WEIGHTED THRESHOLD SECRET SHARING

NIKOLAS MELISSARIS & ALEXANDER WOOD
THE GRADUATE CENTER, CUNY

Abstract. Weighted threshold secret sharing schemes, first introduced by Shamir in 1978 [6], are discussed extensively in the work of Tamir Tassa. In a weighted threshold secret sharing scheme each member in a set of users is assigned its own positive weight. A secret may only be "unlocked" if the sum of the weights of the users exceeds the threshold. In *Characterizing Ideal Weighted Threshold Secret Sharing*, Beimel, Tassa, and Weinreb characterize all ideal threshold access structures as either (1) hierarchical threshold access structures, (2) tripartite threshold access structures, or (3) a combination of two ideal weighted threshold access structures. We go on to discuss *Hierarchical Threshold Secret Sharing* by Tassa in which he presents an ideal perfect hierarchical threshold secret sharing scheme. Lastly, we discuss *Multipartite Secret Sharing and Bivariate Interpolation* by Tassa and Dyn, where they introduce a new way of designing secret sharing schemes by using bivariate Lagrange interpolation for different types of multipartite access structures.

1. Introduction

1.1. **Overview.** A (t, n) secret sharing scheme is a method of sharing a secret among n users so that any combination of more than t users can reconstruct the secret, but no group of t or less of the users can do so. This number t is called the *threshold* for the scheme [8]. Furthermore, no matter how many users are present, running the scheme reveals nothing about any user's personal share of the secret [3].

Secret sharing schemes are used widely in applications such as sharing the key to a central vault in a bank, electronic voting schemes, blind signature schemes, and the millionaire problem [3][8]. Secret sharing schemes, first introduced by Shamir in 1978, presented a solution to these problems [6].

However, sometimes we consider certain users to have higher value of others in the scheme. For instance, the CEO of a large corporation may want to be able to access a certain secret on her own, while requiring at least three supervisors to be present to access the same secret on their own. For problems like this we introduce *weighted secret sharing schemes*.

1.2. **Weighted Secret Sharing Schemes.** In a weighted threshold secret sharing scheme, each user is assigned a positive *weight*. We can only recover the secret if the sum of the weights of the users trying to recover it exceeds the threshold [1]. Schemes such as Shamir's assign each user equal weight, meaning each user has the same status. We now study schemes where users are allowed to have different weights.

Date: December 14, 2015.

A weighted threshold secret sharing scheme has many real-life applications. For example, you may wish to share a secret among shareholders of a company, each of whom holds a different amount of shares [1]. In this way, for instance, it is possible to assign users with higher positions in a company a higher weight.

1.3. **Outline of Paper.** We describe terminology and notation in Section 2. We introduce the concept of a weighted threshold secret sharing scheme as an *access structure* and define several specific types of access structures, including *ideal* access structures.

In Section 3 we discuss *Characterizing Ideal Weighted Threshold Secret Sharing* [1] by Beimel, Tassa, and Weinreb. 3. Here, the authors characterize all ideal weighted threshold access structures as either *hierarchical*, *tripartite*, or a composition of the two.

Next, we discuss *Hierarchical Threshold Secret Sharing* [8] by Tamir Tassa in Section 4. Here, the author outlines a secret sharing scheme for groups where the members differ in authority of confidence level. The scheme is based on Birkhoff interpolation and using polynomial derivatives to generate shares of lesser "weight," and discusses the way to assign identities to the participants.

We conclude by discussing *Multipartite Secret Sharing and Bivariate Interpolation* [5] by Tassa and Dyn in Section 5. Here, the authors use bivariate interpolation to construct ideal secret sharing schemes for compartmented access structures, hierarchical threshold access structures, and a new type of compartmented access structures.

2. Terminology and Notation

In his work Tassa frames the discussion of secret sharing schemes in terms of the language of *access structures*. An access structure is defined in [1] as follows:

Definition 2.0.1 (Access Structure)**.** *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 $C \subset B$.* [1]

The access structure simply provides a set of all possible combinations of users who could unlock the secret together. Using access structures, the authors define a Secret-Sharing Scheme as follows:

Definition 2.0.2 (Secret-Sharing Scheme)**.** *Let S be a finite set of secrets, where $|S| \geq 2$. An n-user* secret-sharing scheme Π *with* domain of secrets S *is a randomized mapping from S to a set of n-tuples $\Pi_{i=1}^{n} S_i$, where S_i is called the* share-domain *of u_i. A dealer shares a secret $s \in S$ among the n users of some set of users U according to Π by first sampling a vector of shares $\Pi(s) = (s_1, \ldots, s_n) \in \Pi_{i=1}^{n} S_i$, and then privately communicating each share s_i to the user u_i. We say that Π realizes an access structure $\Gamma \subseteq 2^U$ if the following two requirements hold:*

- ***Correctness****: The secret s can be reconstructed by any authorized set of users.*
- ***Privacy****: Every unauthorized set can learn nothing about the secret (in the information theoretic sense) from the shares of the users in the set.*

An *ideal* weighted secret sharing scheme is a scheme where the size of the total domain of possible secrets is the size of the domain of shares of each user. More formally, we say that an access structure is ideal if the domain of shares of each user is equal to the domain of secrets S [1]. For instance, consider a secret sharing scheme with the set of possible secrets S, and let T be the set of all possible shares. We define the *information rate* of the scheme as

$$\rho = \frac{\log |T|}{\log |S|},$$

and we say that a scheme is ideal if $\rho = 1$ [2]. As a more concrete example, Shamir's secret sharing scheme is ideal because the secret s is chosen from a field $\mathbb{K}$ and the shares are also chosen from $\mathbb{K}$, hence in $S = T = \mathbb{K}$. We are interested in ideal secret sharing schemes because these are the most space-efficient schemes [1].

A more specific type of access structure is a *weighted threshold access structure* (WTAS), which corresponds to weighted threshold secret sharing schemes. The text defines a WTAS as follows:

Definition 2.0.3 (Weighted Threshold Access Structures (WTAS))**.** *Let $w : U \to \mathbb{N}$ be a weight function on U and $T \in \mathbb{N}$ 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* [1].

Another type of access structure is called *hierarchical threshold access structure* (HTAS). In a HTAS, we split up the set of users into some number of levels, and the users in one level all share the same weight. More formally, a HTAS is defined in [1] as follows:

Definition 2.0.4 (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, $1 \leq i \leq m$.

Another type of access structure is called a *multipartite access structure* (MPAS). An MPAS splits the users into a number of compartments then does not distinguish between different users who are in the same compartment. A MPAS is defined in [5] as follows:

Definition 2.0.5 (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.

Tripartite access schemes (TPASs), schemes where $m = 3$ as defined above, are reviewed in Section 3, while MPASs as a whole are studied in Section 5. A TPAS is defined more precisely in [1] as follows:

Definition 2.0.6 (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:

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

Lastly, we defined an *ideal linear secret sharing scheme*:

Definition 2.0.7 (Ideal Linear Secret Sharing Scheme)**.** *Let $\mathbb{F}$ be a finite field. An ideal linear secret sharing scheme over $\mathbb{F}$ is of the following form: The domain of secrets and shares is $\mathcal{S} = \mathbb{F}$. The scheme is specified by $n+1$ vectors in $\mathbb{F}^d$ for some $d \in \mathbb{Z}$: namely, a vector $\mathbf{u}_i$ for each participant $u_i \in U$, $1 \leq i \leq n$, and a* target vector $\mathbf{t}$*. To share a secret $S \in \mathbb{F}$, the dealer chooses a random vector $\mathbf{w} \in \mathbb{F}^d$ such that $\mathbf{w} \cdot \mathbf{t} = S$, and then the share of participant u_i is $\mathbf{w} \cdot \mathbf{u}_i$.* [5]

3. Characterizing Ideal Weigthed Threshold Secret Sharing

3.1. **Results Overview.** We begin with *Characterizing Ideal Weighted Threshold Secret Sharing* by Beimel, Tassa, and Weinreb. While we have seen schemes for threshold secret sharing [6], in these schemes each users share carries the same weight. We now turn our attention to weighted threshold secret sharing schemes. In their paper, Beimel, Tassa, and Weinreb characterize all weighted threshold secret sharing schemes which are *ideal*, as defined in Section 2. Namely, the authors demonstrate that if we have an ideal WTAS, then it is of one of three possible forms:

1. A *hierarchical threshold access structure*,
2. a *tripartite access structure*, or
3. a combinatorial composition of two ideal weighted threshold access structures which satisfies certain properties [1].

We will describe each of these access structures separately. However, before delving into the meaning of each of these structures, we must first learn the language of a mathematical object called a *matroid*.

3.2. **Matroids.** The authors frame their proofs around the structure of matroids, which provide information on the structure of ideal WTASs. For an ideal WTAS there is a matroid with a corresponding structure, and furthermore every matroid which can be represented over a finite field is the reflection of an ideal access structure. A matroid is defined in [1] as follows:

Definition 3.2.1 (Matroid)**.** *A* matroid $\mathcal{M} = \langle V, \mathcal{I} \rangle$ *is a finite set* V *and a collection* $\mathcal{I}$ *of subsets of* V *which satisfy the following axioms:*
(1) $\emptyset \in \mathcal{I}$*,*
(2) If $X \in \mathcal{I}$ *and* $Y \subseteq X$ *then* $Y \in \mathcal{I}$*, and*
(3) If $X, Y \in \mathcal{I}$ *such that* $|X| = |Y| + 1$*, then there is an element* $x \in X \setminus Y$ *such that* $Y \cup \{x\} \in \mathcal{I}$*.*

Furthermore, we define the following properties:

- The elements of V are called the *points* of the matroid.
- The sets contained in $\mathcal{I}$ are the *independent sets* of the matroid. A set which is not independent is called a *dependent set*.
- Minimally dependent sets are called *circuits*.
- A matroid is *connected* if for every pair of points in V, there is a circuit that contains both of those points.

Matroids provide powerful results for the study of WTASs. Every ideal WTAS Γ has a corresponding matroid $\mathcal{M}$ [1]. If the users of a WTAS Γ are $U = \{u_1, \ldots, u_n\}$, then the points of $\mathcal{M}$ are $U \cup \{u_0\}$, where u_0 is an additional point representing the dealer. The set of all Γ-minterms supplemented by u_0 is defined as $\mathcal{C}_0 = \{X \cup \{u_0\} : X \text{ is a minterm of } T\}$.

There are several properties of matroids which provide useful in the classification of WTASs. First, for any $X = \{x_1, \ldots, x_k\} \in \Gamma$ there is an integer $i < k$ such that $X_{i,k} = \{x_i, \ldots, x_k\}$ is a minterm [1]. We call $X_{i,k}$ a *suffix minterm*. Similarly, a minterm of the form $\{x_1, \ldots, x_j\}$ for some $j < k$ is called a *prefix minterm*. A minterm of the form $A_{i,j} = \{a_k\}_{i \leq k \leq j}$ is called a *run minterm*. Using the properties of matroids, the authors prove the following result:

Lemma 3.2.1. *Any* $X \in \Gamma$ *contains a suffix minterm. If* $X = \{x_1, \ldots, x_k\}$ *and* $X \in \Gamma$*, then there is an* i*,* $1 \leq i \leq k$*, such that* $X_{i,k} = \{x_i, \ldots, x_k\}$ *is a minterm.*

3.3. **Hierarchical Threshold Access Structures.** The authors give a description of the intersection between hierarchical threshold access structures (HTASs) and WTASs. Recall that in a HTAS we split up the set of users U into m disjoint levels, $U = \bigcup_{i=1}^{m} L_i$, and the users in one level all share the same weight. Say the weight for level L_i is given by k_i, where $1 \leq i \leq m$ and $k_i > k_{i+1}$.

Say that a user in the last level L_m of a HTAS is *self-sufficient* if $k_m = 1$. If this is the case then we refer to this level as *trivial*. The authors show that if the last level L_m of Γ is not trivial then m is at most 2. Furthermore, if $m = 2$ and $k_1 - k_2 > 1$ then $|L_1| = k_1 - k_2 + 1$. This means that if a WTAS Γ which is also a HTAS has no self-sufficient users, then there are only either 1 or 2 levels [1].

If there are two levels then either $k_1 = k_2 + 1$ or $|L_1| = k_1 - k_2 + 1$. If the HTAS has self-sufficient users (i.e., the last level L_m has only one user) then restricting Γ to its first $m - 1$ levels yields a WTAS which is also a HTAS, and that restriction has no self-sufficient users. All in all, we see that if Γ is both a WTAS and a HTAS then one of the following conditions is satisfied:

(1) $m = 1$.
(2) $m = 2$ and $k_1 = k_2 + 1$.

(3) $m = 2$ and $|L_1| = k_1 - k_2 + 1$.
(4) $m \in \{2, 3\}$, the level L_m has only one user, and the restriction of Γ_H to the first $m - 1$ levels is of one of the forms $(1) - (3)$.

The converse also holds – if we have a HTAS Γ_H which satisfies one of the above conditions, then there is a weight function and a threshold such that Γ_H coincides with the corresponding WTAS [1]. Therefore we have determined when a HTAS is a WTAS and described the structure of the HTAS when this is the case.

However, the goal of this paper is to characterize *ideal* WTASs. Let Γ be a WTAS on n users with a corresponding weight function $w : U \to N$ and threshold T. Assume that U has minterm $U_{1,k}$ for some $1 \leq k \leq n$ (in other words, a prefix minterm). The authors partition U into levels and determine corresponding thresholds, describing a HTAS denoted Γ_H. Partition U into levels as follows:

- By Lemma 3.2.1, since $U_{1,i} = \{u_1, \ldots, u_i\}$ is authorized for any $k \leq i \leq n$ there is a run minterm ending at u_i. Denote the length of this run minterm by μ_i.
- The sequence $\boldsymbol{\mu} = (\mu_i)_{k \leq i \leq n}$ is monotonically non-increasing. Let m denote the number of distinct values taken by $\boldsymbol{\mu}$. We let m be the number of levels in Γ_H.
- Let k_i denote these values, where k_i is the ith threshold in Γ_H, and note that $k_1 > \cdots > k_m$.
- Now, let ℓ_i be the index of the first user in the first run minterm of length k_i. Note that $\ell_1 = 1$ since $U_{1,k}$ is the first run minterm of length k_1.
- The ith level in Γ_H is given by $L_i = U_{\ell_i, \ell_{i+1}-1}$, where $\ell_{m+1} = n + 1$.

The authors prove that the WTAS Γ described above corresponds with the HTAS Γ_H:

Theorem 3.3.1. *Let Γ be an ideal WTAS on U that has a prefix minterm. Then, Γ is an HTAS* [1].

Therefore, we have characterized a portion of the ideal WTASs as HTASs – namely, ideal WTASs with a prefix minterm are HTASs.

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.

3.4. **Tripartite Threshold Access Structures.** Next, we introduce further notation. 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 $M' \in \Gamma$.

In this section the authors characterize ideal WTASs whose lexicographically minimal minterm takes the form $M = U_{1,d} \cup U_{d+2,k}$, where $1 \leq d \leq k - 2$ and $k \leq n$. Assume

that there are no self-sufficient users and there is at least one minterm starting with user u_2. The authors show that $U_{2,k}$ is, in fact, a minterm of Γ. Ideal WTASs which are TPASs are described as follows:

Theorem 3.4.1. *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* [1].

Example. *Consider a set of nine users $U = \{u_1, \ldots, u_9\}$. Let Γ be a 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 as in Definition 2.0.6. A set is authorized if it contains for or more users from C, or if it has five users where at least two of the five users are from $B \cup C$ [1].

3.5. **WTASs of the Third Type.** So far, we have characterized WTASs as either HTASs or TPASs. When this is not the case, we instead have a *composition* of two ideal WTASs. With this in mind, the authors define a composition of access structures as follows:

Definition 3.5.1 (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*

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

First, the authors show that if Γ is an access structure which is a composition of Γ_1 and Γ_2, then Γ is ideal if and only if Γ_1 and Γ_2 are ideal. The authors characterize ideal WTASs as compositions of access structures by splitting the users into disjoint subsets of *strong users* and *weak users*: the strong users are a subset of the form of a suffix $S = U_{k,n}$ where $k \geq 3$ and the weak users are its complement, $W = U_{1,k-1}$.

To define a strong set more precisely, let a set $Y \subseteq S$ be called an *S-cooperative set* if $Y \notin \Gamma$ but $W \cup Y \in \Gamma$. Let $Y_1, Y_2 \in S$ be any two S-cooperative sets. If $\Gamma_{Y_1,W} = \{Z \subseteq W : Z \cup Y_1 \in \Gamma\}$ and $\Gamma_{Y_2,W} = \{Z \subseteq W : Z \cup Y_2 \in \Gamma\}$ coincide, then the set S is called a strong set of users.

Next, let M_1 be the lexicographically minimal minterm in an ideal WTAS Γ and let u_r be the maximal user in M_1. The authors show that if Γ is neither a HTAS nor a TPAS then $U_{1,r-1}$ contains at least two users that are not in M_1. Call u_ℓ the *minimal* user in M_1 such that at least to users in $U_{1,\ell-1}$ are missing from M_1. Let u_d be the *maximal* user in M_1 such that $U_{1,d} \subset M_1$. Let the set of users in $M_1 \cap U_{\ell,n}$ be called Z, denoted $Z = \{z_1, \ldots, z_m\}$.

The authors show that if none of the S-cooperative sets have size larger than m then S is a strong set. On the other hand, if there *is* an S cooperative set with size greater than m and there is a minterm of Γ which starts with u_2, then $U_{d+2,n}$ is a strong set of users.

All together, the authors prove the following:

- If Γ has self-sufficient users or if u_2 starts no minterm of Γ, then Γ is a composition of two ideal WTASs that are defined on sets smaller than U.
- If Γ has a strong set of users $S = U_{k,n}$ for some $k \geq 3$, then Γ is a composition of two ideal WTASs. Each of the two access structures is defined on a set smaller than U – one is defined on W and the other is defined on S supplemented by an additional user [1].

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. In this case,* $W = U_{1,5}$ *is the set of weak users and* $S = U_{6,8}$ *is the set of strong users. Then* Γ *is a composition of a* 2*-of-*4 *threshold access structure on* $S \cup \{u'\}$ *and a* 3*-of-*5 *access structure on* W, *where* u' *is a dummy variable.*

3.6. **Main Result.** Let Γ be an ideal WTAS defined on a set of n users U and let M_1 be its lexicographically minimal minterm. All in all, the authors conclude that ideal WTAS takes one of the following forms:

(1) If Γ has self-sufficient users or if u_2 starts no minterm of Γ then Γ is a composition of two ideal WTASs on smaller sets of users.
(2) If M_1 is a prefix minterm, then Γ is an HTAS.
(3) If $M_1 = U_{1,d} \cup U_{d+2,k}$ 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.
(4) Otherwise, Γ is a composition of two ideal WTASs defined on sets smaller than U.

4. Hierarchical Threshold Secret Sharing

4.1. **Terminology and Results Overview.** The next paper we review is *Hierarchical Threshold Secret Sharing* by Tamir Tassa. This paper addresses the common problem where sometimes the users in a secret sharing scheme are split into a hierarchy of weights. A simple example of this is that of a bank policy that requires three employees to open a vault, but at least one of them must be the manager. Such a setting requires a special way to share a secret. While hierarchical groups have been studied in the past, none of the proposed solutions were ideal. Tassa presents a perfect secret sharing scheme for hierarchical groups that is, in fact, ideal.

The new idea introduced by Tassa uses derivatives of polynomials to generate the shares for participants that belong to lower levels in the hierarchy. Since the scheme uses *Birkhoff interpolation* to reconstruct the secret, we need to investigate how to assign identities to the players from the underlying finite field.

A *hierarchical secret sharing* is defined in [8] as follows:

Definition 4.1.1 (Hierarchical Threshold Secret Sharing (HTSS))**.** *Let U be a set of n users. We think of U as being composed of m* levels*, meaning that $U = \bigcup_{i=0}^{m} U_i$ where $U_i \cap U_j = \emptyset$ for all $0 \leq i < j \leq m$. If $\boldsymbol{k} = \{k_i\}_{i=0}^{m}$ is a monotonically increasing sequence of integers then a $(\boldsymbol{k}, n)$-hierarchical threshold access structure (HTAS) is given by*

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

A corresponding $(\boldsymbol{k}, n)$-hierarchical threshold secret sharing scheme is a method of assigning each user $u \in U$ a share $\sigma(u)$ of a given secret S such that authorized subsets $V \in \Gamma$ are able to reconstruct the secret, while pooling shares from unauthorized subsets $V \notin \Gamma$ does not reveal anything about the value of the secret. Viewing the secret S as a random variable that takes values in a finite domain $\boldsymbol{S}$ we state that the two requirements mentioned above can be formulated as follows:

$$H(S|\sigma(V)) = 0 \quad \forall V \in \Gamma \text{ (accessibility)}$$

and

$$H(S|\sigma(V)) = H(S) \quad \forall V \notin \Gamma \text{ (perfect security).}$$

Let Σ_u be the set of all possible shares for a user. We call the scheme ideal *if for the information rate of the scheme ρ, where*

$$\rho = \min_{u \in U} \frac{\log_2 |S|}{\log_2 |\Sigma_u|},$$

we have $\rho = 1$. [8]

Note that these definitions are equivalent to the ones provided in Section 2. However, phrasing them in this way proves advantageous for the proofs required in this paper.

4.2. **Ideal Hierarchical Secret Sharing Scheme.** Let $\mathbb{F}$ be a field of large prime order q and consider the HTSS problem $(\mathbf{k}, n)$, $\mathbf{k} = \{k_i\}_{i=0}^{m}$ as defined above. The ideal HTSS proposed in [8] is as follows:

1. The dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$, where
$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_0 = S.$$
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 (k_{i-1})th derivative of $P(x)$ at $x = u$ where $k_{-1} = 0$.

This scheme is ideal. Furthermore, it is of interest to note that Shamir's secret sharing scheme is a special case of the above scheme where there is only one level, and hence no derivatives are used [8], [6].

4.2.1. *Conditions for Accessibility and Perfect Security.* Next, we want to consider whether the scheme defined above meets the requirements for accessibility and perfect security. Let $V = \{u_1, \ldots, u_{|V|}\} \subset U$ and assume that

$$\begin{aligned} u_1, \ldots, u_{l_0} &\in U_0 \\ u_{l_0+1}, \ldots, u_{l_1} &\in U_1 \\ &\vdots \qquad \textit{where } 0 \leq l_0 \leq \cdots \leq l_m = |V| \\ u_{l_{m-1}+1}, \ldots, u_{l_m} &\in U_m \end{aligned}$$

Say that V is *authorized* if and only if $l_i \geq k_i$ for all $0 \leq i \leq m$.

Let $\mathbf{r} : \mathbb{F} \to \mathbb{F}^k$ be a function defined as $\mathbf{r}(x) = (1, x, x^2, \ldots, x^{k-1})$. The share that is distributed to the participants $u \in U_i$ is $\sigma(u) = \mathbf{r}^{(k_{i-1})}(u) \cdot \mathbf{a}$, where $\mathbf{a}$ is the vector of coefficients of $P(x)$. Hence, when all participants combine their shares the system they want to solve is $M_V \mathbf{a} = \boldsymbol{\sigma}$ where M_V is written by rows as

$$\begin{aligned} M_V = (&\mathbf{r}(u_1), \ldots, \mathbf{r}(u_{l_0}); \\ &\mathbf{r}^{(k_0)}(u_{l_0+1}), \ldots, \mathbf{r}^{(k_0)}(u_{l_1}); \\ &\vdots \\ &\mathbf{r}^{(k_{m-1})}(u_{l_{m-1}+1}), \ldots, \mathbf{r}^{(k_{m-1})}(u_{l_m})) \end{aligned}$$

where

$$\sigma = (\sigma(u_1), \sigma(u_2,), \ldots, \sigma(u_{l_m}))^T .$$

Say a matrix is *regular* if its determinant is nonzero in $\mathbb{F}$. Tassa proves that if $0 \in U_0$ and for any minimal subset $V \in \Gamma$ the corresponding square coefficient matrix M_V is regular, then the accessibility and perfect security conditions for the secret sharing scheme hold.

4.2.2. *Random Allocation of Participant Identities.* Next we analyze strategies of allocating the identities of the participants. The first strategy of allocating participant identities is the random one, where

$$\Pr(U = W) = \frac{1}{\binom{q-1}{n}} \qquad \forall W \subset \mathbb{F}\backslash\{0\} \ , \ |W| = n.$$

If we assume the above random allocation of participant identities and if V is a randomly selected subset from 2^U, then if $V \in \Gamma$ we have

$$\Pr(H(S|\sigma(V)) = 0) \geq 1 - \epsilon,$$

while otherwise

$$\Pr(H(S|\sigma(V)) = H(S) \geq 1 - \epsilon$$

where

$$\epsilon = \frac{(k-1)(k-1)}{2(q-k)}.$$

4.2.3. *Monotone Allocation of Participant Identities.* Next we see an allocation method that guarantees both accessibility and perfect security if the field $\mathbb{F}$ is of a sufficiently large prime order q.

For every $0 \leq i \leq m$ we define $n_i = |\cup_{j=0}^{i} U_i|$ and let $n_{-1} = 0$. In Lemma 4.2.1 the basic lower bound for q that guarantees the two aforementioned conditions are proved.

Lemma 4.2.1. *Let (**k**,n) be a hierarchical threshold secret sharing problem and assume that the participants in U are assigned identities in $\mathbb{F}_q$ in a monotone manner. Furthermore, if we assume that $N = \max U$ and that*

$$2^{-k} \cdot (k+1)^{(k+1)/2} \cdot N^{(k-1)k/2} < q = |\mathbb{F}|$$

then the HTSS satisfies the accessibility and perfect security conditions.

The next theorem uses the bound from the Lemma 4.2.1. Using a more delicate analysis gives us a better bound:

Theorem 4.2.1. *Under the conditions of Lemma 4.2.1 the HTSS satisfies the accessibility and perfect security conditions provided that*

$$\alpha(k) N^{(k-1)(k-2)/2} < q = |\mathbb{F}|$$

where $\alpha(k) := 2^{-k+2} \cdot (k-1)^{(k-1)/2} \cdot (k-1)!$.

4.3. **Ideal Scheme for the Disjunctive Hierarchical Secret Sharing Problem.** The requirement in Equation 1 is what we call a *conjunction* of the threshold conditions. In another version of the problem we consider a *disjunction* of the threshold conditions, where

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

Tassa shows that the ideality of the disjunctive HTASs follows immediately from the ideality of the conjuctive ones. Furthermore, he gives the description of an ideal scheme that doesn't have the difficulties found in previous solutions [2], [7] .

The scheme is as follows:

1. The dealer selects a random polynomial $P(x) \in \mathbb{F}_{k-1}[x]$ where
$$P(x) = \sum_{i=0}^{k-1} a_i x^i \quad \text{and} \quad a_{k-1} = S. \tag{2}$$
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 $P^{(k-k_i)}(u)$ instead of the $P^{(k_{i-1})}(u)$ that he was getting in the original scheme.

The simple idea behind the allocation in the last step is that given $V \subset U$, its threshold will be determined by its lowest participant. If we assume that the lowest participant in V is from level U_i then all the participants in V will have shares with derivatives of order $k - k_i$ or higher. This means that all the equations that correspond to those shares involve the k_ith coefficients of $P(x)$ as unknowns. Therefore, we must have at least k_i participants in order to have a sufficient number of equations. Finally, concerning the allocation of participant identities in order to achieve accessibility and perfect

security, the random and monotone allocations that have been described work fine for this modified scheme, as shown by Tassa in the paper [8].

5. Multipartite Secret Sharing by Bivariate Interpolation

5.1. **Terminology and Results Overview.** The final paper we review is *Multipartite Secret Sharing by Bivariate Interpolation* by Tassa and Dyn. The authors study three types of multipartite access structures: *compartmented*, hierarchical threshold, and a new type of compartmented. Furthermore, they propose an ideal secret sharing scheme for these types based on *bivariate interpolation*.

The introduction of a second dimension may create the same hierarchical effect as derivatives and Birkhoff interpolation were shown to do in [8]. Letting $\mathbb{F}$ be a finite field of sufficiently large size q, the secret $S \in \mathbb{F}$ is encoded by the coefficients of an unknown bivariate polynomial $P(x, y) \in \mathbb{F}[x, y]$. The dealer distributes the shares to each participant $u_i \in U$ which are essentially points $(x_i, y_i) \in \mathbb{F}^2$.

We want the authorized subsets to be able to recover $P(x, y)$ while the unauthorized subsets will not be able to gain any information about the secret. Bivariate interpolation is suitable for multipartite settings because we can associate each compartment with a different line in the plane.

In order to prove that a given scheme realizes perfectly some access structure Γ, we want to prove two things. Let V be some subset of U and M_V is the sub-matrix of M that consists of all rows of M with labels in V. We first show that if V is a minterm, then with high probability $\mathbf{t} \in \text{row}(M_V)$. The vectors associated with the members of V span the target vector $\mathbf{t}$ with high probability so V may reconstruct the secret. The matrices M_V will be square for a minterm V, so we just have to show that their determinant is non-zero. We then show that if V is a maximal unauthorized subset then with high probability $\mathbf{t} \notin \text{row}(M_V)$. This is proven by augmenting M_V with the additional row $\mathbf{t}$ and showing that the result is a matrix of full rank. Since this matrix will always be square, with high probability it has a non zero determinant. This proves that V will not gain any information about the secret.

We define two types of compartmented access structures.

Definition 5.1.1 (Compartmented access structure with lower bounds (CASLB))**.** *Let $t_i \in \mathbb{N}$, $1 \leq i \leq m$, and let $t \in \mathbb{N}$ be thresholds such that $t \geq \sum_{i=1}^{m} t_i$. Then*

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

defines a compartmented access structure with lower bounds (CASLB).

Such access structures are useful when the size of an authorized subset must be at leat some threshold t. Moreover, we want every compartment to be represented in the authorized subset.

Furthermore, we have compartmented access structures with upper bounds:

Definition 5.1.2 (Compartmented access structure with upper bounds (CASUB))**.** *Let $s_i \in \mathbb{N}$, $1 \leq i \leq m$, and let $s \in \mathbb{N}$ be thresholds such that $s \leq \sum_{i=1}^{m} s_i$. Then*

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

defines a compartmented access structure with upper bounds (CASUB).

This kind of access structure is useful when we have the opposite demand: while the size of the authorized subset must be of some threshold, we want to limit the number of participants that represent each compartment.

5.2. **Ideal Secret Sharing for Compartmented Access Structures with Upper Bounds.** In this section we describe a linear secret sharing scheme for access structures with upper bounds. Say we have a secret $S \in \mathbb{F}$, and let x_i, $1 \leq i \leq m$, be distinct random points in $\mathbb{F}$. Define random polynomials P_i over $\mathbb{F}$ by

$$P_i(y) = \sum_{j=0}^{s_i-1} a_{i,j} y^j.$$

Let the secret S be given by

$$S = \sum_{i=1}^{m} \sum_{j=0}^{s_i-1} a_{i,j} y^j L_i(x)$$

where $L_i(x)$ are Lagrange polynomials of degree $m-1$. A secret sharing scheme is defined as follows:

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 $x_i' \notin x_1, \ldots, x_m$, $1 \leq i \leq k$.

This is an ideal scheme since the private shares of all users are taken from the domain of secrets $\mathbb{F}$. Since we are given $k = \sum_{i=1}^{m} s_i - s$ free point values, we need s additional points for full recovery. We cannot use more that s_i points from the line $x = x_i$ because any s_i from that line will fully recover $P_i(y)$ but are useless in recovering $P_j(y)$ for $j \neq i$.

Lemmas 5.2.1 and 5.2.2 prove that the resulting scheme is perfect with high probability with respect to the random selection of points.

Lemma 5.2.1. *If $V \in \Delta$ it may recover the secret S with probability $1 - Cq^{-1}$, where the constant C depends on m, s, and $s_1, \ldots, s_m$.*

Lemma 5.2.2. *If $V \notin \Delta$ it may not learn anything about the secret S with probability $1 - Cq^{-1}$, where the constant C depends on m, s, and $s_1, \ldots, s_m$.*

Using these lemmas, the authors prove the main result on Secret Sharing Scheme 1:

Theorem 5.2.1. *The ideal Secret Sharing Scheme 1 is a perfect scheme that realizes the CASUB with probability $1 - \epsilon$, where $\epsilon = \binom{n+1}{s} Cq^{-1}$ with constant C that depends on m, s, and $s_1, \ldots, s_m$.*

5.3. **Ideal Secret Sharing for Compartmented Access Structures with Lower Bounds.** In this section we describe a linear secret sharing scheme for a CASLB. The construction is a scheme for the *dual access structure* Γ^*.

Definition 5.3.1 (Dual compartmented access structure with upper bounds.)**.** *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 $\sum_{i=1}^{m} r_i \geq r + m - 1$.

Next, define m distinct points $x_1, \ldots, x_m$ in $\mathbb{F}$ and let $P_i(y)$ 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

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

We can now present the secret sharing scheme for the dual access structure Γ^*:

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 her 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 $x'_i \notin x_1, \ldots, x_m$, $1 \leq i \leq k$.

Lemmas 5.3.1 and 5.3.2 prove that the resulting scheme is perfect with high probability with respect to the random selection of points.

Lemma 5.3.1. *If* $V \in \Gamma^*$ *it may recover the secret* S *with probability* $1 - Cq^{-1}$*, where the constant* C *depends on* m*,* r*, and* $r_1, \ldots, r_m$*.*

Lemma 5.3.2. *If* $V \notin \Gamma^*$ *it may not learn anything about the secret* S *with probability* $1 - Cq^{-1}$*, where the constant* C *depends on* m*,* r*, and* $r_1, \ldots, r_m$*.*

The main result proven by Tassa and Dyn regarding the second secret sharing scheme is as follows.

Theorem 5.3.1. *The ideal Secret Sharing Scheme 2 is a perfect scheme that realizes a CASLB with probability* $1 - \epsilon$*, where* $\epsilon = \binom{n+1}{r} Cq^{-1}$ *such that constant* C *depends on* m*,* r*, and* $r_1, \ldots, r_m$*.*

5.4. **Hierarchical Threshold Access Structures.** In this section an ideal secret sharing scheme for the realization of HTASs is proposed. The scheme uses Lagrange interpolation of bivariate polynomials.

5.4.1. *Constructibility and Non-Constructibility Results.* We now want to answer the following question: Given the values of a bivariate polynomial in a set of points in the plane, what is the amount of information that those values reveal about the polynomial?

Theorems 5.4.1 and 5.4.2 allow us to understand how the polynomial can be reconstructed and how when the proper conditions are not met there is no information revealed about the secret. We need some further notation. Say a vector $\mathbf{u}$ *dominates* a vector $\mathbf{v}$, denoted $\mathbf{u} \succeq \mathbf{v}$, if for all $1 \leq i \leq n$ we have that $\sum_{j=1}^{i} u_i \geq \sum_{j=1}^{i} v_i$ [5]. Furthermore, let $\{L_1\}_{1\leq i\leq n}$ be n lines in general position in $\mathbb{F}^2$. Consider a finite subset of points V, none of which is an intersection point, which satisfies

$$V \subset \left(\bigcup_{i=1}^{n} L_i\right) \setminus \left(\bigcup_{1\leq i<j\leq n} L_i \cap L_j\right).$$

We say this subset is of *type* $\mathbf{v} \in \mathbb{N}^n$, where $\mathbf{v}$ is such that $0 \leq v_1 \leq v_2 \leq \cdots \leq v_n$, if there is a permutation π of $(1, \ldots, n)$ such that $|V \cap L_{\pi(i)}| = v_i$ for all i, $1 \leq i \leq n$.

Theorem 5.4.1. *Let $\mathbb{F}$ be a finite field of size q and n be a natural number such that $q > C_n := \sum_{k=3}^{n} k^{k+2}$. Let:*

- *$\{L_i\}_{1\leq i\leq n}$ be n lines in general position in $\mathbb{F}^2$ none of which go through $(0,0)$.*
- *V be a randomly selected set of points on those lines, none of which is an intersection point, and let $\boldsymbol{v}$ be the type of that set.*
- *$P(x,y) = \sum_{0\leq i+j\leq n-1} a_{i,j}x^iy^j$ be a polynomial of degree (at most) $n-1$ in $\mathbb{F}[x,y]$ and $P|_V$ be the values of P in the points of V*

Then if $\boldsymbol{v} \succeq (1, 2, \ldots, n)$ the set of values $P|_V$ determines the polynomial P with probability at least $1 - C_n q^{-1}$.

Theorem 5.4.2. *Let*

- *$\{L_i\}_{1\leq i\leq n}$ be n lines in general position in $\mathbb{F}^2$,*
- *V be a set of points on those lines, none of which is an intersection point of type $\boldsymbol{v} \not\succeq (1, 2, \ldots, n)$*
- *$P(x,y) = \sum_{0\leq i+j\leq n-1} a_{i,j}x^iy^j$ be a polynomial of degree (at most) $n-1$ in $\mathbb{F}[x,y]$ and $P|_V$ be the values of P in the points of V,*
- *S be a random linear combination of the coefficients of P.*

Then $P|_V$ does not reveal any information on S with probability at least $1 - q^{-1}$.

5.4.2. *Hierarchical Threshold Access Structures.* We are now ready to present the secret sharing scheme for hierarchical access structures using bivariate Lagrange interpolation. The added dimension achieves the same hierarchical effect as the derivatives in the Birkhoff interpolation based scheme as proposed in [8].

Let $\{L_j\}_{1\leq j\leq n}$ be $n := k_m$ lines in general position in $\mathbb{F}^2$, none of which goes through $(0,0)$. Let $\{w_{i,j}\}_{1\leq i+j\leq n-1}$ be public values selected randomly from $\mathbb{F}$. Finally, let $P(x,y) = \sum_{0\leq i+j\leq n-1} a_{i,j}w_{i,j}$ be a random polynomial in $\mathbb{F}_{n-1}[x,y]$ whose coefficients are selected such that $S = \sum_{0\leq i+j\leq n-1} a_{i,j}w_{i,j}$.

Secret sharing scheme 3:

1. Each participant from level C_i is identified by a public point $L_{k_i} \setminus \left(\bigcup_{\substack{1 \leq j \leq n \\ j \neq k_i}} L_j \right)$ and her private share will be the value of P at that point.
2. We publish the value of P at:
   - k_{i-1} additional points on L_{k_i}, $2 \leq i \leq m$
   - j points on L_j for all $j \in \{1, 2, \ldots, n\} \setminus \{k_i : \ 1 \leq i \leq m\}$.

Theorem 5.4.3. *The ideal Secret Sharing Scheme 3 is a perfect scheme that realizes the HTAS with probability at least* $1 - C_n q^{-1}$*, where* $C_n := \sum_{k=3}^{n} k^{k+2}$.

6. Conclusions

We were able to characterize all ideal WTASs as either a HTAS, a TPAS, or a composition of two ideal WTASs. Furthermore, we presented an ideal perfect hierarchical threshold secret sharing scheme. We saw that adding a second dimension to the interpolation method we gained the ability to associate different compartments with different lines in the plane. Research has already been done in extending bivariate interpolation to multivariate interpolation on flats in several dimensions [4]. This way, it might be possible to design secret sharing schemes for a wide array of interesting access structures.

References

[1] Amos Beimel, Tamir Tassa, and Enav Weinreb: Characterizing Ideal Weighted Threshold Secret Sharing, *SIAM Journal of Discrete Math*, 22(1) (2008), pp. 360-397.

[2] Ernest F. Brickell: Some Ideal Secret Sharing Schemes, *Advances in Cryptology - EUROCRYPT '89* (1990), pp. 468-475.

[3] Ronald Cramer, Ivan Damgård, and Jesper Buus Nielsen: Multiparty Computation, an Introduction, *Contemporary Cryptology*, part of the series Advanced Courses in Mathematics-CRM Barcelona, Birhäuser Basel (2005), pp. 41-81.

[4] C. de Boor, N. Dyn, & A. Ron: Polynomial interpolation to data on flats in $\mathbb{R}^d$, *Journal of Approximation Theory*, 105 (2000), pp. 313-343.

[5] 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.

[6] A. Shamir: How to Share a Secret, *Communications of the ACM*, 22 (1979), pp. 612-613.

[7] G.J. Simmons: How to (really) share a secret, *Advances in Cryptology - CRYPTO 88, LNCS*, 403(1990), 390-448.

[8] Tamir Tassa: Hierarchical Threshold Secret Sharing, *Journal of Cryptography*, 20 (2007), pp. 237-264.