Secret Sharing

Threshold Secret Sharing

Zelda has a **secret** $s \in \{0,1\}^n$.

Def: Let $1 \le t \le m$. **(t, L)-secret sharing** is a way for Zelda to give strings to $A_1, \ldots, A_L$ such that:

1. If any t get together than they can learn the secret.
2. If any $t-1$ get together they cannot learn the secret.

Threshold Secret Sharing Caveats

Cannot learn the secret . Two flavors:

1. Info-theoretic
2. Computational.

Note Access Structure is a set of sets of students closed under superset. Can also look at Secret Sharing with other access structures.

Methods For Secret Sharing

Assume $|s| = n$.

1. Random String Method.
   PRO Can be used for ANY access structure.
   CON For Threshold Zelda may have to give Alice LOTS of strings
2. Poly Method. Uses: t points det poly of deg $t-1$.
   PRO Zelda gives Alice a share of exactly n. Simple.
   CON Only used for threshold secret sharing
   DESCRIPTION Next Slide.

Threshold Secret Sharing With Polynomials: (t, m)

Zelda wants to give strings to $A_1, \ldots, A_m$ such that

Any t of $A_1, \ldots, A_m$ can find s. Any $t-1$ learn **NOTHING** .

Threshold Secret Sharing With Polynomials: (t, m)

Zelda wants to give strings to $A_1, \ldots, A_m$ such that

Any t of $A_1, \ldots, A_m$ can find s. Any $t-1$ learn **NOTHING** .

1. Secret $s \in \mathbb{Z}_p$. Zelda works mod p.

Threshold Secret Sharing With Polynomials: (t, m)

Zelda wants to give strings to $A_1, \ldots, A_m$ such that

Any t of $A_1, \ldots, A_m$ can find s. Any $t-1$ learn **NOTHING** .

1. Secret $s \in \mathbb{Z}_p$. Zelda works mod p.
2. Zelda gen rand $a_{t-1}, \ldots, a_1 \in \mathbb{Z}_p$.

Threshold Secret Sharing With Polynomials: (t, m)

Zelda wants to give strings to $A_1, \ldots, A_m$ such that

Any t of $A_1, \ldots, A_m$ can find s. Any $t-1$ learn **NOTHING** .

1. Secret $s \in \mathbb{Z}_p$. Zelda works mod p.
2. Zelda gen rand $a_{t-1}, \ldots, a_1 \in \mathbb{Z}_p$.
3. Zelda forms polynomial $f(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + s$.

Threshold Secret Sharing With Polynomials: (t, m)

Zelda wants to give strings to $A_1, \ldots, A_m$ such that

Any t of $A_1, \ldots, A_m$ can find s. Any $t-1$ learn **NOTHING** .

1. Secret $s \in \mathbb{Z}_p$. Zelda works mod p.
2. Zelda gen rand $a_{t-1}, \ldots, a_1 \in \mathbb{Z}_p$.
3. Zelda forms polynomial $f(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + s$.
4. For $1 \le i \le m$ Zelda gives A_i $f(i)$ mod p.

Threshold Secret Sharing With Polynomials: (t, m)

Zelda wants to give strings to $A_1, \ldots, A_m$ such that

Any t of $A_1, \ldots, A_m$ can find s. Any $t-1$ learn **NOTHING** .

1. Secret $s \in \mathbb{Z}_p$. Zelda works mod p.
2. Zelda gen rand $a_{t-1}, \ldots, a_1 \in \mathbb{Z}_p$.
3. Zelda forms polynomial $f(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + s$.
4. For $1 \le i \le m$ Zelda gives A_i $f(i)$ mod p.

1. Any t have t points from $f(x)$ so can find $f(x)$, s.

Threshold Secret Sharing With Polynomials: (t, m)

Zelda wants to give strings to $A_1, \ldots, A_m$ such that

Any t of $A_1, \ldots, A_m$ can find s. Any $t-1$ learn **NOTHING** .

1. Secret $s \in \mathbb{Z}_p$. Zelda works mod p.
2. Zelda gen rand $a_{t-1}, \ldots, a_1 \in \mathbb{Z}_p$.
3. Zelda forms polynomial $f(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + s$.
4. For $1 \le i \le m$ Zelda gives A_i $f(i)$ mod p.

1. Any t have t points from $f(x)$ so can find $f(x)$, s.
2. Any $t-1$ have $t-1$ points from $f(x)$. From these $t-1$ points what can they conclude?

Threshold Secret Sharing With Polynomials: (t, m)

Zelda wants to give strings to $A_1, \ldots, A_m$ such that

Any t of $A_1, \ldots, A_m$ can find s. Any $t-1$ learn **NOTHING** .

1. Secret $s \in \mathbb{Z}_p$. Zelda works mod p.
2. Zelda gen rand $a_{t-1}, \ldots, a_1 \in \mathbb{Z}_p$.
3. Zelda forms polynomial $f(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + s$.
4. For $1 \le i \le m$ Zelda gives A_i $f(i)$ mod p.

1. Any t have t points from $f(x)$ so can find $f(x)$, s.
2. Any $t-1$ have $t-1$ points from $f(x)$. From these $t-1$ points what can they conclude? **NOTHING!**

Threshold Secret Sharing With Polynomials: (t, m)

Zelda wants to give strings to $A_1, \ldots, A_m$ such that

Any t of $A_1, \ldots, A_m$ can find s. Any $t-1$ learn **NOTHING** .

1. Secret $s \in \mathbb{Z}_p$. Zelda works mod p.
2. Zelda gen rand $a_{t-1}, \ldots, a_1 \in \mathbb{Z}_p$.
3. Zelda forms polynomial $f(x) = a_{t-1}x^{t-1} + \cdots + a_1 x + s$.
4. For $1 \le i \le m$ Zelda gives A_i $f(i)$ mod p.

1. Any t have t points from $f(x)$ so can find $f(x)$, s.
2. Any $t-1$ have $t-1$ points from $f(x)$. From these $t-1$ points what can they conclude? **NOTHING!** Any constant term is consistent with what they know.‘ So they know NOTHING about s.

Short Shares

If demand Info-theoretic security then shares have to be $\geq |s|$.

We did that in class: If A_t gets a share of length $< |s| - 1$ then $A_1, \ldots, A_{t-1}$ an simulate all $2^{|s|-1}$ possible shares of A_t to find $2^{|s|-1}$ possibilities for the secret. Violates info-theory security.

Using Hardness Assumptiosn can get shares of length $\beta|s|$ for $\beta < 1$. This gives comp security.

Access Structures

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

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:

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 $\mathcal{X}$?

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?

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.

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.

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 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 $TH_A(t_1,m_1) \vee TH_B(t_2,m_2)$ means that:

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 $TH_A(t_1,m_1) \vee TH_B(t_2,m_2)$ 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 $TH_A(t_1, m_1) \vee TH_B(t_2, m_2)$ 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 $TH_A(t_1, m_1) \vee TH_B(t_2, m_2)$ 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 $TH_A(t_1,m_1) \vee \cdots \vee TH_Z(t_{26},m_{26})$

AND of $TH_A(t, m)$s: An Example

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

AND of $TH_A(t,m)$s: An Example

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

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

AND of $TH_A(t, m)$s: An Example

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

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

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

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

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 ≥ 2 of A_i's get together they can find r.

AND of $TH_A(t,m)$s: An Example

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

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 ≥ 2 of A_i's get together they can find r.
   If ≥ 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 ≥ 2 of A_1, A_2, A_3, A_4 AND ≥ 4 of $B_1, \ldots, B_7$ get together than they can learn the secret, but no other groups can.

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 ≥ 2 of A_i's get together they can find r.
   If ≥ 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

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

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.

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.

Non-Ideal Access Structures

There are some- we skip this for the review.

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.

Can do by Random String Method.

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.

Can do by Random String Method.
Can do ANY access structure with Random String Method, though may be lots of shares.

Good Luck on the Exam

Good Luck on the Exam!