Multiparty Distributed Point Functions

Aarushi Goel

Purdue → Rutgers

Mingyuan Wang

NYU Shanghai

Zhiheng Wang

SJTU → NYU Shanghai

Crypto'25 — Aug 20

Function Secret Sharing [Gilboa-Ishai'14, Boyle-Gilboa-Ishai'15]

Sharing $f \in \mathcal{F}$

Local Eval given x

f

- Correctness

$$y_1 + \cdots + y_n = f(x)$$

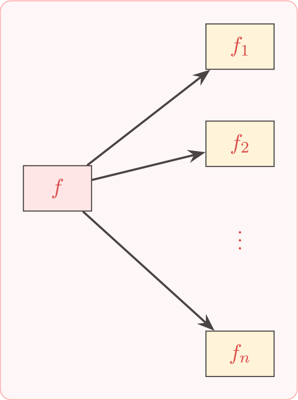
- Privacy: corrupted shares hide $f \in \mathcal{F}$
  - for this talk, $n-1$ corruption
- Efficiency

$$|f_1| + \cdots + |f_n| = o(\mathcal{D})$$

$\mathcal{D}$ denotes domain size.

Function Secret Sharing [Gilboa-Ishai'14, Boyle-Gilboa-Ishai'15]

Sharing $f \in \mathcal{F}$



Local Eval given x

- Correctness

$$y_1 + \cdots + y_n = f(x)$$

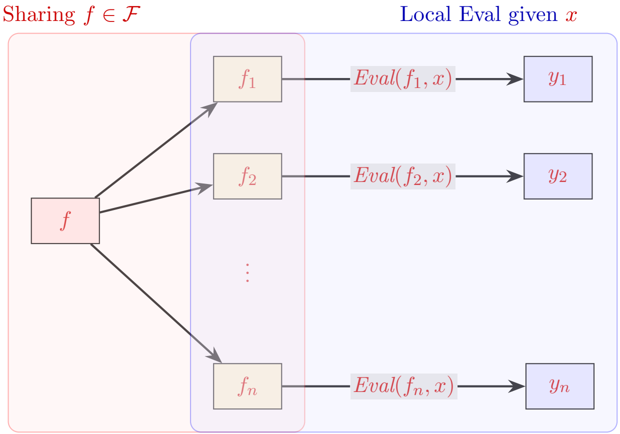
- Privacy: corrupted shares hide $f \in \mathcal{F}$
  - for this talk, $n-1$ corruption

- Efficiency

$$|f_1| + \cdots + |f_n| = o(\mathcal{D})$$

$\mathcal{D}$ denotes domain size.

Function Secret Sharing [Gilboa-Ishai'14, Boyle-Gilboa-Ishai'15]



- Correctness

$$y_1 + \cdots + y_n = f(x)$$

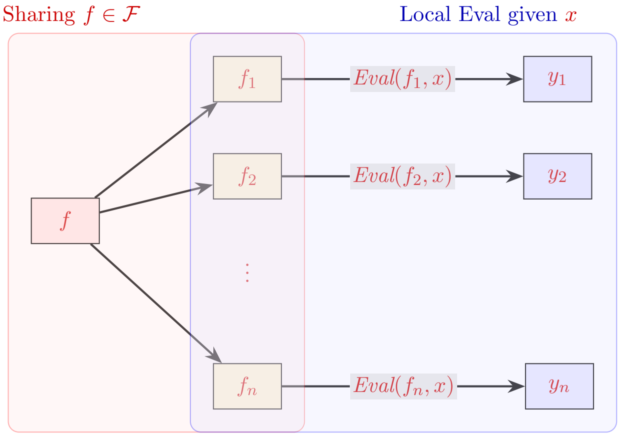
- Privacy: corrupted shares hide $f \in \mathcal{F}$
  - for this talk, $n-1$ corruption

- Efficiency

$$|f_1| + \cdots + |f_n| = o(\mathcal{D})$$

$\mathcal{D}$ denotes domain size.

Function Secret Sharing [Gilboa-Ishai'14, Boyle-Gilboa-Ishai'15]



- Correctness

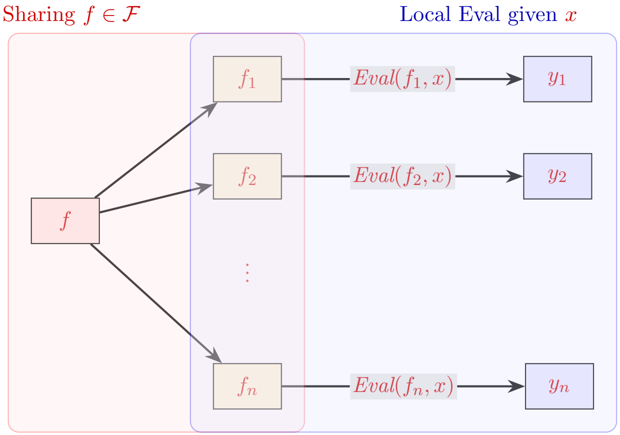
$$y_1 + \cdots + y_n = f(x)$$

- Privacy: corrupted shares hide $f \in \mathcal{F}$
  - for this talk, $n - 1$ corruption
- Efficiency

$$|f_1| + \cdots + |f_n| = o(\mathcal{D})$$

$\mathcal{D}$ denotes domain size.

Function Secret Sharing [Gilboa-Ishai'14, Boyle-Gilboa-Ishai'15]



- Correctness

$$y_1 + \cdots + y_n = f(x)$$

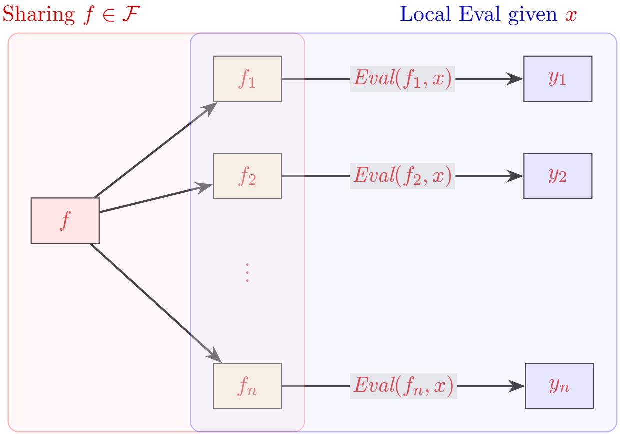
- Privacy: corrupted shares hide $f \in \mathcal{F}$
  - for this talk, $n - 1$ corruption

- Efficiency

$$|f_1| + \cdots + |f_n| = o(\mathcal{D})$$

$\mathcal{D}$ denotes domain size.

Function Secret Sharing [Gilboa-Ishai'14, Boyle-Gilboa-Ishai'15]



- Correctness

$$y_1 + \cdots + y_n = f(x)$$

- Privacy: corrupted shares hide $f \in \mathcal{F}$
  - for this talk, $n - 1$ corruption

- Efficiency

$$|f_1| + \cdots + |f_n| = o(\mathcal{D})$$

$\mathcal{D}$ denotes domain size.

Distributed Point Functions (DPF)

Point Functions

$$f_{\alpha,\beta}(x) = \begin{cases} \beta & \text{if } x = \alpha \\ 0 & \text{otherwise} \end{cases}$$

DPF

Function secret sharing for the family of point functions [Gilboa-Ishai'14].

Applications of DPF / FSS

- Private Information Retrieval (read & write): [Gilboa-Ishai'14,Boyle-Gilboa-Ishai'15, Corrigan-Gibbs-Boneh-Mazières'15, Boneh-Boyle-Corrigan-Gibbs-Gilboa-Ishai'21, Rathee-Zhang-Corrigan-Gibbs-Ada-Popa'24, ...]
- Pseudo-Correlation Generator (PCG): [Boyle-Couteau-Gilboa-Ishai'18, Schoppmann-Gascón-Reichert-Raykova'19, Boyle-Couteau-Gilboa-Ishai-Kohl-Scholl'19'20a'20b', Boyle-Couteau-Gilboa-Ishai-Kohl-Resch-Scholl'22, ...]
- (Structure-aware) PSI: [Garimella-Rosulek-Singh'22'23, Garimella-Goff-Miao'24, ...]
- (Concretely efficient) Distributed ORAM: [Doerner-shelat'17, Vadapalli-Henry-Goldberg'23, Braun-Pancholi-Rachuri-Simkin'23, ...]
- Mix-mode MPC: [Boyle-Gilboa-Ishai'19, Boyle-Chandran-Gilboa-Gupta-Ishai-Kumar-Rathee'21, ...]
- Sublinear MPC: [Couteau-Meyer'21, Boyle-Couteau-Meyer'23, Abram-Roy-Scholl'24, Couteau-Kumar'24, ...]
- Compressing OR proofs: [Boudgoust-Simkin'24]
- ...

Construction of DPFs

Two-party case

- OWF is sufficient. Size: $\lambda \cdot \log \mathcal{D}$ [Gilboa-Ishai'14,Boyle-Gilboa-Ishai'15'16]
- Optimized FSS for other families (multi-point, comparison, decision tree, ...) [Boyle-Gilboa-Ishai'16, Boyle-Gilboa-Hamilis-Ishai-Tu'25, ...]
- Optimized DKG: [Doerner-shelat'17, Boyle-Devadas-Servan-Schreiber'25, ...]

Multiparty case

- Only known construction [BGI'15]: $2^n \cdot \sqrt{\mathcal{D}}$

Multiparty case beyond Minicrypt

- LWE: $\mathrm{polylog}\, \mathcal{D}$ [Dodis-Halevi-Rothblum-Wichs'16]
- Anything else: grow with $\sqrt{\mathcal{D}}$ [Corrigan-Gibbs-Boneh-Mazières'15, Abram-Roy-Scholl'24, Couteau-Kumar'24, ...]

Construction of DPFs

Two-party case

- OWF is sufficient. Size: $\lambda \cdot \log \mathcal{D}$ [Gilboa-Ishai'14,Boyle-Gilboa-Ishai'15'16]
- Optimized FSS for other families (multi-point, comparison, decision tree, ...) [Boyle-Gilboa-Ishai'16, Boyle-Gilboa-Hamilis-Ishai-Tu'25, ...]
- Optimized DKG: [Doerner-shelat'17, Boyle-Devadas-Servan-Schreiber'25, ...]

Multiparty case

- Only known construction [BGI'15]: $2^n \cdot \sqrt{\mathcal{D}}$

Multiparty case beyond Minicrypt

- LWE: $\text{polylog}\, \mathcal{D}$ [Dodis-Halevi-Rothblum-Wichs'16]
- Anything else: grow with $\sqrt{\mathcal{D}}$ [Corrigan-Gibbs-Boneh-Mazières'15, Abram-Roy-Scholl'24, Couteau-Kumar'24, ...]

Construction of DPFs

Two-party case

- OWF is sufficient. Size: $\lambda \cdot \log \mathcal{D}$ [Gilboa-Ishai'14,Boyle-Gilboa-Ishai'15'16]
- Optimized FSS for other families (multi-point, comparison, decision tree, ...) [Boyle-Gilboa-Ishai'16, Boyle-Gilboa-Hamilis-Ishai-Tu'25, ...]
- Optimized DKG: [Doerner-shelat'17, Boyle-Devadas-Servan-Schreiber'25, ...]

Multiparty case

- Only known construction [BGI'15]: $2^n \cdot \sqrt{\mathcal{D}}$

Multiparty case beyond Minicrypt

- LWE: $\text{polylog}\,\mathcal{D}$ [Dodis-Halevi-Rothblum-Wichs'16]
- Anything else: grow with $\sqrt{\mathcal{D}}$ [Corrigan-Gibbs-Boneh-Mazières'15, Abram-Roy-Scholl'24, Couteau-Kumar'24, ...]

Multiparty case

- Only known construction [BGI'15]: $2^n \cdot \sqrt{\mathcal{D}}$

Limitation to the applications

- PIR: no three-party PIR with polylog communication from OWF
- PCG: multiparty correlation through pairwise correction $\rightarrow$ n^2 overhead
- DORAM / Mixed-mode MPC (DPF-route only supports limited number of parties)

Multiparty case

- Only known construction [BGI'15]: $2^n \cdot \sqrt{\mathcal{D}}$

Limitation to the applications

- PIR: no three-party PIR with polylog communication from OWF
- PCG: multiparty correlation through pairwise correction $\rightarrow n^2$ overhead
- DORAM / Mixed-mode MPC (DPF-route only supports limited number of parties)

Multiparty case

- Only known construction [BGI'15]: $2^n \cdot \sqrt{\mathcal{D}}$

Multiparty case

- Only known construction [BGI'15]: $2^n \cdot \sqrt{\mathcal{D}}$

This talk

Do efficient multiparty DPFs exist for any number of parties within Minicrypt?

Multiparty case

- Only known construction [BGI'15]: $2^n \cdot \sqrt{\mathcal{D}}$

This talk

Do efficient multiparty DPFs exist for any number of parties within Minicrypt?

with share size $\mathcal{O}_\lambda\left(n^3 \cdot \sqrt{|\mathcal{D}|}\right)$

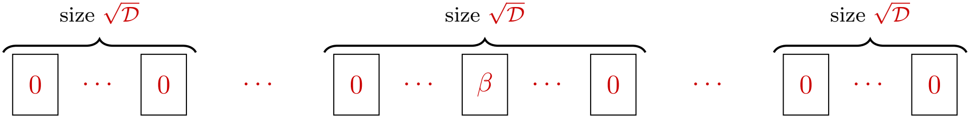
Technical Details

BGI15 Template: Two party

$$\boxed{0} \cdots \boxed{0} \quad \cdots \quad \boxed{0} \cdots \boxed{\beta} \cdots \boxed{0} \quad \cdots \quad \boxed{0} \cdots \boxed{0}$$

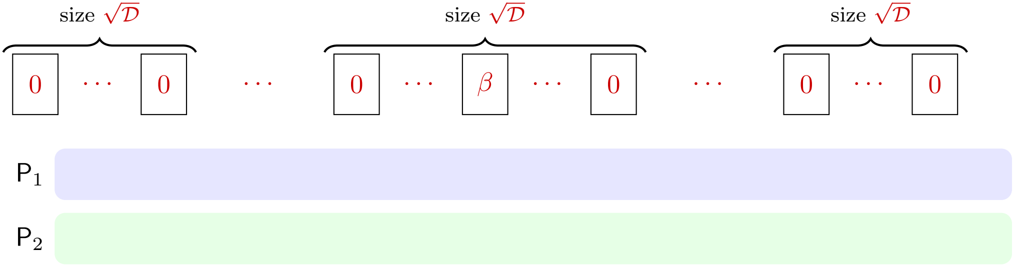
- Local Eval: $G(s^i) \oplus u_i \cdot w$
- Privacy: w is pseudorandom
- Efficiency: $\sqrt{\mathcal{D}}$

BGI15 Template: Two party



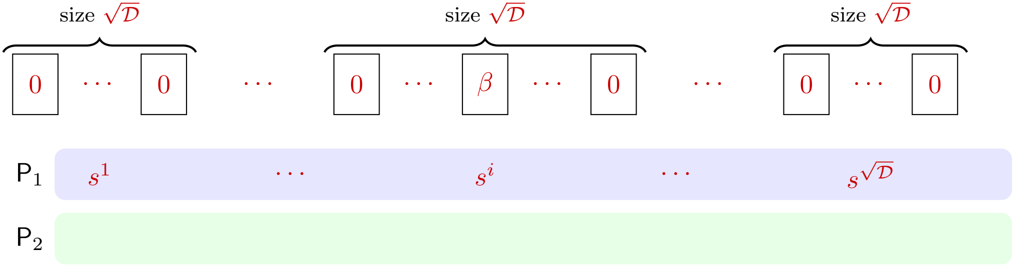
- Local Eval: $G(s^i) \oplus u_i \cdot w$
- Privacy: w is pseudorandom
- Efficiency: $\sqrt{\mathcal{D}}$

BGI15 Template: Two party



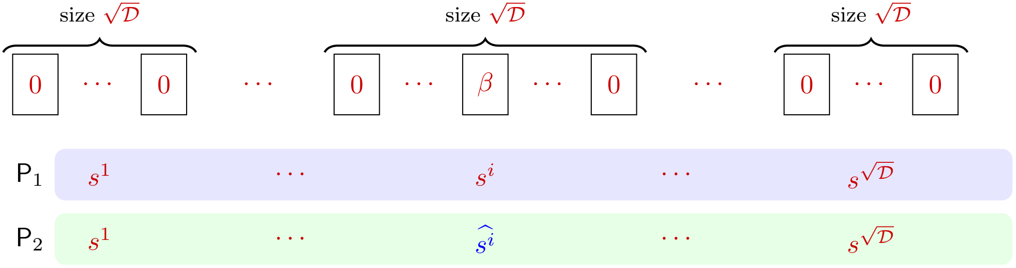
- Local Eval: $G(s^i) \oplus u_i \cdot w$
- Privacy: w is pseudorandom
- Efficiency: $\sqrt{\mathcal{D}}$

BGI15 Template: Two party



- Local Eval: $G(s^i) \oplus u_i \cdot w$
- Privacy: w is pseudorandom
- Efficiency: $\sqrt{\mathcal{D}}$

BGI15 Template: Two party



- Local Eval: $G(s^i) \oplus u_i \cdot w$
- Privacy: w is pseudorandom
- Efficiency: $\sqrt{\mathcal{D}}$

BGI15 Template: Two party

size $\sqrt{\mathcal{D}}$ · size $\sqrt{\mathcal{D}}$ · size $\sqrt{\mathcal{D}}$

$0 \cdots 0 \quad \cdots \quad 0 \cdots \beta \cdots 0 \quad \cdots \quad 0 \cdots 0$

P_1: $s^1 \quad \cdots \quad s^i \quad \cdots \quad s^{\sqrt{\mathcal{D}}}$

P_2: $s^1 \quad \cdots \quad \widehat{s^i} \quad \cdots \quad s^{\sqrt{\mathcal{D}}}$

$G(s^1) \oplus G(s^1) = \overrightarrow{0} \qquad G(s^i) \oplus G(\widehat{s^i}) \qquad G(s^{\sqrt{\mathcal{D}}}) \oplus G(s^{\sqrt{\mathcal{D}}}) = \overrightarrow{0}$

- Local Eval: $G(s^i) \oplus u_i \cdot w$
- Privacy: w is pseudorandom
- Efficiency: $\sqrt{\mathcal{D}}$

BGI15 Template: Two party

size $\sqrt{\mathcal{D}}$ | size $\sqrt{\mathcal{D}}$ | size $\sqrt{\mathcal{D}}$

$\boxed{0}\ \cdots\ \boxed{0}\quad\cdots\quad\boxed{0}\ \cdots\ \boxed{\beta}\ \cdots\ \boxed{0}\quad\cdots\quad\boxed{0}\ \cdots\ \boxed{0}$

P_1: $s^1 \quad \cdots \quad s^i \quad \cdots \quad s^{\sqrt{\mathcal{D}}}$

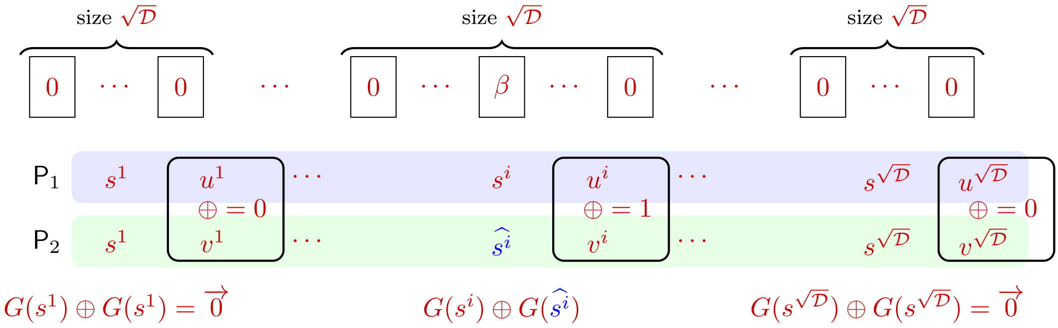
P_2: $s^1 \quad \cdots \quad \widehat{s^i} \quad \cdots \quad s^{\sqrt{\mathcal{D}}}$

$G(s^1) \oplus G(s^1) = \overrightarrow{0}$ $\qquad$ $G(s^i) \oplus G(\widehat{s^i})$ $\qquad$ $G(s^{\sqrt{\mathcal{D}}}) \oplus G(s^{\sqrt{\mathcal{D}}}) = \overrightarrow{0}$

Correction string $w = G(s^i) \oplus G(\widehat{s^i}) \oplus \mathbb{1}_{\alpha,\beta}$

- Local Eval: $G(s^i) \oplus u_i \cdot w$
- Privacy: w is pseudorandom
- Efficiency: $\sqrt{\mathcal{D}}$

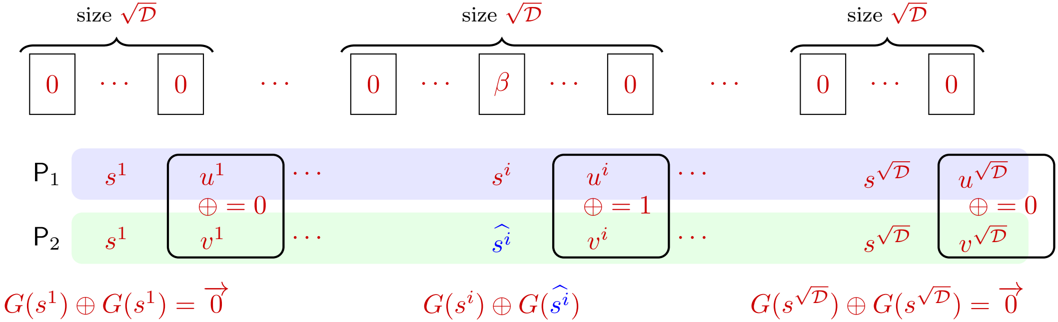
BGI15 Template: Two party



Correction string $w = G(s^i) \oplus G(\widehat{s^i}) \oplus \mathbb{1}_{\alpha,\beta}$

- Local Eval: $G(s^i) \oplus u_i \cdot w$
- Privacy: w is pseudorandom
- Efficiency: $\sqrt{\mathcal{D}}$

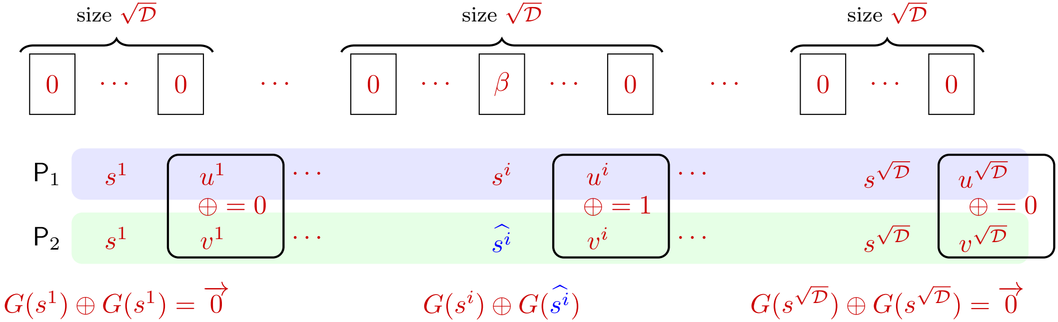
BGI15 Template: Two party



Correction string $w = G(s^i) \oplus G(\widehat{s^i}) \oplus \mathbb{1}_{\alpha,\beta}$

- Local Eval: $G(s^i) \oplus u_i \cdot w$
- Privacy: w is pseudorandom
- Efficiency: $\sqrt{\mathcal{D}}$

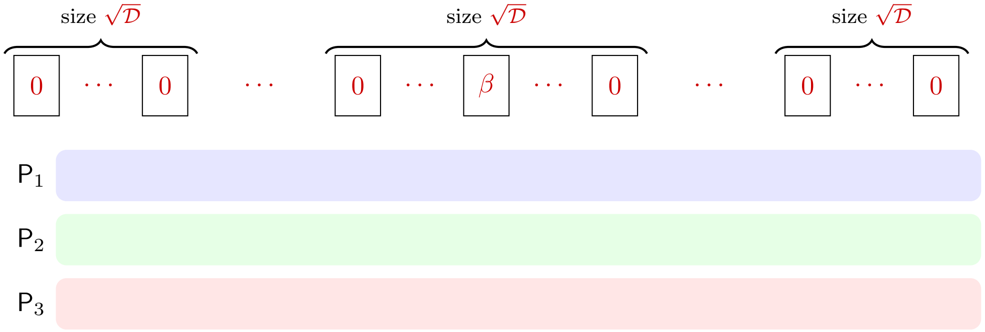
BGI15 Template: Two party



Correction string $w = G(s^i) \oplus G(\widehat{s^i}) \oplus \mathbb{1}_{\alpha,\beta}$

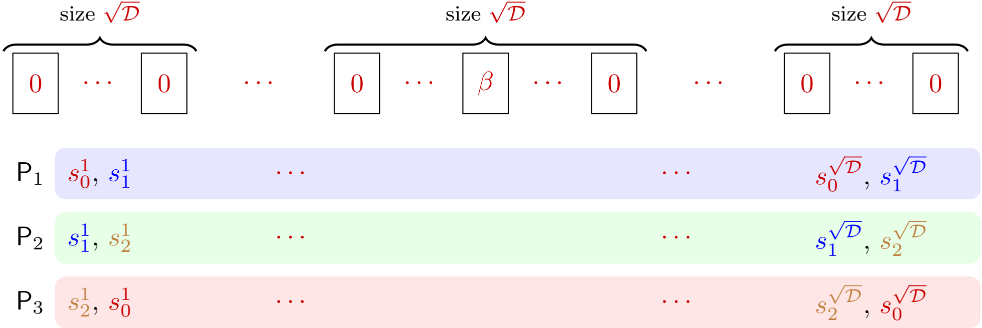
- Local Eval: $G(s^i) \oplus u_i \cdot w$
- Privacy: w is pseudorandom
- Efficiency: $\sqrt{\mathcal{D}}$

BGI15 Template: Three party



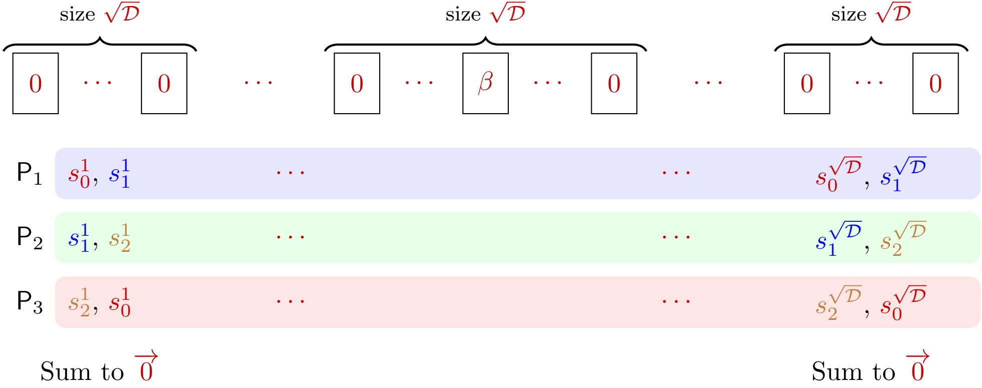
The seed distribution for the special chunk is indistinguishable from the other chunks

BGI15 Template: Three party



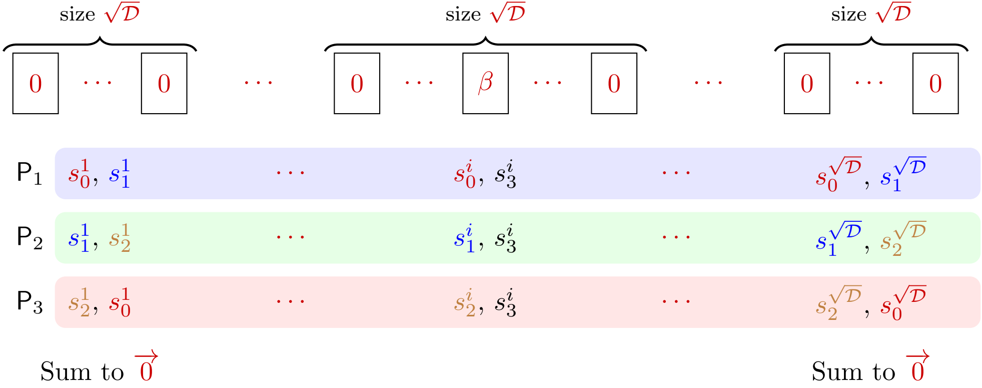
The seed distribution for the special chunk is indistinguishable from the other chunks

BGI15 Template: Three party



The seed distribution for the special chunk is indistinguishable from the other chunks

BGI15 Template: Three party



The seed distribution for the special chunk is indistinguishable from the other chunks

BGI15 Template: Three party

size $\sqrt{\mathcal{D}}$ — size $\sqrt{\mathcal{D}}$ — size $\sqrt{\mathcal{D}}$

$\boxed{0} \cdots \boxed{0} \quad \cdots \quad \boxed{0} \cdots \boxed{\beta} \cdots \boxed{0} \quad \cdots \quad \boxed{0} \cdots \boxed{0}$

P$_1$	s_0^1, s_1^1	$\cdots$	s_0^i, s_3^i	$\cdots$	$s_0^{\sqrt{\mathcal{D}}}, s_1^{\sqrt{\mathcal{D}}}$
P$_2$	s_1^1, s_2^1	$\cdots$	s_1^i, s_3^i	$\cdots$	$s_1^{\sqrt{\mathcal{D}}}, s_2^{\sqrt{\mathcal{D}}}$
P$_3$	s_2^1, s_0^1	$\cdots$	s_2^i, s_3^i	$\cdots$	$s_2^{\sqrt{\mathcal{D}}}, s_0^{\sqrt{\mathcal{D}}}$

Sum to $\vec{0}$

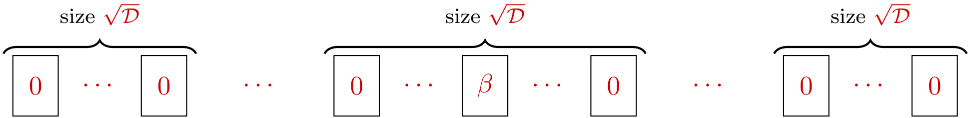
$G(s_1^i) \oplus G(s_1^i) \oplus G(s_2^i) \oplus G(s_3^i)$

sum is pseudorandom

Sum to $\vec{0}$

The seed distribution for the special chunk is indistinguishable from the other chunks

BGI15 Template: Three party



P$_1$	s_0^1, s_1^1	$\cdots$	s_0^i, s_3^i	$\cdots$	$s_0^{\sqrt{\mathcal{D}}}, s_1^{\sqrt{\mathcal{D}}}$
P$_2$	s_1^1, s_2^1	$\cdots$	s_1^i, s_3^i	$\cdots$	$s_1^{\sqrt{\mathcal{D}}}, s_2^{\sqrt{\mathcal{D}}}$
P$_3$	s_2^1, s_0^1	$\cdots$	s_2^i, s_3^i	$\cdots$	$s_2^{\sqrt{\mathcal{D}}}, s_0^{\sqrt{\mathcal{D}}}$

Sum to $\vec{0}$

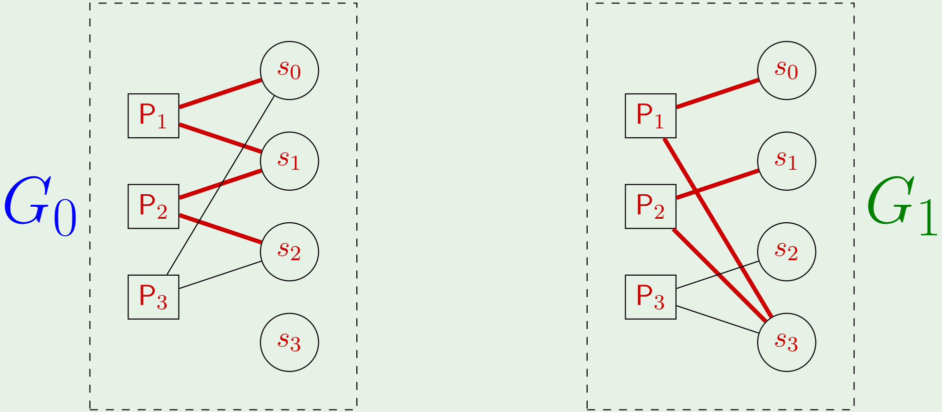
$G(s_1^i) \oplus G(s_1^i) \oplus G(s_2^i) \oplus G(s_3^i)$

sum is pseudorandom

Sum to $\vec{0}$

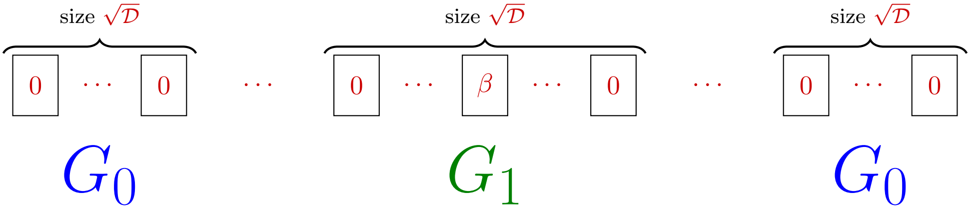
The seed distribution for the special chunk is indistinguishable from the other chunks

Our Abstraction: Special Combinatorial Design



1. **Correctness**: G_0 has only even-degree right vertices.
2. **Pseudorandomness**: G_1 has a dedicated right vertex for every left vertex.
3. **Privacy**: Any induced subgraph are indistinguishable.

BGI15 Template + Special Combinatorial Design

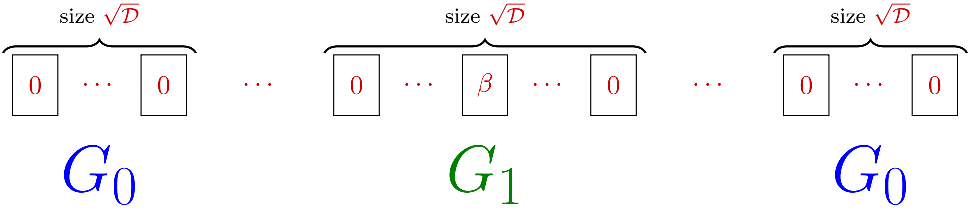


- **Correctness**: non-special chunks sum up to zero.
- **Pseudorandomness**: special chunks sum up to pseudorandomness.
- **Privacy**: seed distribution is indistinguishable.

Efficiency

Size of G_0 and G_1 determine the share size!

BGI15 Template + Special Combinatorial Design

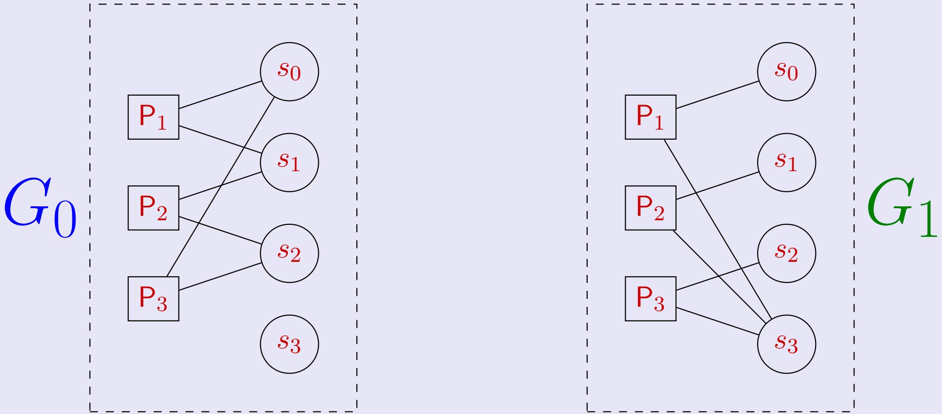


- **Correctness**: non-special chunks sum up to zero.
- **Pseudorandomness**: special chunks sum up to pseudorandomness.
- **Privacy**: seed distribution is indistinguishable.

Efficiency

Size of G_0 and G_1 determine the share size!

BGI15's Construction of Special Combinatorial Design

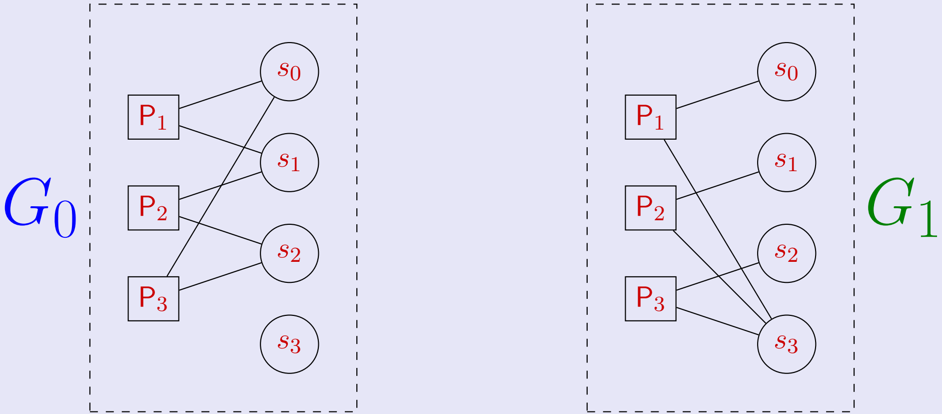


Lower bound

Any deterministic special combinatorial design requires $\mathcal{O}(2^n)$ right vertices.

- BGI15 construction is optimal.

BGI15's Construction of Special Combinatorial Design

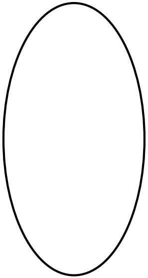


Lower bound

Any deterministic special combinatorial design requires $\mathcal{O}(2^n)$ right vertices.

- BGI15 construction is optimal.

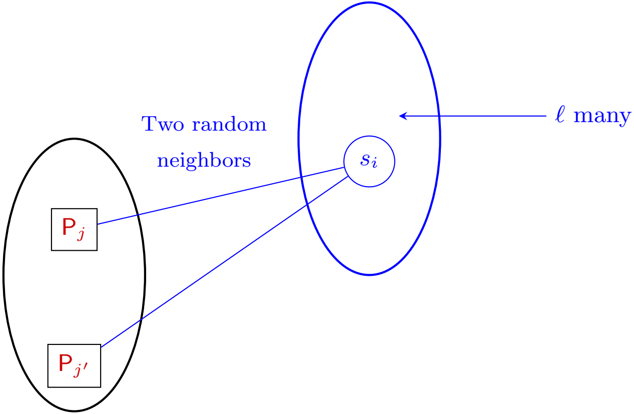
Randomized Construction



- G_0: blue
- G_1: blue and green
- Correctness holds by design
- Pseudorandomness holds by design assuming $t = \Omega(n)$

What about privacy?

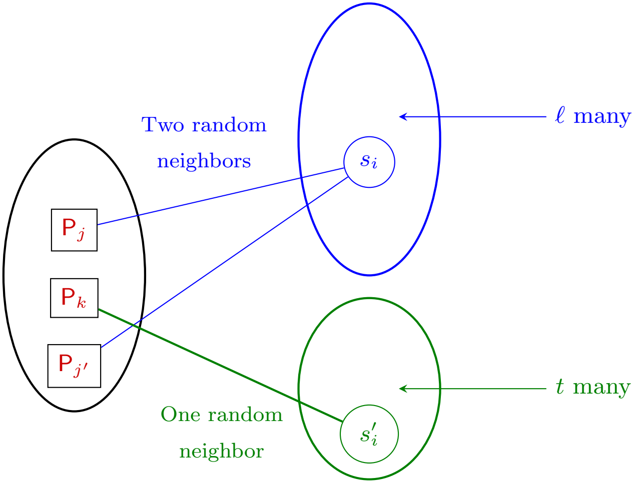
Randomized Construction



- G_0: blue
- G_1: blue and green
- Correctness holds by design
- Pseudorandomness holds by design assuming $t = \Omega(n)$

What about privacy?

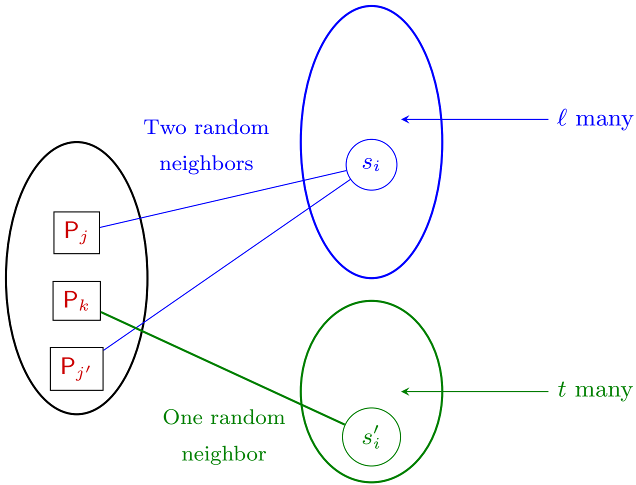
Randomized Construction



- G_0: blue
- G_1: blue and green
- Correctness holds by design
- Pseudorandomness holds by design assuming $t = \Omega(n)$

What about privacy?

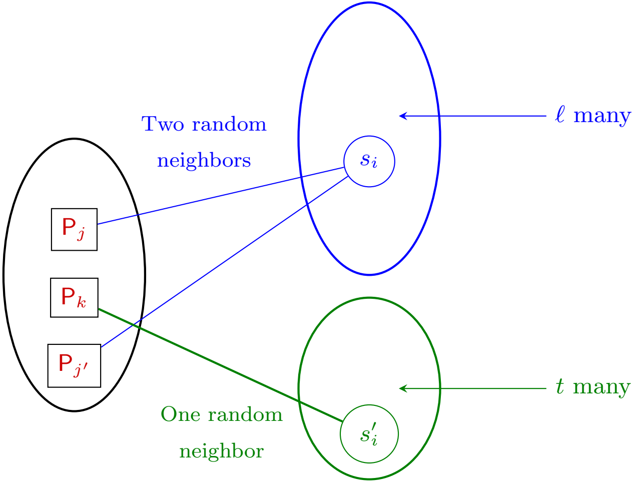
Randomized Construction



- G_0: blue
- G_1: blue and green
- Correctness holds by design
- Pseudorandomness holds by design assuming $t = \Omega(n)$

What about privacy?

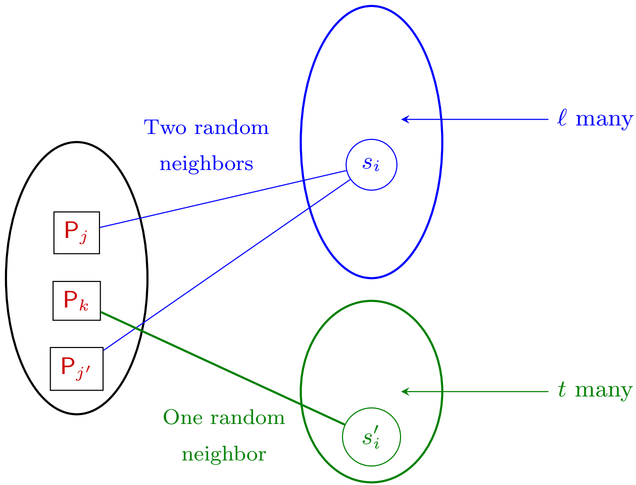
Randomized Construction



- G_0: blue
- G_1: blue and green
- Correctness holds by design
- Pseudorandomness holds by design assuming $t = \Omega(n)$

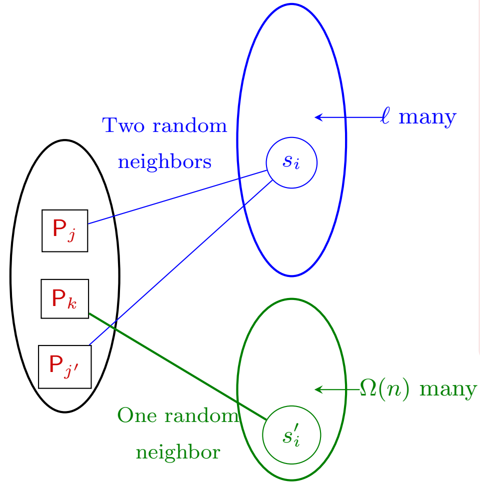
What about privacy?

Randomized Construction



- G_0: blue
- G_1: blue and green
- Correctness holds by design
- Pseudorandomness holds by design assuming $t = \Omega(n)$

What about privacy?

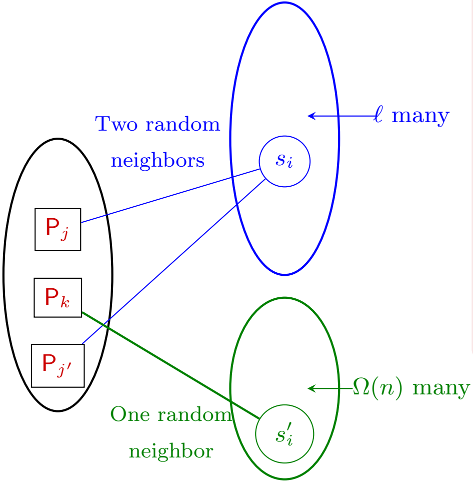


Privacy

- Corrupted parties see $\mathcal{S}$ many single-degree seeds and $\mathcal{T}$ many two-degree seeds.
- Conditioned on $\mathcal{S}$ and $\mathcal{T}$, the actual configuration is identically distributed for G_0 and G_1.
- Only need to argue the closeness of the joint distribution

$$(\mathcal{S}, \mathcal{T})$$

- $\mathcal{T}$ is the identical for G_0 and G_1
- Conditioned on $\mathcal{T}$, distribution of $\mathcal{S}$ is
  - G_0: $\ell - \mathcal{T}$ many Bernolli samples with bias $(n-1)/n$
  - G_1: distribution of G_0 shifted by $\Omega(n)$ many Bernolli samples with bias $(n-1)/n$
- Omitting many details, $\ell = \Omega(n^4)$ suffices!

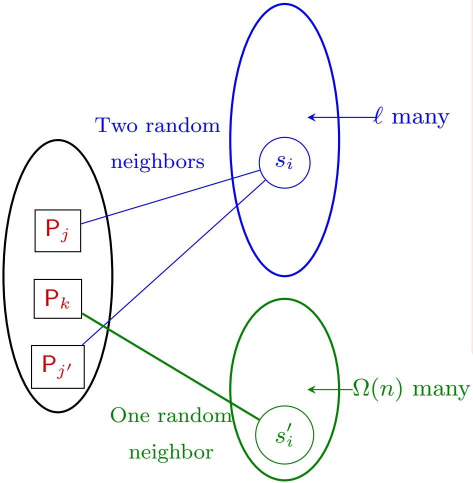


Privacy

- Corrupted parties see $\mathcal{S}$ many single-degree seeds and $\mathcal{T}$ many two-degree seeds.
- Conditioned on $\mathcal{S}$ and $\mathcal{T}$, the actual configuration is identically distributed for G_0 and G_1.
- Only need to argue the closeness of the joint distribution

$$(\mathcal{S},\mathcal{T})$$

- $\mathcal{T}$ is the identical for G_0 and G_1
- Conditioned on $\mathcal{T}$, distribution of $\mathcal{S}$ is
  - G_0: $\ell - \mathcal{T}$ many Bernolli samples with bias $(n-1)/n$
  - G_1: distribution of G_0 shifted by $\Omega(n)$ many Bernolli samples with bias $(n-1)/n$
- Omitting many details, $\ell = \Omega(n^4)$ suffices!

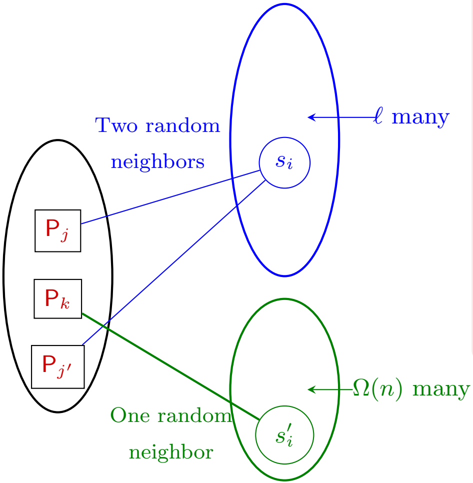


Privacy

- Corrupted parties see $\mathcal{S}$ many single-degree seeds and $\mathcal{T}$ many two-degree seeds.
- Conditioned on $\mathcal{S}$ and $\mathcal{T}$, the actual configuration is identically distributed for G_0 and G_1.
- Only need to argue the closeness of the joint distribution

$$(\mathcal{S}, \mathcal{T})$$

- $\mathcal{T}$ is the identical for G_0 and G_1
- Conditioned on $\mathcal{T}$, distribution of $\mathcal{S}$ is
  - G_0: $\ell - \mathcal{T}$ many Bernolli samples with bias $(n-1)/n$
  - G_1: distribution of G_0 shifted by $\Omega(n)$ many Bernolli samples with bias $(n-1)/n$
- Omitting many details, $\ell = \Omega(n^4)$ suffices!

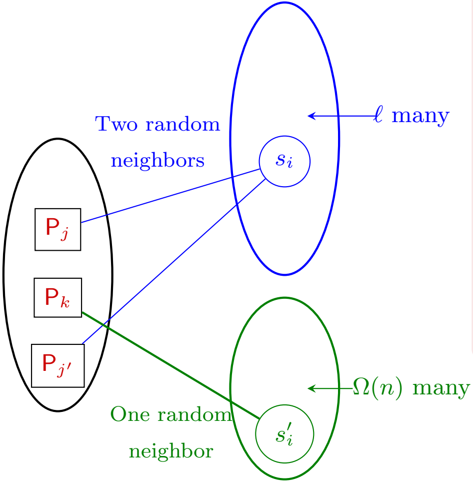


Privacy

- Corrupted parties see $\mathcal{S}$ many single-degree seeds and $\mathcal{T}$ many two-degree seeds.
- Conditioned on $\mathcal{S}$ and $\mathcal{T}$, the actual configuration is identically distributed for G_0 and G_1.
- Only need to argue the closeness of the joint distribution

$$(\mathcal{S}, \mathcal{T})$$

- $\mathcal{T}$ is the identical for G_0 and G_1
- Conditioned on $\mathcal{T}$, distribution of $\mathcal{S}$ is
  - G_0: $\ell - \mathcal{T}$ many Bernolli samples with bias $(n-1)/n$
  - G_1: distribution of G_0 shifted by $\Omega(n)$ many Bernolli samples with bias $(n-1)/n$
- Omitting many details, $\ell = \Omega(n^4)$ suffices!

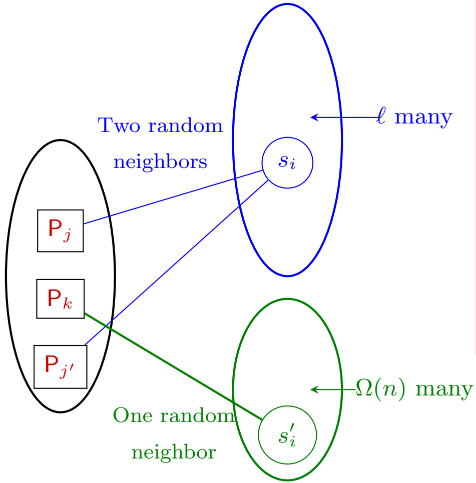


Privacy

- Corrupted parties see $\mathcal{S}$ many single-degree seeds and $\mathcal{T}$ many two-degree seeds.
- Conditioned on $\mathcal{S}$ and $\mathcal{T}$, the actual configuration is identically distributed for G_0 and G_1.
- Only need to argue the closeness of the joint distribution

$$(\mathcal{S}, \mathcal{T})$$

- $\mathcal{T}$ is the identical for G_0 and G_1
- Conditioned on $\mathcal{T}$, distribution of $\mathcal{S}$ is
  - G_0: $\ell - \mathcal{T}$ many Bernolli samples with bias $(n-1)/n$
  - G_1: distribution of G_0 shifted by $\Omega(n)$ many Bernolli samples with bias $(n-1)/n$
- Omitting many details, $\ell = \Omega(n^4)$ suffices!

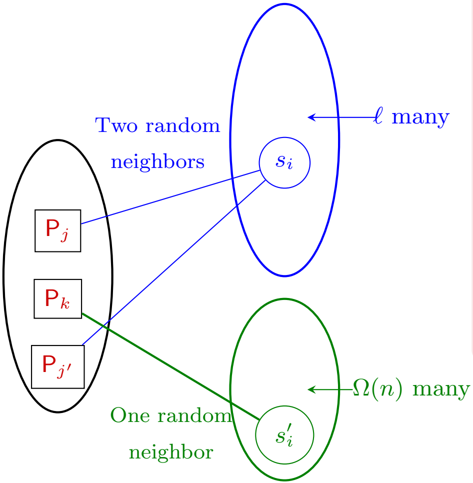


Privacy

- Corrupted parties see $\mathcal{S}$ many single-degree seeds and $\mathcal{T}$ many two-degree seeds.
- Conditioned on $\mathcal{S}$ and $\mathcal{T}$, the actual configuration is identically distributed for G_0 and G_1.
- Only need to argue the closeness of the joint distribution

$$(\mathcal{S}, \mathcal{T})$$

- $\mathcal{T}$ is the identical for G_0 and G_1
- Conditioned on $\mathcal{T}$, distribution of $\mathcal{S}$ is
  - G_0: $\ell - \mathcal{T}$ many Bernolli samples with bias $(n-1)/n$
  - G_1: distribution of G_0 shifted by $\Omega(n)$ many Bernolli samples with bias $(n-1)/n$
- Omitting many details, $\ell = \Omega(n^4)$ suffices!

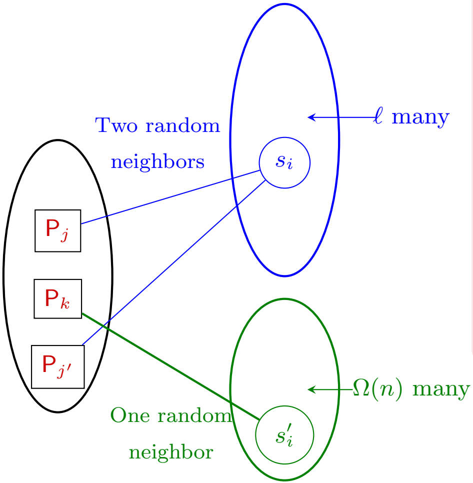


Privacy

- Corrupted parties see $\mathcal{S}$ many single-degree seeds and $\mathcal{T}$ many two-degree seeds.
- Conditioned on $\mathcal{S}$ and $\mathcal{T}$, the actual configuration is identically distributed for G_0 and G_1.
- Only need to argue the closeness of the joint distribution

$$(\mathcal{S}, \mathcal{T})$$

- $\mathcal{T}$ is the identical for G_0 and G_1
- Conditioned on $\mathcal{T}$, distribution of $\mathcal{S}$ is
  - G_0: $\ell - \mathcal{T}$ many Bernolli samples with bias $(n-1)/n$
  - G_1: distribution of G_0 shifted by $\Omega(n)$ many Bernolli samples with bias $(n-1)/n$
- Omitting many details, $\ell = \Omega(n^4)$ suffices!

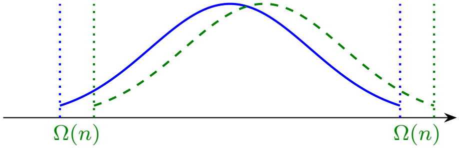


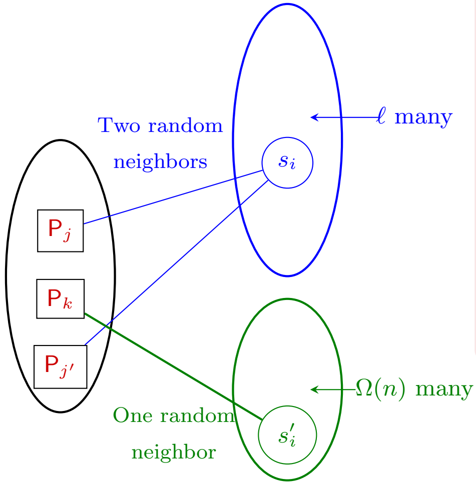
Privacy

- Corrupted parties see $\mathcal{S}$ many single-degree seeds and $\mathcal{T}$ many two-degree seeds.
- Conditioned on $\mathcal{S}$ and $\mathcal{T}$, the actual configuration is identically distributed for G_0 and G_1.
- Only need to argue the closeness of the joint distribution

$$(\mathcal{S}, \mathcal{T})$$

- $\mathcal{T}$ is the identical for G_0 and G_1
- Conditioned on $\mathcal{T}$, distribution of $\mathcal{S}$ is
  - G_0: $\ell - \mathcal{T}$ many Bernolli samples with bias $(n-1)/n$
  - G_1: distribution of G_0 shifted by $\Omega(n)$ many Bernolli samples with bias $(n-1)/n$
- Omitting many details, $\ell = \Omega(n^4)$ suffices!



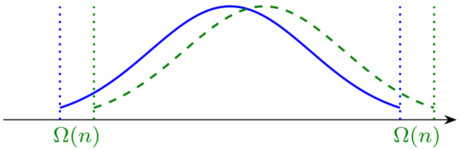


Privacy

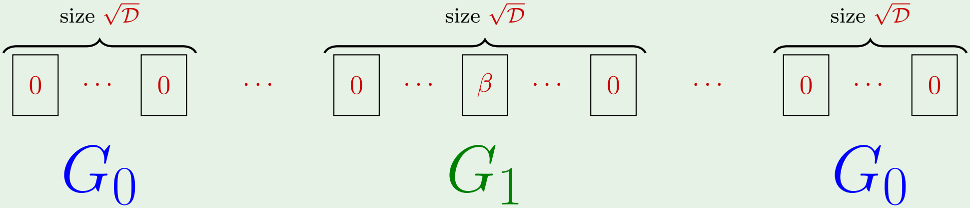
- Corrupted parties see $\mathcal{S}$ many single-degree seeds and $\mathcal{T}$ many two-degree seeds.
- Conditioned on $\mathcal{S}$ and $\mathcal{T}$, the actual configuration is identically distributed for G_0 and G_1.
- Only need to argue the closeness of the joint distribution

$$(\mathcal{S}, \mathcal{T})$$

- $\mathcal{T}$ is the identical for G_0 and G_1
- Conditioned on $\mathcal{T}$, distribution of $\mathcal{S}$ is
  - G_0: $\ell - \mathcal{T}$ many Bernolli samples with bias $(n-1)/n$
  - G_1: distribution of G_0 shifted by $\Omega(n)$ many Bernolli samples with bias $(n-1)/n$
- Omitting many details, $\ell = \Omega(n^4)$ suffices!

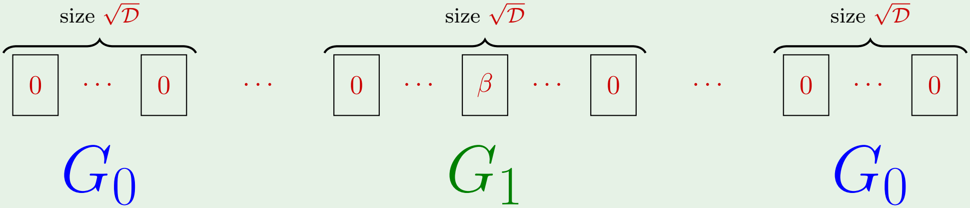


Summary



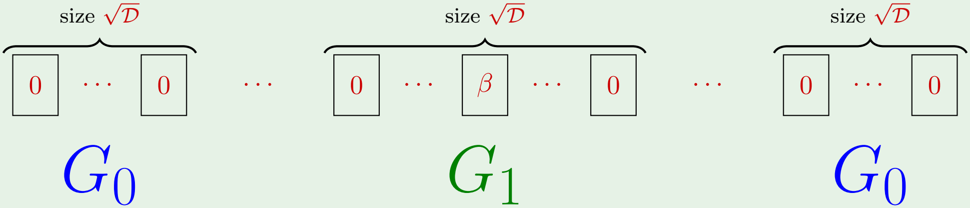
- We construct a randomized special combinatorial design with size $\mathcal{O}(n^4)$
- Overall per party share size $\mathcal{O}\left(n^3 \cdot \sqrt{\mathcal{D}}\right)$

Summary



- We construct a randomized special combinatorial design with size $\mathcal{O}(n^4)$
- Overall per party share size $\mathcal{O}\left(n^3 \cdot \sqrt{\mathcal{D}}\right)$
- Only $1/\mathsf{poly}(\lambda)$-weakly secure, need privacy amplification [Boyle-Gilboa-Ishai-Kolobov'22]

Summary



- We construct a <u>randomized</u> special combinatorial design with size $\mathcal{O}(n^4)$
- Overall per party share size $\mathcal{O}\left(n^3 \cdot \sqrt{\mathcal{D}}\right)$
- Only $1/\mathsf{poly}(\lambda)$-weakly secure, need privacy amplification [Boyle-Gilboa-Ishai-Kolobov'22]

Thanks, questions? `ia.cr/2025/1074`