BILL START THE RECORDING
FILL OUT ALL COURSE EVALS

You got an email asking you to fill out course evals.
FILL OUT ALL COURSE EVALS

You got an email asking you to fill out course evals.

FILL THEM OUT! Three reasons.

1. Teachers reads them and uses it to help their teaching. Especially the comments.
2. The teaching eval comm reads them to help teachers with weak spots. I was the originator and the chair of the Teaching Eval Comm for 12 years. I was frustrated with courses with not-that-many evals filled out! (Nobody should be in any admin position for more than 5 years!)
3. These evals are used in the promotion process (e.g., Tenure). It is our hope that because the Teaching Eval Comm helps people become better teachers, there is NO bad teaching so this is not an obstacle for promotion.
4. And you can help us! By filling out the forms!
FILL OUT ALL COURSE EVALS

You got an email asking you to fill out course evals.

FILL THEM OUT! Three reasons.

1. Teachers reads them and uses it to help their teaching. Especially the comments.
FILL OUT ALL COURSE EVALS

You got an email asking you to fill out course evals.

FILL THEM OUT! Three reasons.

1. Teachers reads them and uses it to help their teaching. Especially the comments.

2. The teaching eval comm reads them to help teachers with weak spots. I was the originator and the chair of the Teaching Eval Comm for 12 years. I was frustrated with courses with not-that-many evals filled out! (Nobody should be in any admin position for more than 5 years!)
You got an email asking you to fill out course evals.

FILL THEM OUT! Three reasons.

1. Teachers reads them and uses it to help their teaching. Especially the comments.

2. The teaching eval comm reads them to help teachers with weak spots. I was the originator and the chair of the Teaching Eval Comm for 12 years. I was frustrated with courses with not-that-many evals filled out! (Nobody should be in any admin position for more than 5 years!)

3. These evals are used in the promotion process (e.g., Tenure). It is our hope that because the Teaching Eval Comm helps people become better teachers, there is NO bad teaching so this is not an obstacle for promotion.
You got an email asking you to fill out course evals.

**FILL THEM OUT!** Three reasons.

1. Teachers reads them and uses it to help their teaching. Especially the comments.

2. The teaching eval comm reads them to help teachers with weak spots. I was the originator and the chair of the Teaching Eval Comm for 12 years. I was frustrated with courses with not-that-many evals filled out! (Nobody should be in any admin position for more than 5 years!)

3. These evals are used in the promotion process (e.g., Tenure). It is our hope that because the Teaching Eval Comm helps people become better teachers, there is NO bad teaching so this is not an obstacle for promotion.

4. And you can help us! By filling out the forms!
Threshold Secret Sharing: Length of Shares
Length of Shares

Random-string method: domain of the secret has \(\{0, 1\}^n\).
Length of Shares

Random-string method: domain of the secret has \( \{0, 1\}^n \).

Poly method: the secret the domain of the secret was \( \mathbb{Z}_p \).
Can Shares be SHORTER than Secret?

Domain is \( \{0, 1\}^n \).
Can Shares be SHORTER than Secret?

Domain is \( \{0, 1\}^n \).
Can Zelda Secret Share with shares SHORTER than the secret?

1. YES and this is known.
2. NO and this is known.
3. YES but needs a hardness assumption.
4. UNKNOWN TO SCIENCE!

VOTE: Answer NO
Can Shares be SHORTER than Secret?

Domain is \(\{0, 1\}^n\).
Can Zelda Secret Share with shares SHORTER than the secret?

1. YES and this is known.
Can Shares be SHORTER than Secret?

Domain is \( \{0, 1\}^n \).

Can Zelda Secret Share with shares SHORTER than the secret?

1. YES and this is known.
2. NO and this is known.
Can Shares be SHORTER than Secret?

Domain is \( \{0, 1\}^n \).
Can Zelda Secret Share with shares SHORTER than the secret?

1. YES and this is known.
2. NO and this is known.
3. YES but needs a hardness assumption.
Can Shares be SHORTER than Secret?

Domain is \( \{0, 1\}^n \).

Can Zelda Secret Share with shares SHORTER than the secret?

1. YES and this is known.
2. NO and this is known.
3. YES but needs a hardness assumption.
4. UNKNOWN TO SCIENCE!
Can Shares be SHORTER than Secret?

Domain is \(\{0, 1\}^n\).

Can Zelda Secret Share with shares SHORTER than the secret?

1. YES and this is known.
2. NO and this is known.
3. YES but needs a hardness assumption.
4. UNKNOWN TO SCIENCE!

VOTE

Answer NO
Can Shares be SHORTER than Secret?

Domain is $\{0, 1\}^n$.

Can Zelda Secret Share with shares SHORTER than the secret?

1. YES and this is known.
2. NO and this is known.
3. YES but needs a hardness assumption.
4. UNKNOWN TO SCIENCE!

VOTE

**Answer** NO
Example of Why Can’t Have Short Shares

Assume there is a (4, 5) Secret Sharing Scheme where Zelda shares a secret of length 7.
Example of Why Can’t Have Short Shares

Assume there is a (4, 5) Secret Sharing Scheme where Zelda shares a secret of length 7.

(This proof will assume NOTHING about the scheme.)
Example of Why Can’t Have Short Shares

Assume there is a (4, 5) Secret Sharing Scheme where Zelda shares a secret of length 7.

(This proof will assume NOTHING about the scheme.)

The players are \( A_1, \ldots, A_5 \)
Example of Why Can’t Have Short Shares

Assume there is a (4, 5) Secret Sharing Scheme where Zelda shares a secret of length 7.
(This proof will assume NOTHING about the scheme.)
The players are $A_1, \ldots, A_5$
Before the protocol begins there are $2^7 = 128$ possibilities for the secret.
Example of Why Can’t Have Short Shares

Assume there is a (4, 5) Secret Sharing Scheme where Zelda shares a secret of length 7.

(This proof will assume NOTHING about the scheme.)
The players are $A_1, \ldots, A_5$

Before the protocol begins there are $2^7 = 128$ possibilities for the secret.

Assume that $A_5$ gets a share of length 6. We show that the scheme is NOT info-theoretic secure.
If $A_1, A_2, A_3, A_5$ got together they learn secret, since it’s a $(4, 5)$ scheme.
If $A_1, A_2, A_3, A_5$ got together they learn secret, since it’s a $(4, 5)$ scheme.

We show that $A_1, A_2, A_3$ can learn SOMETHING about the secret.
Example of Why Can’t Have Short Shares, Cont

If \(A_1, A_2, A_3, A_5\) got together they learn secret, since it’s a \((4, 5)\) scheme.

We show that \(A_1, A_2, A_3\) can learn SOMETHING about the secret.

\[\text{CAND} = \emptyset.\] \(\text{CAND}\) will be set of Candidates for \(s\).
Example of Why Can’t Have Short Shares, Cont

If $A_1, A_2, A_3, A_5$ got together they learn secret, since it’s a $(4, 5)$ scheme.

We show that $A_1, A_2, A_3$ can learn SOMETHING about the secret.

$CAND = \emptyset$. $CAND$ will be set of Candidates for $s$.

For $x \in \{0, 1\}^6$ (go through ALL shares $A_5$ could have)
If $A_1, A_2, A_3, A_5$ got together they learn secret, since it’s a $(4, 5)$ scheme.

We show that $A_1, A_2, A_3$ can learn SOMETHING about the secret.

\[ CAND = \emptyset. \]  
\[ CAND \] will be set of Candidates for $s$.  

For $x \in \{0, 1\}^6$ (go through ALL shares $A_5$ could have)  

$A_1, A_2, A_3$ pretend $A_5$ has $x$ and deduce candidates secret $s'$
Example of Why Can’t Have Short Shares, Cont

If $A_1, A_2, A_3, A_5$ got together they learn secret, since it’s a $(4, 5)$ scheme.

We show that $A_1, A_2, A_3$ can learn SOMETHING about the secret.

$CAND = \emptyset$. $CAND$ will be set of Candidates for $s$.

For $x \in \{0, 1\}^6$ (go through ALL shares $A_5$ could have)

$A_1, A_2, A_3$ pretend $A_5$ has $x$ and deduce candidates secret $s'$

$CAND := CAND \cup \{s'\}$
If $A_1, A_2, A_3, A_5$ got together they learn secret, since it’s a $(4, 5)$ scheme.

We show that $A_1, A_2, A_3$ can learn SOMETHING about the secret.

$CAND = \emptyset$. $CAND$ will be set of Candidates for $s$.

For $x \in \{0,1\}^6$ (go through ALL shares $A_5$ could have)

$A_1, A_2, A_3$ pretend $A_5$ has $x$ and deduce candidates secret $s'$

$CAND := CAND \cup \{s'\}$

Secret is in $CAND$. $|CAND| = 2^6 < 2^7$. 
If $A_1, A_2, A_3, A_5$ got together they learn secret, since it’s a $(4, 5)$ scheme.

We show that $A_1, A_2, A_3$ can learn SOMETHING about the secret.

$CAND = \emptyset$. $CAND$ will be set of Candidates for $s$.

For $x \in \{0, 1\}^6$ (go through ALL shares $A_5$ could have)

$A_1, A_2, A_3$ pretend $A_5$ has $x$ and deduce candidates secret $s'$

$CAND := CAND \cup \{s'\}$

Secret is in $CAND$. $|CAND| = 2^6 < 2^7$.

So $A_1, A_2, A_3$ have **eliminated** many strings from being the secret $s$. 
If $A_1, A_2, A_3, A_5$ got together they learn secret, since it’s a $(4, 5)$ scheme.

We show that $A_1, A_2, A_3$ can learn SOMETHING about the secret.

$CAND = \emptyset$. \textit{CAND} will be set of Candidates for $s$.

For $x \in \{0, 1\}^6$ (go through ALL shares $A_5$ could have)

$A_1, A_2, A_3$ pretend $A_5$ has $x$ and deduce candidates secret $s'$

$CAND := CAND \cup \{s'\}$

Secret is in $CAND$. $|CAND| = 2^6 < 2^7$.

So $A_1, A_2, A_3$ have \textbf{eliminated} many strings from being the secret $s$.

That is INFORMATION!!!!
Are Shorter Shares Ever Possible?

If we demand info-security then everyone gets a share $\geq n$. What if we only demand comp-security? VOTE
Are Shorter Shares Ever Possible?

If we *demand* info-security then *everyone* gets a share $\geq n$. What if we only *demand* comp-security?

**VOTE**

1. Can get shares $< \beta n$ with a hardness assumption.
Are Shorter Shares Ever Possible?

If we demand info-security then everyone gets a share $\geq n$. What if we only demand comp-security?

**VOTE**

1. Can get shares $< \beta n$ with a hardness assumption.
2. Even with hardness assumption REQUIRES shares $\geq n$. 
Are Shorter Shares Ever Possible?

If we demand info-security then everyone gets a share \( \geq n \). What if we only demand comp-security?

**VOTE**

1. Can get shares \( < \beta n \) with a hardness assumption.
2. Even with hardness assumption REQUIRES shares \( \geq n \).

Can get shares \( < \beta n \) with a hardness assumption.
What Hardness Assumption?

What hardness assumption $\Rightarrow$ secret share with short shares?

There exists a computationally secure PRG.

Can we reduce this to assumptions from Number Theory?

Yes

1. Blum-Blum-Shub have a PRG that depends on Quadratic Residue being hard. QR is: Given a number $x$ and $N = pq$, determine if $x$ is a square mod $N$. Only way known to solve this is by factoring, though perhaps there is another way. So $\text{PRG} \leq \text{QR} \leq \text{FACTORING}$.

2. Blum-Micali have a PRG that depends on DL being hard. So $\text{PRG} \leq \text{DL}$.

3. Brown has a PRG based on not-easy-to-state assumptions.

All of these are slow in practice.

There are many fast PRG's that people think are secure.

We now return to Info-Theoretic Secret Sharing.
What Hardness Assumption?

What hardness assumption $\Rightarrow$ secret share with short shares?

There exists a computationally secure PRG.
What Hardness Assumption?

What hardness assumption $\Rightarrow$ secret share with short shares?

There exists a computationally secure PRG.

Can we reduce this to assumptions from Number Theory?

1. Blum-Blum-Shub have a PRG that depends on Quadratic Residue being hard. QR is: Given a number $x$ and $N = pq$, determine if $x$ is a square mod $N$. Only way known to solve this is by factoring, though perhaps there is another way. So PRG $\leq$ QR $\leq$ FACTORING.

2. Blum-Micali have a PRG that depends on DL being hard. So PRG $\leq$ DL.

3. Brown has a PRG based on not-easy-to-state assumptions. All of these are slow in practice.

There are many fast PRG's that people think are secure.

We now return to Info-Theoretic Secret Sharing.
What Hardness Assumption?

What hardness assumption $\Rightarrow$ secret share with short shares?

There exists a computationally secure PRG.

Can we reduce this to assumptions from Number Theory? Yes

1. Blum-Blum-Shub have a PRG that depends on Quadratic Residue being hard. QR is: Given a number $x$ and $N = pq$, determine if $x$ is a square mod $N$. Only way known to solve this is by factoring, though perhaps there is another way. So PRG $\leq$ QR $\leq$ FACTORING.

2. Blum-Micali have a PRG that depends on DL being hard. So PRG $\leq$ DL.

3. Brown has a PRG based on not-easy-to-state assumptions. All of these are slow in practice. There are many fast PRG's that people think are secure.

We now return to Info-Theoretic Secret Sharing.
What Hardness Assumption?

What hardness assumption $\Rightarrow$ secret share with short shares?

There exists a computationally secure PRG.

Can we reduce this to assumptions from Number Theory? Yes

1. **Blum-Blum-Shub** have PRG that depends on Quadratic Residue being hard. QR is: Given a number $x$ and $N = pq$, determine if $x$ is a square mod $N$. Only way known to solve this is by factoring, though perhaps there is another way. So

   \[ \text{PRG} \leq \text{QR} \leq \text{FACTORING}. \]
What Hardness Assumption?

What hardness assumption \( \Rightarrow \) secret share with short shares?

**There exists a computationally secure PRG.** Can we reduce this to assumptions from Number Theory? Yes

1. **Blum-Blum-Shub** have PRG that depends on Quadratic Residue being hard. QR is: Given a number \( x \) and \( N = pq \), determine if \( x \) is a square mod \( N \). Only way known to solve this is by factoring, though perhaps there is another way. So

   \[
   \text{PRG} \leq \text{QR} \leq \text{FACTORING}.
   \]

2. **Blum-Micali** have a PRG that depends on DL being hard. So

   \[
   \text{PRG} \leq \text{DL}.
   \]
What Hardness Assumption?

What hardness assumption ⇒ secret share with short shares?

There exists a computationally secure PRG.

Can we reduce this to assumptions from Number Theory? Yes

1. **Blum-Blum-Shub** have PRG that depends on Quadratic Residue being hard. QR is: Given a number $x$ and $N = pq$, determine if $x$ is a square mod $N$. Only way known to solve this is by factoring, though perhaps there is another way. So

   \[
   \text{PRG} \leq \text{QR} \leq \text{FACTORING}.
   \]

2. **Blum-Micali** have a PRG that depends on DL being hard. So

   \[
   \text{PRG} \leq \text{DL}.
   \]

3. **Brown** has a PRG based on not-easy-to-state assumptions.
What Hardness Assumption?

What hardness assumption $\Rightarrow$ secret share with short shares?

There exists a computationally secure PRG.
Can we reduce this to assumptions from Number Theory? Yes

1. **Blum-Blum-Shub** have PRG that depends on Quadratic Residue being hard. QR is: Given a number $x$ and $N = pq$, determine if $x$ is a square mod $N$. Only way known to solve this is by factoring, though perhaps there is another way. So

   \[
   \text{PRG} \leq \text{QR} \leq \text{FACTORING}.
   \]

2. **Blum-Micali** have a PRG that depends on DL being hard. So

   \[
   \text{PRG} \leq \text{DL}.
   \]

3. **Brown** has a PRG based on not-easy-to-state assumptions.
   All of these are slow in practice.
What Hardness Assumption?

What hardness assumption \( \Rightarrow \) secret share with short shares?

**There exists a computationally secure PRG.**
Can we reduce this to assumptions from Number Theory? **Yes**

1. **Blum-Blum-Shub** have PRG that depends on Quadratic Residue being hard. QR is: Given a number \( x \) and \( N = pq \), determine if \( x \) is a square mod \( N \). Only way known to solve this is by factoring, though perhaps there is another way. So

   \[
   \text{PRG} \leq \text{QR} \leq \text{FACTORING}.
   \]

2. **Blum-Micali** have a PRG that depends on DL being hard. So

   \[
   \text{PRG} \leq \text{DL}.
   \]

3. **Brown** has a PRG based on not-easy-to-state assumptions. All of these are slow in practice. There are many fast PRG’s that people **think** are secure.
What Hardness Assumption?

What hardness assumption ⇒ secret share with short shares?

There exists a computationally secure PRG.
Can we reduce this to assumptions from Number Theory? Yes

1. **Blum-Blum-Shub** have PRG that depends on Quadratic Residue being hard. QR is: Given a number $x$ and $N = pq$, determine if $x$ is a square mod $N$. Only way known to solve this is by factoring, though perhaps there is another way. So

   \[ \text{PRG} \leq \text{QR} \leq \text{FACTORING}. \]

2. **Blum-Micali** have a PRG that depends on DL being hard. So

   \[ \text{PRG} \leq \text{DL}. \]

3. **Brown** has a PRG based on not-easy-to-state assumptions.
All of these are slow in practice.
There are many fast PRG’s that people think are secure.
We now return to Info-Theoretic Secret Sharing.
Generalize The Problem

Our problem: Player $A_1, \ldots, A_m$, secret $s$. 

1. If $t$ of them get together they can find $s$.
2. If $t - 1$ of them get together they cannot find $s$.

That is not quite right. Why?

1. If $\geq t$ of them get together they can find $s$.
2. If $\leq t - 1$ of them get together they cannot find $s$.

We want to generalize and look at other subsets.

Example
1. If an even number of players get together can find $s$.
2. If an odd number of players get together can't find $s$.

Try to find a scheme for this secret sharing problem.

You've Been Punked!
$A_1, A_2$ CAN find $s$ but $A_1, A_2, A_3$ CANNOT. That's Stupid!
Generalize The Problem

Our problem: Player $A_1, \ldots, A_m$, secret $s$.

1. If $t$ of them get together they can find $s$. 

You've Been Punked!

$A_1, A_2$ CAN find $s$ but $A_1, A_2, A_3$ CANNOT. Thats Stupid!
Generalize The Problem

Our problem: Player $A_1, \ldots, A_m$, secret $s$.

1. If $t$ of them get together they can find $s$.
2. If $t - 1$ of them get together they cannot find $s$.

That is not quite right. Why?

Example
1. If an even number of players get together can find $s$.
2. If an odd number of players get together cannot find $s$.

Try to find a scheme for this secret sharing problem.

You've Been Punked!
$A_1, A_2$ CAN find $s$ but $A_1, A_2, A_3$ CANNOT. Thats Stupid!
Generalize The Problem

Our problem: Player $A_1, \ldots, A_m$, secret $s$.

1. If $t$ of them get together they can find $s$.
2. If $t - 1$ of them get together they cannot find $s$.

That is not quite right. Why?

1. If $\geq t$ of them get together they can find $s$. 

You've Been Punked!

$A_1, A_2$ CAN find $s$ but $A_1, A_2, A_3$ CANNOT. Thats Stupid!
Generalize The Problem

Our problem: Player $A_1, \ldots, A_m$, secret $s$.

1. If $t$ of them get together they can find $s$.
2. If $t - 1$ of them get together they cannot find $s$.

That is not quite right. Why?

1. If $\geq t$ of them get together they can find $s$.
2. If $\leq t - 1$ of them get together they cannot find $s$. 

You've Been Punked!

$A_1, A_2$ CAN find $s$ but $A_1, A_2, A_3$ CANNOT. Thats Stupid!
Generalize The Problem

Our problem: Player $A_1, \ldots, A_m$, secret $s$.

1. If $t$ of them get together they can find $s$.
2. If $t - 1$ of them get together they cannot find $s$.

That is not quite right. Why?

1. If $\geq t$ of them get together they can find $s$.
2. If $\leq t - 1$ of them get together they cannot find $s$.

We want to generalize and look at other subsets.

Example
Generalize The Problem

Our problem: Player \(A_1, \ldots, A_m\), secret \(s\).

1. If \(t\) of them get together they can find \(s\).
2. If \(t - 1\) of them get together they cannot find \(s\).

That is not quite right. Why?

1. If \(\geq t\) of them get together they can find \(s\).
2. If \(\leq t - 1\) of them get together they cannot find \(s\).

We want to generalize and look at other subsets.

Example

1. If an even number of players get together can find \(s\).

You've Been Punked!

\(A_1, A_2\) CAN find \(s\) but \(A_1, A_2, A_3\) CANNOT. Thats Stupid!
Generalize The Problem

Our problem: Player $A_1, \ldots, A_m$, secret $s$.

1. If $t$ of them get together they can find $s$.
2. If $t - 1$ of them get together they cannot find $s$.

That is not quite right. Why?

1. If $\geq t$ of them get together they can find $s$.
2. If $\leq t - 1$ of them get together they cannot find $s$.

We want to generalize and look at other subsets.

Example

1. If an even number of players get together can find $s$.
2. If an odd number of players get together can’t find $s$. 
Generalize The Problem

Our problem: Player $A_1, \ldots, A_m$, secret $s$.

1. If $t$ of them get together they can find $s$.
2. If $t - 1$ of them get together they cannot find $s$.

That is not quite right. Why?

1. If $\geq t$ of them get together they can find $s$.
2. If $\leq t - 1$ of them get together they cannot find $s$.

We want to generalize and look at other subsets.

Example

1. If an even number of players get together can find $s$.
2. If an odd number of players get together can’t find $s$.

Try to find a scheme for this secret sharing problem.
Generalize The Problem

Our problem: Player $A_1, \ldots, A_m$, secret $s$.

1. If $t$ of them get together they can find $s$.
2. If $t - 1$ of them get together they cannot find $s$.

That is not quite right. Why?

1. If $\geq t$ of them get together they can find $s$.
2. If $\leq t - 1$ of them get together they cannot find $s$.

We want to generalize and look at other subsets.

Example

1. If an even number of players get together can find $s$.
2. If an odd number of players get together can’t find $s$.

Try to find a scheme for this secret sharing problem.

You’ve Been Punked!

$A_1, A_2$ CAN find $s$ but $A_1, A_2, A_3$ CANNOT. That’s Stupid!
What is it about Threshold?

1. If \( \geq t \) of them get together they can find out secret.
2. If \( \leq t - 1 \) of them get together they cannot find out secret.

Let's rephrase that so we can generalize:

\( X \) is the set of all subsets of \{\( A_1, \ldots, A_m \)\} with \( \geq t \) players.

1. If \( Y \in X \) then the players in \( Y \) can find \( s \).
2. If \( Y \not\in X \) then the players in \( Y \) cannot find \( s \).

This question makes sense. What is it about \( X \) that makes it make sense?

\( X \) is closed under superset: If \( Y \in X \) and \( Y \subseteq Z \) then \( Z \in X \).
What is it about Threshold?

1. If $\geq t$ of them get together they can find out secret.
What is it about Threshold?

1. If $\geq t$ of them get together they can find out secret.
2. If $\leq t - 1$ of them get together they cannot find out secret.

Let’s rephrase that so we can generalize:

$X$ is the set of all subsets of $\{A_1, \ldots, A_m\}$ with $\geq t$ players.

1. If $Y \in X$ then the players in $Y$ can find $s$.
2. If $Y \not\in X$ then the players in $Y$ cannot find $s$.

This question makes sense. What is it about $X$ that makes it make sense?

$X$ is closed under superset: If $Y \in X$ and $Y \subseteq Z$ then $Z \in X$. 
What is it about Threshold?

1. If $\geq t$ of them get together they can find out secret.
2. If $\leq t - 1$ of them get together they cannot find out secret.

Let’s rephrase that so we can generalize:
$X$ is the set of all subsets of $\{A_1, \ldots, A_m\}$ with $\geq t$ players.
What is it about Threshold?

1. If $\geq t$ of them get together they can find out secret.
2. If $\leq t - 1$ of them get together they cannot find out secret.

Let's rephrase that so we can generalize:

$\mathcal{X}$ is the set of all subsets of $\{A_1, \ldots, A_m\}$ with $\geq t$ players.

1. If $Y \in \mathcal{X}$ then the players in $Y$ can find $s$.
What is it about Threshold?

1. If $\geq t$ of them get together they can find out secret.
2. If $\leq t - 1$ of them get together they cannot find out secret.

Let's rephrase that so we can generalize:

$X$ is the set of all subsets of $\{A_1, \ldots, A_m\}$ with $\geq t$ players.

1. If $Y \in X$ then the players in $Y$ can find $s$.
2. If $Y \notin X$ then the players in $Y$ cannot find $s$.

This question makes sense. What is it about $X$ that makes it make sense?
What is it about Threshold?

1. If $\geq t$ of them get together they can find out secret.
2. If $\leq t - 1$ of them get together they cannot find out secret.

Let’s rephrase that so we can generalize:

$\mathcal{X}$ is the set of all subsets of $\{A_1, \ldots, A_m\}$ with $\geq t$ players.

1. If $Y \in \mathcal{X}$ then the players in $Y$ can find $s$.
2. If $Y \notin \mathcal{X}$ then the players in $Y$ cannot find $s$.

This question makes sense. What is it about $\mathcal{X}$ that makes it make sense?

$\mathcal{X}$ is closed under superset:

If $Y \in \mathcal{X}$ and $Y \subseteq Z$ then $Z \in \mathcal{X}$.
Access Structures

**Def** An **Access Structure** is a set of subset of \( \{A_1, \ldots, A_m\} \) closed under superset.

---

1. If \( X \) is an access structure then the following questions make sense:
   1.1 Is there a secret sharing scheme for \( X \)?
   1.2 Is there a secret sharing scheme for \( X \) where all shares are the same size as the secret?

2. \((t, m)\)-Threshold is an access structure. The poly method gives a secret sharing scheme where all the shares are the same length as the secret.

**Def** A secret sharing scheme is ideal if all shares come from the same domain as the secret.
Access Structures

**Def** An **Access Structure** is a set of subset of \( \{A_1, \ldots, A_m\} \) closed under superset.

1. If \( \mathcal{X} \) is an access structure then the following questions make sense:

- Is there a secret sharing scheme for \( \mathcal{X} \)?
- Is there a secret sharing scheme for \( \mathcal{X} \) where all shares are the same size as the secret?

\( (t, m) \)-Threshold is an Access structure. The poly method gives a Secret Sharing scheme where all the shares are the same length as the secret.

**Def** A secret sharing scheme is **ideal** if all shares come from the same domain as the secret.
**Access Structures**

**Def** An **Access Structure** is a set of subset of \( \{A_1, \ldots, A_m\} \) closed under superset.

1. If \( \mathcal{X} \) is an access structure then the following questions make sense:
   1.1 Is there a secret sharing scheme for \( \mathcal{X} \)?

2. \((t, m)\)-Threshold is an Access structure. The poly method gives a Secret Sharing scheme where all the shares are the same length as the secret.

**Def** A secret sharing scheme is **ideal** if all shares come from the same domain as the secret.
Def An **Access Structure** is a set of subset of \( \{A_1, \ldots, A_m\} \) closed under superset.

1. If \( \mathcal{A} \) is an access structure then the following questions make sense:
   1.1 Is there a secret sharing scheme for \( \mathcal{A} \)?
   1.2 Is there a secret sharing scheme for \( \mathcal{A} \) where all shares are the same size as the secret?
**Def** An **Access Structure** is a set of subset of \( \{A_1, \ldots, A_m\} \) closed under superset.

1. If \( \mathcal{X} \) is an access structure then the following questions make sense:
   1.1 Is there a secret sharing scheme for \( \mathcal{X} \)?
   1.2 Is there a secret sharing scheme for \( \mathcal{X} \) where all shares are the same size as the secret?

2. \((t, m)\)-Threshold is an Access structure. The poly method gives a Secret Sharing scheme where all the shares are the same length as the secret.
**Access Structures**

**Def** An **Access Structure** is a set of subset of \( \{A_1, \ldots, A_m\} \) closed under superset.

1. If \( \mathcal{X} \) is an access structure then the following questions make sense:
   1.1 Is there a secret sharing scheme for \( \mathcal{X} \)?
   1.2 Is there a secret sharing scheme for \( \mathcal{X} \) where all shares are the same size as the secret?

2. \((t, m)\)-Threshold is an Access structure. The poly method gives a Secret Sharing scheme where all the shares are the same length as the secret.

**Def** A secret sharing scheme is **ideal** if all shares come from the same domain as the secret.
Want that a group can find the secret if either it has

1. at least 2 of $A_1, A_2, A_3$, OR
2. at least 4 of $B_1, B_2, B_3, B_4, B_5, B_6, B_7$. 

How can Zelda do this?

1. Zelda does (2,3) secret sharing with $A_1, A_2, A_3$.
2. Zelda does (4,7) secret sharing with $B_1, B_2, B_3, B_4, B_5, B_6, B_7$.

To generalize this we need a better notation.
DISJOINT-OR of AND: Ideal Sec Sharing Protocol

Want that a group can find the secret if either it has

1. at least 2 of $A_1, A_2, A_3$, OR

To generalize this we need a better notation.
DISJOINT-OR of AND: Ideal Sec Sharing Protocol

Want that a group can find the secret if either it has

1. at least 2 of $A_1, A_2, A_3$, OR
2. at least 4 of $B_1, B_2, B_3, B_4, B_5, B_6, B_7$.

How can Zelda do this?
Want that a group can find the secret if either it has

1. at least 2 of $A_1, A_2, A_3$, OR
2. at least 4 of $B_1, B_2, B_3, B_4, B_5, B_6, B_7$.

How can Zelda do this?

1. Zelda does $(2, 3)$ secret sharing with $A_1, A_2, A_3$. 
DISJOINT-OR of AND: Ideal Sec Sharing Protocol

Want that a group can find the secret if either it has

1. at least 2 of $A_1, A_2, A_3$, OR
2. at least 4 of $B_1, B_2, B_3, B_4, B_5, B_6, B_7$.

How can Zelda do this?

1. Zelda does $(2, 3)$ secret sharing with $A_1, A_2, A_3$.
2. Zelda does $(4, 7)$ secret sharing with $B_1, B_2, B_3, B_4, B_5, B_6, B_7$. 

To generalize this we need a better notation.
DISJOINT-OR of AND: Ideal Sec Sharing Protocol

Want that a group can find the secret if either it has

1. at least 2 of \( A_1, A_2, A_3 \), OR
2. at least 4 of \( B_1, B_2, B_3, B_4, B_5, B_6, B_7 \).

How can Zelda do this?

1. Zelda does \((2, 3)\) secret sharing with \( A_1, A_2, A_3 \).
2. Zelda does \((4, 7)\) secret sharing with \( B_1, B_2, B_3, B_4, B_5, B_6, B_7 \).

To generalize this we need a better notation.
Notation for Threshold

Let $TH_A(t, m)$ be the Boolean Formula that represents at least $t$ out of $m$ of the $A_i$’s.
Notation for Threshold

Let $TH_A(t, m)$ be the Boolean Formula that represents at least $t$ out of $m$ of the $A_i$’s.

**Example** $TH_A(2, 4)$ is
At least 2 of $A_1, A_2, A_3, A_4$. 

$TH_A(t_1, m_1) \lor TH_B(t_2, m_2)$ means that:
1. $\geq t_1$ of $A_1, \ldots, A_{m_1}$ can learn the secret.
2. $\geq t_2$ of $B_1, \ldots, B_{m_2}$ can learn the secret.
3. No other group can learn the secret (e.g., $A_1, A_2, B_1$ cannot).
Let $TH_A(t, m)$ be the Boolean Formula that represents at least $t$ out of $m$ of the $A_i$'s.

**Example** $TH_A(2, 4)$ is
At least 2 of $A_1, A_2, A_3, A_4$.

**Example** $TH_B(3, 6)$ is
At least 3 of $B_1, \ldots, B_6$. 

**Note** $TH_A(t, m)$ has ideal secret sharing.
Notation for Threshold

Let $TH_A(t, m)$ be the Boolean Formula that represents at least $t$ out of $m$ of the $A_i$'s.

**Example** $TH_A(2, 4)$ is
At least 2 of $A_1, A_2, A_3, A_4$.

**Example** $TH_B(3, 6)$ is
At least 3 of $B_1, \ldots, B_6$.

**Note** $TH_A(t, m)$ has ideal secret sharing.
Notation for Threshold

Let $TH_A(t, m)$ be the Boolean Formula that represents at least $t$ out of $m$ of the $A_i$'s.

**Example** $TH_A(2, 4)$ is
At least 2 of $A_1, A_2, A_3, A_4$.

**Example** $TH_B(3, 6)$ is
At least 3 of $B_1, \ldots, B_6$.

**Note** $TH_A(t, m)$ has ideal secret sharing.

**Notation** $TH_A(t_1, m_1) \lor TH_B(t_2, m_2)$ means that:
Notation for Threshold

Let $\text{TH}_A(t, m)$ be the Boolean Formula that represents at least $t$ out of $m$ of the $A_i$'s.

**Example** $\text{TH}_A(2, 4)$ is
At least 2 of $A_1, A_2, A_3, A_4$.

**Example** $\text{TH}_B(3, 6)$ is
At least 3 of $B_1, \ldots, B_6$.

**Note** $\text{TH}_A(t, m)$ has ideal secret sharing.

**Notation** $\text{TH}_A(t_1, m_1) \lor \text{TH}_B(t_2, m_2)$ means that:

1. $\geq t_1$ $A_1, \ldots, A_{m_1}$ can learn the secret.
**Notation for Threshold**

Let $TH_A(t, m)$ be the Boolean Formula that represents at least $t$ out of $m$ of the $A_i$'s.

**Example** $TH_A(2, 4)$ is
At least 2 of $A_1, A_2, A_3, A_4$.

**Example** $TH_B(3, 6)$ is
At least 3 of $B_1, \ldots, B_6$.

**Note** $TH_A(t, m)$ has ideal secret sharing.

**Notation** $TH_A(t_1, m_1) \lor TH_B(t_2, m_2)$ means that:

1. $\geq t_1$ $A_1, \ldots, A_{m_1}$ can learn the secret.
2. $\geq t_2$ $B_1, \ldots, B_{m_2}$ can learn the secret.
Notation for Threshold

Let $TH_A(t, m)$ be the Boolean Formula that represents at least $t$ out of $m$ of the $A_i$'s.

**Example** $TH_A(2, 4)$ is
At least 2 of $A_1, A_2, A_3, A_4$.

**Example** $TH_B(3, 6)$ is
At least 3 of $B_1, \ldots, B_6$.

**Note** $TH_A(t, m)$ has ideal secret sharing.

**Notation** $TH_A(t_1, m_1) \lor TH_B(t_2, m_2)$ means that:

1. $\geq t_1$ $A_1, \ldots, A_{m_1}$ can learn the secret.
2. $\geq t_2$ $B_1, \ldots, B_{m_2}$ can learn the secret.
3. No other group can learn the secret (e.g., $A_1, A_2, B_1$ cannot)
Disjoint OR of $TH_A(t, m)$’s: Ideal Sec Sharing

There is Ideal Secret Sharing for $TH_A(t_1, m_1) \lor \cdots \lor TH_Z(t_{26}, m_{26})$
Disjoint OR of $TH_A(t, m)$’s: Ideal Sec Sharing

There is Ideal Secret Sharing for $TH_A(t_1, m_1) \lor \cdots \lor TH_Z(t_{26}, m_{26})$

1. Zelda and the $A_1, \ldots, A_{m_1}$ do $(t_1, m_1)$ secret sharing.
Disjoint OR of $TH_A(t, m)$’s: Ideal Sec Sharing

There is Ideal Secret Sharing for $TH_A(t_1, m_1) \lor \cdots \lor TH_Z(t_{26}, m_{26})$

1. Zelda and the $A_1, \ldots, A_{m_1}$ do $(t_1, m_1)$ secret sharing.

2. \ldots
Disjoint OR of $TH_A(t, m)$’s: Ideal Sec Sharing

There is Ideal Secret Sharing for $TH_A(t_1, m_1) \lor \cdots \lor TH_Z(t_{26}, m_{26})$

1. Zelda and the $A_1, \ldots, A_{m_1}$ do $(t_1, m_1)$ secret sharing.

2.  

3. Zelda and the $Z_1, \ldots, Z_{m_{26}}$ do $(t_{26}, m_{26})$ secret sharing.

Note We now have a large set of non-threshold scenarios that have ideal secret sharing.
AND of $TH_A(t, m)$s: An Example

We want that if $\geq 2$ of $A_1, A_2, A_3, A_4$ AND $\geq 4$ of $B_1, \ldots, B_7$ get together than they can learn the secret, but no other groups can. Think about it.
AND of $TH_A(t, m)$s: An Example

We want that if $\geq 2$ of $A_1, A_2, A_3, A_4$ AND $\geq 4$ of $B_1, \ldots, B_7$ get together than they can learn the secret, but no other groups can. Think about it.

1. Zelda has secret $s$, $|s| = n$. 
AND of $TH_A(t, m)$s: An Example

We want that if $\geq 2$ of $A_1, A_2, A_3, A_4$ AND $\geq 4$ of $B_1, \ldots, B_7$ get together than they can learn the secret, but no other groups can. Think about it.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r \in \{0, 1\}^n$. 
AND of $TH_A(t, m)$s: An Example

We want that if $\geq 2$ of $A_1, A_2, A_3, A_4$ AND $\geq 4$ of $B_1, \ldots, B_7$ get together than they can learn the secret, but no other groups can. Think about it.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r \in \{0, 1\}^n$.
3. Zelda does (2, 4) secret sharing of $r$ with $A_1, A_2, A_3, A_4$. 
AND of $TH_A(t, m)$s: An Example

We want that if $\geq 2$ of $A_1, A_2, A_3, A_4$ AND $\geq 4$ of $B_1, \ldots, B_7$ get together than they can learn the secret, but no other groups can. Think about it.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r \in \{0, 1\}^n$.
3. Zelda does $(2, 4)$ secret sharing of $r$ with $A_1, A_2, A_3, A_4$.
4. Zelda does $(4, 7)$ secret sharing of $r \oplus s$ with $B_1, \ldots, B_7$. 
AND of $TH_A(t, m)$s: An Example

We want that if $\geq 2$ of $A_1, A_2, A_3, A_4$ AND $\geq 4$ of $B_1, \ldots, B_7$ get together than they can learn the secret, but no other groups can. Think about it.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r \in \{0, 1\}^n$.
3. Zelda does $(2, 4)$ secret sharing of $r$ with $A_1, A_2, A_3, A_4$.
4. Zelda does $(4, 7)$ secret sharing of $r \oplus s$ with $B_1, \ldots, B_7$.
5. If $\geq 2$ of $A_i$’s get together they can find $r$. 
AND of $TH_A(t, m)$s: An Example

We want that if $\geq 2$ of $A_1, A_2, A_3, A_4$ AND $\geq 4$ of $B_1, \ldots, B_7$ get together than they can learn the secret, but no other groups can. Think about it.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r \in \{0, 1\}^n$.
3. Zelda does $(2,4)$ secret sharing of $r$ with $A_1, A_2, A_3, A_4$.
4. Zelda does $(4,7)$ secret sharing of $r \oplus s$ with $B_1, \ldots, B_7$.
5. If $\geq 2$ of $A_i$’s get together they can find $r$.
   If $\geq 4$ of $B_i$’s get together they can find $r \oplus s$. 
AND of $TH_A(t, m)$s: An Example

We want that if $\geq 2$ of $A_1, A_2, A_3, A_4$ AND $\geq 4$ of $B_1, \ldots, B_7$ get together than they can learn the secret, but no other groups can.

Think about it.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r \in \{0, 1\}^n$.
3. Zelda does $(2, 4)$ secret sharing of $r$ with $A_1, A_2, A_3, A_4$.
4. Zelda does $(4, 7)$ secret sharing of $r \oplus s$ with $B_1, \ldots, B_7$.
5. If $\geq 2$ of $A_i$’s get together they can find $r$.
   If $\geq 4$ of $B_i$’s get together they can find $r \oplus s$.
   So if they all get together they can find

   $$ r \oplus (r \oplus s) = s $$
AND of $TH_A(t, m)$s: General

$TH_A(t_1, m_1) \land \cdots \land TH_Z(t_{26}, m_{26})$ can do secret sharing.
AND of $TH_A(t, m)$s: General

$TH_A(t_1, m_1) \land \cdots \land TH_Z(t_{26}, m_{26})$ can do secret sharing.

1. Zelda has secret $s$, $|s| = n$. 

2. Zelda generates random $r_1, \ldots, r_{25} \in \{0, 1\}^n$.

3. Zelda does $\langle t_1, m_1 \rangle$ secret sharing of $r_1$ with $A_i$'s.

4. ...

5. Zelda does $\langle t_{25}, m_{25} \rangle$ secret sharing of $r_{25}$ with $Y_i$'s.

6. Zelda does $\langle t_{26}, m_{26} \rangle$ secret sharing of $r_1 \oplus \cdots \oplus r_{25} \oplus s$ with $Z_i$'s.

7. If $\geq t_1$ of $A_i$'s get together they can find $r_1$. If $\geq t_2$ of $B_i$'s get together they can find $r_2$. \ldots If $\geq t_{25}$ of $Y_i$'s get together they can find $r_{25}$. If $\geq t_{26}$ of $Z_i$'s get together they can find $r_1 \oplus \cdots \oplus r_{25} \oplus (r_1 \oplus \cdots \oplus r_{25} \oplus s) = s$. So if they call get together they can find $r_1 \oplus \cdots \oplus r_{25} \oplus (r_1 \oplus \cdots \oplus r_{25} \oplus s)$.
AND of $TH_A(t, m)$s: General

$TH_A(t_1, m_1) \land \cdots \land TH_Z(t_{26}, m_{26})$ can do secret sharing.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r_1, \ldots, r_{25} \in \{0, 1\}^n$. 
AND of $TH_A(t, m)$s: General

$TH_A(t_1, m_1) \land \cdots \land TH_Z(t_{26}, m_{26})$ can do secret sharing.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r_1, \ldots, r_{25} \in \{0, 1\}^n$.
3. Zelda does $(t_1, m_1)$ secret sharing of $r_1$ with $A_i$'s.
AND of $TH_A(t, m)$s: General

$TH_A(t_1, m_1) \land \cdots \land TH_Z(t_{26}, m_{26})$ can do secret sharing.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r_1, \ldots, r_{25} \in \{0, 1\}^n$.
3. Zelda does $(t_1, m_1)$ secret sharing of $r_1$ with $A_i$'s.

4. ...
AND of $TH_A(t, m)$s: General

$TH_A(t_1, m_1) \land \cdots \land TH_Z(t_{26}, m_{26})$ can do secret sharing.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r_1, \ldots, r_{25} \in \{0, 1\}^n$.
3. Zelda does $(t_1, m_1)$ secret sharing of $r_1$ with $A_i$'s.

4. : 
5. Zelda does $(t_{25}, m_{25})$ secret sharing of $r_{25}$ with $Y_i$'s.
AND of $TH_A(t, m)$s: General

$TH_A(t_1, m_1) \land \cdots \land TH_Z(t_{26}, m_{26})$ can do secret sharing.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r_1, \ldots, r_{25} \in \{0, 1\}^n$.
3. Zelda does $(t_1, m_1)$ secret sharing of $r_1$ with $A_i$'s.
4. $\vdots$
5. Zelda does $(t_{25}, m_{25})$ secret sharing of $r_{25}$ with $Y_i$'s.
6. Zelda does $(t_{26}, m_{26})$ secret sharing of $r_1 \oplus \cdots \oplus r_{25} \oplus s$ with $Z_i$'s.
AND of $TH_A(t, m)$s: General

$TH_A(t_1, m_1) \land \cdots \land TH_Z(t_{26}, m_{26})$ can do secret sharing.

1. Zelda has secret $s$, $|s| = n$.
2. Zelda generates random $r_1, \ldots, r_{25} \in \{0, 1\}^n$.
3. Zelda does $(t_1, m_1)$ secret sharing of $r_1$ with $A_i$’s.
4. :
5. Zelda does $(t_{25}, m_{25})$ secret sharing of $r_{25}$ with $Y_i$’s.
6. Zelda does $(t_{26}, m_{26})$ secret sharing of $r_1 \oplus \cdots \oplus r_{25} \oplus s$ with $Z_i$’s.
7. If $\geq t_1$ of $A_i$’s get together they can find $r_1$. If $\geq t_2$ of $B_i$’s get together they can find $r_2$. \cdots If $\geq t_{25}$ of $Y_i$’s get together they can find $r_{25}$. If $\geq t_{26}$ of $Z_i$’s get together they can find $r_1 \oplus \cdots \oplus r_{25} \oplus s$. So if they call get together they can find

$$r_1 \oplus \cdots \oplus r_{25} \oplus (r_1 \oplus \cdots \oplus r_{25} \oplus s) = s$$
**Definition** A **monotone formula** is a Boolean formula with no NOT signs.

If you put together what we did with $TH$ and use induction you can prove the following:

**Theorem** Let $X_1, \ldots, X_N$ each be a threshold $TH_A(t, m)$ but all using DIFFERENT players.

Let $F(X_1, \ldots, X_N)$ be a monotone Boolean formula where each $X_i$ appears only once. Then Zelda can do ideal secret sharing where only sets that satisfy $F(X_1, \ldots, X_N)$ can learn the secret.
**General Theorem**

**Definition** A **monotone formula** is a Boolean formula with no NOT signs.

If you put together what we did with $TH$ and use induction you can prove the following:

**Theorem** Let $X_1, \ldots, X_N$ each be a threshold $TH_A(t, m)$ but all using DIFFERENT players.

Let $F(X_1, \ldots, X_N)$ be a monotone Boolean formula where each $X_i$ appears only once. Then Zelda can do ideal secret sharing where only sets that satisfy $F(X_1, \ldots, X_N)$ can learn the secret.

Routine proof left to the reader. Might be on a HW or the Final.
Access Structures That Admit Ideal Sec. Sharing

1. Threshold Secret sharing: if $t$ or more get together. We did this.

2. Monotone Boolean Formulas of Threshold where every set of players appears only once. We did this.

3. Monotone Span Programs (Omitted – it's a Matrix Thing) We did not do this and will not.
Access Structures That Admit Ideal Sec. Sharing

1. Threshold Secret sharing: if $t$ or more get together. We did this.
Access Structures That Admit Ideal Sec. Sharing

1. Threshold Secret sharing: if $t$ or more get together. We did this.

2. Monotone Boolean Formulas of Threshold where every set of players appears only once. We did this.
1. Threshold Secret sharing: if $t$ or more get together. **We did this.**

2. Monotone Boolean Formulas of Threshold where every set of players appears only once. **We did this.**

3. Monotone Span Programs (Omitted – it’s a Matrix Thing) **We did not do this and will not.**
Non-Ideal Access Structures

1. \((A_1 \land A_2) \lor (A_2 \land A_3) \lor (A_3 \land A_4)\)

2. \((A_1 \land A_2 \land A_3) \lor (A_1 \land A_4) \lor (A_2 \land A_4) \lor (A_3 \land A_4)\) (Captain and Crew)

   \(A_1, A_2, A_3\) is the crew, and \(A_4\) is the captain.

   Entire crew, or captain and 1 crew, can get \(s\).

3. \((A_1 \land A_2 \land A_3) \lor (A_1 \land A_4) \lor (A_2 \land A_4) \lor (A_3 \land A_4)\) (Captain and Rival)

   \(A_1, A_2, A_3\) is the crew, \(A_3\) is a rival, \(A_4\) is the captain.

   Entire crew, or captain and 1 crew who is NOT rival, can get \(s\).

4. Any access structure that contains any of the above.

In all of the above, all get a share of size 1.

5. \(n\) and this is optimal.

The proof of this is difficult and hence omitted.
Non-Ideal Access Structures

1. \((A_1 \land A_2) \lor (A_2 \land A_3) \lor (A_3 \land A_4)\)
1. \((A_1 \land A_2) \lor (A_2 \land A_3) \lor (A_3 \land A_4)\)

2. \((A_1 \land A_2 \land A_3) \lor (A_1 \land A_4) \lor (A_2 \land A_4) \lor (A_3 \land A_4)\) (Captain and Crew) \(A_1, A_2, A_3\) is the crew, and \(A_4\) is the captain. Entire crew, or captain and 1 crew, can get \(s\).
Non-Ideal Access Structures

1. \((A_1 \land A_2) \lor (A_2 \land A_3) \lor (A_3 \land A_4)\)

2. \((A_1 \land A_2 \land A_3) \lor (A_1 \land A_4) \lor (A_2 \land A_4) \lor (A_3 \land A_4)\)  \textbf{(Captain and Crew)}  
   \(A_1, A_2, A_3\) is the crew, and \(A_4\) is the captain. 
   Entire crew, or captain and 1 crew, can get \(s\).

3. \((A_1 \land A_2 \land A_3) \lor (A_1 \land A_4) \lor (A_2 \land A_4)\)  \textbf{(Captain and Rival)}  
   \(A_1, A_2, A_3\) is the crew, \(A_3\) is a rival, \(A_4\) is the captain. 
   Entire crew, or captain and 1 crew who is NOT rival, can get \(s\).
Non-Ideal Access Structures

1. \((A_1 \land A_2) \lor (A_2 \land A_3) \lor (A_3 \land A_4)\)
2. \((A_1 \land A_2 \land A_3) \lor (A_1 \land A_4) \lor (A_2 \land A_4) \lor (A_3 \land A_4)\) (Captain and Crew) \(A_1, A_2, A_3\) is the crew, and \(A_4\) is the captain. Entire crew, or captain and 1 crew, can get \(s\).

3. \((A_1 \land A_2 \land A_3) \lor (A_1 \land A_4) \lor (A_2 \land A_4)\) (Captain and Rival) \(A_1, A_2, A_3\) is the crew, \(A_3\) is a rival, \(A_4\) is the captain. Entire crew, or captain and 1 crew who is NOT rival, can get \(s\).

4. Any access structure that contains any of the above.

In all of the above, all get a share of size \(1.5n\) and this is optimal. The proof of this is difficult and hence omitted.
Can Zelda Always Secret Share?

Zelda wants to share secret such that:

1. If $A_1, A_2, A_3$ get together they can get secret.
2. If $A_1, A_4$ get together they can get secret.
3. If $A_2, A_4$ get together they can get secret.

By the last slide we know that CANNOT do ideal secret sharing.
Can Zelda Always Secret Share?

Zelda wants to share secret such that:

1. If $A_1, A_2, A_3$ get together they can get secret.
2. If $A_1, A_4$ get together they can get secret.
3. If $A_2, A_4$ get together they can get secret.

By the last slide we know that CANNOT do ideal secret sharing. Can Zelda do secret sharing? VOTE Yes or NO.
Can Zelda Always Secret Share?

Zelda wants to share secret such that:

1. If $A_1, A_2, A_3$ get together they can get secret.
2. If $A_1, A_4$ get together they can get secret.
3. If $A_2, A_4$ get together they can get secret.

By the last slide we know that CANNOT do ideal secret sharing.

Can Zelda do secret sharing? VOTE Yes or NO.

YES- but do not use polynomials, use the random string method.
Open Question

Known
Open Question

**Known**

1. Using Random String Method every Access Structure with $m$ people has a secret sharing scheme with $2^m n$ sized shares.
Open Question

Known

1. Using Random String Method every Access Structure with $m$ people has a secret sharing scheme with $2^m n$ sized shares.
2. Threshold and many other Access Structures can do secret sharing with $n$-sized shares.
Open Question

Known

1. Using Random String Method every Access Structure with $m$ people has a secret sharing scheme with $2^mn$ sized shares.
2. Threshold and many other Access Structures can do secret sharing with $n$-sized shares.
Open Question

Known
1. Using Random String Method every Access Structure with $m$ people has a secret sharing scheme with $2^m n$ sized shares.
2. Threshold and many other Access Structures can do secret sharing with $n$-sized shares.

Open Determine for every access structure the functions $f(n)$ and $g(n)$ such that
Open Question

Known

1. Using Random String Method every Access Structure with $m$ people has a secret sharing scheme with $2^m n$ sized shares.
2. Threshold and many other Access Structures can do secret sharing with $n$-sized shares.

Open

Determine for every access structure the functions $f(n)$ and $g(n)$ such that

1. (∃) Scheme where everyone gets $\leq f(n)$ sized share.
Open Question

Known

1. Using Random String Method every Access Structure with \( m \) people has a secret sharing scheme with \( 2^m n \) sized shares.
2. Threshold and many other Access Structures can do secret sharing with \( n \)-sized shares.

Open Determine for every access structure the functions \( f(n) \) and \( g(n) \) such that

1. \( \exists \) Scheme where everyone gets \( \leq f(n) \) sized share.
2. \( \forall \) Scheme someone gets \( \geq g(n) \) sized share.
Open Question

**Known**

1. Using Random String Method every Access Structure with $m$ people has a secret sharing scheme with $2^m n$ sized shares.

2. Threshold and many other Access Structures can do secret sharing with $n$-sized shares.


**Open** Determine for every access structure the functions $f(n)$ and $g(n)$ such that

1. (∃) Scheme where everyone gets $\leq f(n)$ sized share.

2. (∀) Scheme someone gets $\geq g(n)$ sized share.

3. $f(n)$ and $g(n)$ are close together.