Weighted Threshold Secret Sharing

Nikolas Melissaris & Alexander Wood

December 17, 2015

Overview

1. Introduction & Terminology
   - Weighted Threshold Secret Sharing
   - Access Structures
2. Characterizing Ideal Weighted Threshold Access Structures
   - Hierarchical Threshold Access Structures
   - Tripartite Access Structures
   - Compositions of Access Structures
3. Hierarchical Threshold Access Structures
   - HTSS Scheme 1
   - HTSS Scheme 2
4. Multipartite Access Structures
   - Compartmented Access Structures with Upper Bounds
   - Compartmented Access Structures with Lower Bounds
5. References

(t, n) Threshold Secret Sharing

- A way of sharing a secret amont n users

(t, n) Threshold Secret Sharing

- A way of sharing a secret amont n users
- Any group of t or more users can recover the secret

(t, n) Threshold Secret Sharing

- A way of sharing a secret amont n users
- Any group of t or more users can recover the secret
- No group of less than t users can learn anything about the secret

Weighted Threshold Secret Sharing

- Each user is assigned a positive *weight*

Weighted Threshold Secret Sharing

- Each user is assigned a positive *weight*
- Their weights may be different

Weighted Threshold Secret Sharing

- Each user is assigned a positive *weight*
- Their weights may be different
- We can only recover the secret if the sum of the weights of users exceeds threshold

Access Structure

Definition (Access Structures)

Let $U = \{u_1, \ldots, u_n\}$ be a set of users. A collection $\Gamma \subseteq 2^U$ is monotone if $B \in \Gamma$ and $B \subseteq C$ implies that $C \in \Gamma$. An access structure *is a monotone collection $\Gamma \subseteq 2^U$ of non-empty subsets of U. Sets in Γ are called* authorized *and sets not in Γ are called* unauthorized*. A set B is called a* minterm *of Γ if $B \in \Gamma$ and $C \notin \Gamma$ for any $C \subset B$.*

Weighted Threshold Access Structures

Definition (Weighted Threshold Access Structures (WTAS))

Let $w : U \to \mathbb{N}$ *be a weight function on* U *and* $T \in \mathbb{N}$ *be a threshold. Define* $w(A) := \sum_{u \in A} w(u)$ *and* $\Gamma = \{A \subseteq U : w(A) \geq T\}$*. Then,* Γ *is called a* weighted threshold access structure *on* U*.*

Secret Sharing Schemes

- The authors define a *secret sharing scheme* in terms of an access structure Γ.

Secret Sharing Schemes

- The authors define a *secret sharing scheme* in terms of an access structure Γ.
- Authorized sets of users are able to unlock the secret (correctness).

Secret Sharing Schemes

- The authors define a *secret sharing scheme* in terms of an access structure Γ.
- Authorized sets of users are able to unlock the secret (correctness).
- Unauthorized sets of users are unable to learn anything about the secret from the shares of the users in the set (privacy).

Ideal Secret Sharing Schemes

- A secret sharing scheme is called *ideal* if the size of the domain of possible secrets is the size of the domain of shares of each user

Ideal Secret Sharing Schemes

- A secret sharing scheme is called *ideal* if the size of the domain of possible secrets is the size of the domain of shares of each user
- *Example: Shamir's Secret Sharing Scheme* The secret s is chosen from some field $\mathbb{K}$. The users' shares are chosen from the same field, $\mathbb{K}$.

Ideal Weighted Threshold Secret Sharing

We want to characterize all ideal weighted threshold secret sharing schemes.

Ideal Weighted Threshold Secret Sharing

We want to characterize all ideal weighted threshold secret sharing schemes.
We follow Beimel, Tassa, and Weinreb's *Characterizing Ideal Weighted Threshold Secret Sharing*

Hierarchical Threshold Access Structures

Definition (Hierarchical Threshold Access Structures)

Let m be an integer, U a set of users, and $\{L_i\}_{1 \leq i \leq m}$ a partition of U into m disjoint levels. Call L_i the levels *in the HTAS. Let $\{k_i\}_{1 \leq i \leq m}$ be a sequence of decreasing thresholds. This hierarchy and sequence of thresholds induces a* hierarchical threshold access structure (HTAS) *on U:*

$$\Gamma_H = \left\{ A \subset U : \text{ There exists } i \in \{1, \ldots, m\} \text{ such that } \left| A \cap \bigcup_{j=i}^{m} L_j \right| \geq k_i \right\}.$$

In other words, $A \subseteq U$ is in Γ_H if and only if it contains at least k_i users from the ith level and above for some i, $1 \leq i \leq m$.

Hierarchical Threshold Access Structures

- Let Γ be a WTAS on n users with weight function $w : U \to \mathbb{N}$ and threshold T

Hierarchical Threshold Access Structures

- Let Γ be a WTAS on n users with weight function $w : U \to \mathbb{N}$ and threshold T
- Assume $U = \{u_1, \ldots, u_n\}$ has a prefix minterm $U_{1,k} = \{u_1, \ldots, u_k\} \in \Gamma$

Hierarchical Threshold Access Structures

- Let Γ be a WTAS on n users with weight function $w : U \to \mathbb{N}$ and threshold T
- Assume $U = \{u_1, \ldots, u_n\}$ has a prefix minterm $U_{1,k} = \{u_1, \ldots, u_k\} \in \Gamma$
- Partition U into levels to describe an equivalent hierarchical threshold access structure Γ_H

Ideal WTASs as HTASs

Theorem

Let Γ be an ideal WTAS on U that has a prefix minterm. Then, Γ is a HTAS.

HTAS – An Example

Say we have an ideal WTAS Γ which has 14 users whose weights respectively are

$$5, 5, 5, 5, 6, 6, 6, 6, 6, 6, 6, 30, 30, 30$$

with threshold $T = 30$. Then L_1 contains the four users with weight 5, L_2 contains the seven users with weight 6, and L_3 contains the three self-sufficient users with weight 30.

Tripartite Access Structures

Definition (Tripartite Access Structure (TPAS))

Let U be a set of n users such that $U = A \cup B \cup C$, where A, B, and C are pairwise disjoint and A and C are not empty. Let m, d, t be positive integers such that $m \geq t$. Then, the following defines a tripartite access structure (TPAS) *on U:*

$$\Delta_1 = \{X \subseteq U : (|X| \geq m \text{ and } |X \cap (B \cup C)| \geq m - d) \text{ or } |X \cap C| \geq t\}.$$

Namely, a set X is in Δ_1 if either it has at least m users, $(m - d)$ of which are from $B \cup C$, or it has at least t users from C. If $|B| \leq d + t - m$, then the following is another type of TPAS:

$$\Delta_2 = \{X \subseteq U : (|X| \geq m \text{ and } |X \cap C| \geq m - d) \text{ or } |X \cap (B \cup C)| \geq t\}.$$

Lexicographically Minimal Minterm

Let $A = \{a_j\}_{1 \leq j \leq k}$ and $B = \{b_j\}_{1 \leq j \leq \ell}$ be two ordered subsets of $U = \{u_1, \ldots, u_n\}$. Say that for users u_i and u_j, we have that $u_i \prec u_j$ if $i < j$. Furthermore we let $A \prec B$ denote that:

- $\emptyset \prec A$ for all nonempty $A \subset U$.
- If $a_1 \prec b_1$ then $A \prec B$; if $b_1 \prec a_1$ then $B \prec A$; otherwise $A \prec B$ if and only if $(A \setminus \{a_1\}) \prec (B \setminus \{b_1\})$.

Let M be the *lexicographically minimal minterm* of a WTAS Γ on U if M is a minterm in Γ such that $M \prec M'$ for all other minterms $M' \in \Gamma$.

Ideal WTASs as TPASs

Theorem

Let Γ be an ideal WTAS such that $M = U_{1,d} \cup U_{d+2,k}$ is its lexicographically minimal minterm for some $1 \leq d \leq k-2$ and $k \leq n$. If there is a minterm in Γ with u_2 as its minimal member and if Γ has no self-sufficient users, then Γ is a TPAS.

TPAS – An Example

Consider a set of nine users $U = \{u_1, \ldots, u_9\}$. Let Γ be an ideal WTAS with weights $16, 16, 17, 18, 19, 24, 24, 24,$ and 24, respectively. Let the threshold $T = 92$. Note that there is no prefix minterm, since

$$w(U_{2,6}) = 16 + 17 + 18 + 19 + 24 = 94 \geq T$$

but $w(U_{1,5}) < T$. Thus, $k = 6$. The lexicographically minimal minterm for this example is $U_{1,3} \cup U_{5,6}$, so $d = 3$. We have the TPAS with three sets of users: $A = U_{1,4}$, $B = \{u_5\}$, and $C = U_{6,9}$. In other words, we have that $r = 5$ with thresholds $k_1 = 5$ and $k_2 = 4$, and since $r > d - 1$ this is an access structure of type Δ_1.

Compositions of Access Structures

Definition (Composition of access structures)

Let U_1 and U_2 be disjoint sets of users, and let Γ_1 and Γ_2 be access structures on U_1 and U_2 respectively. Let $u_1 \in U_1$ and set $U = (U_1 \cup U_2) \setminus \{u_1\}$. Then the composition *of Γ_1 and Γ_2 via u_1 is*

$$\Gamma = \left\{ X \subseteq U : \substack{X_1 \in \Gamma_1 \text{ or } (X_2 \in \Gamma_2 \text{ and } X_1 \cup \{u_1\} \in \Gamma_1), \\ \text{where } X_1 = X \cap U_1 \text{ and } X_2 = X \cap U_2} \right\}$$

- The composition of two ideal WTASs is an ideal WTAS

- The composition of two ideal WTASs is an ideal WTAS
- A WTAS which is not a HTAS or a TPAS is a composition of two ideal WTASs that are defined on sets smaller than U

Composition of Access Structures – An Example

Consider a WTAS with users $U = \{u_1, \ldots, u_8\}$ with weights 1, 1, 1, 1, 1, 3, 3, 3 and threshold $T = 6$. This access structure has lexicographically minimal minterm $\{u_1, u_2, u_3, u_6\}$. Therefore, Γ is neither a HTAS nor a TPAS.

Composition of Access Structures – An Example

Consider a WTAS with users $U = \{u_1, \ldots, u_8\}$ with weights 1, 1, 1, 1, 1, 3, 3, 3 and threshold $T = 6$. This access structure has lexicographically minimal minterm $\{u_1, u_2, u_3, u_6\}$. Therefore, Γ is neither a HTAS nor a TPAS.

Let $\Gamma_1 = U_{1,5}$ and $\Gamma_2 = U_{6,8}$. Then Γ is a composition of a 2-of-4 threshold access structure on $\Gamma_2 \cup \{u'\}$ and a 3-of-5 access structure on Γ_1, where u' is a dummy variable.

Overview

Let Γ be an ideal WTAS defined on a set of n users. Γ can be characterized as one of the following:

Overview

Let Γ be an ideal WTAS defined on a set of n users. Γ can be characterized as one of the following:

1. A hierarchical threshold access structure

Overview

Let Γ be an ideal WTAS defined on a set of n users. Γ can be characterized as one of the following:

1. A hierarchical threshold access structure
2. A tripartite access structure

Overview

Let Γ be an ideal WTAS defined on a set of n users. Γ can be characterized as one of the following:

1. A hierarchical threshold access structure
2. A tripartite access structure
3. A composition of two ideal WTASs

Hierarchical Threshold Secret Sharing

We follow Tassa's *Hierachical Threshold Secret Sharing*

Hierarchical Threshold Secret Sharing

We follow Tassa's *Hierachical Threshold Secret Sharing*
We introduce secret sharing schemes based on Birkoff interpolation

Hierarchical Threshold Secret Sharing

Let U have m levels, and say $\mathbf{k} = \{k_i\}_{i=1}^{m}$ is a increasing sequence of thresholds. Let $\sigma(u)$ denote each user u's share of the secret S.
We have the following conditions:

Hierarchical Threshold Secret Sharing

Let U have m levels, and say $\mathbf{k} = \{k_i\}_{i=1}^{m}$ is a increasing sequence of thresholds. Let $\sigma(u)$ denote each user u's share of the secret S.
We have the following conditions:

- Accessibility: $H\left(S|\sigma(V)\right) = 0 \quad \forall V \in \Gamma$

Hierarchical Threshold Secret Sharing

Let U have m levels, and say $\mathbf{k} = \{k_i\}_{i=1}^{m}$ is a increasing sequence of thresholds. Let $\sigma(u)$ denote each user u's share of the secret S.
We have the following conditions:

- Accessibility: $H(S|\sigma(V)) = 0 \quad \forall V \in \Gamma$
- Perfect security: $H(S|\sigma(V)) = H(S) \quad \forall V \notin \Gamma$

Hierarchical Threshold Secret Sharing Scheme 1

Let $\mathbb{F}$ be a field of large prime order q

1. The dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$, where

$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_0 = S.$$

Hierarchical Threshold Secret Sharing Scheme 1

Let $\mathbb{F}$ be a field of large prime order q

1. The dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$, where

$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_0 = S.$$

2. The dealer identifies each participant $u \in U$ with a field element, also denoted u

Hierarchical Threshold Secret Sharing Scheme 1

Let $\mathbb{F}$ be a field of large prime order q

1. The dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$, where

$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_0 = S.$$

2. The dealer identifies each participant $u \in U$ with a field element, also denoted u
3. Each user from the ith level in the hierarchy will receive the $P^{(k_{i-1})}(u)$ where $k_{-1} = 0$.

HTSS Scheme 1: Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$

HTSS Scheme 1: Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$

HTSS Scheme 1: Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$
- Polynomial $P(x) = \sum_{i=0}^{6} a_i x^i$, $a_0 = S$

HTSS Scheme 1: Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$
- Polynomial $P(x) = \sum_{i=0}^{6} a_i x^i$, $a_0 = S$
-
    - At Level 0 users receive $P(u)$

HTSS Scheme 1: Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$
- Polynomial $P(x) = \sum_{i=0}^{6} a_i x^i$, $a_0 = S$
-
  - At Level 0 users receive $P(u)$
  - At Level 1 users receive $P''(u)$ since $k_0 = 2$

HTSS Scheme 1: Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$
- Polynomial $P(x) = \sum_{i=0}^{6} a_i x^i$, $a_0 = S$
-
    - At Level 0 users receive $P(u)$
    - At Level 1 users receive $P''(u)$ since $k_0 = 2$
    - At level 2 users receive $P^{(4)}(u)$ since $k_1 = 4$

Disjunctive HTSS Problem

The disjunctive access structure is:

$$\Gamma = \left\{ V \subset U : \exists i \in \{0, 1, \ldots, m\} \text{ for which } \left| V \cap \left(\cup_{j=0}^{i} U_j \right) \right| \geq k_i \right\}$$

Ideal HTSS Scheme 2

The scheme is as follows:

Ideal HTSS Scheme 2

The scheme is as follows:

1. The dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$ where

$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_{k-1} = S.$$

Ideal HTSS Scheme 2

The scheme is as follows:

1. The dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$ where

$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_{k-1} = S.$$

2. The dealer identifies each participant $u \in U$ with a field element, denoted simply by u.

Ideal HTSS Scheme 2

The scheme is as follows:

1. The dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$ where

$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_{k-1} = S.$$

2. The dealer identifies each participant $u \in U$ with a field element, denoted simply by u.
3. The dealer distributes shares to all the participants in such a way that each participant of the ith level in the hierarchy receives the share $P^{(k-k_i)}(u)$

Ideal HTSS Scheme 2 Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$

Ideal HTSS Scheme 2 Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds: $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$

Ideal HTSS Scheme 2 Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds: $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$
- Dealer selects $\sum_{i=0}^{6} a_i x^i$ where $a_6 = S$

Ideal HTSS Scheme 2 Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds: $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$
- Dealer selects $\sum_{i=0}^{6} a_i x^i$ where $a_6 = S$
- Distribution:

Ideal HTSS Scheme 2 Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds: $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$
- Dealer selects $\sum_{i=0}^{6} a_i x^i$ where $a_6 = S$
- Distribution:
  - $u \in U_0$ will get $P^{(5)}(u)$

Ideal HTSS Scheme 2 Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds: $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$
- Dealer selects $\sum_{i=0}^{6} a_i x^i$ where $a_6 = S$
- Distribution:
  - $u \in U_0$ will get $P^{(5)}(u)$
  - $u \in U_1$ will get $P^{(3)}(u)$

Ideal HTSS Scheme 2 Example

- Three levels: $U = U_0 \cup U_1 \cup U_2$
- Thresholds: $\mathbf{k} = (k_0, k_1, k_2) = (2, 4, 7)$
- Dealer selects $\sum_{i=0}^{6} a_i x^i$ where $a_6 = S$
- Distribution:
  - $u \in U_0$ will get $P^{(5)}(u)$
  - $u \in U_1$ will get $P^{(3)}(u)$
  - $u \in U_2$ will get $P(u)$

Multipartite Secret Sharing

We follow Tassa and Dyn's *Multipartite Secret Sharing by Bivariate Interpolation*

Multipartite Access Structures

Definition (Multipartite Access Structure (MPAS))

Let U be a set of users and assume that U is partitioned into m disjoint compartments,

$$U = \bigcup_{i=1}^{m} C_i.$$

Let $\Gamma = 2^U$ be an access structure on U and assume that for all permutations $\pi : U \to U$ such that $\pi(C_i) = C_i$, $1 \leq i \leq m$, then $V \in \Gamma$ if and only if $\pi(V) \in \Gamma$. Then Γ is called m-partite or multipartite with respect to the partition.

Compartmented Access Structures

- With lower bounds:

$$\Gamma = \{V \subseteq U : \exists W \subseteq V \text{ such that } |W \cap C_i| \geq t_i,\ 1 \leq i \leq m, \\ \text{and } |W| = t\}$$

Compartmented Access Structures

- With lower bounds:

$$\Gamma = \{V \subseteq U : \exists W \subseteq V \text{ such that } |W \cap C_i| \geq t_i,\ 1 \leq i \leq m, \text{ and } |W| = t\}$$

- With upper bounds:

$$\Delta = \{V \subseteq U : \exists W \subseteq V \text{ such that } |W \cap C_i| \leq s_i,\ 1 \leq i \leq m, \text{ and } |W| = s\}$$

CASUB Secret Sharing Scheme 1:

- Secret $S \in \mathbb{F}$

CASUB Secret Sharing Scheme 1:

- Secret $S \in \mathbb{F}$
- x_i, $1 \leq i \leq m$, distinct random points in $\mathbb{F}$

CASUB Secret Sharing Scheme 1:

- Secret $S \in \mathbb{F}$
- x_i, $1 \leq i \leq m$, distinct random points in $\mathbb{F}$
- $P_i(y) = \sum_{j=0}^{s_i - 1} a_{i,j} y^j$ random polynomials over $\mathbb{F}$

CASUB Secret Sharing Scheme 1:

- Secret $S \in \mathbb{F}$
- x_i, $1 \leq i \leq m$, distinct random points in $\mathbb{F}$
- $P_i(y) = \sum_{j=0}^{s_i-1} a_{i,j} y^j$ random polynomials over $\mathbb{F}$
- Secret $S = \sum_{i=1}^{m} \sum_{j=0}^{s_i-1} a_{i,j} y^j L_i(x)$, where $L_i(x)$ are Lagrange polynomials of degree $m-1$

CASUB Secret Sharing Scheme 1:

1. Each participant $u_{i,j}$ from compartment C_i is identified by a unique public point $(x_i, y_{i,j})$, where $y_{i,j} \neq 1$ is random and $P(x_i, y_{i,j})$ is the private share of the user.

CASUB Secret Sharing Scheme 1:

1. Each participant $u_{i,j}$ from compartment C_i is identified by a unique public point $(x_i, y_{i,j})$, where $y_{i,j} \neq 1$ is random and $P(x_i, y_{i,j})$ is the private share of the user.
2. We publish the value of P at $k := \sum_{i=1}^{m} s_i - s$ random points (x'_i, z_i) where $x'_i \notin x_1, \ldots, x_m$, $1 \leq i \leq k$.

Secret Sharing Scheme 1 Example:

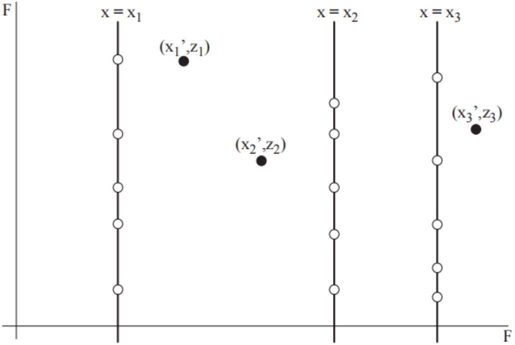

Figure: Case where $m = 3$ compartments, and $k = s_1 + s_2 + s_3 - s = 3$

Dual Access Structure

Definition

The dual access structure Γ^* *is defined by:*

$$\Gamma^* = \{V \subseteq U \;:\; |V| \geq r \text{ or } |V \cap C_i| \geq r_i \text{ for some } 1 \leq i \leq m\}$$

where

$$r = n - t + 1 \text{ and } r_i = n_i - t_i + 1 \;,\; 1 \leq i \leq m.$$

The thresholds in the dual access structure satisfy $\sum_{i=1}^{m} r_i \geq r + m - 1$.

CASLB Secret Sharing Scheme 2:

- m distinct points $x_1, \ldots, x_m$ in $\mathbb{F}$

CASLB Secret Sharing Scheme 2:

- m distinct points $x_1, \ldots, x_m$ in $\mathbb{F}$
- $P_i(y)$ be a polynomial of degree $r_i - 1$ over $\mathbb{F}$ satisfying

$$P_1(0) = \cdots = P_m(0) = S,$$

for a secret S.

CASLB Secret Sharing Scheme 2:

- m distinct points $x_1, \ldots, x_m$ in $\mathbb{F}$
- $P_i(y)$ be a polynomial of degree $r_i - 1$ over $\mathbb{F}$ satisfying

$$P_1(0) = \cdots = P_m(0) = S,$$

  for a secret S.
- Define P as

$$P(x, y) = \sum_{i=1}^{m} P_i(y) L_i(x) = \sum_{i=1}^{m} \sum_{j=0}^{r_i - 1} a_{i,j} y^j L_i(x).$$

CASLB Secret Sharing Scheme 2:

1. Each participant $u_{i,j}$ from compartment C_i will be identified by a unique public point $(x_i, y_{i,j})$ where $y_{i,j} \neq 0$ is random and his private share will be the value of P at that point.

CASLB Secret Sharing Scheme 2:

1. Each participant $u_{i,j}$ from compartment C_i will be identified by a unique public point $(x_i, y_{i,j})$ where $y_{i,j} \neq 0$ is random and his private share will be the value of P at that point.
2. We publish the value of P at $k = g - r$ random points $(x_i^{'}, z_i)$ where $x_i^{'} \notin x_1, \ldots, x_m$, $1 \leq i \leq k$.

THANK YOU!

References

- Amos Beimel, Tamir Tassa, and Enav Weinreb: Characterizing Ideal Weighted Threshold Secret Sharing, *SIAM Journal of Discrete Math*, 22(1) (2008), pp. 360-397.
- Nira Dyn and Tamir Tassa: Multipartite Secret Sharing by Bivariate Interpolation, in the Proc. of the 33rd International Colloquium on Automata, Langauges and Programming, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, eds., vol. 4052 of Lecture Notes in Computer Sciences, Springer-Verlag (2006), pp. 288-299.
- A. Shamir: How to Share a Secret, *Communications of the ACM*, 22 (1979), pp. 612-613.
- Tamir Tassa: Hierarchical Threshold Secret Sharing, *Journal of Cryptography*, 20 (2007), pp. 237-264.