Towards Breaking the Exponential Barrier for General Secret Sharing

Tianren Liu
MIT

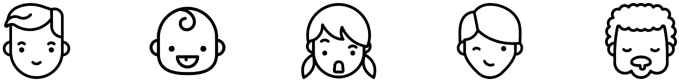
Vinod Vaikuntanathan
MIT

Hoeteck Wee
CNRS and ENS

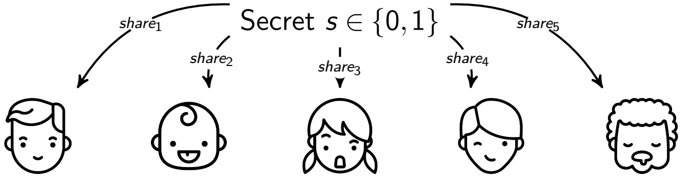
May 6, 2018

Secret Sharing [Blakley'79,Shamir'79,Ito-Saito-Nishizeki'87]

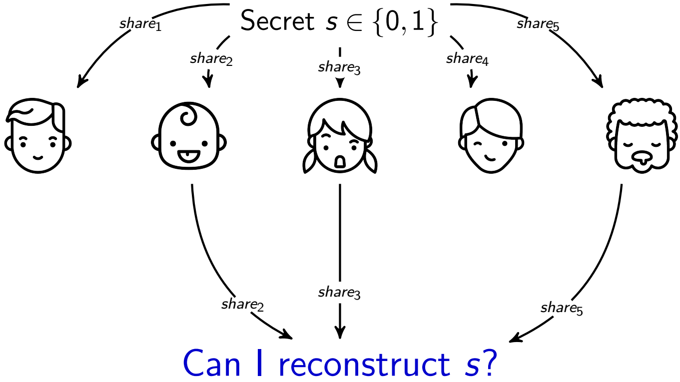
Secret $s \in \{0, 1\}$



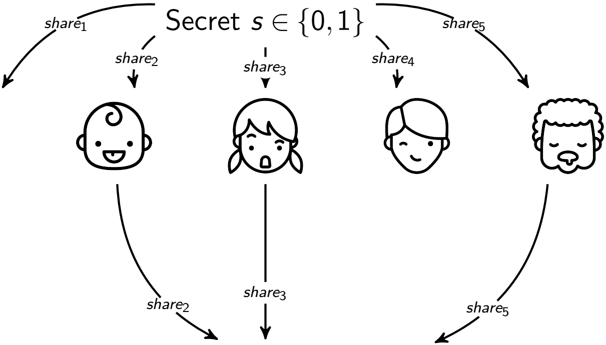
Secret Sharing [Blakley'79,Shamir'79,Ito-Saito-Nishizeki'87]



Secret Sharing [Blakley'79,Shamir'79,Ito-Saito-Nishizeki'87]



Secret Sharing [Blakley'79,Shamir'79,Ito-Saito-Nishizeki'87]



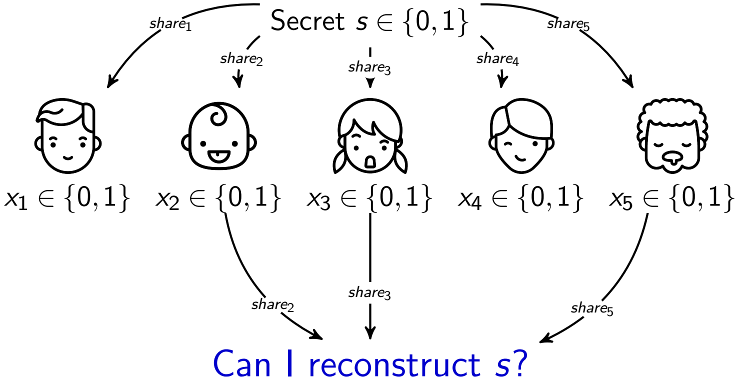
Can I reconstruct s?

Threshold Secret Sharing [Shamir'79]

YES if I gets $\geq t$ shares;

NO INFO if I gets $< t$ shares.

Secret Sharing [Blakley'79,Shamir'79,Ito-Saito-Nishizeki'87]

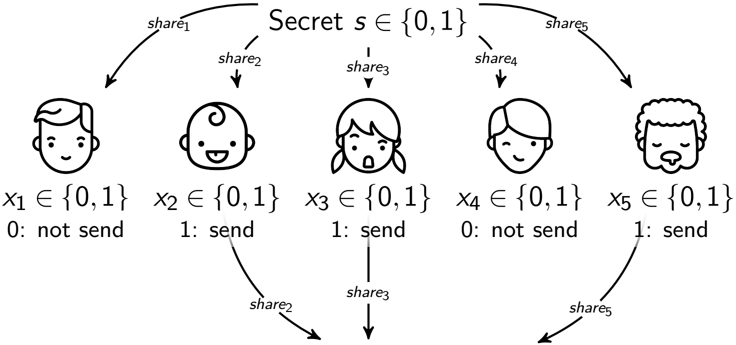


Threshold Secret Sharing [Shamir'79]

YES if I gets $\geq t$ shares;

NO INFO if I gets $< t$ shares.

Secret Sharing [Blakley'79,Shamir'79,Ito-Saito-Nishizeki'87]



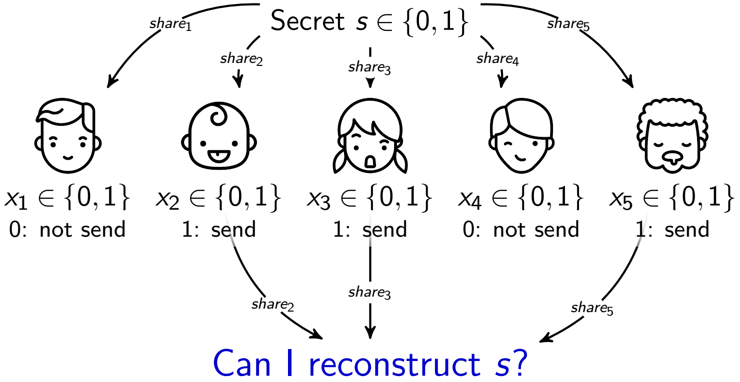
Can I reconstruct s?

Threshold Secret Sharing [Shamir'79]

YES if I gets $\geq t$ shares;

NO INFO if I gets $< t$ shares.

Secret Sharing [Blakley'79,Shamir'79,Ito-Saito-Nishizeki'87]

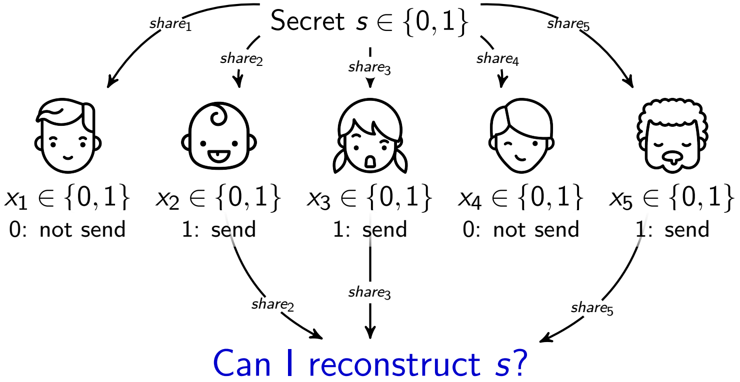


Threshold Secret Sharing [Shamir'79]

YES if $\text{threshold}_t(x_1, \ldots, x_n) = 1$;

NO INFO if $\text{threshold}_t(x_1, \ldots, x_n) = 0$.

Secret Sharing [Blakley'79,Shamir'79,Ito-Saito-Nishizeki'87]



General Secret Sharing [ISN'89] monotone $F : \{0,1\}^n \to \{0,1\}$

YES if $F(x_1, \ldots, x_n) = 1$;

NO INFO if $F(x_1, \ldots, x_n) = 0$.

Key Complexity Measure: Total Share Size

Best Known Secret Sharing Schemes

Share size $\leq O(\text{monotone formula size}) \leq \tilde{O}(2^n)$. [Benaloh-Leichter'88]
Share size $\leq O(\text{monotone span program size}) \leq \tilde{O}(2^n)$. [Karchmer-Wigderson'93]

Key Complexity Measure: Total Share Size

Best Known Secret Sharing Schemes

Share size $\leq O(\text{monotone formula size}) \leq \tilde{O}(2^n)$. [Benaloh-Leichter'88]
Share size $\leq O(\text{monotone span program size}) \leq \tilde{O}(2^n)$. [Karchmer-Wigderson'93]

Lower Bounds

$\exists F$ that share size $\geq \tilde{O}(2^{n/2})$ for *linear* secret sharing. [KW'93]
$\exists F$ that total share size $\geq \tilde{\Omega}(n^2)$. [Csirmaz'97]

Key Complexity Measure: Total Share Size

Best Known Secret Sharing Schemes

Share size $\leq O(\text{monotone formula size}) \leq \tilde{O}(2^n)$. [Benaloh-Leichter'88]
Share size $\leq O(\text{monotone span program size}) \leq \tilde{O}(2^n)$. [Karchmer-Wigderson'93]

Lower Bounds

$\exists F$ that share size $\geq \tilde{O}(2^{n/2})$ for *linear* secret sharing. [KW'93]
$\exists F$ that total share size $\geq \tilde{\Omega}(n^2)$. [Csirmaz'97]

Empirical Observation: In general secret sharing, share size grows (polynomially) on representation size.

Key Complexity Measure: Total Share Size

Best Known Secret Sharing Schemes

Share size $\leq O(\text{monotone formula size}) \leq \tilde{O}(2^n)$. [Benaloh-Leichter'88]
Share size $\leq O(\text{monotone span program size}) \leq \tilde{O}(2^n)$. [Karchmer-Wigderson'93]

Lower Bounds

$\exists F$ that share size $\geq \tilde{O}(2^{n/2})$ for *linear* secret sharing. [KW'93]
$\exists F$ that total share size $\geq \tilde{\Omega}(n^2)$. [Csirmaz'97]

Empirical Observation: In general secret sharing, share size grows (polynomially) on representation size.

Representation Size Barrier?

For any collection of $2^{2^{\Omega(n)}}$ monotone access functions,
$\exists F$ in the collection that requires $2^{\Omega(n)}$ share size.

Our results

Representation Size Barrier?

For any collection of $2^{2^{\Omega(n)}}$ monotone access functions,
$\exists F$ in the collection that requires $2^{\Omega(n)}$ share size.

Our results

Representation Size Barrier?

For any collection of $2^{2^{\Omega(n)}}$ monotone access functions,
$\exists F$ in the collection that requires $2^{\Omega(n)}$ share size.

Our Theorem: Overcoming the Representation Size Barrier

There is a collection of $2^{2^{n/2}}$ monotone access functions, s.t.
$\forall F$ in the family has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.

Our results

Representation Size Barrier?

For any collection of $2^{2^{\Omega(n)}}$ monotone access functions,
$\exists F$ in the collection that requires $2^{\Omega(n)}$ share size.

Our Theorem: Overcoming the Representation Size Barrier

There is a collection of $2^{2^{n/2}}$ monotone access functions, s.t.
$\forall F$ in the family has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.

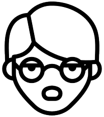
Main Tool: Multi-party Conditional Disclosure of Secrets (CDS)

Multi-party CDS scheme with communication complexity $2^{\tilde{O}(\sqrt{n})}$.

Multi-party Conditional Disclosure of Secrets

[Gertner-Ishai-Kushilevitz-Malkin'00]

$x_1 \in \{0,1\}$ $x_2 \in \{0,1\}$ $x_3 \in \{0,1\}$ $\cdots$ $x_n \in \{0,1\}$

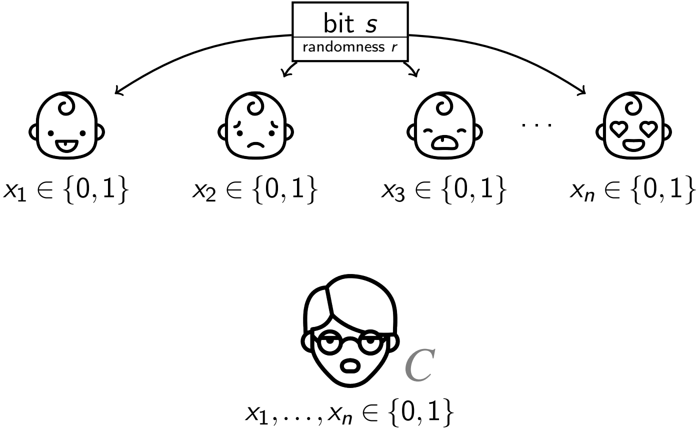


C

$x_1, \ldots, x_n \in \{0,1\}$

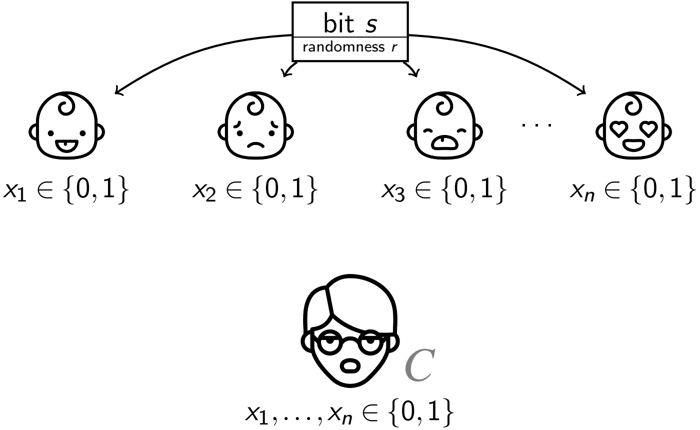
Multi-party Conditional Disclosure of Secrets

[Gertner-Ishai-Kushilevitz-Malkin'00]



Multi-party Conditional Disclosure of Secrets

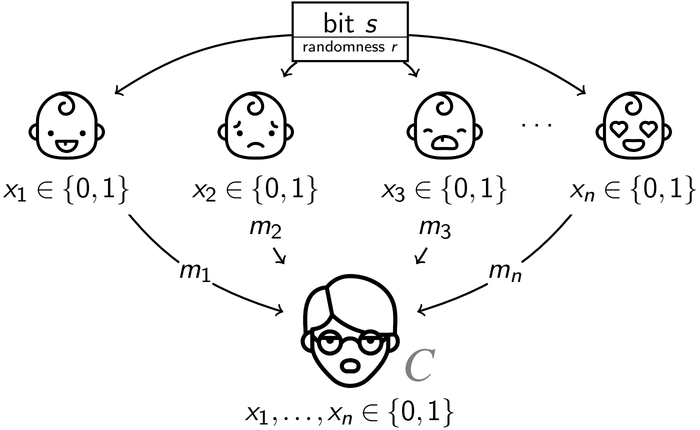
[Gertner-Ishai-Kushilevitz-Malkin'00]



gets s if and only if $F(x_1, \ldots, x_n) = 1$

Multi-party Conditional Disclosure of Secrets

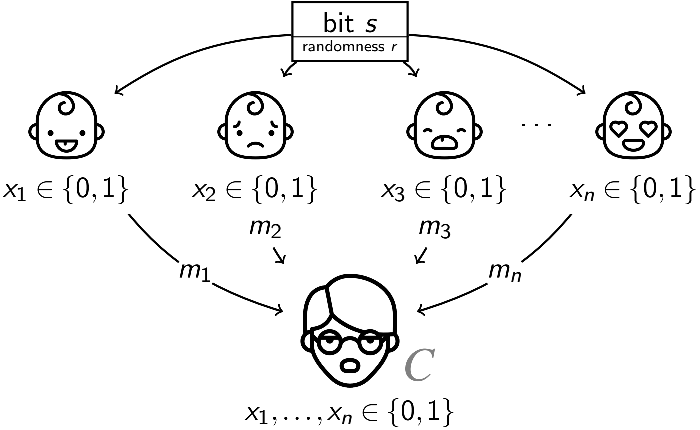
[Gertner-Ishai-Kushilevitz-Malkin'00]



gets s if and only if $F(x_1, \ldots, x_n) = 1$

Multi-party Conditional Disclosure of Secrets

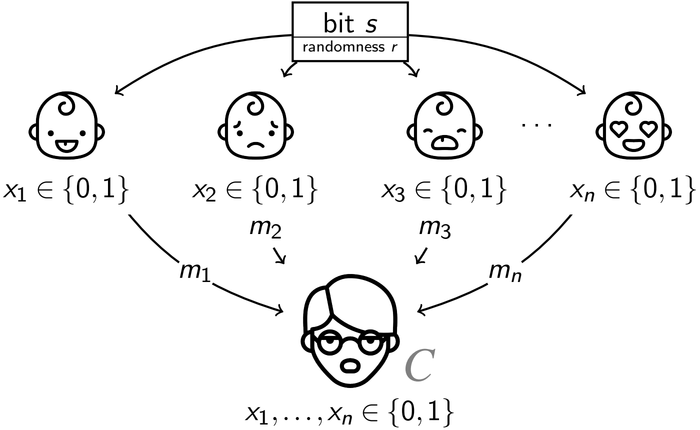
[Gertner-Ishai-Kushilevitz-Malkin'00]



- Correctness: When $F(x_1, \ldots, x_n) = 1$, Charlie gets s.

Multi-party Conditional Disclosure of Secrets

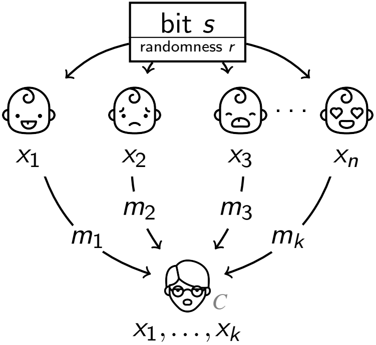
[Gertner-Ishai-Kushilevitz-Malkin'00]



- Correctness: When $F(x_1, \dots, x_n) = 1$, Charlie gets s.
- IT Privacy: When $F(x_1, \dots, x_n) = 0$, Charlie learns nothing about s.

Multi-party Conditional Disclosure of Secrets [GIKM'00]

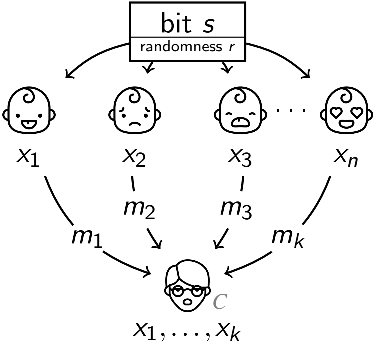
Multi-party CDS



gets s iff $F(x_1, \ldots, x_n) = 1$
for some public F

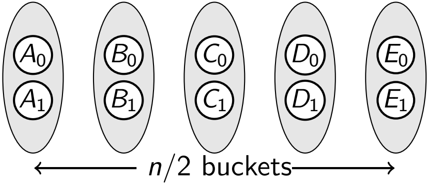
Multi-party Conditional Disclosure of Secrets [GIKM'00]

Multi-party CDS



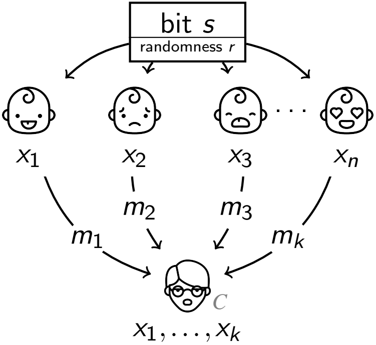
gets s iff $F(x_1, \ldots, x_n) = 1$
for some public F

"Promise" secret sharing



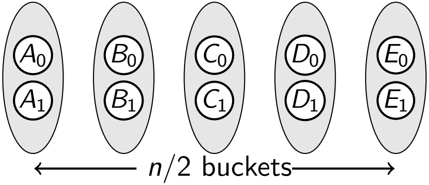
Multi-party Conditional Disclosure of Secrets [GIKM'00]

Multi-party CDS



gets s iff $F(x_1, \ldots, x_n) = 1$
for some public F

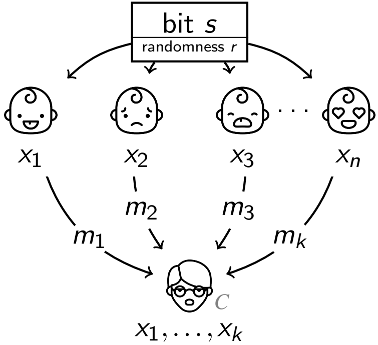
"Promise" secret sharing



- Promise: Exactly one participant from each bucket

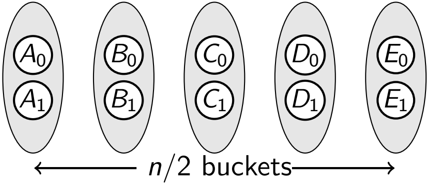
Multi-party Conditional Disclosure of Secrets [GIKM'00]

Multi-party CDS



gets s iff $F(x_1, \ldots, x_n) = 1$
for some public F

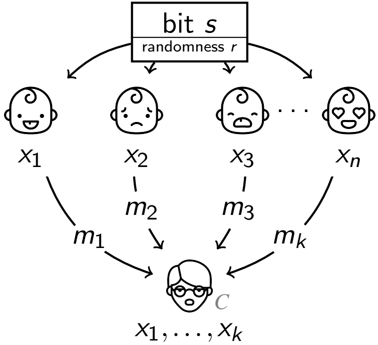
"Promise" secret sharing



- Promise: Exactly one participant from each bucket
- $A_{x_1}, B_{x_2}, \ldots, E_{x_5}$ recover s if $F(x_1, \ldots, x_5) = 1$

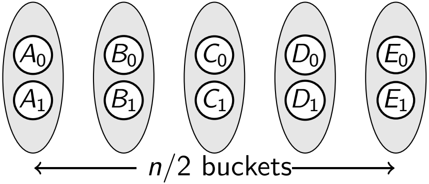
Multi-party Conditional Disclosure of Secrets [GIKM'00]

Multi-party CDS



gets s iff $F(x_1, \ldots, x_n) = 1$
for some public F

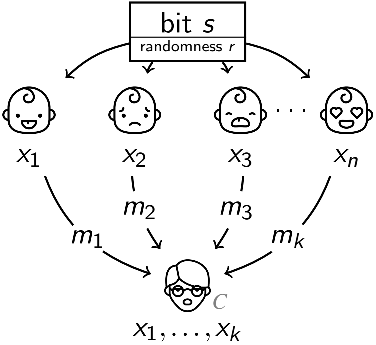
"Promise" secret sharing



- Promise: Exactly one participant from each bucket
- $A_{x_1}, B_{x_2}, \ldots, E_{x_5}$ recover s if $F(x_1, \ldots, x_5) = 1$
- $\#$ access functions $= 2^{2^{n/2}}$

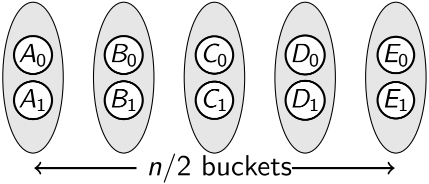
Multi-party Conditional Disclosure of Secrets [GIKM'00]

Multi-party CDS



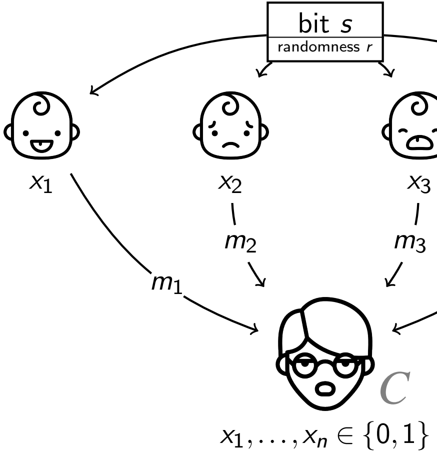
gets s iff $F(x_1, \dots, x_n) = 1$
for some public F

"Promise" secret sharing



- Promise: Exactly one participant from each bucket
- $A_{x_1}, B_{x_2}, \dots, E_{x_5}$ recover s if $F(x_1, \dots, x_5) = 1$
- $\#$ access functions $= 2^{2^{n/2}}$
- A_0's share $= m_1(0, s, r)$,
  A_1's share $= m_1(1, s, r)$, etc

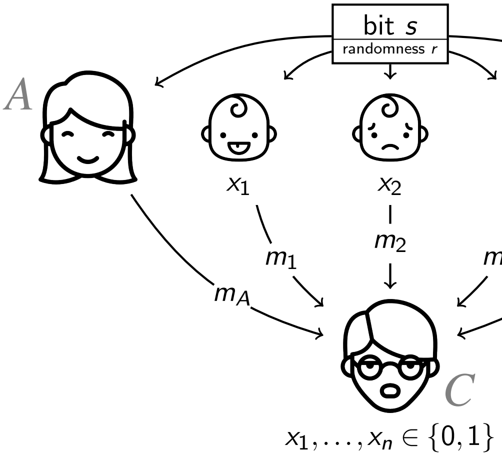
Multi-party Conditional Disclosure of Secrets [GIKM'00]



Public $F : \{0,1\}^n \to \{0,1\}$

- Correctness: When $F(x_1, \ldots, x_n) = 1$, Charlie gets s.
- IT Privacy: When $F(x_1, \ldots, x_n) = 0$, Charlie learns nothing about s.

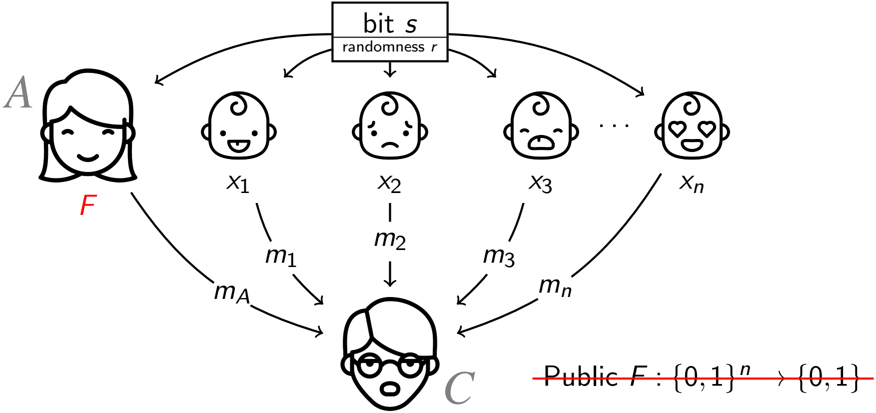
Multi-party Conditional Disclosure of Secrets [GIKM'00]



Public $F : \{0,1\}^n \to \{0,1\}$

- Correctness: When $F(x_1, \ldots, x_n) = 1$, Charlie gets s.
- IT Privacy: When $F(x_1, \ldots, x_n) = 0$, Charlie learns nothing about s.

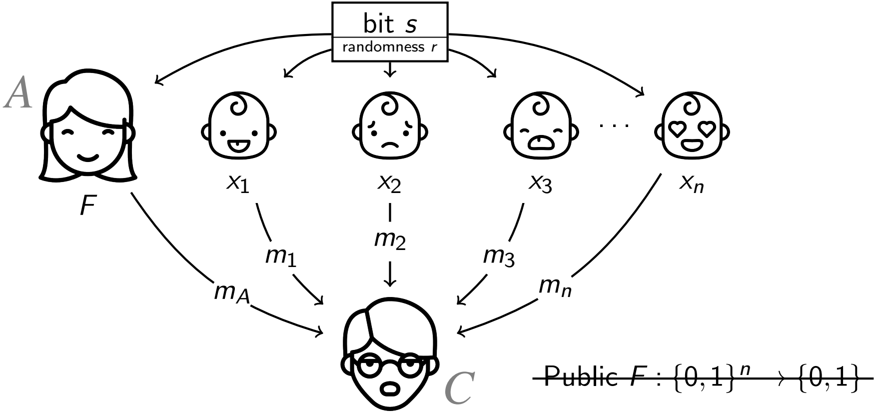
Multi-party Conditional Disclosure of Secrets [GIKM'00]



$F \in \{0,1\}^{2^n}$, $x_1, \dots, x_n \in \{0,1\}$

- Correctness: When $F(x_1, \dots, x_n) = 1$, Charlie gets s.
- IT Privacy: When $F(x_1, \dots, x_n) = 0$, Charlie learns nothing about s.

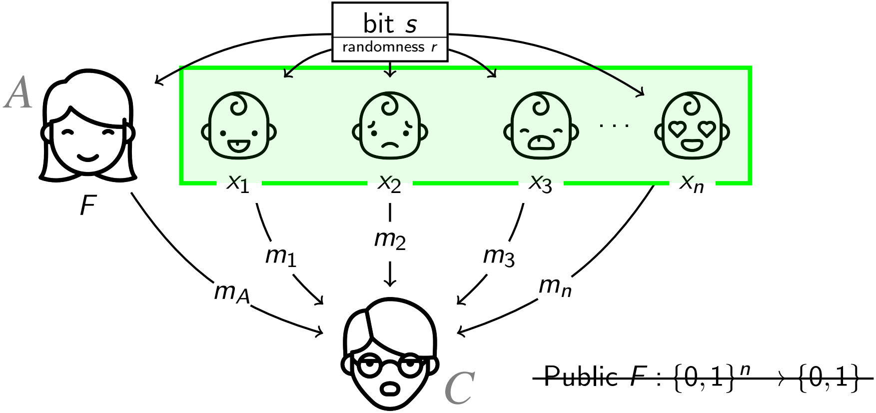
Multi-party Conditional Disclosure of Secrets [GIKM'00]



$F \in \{0,1\}^{2^n}$, $x_1, \ldots, x_n \in \{0,1\}$

- Correctness: When $F(x_1, \ldots, x_n) = 1$, Charlie gets s.
- IT Privacy: When $F(x_1, \ldots, x_n) = 0$, Charlie learns nothing about s.

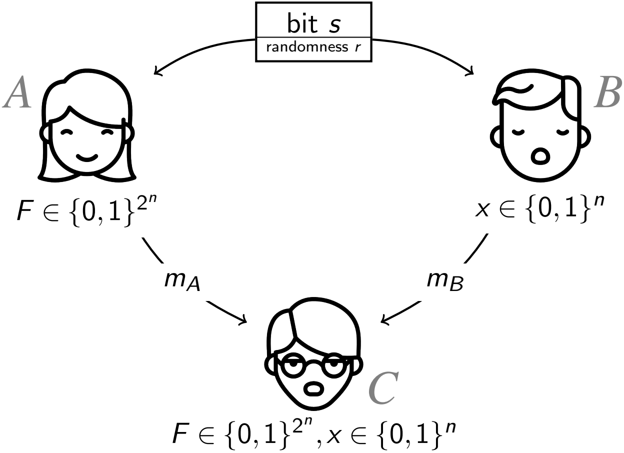
Multi-party Conditional Disclosure of Secrets [GIKM'00]



$F \in \{0,1\}^{2^n}$, $x_1, \ldots, x_n \in \{0,1\}$

- Correctness: When $F(x_1, \ldots, x_n) = 1$, Charlie gets s.
- IT Privacy: When $F(x_1, \ldots, x_n) = 0$, Charlie learns nothing about s.

2-party Conditional Disclosure of Secrets [GIKM'00]



- Correctness: When $F(x) = 1$, Charlie gets s.
- IT Privacy: When $F(x) = 0$, Charlie learns nothing about s.

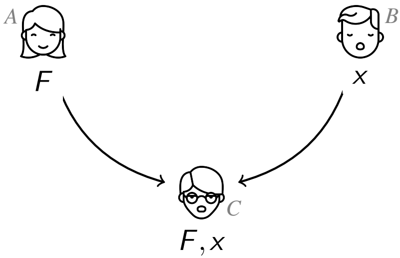
2-party CDS: Previous Works

2-Party CDS

Communication Complexity		Reconstruction
$\Theta(2^{n/2})$	[GKW'15]	linear
$\Theta(2^{n/3})$	[LVW'17]	quadratic
$2^{\tilde{O}(\sqrt{n})}$	[LVW'17]	general
$\Omega(n)$	[GKW'15]	general

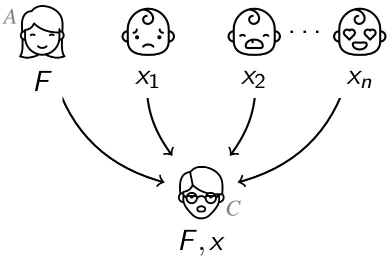
2-party CDS $\implies$ Multi-party CDS

2-party CDS



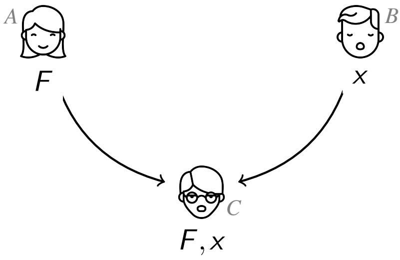
- $O(2^{n/2})$ linear reconstruction [GKW'15]
- $O(2^{n/3})$ quadratic reconstruction [LVW'17]
- $2^{\tilde{O}(\sqrt{n})}$ general reconstruction [LVW'17]

Multi-party CDS



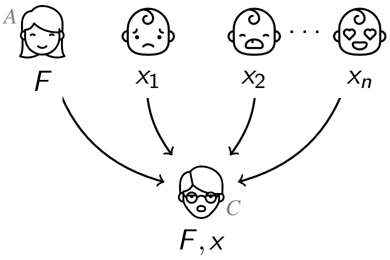
2-party CDS $\Longrightarrow$ Multi-party CDS

2-party CDS



- $O(2^{n/2})$ linear reconstruction [GKW'15]
- $O(2^{n/3})$ quadratic reconstruction [LVW'17]
- $2^{\tilde{O}(\sqrt{n})}$ general reconstruction [LVW'17]

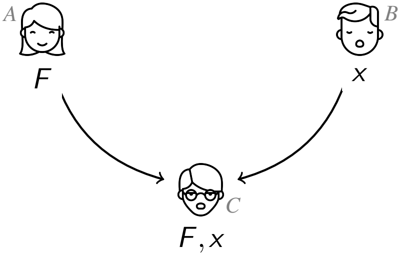
Multi-party CDS



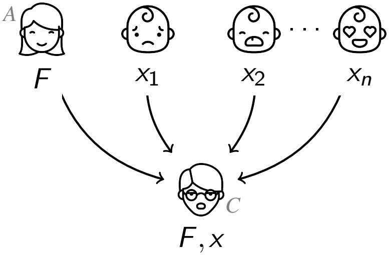
???

2-party CDS $\Longrightarrow$ Multi-party CDS

2-party CDS



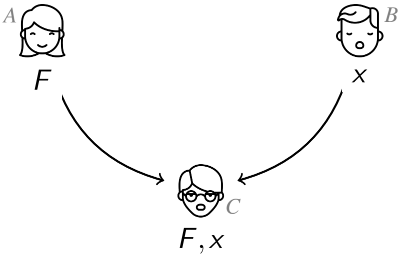
Multi-party CDS



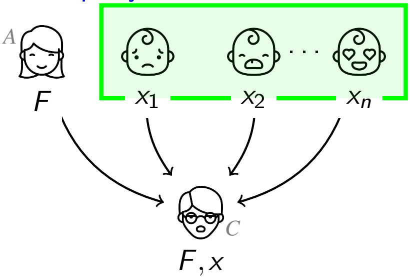
- $O(2^{n/2})$ linear reconstruction [GKW'15] $\longrightarrow$ $O(2^{n/2})$ linear reconstruction
- $O(2^{n/3})$ quadratic reconstruction [LVW'17] $\longrightarrow$ $O(2^{n/3})$ quadratic reconstruction
- $2^{\tilde{O}(\sqrt{n})}$ general reconstruction [LVW'17] $\longrightarrow$ $2^{\tilde{O}(\sqrt{n})}$ general reconstruction

2-party CDS $\Longrightarrow$ Multi-party CDS

2-party CDS



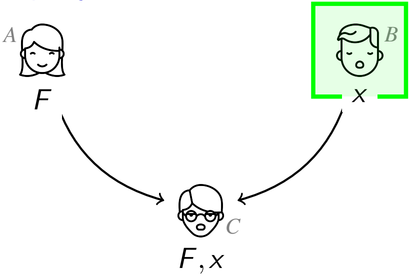
Multi-party CDS



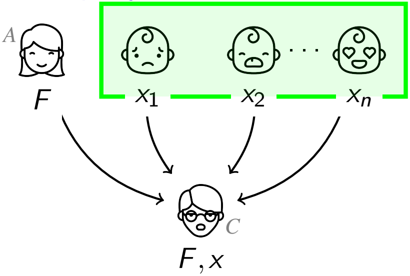
- $O(2^{n/2})$ linear reconstruction [GKW'15] $\longrightarrow$ $O(2^{n/2})$ linear reconstruction
- $O(2^{n/3})$ quadratic reconstruction [LVW'17] $\longrightarrow$ $O(2^{n/3})$ quadratic reconstruction
- $2^{\tilde{O}(\sqrt{n})}$ general reconstruction [LVW'17] $\longrightarrow$ $2^{\tilde{O}(\sqrt{n})}$ general reconstruction

2-party CDS $\Longrightarrow$ Multi-party CDS

2-party CDS

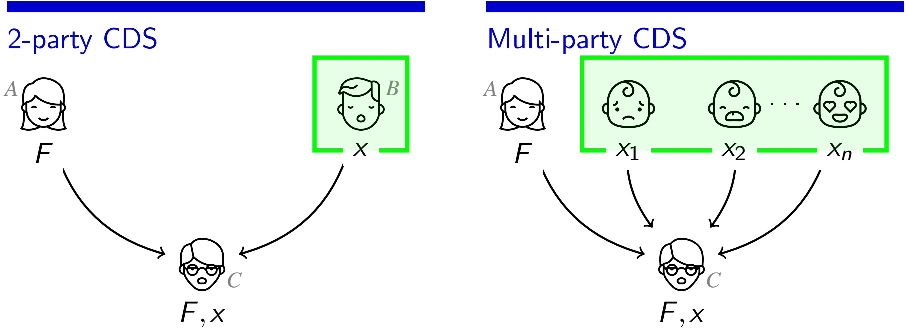


Multi-party CDS



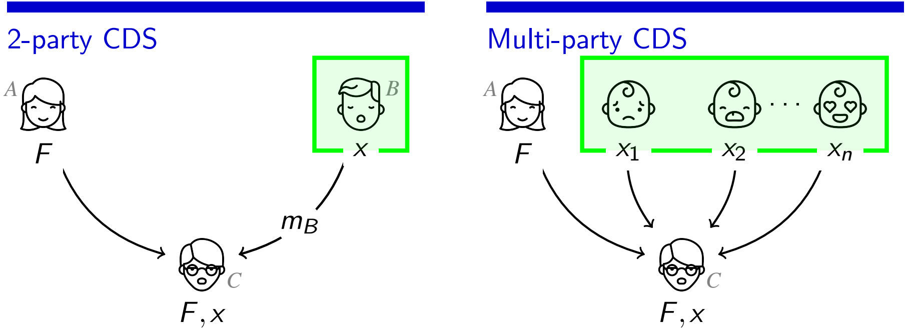
- $O(2^{n/2})$ linear reconstruction [GKW'15] $\longrightarrow$ $O(2^{n/2})$ linear reconstruction
- $O(2^{n/3})$ quadratic reconstruction [LVW'17] $\longrightarrow$ $O(2^{n/3})$ quadratic reconstruction
- $2^{\tilde{O}(\sqrt{n})}$ general reconstruction [LVW'17] $\longrightarrow$ $2^{\tilde{O}(\sqrt{n})}$ general reconstruction

2-party CDS $\Longrightarrow$ Multi-party CDS



Key Idea: Player Emulation [Hirt-Maurer'00]

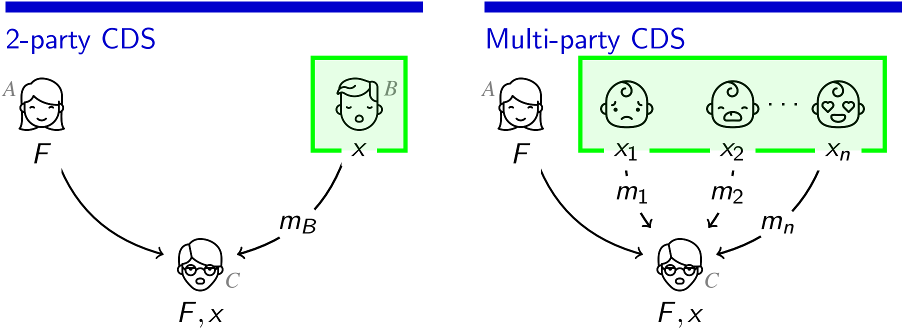
2-party CDS $\implies$ Multi-party CDS



Key Idea: Player Emulation [Hirt-Maurer'00]

- What is sent by Bob? $m_B(x, s, r)$

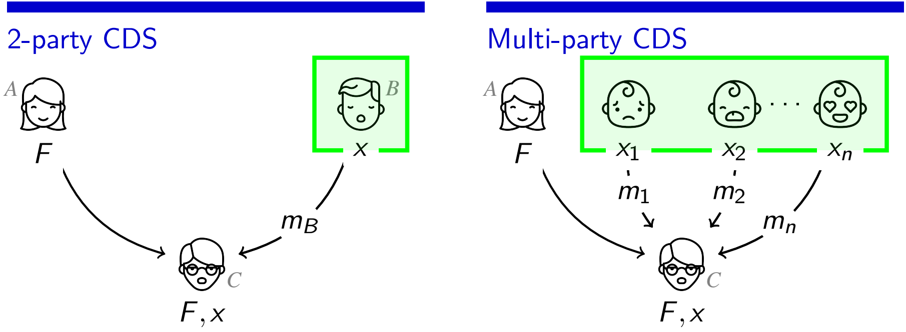
2-party CDS $\Longrightarrow$ Multi-party CDS



Key Idea: Player Emulation [Hirt-Maurer'00]

- What is sent by Bob? $m_B(x, s, r)$
- How can n players jointly compute m_B... revealing nothing else?

2-party CDS $\implies$ Multi-party CDS



Key Idea: Player Emulation [Hirt-Maurer'00]

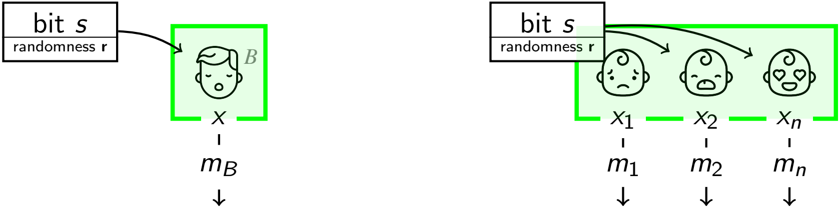
- What is sent by Bob? $m_B(x, s, r)$
- How can n players jointly compute m_B... revealing nothing else?
- PSM (Private Simultaneous Messages) [FKN'94] $\approx$ Non-Interactive MPC

2-party CDS $\Longrightarrow$ Multi-party CDS

2-party CDS $\Longrightarrow$ Multi-party CDS

What is sent by Bob?

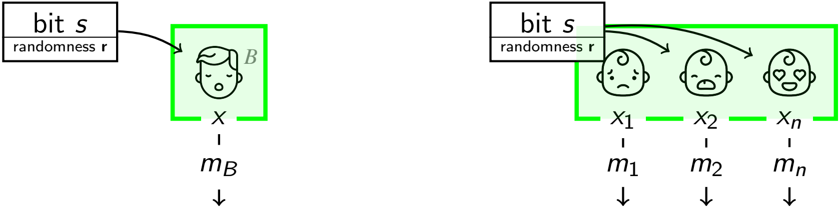
2-party CDS $\Longrightarrow$ Multi-party CDS



What is sent by Bob?

- Bob sends $m_B := \mathbf{r} + s \cdot \mathbf{u}_x$

2-party CDS $\Longrightarrow$ Multi-party CDS



What is sent by Bob?

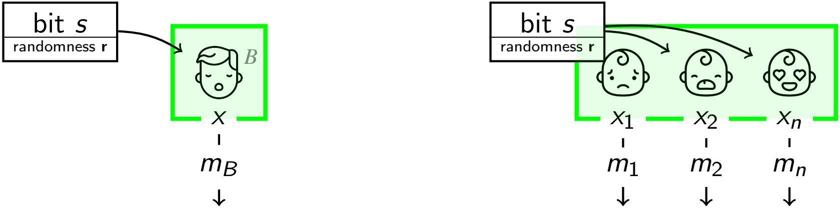
- Bob sends $m_B := \mathbf{r} + s \cdot \mathbf{u}_x$
- $\mathbf{u}_x$: matching vector
  $\mathbf{u}_x, \mathbf{v}_x \in \mathbb{Z}_6^\ell$ for each $x \in \{0,1\}^n$
  $$\langle \mathbf{u}_x, \mathbf{v}_y \rangle = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$

2-party CDS $\Longrightarrow$ Multi-party CDS

What is sent by Bob?

- Bob sends $m_B := \mathbf{r} + s \cdot \mathbf{u}_x$
- $\mathbf{u}_x$: matching vector
  $\mathbf{u}_x, \mathbf{v}_x \in \mathbb{Z}_6^\ell$ for each $x \in \{0,1\}^n$
  $$\langle \mathbf{u}_x, \mathbf{v}_y \rangle = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$
- $\ell = 2^{O(\sqrt{n \log n})}$ [BBR'94,Gro'00]

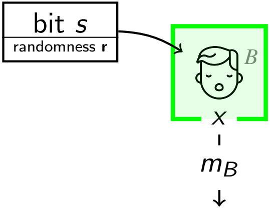
2-party CDS $\Longrightarrow$ Multi-party CDS

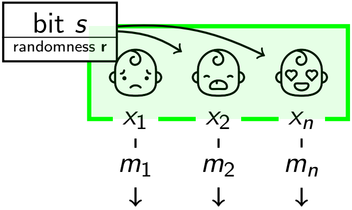


What is sent by Bob?

- Bob sends $m_B := \mathbf{r} + s \cdot \mathbf{u}_x$
- $\mathbf{u}_x$: matching vector
  $\mathbf{u}_x, \mathbf{v}_x \in \mathbb{Z}_6^\ell$ for each $x \in \{0,1\}^n$
  $$\langle \mathbf{u}_x, \mathbf{v}_y \rangle = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$
- $\ell = 2^{O(\sqrt{n \log n})}$ [BBR'94,Gro'00]
- Communication $= \ell = 2^{O(\sqrt{n \log n})}$

2-party CDS $\Longrightarrow$ Multi-party CDS



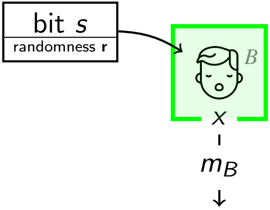


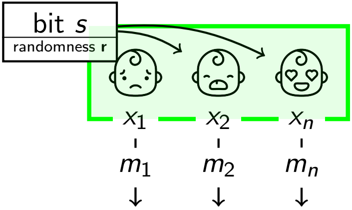
What is sent by Bob?

- Bob sends $m_B := \mathbf{r} + s \cdot \mathbf{u}_x$
- $\mathbf{u}_x$: matching vector
  $\mathbf{u}_x, \mathbf{v}_x \in \mathbb{Z}_6^\ell$ for each $x \in \{0,1\}^n$
  $$\langle \mathbf{u}_x, \mathbf{v}_y \rangle = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$
- $\ell = 2^{O(\sqrt{n \log n})}$ [BBR'94,Gro'00]
- Communication $= \ell = 2^{O(\sqrt{n \log n})}$

PSM protocol computing m_B?

2-party CDS $\implies$ Multi-party CDS





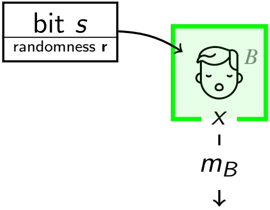
What is sent by Bob?

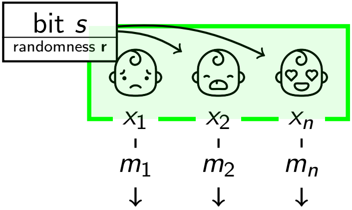
- Bob sends $m_B := \mathbf{r} + s \cdot \mathbf{u}_x$
- $\mathbf{u}_x$: matching vector
  $\mathbf{u}_x, \mathbf{v}_x \in \mathbb{Z}_6^\ell$ for each $x \in \{0,1\}^n$
  $$\langle \mathbf{u}_x, \mathbf{v}_y \rangle = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$
- $\ell = 2^{O(\sqrt{n \log n})}$ [BBR'94,Gro'00]
- Communication $= \ell = 2^{O(\sqrt{n \log n})}$

PSM protocol computing m_B?

- If $m_B(x, s, \mathbf{r})$ computable by small arithmetic formula, PSM communication is small. [IK'02,AIK'04]

2-party CDS $\Longrightarrow$ Multi-party CDS





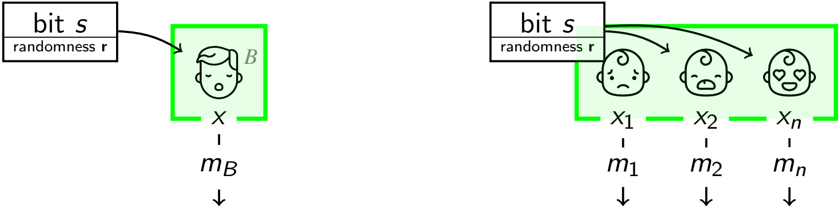
What is sent by Bob?

- Bob sends $m_B := \mathbf{r} + s \cdot \mathbf{u}_x$
- $\mathbf{u}_x$: matching vector
  $\mathbf{u}_x, \mathbf{v}_x \in \mathbb{Z}_6^\ell$ for each $x \in \{0,1\}^n$
  $$\langle \mathbf{u}_x, \mathbf{v}_y \rangle = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$
- $\ell = 2^{O(\sqrt{n \log n})}$ [BBR'94,Gro'00]
- Communication $= \ell = 2^{O(\sqrt{n \log n})}$

PSM protocol computing m_B?

- If $m_B(x, s, \mathbf{r})$ computable by small arithmetic formula, PSM communication is small. [IK'02,AIK'04]
- Is $x \mapsto \mathbf{u}_x$ simple?

2-party CDS $\implies$ Multi-party CDS



New Construction of Matching Vectors

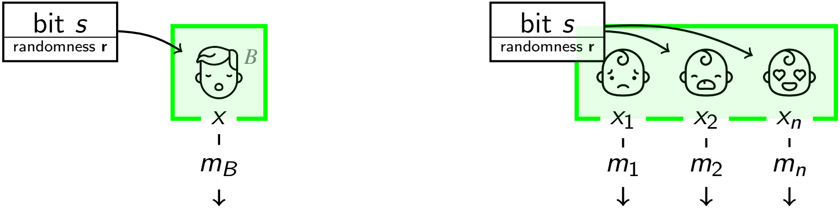
- mapping $x \mapsto \mathbf{u}_x$ computable by small formula

2-party CDS $\Longrightarrow$ Multi-party CDS

New Construction of Matching Vectors

- mapping $x \mapsto \mathbf{u}_x$ computable by small formula
- $\forall x,\ \mathbf{u}_x = \mathbf{u}_{1,x_1} \circ \ldots \circ \mathbf{u}_{n,x_n}$
  n pairs of vectors $(\mathbf{u}_{1,0}, \mathbf{u}_{1,1}), \ldots, (\mathbf{u}_{n,0}, \mathbf{u}_{n,1})$

2-party CDS $\Longrightarrow$ Multi-party CDS



New Construction of Matching Vectors

- mapping $x \mapsto \mathbf{u}_x$ computable by small formula
- $\forall x,\ \mathbf{u}_x = \mathbf{u}_{1,x_1} \circ \ldots \circ \mathbf{u}_{n,x_n}$
  n pairs of vectors $(\mathbf{u}_{1,0}, \mathbf{u}_{1,1}), \ldots, (\mathbf{u}_{n,0}, \mathbf{u}_{n,1})$
- i-th bit of $m_B = \mathbf{r} + s \cdot \mathbf{u}_x$ computable by
  size-$O(n)$ arithmetic formula $\mathbf{r}[i] + s \cdot \mathbf{u}_{1,x_1}[i] \cdot \ldots \cdot \mathbf{u}_{n,x_n}[i]$

2-party CDS $\Longrightarrow$ Multi-party CDS

New Construction of Matching Vectors

- mapping $x \mapsto \mathbf{u}_x$ computable by small formula
- $\forall x,\ \mathbf{u}_x = \mathbf{u}_{1,x_1} \circ \ldots \circ \mathbf{u}_{n,x_n}$
  n pairs of vectors $(\mathbf{u}_{1,0}, \mathbf{u}_{1,1}), \ldots, (\mathbf{u}_{n,0}, \mathbf{u}_{n,1})$
- i-th bit of $m_B = \mathbf{r} + s \cdot \mathbf{u}_x$ computable by
  size-$O(n)$ arithmetic formula $\mathbf{r}[i] + s \cdot \mathbf{u}_{1,x_1}[i] \cdot \ldots \cdot \mathbf{u}_{n,x_n}[i]$
- $\ell =$ ~~$2^{O(\sqrt{n \log n})}$~~ $2^{O(\sqrt{n}\log n)}$

2-party CDS $\implies$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

2-party CDS $\Longrightarrow$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

- Each $x \in \{0,1\}^n$ is mapped to $\mathbf{z}_x \in \{0,1\}^{n^2}$ s.t. $\mathbf{z}_x$ has $\frac{n}{\log n}$ 1's

2-party CDS $\Longrightarrow$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

- Each $x \in \{0,1\}^n$ is mapped to $\mathbf{z}_x \in \{0,1\}^{n^2}$ s.t. $\mathbf{z}_x$ has $\frac{n}{\log n}$ 1's
- There exists polynomials $\{p_x\}_x$ for each x s.t. degree-$O(\sqrt{n/\log n})$ over $\mathbb{Z}_6$

$$p_y(\mathbf{z}_x) = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$

2-party CDS $\implies$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

- Each $x \in \{0,1\}^n$ is mapped to $\mathbf{z}_x \in \{0,1\}^{n^2}$ s.t. $\mathbf{z}_x$ has $\frac{n}{\log n}$ 1's
- There exists polynomials $\{p_x\}_x$ for each x s.t. degree-$O(\sqrt{n/\log n})$ over $\mathbb{Z}_6$
$$p_y(\mathbf{z}_x) = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$
- Let $\mathbf{v}_x$ be the coefficients of p_y and $\mathbf{u}_x$ be all degree-$O(\sqrt{n/\log n})$ monomials of $\mathbf{z}_x$

2-party CDS $\Longrightarrow$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

- Each $x \in \{0,1\}^n$ is mapped to $\mathbf{z}_x \in \{0,1\}^{n^2}$ s.t. $\mathbf{z}_x$ has $\frac{n}{\log n}$ 1's
- There exists polynomials $\{p_x\}_x$ for each x s.t. degree-$O(\sqrt{n/\log n})$ over $\mathbb{Z}_6$

  $$p_y(\mathbf{z}_x) = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$

- Let $\mathbf{v}_x$ be the coefficients of p_y and $\mathbf{u}_x$ be all degree-$O(\sqrt{n/\log n})$ monomials of $\mathbf{z}_x$
- $\langle \mathbf{u}_x, \mathbf{v}_y \rangle = p_y(\mathbf{z}_x)$ length $=$ # monomials $= (n^2)^{O(\sqrt{n/\log n})} = 2^{O(\sqrt{n \log n})}$

2-party CDS $\Longrightarrow$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

- Each $x \in \{0,1\}^n$ is mapped to $\mathbf{z}_x \in \{0,1\}^{n^2}$ s.t. $\mathbf{z}_x$ has $\frac{n}{\log n}$ 1's
- There exists polynomials $\{p_x\}_x$ for each x s.t. degree-$O(\sqrt{n/\log n})$ over $\mathbb{Z}_6$

$$p_y(\mathbf{z}_x) = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$

- Let $\mathbf{v}_x$ be the coefficients of p_y and $\mathbf{u}_x$ be all degree-$O(\sqrt{n/\log n})$ monomials of $\mathbf{z}_x$
- $\langle \mathbf{u}_x, \mathbf{v}_y \rangle = p_y(\mathbf{z}_x)$
  length $= \#$ monomials $= (n^2)^{O(\sqrt{n/\log n})} = 2^{O(\sqrt{n \log n})}$

simple
$\mathbf{z}_x \mapsto \mathbf{u}_x$

2-party CDS $\Longrightarrow$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

- Each $x \in \{0,1\}^n$ is mapped to $\mathbf{z}_x \in \{0,1\}^{n^2}$ s.t. $\mathbf{z}_x$ has $\frac{n}{\log n}$ 1's — simplify $x \mapsto \mathbf{z}_x$
- There exists polynomials $\{p_x\}_x$ for each x s.t. degree-$O(\sqrt{n/\log n})$ over $\mathbb{Z}_6$

$$p_y(\mathbf{z}_x) = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$

- Let $\mathbf{v}_x$ be the coefficients of p_y and $\mathbf{u}_x$ be all degree-$O(\sqrt{n/\log n})$ monomials of $\mathbf{z}_x$ — simple $\mathbf{z}_x \mapsto \mathbf{u}_x$
- $\langle \mathbf{u}_x, \mathbf{v}_y \rangle = p_y(\mathbf{z}_x)$
length $= \#$ monomials $= (n^2)^{O(\sqrt{n/\log n})} = 2^{O(\sqrt{n \log n})}$

2-party CDS $\implies$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

- Each $x \in \{0,1\}^n$ is mapped to $\mathbf{z}_x \in \{0,1\}^{2n}$ s.t. $\mathbf{z}_x$ has n 1's — simplify $x \mapsto \mathbf{z}_x$
- There exists polynomials $\{p_x\}_x$ for each x s.t. degree-$O(\sqrt{n/\log n})$ over $\mathbb{Z}_6$
$$p_y(\mathbf{z}_x) = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$
- Let $\mathbf{v}_x$ be the coefficients of p_y and $\mathbf{u}_x$ be all degree-$O(\sqrt{n/\log n})$ monomials of $\mathbf{z}_x$ — simple $\mathbf{z}_x \mapsto \mathbf{u}_x$
- $\langle \mathbf{u}_x, \mathbf{v}_y \rangle = p_y(\mathbf{z}_x)$
length $= \#$ monomials $= (n^2)^{O(\sqrt{n/\log n})} = 2^{O(\sqrt{n \log n})}$

2-party CDS $\implies$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

- Each $x \in \{0,1\}^n$ is mapped to $\mathbf{z}_x \in \{0,1\}^{2n}$ s.t. $\mathbf{z}_x$ has n 1's; map $0 \mapsto 01$, $1 \mapsto 10$

  simplify $x \mapsto \mathbf{z}_x$

- There exists polynomials $\{p_x\}_x$ for each x s.t. degree-$O(\sqrt{n/\log n})$ over $\mathbb{Z}_6$
  $$p_y(\mathbf{z}_x) = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$
- Let $\mathbf{v}_x$ be the coefficients of p_y and $\mathbf{u}_x$ be all degree-$O(\sqrt{n/\log n})$ monomials of $\mathbf{z}_x$

  simple $\mathbf{z}_x \mapsto \mathbf{u}_x$

- $\langle \mathbf{u}_x, \mathbf{v}_y \rangle = p_y(\mathbf{z}_x)$
  length $= \#$ monomials $= (n^2)^{O(\sqrt{n/\log n})} = 2^{O(\sqrt{n \log n})}$

2-party CDS $\implies$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

- Each $x \in \{0,1\}^n$ is mapped to $\mathbf{z}_x \in \{0,1\}^{2n}$ s.t. $\mathbf{z}_x$ has n 1's; map $0 \mapsto 01$, $1 \mapsto 10$

  simplify $x \mapsto \mathbf{z}_x$

- There exists polynomials $\{p_x\}_x$ for each x s.t. degree-$O(\sqrt{n})$ over $\mathbb{Z}_6$

$$p_y(\mathbf{z}_x) = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$

- Let $\mathbf{v}_x$ be the coefficients of p_y and $\mathbf{u}_x$ be all degree-$O(\sqrt{n})$ monomials of $\mathbf{z}_x$

  simple $\mathbf{z}_x \mapsto \mathbf{u}_x$

- $\langle \mathbf{u}_x, \mathbf{v}_y \rangle = p_y(\mathbf{z}_x)$
  length $= \#$ monomials $= (n^2)^{O(\sqrt{n/\log n})} = 2^{O(\sqrt{n \log n})}$

2-party CDS $\implies$ Multi-party CDS

New Construction of Matching Vectors $x \mapsto (\mathbf{u}_x, \mathbf{v}_x)$

- Each $x \in \{0,1\}^n$ is mapped to $\mathbf{z}_x \in \{0,1\}^{2n}$ s.t. $\mathbf{z}_x$ has n 1's; map $0 \mapsto 01$, $1 \mapsto 10$

  simplify $x \mapsto \mathbf{z}_x$

- There exists polynomials $\{p_x\}_x$ for each x s.t. degree-$O(\sqrt{n})$ over $\mathbb{Z}_6$

$$p_y(\mathbf{z}_x) = \begin{cases} 0, & \text{if } x = y \\ \neq 0, & \text{o.w.} \end{cases}$$

- Let $\mathbf{v}_x$ be the coefficients of p_y and $\mathbf{u}_x$ be all degree-$O(\sqrt{n})$ monomials of $\mathbf{z}_x$

  simple $\mathbf{z}_x \mapsto \mathbf{u}_x$

- $\langle \mathbf{u}_x, \mathbf{v}_y \rangle = p_y(\mathbf{z}_x)$
  length $= \#$ monomials $= (2n)^{O(\sqrt{n})} = 2^{O(\sqrt{n} \log n)}$

2-party CDS $\implies$ Multi-party CDS

- Simpler matching vector $x \mapsto \mathbf{u}_x$

2-party CDS $\implies$ Multi-party CDS

- Simpler matching vector $x \mapsto \mathbf{u}_x$
- (2-party CDS) Bob's message is a small formula

2-party CDS $\implies$ Multi-party CDS

- Simpler matching vector $x \mapsto \mathbf{u}_x$
- (2-party CDS) Bob's message is a small formula
- (multi-party CDS) n parties can be efficiently emulate Bob

Our Results

- Simpler matching vector $x \mapsto \mathbf{u}_x$
- (2-party CDS) Bob's message is a small formula
- (multi-party CDS) n parties can be efficiently emulate Bob

Multi-party CDS

There is a multi-party CDS scheme with communication complexity $2^{O(\sqrt{n}\log n)}$ as long as the total input length is n bits.

Our Results

- Simpler matching vector $x \mapsto \mathbf{u}_x$
- (2-party CDS) Bob's message is a small formula
- (multi-party CDS) n parties can be efficiently emulate Bob

Multi-party CDS

There is a multi-party CDS scheme with communication complexity $2^{O(\sqrt{n}\log n)}$ as long as the total input length is n bits.

Secret sharing for double-exponentially many access functions

There is a collection of $2^{2^{n/2}}$ access functions, s.t.
$\forall F$ in the family has a secret sharing scheme with share size $2^{O(\sqrt{n}\log n)}$.

Our Results

2-party CDS

$O(2^{n/2})$ [GKW'15]

linear reconstruction

$O(2^{n/3})$ [LVW'17]

quadratic reconstruction

$2^{O(\sqrt{n}\log n)}$ [LVW'17] ⟶

general reconstruction

Multi-party CDS

$2^{O(\sqrt{n}\log n)}$ [This]

general reconstruction

Our Results

2-party CDS

$O(2^{n/2})$ [GKW'15] → $O(2^{n/2})$ [This,BP'18]

linear reconstruction → linear reconstruction, optimal

$O(2^{n/3})$ [LVW'17] → $O(2^{n/3})$

quadratic reconstruction → quadratic reconstruction, optimal

$2^{O(\sqrt{n}\log n)}$ [LVW'17] → $2^{O(\sqrt{n}\log n)}$ [This]

general reconstruction → general reconstruction

Multi-party CDS

Subsequent Works on Secret Sharing

Secret sharing for even more access functions [This,BKN'18]

There is a collection of $2^{\binom{n}{n/2}}$ access functions, s.t.
$\forall F$ in the family has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.

Subsequent Works on Secret Sharing

Secret sharing for even more access functions [This,BKN'18,LV'18]

There is a collection of $2^{\binom{n}{n/2}+2^{\Omega(n)}}$ access functions, s.t.
$\forall F$ in the family has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.

Subsequent Works on Secret Sharing

monotone function $\leq 2^{\binom{n}{n/2} \cdot (1 + \frac{O(\log n)}{n})}$

Secret sharing for even more access functions [This,BKN'18,LV'18]

There is a collection of $2^{\binom{n}{n/2} + 2^{\Omega(n)}}$ access functions, s.t.
$\forall F$ in the family has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.

Subsequent Works on Secret Sharing

$\#$ monotone function $\leq 2^{\binom{n}{n/2}\cdot(1+\frac{O(\log n)}{n})}$

$\updownarrow$

Secret sharing for even more access functions [This,BKN'18,LV'18]

There is a collection of $2^{\binom{n}{n/2}+2^{\Omega(n)}}$ access functions, s.t.
$\forall F$ in the family has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.

Secret sharing for all access functions [LV'18 @STOC]

$\forall F$ has a secret sharing scheme with share size $2^{0.994n}$.

To Summarize

(or representation)

Can communication $\ll$ computation size?

To Summarize

(or representation)

Can communication $\ll$ computation size?

Computational

- FHE

To Summarize

(or representation)

Can communication $\ll$ computation size?

Computational

- FHE

Information theoretic

- Private Information Retrieval

To Summarize

(or representation)

Can communication $\ll$ computation size?

Computational

- FHE

Information theoretic

- Private Information Retrieval
- Conditional Disclosure of Secrets

  2-party & multiparty case

To Summarize

(or representation)

Can communication $\ll$ computation size?

Computational

- FHE

Information theoretic

- Private Information Retrieval
- Conditional Disclosure of Secrets

  2-party & multiparty case
- Secret Sharing

  for $2^{2^{\Omega(n)}}$ access functions

  potentially for all access functions

To Summarize

(or representation)

Can communication $\ll$ computation size?

Computational

- FHE

Information theoretic

- Private Information Retrieval
- Conditional Disclosure of Secrets

  2-party & multiparty case
- Secret Sharing

  for $2^{2^{\Omega(n)}}$ access functions

  potentially for all access functions
- What's next?