Disjunctive Multi-Level Secret Sharing

Mira Belenkiy
Brown University
Providence, RI 02912 USA
mira@cs.brown.edu

January 11, 2008

Abstract

A disjunctive multi-level secret sharing scheme divides users into different levels. Each level L is associated with a threshold t_L, and a group of users can only recover the secret if, for some L, there are at least t_L users at levels 0....L in the group. We present a simple ideal disjunctive multi-level secret sharing scheme – in fact, the simplest and most direct scheme to date. It is the first polynomial-time solution that allows the dealer to add new users dynamically. Our solution is by far the most efficient; the dealer must perform $O(t)$ field operations per user, where t is the highest threshold in the system. We demonstrate the simplicity of our scheme by extending our construction into a distributed commitment scheme using standard techniques.

Keywords Multi-level secret sharing, hierarchical secret sharing, threshold cryptography

1 Introduction

Secret sharing is one of the most fundamental primitives in cryptography. A dealer gives shares of a secret to a group of users $\mathcal{U}$. An access structure $\Gamma \subseteq \mathcal{P}(\mathcal{U})$ defines the sets of users that are authorized to learn the secret if they work together. A secret sharing scheme is a perfect realization of Γ if $\forall A \in \Gamma$, the users in A can always reconstruct the secret and $\forall B \notin \Gamma$, the users in B collectively cannot learn anything about the secret, in the information-theoretic sense.

Shamir [Sha79] and Blakley [Bla79] introduced the idea of threshold secret sharing. In a threshold access structure with threshold t, any group of t or more users is authorized to learn the secret. A multi-level access structure is a common generalization that appears in the literature. Each user is assigned to a level. Users at lower levels are more important than users at higher levels. Each level L is associated with a threshold t_L such that $t_0 < t_1 < \ldots < t_n$. There are two types of multi-level access structures. Simmons [Sim88] introduced the disjunctive multi-level access structure: a group of users can reconstruct the secret if the group contains at least t_L users at levels 0....L for *some* level L. Tassa [Tas04] introduced the conjunctive multi-level access structure: a group of users can reconstruct the secret if there are at least t_L users at levels 0....L for *every* level L.

There are several ways to compare secret sharing schemes. The most obvious is dealer efficiency and user efficiency; these are, respectively, how quickly the dealer computes shares and how quickly an authorized set of users reconstructs the secret. Another criterion is how large a share a user must store compared to the size of the secret. Given the set of all possible secrets S and the set of

all possible shares T, the information rate ρ of a secret sharing scheme is $\rho = \log|S|/\log|T|$. For example, if the secret is an element of a field $\mathbb{F}_q$, and each share consists of two elements from $\mathbb{F}_q$, the information rate for the scheme is $\rho = 1/2$. An *ideal* secret sharing scheme has information rate 1. The simplicity of a secret sharing scheme is also important. Besides increasing our understanding of this fundamental primitive, simple and direct schemes are easier to compose with other protocols.

Disjunctive access structures are interesting because they are a building block for other ideal access structures. For example, in a weighted threshold access structure, all users are assigned a weight, and a group of users is authorized only if the sum of their weights is above a certain threshold. Beimel et al. [BTW05] show that any ideal weighted threshold access structure is a composition of a disjunctive access structure and a tripartite access structure.

Our Results We construct a simple and efficient ideal disjunctive secret sharing scheme. It is the first polynomial-time scheme that lets the dealer add users to the system at any time. Our scheme is the most efficient to date. The dealer needs to perform $O(t)$ field operations to calculate the shares of a single user, where t is the highest threshold. A group of users needs to perform $O(t^3)$ field operations to reconstruct the secret. The dealer can add users to the system at any time.

Suppose the disjunctive access structure has thresholds $t_0 < t_1 < \ldots < t_n$. To share a secret s, the dealer chooses random coefficients $a_0, \ldots, a_{t-2}$, and sets $a_{t-1} = s$. These coefficients define a polynomial $f = \sum a_i x^i$. The share of user u at level L is simply $f^{(t_n - t_L)}(u)$, the $(t_n - t_L)$th derivative of f evaluated at u. As a result, each user gets a linear equation in terms of the secret coefficients of f. An authorized set of users can work together to solve the system of equations and learn s. Care must be taken in deciding where to evaluate the derivatives. We show that the ids u must be chosen either at random or in monotonically decreasing order by level. We state our construction formally in Section 3.3.

Our scheme is based on interpolating polynomials and their derivatives, also known as Birkhoff interpolation. The Birkhoff interpolation problem takes as input a sequence of points on various derivatives of an unknown polynomial: $y_i = f^{(d_i)}(u_i)$. The goal is to calculate the polynomial f. There is no known algorithm for solving an arbitrary Birkhoff interpolation problem; in fact, some instances have multiple solutions, while others have none. For many cases, determining the number of solutions is an open problem. However, there are a few known necessary and sufficient conditions. Tassa [Tas04] shows that these conditions can be leveraged to create a conjunctive secret sharing scheme.

Prior Work The earliest disjunctive secret sharing scheme is due to Simmons [Sim88]. However, his solution is not ideal. It is also inefficient because the dealer needs to find a set of points on a sequence of nested hyperplanes that meet some difficult to satisfy conditions. Brickell [Bri89] shows how to do this for access structures with a small number of levels; the dealer runs in exponential time in the number of levels and linear time in the size of the field.

Brickell [Bri89] also constructs an ideal disjunctive secret sharing scheme, which Shoup [Sho93] subsequently shows runs in *expected* polynomial-time. The dealer chooses a different polynomial for each level, and gives a user u at level L the point $f_L(u)$. By carefully selecting which ids u to use, Brickell ensures that any authorized set of users can reconstruct the secret. Brickell's solution allows the dealer to add new users dynamically. However, there are two major drawbacks to his scheme. First of all, it only works for secrets in $GF(q^\beta)$, where β is a function of the number of levels in the access structure and the highest threshold. Thus the domain of the secret depends on the access structure. Secondly, Brickell's claimed result takes exponential time. The bottleneck

occurs when the dealer must choose an irreducible polynomial over $GF(q)$. Using Shoup's guess-and-check algorithm [Sho93], it takes an expected $O(\beta^2 \log \beta + \beta \log q)$ field operations to find this polynomial.

Ghodosi, Pieprzyk and Safavi-Naini [GPSN98] construct an ideal polynomial-time disjunctive secret sharing scheme that only works for small numbers of users. It is impossible to add new users to the system on the fly. We briefly explain the difficulty with their scheme: The dealer constructs a sequence of distinct polynomials $f_0, f_1, \ldots, f_n$. A user u at level L learns the point $f_L(u)$. The polynomials are constructed in such a way that $f_L(u) = f_{L+1}(u) = \cdots = f_n(u)$. Therefore, users at lower levels can help interpolate higher level polynomials, but not vice versa. In general, it takes t points to interpolate a polynomial of degree $t-1$. In this scheme, the degree of polynomial f_L depends on the number of users at levels $0...L-1$, because that is the only way to ensure that f_L is consistent with the shares of those users. Since the degree of f_L can be arbitrarily high depending on the number of users, t_L users at levels $0...L$ might not be able to reconstruct the secret. Ghodosi et al. get around this by emphasizing that they create $(t_L, N_L)_{T_L}$ extensions for each level of the access structure: there are N_L users on level L, and while less than t_L users at levels $0...L$ cannot learn the secret, $T_L \geq t_L$ users are guaranteed to be able to do so. Finally, though Ghodosi et al. do not give an efficiency analysis, it is easy to see that their scheme is less efficient than ours. Computing all of the f_L requires solving n systems of linear equations, with each system having up to T_n variables. Using Gaussian elimination, this takes $O(nT_n^3)$ field operations. Their reconstruction time is slightly faster than ours, taking $O(T_n)$ time because the users perform Lagrange interpolation.

Tassa [Tas04] constructs an ideal disjunctive secret sharing scheme that can be computed in polynomial-time. Tassa shows that the dual of a disjunctive access structure Γ with thresholds t_L is a conjunctive access structure Γ^* with thresholds $t_L^* = |\{u : \mathcal{L}(u) \leq L\}| - t_L + 1$. Tassa [Tas04] and Tassa and Dyn [TD06] present two different polynomial-time ideal conjunctive secret sharing schemes. It is possible to use either one to create an ideal monotone span program for Γ^* (see [KW93] for definition of monotone span programs). Using Fehr's [Feh99] transform, we can compute an ideal monotone span program that realizes Γ in $O(|\mathcal{U}|^3)$ field operations. We can then extract the share of each user from this program. Our disjunctive scheme is more efficient than the above scheme because the dealer performs $O(t|\mathcal{U}|)$ operations in total ($O(t)$ per user). Our scheme lets the dealer add new users dynamically, while Tassa's does not because the thresholds of Γ^* depend on $|\mathcal{U}|$. Finally, our scheme is much simpler and more direct: all the dealer has to do is compute a point on the derivative of a polynomial.

Our scheme uses techniques developed by Tassa [Tas04]. The conjunctive secret sharing scheme that Tassa presents is based on the Birkhoff interpolation problem. Users learn a point either on a polynomial or its derivative. We present a detailed description of Tassa's conjunctive scheme in Section 3.2. Our contribution is to show that it is possible to apply this method directly to disjunctive secret sharing, without using a conjunctive scheme as an intermediary. However, our security proofs show that there is a strong connection between conjunctive and disjunctive secret sharing. We demonstrate the simplicity of our scheme by extending it to verifiable secret sharing using standard techniques developed by Pedersen [Ped92]. We can do this because our scheme is based on polynomial interpolation. (Tassa's [Tas04] disjunctive scheme can also be made verifiable).

We go over some standard notation in Section 2. Then we show how to construct our scheme in Section 3. In Section 4, we show how to add verifiability without losing information-theoretic security.

2 Definitions

We begin with a quick note on notation. If A is a set, then we write $|A|$ to indicate the number of elements in A. Let q be a prime; then $\mathbb{F}_q$ is a finite field of order q. Let a, b, c be vectors, where $a = (a_0, \ldots, a_n)$ and b and c are similarly defined. Then $a \cdot b = a_0 b_0 + \cdots + a_n b_n$. We introduce a new vector operation $a \diamond b = (a_0, b_0, \ldots, a_n b_n)$. We note that $(a \diamond b) \cdot c = a \cdot (b \diamond c)$. Finally, if D is a matrix, $D \cdot a$ is the standard matrix times vector multiplication. (We use the $\cdot$ to avoid confusion when the matrix and vector have complicated names).

Now we review some standard definitions related to secret sharing.

Definition 2.1 (Access structure)**.** *Let $\mathcal{U}$ be a set of users. An access structure $\Gamma \subseteq \mathcal{P}(\mathcal{U})$ must meet the following two conditions: (1)* monotonicity: *if $A \in \Gamma$ and $A \subseteq B$ then $B \in \Gamma$ and (2)* non-triviality: *if $A \in \Gamma$ then $|A| > 0$.*

We say that every set $A \in \Gamma$ is *authorized* and every set $B \notin \Gamma$ is *unauthorized*.

Definition 2.2 (Minterm)**.** *Let Γ be an access structure. We say that $A \in \Gamma$ is a minterm if $\forall u \in A : A - \{u\} \notin \Gamma$.*

There are many possible access structures. The most well known is the threshold access structure introduced by Shamir [Sha79] and Blakley [Bla79].

Definition 2.3 (Threshold access structure)**.** *We say that Γ is a threshold access structure corresponding to threshold t if $\Gamma = \{A \subseteq \mathcal{U} : |A| \geq t\}$.*

In a multi-level access structure, all users are assigned to a level using some function $\mathcal{L} : \mathcal{U} \to \mathbb{Z}$ (each user is assigned to exactly one level, but multiple users can be assigned to the same level). Each level L is associated with a threshold t_L such that $t_0 < t_1 < \ldots < t_n$. In the case of the conjunctive multi-level access structure, the secret can only be recovered if for *every* level L, there are at least t_L users at levels $0...L$. For a disjunctive multi-level access structure, the secret can be recovered if for *some* level L, there are at least t_L users at level $0...L$. Formally:

Definition 2.4 (Conjunctive multi-level access structure)**.** *We say that Γ is a conjunctive multi-level access structure corresponding to a sequence of thresholds $t_0 < t_1 < \ldots < t_n$ and level assigning function $\mathcal{L}$ if $\Gamma = \{A \subseteq \mathcal{U} : \quad \forall L \in [0, n]$ it holds that $|\{u \in A : \mathcal{L}(u) \leq L\}| \geq t_L\}$*

Definition 2.5 (Disjunctive multi-level access structure)**.** *We say that Γ is a disjunctive multi-level access structure corresponding to a sequence of thresholds $t_0 < t_1 < \ldots < t_n$ and level assigning function $\mathcal{L}$ if $\Gamma = \{A \subseteq \mathcal{U} : \quad \exists L \in [0, n]$ such that $|\{u \in A : \mathcal{L}(u) \leq L\}| \geq t_L\}$*

Sometimes, users can be assigned to different levels depending on the context. To handle this, we write $A(\mathcal{L})$ to indicate a set of users A whose levels are calculated using level assignment function $\mathcal{L}$. Thus, for a multi-level access structure, we would write that $A(\mathcal{L}) \in \Gamma$. It is quite possible that for the same A, there exists another level assignment function $\mathcal{L}'$ such that $A(\mathcal{L}') \notin \Gamma$.

To realize an access structure, we need to construct a secret sharing scheme. There are two types of players: users and the dealer. The dealer chooses a secret at random from some domain S and distributes shares of the secret to each user.

Definition 2.6 (Secret Sharing Scheme)**.** *Suppose there are n users in the system. Let S be the domain of the secret. A dealer takes a secret $s \in S$, chooses a random string r, and uses the function $(s_1, s_2, \ldots, s_{|A|}) \leftarrow \mathsf{Share}_r(s, A, \mathcal{L}, \Gamma)$ to calculate the shares of users A when they are assigned to levels according to $\mathcal{L}$. We say that a secret sharing scheme is* dynamic *if the dealer can invoke* Share *multiple times with the same randomness r but different sets of users and still get consistent sharings of the same secret.*

A secret sharing scheme is a perfect realization of an access structure Γ if the following two conditions hold: (1) Correctness – regardless of the secret s and the random choices taken by the dealer, $\forall A \in \Gamma$, the users in A can always reconstruct s. (2) Privacy – $\forall B \notin \Gamma$ the shares of B are information theoretically independent of the secret.

3 Constructions

We begin by presenting some previous constructions. For completeness, we start with Shamir's [Sha79] construction for a threshold secret sharing scheme in Section 3.1. Then we describe Tassa's [Tas04] secret sharing scheme in Section 3.2. Finally, in Section 3.3, we present our construction and prove it is secure.

All of the following constructions are based on polynomial interpolation. The dealer picks a polynomial, and the share of a user with id u is the polynomial, or a derivative of it, evaluated at u. As a result, we have to assume that the ids are distinct, the dealer knows every user's id, and each user knows his own id. Since all operations will be done over a field $\mathbb{F}_q$ of prime order, the ids must be elements of this field. Shamir's secret sharing scheme allows for selecting arbitrary field elements. Tassa's conjunctive secret sharing scheme and our disjunctive secret sharing scheme have some restrictions on how the ids may be chosen, which we will indicate in the constructions.

3.1 Shamir's Threshold Secret Sharing Scheme

Shamir [Sha79] shows how to share a secret for a threshold access structure. Suppose the threshold is t. To share a secret $s \in \mathbb{F}_q$, the dealer chooses a sequence of values $a_1, a_2, \ldots, a_{t-1}$ at random and sets $a_0 = s$. These values define the polynomial $f(x) = \sum_{i=0}^{t-1} a_i x^i$. The share of a user with id u is $f(u)$. Any group of users A, such that $|A| > t$, can reconstruct the secret using Lagrange interpolation:

$$s = f(0) = \sum_{u \in A} f(u) \prod_{\substack{v \in A \\ v \neq u}} \frac{u}{u - v}$$

Let us briefly reinterpret Shamir's construction from the point of view of solving a system of linear equations. The sequence of values $a_0, a_1, \ldots, a_{t-1}$ constitute the t unknowns. Each user u learns a *linear* equation in terms of these variables, where the u^i constitute the known coefficients. If there are t users, then they possess t equations with t variables. The users can solve this system of equations if and only if the equations are linearly independent. Using the coefficients $1, u, u^2, \ldots, u^{t-1}$ ensures that the equations are linearly independent for *any* choice of user ids.

3.2 Tassa's Conjunctive Secret Sharing Scheme

Tassa [Tas04] constructs a conjunctive multi-level secret sharing scheme based on the Birkhoff interpolation problem. Suppose the sequence of thresholds is $t_0 < t_1 < \ldots < t_n$, and let $t = t_n$. To share a secret $s \in \mathbb{F}_q$, the dealer chooses a sequence of values $a_1, a_2, \ldots, a_{t-1}$ and sets $a_0 = s$. These values define the polynomial $f(x) = \sum_{i=0}^{t-1} a_i x^i$. The share of user u at level $L = \mathcal{L}(u)$ is $f^{(t_{L-1})}(u)$. To reconstruct the secret, the users solve a system of linear equations to learn *all* of the a_i, including $s = a_0$.

Not all ids lead to a valid sharing of the secret. Tassa shows under what conditions derivatives of f are guaranteed to result in linearly independent equations:

Theorem 3.1 ([Tas04])**.** *Let Γ be a conjunctive access structure, with maximum threshold t, and let the underlying finite field be $\mathbb{F}_q$. Assume that the users in $\mathcal{U}$ were assigned ids in an increasing monotone manner, such that $\forall u, v \in \mathcal{U} : u < v \Leftrightarrow \mathcal{L}(u) < \mathcal{L}(v)$. Let $N = \max\{u \in \mathcal{U}\}$. Then the above secret sharing scheme is a perfect realization of Γ as long as:*

$$2^{-t} \cdot (t+1)^{(t+1)/2} \cdot N^{(t-1)t/2} < q$$

Theorem 3.2 ([Tas04])**.** *Let Γ be a conjunctive access structure, with maximum threshold t, and let the underlying finite field be $\mathbb{F}_q$. Assume a random allocation of user identities. For a randomly choosen $A \subseteq \mathcal{U}$, (1) if $A \in \Gamma$, then the probability that the shares given to A let it reconstruct the secret is at least $1 - \nu(t, q)$ and (2) if $A \notin \Gamma$, then the probability that the shares reveal no information about the secret in the information theoretic sense is at least $1 - \nu(t, q)$, where:*

$$\nu(t, q) = \frac{(t-2)(t-1)}{2(q-t)}$$

We reinterpret Tassa's secret sharing scheme in terms of vector operations. Let $c : \mathbb{F}_q \to \mathbb{F}_q^t$ be defined as $c(x) = (1, x, x^2, \ldots, x^{t-1})$. We write $c^{(i)}(x)$ to denote the ith derivative of that vector. The share of user u at level L can be written as $c^{(t_{L-1})}(u) \cdot \mathbf{a}$, where $\mathbf{a} = (a_0, a_1, \ldots, a_{t-1})$. Thus, a user a level $L = 0$ gets information about a_0, but a user at a higher level only learns a linear equation in terms of $(a_{t_{L-1}}, \ldots, a_{t-1})$ (because taking the (t_{L-1})th derivative zeroes-out the other coefficients of c).

An authorized set of users can reconstruct the secret by solving a system of linear equations. Suppose we have a set of m users $A(\mathcal{L}) = \{u_0, u_1, \ldots, u_m\}$. We put the users in order by level, so that $\mathcal{L}(u_i) \leq \mathcal{L}(u_j)$, for all $i < j$. We create a coefficient matrix $C_{A(\mathcal{L})}$ corresponding to A, where the ith row of $C_{A(\mathcal{L})}$ is the row vector $c^{(t_{L-1})}(u_i)$. Let σ be the vector of shares known by $A(\mathcal{L})$. To learn the secret, the users need to solve the equation $C_{A(\mathcal{L})} \cdot \mathbf{a} = \sigma$. Suppose $A(\mathcal{L})$ is a minterm of Γ. Tassa [Tas04] shows that in that case, under certain conditions, $C_{A(\mathcal{L})}$ has a non-zero determinant, which means that the users can find a *unique* solution for $\mathbf{a}$ and recover the secret.

Corollary 3.3 ([Tas04], from the proof of Lemma 2)**.** *Let Γ be a conjunctive access structure, with maximum threshold t, and let the underlying finite field be $\mathbb{F}_q$. Assume that the users in $\mathcal{U}$ were assigned ids in an increasing monotone manner, such that $\forall u, v \in \mathcal{U} : u < v \Leftrightarrow \mathcal{L}(u) < \mathcal{L}(v)$. Let $N = \max\{u \in \mathcal{U}\}$. Furthermore, $2^{-t} \cdot (t+1)^{(t+1)/2} \cdot N^{(t-1)t/2} < q$. Then for every $A(\mathcal{L})$ that is a minterm of Γ, $\det(C_{A(\mathcal{L})}) \neq 0$*

Corollary 3.4 ([Tas04], from the proof of Theorem 3)**.** *Let Γ be a conjunctive access structure, with maximum threshold t, and let the underlying finite field be $\mathbb{F}_q$. Assume a random allocation of user identities. Then for every $A(\mathcal{L})$ that is a minterm of Γ, the probability that $\det(C_{A(\mathcal{L})}) \neq 0$ is at least $1 - \nu(t, q)$, where $\nu(t, q) = ((t-2)(t-1))/2(q-t)$.*

3.3 New Disjunctive Multi-Level Secret Sharing Scheme

The share of user u at level L will be a linear equation of t_L variables, one of which will be the secret. We choose the coefficients for these equations using Tassa's technique of taking derivatives: user u at level L will receive $f^{(t-t_L)}(u)$, where t is the highest threshold. Using a reduction to conjunctive multi-level secret sharing, we will show that any authorized set of users learns a sufficient number of linearly independent equations to reconstruct the secret.

Construction 3.5. *Suppose the sequence of thresholds is $t_0 < t_1 < \ldots < t_n$, and let $t = t_n$. To share a secret $s \in \mathbb{F}_q$, the dealer chooses a random sequence of values $a_0, a_1, \ldots, a_{t-2}$ and sets $a_{t-1} = s$. The sequence of values defines the polynomial $f(x) = \sum_{i=0}^{t-1} a_i x^i$. The share of user u at level $L = \mathcal{L}(u)$ is $f^{(t-t_L)}(u)$. The ids u can be chosen either at random or in monotonically decreasing order. Any authorized set of users can solve the system of linear equations to learn $s = a_{t-1}$.*

Thus, users at level L get an equation in terms of t_L variables: $a_{t-t_L}, \ldots, a_{t-1}$, where $a_{t-1} = s$ is the secret.

Theorem 3.6. *Let Γ be a disjunctive access structure, with maximum threshold t, and let the underlying finite field be $\mathbb{F}_q$. Assume that the users are assigned ids in a decreasing monotone manner, such that $\forall u, v \in \mathcal{U} : u > v \Leftrightarrow \mathcal{L}(u) < \mathcal{L}(v)$. Let $N = \max\{u \in \mathcal{U}\}$. Then the secret sharing scheme in Construction 3.5 is a perfect realization of Γ, as long as:*

$$2^{-t} \cdot (t+1)^{(t+1)/2} \cdot N^{(t-1)t/2} < q$$

Theorem 3.7. *Let Γ be a disjunctive access structure, with maximum threshold t, and let the underlying finite field be $\mathbb{F}_q$. Assume a random allocation of user identities. For a randomly choosen $A \subseteq \mathcal{U}$, (1) if $A \in \Gamma$, then the probability that the shares given to A let it reconstruct the secret is at least $1 - \nu(t, q)$ and (2) if $A \notin \Gamma$, then the probability that the shares reveal no information about the secret in the information theoretic sense is at leat $1 - \nu(t, q)$, where:*

$$\nu(t, q) = \frac{(t-2)(t-1)}{2(q-t)}$$

We reinterpret our disjunctive scheme in terms of vector operations. Let $d : \mathbb{F}_q \to \mathbb{F}_q^t$ be defined as $d(x) = (1, x, x^2, \ldots, x^{t-1})$. We write $d^{(i)}(x)$ to denote the ith derivative of that vector. The share of user u at level L can be written as $d^{(t-t_L)}(u) \cdot \mathbf{a}$, where $\mathbf{a} = (a_0, a_1, \ldots, a_{t-1})$. Suppose we have a set of m users $A(\mathcal{L})$ and the highest level of user is M. The users might not be able to recover the entire vector $\mathbf{a}$ because they would have information only about $(a_{t-t_M}, \ldots, a_{t-1})$ (because taking the derivative zeroes-out the other coefficients of d). Let $\mathbf{a}_M$ and $d_M^{(i)}$ be the $t - t_M$ leftmost coefficients of those respective vectors. In this case, each user $u \in A(\mathcal{L})$ at level L can write his share as $d_M^{(t-t_L)}(u) \cdot \mathbf{a}_M$. We order the users in $A(\mathcal{L}) = \{u_0, u_1, \ldots, u_m\}$ by level, so that

$\mathcal{L}(u_i) \geq \mathcal{L}(u_j)$ for all $i < j$. We can then create the coefficient matrix $D_{A(\mathcal{L})}$, where the ith row of $D_{A(\mathcal{L})}$ is $d_M^{(t-t_L)}(u_i)$. Users in $A(\mathcal{L})$ can try to recover $\mathbf{a}_M$ by solving $D_{A(\mathcal{L})} \cdot \mathbf{a}_M = \sigma$, where σ is a vector of their of shares.

Before proving Theorems 3.6 and 3.7, we first prove a few interesting claims that show the link between disjunctive and conjunctive access structures and secret sharing schemes.

Let Γ be a disjunctive multi-level access structure with thresholds $t_0 < t_1 < \ldots < t_n$; we set $t = t_n$. Let $\mathcal{L}$ be some level assignment function. We take an arbitrary set of users $A \subseteq \mathcal{U}$; let M be the highest level of user in $A(\mathcal{L})$. We define $\mathcal{L}'$ as: $\mathcal{L}'(u) = M - \mathcal{L}(u)$. We also define the conjunctive access structure Γ' with thresholds $t'_0 < t'_1 < \ldots < t'_M$, where $t'_M = t_M$ and $\forall 0 \leq L < M : t'_L = t_M - t_{M-L-1}$.

We give some intuition about the above transformation. Suppose $A(\mathcal{L})$ is a minterm of Γ. For every user at level M in $A(\mathcal{L})$, there is a user at level 0 in $A(\mathcal{L}')$. We can calculate a lower bound on the number of users in $A(\mathcal{L})$ at level M; if there is not enough, there will be t_{M-1} users at levels $0...M-1$, thus contradicting the fact that $A(\mathcal{L})$ is a minterm. As a result, we can calculate a lower bound on the number of users at level 0 in $A(\mathcal{L}')$. We can do the same for every level. Due to this property, we were able to chose the thresholds for Γ' in such a way as to ensure that $A(\mathcal{L}')$ is a minterm of Γ'. More importantly, the share that a user u receives for Γ is algebraically related to the share that the user receives for Γ'. We now prove these claims formally:

Claim 3.8. If $A(\mathcal{L})$ is a minterm of Γ then $A(\mathcal{L}')$ is a minterm of Γ'.

Proof. Let $A(\mathcal{L})$ be a minterm of Γ. We need to show that there are at least $t'_M = t_M$ users in $A(\mathcal{L}')$ at levels $0...M$ and $t'_L = t_M - t_{M-L-1}$ users at levels $0...L$ for all $L < M$. Let us begin with level M. We know that $|A| = t_M$ because $A(\mathcal{L})$ is a minterm of Γ. This means that there are exactly $t'_M = t_M$ users in $A(\mathcal{L}')$ at levels $0...M$. The case for levels $L < M$ is also straightforward. If there is a set $B \subset A$ such that $B(\mathcal{L})$ had t_{M-L-1} users at levels $0...M-L-1$ then $B(\mathcal{L}) \in \Gamma$, thus contradicting the fact that $A(\mathcal{L})$ is a minterm of Γ. Therefore, there are at least $t_M - t_{M-L-1} + 1$ users at levels $M - L...M$ in $A(\mathcal{L})$. Applying $\mathcal{L}'$, we see that there are at least $t_M - t_{M-L-1} + 1$ users at levels $0...L$ in $A(\mathcal{L}')$. Ergo, there are at least $t_M - t_{M-L-1}$ users at levels $0...L$ in $A(\mathcal{L}')$. Thus, we have shown that $A(\mathcal{L}') \in \Gamma'$. $A(\mathcal{L}')$ must be a minterm of Γ because any subset of $A(\mathcal{L}')$ would have less than t'_M users at levels $0...M$, so it would be unauthorized. □

Claim 3.9. If $A(\mathcal{L}) \notin \Gamma$ then $A(\mathcal{L}') \notin \Gamma'$.

Proof. Suppose $A(\mathcal{L}) \notin \Gamma$. If M is the highest level of user in $A(\mathcal{L})$, then $|A| < t_M = t'_M$. Since Γ' is a conjunctive access structure, $A(\mathcal{L}') \notin \Gamma'$. □

Recall the pairwise multiplication operator $a \diamond b = (a_0 b_0, \ldots, a_n b_n)$.

Claim 3.10. Let $A(\mathcal{L})$ be a minterm of Γ, and let Γ' be the corresponding conjunctive access structure. If the dealer for Γ and the dealer for Γ' pick the same secret values, then there exists a positive vector $\mathbf{b}$ such that: $D_{A(\mathcal{L})} \cdot \mathbf{a}_M = C_{A(\mathcal{L}')} \cdot (\mathbf{b} \diamond \mathbf{a}_M)$.

Proof. Let $A(\mathcal{L})$ be a minterm of Γ. Let M be the highest level of user in A. The share of user u at level L according to Γ' is $d_M^{(t-t_L)}(u) \cdot \mathbf{a}_M = d_M^{((t-t_M)+(t_M-t_L))}(u) \cdot \mathbf{a}_M$. We can relate $d_M^{(t-t_M)}$ to c (the vector used to calculate shares in Γ') as follows:

$$d_M^{(t-t_M)} = (x^{t-t_M}, \ldots, x^{t-1})^{(t-t_M)} = (1, \ldots, x^{t_M-1}) \diamond \mathbf{b} = c \diamond \mathbf{b}$$

In the above equations, $\mathbf{b}$ is the vector of coefficients that result from calculating a derivative; all of its entries are positive. Using this result, we get that the share of u in Γ is equal to:

$$\begin{aligned} d_M^{(t-t_L)}(u) \cdot \mathbf{a}_M &= d_M^{((t-t_M)+(t_M-t_L))}(u) \cdot \mathbf{a}_M \\ &= (c^{t_M-t_L}(u) \diamond \mathbf{b}) \cdot \mathbf{a}_M \\ &= c^{t_{L'-1}}(u) \cdot (\mathbf{b} \diamond \mathbf{a}_M) \end{aligned}$$

Therefore, if the dealer for Γ' chooses the same vector of secret values as the dealer for Γ, we would have the relation: $D_{A(\mathcal{L})} \cdot \mathbf{a}_M = C_{A(\mathcal{L})} \cdot (\mathbf{b} \diamond \mathbf{a}_M)$. □

Now we will show that in order to prove privacy and correctness, it is sufficient to prove that for any minterm $A(\mathcal{L}) \in \Gamma$, $\det(D_{A(\mathcal{L})}) \neq 0$.

Claim 3.11. If for every minterm $A(\mathcal{L}) \in \Gamma$ it holds that $\det(D_{A(\mathcal{L})}) \neq 0$, then the secret sharing scheme in Construction 3.5 is correct.

Proof. Assume every minterm of Γ has an associated coefficient matrix with non-zero determinant. Let $A(\mathcal{L})$ be a minterm of Γ. Let M be the highest level of user in $A(\mathcal{L})$ and let σ be a vector of shares owned by $A(\mathcal{L})$. We know that $D_{A(\mathcal{L})} \cdot \mathbf{a}_M = \sigma$. Since $A(\mathcal{L})$ is a minterm, $\det(D_{A(\mathcal{L})}) \neq 0$. This means that we can calculate the inverse of $D_{A(\mathcal{L})}$ and learn $\mathbf{a}_M$, which includes the secret $s = a_{t-1}$. Every authorized set of users contains at least one minterm as a subset. The authorized users can recover the secret using the minterm. □

Claim 3.12. If for every minterm $A(\mathcal{L}) \in \Gamma$ it holds that $\det(D_{A(\mathcal{L})}) \neq 0$, then the secret sharing scheme in Construction 3.5 preserves privacy.

Proof. Assume every minterm in Γ has a corresponding coefficient matrix with a non-zero determinant. We will use the phantom user technique introduced by Tassa [Tas04] to prove Claim 3.12. We introduce a phantom user $u_0 \in \mathcal{U}$ and set $\mathcal{L}(u_0) = 0$. No real user will ever get the share assigned to user u_0.

Fix some $A(\mathcal{L}) \notin \Gamma$, and let M be the highest level of user in $A(\mathcal{L})$. For now, assume that $|A| = t_M - 1$. If we let $A_0 = A + \{u_0\}$, then A_0 has t_M users at levels $0...M$, so $A_0(\mathcal{L}) \in \Gamma$. We will show that users A_0 can recover the entire vector $\mathbf{a}_M$. The users can recover $\mathbf{a}_M$ only if the equation $D_{A_0} \cdot \mathbf{a}_M = \sigma$ has a unique solution, which is the case if and only if $\det(D_{A_0}) \neq 0$. This means that the row in D_{A_0} corresponding to u_0 is independent of the rows fcorresponding to users in A. Since u_0 is at the lowest level, it is on the bottom row of D_{A_0}. Therefore, $(0, \ldots, 0, 1) \notin$ row-space(D_A). Thus, the secret $s = a_{t-1}$ is information theoretically independent of the view of A.

Suppose $A_0(\mathcal{L})$ is a minterm. Then, the corresponding matrix D_{A_0} has a non-zero determinant. Let σ be the shares of A_0. We can find a unique solution to the equation $D_{A_0} \cdot \mathbf{a}_M = \sigma$ and learn the entire vector $\mathbf{a}_M$. This means that the secret is independent of the view of A.

However, A_0 might *not* be a minterm of Γ. This is because the addition of u_0 might create a set of t_L users at levels $0...L$, where $L < M$. Therefore, we divide A_0 into two sets of users: A_{low} and A_{high}. A_{low} contains all users at levels $0...L$, while A_{high} contains all users at levels $L+1...M$. A_{low} is a minterm of Γ. (If A_{low} was not a minterm, then we could remove a user from A_{low} and still have t_L users at levels $0...L$. This means we can remove u_0 from A_{low} and still have t_L users at levels $0...L$. In this case, A would be authorized, which is a contradiction.) We divide the vector

of shares σ into σ_{low} and σ_{high} in a similar fashion. Finally, we take the vector of unknown secret values $\mathbf{a}_M$ and divide it into $\mathbf{a}_{low}$ and $\mathbf{a}_{high}$.

We now show that the users in A_0 can solve $D_{A_0} \cdot \mathbf{a} = \sigma$. D_{A_0} is a $t_M \times t_M$ matrix. The bottom t_L rows consist of $t_M - t_L$ columns of zeroes on the left, followed by $D_{A_{low}}$. The top $t_M - t_L$ rows consist of $D_{A_{high}}$. (We draw a diagram of D_{A_0} on the next page). To solve for $\mathbf{a}_M$, we create the augmented matrix $D_{A_0}|\sigma$. Then we perform the following two operations:

Step 1: We perform Gaussian elimination on the bottom rows corresponding to A_{low} to learn $\mathbf{a}_{low}$. We can do this because A_{low} is a minterm of Γ, and therefore, the determinant of $D_{A_{low}}$ is non-zero. Gaussian elimination will result in the identity submatrix in the rightmost t_L columns of those rows.

Step 2: Next, we use the bottom t_L rows of D_{A_0} to completely zero out the rightmost t_L columns of D_{A_0}. This leaves the leftmost $t_M - t_L$ columns untouched, but changes σ_{high} to some σ_1.

Graphically, these two steps result in the following transformation:

$$D_{A_0}|\sigma = \left(\begin{array}{cc|c} D_{A_{high}} & & \sigma_{high} \\ 0 & D_{A_{low}} & \sigma_{low} \end{array}\right) \rightarrow \left(\begin{array}{cc|c} D_{A_{high}} & & \sigma_{high} \\ 0 & I & \mathbf{a}_{low} \end{array}\right) \rightarrow \left(\begin{array}{cc|c} D_{A_1} & 0 & \sigma_1 \\ 0 & I & \mathbf{a}_{low} \end{array}\right)$$

Consider the $(t_M - t_L)$ x $(t_M - t_L)$ matrix D_{A_1}. We get the equation $D_{A_1} \cdot \mathbf{a}_{high} = \sigma_1$. The vector σ_1 is whatever results when we zero out the rightmost columns. The matrix D_{A_1} is an abridgement of the rows corresponding to $D_{A_{high}}$. Essentially, we have transformed the shares of A_{high} from access structure Γ to the shares of some set of users A_1 from some other disjunctive access structure Γ_1. Due to the equation $D_{A_1} \cdot \mathbf{a}_{high} = \sigma_1$, we know that the secret values chosen by the dealer for Γ_1 are $\mathbf{a}_{high}$.

It is easy to see that A_1 is in Γ_1. The users in A_1 are assigned to levels $J...K$ via some (unknown) labeling function $\mathcal{L}_1$. The lowest row of D_{A_1} represents the share of the user at level K. Since D_{A_1} is a $(t_M - t_L) \times (t_M - t_L)$ square matrix, we know the threshold for level K is $t_M - t_L$. Since $|A_1| = t_M - t_L$, $A_1(\mathcal{L}_1) \in \Gamma_1$.

If $A_1(\mathcal{L}_1)$ is a minterm of Γ_1, then $\det(D_{A_1}) \neq 0$ and we can solve for $\mathbf{a}_{high}$. If $A_1(\mathcal{L}_1)$ is not a minterm of Γ_1, then we can keep repeating the reduction we performed on A_0 until we have solved for the entire secret vector $\mathbf{a}_{high}$. Since we can solve for $\mathbf{a}_{high}$ and $\mathbf{a}_{low}$, this means we have recovered the entire vector $\mathbf{a}_M$. As stated earlier, this means the secret is information theoretically independent of view of the users in A.

Finally, we have to consider the possibility that $|A| \neq t_M - 1$. If $|A| > t_M - 1$, then $A(\mathcal{L}) \in \Gamma$. If $|A| < t_M - 1$, we can always augment it until it does have $t_M - 1$ users at levels $0...M$. However, the view of this augmented set of users will still be information theoretically independent of the secret. Therefore, the view of A is also independent of the secret. □

We are now ready to prove that our secret sharing scheme is secure.

Proof of Theorem 3.6. Let Γ be a disjunctive secret sharing scheme. By Claims 3.11 and 3.12, to prove privacy and correctness, all we need to show is that for all minterms $A(\mathcal{L}) \in \Gamma$, $\det(D_{A(\mathcal{L})}) \neq 0$.

Let $A(\mathcal{L})$ be a minterm of Γ, and let Γ' be the corresponding disjunctive access structure. By Claim 3.10, if the dealer for Γ and the dealer for Γ' pick the same secret values, then there exists a positive vector $\mathbf{b}$ such that: $D_{A(\mathcal{L})} \cdot \mathbf{a}_M = C_{A(\mathcal{L}')} \cdot (\mathbf{b} \diamond \mathbf{a}_M)$. If $C_{A(\mathcal{L}')}$ has a non-zero determinant,

then we can solve for $\mathbf{b} \diamond \mathbf{a}_M$. Since $\mathbf{b}$ is a constant positive vector whose values depend solely on the access structure Γ (recall that $\mathbf{b}$ is the coefficients of a derivative), we can recover $\mathbf{a}_M$. Since this is the case, $D_{a(\mathcal{L})}$ must also have a non-zero determinant.

Therefore, $D_{A(\mathcal{L})}$ has a non-zero determinant if $C_{A(\mathcal{L}')}$ has a non-zero determinant, which occurs if all the conditions in Corollary 3.3 hold. We have to ensure that $A(\mathcal{L}')$ is a minterm of Γ', the ids of the users increase monotonically in $\mathcal{L}'$ and that the field is large enough. Since $A(\mathcal{L})$ is a minterm of Γ, by Claim 3.8, $A(\mathcal{L}')$ is a minterm of Γ'. Monotonicity is easy; if we assign users ids in monotonically decreasing order in terms of $\mathcal{L}$, they will be in monotonically increasing order in terms of every possible $\mathcal{L}'$. As far as field size, Tassa's scheme expresses it in terms of N, the highest possible id of user in the system, and t', the highest threshold associated with Γ'. The highest threshold in any Γ' is $t'_M = t_M$ where M is the highest level of authorized user. Therefore, the highest t' is simply t, the highest threshold for Γ. Thus, the lower bound on the size of the field is the same as in Corollary 3.3. □

Proof of Theorem 3.7. The privacy and correctness proof is essentially the same. Once again, we need to prove that $C_{A(\mathcal{L}')}$ has a non-zero determinant. This is true if the the conditions of Corollary 3.4 hold. We've already shown that $A(\mathcal{L}')$ is a minterm of Γ'. Id selection is easy: if we assign ids to all users at random in the disjunctive scheme, then they are equally random as far as Γ' is concerned. We know that the determinant is non-zero with probability at least $1 - \nu(t', q')$. If we take the lower bound for $1 - \nu(t', q')$, for every possible Γ' that arises from an authorized set $A(\mathcal{L}) \in \Gamma$, we will have a lower bound on the probability that users in A can reconstruct the secret. We know that the underlying field size q is the same in all cases. By Corollary 3.4, we see that $1 - \nu(t', q')$ is lower when t' is higher. The highest value for t' is simply t. Therefore, with random id allocation, our disjunctive construction is correct with probability $1 - \nu(t, q)$. □

4 Secret Sharing With a Dishonest Dealer

We want to protect users against a malicious dealer who tries to distribute inconsistent shares. This problem is called distributed commitment. (Verifiable secret sharing is a related problem that deals also with dishonest users). A distributed commitment scheme must have the same propeties of correctness and privacy as a regular secret sharing scheme. However, we add the additional properties of completeness and binding:

Completeness For all secrets, if the dealer follows the distribution protocol, and user u follows the verification protocol, then u accepts his share with probability 1.

Binding Let k be a security parameter. If two authorized sets of users A_1 and A_2 reconstruct the secret to s_1 and s_2, respectively, then $Pr[s_1 \neq s_2] < 2^{-k}$.

We use standard techniques developed by Pedersen [Ped92] to transform our disjunctive secret sharing scheme into a distributed commitment scheme. In the setup phase, some trusted third party chooses generators h_1, h_2 of some finite field $\mathbb{F}_q$ of prime order q. The Pedersen commitment [Ped92] of $x, y \in \mathbb{Z}_q$ is $\mathsf{Ped}(x, y) = h_1^x h_2^y$. Suppose the sequence of thresholds is $t_0 < t_1 < \ldots < t_n$, and let $t = t_n$. To share a secret $s \in \mathbb{Z}_q$, the dealer performs the following four steps:

1. The dealer chooses a random sequence of values $a_0, a_1, \ldots, a_{t-2}$ and sets $a_{t-1} = s$. The sequence of values defines the polynomial $f(x) = \sum_{i=0}^{t-1} a_i x^i$.

2. The dealer chooses a random sequence of values $b_0, b_1, \ldots, b_{t-1}$. The sequence of values defines the polynomial $g(x) = \sum_{i=0}^{t-1} b_i x^i$.

3. The dealer sends each user u at level $L = \mathcal{L}(u)$ his share $(f^{(t-t_L)}(u), g^{(t-t_L)}(u))$.

4. The dealer calculates $C_i = \mathsf{Ped}(a_i, b_i)$ and publishes $C_0, \ldots, C_{t-1}$.

A user u at level $L = \mathcal{L}(u)$ can verify the validity of his share (x, y) by checking that:

$$\mathsf{Ped}(x, y) = \prod_{i=t-t_L}^{t-1} C_i^{\frac{i!}{(i-t+t_L)!} u^{i-t+t_L}}$$

Theorem 4.1. *The above construction results in a private, correct, complete, and binding distributed commitment scheme as long as the dealer cannot compute* $\log_{h_1} h_2$.

Proof. Correctness follows from Theorem 3.6 because each users's share contains the same $f^{(t-t_L)}(u)$ as in Construction 3.5. Privacy is also straightforward. The only extra information received by a user u at level L are Pedersen [Ped92] commitments to the coefficients of the polynomials f and g, as well as $g^{(t-t_L)}(u)$. Pedersen commitments do not provide any extra information, while the $g^{(t-t_L)}(u)$ does not provide any more information about g than $f^{(t-t_L)}(u)$ does about f. Thus, an unauthorized set of users gains no advantage when trying to learn the secret. Completeness follows from the fact that:

$$\mathsf{Ped}(x, y) = \prod_{i=t-t_L}^{t-1} C_i^{\frac{i!}{(i-t+t_L)!} u^{i-t+t_L}} = \prod_{i=t-t_L}^{t-1} (h_1^{a_i} h_2^{b_i})^{\frac{i!}{(i-t+t_L)!} u^{i-t+t_L}} = h_1^{f^{(t-t_L)}(u)} h_2^{f^{(t-t_L)}(u)}$$

All that's left is to prove that the scheme is binding. We essentially follow Pedersen's proof [Ped92]. If an authorized set of users accepts all of its shares, then, due to correctness, the users can reconstruct some pair of polynomials f and g that are consistent with their shares. This implies that $C_0 = \mathsf{Ped}(f(0), g(0))$. Now suppose that there are two (possibly overlapping) sets of users A and A' that reconstruct different secrets from their shares. This means that there exist values s, s', t, t', where $s \neq s'$ and $t \neq t'$, such that $C_0 = \mathsf{Ped}(s, t) = \mathsf{Ped}(s', t')$. In this case, we can use the shares of A and A' to calculate $\log_{h_1} h_2$ using standard techniques [Ped92]. All the dealer has to do is find two sets of users with inconsistent shares and use them to calculate the discrete logarithm.

To do this, the dealer starts with an arbitrary minterm A, such that $|A| = t$, the highest threshold. The dealer uses the shares assigned to those users to calculate f and g (a minterm of size t ensures the dealer can reconstruct f and g completely, rather than just their derivatives). Next, the dealer goes through every other user $u \in \mathcal{U}$ and checks if that user's share $(x, y) = (f^{(t-t_L)}(u), g^{(t-t_L)}(u))$, where $L = \mathcal{L}(u)$. If the user's share is inconsistent, the dealer constructs a new set of users $A' = A - V + \{u\}$, where V is the set of users that need to be removed to ensure A' is a minterm. Since u has a share that is not on f, g, the dealer can use the shares of A' to reconstruct a different pair of polynomials with a different secret than that of A. □

Remark Our distributed commitment scheme is perfectly private (unauthorized sets of users gain no information about the secret). We note that Ballico et al. [BBFG05] construct a distributed commitment scheme from Tassa's [Tas04] conjunctive secret sharing scheme; their scheme is more efficient than ours, but preserves privacy only under the discrete logarithm assumption. Applying their result to our disjunctive scheme is straightforward.

References

[BBFG05] Edoardo Ballico, Giulia Boato, Claudio Fontanari, and Fabrizio Granelli. Hierarchical secret sharing in ad hoc networks through birkhoff interpolation. In *International Conference on Telecommunications and Networking (TeNE 2005)*, 2005.

[Bla79] George Robert Blakley. Safeguarding cryptographic keys. In *Proceedings of the National Computer Conference 1979*, volume 48 of *American Federation of Information Processing Societies Proceedings*, pages 313–317, 1979.

[Bri89] Ernest F. Brickell. Some ideal secret sharing schemes. In *Journal of Combinatorial Mathematics and Combinatorial Computing*, volume 9, pages 105–113, 1989.

[BTW05] Amos Beimel, Tamir Tassa, and Enav Weinreb. Characterizing ideal weighted threshold secret sharing. In *Theory of Cryptography Conference – TCC 2005*, volume 3378 of *Lecture Notes in Computer Science*, pages 600–619. Springer-Verlag, 2005.

[Feh99] Serge Fehr. Efficient construction of the dual span program. Available at `http://citeseer.ist.psu.edu/fehr99efficient.html`, 1999.

[GPSN98] Hossein Ghodosi, Josef Pieprzyk, and Rei Safavi-Naini. Secret sharing in multilevel and compartmented groups. In C. Boyd and E. Dawson, editors, *ACISP '98: Proceedings of the Third Australasian Conference on Information Security and Privacy*, volume 1438 of *Lecture Notes in Computer Science*, pages 367–378. Springer Verlag, 1998.

[KW93] Mauricio Karchmer and Avi Wigderson. On span programs. In *8th Annual Conference on Structures in Complexity Theory (SCTC'93)*, pages 102–111. IEEE Computer Society Press, 1993.

[Ped92] Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In Joan Feigenbaum, editor, *Advances in Cryptology – CRYPTO '91*, volume 576 of *Lecture Notes in Computer Science*, pages 129–140. Springer Verlag, 1992.

[Sha79] Adi Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, November 1979.

[Sho93] Victor Shoup. Fast construction of irreducible polynomials over finite fields. In *SODA: ACM-SIAM Symposium on Discrete Algorithms*, 1993.

[Sim88] Gustavus J. Simmons. How to (really) share a secret. In Shafi Goldwasser, editor, *Advances in Cryptology — CRYPTO '88*, volume 403 of *Lecture Notes in Computer Science*, pages 390–448. Springer Verlag, 1988.

[Tas04] Tamir Tassa. Hierarchical threshold secret sharing. In Moni Naor, editor, *Theory of Cryptography: First Theory of Cryptography Conference, TCC 2004*, Lecture Notes in Computer Science, pages 473–490, Cambridge, MA, 2004.

[TD06] Tamir Tassa and Nira Dyn. Multipartite secret sharing by bivariate interpolation. In *ICAALP 2006, Part II*, volume 4052 of *Lecture Notes in Computer Science*, pages 288–299, Venice, Italy, 2006.