Conditional Disclosure of Secrets via Non-Linear Reconstruction

Tianren Liu
MIT

Vinod Vaikuntanathan
MIT

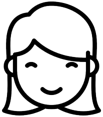
Hoeteck Wee
CNRS & ENS

September 11, 2017

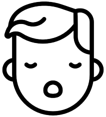
Conditional Disclosure of Secrets

[Gertner-Ishai-Kushilevitz-Malkin'00]

A

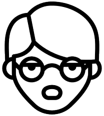


$f : [N] \to \{0, 1\}$



B

$i \in [N]$



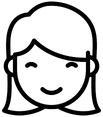
C

f, i

Conditional Disclosure of Secrets

[Gertner-Ishai-Kushilevitz-Malkin'00]

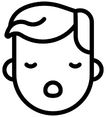
A



$f : [N] \to \{0, 1\}$

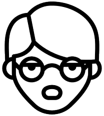
bit s

B



$i \in [N]$

bit s



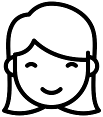
C

f, i

Conditional Disclosure of Secrets

[Gertner-Ishai-Kushilevitz-Malkin'00]

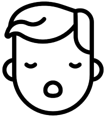
A



$f : [N] \to \{0,1\}$

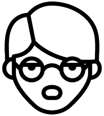
bit s

B



$i \in [N]$

bit s



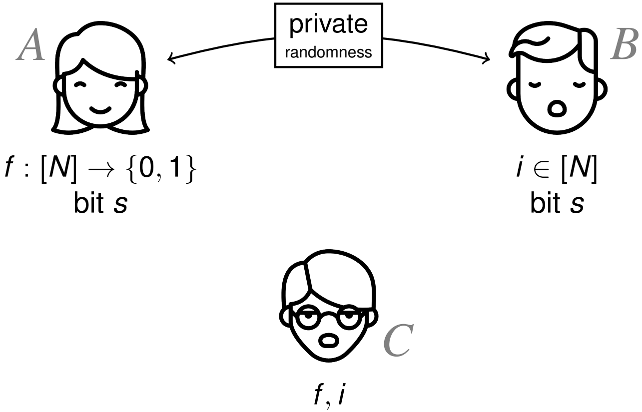
C

f, i

Charlie gets s iff $f(i) = 1$

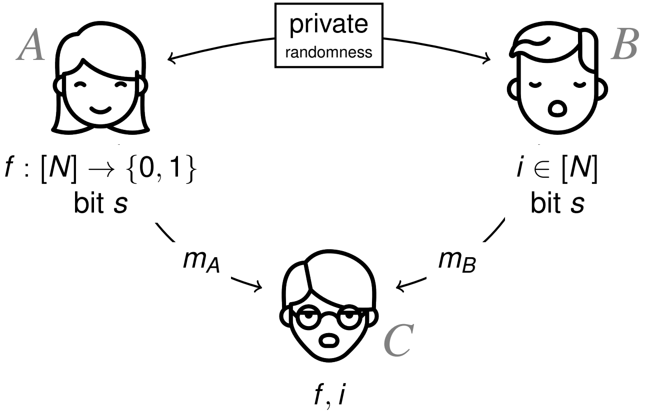
Conditional Disclosure of Secrets

[Gertner-Ishai-Kushilevitz-Malkin'00]



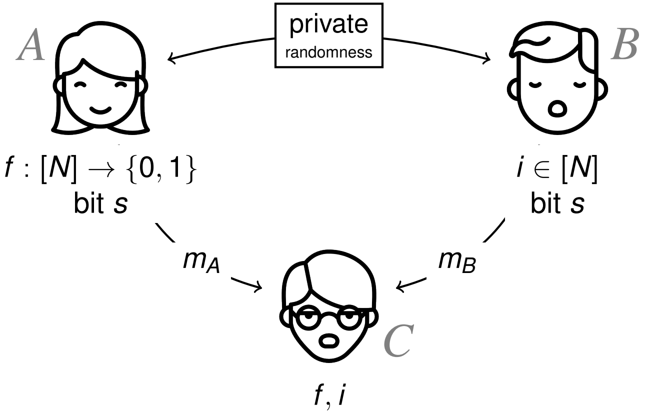
Conditional Disclosure of Secrets

[Gertner-Ishai-Kushilevitz-Malkin'00]



Conditional Disclosure of Secrets

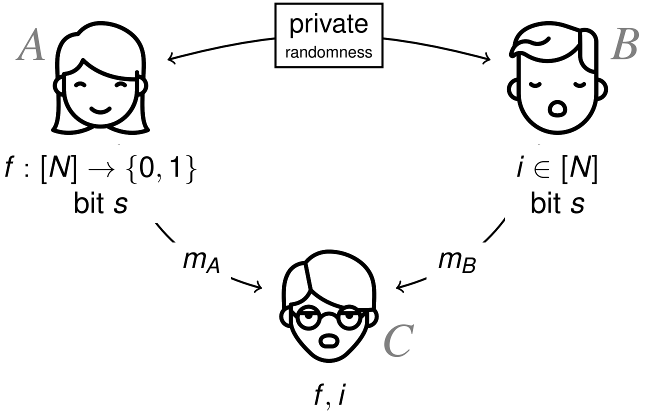
[Gertner-Ishai-Kushilevitz-Malkin'00]



- Correctness: When $f(i) = 1$, Charlie gets s.

Conditional Disclosure of Secrets

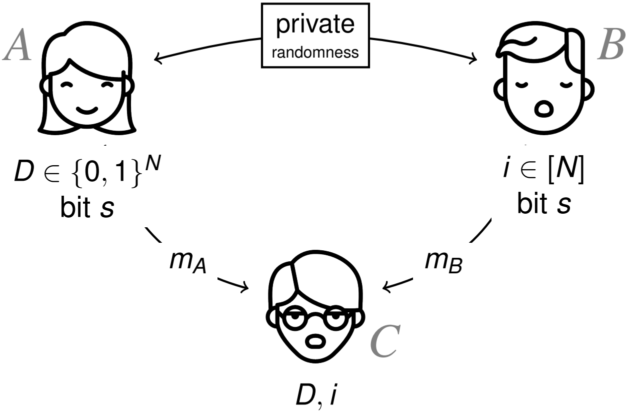
[Gertner-Ishai-Kushilevitz-Malkin'00]



- Correctness: When $f(i) = 1$, Charlie gets s.
- IT Privacy: When $f(i) = 0$, (m_A, m_B) can be *perfectly* simulated.

Conditional Disclosure of Secrets

[Gertner-Ishai-Kushilevitz-Malkin'00]

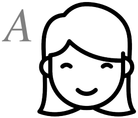


- Correctness: When $D_i = 1$, Charlie gets s.
- IT Privacy: When $D_i = 0$, (m_A, m_B) can be *perfectly* simulated.

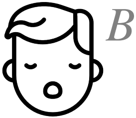
Conditional Disclosure of Secrets

- Symmetric PIR [GIKM'00]
  - How to handle malicious clients in SPIR
- Secret Sharing [SS'97,BIKK'14]
  - For certain graph-based access structures
- Attribute-Based Encryption [Att'14,Wee'14,CGW'15]
  - CDS = 1-key, 1-ciphertext, private-key ABE

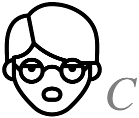
Simple CDS Protocol I



$D \in \{0,1\}^N$
bit s

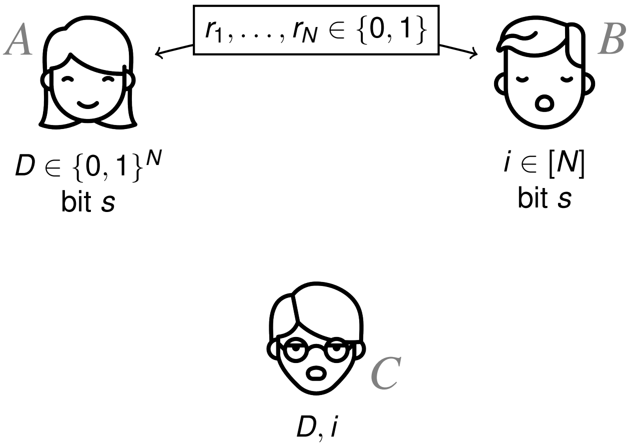


$i \in [N]$
bit s

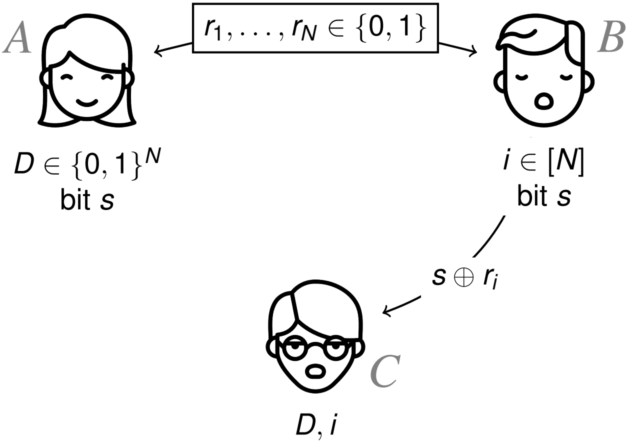


D, i

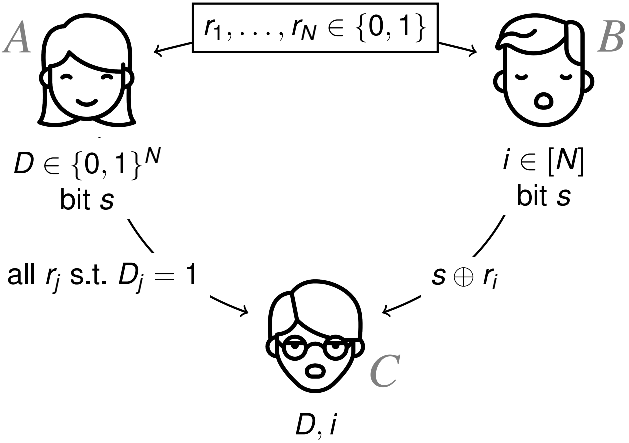
Simple CDS Protocol I



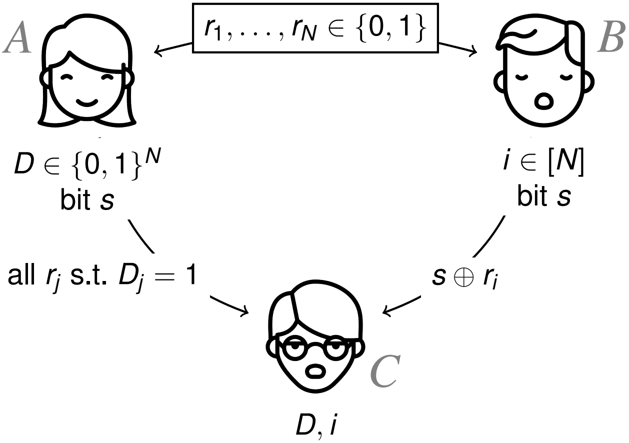
Simple CDS Protocol I



Simple CDS Protocol I

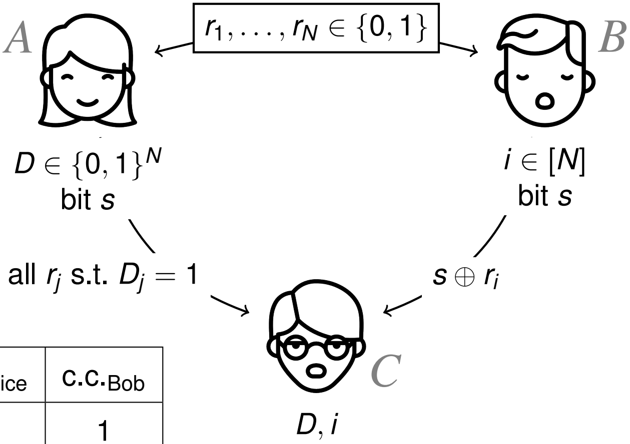


Simple CDS Protocol I



- Correctness: When $D_i = 1$, Alice sends r_i
- IT Privacy: When $D_i = 0$, Alice does not send r_i

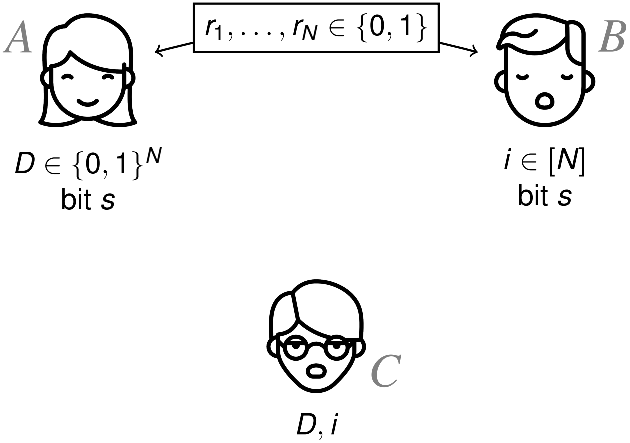
Simple CDS Protocol I



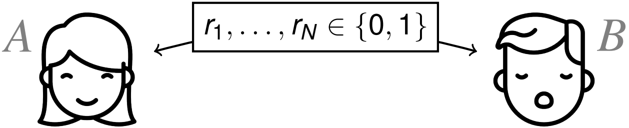
c.c.$_{\text{Alice}}$	c.c.$_{\text{Bob}}$
N	1

- Correctness: When $D_i = 1$, Alice sends r_i
- IT Privacy: When $D_i = 0$, Alice does not send r_i

Simple CDS Protocol II

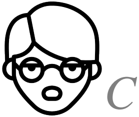


Simple CDS Protocol II



$D \in \{0, 1\}^N$
bit s

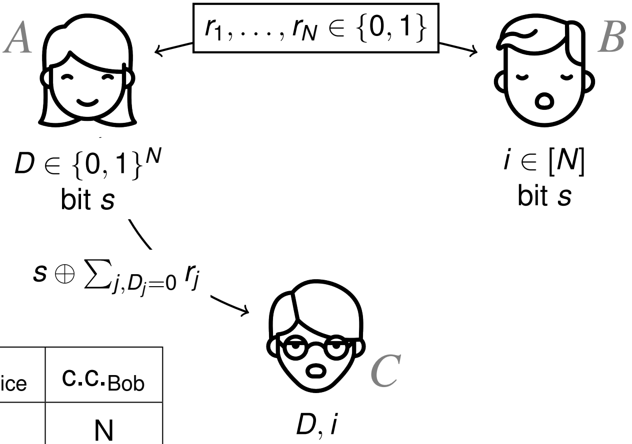
$i \in [N]$
bit s



D, i

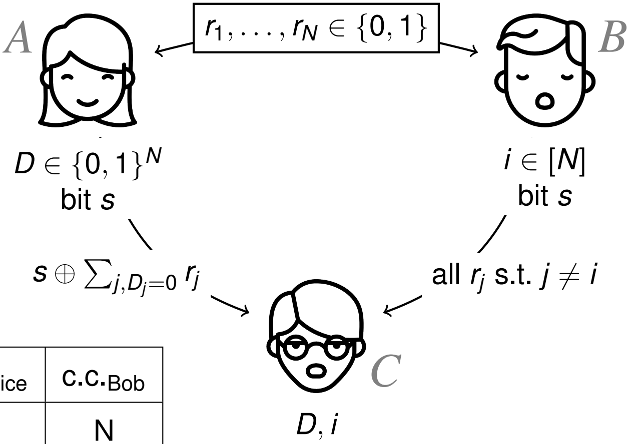
$\text{c.c.}_{\text{Alice}}$	c.c._{Bob}
1	N

Simple CDS Protocol II



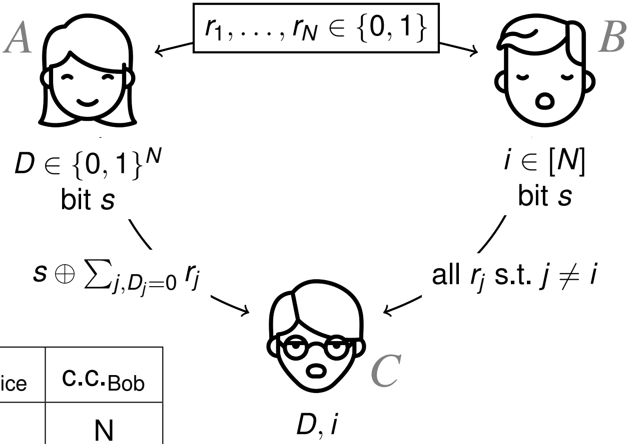
C.C.$_{\text{Alice}}$	C.C.$_{\text{Bob}}$
1	N

Simple CDS Protocol II



c.c.$_{\text{Alice}}$	c.c.$_{\text{Bob}}$
1	N

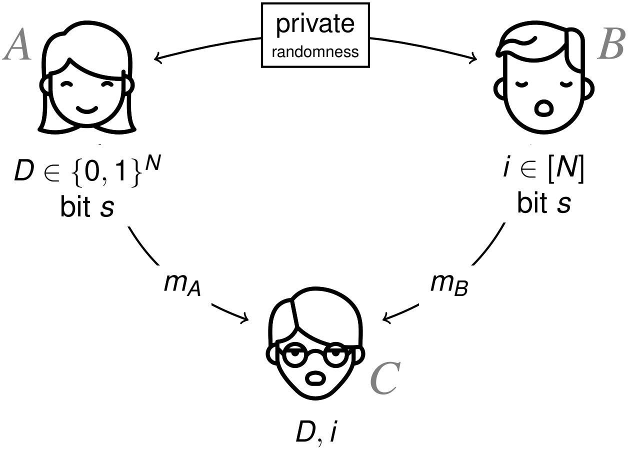
Simple CDS Protocol II



c.c.$_{\text{Alice}}$	c.c.$_{\text{Bob}}$
1	N

- Correctness: When $D_i = 1$, Bob sends all r_j s.t. $D_j = 0$
- IT Privacy: When $D_i = 0$, Bob does not send r_i

CDS with Linear Reconstruction [GKW'15]



Charlie's reconstruction function $C_{i,D}(m_A, m_B) \mapsto s$ is linear.

Previous Works

Communication Complexity	Reconstruction
$(N, 1)$	linear
$(1, N)$	linear

Previous Works

Communication Complexity		Reconstruction
$(N, 1)$		linear
$(1, N)$		linear
$O(\sqrt{N})$	[GKW'15,...]	linear

Previous Works

Communication Complexity		Reconstruction
$(N, 1)$		linear
$(1, N)$		linear
$O(\sqrt{N})$	[GKW'15,...]	linear
$\Omega(\sqrt{N})$	[GKW'15]	linear

Previous Works

Communication Complexity		Reconstruction
$(N, 1)$		linear
$(1, N)$		linear
$O(\sqrt{N})$	[GKW'15,...]	linear
$\Omega(\sqrt{N})$	[GKW'15]	linear
$\Omega(\log N)$	[GKW'15]	general

Previous Works

Communication Complexity		Reconstruction
$(N, 1)$		linear
$(1, N)$		linear
$O(\sqrt{N})$	[GKW'15,...]	linear
$\Omega(\sqrt{N})$	[GKW'15]	linear
An exponential gap here Non-linear reconstruction needed!		
$\Omega(\log N)$	[GKW'15]	general

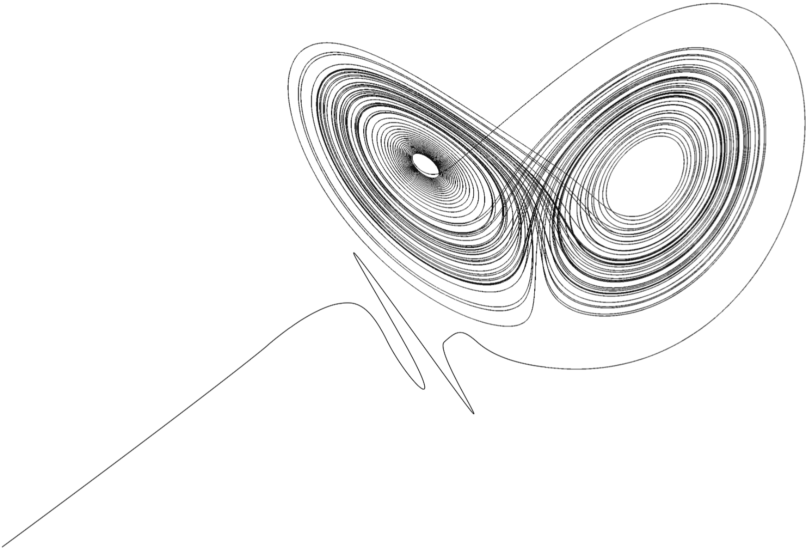
Our Results

Communication Complexity		Reconstruction
$(N, 1)$		linear
$(1, N)$		linear
$O(\sqrt{N})$	[GKW'15,...]	linear
$\Omega(\sqrt{N})$	[GKW'15]	linear
$\Theta(\sqrt[3]{N})$	[This work]	quadratic
$\Omega(\log N)$	[GKW'15]	general

Our Results

Communication Complexity		Reconstruction
$(N, 1)$		linear
$(1, N)$		linear
$O(\sqrt{N})$	[GKW'15,...]	linear
$\Omega(\sqrt{N})$	[GKW'15]	linear
$\Theta(\sqrt[3]{N})$	[This work]	quadratic
$2^{\tilde{O}(\sqrt{\log N})}$	[This work]	general
$\Omega(\log N)$	[GKW'15]	general

CDS: Need Non-linear Techniques!



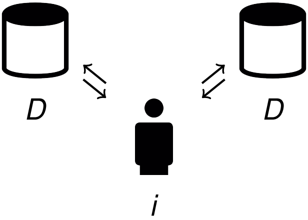
CDS: Need Non-linear Techniques!

2-server PIR
[CGKS'95]

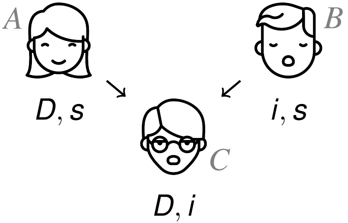
CDS
[GIKM'00]

CDS: Need Non-linear Techniques!

2-server PIR
[CGKS'95]

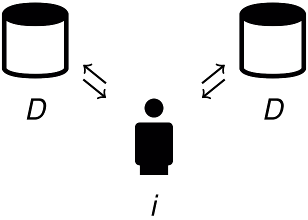


CDS
[GIKM'00]

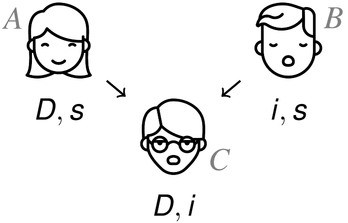


CDS: Need Non-linear Techniques!

2-server PIR
[CGKS'95]



CDS
[GIKM'00]

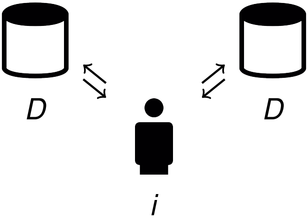


- $O(\sqrt{N})$ c.c. [CGKS'95]
  linear server

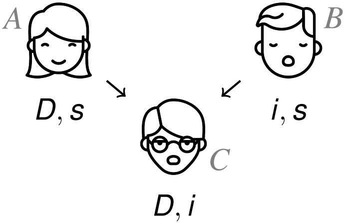
- $O(\sqrt{N})$ c.c. [GKW'15,...]
  linear reconstruction

CDS: Need Non-linear Techniques!

2-server PIR
[CGKS'95]



CDS
[GIKM'00]

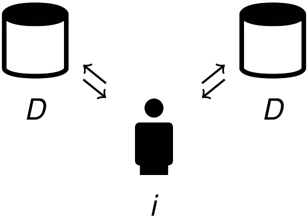


- $O(\sqrt{N})$ c.c. [CGKS'95]
  linear server
- $O(\sqrt[3]{N})$ c.c. [CGKS'95,WY'05]
  quadratic server
- $2^{\tilde{O}(\sqrt{\log N})}$ c.c. [DG'15]
  general server

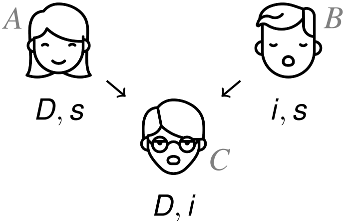
- $O(\sqrt{N})$ c.c. [GKW'15,...]
  linear reconstruction

CDS: Need Non-linear Techniques!

2-server PIR
[CGKS'95]



CDS
[GIKM'00]



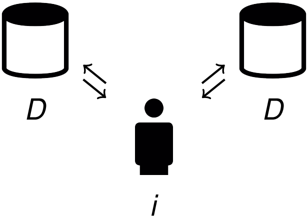
- $O(\sqrt{N})$ c.c. [CGKS'95]
  linear server
- $O(\sqrt[3]{N})$ c.c. [CGKS'95,WY'05]
  quadratic server
- $2^{\tilde{O}(\sqrt{\log N})}$ c.c. [DG'15]
  general server

- $O(\sqrt{N})$ c.c. [GKW'15,...]
  linear reconstruction

??

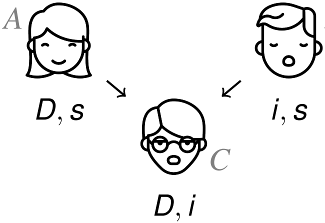
CDS: Need Non-linear Techniques!

2-server PIR
[CGKS'95]



- $O(\sqrt{N})$ c.c. [CGKS'95]
  linear server
- $O(\sqrt[3]{N})$ c.c. [CGKS'95,WY'05]
  quadratic server
- $2^{\tilde{O}(\sqrt{\log N})}$ c.c. [DG'15]
  general server

CDS
[GIKM'00]



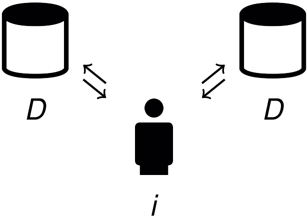
- $O(\sqrt{N})$ c.c. [GKW'15,...]
  linear reconstruction

??

$\sqrt{N}$ c.c. PSM [BIKK'14] from 4-server $\sqrt[4]{N}$ c.c. PIR [CGKS'95]

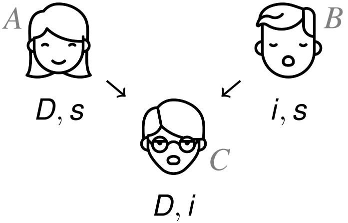
CDS: Need Non-linear Techniques!

2-server PIR
[CGKS'95]



- $O(\sqrt{N})$ c.c. [CGKS'95]
  linear server
- $O(\sqrt[3]{N})$ c.c. [CGKS'95,WY'05]
  quadratic server
- $2^{\tilde{O}(\sqrt{\log N})}$ c.c. [DG'15]
  general server

CDS
[GIKM'00]



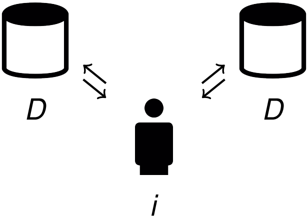
- $O(\sqrt{N})$ c.c. [GKW'15,...]
  linear reconstruction

??

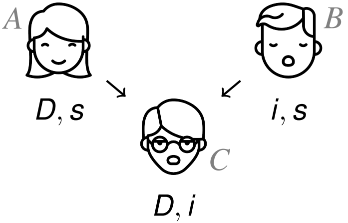
$\sqrt{N}$ c.c. PSM [BIKK'14] from 4-server $\sqrt[4]{N}$ c.c. PIR [CGKS'95]

CDS: Need Non-linear Techniques!

2-server PIR
[CGKS'95]



CDS
[GIKM'00]

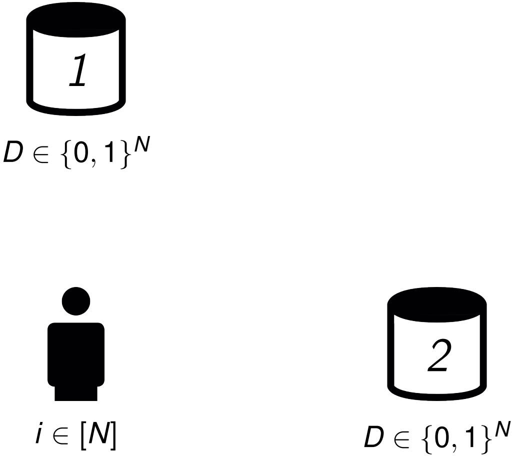


- $O(\sqrt{N})$ c.c. [CGKS'95]
  linear server
- $O(\sqrt[3]{N})$ c.c. [CGKS'95,WY'05] ⟶
  quadratic server
- $2^{\tilde{O}(\sqrt{\log N})}$ c.c. [DG'15] ⟶
  general server

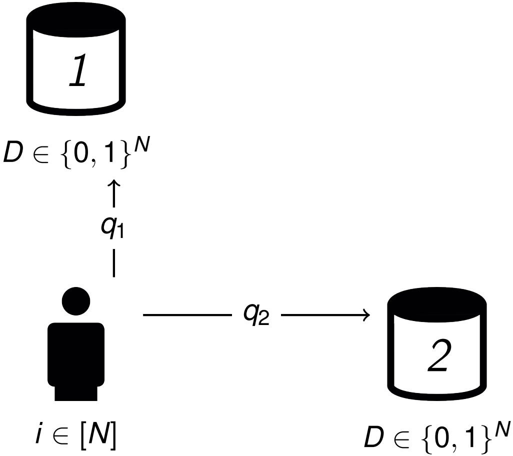
- $O(\sqrt{N})$ c.c. [GKW'15,...]
  linear reconstruction
- $O(\sqrt[3]{N})$ c.c. [This work]
  quadratic reconstruction
- $2^{\tilde{O}(\sqrt{\log N})}$ c.c. [This work]
  general reconstruction

$\sqrt{N}$ c.c. PSM [BIKK'14] from 4-server $\sqrt[4]{N}$ c.c. PIR [CGKS'95]

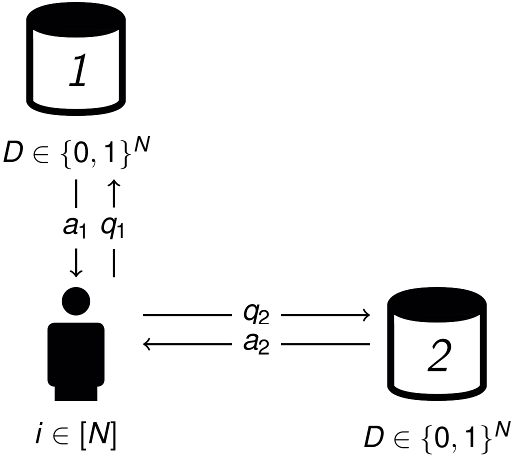
Private Information Retrieval



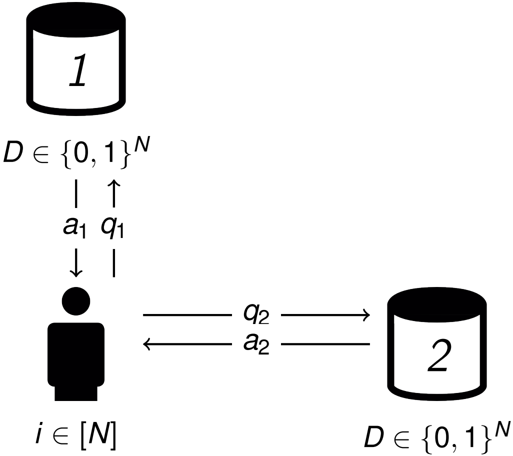
Private Information Retrieval



Private Information Retrieval

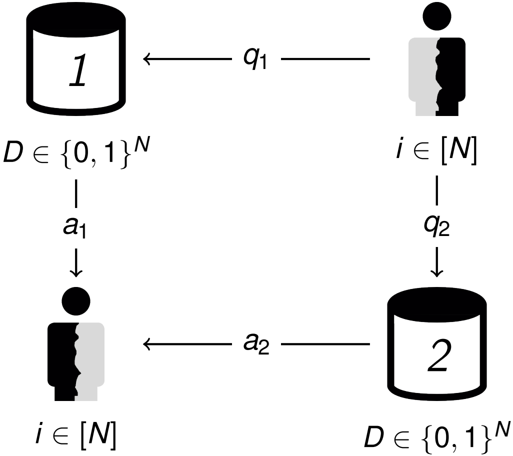


Private Information Retrieval

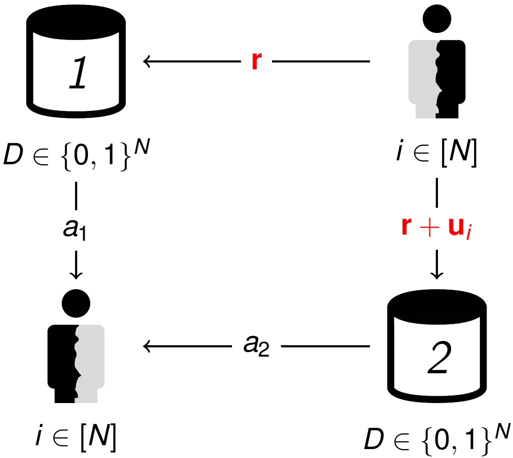


- Correctness: Client gets D_i
- IT Privacy: q_1 (resp. q_2) leaks nothing about i

Private Information Retrieval

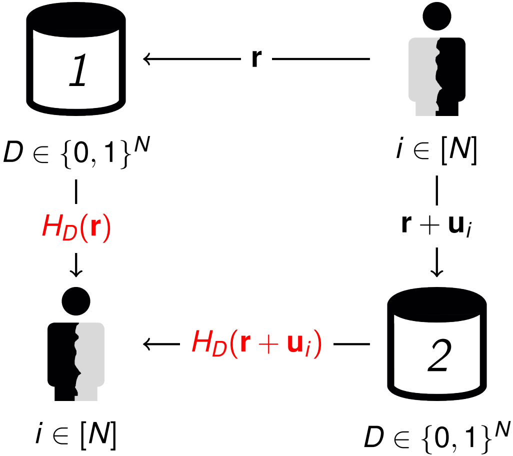


Private Information Retrieval



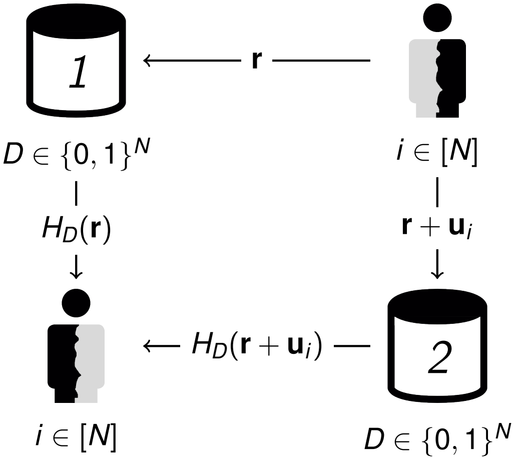
Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Private Information Retrieval



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

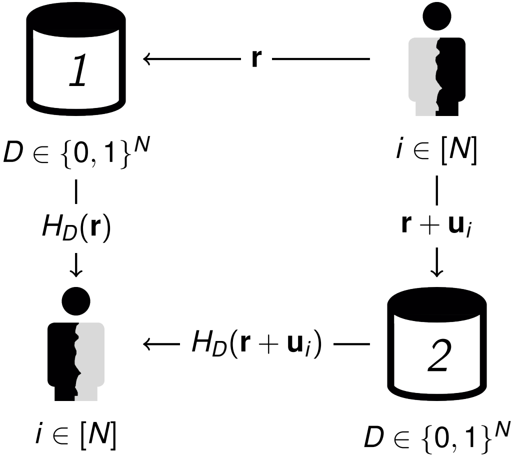
Private Information Retrieval



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = D_i$

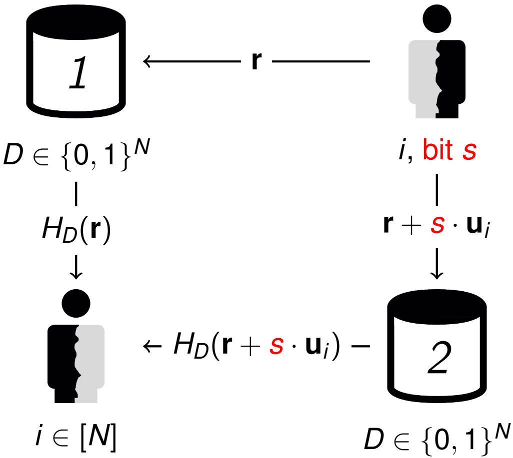
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = D_i$

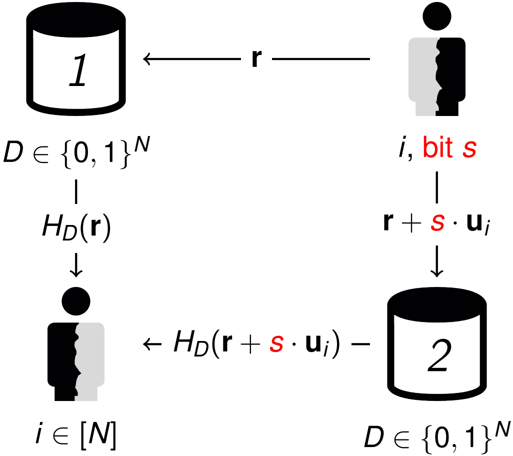
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = ?$

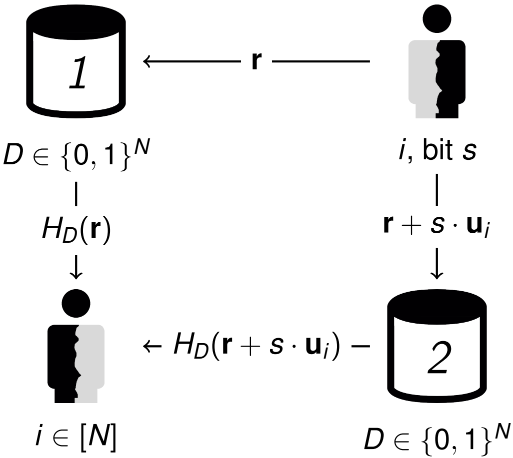
Private Information Retrieval $\implies$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \dots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

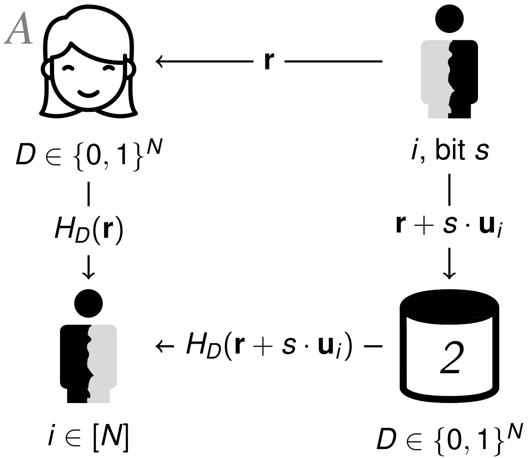
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

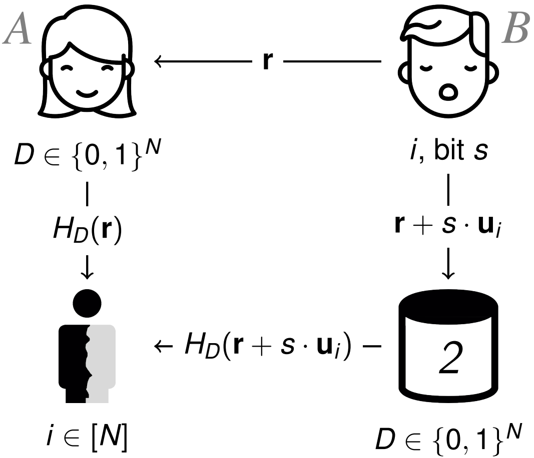
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

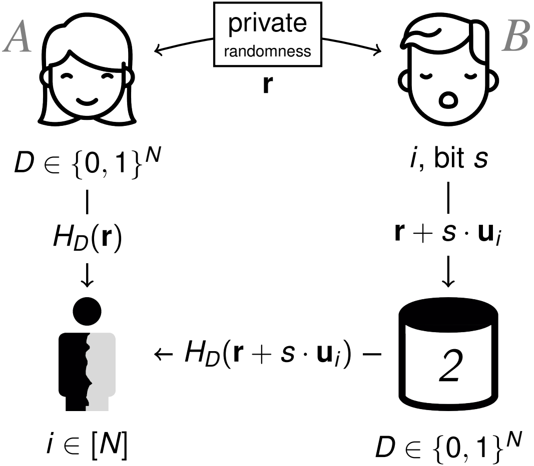
Private Information Retrieval $\implies$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

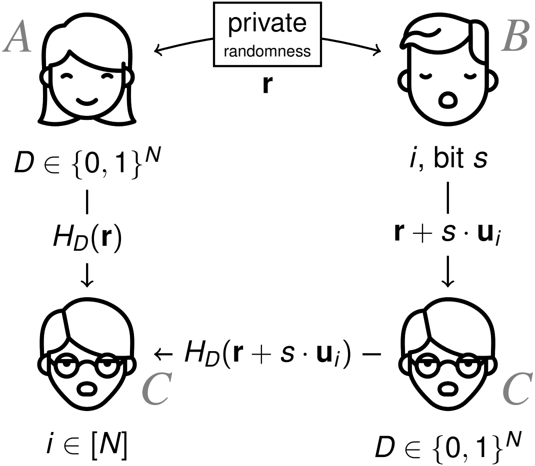
Private Information Retrieval $\implies$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i)\rangle - \langle \mathbf{u}_i, H_D(\mathbf{r})\rangle = s \cdot D_i$

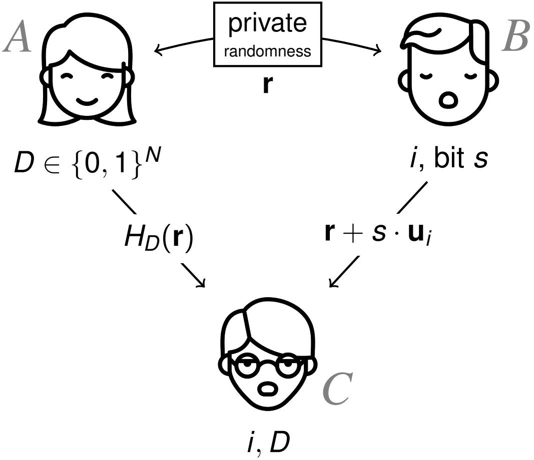
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

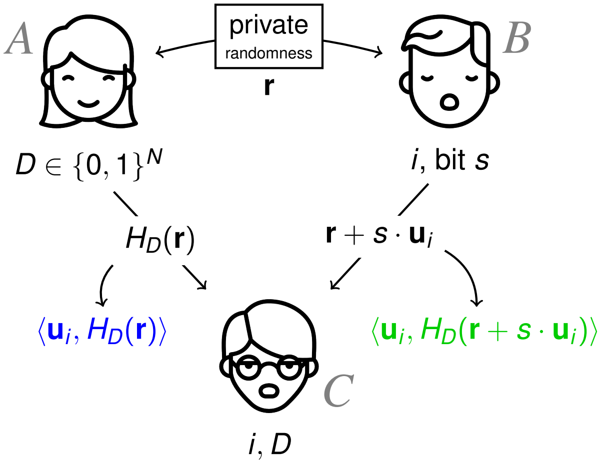
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

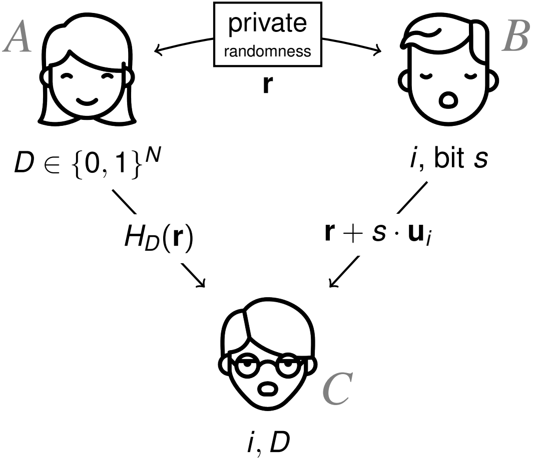
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

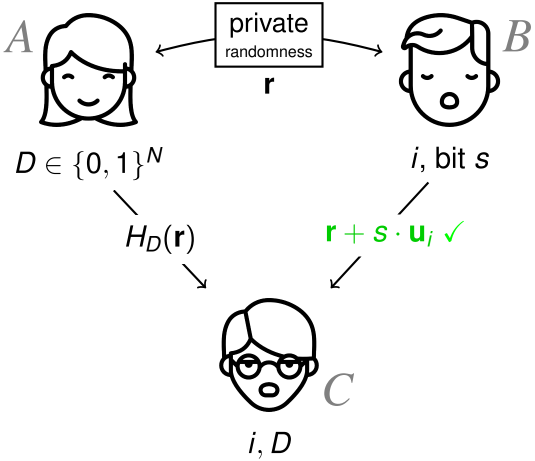
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

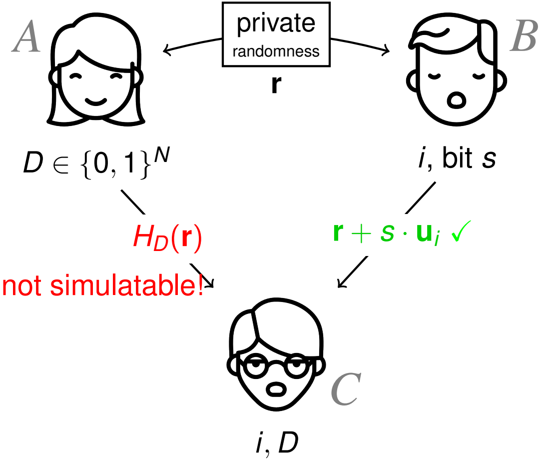
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 “Linear client”: $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

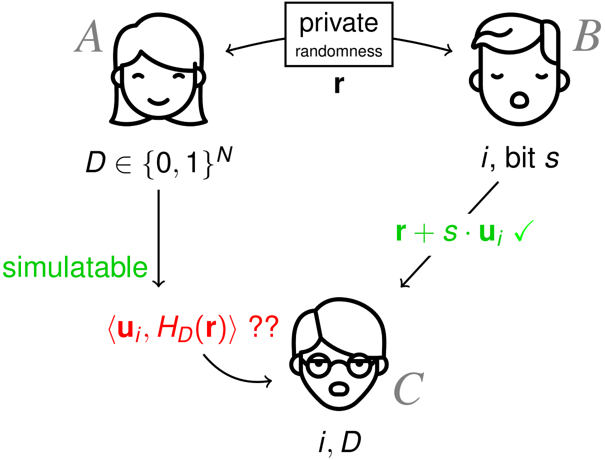
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

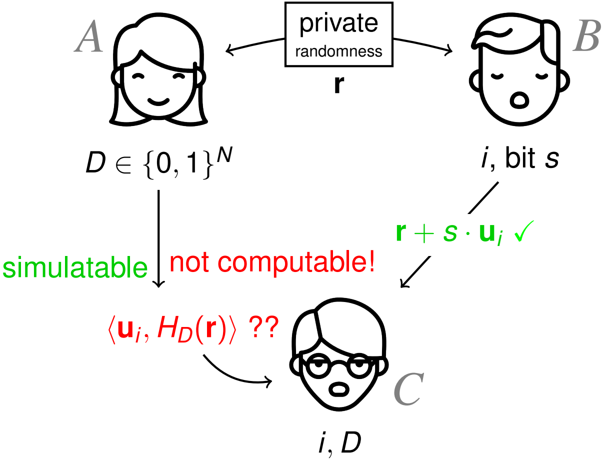
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

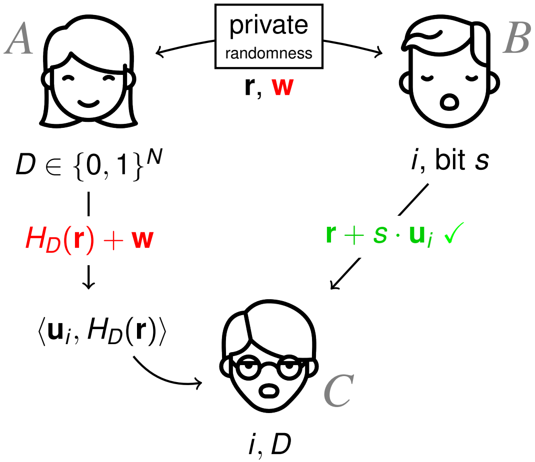
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

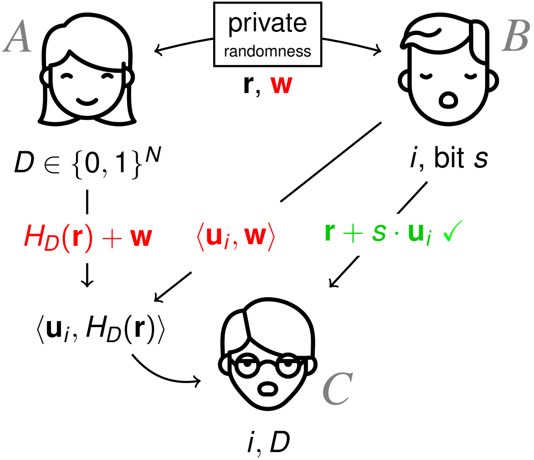
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

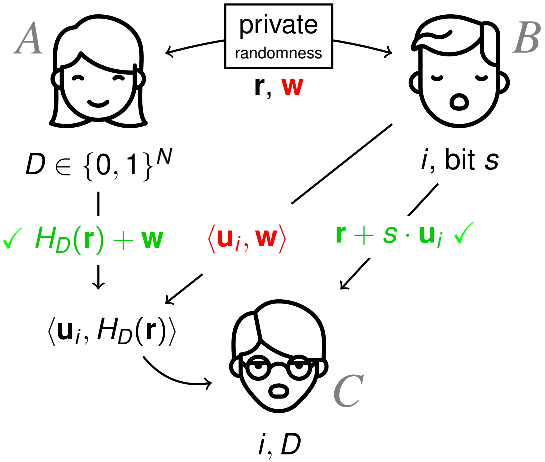
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i)\rangle - \langle \mathbf{u}_i, H_D(\mathbf{r})\rangle = s \cdot D_i$

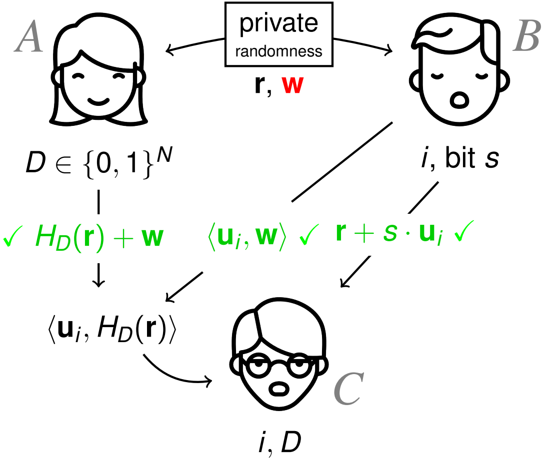
Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

Private Information Retrieval $\Longrightarrow$ CDS



Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

Private Information Retrieval $\Longrightarrow$ CDS

Prop. 1 Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

2-server PIR	CDS
$O(\sqrt{N})$ [CGKS'95] linear server function H_D	
$O(\sqrt[3]{N})$ [CGKS'95,WY'05] quadratic server function H_D	
$2^{\tilde{O}(\sqrt{\log N})}$ [DG'15] general server function H_D	

Private Information Retrieval $\implies$ CDS

Prop. 1 ~~Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$~~

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

2-server PIR	CDS
$O(\sqrt{N})$ [CGKS'95] linear server function H_D	
$O(\sqrt[3]{N})$ [CGKS'95,WY'05] quadratic server function H_D	
$2^{\tilde{O}(\sqrt{\log N})}$ [DG'15] general server function H_D	

Private Information Retrieval $\Longrightarrow$ CDS

Prop. 1 ~~Vectors $\mathbf{u}_1, \dots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$~~

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

2-server PIR	CDS
$O(\sqrt{N})$ [CGKS'95] $\longrightarrow$ linear server function H_D	$O(\sqrt{N})$ linear reconstruction
$O(\sqrt[3]{N})$ [CGKS'95,WY'05] $\longrightarrow$ quadratic server function H_D	$O(\sqrt[3]{N})$ quadratic reconstruction
$2^{\tilde{O}(\sqrt{\log N})}$ [DG'15] $\longrightarrow$ general server function H_D	$2^{\tilde{O}(\sqrt{\log N})}$ general reconstruction

Dvir-Gopi's $2^{\tilde{O}(\sqrt{\log N})}$ PIR $\implies$ CDS

Prop. 1 ~~Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$~~

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

Dvir-Gopi's $2^{\tilde{O}(\sqrt{\log N})}$ PIR $\implies$ CDS

Prop. 1 ~~Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$~~

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

- Matching vector family $\mathbf{u}_i \in \mathbb{Z}_6^\ell$

$$\langle \mathbf{u}_i, \mathbf{u}_i \rangle = 0 \pmod 6$$
$$\langle \mathbf{u}_i, \mathbf{u}_j \rangle = 1, 3 \text{ or } 4 \pmod 6 \text{ for } i \neq j$$

and $\ell = 2^{O(\sqrt{\log N \log \log N})}$ [Barrington-Beigel-Rudich'94].

Dvir-Gopi's $2^{\tilde{O}(\sqrt{\log N})}$ PIR $\implies$ CDS

Prop. 1 ~~Vectors $\mathbf{u}_1, \ldots, \mathbf{u}_N$. Queries are additive secret sharing of $\mathbf{u}_i$~~

Prop. 2 "Linear client": $\langle \mathbf{u}_i, H_D(\mathbf{r} + s \cdot \mathbf{u}_i) \rangle - \langle \mathbf{u}_i, H_D(\mathbf{r}) \rangle = s \cdot D_i$

- Matching vector family $\mathbf{u}_i \in \mathbb{Z}_6^\ell$

$$\langle \mathbf{u}_i, \mathbf{u}_i \rangle = 0 \pmod 6$$
$$\langle \mathbf{u}_i, \mathbf{u}_j \rangle = 1, 3 \text{ or } 4 \pmod 6 \text{ for } i \neq j$$

  and $\ell = 2^{O(\sqrt{\log N \log \log N})}$ [Barrington-Beigel-Rudich'94].

- H_D is super non-linear

$$H_D(\mathbf{w}) = \sum_y D_j \cdot \mathbf{u}_j \cdot (-1)^{\langle \mathbf{u}_j, \mathbf{w} \rangle} \pmod 6$$

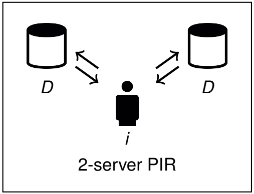
To Summarize

communication complexity		reconstruction
$\Theta(\sqrt{N})$	[GKW'15,...]	linear
$\Theta(\sqrt[3]{N})$	[This work,GKW'15]	quadratic
$2^{\tilde{O}(\sqrt{\log N})}$	[This work]	general
$\Omega(\log N)$	[GKW'15]	general

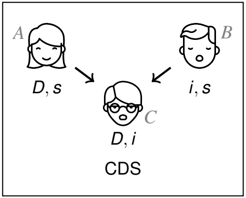
To Summarize

communication complexity		reconstruction
$\Theta(\sqrt{N})$	[GKW'15,...]	linear
$\Theta(\sqrt[3]{N})$	[This work,GKW'15]	quadratic
$2^{\tilde{O}(\sqrt{\log N})}$	[This work]	general
$\Omega(\log N)$	[GKW'15]	general

From



to



To Summarize

communication complexity		reconstruction
$\Theta(\sqrt{N})$	[GKW'15,...]	linear
$\Theta(\sqrt[3]{N})$	[This work,GKW'15]	quadratic
$2^{\tilde{O}(\sqrt{\log N})}$	[This work]	general
$\Omega(\log N)$	[GKW'15]	general

To Summarize

communication complexity		reconstruction
$\Theta(\sqrt{N})$	[GKW'15,...]	linear
$\Theta(\sqrt[3]{N})$	[This work,GKW'15]	quadratic
$2^{\tilde{O}(\sqrt{\log N})}$	[This work]	general
$\Omega(\log N)$	[GKW'15]	general

Additional results

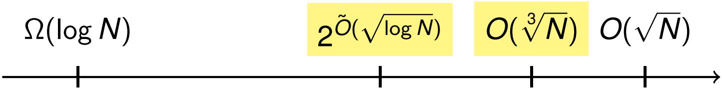
Secret sharing on forbidden graph	
$O(\sqrt{N})$	[BIKK'14]
$2^{\tilde{O}(\sqrt{\log N})}$	[This work]

To Summarize

communication complexity		reconstruction
$\Theta(\sqrt{N})$	[GKW'15,...]	linear
$\Theta(\sqrt[3]{N})$	[This work,GKW'15]	quadratic
$2^{\tilde{O}(\sqrt{\log N})}$	[This work]	general
$\Omega(\log N)$	[GKW'15]	general

Open Problems

communication complexity		reconstruction
$\Theta(\sqrt{N})$	[GKW'15,...]	linear
$\Theta(\sqrt[3]{N})$	[This work,GKW'15]	quadratic
$2^{\tilde{O}(\sqrt{\log N})}$	[This work]	general
$\Omega(\log N)$	[GKW'15]	general



Open Problems

	communication complexity	reconstruction
$\Theta(\sqrt{N})$	[GKW'15,...]	linear
$\Theta(\sqrt[3]{N})$	[This work,GKW'15]	quadratic
$2^{\tilde{O}(\sqrt{\log N})}$	[This work]	general
$\Omega(\log N)$	[GKW'15]	general