Multi-party PSM, Revisited:

Improved Communication and Unbalanced Communication

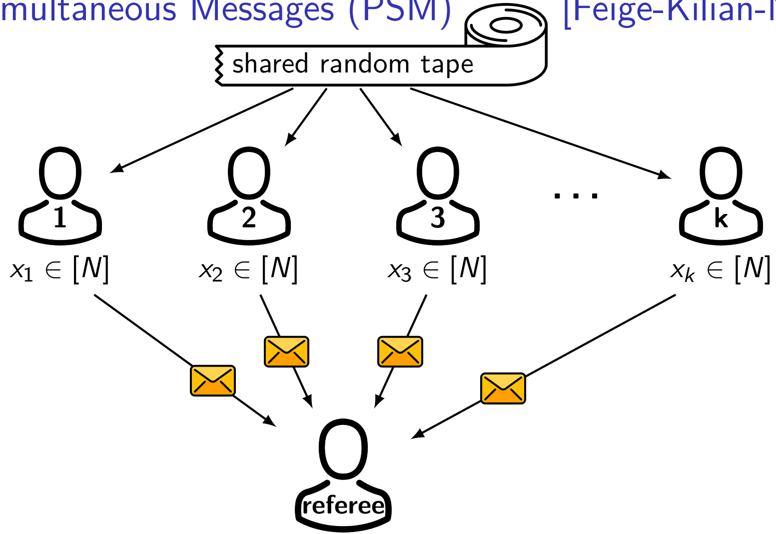
Tianren Liu[1] Léonard Assouline[2]

[1]University of Washington, Seattle → Peking University, Beijing

[2]École Normale Supérieure, Paris

TCC 2021

Private Simultaneous Messages (PSM) [Feige-Kilian-Naor 94]



- Correctness: The referee learns $f(x_1, \ldots, x_k)$
- Security: Unbounded referee learns nothing else
- Communication complexity

Motivations

PSM is of theoretical interest

- Minimal model of secure computation

Close connection to . . .

- Ad-hoc PSM [BGIK16, BIK17]
- Conditional Disclosure of Secrets (CDS) [GIKM00,LVW18]
- Non-interactive MPC [BGIKMP14]
- (Decomposable) randomized encoding
- Information-theoretic GC [Yao86]
  $\approx$ PSM where each party has 1-bit input

How communication complexity depends on N, k (worst-case f)

Can communication $\ll N^k$?

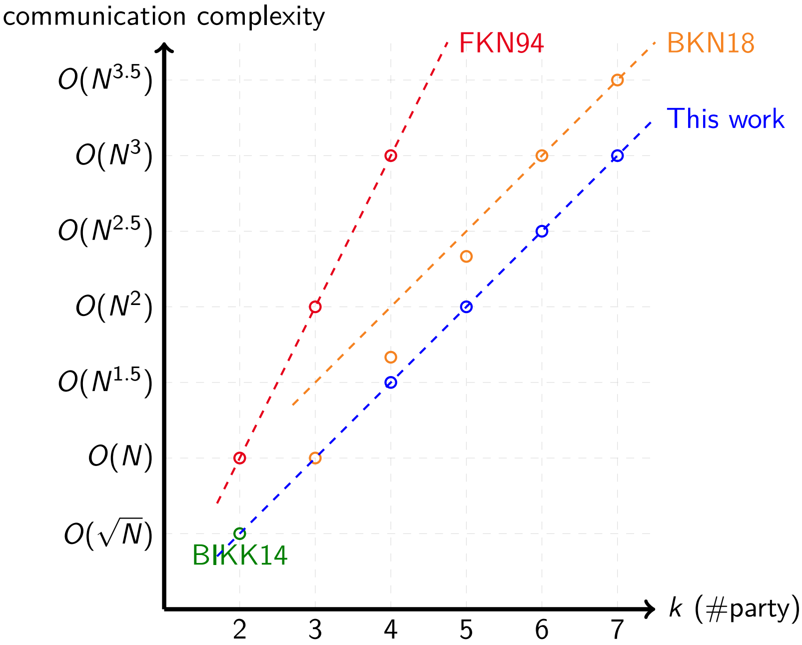
e.g. CDS's communication $\approx 2^{\sqrt{k \log N}}$

How communication complexity depends on computation complexity (circuit size, branching program size, etc)

Previous Works and Our Results

	Communication for $f : [N]^k \to \{0,1\}$ in PSM model
[FKN94]	$O(N^{k-1}) \quad =$ all-but-one-party input space size
[BKN18]	$O_k(N^{k/2}) \quad = \sqrt{\text{total input space size}}$
[BIKK14]	$O(N^{1/2})$ for $k = 2$ $\quad$ **= ????**
[BKN18]	$O(N)$, $O(N^{5/3})$, $O(N^{7/3})$ for $k = 3, 4, 5$ resp. **= ????**
This work	$O_k(N^{\frac{k-1}{2}}) \quad = \sqrt{\text{all-but-one-party input space size}}$ - Yield BIKK and BKN as special cases when $k = 2$ or 3 - For infinitely many k, including all $k \leq 20$

Previous Works and Our Results



Previous Works and Our Results (2-party)

	Communication for $f : [N] \times [N] \to \{0,1\}$ in PSM model
[BIKK14]	$O(N^{1/2})$
[FKN94]	$O(N)$ for one party, $O(\log N)$ for the other
This work	$O(N^{\eta})$ for one party, $O(N^{1-\eta})$ for the other - Yield BIKK construction as a special case when $\eta = 1/2$ - For rational $\eta \in (0,1)$ whose denominator ≤ 20

There are more questions than answers.

(will discuss them in the "open problem" section)

Idea I [CGKS95,BIKK14]

$$\text{Target} \;=\; f(x_1,\dots,x_k) \;=\; \langle F, \vec{x}_1 \otimes \cdots \otimes \vec{x}_k \rangle$$

Notations:

- $\langle \;\cdot\;,\;\cdot\;\rangle$ denotes the inner product
- F is the truth-table of f, which is a dimension-$(\underbrace{N \times \cdots \times N}_{k \text{ times}})$ array
- $\vec{x}_i$ is a dimension-N vector, $\vec{x}_i = \begin{array}{|c|c|c|c|c|c|}\hline 0 & 0 & 0 & 0 & 1 & 0 \\ \hline \end{array}$

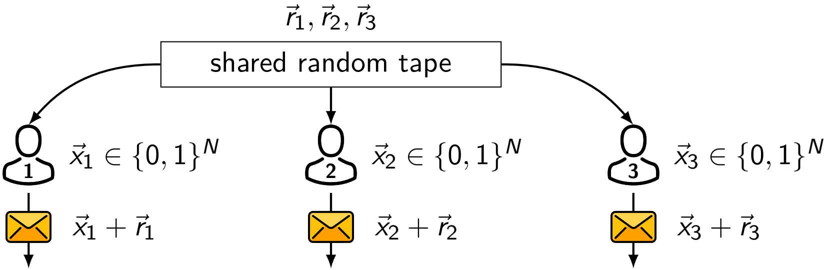
  x_i-th coordinate
- $\otimes$ denotes tensor product, e.g. $\vec{x}_i \otimes \vec{x}_j = \begin{array}{|c|c|c|c|c|c|}\hline 0&0&0&0&0&0\\ \hline 0&0&0&0&0&0\\ \hline 0&0&0&0&0&0\\ \hline 0&0&0&0&0&0\\ \hline 0&0&0&1&0&0\\ \hline 0&0&0&0&0&0\\ \hline \end{array}$

  (x_i, x_j)-th coordinate

Idea I [CGKS95,BIKK14]

$$\text{Target} \;=\; f(x_1, \ldots, x_k) \;=\; \langle F, \vec{x}_1 \otimes \cdots \otimes \vec{x}_k \rangle$$

Recap 3-party PSM [BKN18]



The referee can compute $\boxed{\langle F, (\vec{x}_1 + \vec{r}_1) \otimes (\vec{x}_2 + \vec{r}_2) \otimes (\vec{x}_3 + \vec{r}_3) \rangle}$

Idea I [CGKS95,BIKK14]

Target $= f(x_1, \ldots, x_k) = \langle F, \vec{x}_1 \otimes \cdots \otimes \vec{x}_k \rangle$

Recap 3-party PSM [BKN18]

P_i sends OTP $\vec{x}_i + \vec{r}_i$.

$$\boxed{\langle F, (\vec{x}_1 + \vec{r}_1) \otimes (\vec{x}_2 + \vec{r}_2) \otimes (\vec{x}_3 + \vec{r}_3) \rangle} = \langle F, \vec{x}_1 \overset{\text{target}}{\otimes} \vec{x}_2 \otimes \vec{x}_3 \rangle$$

has c.c. $O(N)$ in PSM model

$$\underbrace{\begin{array}{l} + \langle P_1 \text{ knows}, \vec{x}_2 \rangle + \langle P_1 \text{ knows}, \vec{x}_3 \rangle + \langle P_2 \text{ knows}, \vec{x}_3 \rangle \\ + \langle F, P_1 \text{ knows } \vec{r}_3 \rangle + \langle F, P_2 \text{ knows } \vec{r}_3 \rangle + \langle F, P_3 \text{ knows } \vec{x}_3 \rangle + \langle F, P_1 \text{ knows } \vec{r}_3 \rangle \end{array}}_{\text{deg-2 poly with } O(N) \text{ monomials (after local preprocessing)}}$$

Idea II [IK97,BKN18]

Polynomials have complexity $O_{\text{degree}}(\#[\mathit{monomials}])$ in PSM model

5-party PSM with communication $O(N^2)$

P_i sends OTP $\vec{x}_i + \vec{r}_i$ ($\vec{r}_i \leftarrow$ shared randomness).

$$\boxed{\langle F, (\vec{x}_1 + \vec{r}_1) \otimes (\vec{x}_2 + \vec{r}_2) \otimes (\vec{x}_3 + \vec{r}_3) \otimes (\vec{x}_4 + \vec{r}_4) \otimes (\vec{x}_5 + \vec{r}_5)\rangle}$$

$$= \langle F, \vec{x}_1 \otimes \vec{x}_2 \otimes \vec{x}_3 \otimes \vec{x}_4 \otimes \vec{x}_5\rangle \leftarrow \text{target}$$

hard to eliminate?

$$+\langle F, \vec{x}_1 \otimes \vec{x}_2 \otimes \vec{x}_3 \otimes \vec{x}_4 \otimes \vec{r}_5\rangle + \langle F, \vec{x}_1 \otimes \vec{x}_2 \otimes \vec{x}_3 \otimes \vec{r}_4 \otimes \vec{x}_5\rangle + \langle F, \vec{x}_1 \otimes \vec{x}_2 \otimes \vec{r}_3 \otimes \vec{x}_4 \otimes \vec{x}_5\rangle + \langle F, \vec{x}_1 \otimes \vec{r}_2 \otimes \vec{x}_3 \otimes \vec{x}_4 \otimes \vec{x}_5\rangle + \langle F, \vec{r}_1 \otimes \vec{x}_2 \otimes \vec{x}_3 \otimes \vec{x}_4 \otimes \vec{x}_5\rangle$$

$$+\langle P_1 \text{ knows}, \vec{x}_2 \otimes \vec{x}_3\rangle + \langle P_1 \text{ knows}, \vec{x}_2 \otimes \vec{x}_4\rangle + \langle P_1 \text{ knows}, \vec{x}_3 \otimes \vec{x}_4\rangle + \langle P_2 \text{ knows}, \vec{x}_3 \otimes \vec{x}_4\rangle + \langle P_1 \text{ knows}, \vec{x}_2 \otimes \vec{x}_5\rangle$$

$$+\langle P_1 \text{ knows}, \vec{x}_3 \otimes \vec{x}_5\rangle + \langle P_2 \text{ knows}, \vec{x}_3 \otimes \vec{x}_5\rangle + \langle P_1 \text{ knows}, \vec{x}_4 \otimes \vec{x}_5\rangle + \langle P_2 \text{ knows}, \vec{x}_4 \otimes \vec{x}_5\rangle + \langle P_3 \text{ knows}, \vec{x}_4 \otimes \vec{x}_5\rangle$$

$$+\langle P_1 \text{ knows}, \vec{x}_2\rangle + \langle P_1 \text{ knows}, \vec{x}_3\rangle + \langle P_2 \text{ knows}, \vec{x}_3\rangle + \langle P_1 \text{ knows}, \vec{x}_4\rangle + \langle P_2 \text{ knows}, \vec{x}_4\rangle$$

$$+\langle P_3 \text{ knows}, \vec{x}_4\rangle + \langle P_1 \text{ knows}, \vec{x}_5\rangle + \langle P_2 \text{ knows}, \vec{x}_5\rangle + \langle P_3 \text{ knows}, \vec{x}_5\rangle + \langle P_4 \text{ knows}, \vec{x}_5\rangle$$

$$+ P_1 \text{ knows} + P_2 \text{ knows} + P_3 \text{ knows} + P_4 \text{ knows} + P_5 \text{ knows}$$

$$+ P_1 \text{ knows}$$

deg-3 poly with $O(N^2)$ monomials (after local preprocessing)

5-party PSM with communication $O(N^2)$

P_i sends OTP $\vec{x}_i + \vec{r}_i$ ($\vec{r}_i \leftarrow$ shared randomness). $\longleftarrow$ communication $\ll N^2$

$$\boxed{\langle F, (\vec{x}_1 + \vec{r}_1) \otimes (\vec{x}_2 + \vec{r}_2) \otimes (\vec{x}_3 + \vec{r}_3) \otimes (\vec{x}_4 + \vec{r}_4) \otimes (\vec{x}_5 + \vec{r}_5) \rangle}$$

$$= \langle F, \vec{x}_1 \otimes \vec{x}_2 \otimes \vec{x}_3 \otimes \vec{x}_4 \otimes \vec{x}_5 \rangle + \boxed{\text{hard terms}} + \boxed{\text{easy terms}}$$

P_i, P_j "jointly send" OTP $\vec{x}_i \otimes \vec{x}_j + R_{i,j}$ ($R_{i,j} \leftarrow$ shared randomness).

$$\boxed{\langle F, (\vec{x}_1 \otimes \vec{x}_2 + R_{1,2}) \otimes (\vec{x}_3 + \vec{r}_3) \otimes (\vec{x}_4 + \vec{r}_4) \otimes (\vec{x}_5 + \vec{r}_5) \rangle},$$

$$\boxed{\langle F, (\vec{x}_1 \otimes \vec{x}_2 + R_{1,2}) \otimes (\vec{x}_3 \otimes \vec{x}_4 + R_{3,4}) \otimes (\vec{x}_5 + \vec{r}_5) \rangle},$$

$$\boxed{\langle F, (\vec{x}_1 \otimes \vec{x}_2 + R_{1,2}) \otimes (\vec{x}_3 + \vec{r}_3) \otimes (\vec{x}_4 \otimes \vec{x}_5 + R_{4,5}) \rangle}, \text{ etc}$$

Each of them $= \langle F, \vec{x}_1 \otimes \vec{x}_2 \otimes \vec{x}_3 \otimes \vec{x}_4 \otimes \vec{x}_5 \rangle + \boxed{\text{hard terms}} + \boxed{\text{easy terms}}$

Idea IV

Hard term cancellation (basic linear algebra)

5-party PSM with communication $O(N^2)$

P_i sends OTP $\vec{x}_i + \vec{r}_i$ ($\vec{r}_i \leftarrow$ shared randomness).

P_i, P_j "jointly send" OTP $\vec{x}_i \otimes \vec{x}_j + R_{i,j}$ ($R_{i,j} \leftarrow$ shared randomness).

$$\begin{pmatrix} -\boxed{\langle F, (\vec{x}_1 \otimes \vec{x}_2 + R_{1,2}) \otimes (\vec{x}_3 + \vec{r}_3) \otimes (\vec{x}_4 + \vec{r}_4) \otimes (\vec{x}_5 + \vec{r}_5) \rangle} \\ +\boxed{\langle F, (\vec{x}_1 \otimes \vec{x}_2 + R_{1,2}) \otimes (\vec{x}_3 \otimes \vec{x}_4 + R_{3,4}) \otimes (\vec{x}_5 + \vec{r}_5) \rangle} \\ +\boxed{\langle F, (\vec{x}_1 \otimes \vec{x}_2 + R_{1,2}) \otimes (\vec{x}_3 \otimes \vec{x}_5 + R_{3,5}) \otimes (\vec{x}_4 + \vec{r}_4) \rangle} \\ +\boxed{\langle F, (\vec{x}_1 \otimes \vec{x}_2 + R_{1,2}) \otimes (\vec{x}_3 + \vec{r}_3) \otimes (\vec{x}_4 \otimes \vec{x}_5 + R_{4,5}) \rangle} \end{pmatrix}$$

referee-computable

$$= 2 \times \langle F, \vec{x}_1 \otimes \vec{x}_2 \otimes \vec{x}_3 \otimes \vec{x}_4 \otimes \vec{x}_5 \rangle + \boxed{\text{easy terms}}$$

$2 \neq 0$

target

has c.c. $O(N^2)$
in PSM model

Idea IV

Hard term cancellation (basic linear algebra)

k-party PSM with communication $O(N^{(k-1)/2})$

$\forall S \subseteq [k]$ that $|S| \leq \frac{k-1}{2}$, "jointly send" the OTP of $\bigotimes_{i \in S} \vec{x}_i$,

i.e. $\bigotimes_{i \in S} \vec{x}_i + R_S$ ($R_S \leftarrow$ shared randomness).

Every $\boxed{\text{referee-computable term}}$ $=$ target $+$ $\boxed{\text{hard terms}}$ $+$ $\boxed{\text{easy terms}}$

Do linear algebra to cancel out the hard terms:

$\boxed{\text{a linear combination of referee-computable terms}}$ $= c \cdot$ target $+$ $\boxed{\text{easy terms}}$

- Extra work to "use up the budget" when k is even. (next slide)
- Computer did the linear algebra when $k \leq 20$.
- We did the linear algebra for all $k = \text{prime}^{\text{power}} - 1$.

Extra work when k is even

Idea I [CGKS95,BIKK14]

$$\text{Target} = f(x_1, \ldots, x_k) = \langle F, \vec{x}_{1,H} \otimes \vec{x}_{1,L} \otimes \cdots \otimes \vec{x}_{k,H} \otimes \vec{x}_{k,L} \rangle$$

- $\vec{x}_i$ is a dimension-N vector, $\vec{x}_i := \begin{array}{|c|c|c|c|c|c|c|c|c|c|} \hline 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array}$

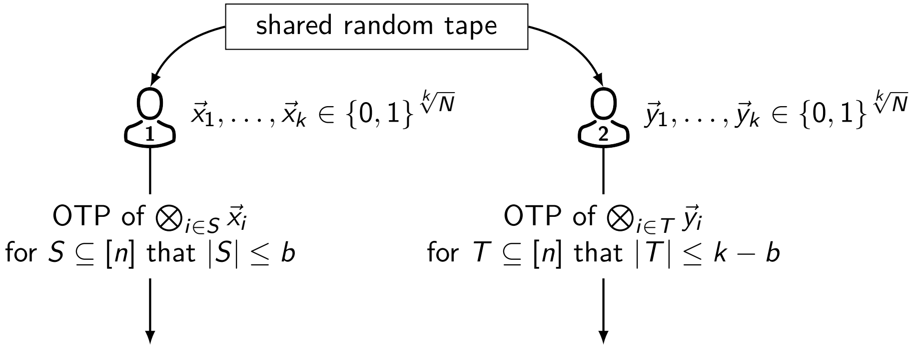
  x_i-th coordinate
- Split $x_i \in [N]$ into $x_{i,H}, x_{i,L} \in [\sqrt{N}]$

  Consider $\vec{x}_{i,H} := \begin{array}{|c|c|c|c|} \hline 0 & 1 & 0 & 0 \\ \hline \end{array}$, $\vec{x}_{i,L} := \begin{array}{|c|c|c|c|} \hline 0 & 0 & 1 & 0 \\ \hline \end{array}$

  $x_{i,H}$-th coordinate $x_{i,L}$-th coordinate
- Then $\vec{x}_i = \vec{x}_{i,H} \otimes \vec{x}_{i,L}$ (flattened)

2-party PSM communication trade-off

Budget: one party sends $O(N^{\frac{b}{k}})$ bits, the other party sends $O(N^{\frac{k-b}{k}})$ bits



Idea III

Use up the communication budget!

2-party PSM communication trade-off

Budget: one party sends $O(N^{\frac{b}{k}})$ bits, the other party sends $O(N^{\frac{k-b}{k}})$ bits

- Use up the budget:
  P_1 sends the OTP of $\bigotimes_{i \in S} \vec{x}_i$ for every $S \subseteq [n]$ that $|S| \leq b$
  P_2 sends the OTP of $\bigotimes_{i \in T} \vec{y}_i$ for every $T \subseteq [n]$ that $|T| \leq k - b$

- Every $\boxed{\text{referee-computable term}}$ $=$ target $+$ $\boxed{\text{hard terms}}$ $+$ $\boxed{\text{easy terms}}$

  c.c. $\leq$ budget in PSM model

- Do linear algebra:
  $\boxed{\text{a linear combination of referee-computable terms}}$ $=$ target $+$ $\boxed{\text{easy terms}}$

- Computer did the linear algebra when $0 < b < k \leq 20$.

Our Results

k-party PSM with c.c. $O_k(N^{\frac{k-1}{2}})$, for infinitely many k.

2-party PSM with c.c. $O(N^{\frac{d}{k}}), O(N^{\frac{k-d}{k}})$, for any $0 < d < k \leq 20$.

...generate more **open questions** than answers.

Our Conjectures Our frameworks work for any integer k.

Dependency on k *Symmetry* simplifies the analysis, but leads to exponential dependency on k.

Why it works? Beyond "the system of linear equations has a solution".

Why it doesn't work? E.g. 2-party PSM with c.c. $N^{10/21}$? 653 referee-computable terms, 139 hard terms, 0 solution.

Moon shot PSM with sub-exponential communication on $k \log N$.