoding of histograms
- $p_{L+1} = 2^{O(L)}$ and $Comm(\Pi_{UR}) = O(n \log p_{L+1})$, so it is crucial to use small L

Encoding of Histograms

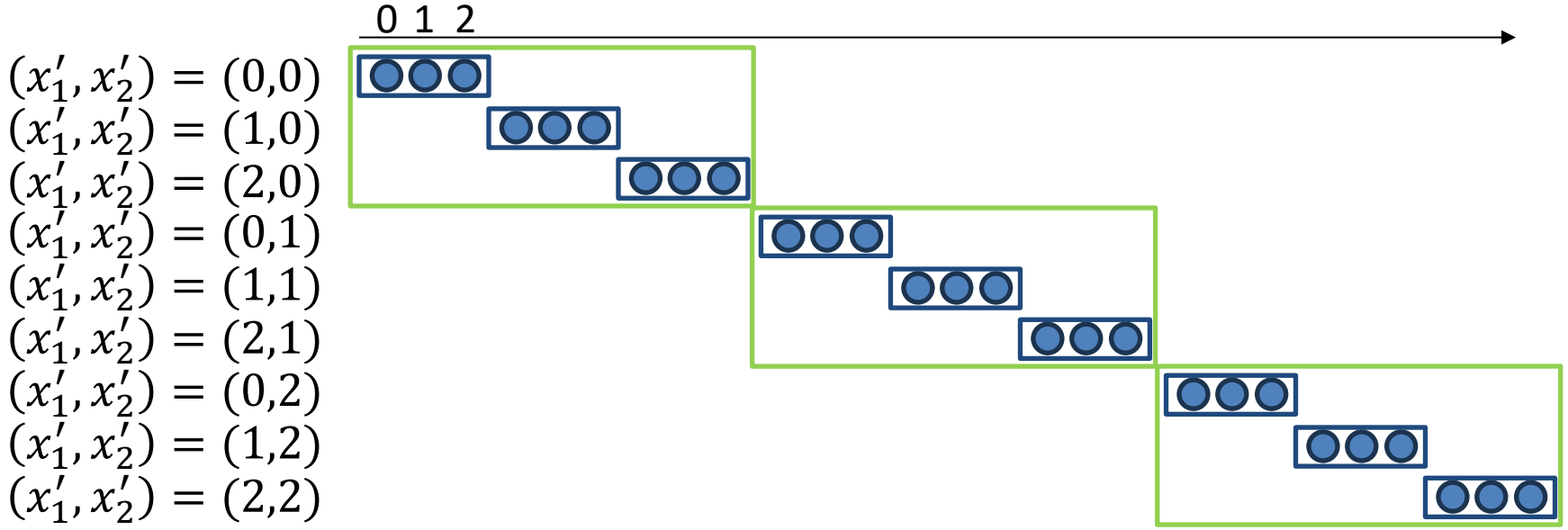
- $I_v(x') \coloneqq v_0 x'_0 + v_1 x'_1 + \cdots + v_{d-2} x'_{d-2}$
  - WLOG, $1 \leq v_0 \leq v_1 \leq \cdots \leq v_{d-2}$
    (NOTE: $1 \leq v_{d-2} \leq \cdots \leq v_1 \leq v_0$ in the paper)
- I_v must be injective on the set
  $B \coloneqq \{x' : x'_k \geq 0\ (\forall k), x'_0 + x'_1 + \cdots + x'_{d-2} \leq n\}$
- $L = n v_{d-2}$ must be as small as possible
- We construct such a coefficient vector $v = (v_0, v_1, \ldots, v_{d-2})$ recursively

Contents

- Background
- [Eriguchi & Shinagawa, EC' 25]
- Our Results

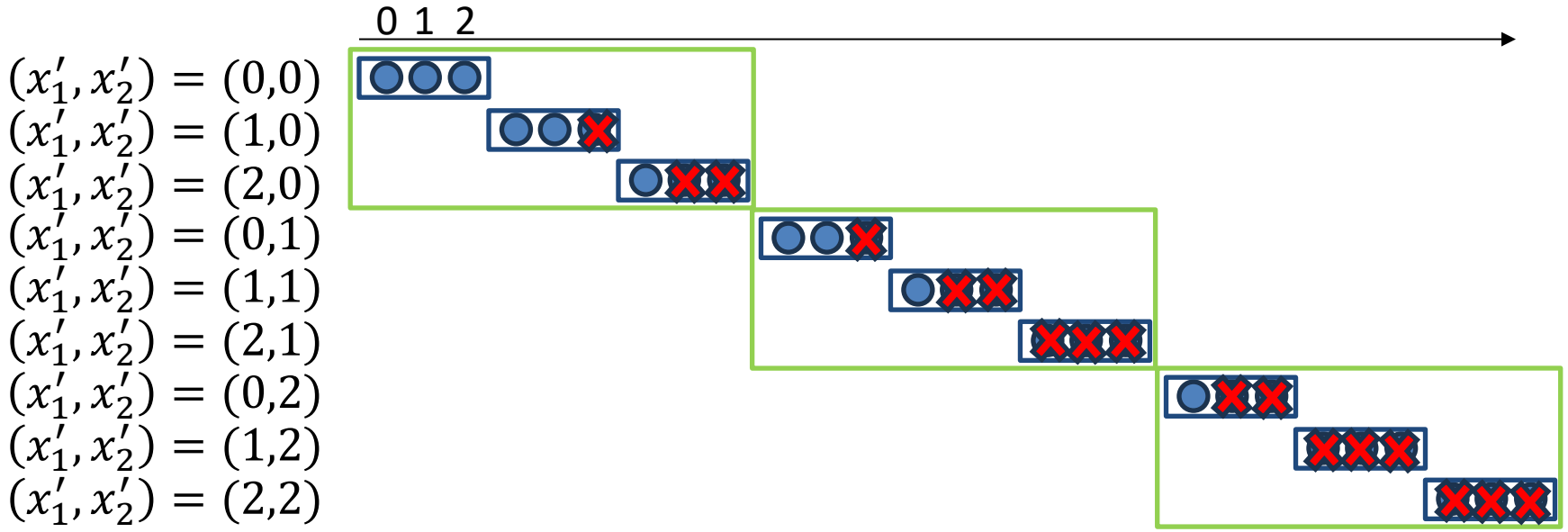
Encoding of Histograms

- E.g., $v = (v_0, v_1, v_2), n = 2, v_0 = 1$
- If B were $\{x' : x'_k \geq 0, \boldsymbol{x'_k \leq n}\}$, then $v_1 = (n+1)^1$, $v_2 = (n+1)^2$ would be best
  - The construction in [E&S, EC' 25]



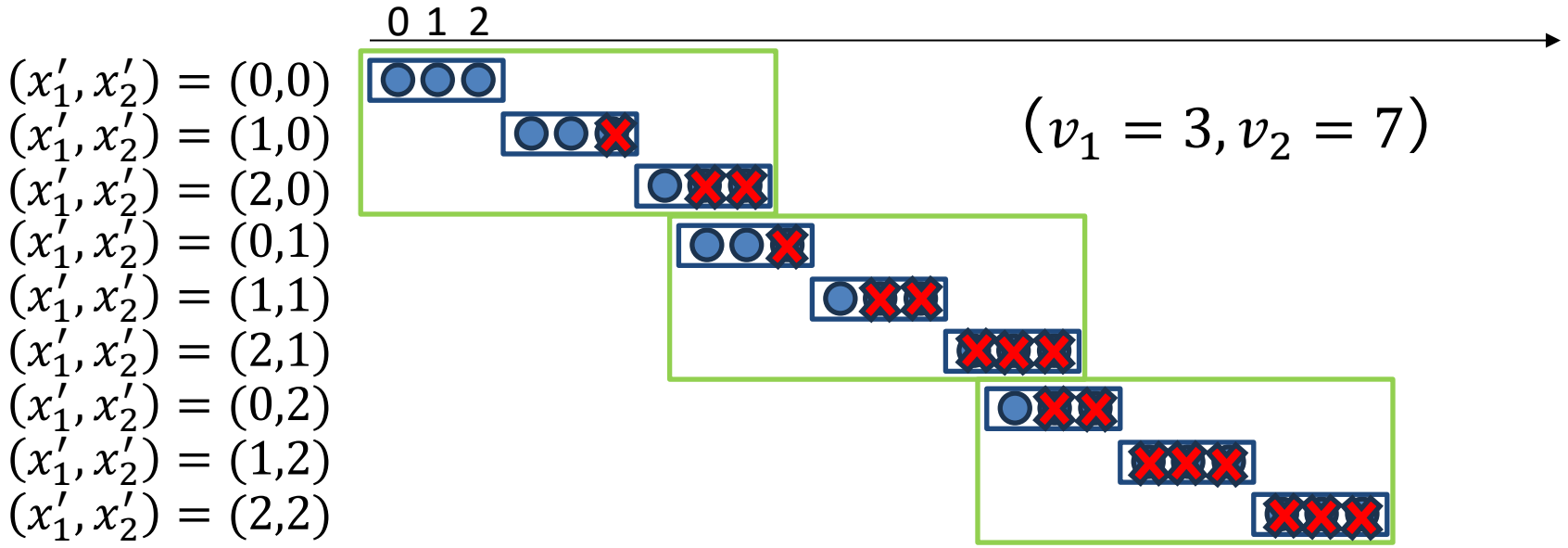
Encoding of Histograms

- E.g., $v = (v_0, v_1, v_2), n = 2, v_0 = 1$
- But in fact $B = \{x' : x'_k \geq 0, \boldsymbol{wt(x') \leq n}\}$



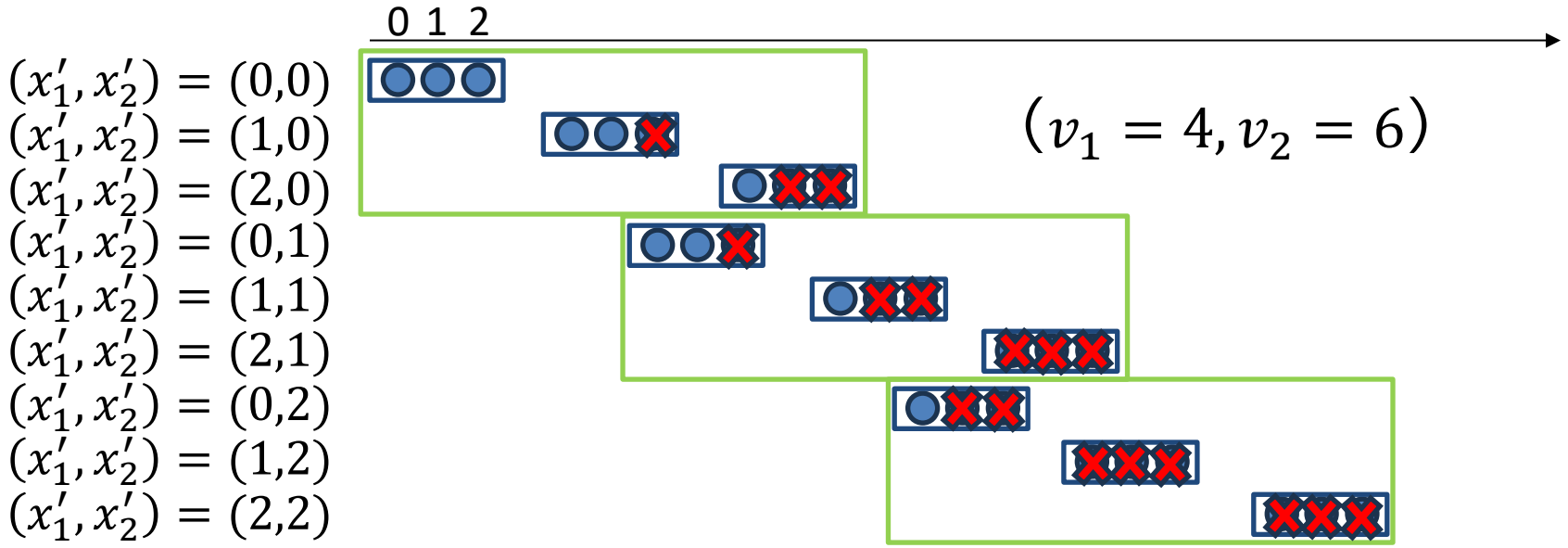
Encoding of Histograms

- E.g., $v = (v_0, v_1, v_2), n = 2, v_0 = 1$
- But in fact $B = \{x' : x'_k \geq 0, \boldsymbol{wt(x') \leq n}\}$
- So we can shift them to the left



Encoding of Histograms

- E.g., $v = (v_0, v_1, v_2), n = 2, v_0 = 1$
- But in fact $B = \{x' : x'_k \geq 0, \boldsymbol{wt(x') \leq n}\}$
- … or more cleverly



Encoding of Histograms

- By careful analysis, we obtain a coefficient vector $v = (v_0, v_1, \ldots, v_{d-2})$ with $v_{d-2} = O(c^{d-1}n^{d-2})$, $L = O\left(c^{d-1}n^{d-1}\right)$ where $c = 1/\sqrt{2} + o(1) < 1$
  - In [E&S, EC' 25], $v_{d-2} = O(n^{d-2})$, $L = O\left(n^{d-1}\right)$
  - Exponential (in d) improvement

Our PSM Protocols

- Combining it with [E&S, EC' 25], we have $Comm(\Pi_{UR}) = O\left(c^{d-1}(n-1)^d\right)$ and $Rand(\Pi_{UR}) = O(c^{d-1}(n-1)^d)$ where $c = 1/\sqrt{2} + o(1) < 1$
  - In [E&S, EC' 25], $O((n-1)^d)$
- Moreover, $Comm(\Pi) = O\left(c^{\approx d/3} n^{\approx 2d/3}\right)$ and $Rand(\Pi) = O\left(c^{\approx d/3} n^{\approx 2d/3}\right)$
  - In [E&S, EC' 25], $O(n^{\approx 2d/3})$
  - Exponential (in d) improvement

Conclusion

- PSM protocols for symmetric functions $f:\{0,1,\dots,d-1\}^n \to \{0,1\}$ w/ and w/o universal reconstruction
  - exponentially (in d) better than [E&S, EC' 25]
- Future work: More efficient encoding of histograms (⇒ more efficient PSM)
  - Our computer experiment showed that our choice of coefficient vector is still not optimal