Some Ideal Secret Sharing Schemes

Ernest F. Brickell*
Sandia National Laboratories
Albuquerque, NM 87185

Abstract

In a secret sharing scheme, a dealer has a secret. The dealer gives each participant in the scheme a share of the secret. There is a set Γ of subsets of the participants with the property that any subset of participants that is in Γ can determine the secret. In a perfect secret sharing scheme, any subset of participants that is not in Γ cannot obtain any information about the secret. We will say that a perfect secret sharing scheme is ideal if all of the shares are from the same domain as the secret. Shamir and Blakley constructed ideal threshold schemes, and Benaloh has constructed other ideal secret sharing schemes. In this paper, we construct ideal secret sharing schemes for more general access structures which include the multilevel and compartmented access structures proposed by Simmons.

1 Introduction

Given a set of n participants and a set Γ of subsets of the participants, a *secret sharing scheme* for Γ is a method of distributing shares to each of the participants such that any subset of the participants in Γ can determine the secret, but any subset of participants that is not in Γ cannot determine the secret. The *share* of a participant refers specifically to the information that the dealer sends in private to the participant. If any subset of participants that is not in Γ cannot determine any information about the secret, then the secret sharing scheme is said to be perfect. Given a secret sharing scheme in which S is the set of possible secrets and T is the set of possible shares, we define the *information rate*, ρ, of the scheme as $\rho = \log|T|/\log|S|$. For example, if the secret is a random element of GF(q), and all shares are elements of GF(q), then the information rate is 1. Simmons [5] defined a related notion. He called a secret sharing scheme *extrinsic* if the set T of possible shares is the same for all participants. We will say that a secret sharing scheme is *ideal* if it is perfect and has information rate 1.

*This work performed at Sandia National Laboratories and supported by the U.S. Department of Energy under contract No. DE-AC04-76DP00789.

The first constructions of secret sharing schemes were due to Blakley [2] and Shamir [4]. Their schemes are called threshold schemes because they have the property that for some t, only the subsets of participants of cardinality at least t can determine the secret. Both the Blakley and the Shamir schemes are perfect and can be ideal as we will demonstrate later in this section.

Given a secret sharing scheme, the access structure, Γ, is defined as the set of subsets of participants that can determine the secret. In this paper, we will restrict our attention to secret sharing schemes in which Γ is monotone, that is if $B \in \Gamma$, and if B is contained in C, then $C \in \Gamma$.

Ito, Saito, and Nishizeki [3] have shown that for any monotone set of subsets, Γ, there exists a perfect secret sharing scheme for which Γ is the access structure. Benaloh [1] has proven this result using a construction that has a lower information rate than the construction of Ito, et.al. although his construction is far from ideal for arbitrary Γ. Benaloh has also shown that there exist monotone sets Γ, which cannot be the access structure for an ideal secret sharing scheme. We will say that a monotone set of subsets, Γ, is an *ideal access structure* if there is some ideal secret sharing scheme for which Γ is the access structure.

The motivation for the current paper is to find ideal secret sharing schemes with access structures that are more general than threshold access structures.

Simmons [5] has described an access structure that arises in a practical application of secret sharing. A *multilevel access structure* is one in which each participant is assigned a level which is a positive integer and the access structure consists of those subsets which contain at least r participants all of level at most r. In other words, 2 participants of level 2 can determine the secret, as can 3 of level 3. But also 1 participant of level 2 and 2 participants of level 3 can determine the secret. Simmons asked whether all multilevel access structures are ideal access structures.

In this paper, we answer Simmons' question in the affirmative. Specifically, in Theorem 1, we show that given any multilevel access structure, there exists Q such that for any q a prime power with $q > Q$, there is an ideal secret sharing scheme realizing this access structure over GF(q).

One drawback to the construction given in Theorem 1 is that it requires the dealer to check many (possibly exponentially many) matrices to see that they are nonsingular. In Theorem 2, we give a different construction for realizing multilevel access structures that removes this undesirable property.

Simmons also pointed out that there were potential applications for compartmented access structures. In a *compartmented access structure* , there are different compartments, say $C_1, \ldots, C_u$, and positive integers $t_1, \ldots, t_u$ and t. The access structure consists of all subsets containing at least t_i participants from C_i for $1 \leq i \leq u$, and a total of at least t participants. Simmons' original notion of compartmented schemes had $t = \sum_{i=1}^{u} t_i$, but we have generalized his notion slightly since we have been able to construct more general ideal secret sharing schemes. In section 3, we show that for any compartmented access structure, there exists a Q, such that for $q > Q$, there exists an ideal secret sharing scheme for Γ over GF(q).

We conclude this section with a brief description of the threshold schemes of Shamir and Blakley.

The scheme of Shamir [4] is based on polynomials over GF(q). Let $f(x) = \sum_{i=0}^{t-1} a_i x^i$. The secret is $f(0) = a_0$. Participant P_j will receive an ordered pair $(x_j, f(x_j))$. It is easy to show that this is a threshold scheme, since for any t participants, there is only one polynomial of degree $t-1$ passing through their t points. Also it is a perfect threshold scheme since for any $t-1$ participants and any point $(0, a)$, there is a polynomial of degree t passing through their $t-1$ points and $(0, a)$. This scheme will be ideal if the value of x_j is publicly revealed so that the share of participant P_j is just the value of $f(x_j)$.

The scheme of Blakley [2] is based on geometries over finite fields. Let V be a t-dimensional vector space over GF(q) and let e_1 be the t-dimensional vector $(1, 0, \ldots, 0)$. The dealer picks a 1-dimensional flat, g, that is not perpendicular to e_1 and a $(t-1)$-dimensional flat, H, such that g and H intersect in a single point, P. The secret will be the first coordinate of P. g will be made public but H will be kept secret. The dealer will pick n points $p_i, i = 1, \ldots, n$ such that these points together with P are in general position, that is any t of the points generate a $(t-1)$-dimensional flat. Participant P_i will receive the point p_i. This is a perfect secret sharing scheme since any t of the participants can use their points to determine the hyperplane H, but for any $t-1$ of the participants, there is a hyperplane passing through their points and any given point on g. The Blakley scheme can be modified slightly so that it is ideal. Let g be the first coordinate axis. When the dealer gives point p_i to participant P_i, he can make public all the coordinates except the first coordinate, and give only the first coordinate to P_i in secret. So P_i's share is only the first coordinate.

2 A Basic Secret Sharing Scheme

In this section, we give a slight generalization of the Shamir and Blakley schemes which is guaranteed to have information rate 1, and in Proposition 1, give sufficient conditions for it to be perfect and thus an ideal secret sharing scheme.

The Basic Secret Sharing Scheme: The secret is an element in some finite field GF(q). The dealer chooses a vector $\mathbf{a} = (a_0, \ldots, a_t)$ for some t, where each $a_j \in$ GF(q), and a_0 is the secret. Denote the participants by P_i for $1 \leq i \leq n$. For each P_i, the dealer will pick a t-dimensional vector $\mathbf{v}_i$ over GF(q). All of the vectors $\mathbf{v}_i$ for $1 \leq i \leq n$ will be made public. The share that the dealer gives to P_i will be $s_i = \mathbf{v}_i \cdot \mathbf{a}$. Let $\mathbf{e}_i$ denote the i'th t-dimensional unit coordinate vector (i.e. $\mathbf{e}_1 = (1, 0, \ldots, 0)$).

Proposition 1 *Let $\gamma = \{P_{i_1}, \ldots, P_{i_k}\}$ be a set of participants.*

(1) The participants in γ can determine the secret if the subspace $\langle \mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_k} \rangle$ contains $\mathbf{e}_1$.

(2) The participants in γ receive no information about the secret if the subspace $\langle \mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_k} \rangle$ does not contain $\mathbf{e}_1$.

Proof Let M be the matrix with rows $\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_k}$. Let $\mathbf{s} = (s_{i_1}, \ldots, s_{i_k})$. To prove (1), let $\mathbf{w}$ be the vector such that $\mathbf{w}M = \mathbf{e}_1$. Then $\mathbf{w}M\mathbf{a} = a_0$. Hence $\mathbf{w} \cdot \mathbf{s} = a_0$.

To prove (2), let $\mathbf{w}_0, \ldots, \mathbf{w}_t$ be the column vectors of M. If $\mathbf{w}_0 \notin \langle \mathbf{w}_1, \ldots, \mathbf{w}_t \rangle$, then there exists $\mathbf{d}$ such that $\mathbf{d} \cdot \mathbf{w}_i = 0$ for $1 \leq i \leq t$ and $\mathbf{d} \cdot \mathbf{w}_0 = 1$. So $\mathbf{d}M = \mathbf{e}_1$, but this contradicts the assumption that $\mathbf{e}_1 \notin \langle \mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_k} \rangle$. Hence, $\mathbf{w}_0 \in \langle \mathbf{w}_1, \ldots, \mathbf{w}_t \rangle$. So there exists $\mathbf{b}$ such that $M\mathbf{b} = \mathbf{0}$ and $b_0 \neq 0$. The only information the participants in γ have about a_0 is that $M\mathbf{a} = \mathbf{s}$. But $\mathbf{s} = M\mathbf{a} = M(\mathbf{a} + \alpha\mathbf{b})$ for all $\alpha \in \mathrm{GF(q)}$. Consequently, given any $c_0 \in \mathrm{GF(q)}$, there exists $\mathbf{c} = (c_0, \ldots, c_t)$ with $c_i \in \mathrm{GF(q)}$ for $1 \leq i \leq t$ such that $M\mathbf{c} = \mathbf{s}$. Therefore, the participants in γ cannot rule out any element of $\mathrm{GF}(q)$ as a possibility for a_0. □

3 Multilevel Schemes

In this section, we give an existence proof that any multilevel access structure can be achieved in an ideal secret sharing scheme. Then we give a different construction that requires less computation on the part of the dealer.

The Basic Multilevel Scheme: Let Γ be a multilevel access structure with levels $l_1 < l_2 < \ldots < l_R$. Let N_r be the number of participants of level l_r. Denote the participants by P_i for $1 \leq i \leq n$, and let L_i be the level of P_i. We will use the basic secret sharing scheme. So we need only specify how the dealer will choose the vectors $\mathbf{v}_i$. For each P_i, the dealer will pick an $x_i \in \mathrm{GF(q)}$. Let $\mathbf{v}_i$ be the l_R-dimensional vector $(1, x_i, x_i^2, \ldots, x_i^{L_i - 1}, 0, \ldots, 0)$. Note that if $l_1 = 1$ and P_i is a participant with $L_i = 1$, then $\mathbf{v}_i = \mathbf{e}_1$. Define polynomials $f_j(x) = \sum_{i=o}^{j-1} a_i x^i$. The share s_i that the dealer gives to P_i will satisfy $s_i = f_{L_i}(x_i)$.

To complete the proof that there exists an ideal secret sharing scheme for any multilevel access structure, we need only to show that for any multilevel access structure, there is a method for the dealer to choose the x_i so that $\langle \mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_k} \rangle$ contains $\mathbf{e}_1$ iff $\{P_{i_1}, \ldots, P_{i_k}\} \in \Gamma$. In the remainder of this section, we give three different methods for the dealer to choose the x_i.

Theorem 1 *Let Γ be a multilevel access structure with levels $l_1 < l_2 < \ldots < l_R$. Let N_r be the number of participants of level l_r. Let n be the total number of participants. If $q > (l_R - 1)\binom{n}{l_R - 1}$, then there is an ideal secret sharing scheme for Γ over GF(q).*

Proof We will use the basic multilevel scheme construction. We only need to show how the dealer will choose the x_i. Let $\mathbf{v}_0 = \mathbf{e}_1$ (although there is no participant P_0). Suppose the dealer has chosen x_i for all i, $0 \leq i < h$. Let Ω be the set of subspaces spanned by some subset of size $L_h - 1$ of the vectors $\{\mathbf{v}_i \mid 0 \leq i < h\}$. $|\Omega| < \binom{h}{L_h - 1}$. The dealer then picks x_h so that the L_R-dimensional vector $\mathbf{v}_h = (1, x_h, x_h^2, \ldots, x_h^{L_h - 1}, 0, \ldots, 0)$ is not in any of the subspaces in Ω. To see that this is possible, let $H \in \Omega$, and let $\mathbf{w} = (w_0, w_1, \ldots, w_{L_h - 1}, 0, \ldots, 0)$ be a normal vector to H. Then $\sum_{i=0}^{L_h - 1} w_i x^i = 0$ has at most $L_h - 1$ solutions over $\mathrm{GF}(q)$.

Suppose that k participants, $P_{i_1}, \ldots, P_{i_k}$, of level at most k try to recover the secret and suppose that there is no subset of this set which contains l participants of level at most l for any $l < k$. The vectors $\mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_k}$ are independent and are contained in the k-dimensional space spanned by $\mathbf{e}_1, \ldots, \mathbf{e}_k$. Hence, $\mathbf{e}_1 \in \langle \mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_k} \rangle$ and so by Proposition 1, these participants can determine the secret.

Suppose now that a set $\gamma \notin \Gamma$ of participants try to recover the secret. Let $\gamma = \{P_{i_1}, \ldots, P_{i_k}\}$. Since the vectors $\mathbf{e}_1, \mathbf{v}_{i_1}, \ldots, \mathbf{v}_{i_k}$ are independent, by Proposition 1, these participants cannot obtain any information about a_0. □

The Blakley scheme can also be modified to implement a multilevel access structure. The dealer again picks g to be the first coordinate axis and a sequence of flats F_i satisfying: $F_1 \subset F_2 \subset \ldots \subset F_R$, $F_1 \cap g$ is nonempty, and $g \not\subseteq F_R$. The secret is $P = F_1 \cap g$. A person of level r will be given a point on F_{r-1}. The points should be selected so that any r participants of rank at most r can determine the point P, and also so that for the flat, F, generated by a group of participants in which for any r there is no subset of r participants who all have rank at most r, $F \cap g$ must be empty. This construction was also discovered by Simmons [6].

One other issue to consider is the amount of computation needed for the dealer to construct a system. For the original Blakley system, the dealer must do a check to make sure that the points are in general position. An obvious way to do this requires $\binom{n}{k}$ time, although if the points are carefully selected, no such check is necessary. Also, no such check is needed for the Shamir scheme. Unfortunately, this nice property does not hold in the above construction for multilevel schemes. The obvious way to implement the scheme presented in Theorem 1 would require many checks to be sure that the points are in general position. We have however found some constructions which do not require checking.

The first construction we will mention is only feasible if there are not too many levels involved. We will use the basic multilevel scheme and so we simply need to describe how the dealer will pick the x_i. For illustration, suppose that we want to allow levels 2 or 3. Pick $q = p^2$. Let α be algebraic of degree 2 over GF(p) (i.e. α satisfies an irreducible polynomial of degree 2 over GF(p)). The dealer picks an element y_i in GF(p) for each participant P_i so that if $i \neq j$ and $L_i = L_j$, then $y_i \neq y_j$. For a participant of level 3, the dealer sets $x_i = y_i$. For a participant of level 2, he uses $x_i = \alpha y_i$. This system will have the desired properties. To see that three participants $P_{i_1}, P_{i_2}, P_{i_3}$ with $L_{i_1} = 2$, and $L_{i_2} = L_{i_3} = 3$ can determine the secret, consider the matrix M formed by $\mathbf{v}_{i_1}, \mathbf{v}_{i_2}, \mathbf{v}_{i_3}$. The determinant of this matrix is a polynomial in α of degree at most 1. It can be shown that the constant term in this polynomial is nonzero. Since α is algebraic of degree 2, the value of the polynomial must be nonzero.

In the more general setting, with levels $l_1 < \ldots < l_R$, the dealer picks $\alpha_1, \ldots, \alpha_{R-1}$, where α_r satisfies an irreducible of degree $\left\lfloor \frac{l_r^2}{2} \right\rfloor + 1$ over

$$\mathrm{GF}(p^{\prod_{j=r+1}^{R-1} \left(\left\lfloor \frac{l_j^2}{2} \right\rfloor + 1 \right)}).$$

The dealer then sets $x_i = \alpha_{L_i} y_i$. The proof that this system has the desired properties is an extension of the above arguement. We will not include the arguement here because the following theorem constructs ideal multilevel schemes in a more efficient manner.

Theorem 2 *Let Γ be a multilevel access structure with levels $1 = l_0 < l_1 < \ldots < l_R$. Let q be a prime satisfying $q > N_r + 1$ for $1 \leq r \leq R$. Let $\beta = Rl_R^2$. Then there is an ideal secret sharing scheme for Γ over GF(q^β) which can be constructed in time polynomial in $(N_1, \ldots, N_R, q)$.*

Proof Once again, we just need to show how the dealer will pick the x_i to use in the basic multilevel scheme. If there is no participant of level 1, add a participant P_0 with $L_0 = 1$. The dealer selects a y_i for each P_i so that $y_i \neq y_j$ if $L_i = L_j$ and $i \neq j$. Define $\rho(i)$ to be the integer j such that $L_i = l_j$. The dealer also picks an α that satisfies an irreducible of degree Rl_R^2 over GF(p). Let $x_i = y_i \alpha^{R-\rho(i)}$.

Let $\gamma = \{P_{i_1}, \ldots, P_{i_k}\}$, be a set of k participants each of whom has level at most k and suppose that there is no subset of γ which contains more than l participants of rank at most l for any $l < k$. Let n_j be the number of these participants of rank l_j. Let $M'(\gamma)$ be the matrix whose rows are the vectors $\mathrm{v}_{i_1}, \ldots, \mathrm{v}_{i_k}$. Let $M(\gamma)$ be the matrix consisting of only the first k columns of $M'(\gamma)$. $M(\gamma)$ is essentially the same matrix as $M'(\gamma)$ since all of the columns removed consisted of all zeros.

To show that $M = M(\gamma)$ is nonsingular, we will show that the determinant of M can be written as a polynomial in α of degree less than Rl_R^2. We will show that the polynomial is not identically zero by showing that the constant term is nonzero.

Consider the determinant of M as a polynomial in α. Let $M = (m_{i,j})$. Recall that the determinant is the sum of all elementary signed products of M, where an elementary signed product is the product of the terms $m_{1,c_1}, \ldots, m_{k,c_k}$ with the appropriate sign, where $c_1, \ldots, c_k$ is a permutation of $1, \ldots, k$. Any nonzero elementary signed product will satisfy $c_i \leq L_i$ for $1 \leq i \leq k$. The maximum exponent of α in a row i of M is $(R - \rho(i))(L_i - 1)$. Therefore the maximum exponent of α in an elementary signed product is $\leq \sum_{r=1}^{R-1}(R-r)(l_r - 1)n_r < Rl_R \sum_{r=1}^{R-1} n_r \leq Rl_R^2$.

Let $T_{-1} = 0$, and let $T_j = \sum_{i=0}^{j} n_i$ for $0 \leq j \leq R$. The exponent of α in a nonzero elementary signed product will be $\sum_{i=1}^{k}(c_i - 1)(R - \rho(i))$. This sum achieves its minimum exactly when $\{c_{T_{r-1}+1}, \ldots, c_{T_r}\} = \{T_{r-1}+1, \ldots, T_r\}$ for $0 \leq r \leq R$. Let D_r be the n_r by n_r submatrix of M generated by the rows and columns $T_{r-1}+1, \ldots, T_r$. Let z be the minimum exponent of α in the determinant of M. Then the term $\theta\alpha^z$ for $\theta \in$ GF(q) in the determinant of M satisfies $\theta\alpha^z = \prod_{r=1}^{R} |D_r|$. Since each D_r is a multiple of a Van der Monde matrix, $|D_r| \neq 0$. Therefore, the coefficient of α^z is nonzero. Thus, since $M(\gamma)$ is nonsingular, the participants in γ can determine a_0.

Suppose now that γ is a set of $k-1$ participants each of level at most k and suppose that there is no subset of γ which contains l participants of level at most l for any $l < k$. Let $\gamma' = \gamma \cup \{P_0\}$. Now γ' is a set of k participants each of level at most k and there is no subset of γ' which contains more than l participants of level at most l for any $l < k$. The matrix $M(\gamma')$ will thus be nonsingular. Therefore, $\mathrm{e}_1 \notin \langle \mathrm{v}_i \mid P_i \in \gamma \rangle$. From Proposition 1, the participants in γ receive no information about the value of a_0. □

4 Compartmented schemes

In a compartmented scheme, there are disjoint sets of participants $C_1, \ldots, C_u$. The access structure consists of subsets of participants containing at least t_i from C_i for $i = 1, \ldots, u$, and a total of at least t participants. Let n be the total number of participants.

Theorem 3 *Let Γ be a compartmented access structure. If $q > \binom{n}{t}$, then there is an ideal secret sharing scheme for Γ over GF(q).*

Proof WLOG, we may assume that $T = t - \sum_{i=1}^{u} t_i \geq 0$. The dealer chooses a vector $\mathbf{a} = (a_0, \ldots, a_{t-1})$ where a_0 is the secret. Let $T_0 = T$, and let $T_i = T + \sum_{j=1}^{i} t_j$ for $1 \leq i \leq u$. Denote the participants by $P_{r,i}$ where $P_{r,i}$ is in compartment C_r. For participant $P_{r,i}$, the dealer will pick a t-dimensional vector over GF(q) of the form

$$\mathbf{v}_{r,i} = (1, x_{r,i}, x_{r,i}^2, \ldots, x_{r,i}^{T-1}, 1, \ldots, 1, \underbrace{x_{r,i}^{T}, \ldots, x_{r,i}^{T+t_r-1}}_{\text{coordinates } T_{r-1}+1,\ldots,T_r}, 1, \ldots, 1)$$

for some $x_{r,i} \in \mathrm{GF}(q)$. As in Theorem 1, the dealer must be careful in choosing the $x_{r,i}$. Let $\prec$ denote lexicographic ordering on ordered pairs. I.e. $(r,i) \prec (s,j)$ iff $r < s$ or ($r = s$ and $i < j$). Let $\mathbf{v}_{0,0} = \mathbf{e}_1$. Suppose that the dealer has chosen $x_{r,i}$ for all $(r,i) \prec (s,j)$. Then the dealer must choose $x_{s,j} \neq 1$ so that the vector $\mathbf{v}_{s,j}$ is not in any subspace spanned by a set of vectors consisting of at least t_r of the $\mathbf{v}_{r,i}$ for each $r < s$ and at least $t_s^* = \min(t_s - 1, j - 1)$ of the $\mathbf{v}_{s,i}$ for $i < j$ and a total of at most $T + t_s^* + \sum_{r=1}^{s-1} t_r$ of the $\mathbf{v}_{r,i}$ for $(0,0) \preceq (r,i) \prec (s,j)$. Since $q > \binom{N}{t}$, it is easy to see that this is possible by using similar arguments to those used in Theorem 1.

A set of participants in Γ can determine the secret since the vectors $\mathbf{v}_{r,i}$ are independent. Conversely, suppose that a set $\gamma = \{P_{r,i} \mid (r,i) \in I\}$ of participants is not in Γ. Suppose there is a C_s such that γ does not contain at least t_s of the participants in C_s. Let M be the matrix with rows $\mathbf{v}_{r,i}$ for $(r,i) \in I$. Let M' be the matrix consisting of columns $1, T_s+1, \ldots, T_s+t_s$ of M. There are only t_s distinct rows in M', namely the rows corresponding to the vectors $\mathbf{v}_{r,i}$ with $r = s$ and $(r,i) \in I$, and the vector $(1,1,\ldots,1)$. Let $\{i_1, \ldots, i_{t_s-1}\} = \{i \mid (s,i) \in I\}$. Let M'' be the matrix consisting of the rows $\mathbf{e}_1, \mathbf{v}_{s,i_1}, \ldots, \mathbf{v}_{s,i_{t_s-1}}$. Then $|M''| = |M''_{11}|$, where M''_{11} is the matrix M'' with the first row and column removed. But M''_{11} is just a Van der Monde matrix with row i_j multiplied by x_{s,i_j}^T for $1 \leq j \leq t_s - 1$. So $|M''_{11}| \neq 0$. Therefore $\mathbf{e}_1$ is not in $\langle \mathbf{v}_{r,i} \mid (r,i) \in I \rangle$. If γ contains at least t_r participants from C_r for $1 \leq r \leq u$, but does not contain a total of at least t participants, then the participants in γ receive no information about a_0 since $\mathbf{e}_1$ and the vectors $\mathbf{v}_{r,i}$ for $(r,i) \in I$ are independent. □

The construction presented in Theorem 3 requires that the dealer check exponentially many subspaces. It is easy to give an efficient implementation in the case that $t = \sum_{i=0}^{u} t_i$. The dealer can simply choose a_0 as the secret, and then randomly pick

$b_1, \ldots, b_u$ such that $a_0 = \sum_{i=0}^{u} b_i$. He then uses a threshold scheme with threshold t_i and secret b_i to distribute shares to the participants in C_i. However, we have found no efficient construction for the more general compartmented access structures.

5 Remarks

Benaloh [1] has shown that any set of subsets which can be recognized by a monotone circuit in which all gates and all inputs have fanout 1 can be realized as the access structure of an ideal secret sharing scheme. He also pointed out that since threshold schemes were ideal secret sharing schemes, threshold gates could be added to the circuits as well. Since we have now shown that multilevel schemes and compartmented schemes are ideal, gates realizing these access structures can be added as well.

6 Acknowledgments

I would like to thank Gus Simmons for introducing me to multilevel and compartmented secret sharing schemes and to Dan Davenport for useful conversations concerning this paper.

References

[1] Josh C. Benaloh and Jerry Leichter. Generalized secret sharing and monotone functions. to appear in Advances in Cryptology - CRYPTO88.

[2] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings AFIPS 1979 National Computer Conference*, pages 313–317, 1979.

[3] M. Ito, A. Saito, and T Nishizeki. Secret sharing scheme realizing general access structure. In *Proceedings IEEE Globcom'87*, pages 99–102, Tokyo, Japan, 1987.

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

[5] Gustavus J. Simmons. How to (really) share a secret. to appear in Advances in Cryptology - CRYPTO88.

[6] Gustavus J. Simmons. Robust shared secret schemes. to appear in Congressus Numerantium, Vol. 68-69.