Threshold Secret Sharing: Length of Shares
Length of Shares

$s = 1111$, length 4. This is 15 in base 10, so we go to smallest prime $> 15$, namely 17.

We use $p = 17$. $s = 1111$, $|s| = 4$.

Elements of $\mathbb{Z}_{17}$ are represented by strings of length 5

1. Everyone gets at least one share.
2. All shares length 5, even though $s$ is length 4.

Can we always get length $n$? Length $n + 1$?
Length of Shares

If $|s| = n$ want prime $p$ with $2^n < p$.

**Known**: For all $n$ there exists prime $p$ with $2^n \leq p \leq 2^{n+1}$.

**Upshot**: The secret is length $n$, the shares are of length $n + 1$.

**Good News**: Every $A_i$ gets ONE share.

**Bad News**: That share is of length $n + 1$, not $n$.

**VOTE**: Can Zelda do threshold secret sh. where every student gets ONE share of length $n$?

1. YES
2. NO
3. YES given some hardness assumption
4. UNKNOWN TO SCIENCE
Length of Shares

If $|s| = n$ want prime $p$ with $2^n < p$.

**Known:** For all $n$ there exists prime $p$ with $2^n \leq p \leq 2^{n+1}$.

**Upshot:** The secret is length $n$, the shares are of length $n + 1$.

**Good News:** Every $A_i$ gets ONE share.

**Bad News:** That share is of length $n + 1$, not $n$.

**VOTE:** Can Zelda do threshold secret sh. where every student gets ONE share of length $n$?

1. YES
2. NO
3. YES given some hardness assumption
4. UNKNOWN TO SCIENCE

YES
Why Did We Use Primes?

We used $\mathbb{Z}_p$ since need every element to have a *-inverse.

**Def:** A **Field** is a set $F$ together with operations $+, \ast$ such that

1. 0 is the +-identity: $(\forall x)[x + 0 = x]$.
2. 1 is the *-identity: $(\forall x)[x \ast 1 = x]$.
3. +,* commutative: $(\forall x, y)[(x + y = y + x) \land (x \ast y = y \ast x)]$.
4. +,* associative:
   
   $$(\forall x, y, z)[(x + (y + z) = (x + y) + z) \land ((x \ast y) \ast z = x \ast (y \ast z))].$$
5. (*, +) distributive: $(\forall x, y, z)[x \ast (y + z) = x \ast y + x \ast z]$.
6. Exists +-inverse: $(\forall x)(\exists y)[x + y = 0]$.
7. Exists *-inverses: $(\forall x \neq 0)(\exists y)[x \ast y = 1].$ **IMPORTANT!**

**WE USED:** $p$ prime iff $\mathbb{Z}_p$ a field.
Can We use a Different Field?

**KEY:** There is a field of size $p^n$ for all primes $p$ and $n \geq 1$. 
Can We use a Different Field?

**KEY:** There is a field of size $p^n$ for all primes $p$ and $n \geq 1$.

**WE USE:** For all $n$, there is a field on $2^n$ elements. If secret is $s$ of length $n$, use the field on $2^n$ elements. All elements of it are of length $n$. 
Can We use a Different Field?

**KEY:** There is a field of size $p^n$ for all primes $p$ and $n \geq 1$.

**WE USE:** For all $n$, there is a field on $2^n$ elements. If secret is $s$ of length $n$, use the field on $2^n$ elements. All elements of it are of length $n$.

**Upshot:** For threshold there is a secret sh. scheme where everyone gets ONE share of size EXACTLY the size of the secret.
Example: A Field of 32 elements

\[ \mathbb{Z}_2[x] \] is the set of polys over \( \mathbb{Z}_2 \). \( x^5 + x^2 + 1 \) is irreducible in \( \mathbb{Z}_2[x] \) (so it is not the product of two other elements of \( \mathbb{Z}_2[x] \)).

Field on \( 2^5 \) elements:
Example: A Field of 32 elements

\[ \mathbb{Z}_2[x] \] is the set of polys over \( \mathbb{Z}_2 \). \( x^5 + x^2 + 1 \) is irreducible in \( \mathbb{Z}_2[x] \) (so it is not the product of two other elements of \( \mathbb{Z}_2[x] \)).

Field on \( 2^5 \) elements:

1. The elements are polys in \( \mathbb{Z}_2[x] \) of degree \( \leq 4 \).
Example: A Field of 32 elements

\( \mathbb{Z}_2[x] \) is the set of polys over \( \mathbb{Z}_2 \). \( x^5 + x^2 + 1 \) is irreducible in \( \mathbb{Z}_2[x] \) (so it is not the product of two other elements of \( \mathbb{Z}_2[x] \)).

Field on \( 2^5 \) elements:

1. The elements are polys in \( \mathbb{Z}_2[x] \) of degree \( \leq 4 \).
2. Addition and subtraction are as usual.
Example: A Field of 32 elements

\( \mathbb{Z}_2[x] \) is the set of polys over \( \mathbb{Z}_2 \). \( x^5 + x^2 + 1 \) is irreducible in \( \mathbb{Z}_2[x] \) (so it is not the product of two other elements of \( \mathbb{Z}_2[x] \)).

Field on \( 2^5 \) elements:

1. The elements are polys in \( \mathbb{Z}_2[x] \) of degree \( \leq 4 \).
2. Addition and subtraction are as usual.
3. Mult is MOD \( x^5 + x^2 + 1 \). So Mult two polys together and
Example: A Field of 32 elements

\( \mathbb{Z}_2[x] \) is the set of polys over \( \mathbb{Z}_2 \). \( x^5 + x^2 + 1 \) is irreducible in \( \mathbb{Z}_2[x] \) (so it is not the product of two other elements of \( \mathbb{Z}_2[x] \)).

Field on \( 2^5 \) elements:

1. The elements are polys in \( \mathbb{Z}_2[x] \) of degree \( \leq 4 \).
2. Addition and subtraction are as usual.
3. Mult is MOD \( x^5 + x^2 + 1 \). So Mult two polys together and Replace \( x^5 \) with \( -x^2 - 1 = x^2 + 1 \)
Example: A Field of 32 elements

$\mathbb{Z}_2[x]$ is the set of polys over $\mathbb{Z}_2$. $x^5 + x^2 + 1$ is irreducible in $\mathbb{Z}_2[x]$ (so it is not the product of two other elements of $\mathbb{Z}_2[x]$).

Field on $2^5$ elements:

1. The elements are polys in $\mathbb{Z}_2[x]$ of degree $\leq 4$.
2. Addition and subtraction are as usual.
3. Mult is MOD $x^5 + x^2 + 1$. So Mult two polys together and
   Replace $x^5$ with $-x^2 - 1 = x^2 + 1$
   Replace $x^6$ with $-x^3 - x = x^3 + x$
Example: A Field of 32 elements

$\mathbb{Z}_2[x]$ is the set of polys over $\mathbb{Z}_2$. $x^5 + x^2 + 1$ is irreducible in $\mathbb{Z}_2[x]$ (so it is not the product of two other elements of $\mathbb{Z}_2[x]$).

Field on $2^5$ elements:

1. The elements are polys in $\mathbb{Z}_2[x]$ of degree $\leq 4$.
2. Addition and subtraction are as usual.
3. Mult is MOD $x^5 + x^2 + 1$. So Mult two polys together and Replace $x^5$ with $-x^2 - 1 = x^2 + 1$
   Replace $x^6$ with $-x^3 - x = x^3 + x$
   Replace $x^7$ with $-x^4 - x^2 = x^4 + x^2$
Example: A Field of 32 elements

\[ \mathbb{Z}_2[x] \] is the set of polys over \( \mathbb{Z}_2 \). \( x^5 + x^2 + 1 \) is irreducible in \( \mathbb{Z}_2[x] \) (so it is not the product of two other elements of \( \mathbb{Z}_2[x] \)).

Field on \( 2^5 \) elements:

1. The elements are polys in \( \mathbb{Z}_2[x] \) of degree \( \leq 4 \).
2. Addition and subtraction are as usual.
3. Mult is MOD \( x^5 + x^2 + 1 \). So Mult two polys together and
   Replace \( x^5 \) with \( -x^2 - 1 = x^2 + 1 \)
   Replace \( x^6 \) with \( -x^3 - x = x^3 + x \)
   Replace \( x^7 \) with \( -x^4 - x^2 = x^4 + x^2 \)
   Replace \( x^8 \) with \( -x^5 - x^3 = x^5 + x^3 \equiv x^3 + x^2 + 1 \)
\( \mathbb{Z}_2[x] \) is the set of polys over \( \mathbb{Z}_2 \). \( x^5 + x^2 + 1 \) is irreducible in \( \mathbb{Z}_2[x] \) (so it is not the product of two other elements of \( \mathbb{Z}_2[x] \)).

Field on \( 2^5 \) elements:

1. The elements are polys in \( \mathbb{Z}_2[x] \) of degree \( \leq 4 \).
2. Addition and subtraction are as usual.
3. Mult is MOD \( x^5 + x^2 + 1 \). So Mult two polys together and Replace \( x^5 \) with \( -x^2 - 1 = x^2 + 1 \)
   Replace \( x^6 \) with \( -x^3 - x = x^3 + x \)
   Replace \( x^7 \) with \( -x^4 - x^2 = x^4 + x^2 \)
   Replace \( x^8 \) with \( -x^5 - x^3 = x^5 + x^3 \equiv x^3 + x^2 + 1 \)
4. One can show that this is a Field—mult has inverses. For that proof need that the poly \( x^5 + x^2 + 1 \) is irreducible.
Field on $p^a$ Elements

$\mathbb{Z}_p[x]$ is the set of polynomials over $\mathbb{Z}_p$.
$f(x)$ is irreducible in $\mathbb{Z}_p[x]$, and of degree $a$

Field on $p^a$ elements:

1. The elements are polys in $\mathbb{Z}_p[x]$ of degree $\leq a - 1$.
2. Addition and subtraction are as usual.
3. Mult is MOD $f(x)$. So Multiply two polys together and mod down to degree $\leq a - 1$ by assuming $f(x) = 0$.
4. One can show that this is a Field- mult has inverses. For that proof need that the poly $f(x)$ is irreducible.
1. We **could** from now on, on HW and exams and slides and notes, work over the field on $2^n$ elements and have shares of length **exactly** the size of the secret.
Practical and Pedagogical Point

1. We **could** from now on, on HW and exams and slides and notes, work over the field on $2^n$ elements and have shares of length **exactly** the size of the secret.

2. That would be **madness!**
Practical and Pedagogical Point

1. We **could** from now on, on HW and exams and slides and notes, work over the field on $2^n$ elements and have shares of length **exactly** the size of the secret.

2. That would be **madness!**  **Madness I say!**
1. We could from now on, on HW and exams and slides and notes, work over the field on $2^n$ elements and have shares of length exactly the size of the secret.

2. That would be madness! Madness I say!

3. For pedagogy we work over $\mathbb{Z}_p$ for some well chosen $p$. 

1. We could from now on, on HW and exams and slides and notes, work over the field on $2^n$ elements and have shares of length exactly the size of the secret.

2. That would be madness! Madness I say!

3. For pedagogy we work over $\mathbb{Z}_p$ for some well chosen $p$.

4. We will cheat and lie. We will say the shares are the same length as the secret when may be off by 1 (YES, just by 1) because we use primes instead of the field on $2^n$ elements.)
1. We could from now on, on HW and exams and slides and notes, work over the field on $2^n$ elements and have shares of length exactly the size of the secret.

2. That would be madness! Madness I say!

3. For pedagogy we work over $\mathbb{Z}_p$ for some well chosen $p$.

4. We will cheat and lie. We will say the shares are the same length as the secret when may be off by 1 (YES, just by 1) because we use primes instead of the field on $2^n$ elements.)

5. In the real world they use primes.
1. We could from now on, on HW and exams and slides and notes, work over the field on $2^n$ elements and have shares of length exactly the size of the secret.

2. That would be madness! Madness I say!

3. For pedagogy we work over $\mathbb{Z}_p$ for some well chosen $p$.

4. We will cheat and lie. We will say the shares are the same length as the secret when may be off by 1 (YES, just by 1) because we use primes instead of the field on $2^n$ elements.)

5. In the real world they use primes. I think.
Practical and Pedagogical Point

1. We **could** from now on, on HW and exams and slides and notes, work over the field on $2^n$ elements and have shares of length **exactly** the size of the secret.

2. That would be **madness**! *Madness* I say!

3. For pedagogy we work over $\mathbb{Z}_p$ for some well chosen $p$.

4. We will **cheat and lie**. We will say the shares are the same length as the secret when may be off by 1 (YES, just by 1) because we use primes instead of the field on $2^n$ elements.)

5. In the real world they use primes. I think. I’ll ask Putin.
Can Shares be SHORTER than Secret?

1. If we use Fields, we have size-of-shares EQUALS size-of-secret.
2. If we use Mod $p$ with $p$ prime, we have size-of-shares EQUALS size-of-secret (+1).

Can Zelda Secret Share with shares SHORTER than the secret?

1. YES
2. NO
3. YES but needs a hardness assumption.
4. UNKNOWN TO SCIENCE

VOTE
Can Shares be SHORTER than Secret?

1. If we use Fields, we have size-of-shares EQUALS size-of-secret.
2. If we use Mod $p$ with $p$ prime, we have size-of-shares EQUALS size-of-secret (+1).

Can Zelda Secret Share with shares SHORTER than the secret?

1. YES
2. NO
3. YES but needs a hardness assumption.
4. UNKNOWN TO SCIENCE

VOTE

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. (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 COULD learn the secret, since its 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 $CAND$. $|CAND| = 2^6 < 2^6$. So $A_1, A_2, A_3$ have eliminated many strings from being the secret $s$ That is INFORMATION!!!!

On the HW you will do more examples and perhaps generalize to show can NEVER have shorter shares.
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.**
Will do that later.
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?
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 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. 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 $s$.
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 sh. 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 sh. problem.

You’ve Been Punked!

$A_1, A_2$ CAN find $s$ but $A_1, A_2, A_3$ CANNOT. Thats 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.

Lets rephrase that so we can generalize:

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

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:
$\mathcal{X}$ 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?
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

Definition
An **Access Structure** is a 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 sh. scheme for \( \mathcal{X} \)?
   1.2 Is there a secret sh. 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.

Definition
A sec. sharing sch. is **ideal** if all shares same size as secret.
Want

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?
OR of AND: Ideal Sec Sharing Protocol

Want

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 sh. with $A_1, A_2, A_3$.
2. Zelda does $(4, 7)$ secret sh. with $B_1, \ldots, B_7$. 

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

Want

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 sh. with $A_1, A_2, A_3$.
2. Zelda does (4, 7) secret sh. with $B_1, \ldots, B_7$.

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 $A_1, A_2, A_3, A_4$. 
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 $B_1, \ldots, B_6$. 
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 sh..
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 sh..

**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)
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 sh..

2. 

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

**Note** We now have a large set of non-threshold scenarios that have ideal secret sh..
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 $s$, $|s| = n$.
2. Zelda generates random $r \in \{0, 1\}^n$.
3. Zelda does $(2, 4)$ secret sh. of $r$ with $A_1, A_2, A_3, A_4$.
4. Zelda does $(4, 7)$ secret sh. 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 call 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 sh..

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 sh. of $r_1$ with $A_i$’s.

4. :

5. Zelda does $(t_{25}, m_{25})$ secret sh. of $r_{25}$ with $Y_i$’s.

6. Zelda does $(t_{26}, m_{26})$ secret sh. 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 sh. 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. Let \( G \) be a graph. Let \( s, t \) be nodes. People are edges. Any connected path can get the secret. WE DIDN”T DO THIS AND WON”T.
4. Monotone Span Programs (Omitted – its a Matrix Thing) WE DIDN”T DO THIS AND WON”T.
Access Structures that do not admit Ideal Sec Sharing

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

2. \((A_1 \land A_2 \land A_3) \lor (A_1 \land A_4) \lor (A_2 \land A_4) \lor (A_3 \lor A_4)\) (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.
Open Question

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