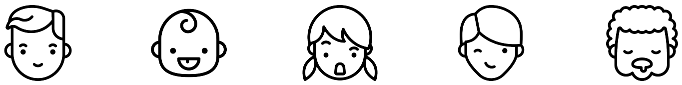
Breaking the Circuit-Size Barrier in Secret Sharing

Tianren Liu   Vinod Vaikuntanathan
MIT   MIT

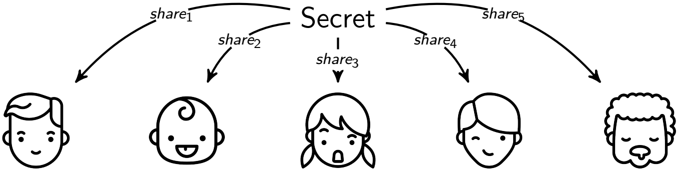
50th ACM Symposium on Theory of Computing
June 27, 2018

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

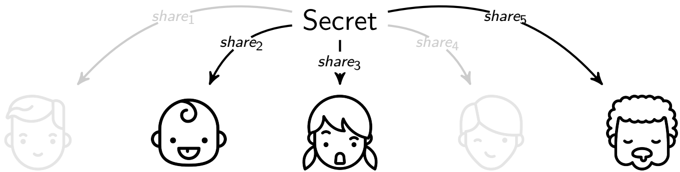
Secret



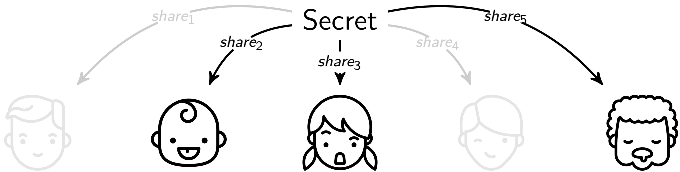
Secret Sharing [Blakley'79,Shamir'79,Ito-Saito-Nishizeki'87]



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

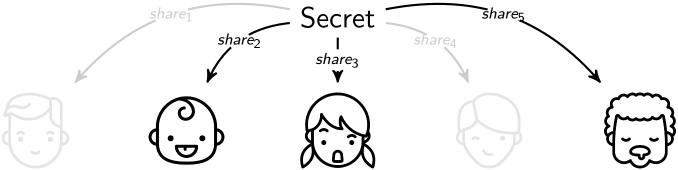


Secret Sharing [Blakley'79,Shamir'79,Ito-Saito-Nishizeki'87]



Can this subset of participants recover the secret?

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

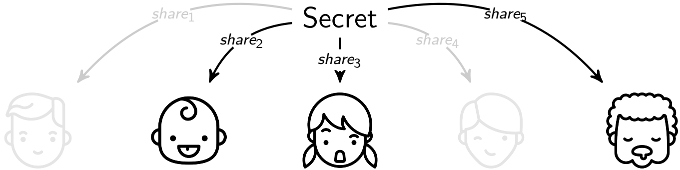


Can this subset of participants recover the secret?

Threshold Secret Sharing [Shamir'79]

Any subset of $\geq k$ participants can recover the secret.
Any subset of $< k$ participants learns no information.

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



Can this subset of participants recover the secret?

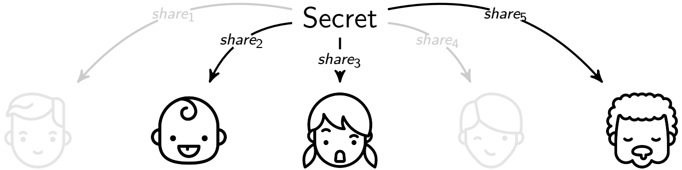
Threshold Secret Sharing [Shamir'79]

Any subset of $\geq k$ participants can recover the secret.
Any subset of $< k$ participants learns no information.

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

Any subset X that $F(X) = 1$ can recover the secret.
Any subset X that $F(X) = 0$ learns no information.

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



Can this subset of participants recover the secret?

Threshold Secret Sharing [Shamir'79]

Any subset of $\geq k$ participants can recover the secret.
Any subset of $< k$ participants learns no information.

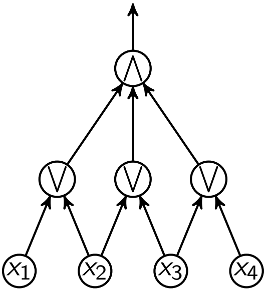
General Secret Sharing [ISN'89] **monotone** $F : \{0,1\}^n \rightarrow \{0,1\}$

Any subset X that $F(X) = 1$ can recover the secret.
Any subset X that $F(X) = 0$ learns no information.

A General Secret Sharing Scheme [Benaloh-Leichter'88]

F is computed by some monotone formula

- Generate a tag for each wire
  - Output wire tag: the secret s
  - AND gate: additively share the output wire tag
  - OR gate: copy the output wire tag
- The i-th participant's share: all tags of its input wires

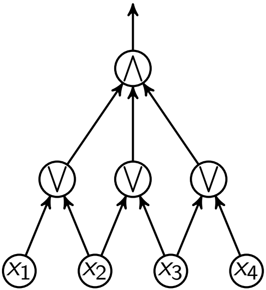


Total share size = formula size of $F \leq \tilde{O}(2^n)$

A General Secret Sharing Scheme [Benaloh-Leichter'88]

F is computed by some monotone formula

- Generate a tag for each wire
  - Output wire tag: the secret s
  - AND gate: additively share the output wire tag
  - OR gate: copy the output wire tag
- The i-th participant's share: all tags of its input wires

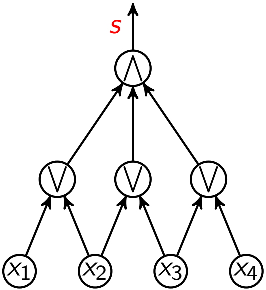


Total share size = formula size of $F \leq \tilde{O}(2^n)$

A General Secret Sharing Scheme [Benaloh-Leichter'88]

F is computed by some monotone formula

- Generate a tag for each wire
  - Output wire tag: the secret s
  - AND gate: additively share the output wire tag
  - OR gate: copy the output wire tag
- The i-th participant's share: all tags of its input wires

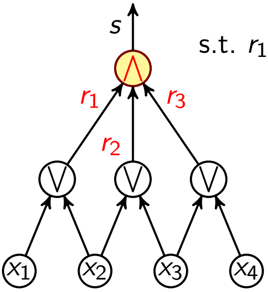


Total share size = formula size of $F \leq \tilde{O}(2^n)$

A General Secret Sharing Scheme [Benaloh-Leichter'88]

F is computed by some monotone formula

- Generate a tag for each wire
  - Output wire tag: the secret s
  - AND gate: additively share the output wire tag
  - OR gate: copy the output wire tag
- The i-th participant's share: all tags of its input wires



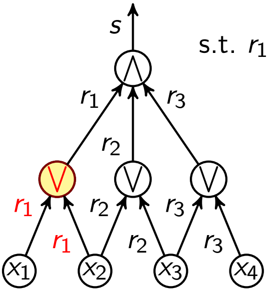
s.t. $r_1 + r_2 + r_3 = s$

Total share size = formula size of $F \leq \tilde{O}(2^n)$

A General Secret Sharing Scheme [Benaloh-Leichter'88]

F is computed by some monotone formula

- Generate a tag for each wire
  - Output wire tag: the secret s
  - AND gate: additively share the output wire tag
  - OR gate: copy the output wire tag
- The i-th participant's share: all tags of its input wires



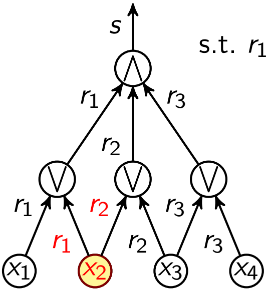
s.t. $r_1 + r_2 + r_3 = s$

Total share size $=$ formula size of $F \leq \tilde{O}(2^n)$

A General Secret Sharing Scheme [Benaloh-Leichter'88]

F is computed by some monotone formula

- Generate a tag for each wire
    - Output wire tag: the secret s
    - AND gate: additively share the output wire tag
    - OR gate: copy the output wire tag
- The i-th participant's share: all tags of its input wires



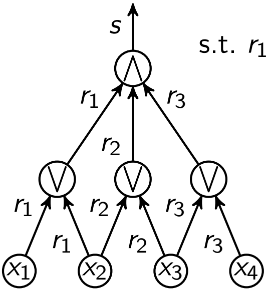
s.t. $r_1 + r_2 + r_3 = s$

Total share size $=$ formula size of $F \leq \tilde{O}(2^n)$

A General Secret Sharing Scheme [Benaloh-Leichter'88]

F is computed by some monotone formula

- Generate a tag for each wire
  - Output wire tag: the secret s
  - AND gate: additively share the output wire tag
  - OR gate: copy the output wire tag
- The i-th participant's share: all tags of its input wires



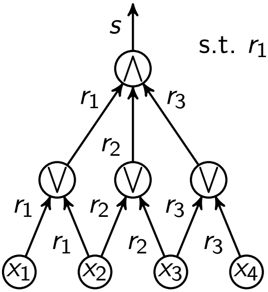
s.t. $r_1 + r_2 + r_3 = s$

Total share size $=$ formula size of $F \le \tilde{O}(2^n)$

A General Secret Sharing Scheme [Benaloh-Leichter'88]

F is computed by some monotone formula

- Generate a tag for each wire
  - Output wire tag: the secret s
  - AND gate: additively share the output wire tag
  - OR gate: copy the output wire tag
- The i-th participant's share: all tags of its input wires



s.t. $r_1 + r_2 + r_3 = s$

Total share size $=$ formula size of $F \le \tilde{O}(2^n)$

Key Complexity Measure: Total Share Size

Upper Bounds

Share size $= O$(monotone formula size) [Benaloh-Leichter'88]

Key Complexity Measure: Total Share Size

Upper Bounds

Share size $= O$(monotone formula size) [Benaloh-Leichter'88]

Share size $= O$(monotone span program size) [Karchmer-Wigderson'93]

Key Complexity Measure: Total Share Size

Upper Bounds

Share size $= O(\text{monotone formula size}) \leq \frac{2^n}{\text{poly}(n)}$.

Share size $= O(\text{monotone span program size}) \leq \frac{2^n}{\text{poly}(n)}$.

Key Complexity Measure: Total Share Size

Upper Bounds

Share size $= O(\text{monotone formula size}) \leq \frac{2^n}{\text{poly}(n)}$.

Share size $= O(\text{monotone span program size}) \leq \frac{2^n}{\text{poly}(n)}$.

Lower Bounds

Exists an explicit F s.t. total share size $= \tilde{\Omega}(n^2)$. [Csirmaz'97]

Key Complexity Measure: Total Share Size

Upper Bounds

Share size $= O(\text{monotone formula size}) \leq \frac{2^n}{\text{poly}(n)}$.

Share size $= O(\text{monotone span program size}) \leq \frac{2^n}{\text{poly}(n)}$.

Lower Bounds

Exists an explicit F s.t. total share size $= \tilde{\Omega}(n^2)$. [Csirmaz'97]

(No better lower bounds, even existentially.)

Key Complexity Measure: Total Share Size

Upper Bounds

Share size $= O(\text{monotone formula size}) \leq \frac{2^n}{\text{poly}(n)}$.

Share size $= O(\text{monotone span program size}) \leq \frac{2^n}{\text{poly}(n)}$.

Lower Bounds

Exists an explicit F s.t. total share size $= \tilde{\Omega}(n^2)$. [Csirmaz'97]

(No better lower bounds, even existentially.)

Can we do better?

30^{+}-year-old open problem

Our Results

Yes, we can!

Theorem 1

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

Key Complexity Measure: Total Share Size

Upper Bounds: *Linear* Secret Sharing

Share size $= O(\text{monotone formula size}) \leq \frac{2^n}{\text{poly}(n)}$.

Share size $= \Theta(\text{monotone span program size}) \leq \frac{2^n}{\text{poly}(n)}$.

Lower Bounds: *Linear* Secret Sharing

Exists $\{F_n\}$ s.t. total share size $= \tilde{\Omega}(2^{n/2})$.

Can we do better?

Key Complexity Measure: Total Share Size

Upper Bounds: *Linear* Secret Sharing

Share size $= O(\text{monotone formula size}) \leq \frac{2^n}{\text{poly}(n)}$.

Share size $= \Theta(\text{monotone span program size}) \leq \frac{2^n}{\text{poly}(n)}$.

Lower Bounds: *Linear* Secret Sharing

Exists $\{F_n\}$ s.t. total share size $= \tilde{\Omega}(2^{n/2})$.

($2^{\Omega(n)}$ for an explicit $\{F_n\}$ [Pitassi-Robere'18])

Can we do better?

Our Results

Yes, we can!

Theorem 2

Every monotone F has a *linear* secret sharing with share size $2^{0.999n}$.

Our Results

Yes, we can!

Theorem 2

Every monotone F has a *linear* secret sharing with share size $2^{0.999n}$.

Corollary

Every monotone F has a monotone span program of size $2^{0.999n}$.

Our Approach

Every monotone F can be computed by a monotone formula s.t.

Prop. I

Prop. II

Our Approach

Every monotone F can be computed by a monotone formula s.t.

Prop. I has size $2^{0.994n}$

Prop. II

Our Approach

Every monotone F can be computed by a monotone formula s.t.

Prop. I   has size $2^{0.994n}$

Prop. II

$$\text{Formula size} \gtrsim \log(\#\text{Monotone Functions}) \geq \frac{2^n}{\text{poly}(n)}$$

Our Approach

Every monotone F can be computed by a monotone formula s.t.

Prop. I has size $2^{0.994n}$

Prop. II

$$\text{Formula size} \times \log(\#\text{Base Gates}) \geq \log(\#\text{Monotone Functions}) \geq \frac{2^n}{\text{poly}(n)}$$

Our Approach

Every monotone F can be computed by a monotone formula s.t.

Prop. I has size $2^{0.994n}$

Prop. II

$$\text{Formula size} \times \log(\#\text{Base Gates}) \geq \log(\#\text{Monotone Functions}) \geq \frac{2^n}{\text{poly}(n)}$$

$\implies$ Requires $2^{\tilde{\Omega}(2^n)}$ gates in formula basis.

Our Approach

Every monotone F can be computed by a monotone formula s.t.

Prop. I has size $2^{0.994n}$ using an extended basis of $2^{\tilde{\Omega}(2^n)}$ gates

Prop. II

Our Approach

Every monotone F can be computed by a monotone formula s.t.

Prop. I has size $2^{0.994n}$ using an extended basis of $2^{\tilde{\Omega}(2^n)}$ gates

Prop. II every gate in the basis is a monotone function that has an efficient secret sharing scheme

Our Approach

Every monotone F can be computed by a monotone formula s.t.

- Prop. I has size $2^{0.994n}$ using an extended basis of $2^{\tilde{\Omega}(2^n)}$ gates
- Prop. II every gate in the basis is a monotone function that has an efficient secret sharing scheme

Base gates [Liu-Vaikuntanathan-Wee'18]

We define **slice functions**, there are $2^{\binom{n}{n/2}}$ of them and they have secret scharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.

Our Approach

Slice Functions

all F such that
$\|x\| > n/2 \implies F(x) = 1$
$\|x\| < n/2 \implies F(x) = 0$

$\#\text{functions} = 2^{\binom{n}{n/2}}$

Share size $= 2^{\tilde{O}(\sqrt{n})}$

Our Approach

Slice Functions

all F such that
$\|x\| > n/2 \implies F(x) = 1$
$\|x\| < n/2 \implies F(x) = 0$

$\#\text{functions} = 2^{\binom{n}{n/2}}$

Share size $= 2^{\tilde{O}(\sqrt{n})}$

Monotone Functions

all monotone F

Share size $= 2^{0.994n}$

monotone formula
size: $2^{0.994n}$
depth: constant
gates: $\wedge, \vee$, slice functions

Our Approach

Slice Functions	*Fat-Slice Functions*	*Monotone Functions*
all F such that $\|x\| > n/2 \implies F(x) = 1$ $\|x\| < n/2 \implies F(x) = 0$	all F such that $\|x\| > .51n \Rightarrow F(x) = 1$ $\|x\| < .49n \Rightarrow F(x) = 0$	all monotone F
$\#\text{functions} = 2^{\binom{n}{n/2}}$		
Share size $= 2^{\tilde{O}(\sqrt{n})}$	Share size $= 2^{(1-c)n}$	Share size $= 2^{0.994n}$

monotone formula

size: $2^{0.994n}$

depth: constant

gates: $\wedge, \vee$, slice functions

Our Approach

Slice Functions	*Fat-Slice Functions*	*Monotone Functions*
all F such that $\|x\| > n/2 \implies F(x) = 1$ $\|x\| < n/2 \implies F(x) = 0$	all F such that $\|x\| > .51n \Rightarrow F(x) = 1$ $\|x\| < .49n \Rightarrow F(x) = 0$	all monotone F
$\#\text{functions} = 2^{\binom{n}{n/2}}$		
Share size $= 2^{\tilde{O}(\sqrt{n})}$	Share size $= 2^{(1-c)n}$	Share size $= 2^{0.994n}$

monotone formula
size: $2^{(1-c)n}$
depth: constant
gates: $\wedge, \vee$, slice func

monotone formula
size: $2^{(1-c')n}$
depth: constant
gates: $\wedge, \vee, 1\times$fat-slice func

Our Approach

Slice Functions

all F such that

$\|x\| > n/2 \implies F(x) = 1$

$\|x\| < n/2 \implies F(x) = 0$

$\#\text{functions} = 2^{\binom{n}{n/2}}$

Share size $= 2^{\tilde{O}(\sqrt{n})}$

Fat-Slice Functions

all F such that

$\|x\| > .51n \Rightarrow F(x) = 1$

$\|x\| < .49n \Rightarrow F(x) = 0$

Share size $= 2^{(1-c)n}$

Monotone Functions

all monotone F

Share size $= 2^{0.994n}$

monotone formula
size: $2^{(1-c)n}$
depth: constant
gates: $\wedge, \vee$, slice func

monotone formula
size: $2^{(1-c')n}$
depth: constant
gates: $\wedge, \vee, 1\times$fat-slice func

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ as the following:

$$F_{\text{bot}}(x) = \bigvee_{\substack{y \text{ s.t.} \\ \|y\|<.49n \\ F(y)=1}} \mathbb{1}_{x \geq y} = \bigvee_{\substack{y \text{ s.t.} \\ \|y\|<.49n \\ F(y)=1}} \bigwedge_{i, y_i=1} x_i$$

$$F_{\text{mid}}(x) = \begin{cases} 0, & \text{if } \|x\| < .49n \\ F(x), & \text{if } \|x\| \approx .5n \\ 1, & \text{if } \|x\| > .51n \end{cases}$$

F_{mid} is a fat-slice function.

$$F_{\text{top}}(x) = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\|>.51n \\ F(y)=0}} \mathbb{1}_{x \not\leq y} = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\|>.51n \\ F(y)=0}} \bigvee_{i, y_i=0} x_i$$

F_{bot} is the smallest monotone function that agrees with F on all input x that $\|x\| < .49n$.

F_{top} is the largest monotone function that agrees with F on all input x that $\|x\| > .51n$.

Fat-Slice Functions $\Longrightarrow$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ as the following:

$$F_{\text{bot}}(x) = \bigvee_{\substack{y \text{ s.t.} \\ \|y\| < .49n \\ F(y)=1}} \mathbb{1}_{x \geq y} = \bigvee_{\substack{y \text{ s.t.} \\ \|y\| < .49n \\ F(y)=1}} \bigwedge_{i, y_i = 1} x_i$$

$$F_{\text{mid}}(x) = \begin{cases} 0, & \text{if } \|x\| < .49n \\ F(x), & \text{if } \|x\| \approx .5n \\ 1, & \text{if } \|x\| > .51n \end{cases}$$

F_{mid} is a fat-slice function.

$$F_{\text{top}}(x) = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\| > .51n \\ F(y)=0}} \mathbb{1}_{x \not\leq y} = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\| > .51n \\ F(y)=0}} \bigvee_{i, y_i = 0} x_i$$

F_{bot} is the smallest monotone function that agrees with F on all input x that $\|x\| < .49n$.

F_{top} is the largest monotone function that agrees with F on all input x that $\|x\| > .51n$.

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ as the following:

$$F_{\text{bot}}(x) = \bigvee_{\substack{y \text{ s.t.} \\ \|y\|<.49n \\ F(y)=1}} \mathbb{1}_{x \geq y} = \bigvee_{\substack{y \text{ s.t.} \\ \|y\|<.49n \\ F(y)=1}} \bigwedge_{i, y_i=1} x_i$$

$$F_{\text{mid}}(x) = \begin{cases} 0, & \text{if } \|x\| < .49n \\ F(x), & \text{if } \|x\| \approx .5n \\ 1, & \text{if } \|x\| > .51n \end{cases}$$

F_{mid} is a fat-slice function.
Share size $= 2^{(1-c)n}$

$$F_{\text{top}}(x) = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\|>.51n \\ F(y)=0}} \mathbb{1}_{x \not\leq y} = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\|>.51n \\ F(y)=0}} \bigvee_{i, y_i=0} x_i$$

F_{bot} is the smallest monotone function that agrees with F on all input x that $\|x\| < .49n$.

F_{top} is the largest monotone function that agrees with F on all input x that $\|x\| > .51n$.

Fat-Slice Functions $\Longrightarrow$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ as the following:

$$F_{\text{bot}}(x) = \bigvee_{\substack{y \text{ s.t.} \\ \|y\|<.49n \\ F(y)=1}} \mathbb{1}_{x \geq y} = \bigvee_{\substack{y \text{ s.t.} \\ \|y\|<.49n \\ F(y)=1}} \bigwedge_{i, y_i=1} x_i$$

$$F_{\text{mid}}(x) = \begin{cases} 0, & \text{if } \|x\| < .49n \\ F(x), & \text{if } \|x\| \approx .5n \\ 1, & \text{if } \|x\| > .51n \end{cases}$$

F_{mid} is a fat-slice function.
Share size $= 2^{(1-c)n}$

$$F_{\text{top}}(x) = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\|>.51n \\ F(y)=0}} \mathbb{1}_{x \not\leq y} = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\|>.51n \\ F(y)=0}} \bigvee_{i, y_i=0} x_i$$

F_{bot} is the smallest monotone function that agrees with F on all input x that $\|x\| < .49n$.

F_{top} is the largest monotone function that agrees with F on all input x that $\|x\| > .51n$.

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ as the following:

$$F_{\text{bot}}(x) = \bigvee_{\substack{y \text{ s.t.} \\ \|y\| < .49n \\ F(y)=1}} \mathbb{1}_{x \geq y} = \bigvee_{\substack{y \text{ s.t.} \\ \|y\| < .49n \\ F(y)=1}} \bigwedge_{i, y_i = 1} x_i$$

$$F_{\text{mid}}(x) = \begin{cases} 0, & \text{if } \|x\| < .49n \\ F(x), & \text{if } \|x\| \approx .5n \\ 1, & \text{if } \|x\| > .51n \end{cases}$$

F_{mid} is a fat-slice function.
Share size $= 2^{(1-c)n}$

$$F_{\text{top}}(x) = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\| > .51n \\ F(y)=0}} \mathbb{1}_{x \not\leq y} = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\| > .51n \\ F(y)=0}} \bigvee_{i, y_i = 0} x_i$$

F_{bot} is the smallest monotone function that agrees with F on all input x that $\|x\| < .49n$.

F_{top} is the largest monotone function that agrees with F on all input x that $\|x\| > .51n$.

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ as the following:

$$F_{\text{bot}}(x) = \bigvee_{\substack{y \text{ s.t.} \\ \|y\|<.49n \\ F(y)=1}} \mathbb{1}_{x \geq y} = \bigvee_{\substack{y \text{ s.t.} \\ \|y\|<.49n \\ F(y)=1}} \bigwedge_{i, y_i=1} x_i$$

$$F_{\text{mid}}(x) = \begin{cases} 0, & \text{if } \|x\| < .49n \\ F(x), & \text{if } \|x\| \approx .5n \\ 1, & \text{if } \|x\| > .51n \end{cases}$$

F_{mid} is a fat-slice function.
Share size $= 2^{(1-c)n}$

$$F_{\text{top}}(x) = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\|>.51n \\ F(y)=0}} \mathbb{1}_{x \not\leq y} = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\|>.51n \\ F(y)=0}} \bigvee_{i, y_i=0} x_i$$

F_{bot} is the smallest monotone function that agrees with F on all input x that $\|x\| < .49n$.

F_{top} is the largest monotone function that agrees with F on all input x that $\|x\| > .51n$.

Fat-Slice Functions $\Longrightarrow$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ as the following:

$$F_{\text{bot}}(x) = \bigvee_{\substack{y \text{ s.t.} \\ \|y\|<.49n \\ F(y)=1}} \mathbb{1}_{x \geq y} = \bigvee_{\substack{y \text{ s.t.} \\ \|y\|<.49n \\ F(y)=1}} \bigwedge_{i, y_i=1} x_i$$

$$F_{\text{mid}}(x) = \begin{cases} 0, & \text{if } \|x\| < .49n \\ F(x), & \text{if } \|x\| \approx .5n \\ 1, & \text{if } \|x\| > .51n \end{cases}$$

F_{mid} is a fat-slice function.
Share size $= 2^{(1-c)n}$

$$F_{\text{top}}(x) = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\|>.51n \\ F(y)=0}} \mathbb{1}_{x \not\leq y} = \bigwedge_{\substack{y \text{ s.t.} \\ \|y\|>.51n \\ F(y)=0}} \bigvee_{i, y_i=0} x_i$$

$F_{\text{bot}}, F_{\text{top}}$ has monotone formula of size $2^{h(.49)\cdot n} = 2^{(1-c')n}$
$\Longrightarrow$ Share size $= 2^{(1-c')n}$

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ such that:

<table>
<tr><th></th><th>$F_{\text{bot}}(x)$</th><th>$F_{\text{mid}}(x)$</th><th>$F_{\text{top}}(x)$</th></tr>
<tr><td>$\|x\| < .49n$</td><td>$= F(x)$</td><td>$= 0$</td><td rowspan="2">$\geq F(x)$</td></tr>
<tr><td>$\|x\| \in [.49n, .51n]$</td><td rowspan="2">$\leq F(x)$</td><td>$= F(x)$</td></tr>
<tr><td>$\|x\| > .51n$</td><td>$= 1$</td><td>$= F(x)$</td></tr>
</table>

- $F(x) = \text{Majority}(F_{\text{bot}}(x), F_{\text{mid}}(x), F_{\text{top}}(x))$

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ such that:

<table>
<tr><th></th><th>$F_{\text{bot}}(x)$</th><th>$F_{\text{mid}}(x)$</th><th>$F_{\text{top}}(x)$</th></tr>
<tr><td>$\|x\| < .49n$</td><td>$= F(x)$</td><td>$= 0$</td><td rowspan="2">$\geq F(x)$</td></tr>
<tr><td>$\|x\| \in [.49n, .51n]$</td><td rowspan="2">$\leq F(x)$</td><td>$= F(x)$</td></tr>
<tr><td>$\|x\| > .51n$</td><td>$= 1$</td><td>$= F(x)$</td></tr>
</table>

- $F(x) = \text{Majority}(F_{\text{bot}}(x), F_{\text{mid}}(x), F_{\text{top}}(x))$

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ such that:

<table>
<tr><th></th><th>$F_{\text{bot}}(x)$</th><th>$F_{\text{mid}}(x)$</th><th>$F_{\text{top}}(x)$</th></tr>
<tr><td>$\|x\| < .49n$</td><td>$= F(x)$</td><td>$= 0$</td><td rowspan="2">$\geq F(x)$</td></tr>
<tr><td>$\|x\| \in [.49n, .51n]$</td><td rowspan="2">$\leq F(x)$</td><td>$= F(x)$</td></tr>
<tr><td>$\|x\| > .51n$</td><td>$= 1$</td><td>$= F(x)$</td></tr>
</table>

- $F(x) = (F_{\text{bot}}(x) \vee F_{\text{mid}}(x)) \wedge F_{\text{top}}(x)$

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ such that:

- F_{mid} lays in "a fat slice" $[49\%, 51\%]$
  $\implies$ Share size of $F_{\text{mid}} = 2^{(1-c)n}$
- $F_{\text{bot}}, F_{\text{top}}$ computed by size-$2^{h(.49)\cdot n}$ formula
  $\implies$ Share size of $F_{\text{bot}}, F_{\text{top}} = 2^{(1-c')n}$
- $F(x) = F_{\text{bot}}(x) \vee F_{\text{mid}}(x) \wedge F_{\text{top}}(x)$
  $\implies$ Share size of $F = 2^{(1-c)n} + 2 \cdot 2^{(1-c')n}$
  $= O(2^{\max(1-c, 1-c')n})$

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ such that:

- F_{mid} lays in "a fat slice" $[49\%, 51\%]$
  $\implies$ Share size of $F_{\text{mid}} = 2^{(1-c)n}$
- $F_{\text{bot}}, F_{\text{top}}$ computed by size-$2^{h(.49)\cdot n}$ formula
  $\implies$ Share size of $F_{\text{bot}}, F_{\text{top}} = 2^{(1-c')n}$
- $F(x) = F_{\text{bot}}(x) \vee F_{\text{mid}}(x) \wedge F_{\text{top}}(x)$
  $\implies$ Share size of $F = 2^{(1-c)n} + 2 \cdot 2^{(1-c')n}$
  $= O(2^{\max(1-c,1-c')n})$

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ such that:

- F_{mid} lays in "a fatter slice" $[40\%, 60\%]$
  $\implies$ Share size of $F_{\text{mid}} = 2^{(1-c)n}$
- $F_{\text{bot}}, F_{\text{top}}$ computed by size-$2^{h(.49)\cdot n}$ formula
  $\implies$ Share size of $F_{\text{bot}}, F_{\text{top}} = 2^{(1-c')n}$
- $F(x) = F_{\text{bot}}(x) \vee F_{\text{mid}}(x) \wedge F_{\text{top}}(x)$
  $\implies$ Share size of F $= 2^{(1-c)n} + 2 \cdot 2^{(1-c')n}$
  $= O(2^{\max(1-c, 1-c')n})$

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ such that:

- F_{mid} lays in "a fatter slice" $[40\%, 60\%]$
  $\implies$ Share size of $F_{\text{mid}} = 2^{(1-c)n}$ increase$\uparrow\uparrow$
- $F_{\text{bot}}, F_{\text{top}}$ computed by size-$2^{h(.49)\cdot n}$ formula
  $\implies$ Share size of $F_{\text{bot}}, F_{\text{top}} = 2^{(1-c')n}$
- $F(x) = F_{\text{bot}}(x) \vee F_{\text{mid}}(x) \wedge F_{\text{top}}(x)$
  $\implies$ Share size of F $= 2^{(1-c)n} + 2 \cdot 2^{(1-c')n}$
  $= O(2^{\max(1-c, 1-c')n})$

Fat-Slice Functions $\Longrightarrow$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ such that:

- F_{mid} lays in "a fatter slice" $[40\%, 60\%]$
  $\Longrightarrow$ Share size of $F_{\text{mid}} = 2^{(1-c)n}$ increase$\uparrow\uparrow$
- $F_{\text{bot}}, F_{\text{top}}$ computed by size-$2^{h(.4)\cdot n}$ formula
  $\Longrightarrow$ Share size of $F_{\text{bot}}, F_{\text{top}} = 2^{(1-c')n}$
- $F(x) = F_{\text{bot}}(x) \vee F_{\text{mid}}(x) \wedge F_{\text{top}}(x)$
  $\Longrightarrow$ Share size of $F = 2^{(1-c)n} + 2 \cdot 2^{(1-c')n}$
  $= O(2^{\max(1-c, 1-c')n})$

Fat-Slice Functions $\implies$ All Monotone Functions

Let F be any monotone function.
Define $F_{\text{bot}}, F_{\text{mid}}, F_{\text{top}}$ such that:

- F_{mid} lays in "a fatter slice" $[40\%, 60\%]$
  $\implies$ Share size of $F_{\text{mid}} = 2^{(1-c)n}$ increase↑↑
- $F_{\text{bot}}, F_{\text{top}}$ computed by size-$2^{h(.4)\cdot n}$ formula
  $\implies$ Share size of $F_{\text{bot}}, F_{\text{top}} = 2^{(1-c')n}$ decrease↓↓
- $F(x) = F_{\text{bot}}(x) \vee F_{\text{mid}}(x) \wedge F_{\text{top}}(x)$
  $\implies$ Share size of F $= 2^{(1-c)n} + 2 \cdot 2^{(1-c')n}$
  $= O(2^{\max(1-c,1-c')n})$

To Summarize

Slice Functions

all F such that

$\|x\| > n/2 \implies F(x) = 1$

$\|x\| < n/2 \implies F(x) = 0$

$\#\text{functions} = 2^{\binom{n}{n/2}}$

Share size $= 2^{\tilde{O}(\sqrt{n})}$

Fat-Slice Functions

all F such that

$\|x\| > .51n \Rightarrow F(x) = 1$

$\|x\| < .49n \Rightarrow F(x) = 0$

Share size $= 2^{(1-c')n}$

Monotone Functions

all monotone F

Share size $= 2^{(1-c)n}$

monotone formula

$F(x) = F_{\text{bot}}(x) \vee F_{\text{mid}}(x) \wedge F_{\text{top}}(x)$

To Summarize

Slice Functions

all F such that
$\|x\| > n/2 \implies F(x) = 1$
$\|x\| < n/2 \implies F(x) = 0$

$\#\text{functions} = 2^{\binom{n}{n/2}}$

Share size $= 2^{\tilde{O}(\sqrt{n})}$

Fat-Slice Functions

all F such that
$\|x\| > .51n \Rightarrow F(x) = 1$
$\|x\| < .49n \Rightarrow F(x) = 0$

Share size $= 2^{(1-c')n}$

Monotone Functions

all monotone F

Share size $= 2^{0.994n}$

monotone formula
size: $2^{0.994n}$
depth: constant
gates: $\wedge, \vee$, slice functions

To Summarize

Slice Functions	*Fat-Slice Functions*	*Monotone Functions*
all F such that $\|x\| > n/2 \implies F(x) = 1$ $\|x\| < n/2 \implies F(x) = 0$	all F such that $\|x\| > .51n \Rightarrow F(x) = 1$ $\|x\| < .49n \Rightarrow F(x) = 0$	all monotone F
$\#\text{functions} = 2^{\binom{n}{n/2}}$		
Share size $= 2^{\tilde{O}(\sqrt{n})}$	Share size $= 2^{(1-c')n}$	Share size $= 2^{0.994n}$

Previous Work [LVW'18]

monotone formula
size: $2^{0.994n}$
depth: constant
gates: $\wedge, \vee$, slice functions

Our Result

To Summarize

Slice Functions

all F such that
$\|x\| > n/2 \implies F(x) = 1$
$\|x\| < n/2 \implies F(x) = 0$

$\#\text{functions} = 2^{\binom{n}{n/2}}$

Share size $= 2^{\tilde{O}(\sqrt{n})}$

Fat-Slice Functions

all F such that
$\|x\| > .51n \Rightarrow F(x) = 1$
$\|x\| < .49n \Rightarrow F(x) = 0$

Share size $= 2^{(1-c')n}$

Monotone Functions

all monotone F

Share size $= 2^{0.994n}$

monotone formula
size: $2^{0.994n}$
depth: constant
gates: $\wedge, \vee$, slice functions

To Summarize

Slice Functions	*Fat-Slice Functions*	*Monotone Functions*
all F such that $\|x\| > n/2 \Longrightarrow F(x) = 1$ $\|x\| < n/2 \Longrightarrow F(x) = 0$	all F such that $\|x\| > .51n \Rightarrow F(x) = 1$ $\|x\| < .49n \Rightarrow F(x) = 0$	all monotone F
$\#$functions $= 2^{\binom{n}{n/2}}$		
Share size $= 2^{\tilde{O}(\sqrt{n})}$	Share size $= 2^{(1-c')n}$	Share size $= 2^{0.1n}$

monotone formula
size: $2^{0.1n}$
depth: constant
gates: $\wedge, \vee$, slice functions

Open Problem!

To Summarize

Slice Functions

all F such that
$\|x\| > n/2 \implies F(x) = 1$
$\|x\| < n/2 \implies F(x) = 0$

$\#\text{functions} = 2^{\binom{n}{n/2}}$

Share size $= 2^{\tilde{O}(\sqrt{n})}$

Fat-Slice Functions

all F such that
$\|x\| > .51n \Rightarrow F(x) = 1$
$\|x\| < .49n \Rightarrow F(x) = 0$

Share size $= 2^{(1-c')n}$

Monotone Functions

all monotone F

Share size $= 2^{\tilde{O}(\sqrt{n})}$

monotone formula
size: $2^{\tilde{O}(\sqrt{n})}$
depth: constant
gates: $\wedge, \vee$, slice functions

$\boxed{\textit{Open Problem!}}$

To Summarize (Linear Secret Sharing)

Slice Functions

all F such that
$\|x\| > n/2 \implies F(x) = 1$
$\|x\| < n/2 \implies F(x) = 0$

$\#\text{functions} = 2^{\binom{n}{n/2}}$

Share size $= \tilde{\Theta}(2^{n/2})$

Monotone Functions

all monotone F

Share size $= 2^{0.999n}$

monotone formula
size: $2^{0.999n}$
depth: constant
gates: $\wedge, \vee$, $2^{0.499} \times$slice functions

To Summarize (Linear Secret Sharing)

Slice Functions

all F such that
$\|x\| > n/2 \implies F(x) = 1$
$\|x\| < n/2 \implies F(x) = 0$

$\#\text{functions} = 2^{\binom{n}{n/2}}$

Share size $= \tilde{\Theta}(2^{n/2})$ (tight)

Monotone Functions

all monotone F

Share size $= 2^{0.999n}$

monotone formula
size: $2^{0.999n}$
depth: constant
gates: $\wedge, \vee$, $2^{0.499} \times$slice functions

To Summarize (Linear Secret Sharing)

Slice Functions

all F such that
$\|x\| > n/2 \implies F(x) = 1$
$\|x\| < n/2 \implies F(x) = 0$

$\#\text{functions} = 2^{\binom{n}{n/2}}$

Share size $= \tilde{\Theta}(2^{n/2})$ (tight)

Monotone Functions

all monotone F

Share size $= 2^{0.999n}$

Corollary: Monotone Span Program Complexity

Every monotone F has a monotone span program of size $2^{0.999n}$.

To Summarize

Secret sharing for any monotone function:

To Summarize

Secret sharing for any monotone function:

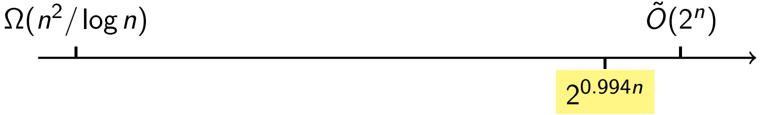
$\Omega(n^2/\log n)$ $\tilde{O}(2^n)$

Linear secret sharing for any monotone function:

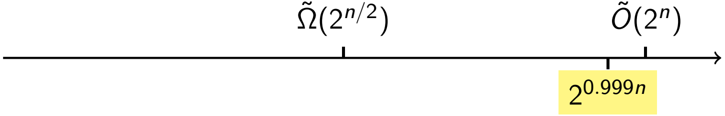
$\tilde{\Omega}(2^{n/2})$ $\tilde{O}(2^n)$

To Summarize

Secret sharing for any monotone function:



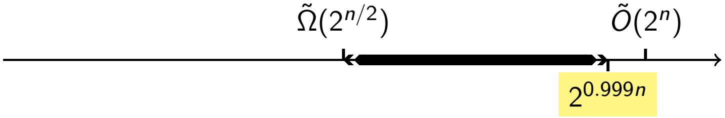
Linear secret sharing for any monotone function:



To Summarize

Secret sharing for any monotone function:

Linear secret sharing for any monotone function:



To Summarize

All Monotone Functions

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

$\forall F$ has a linear secret sharing scheme with share size $2^{0.999n}$.

To Summarize

All Monotone Functions

$\forall F$ has a secret sharing scheme with share size $2^{0.994n}$.
$\forall F$ has a linear secret sharing scheme with share size $2^{0.999n}$.

Slice Functions [LVW'18,BKN'18]

Every slice function (there are $2^{\binom{n}{n/2}}$ of them) has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.

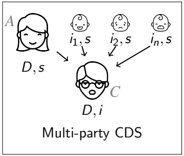
To Summarize

All Monotone Functions

$\forall F$ has a secret sharing scheme with share size $2^{0.994n}$.
$\forall F$ has a linear secret sharing scheme with share size $2^{0.999n}$.

Slice Functions [LVW'18,BKN'18]

Every slice function (there are $2^{\binom{n}{n/2}}$ of them) has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.



[LVW'18]

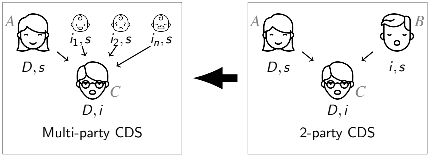
To Summarize

All Monotone Functions

$\forall F$ has a secret sharing scheme with share size $2^{0.994n}$.
$\forall F$ has a linear secret sharing scheme with share size $2^{0.999n}$.

Slice Functions [LVW'18,BKN'18]

Every slice function (there are $2^{\binom{n}{n/2}}$ of them) has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.



[LVW'18] [LVW'17]

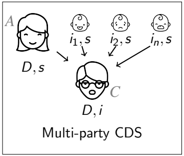
To Summarize

All Monotone Functions

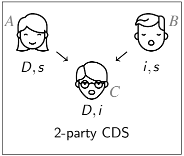
$\forall F$ has a secret sharing scheme with share size $2^{0.994n}$.
$\forall F$ has a linear secret sharing scheme with share size $2^{0.999n}$.

Slice Functions [LVW'18,BKN'18]

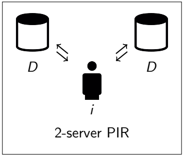
Every slice function (there are $2^{\binom{n}{n/2}}$ of them) has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.



[LVW'18]



[LVW'17]



[Yek'08,Efr'09,DG'15]

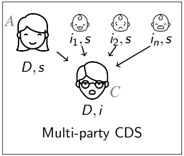
To Summarize

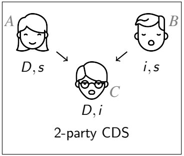
All Monotone Functions

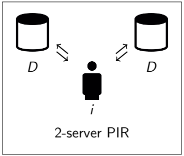
$\forall F$ has a secret sharing scheme with share size $2^{0.994n}$.
$\forall F$ has a linear secret sharing scheme with share size $2^{0.999n}$.

Slice Functions [LVW'18,BKN'18]

Every slice function (there are $2^{\binom{n}{n/2}}$ of them) has a secret sharing scheme with share size $2^{\tilde{O}(\sqrt{n})}$.







Matching Vectors, OR-poly

[LVW'18] [LVW'17] [Yek'08,Efr'09,DG'15] [BBR'94]