A comment on group independent threshold sharing

Abstract

Secret sharing is important in the cases where a secret needs to be distributed over a set of n devices so that only authorized subsets of devices can recover the secret. Some secret sharing schemes can be used with only certain algebraic structures (for example fields). Group independent linear threshold sharing refers to a t out of n linear threshold secret sharing scheme that can be used with any finite abelian group. Group independent secret sharing schemes were introduced in [16] and a formal definition was given in [26] and [10]. Here we describe additional properties of group independent sharing schemes. In particular, we discuss how to construct the dual from the shareholder reconstruction matrix, new bounds on the computational requirements of group independent sharing and new necessary and sufficient conditions to test if a matrix will provide a group independent sharing scheme.
keywords: secret sharing, threshold cryptography, monotone span programs, integer span programs, group independent threshold schemes, black-box sharing

1 Introduction

Secret sharing is important in the cases where a secret needs to be distributed over a set of n devices so that only authorized subsets of devices can recover the secret. Secret sharing is typically used in situations where it is not possible for the secret to reside on a single device. A setting where the authorized sets consists of all subsets of t or more is called a t out of n threshold secret sharing scheme. The importance of threshold cryptography, especially in the context of threshold signature sharing, was noted in [9, 14].

Threshold cryptography is closely tied to public-key cryptography. Many applications of threshold sharing revolve around the use of digital signatures which use public-key primitives. Within a threshold signature scheme, the participants are not recovering the secret but a function of the secret (i.e. a signature). Shamir's scheme [28] provides an efficient way to construct t out of n threshold sharing over a field. However if the algebraic setting of the signature scheme is not a field then one cannot use Shamir's scheme. In such cases, one must use the algebraic setting for which the secret space resides. RSA is an example of a public-key primitive whose secret space is not a field. When developing RSA threshold signature schemes an alternative to Shamir's scheme must be used. Some of these alternatives rely on tailoring the scheme to this algebraic setting, some examples of this approach include [19, 20, 22]. Other alternatives introduced the concept of developing threshold schemes which can be used over any finite abelian group, see [13, 16]. A very efficient threshold RSA signature scheme was developed in [29]. Thus there are a number of ways to achieve threshold RSA signatures and many of them are "efficient". However, if one is interested in developing zero-knowledge threshold schemes (see [16]), then one cannot tailor the scheme to the algebraic setting, and so the only alternative is to use threshold sharing schemes that can be used over any finite abelian group. Known methods to construct group independent sharing schemes have succeeded at an expense of share expansion (for example [16]). However a recent result at Crypto 2002 [10] has established that the share expansion is not as costly as previously thought.

Further, there is increase in activity to develop public-key primitives based on new number-theoretic problems[1]. Some of these primitives will fall to the wayside, while others, perhaps because of some

[1]New in the sense that such problems in the past may not have not been thought of as good problems to base a public-key

efficiency property may become popular. Many of these primitives are based in a finite abelian group and not in a field. Once a new primitive becomes popular, threshold applications will soon follow. The specter of developing threshold cryptography for an arbitrary finite abelian group does loom. So it is important to discuss group independent threshold sharing schemes, the computational requirements for group independent threshold sharing schemes, properties of group independent threshold sharing schemes, and methods to construct group independent threshold sharing schemes.

Group independent threshold sharing schemes were first introduced in [16]. A formal definition of group independent threshold sharing schemes called GILTS was given [26]. In [10], an equivalent but distinct definition of group independent threshold sharing schemes called Black-box sharing was given. Our goal here is to discuss additional properties of group independent threshold sharing schemes. In particular we provide an illustration on how to construct the dual of a group independent threshold sharing scheme from the shareholder reconstruction matrix. We also provide new computational requirements concerning the generation of group independent sharing schemes, in particular on the amount of randomness required. Lastly we provide new necessary and sufficient conditions which will allow us to test if a reconstruction matrix truly describes a group independent threshold sharing scheme (i.e. will the reconstruction matrix provide the needed security requirements.) We point out that the **redistribution matrix** is a more natural way to view a secret sharing scheme, since this represents how the participants must act. Whereas an **integer span program** represents how the distributor will construct the shares. However the integer span program provides much more algebraic structure to derive properties of group independent sharing schemes.

The outline of the paper is as follows: Sections 2 and 3 provide definitions and some mathematical background. Section 4 describes the two definitions of group independent threshold sharing, GILTS and Black-box sharing. Section 5 describes group independent sharing schemes and their relation to integer span programs. Section 6 describes the dual of group independent threshold sharing. Section 7 provides some observations about group independent sharing, Section 8 describes new bounds on randomness required in a group independent threshold sharing scheme and Section 9 describes new necessary and sufficient conditions for group independent sharing schemes.

2 Definitions and notation

If A is some subset of a universal set $\mathcal{U}$ then we will use $\tilde{A}$ to denote the complement of A. Let $\mathbf{Z}^{m,n}$ represent the set of all m by n matrices with integer entries. If A is a matrix, it's transpose will be denoted by A^t. A row (column) operation of type I is a row (column) interchange. A row (column) operation of type II is a row (column) multiplied by a nonzero constant. A row (column) operation of type III is a row (column) multiplied by a nonzero constant added to another row (column) leaving this result in the second row (column). The rank of a matrix is the number of linearly independent rows within the matrix. We will denote a row matrix by $\vec{x}$ and a column matrix by $\overline{y}$. If $\vec{x}_1 \dots \vec{x}_n$ are vectors then a linear combination is $\sum_{i=1}^{n} \lambda_i \vec{x}_i$ where $\lambda_i \in \mathbf{Z}$. $GL(n, \mathbf{Z})$ will denote the group with respect to matrix multiplication of all $n \times n$ nonsingular integer matrices. All row vectors will be denoted as $\vec{x}$. If A is a matrix where A is partitioned by $A = [A_1|A_2|\cdots|A_n]$ and $\vec{x}$ is a row of A, then we can partition $\vec{x}$ as $\vec{x} = (\vec{x}_1, \vec{x}_2, \dots, \vec{x}_n)$. Column vectors will be denoted by $\overline{x}$. The exponent of a group G is the smallest positive integer a such that $a \cdot g$ is the identity for all elements $g \in G$.[2] The set Γ of all sets of t or more participants is called the access structure. Because every set of t or more participants contains a set of precisely t participants, we will use Γ_0 to represent those sets which contain exactly t participants. Let μ and τ be positive integers, $M \in \mathbf{Z}^{\mu,\tau}$ and suppose that there exists a function ρ which labels each

cryptosystem on.

[2]If G is an additive group then the exponent is the smallest positive integer a such that $ag = e$ for all $g \in G$ (here e denotes the identity of G).

column of M with an element of $\{1, 2, \ldots, n\}$. Now observe that if $B \subset \{1, 2, \ldots, n\}$ then M_B is the matrix which consists of all columns in M which are labeled to an element in B by ρ. (A simple example of a ρ, is a partition of $M = [M_1|\cdots|M_n]$.)

3 Background mathematics

Most of the mathematics in this section can be derived using simple tools from linear algebra. We do provide some of their proofs in the appendix as an aid to the reader. Let $A \in \mathbf{Z}^{\mu,\tau}$. Then the null space of A is defined as

$$ker(A) = \{\overline{x} \in \mathbf{Z}^{\tau} : A\overline{x} = \overline{0}\}.$$

We define the column space of A as

$$im(A^t) = \{\overline{y} \in \mathbf{Z}^{\tau} : y = A^t\overline{z} \text{ for some } \overline{z}\}.$$

Lemma 1 *For all $\overline{x} \in ker(A)$ and $\overline{y} \in im(A^t)$, $\overline{y}^t\overline{x} = \overline{x}^t\overline{y} = 0$.*

Let $\mathcal{B} = \{\overline{b}_1, \overline{b}_2, \ldots, \overline{b}_\beta\}$ be a basis for $ker(A)$ and let $\mathcal{C} = \{\overline{c}_1, \overline{c}_2, \ldots, \overline{c}_\gamma\}$ be a basis for $im(A^t)$. Then the $span(\mathcal{B} \cup \mathcal{C})$ is the group generated by $\mathcal{B} \cup \mathcal{C}$. Consequently for each $z \in span(\mathcal{B} \cup \mathcal{C})$, there exists integers $u_1, \ldots u_\beta, v_1, \ldots, v_\gamma$ such that $z = \sum_{i=1}^{\beta} u_i\overline{b}_i + \sum_{i=1}^{\gamma} v_i\overline{c}_i$.

Lemma 2 *Let $\overline{z} \in span(\mathcal{B} \cup \mathcal{C})$ and suppose that for all $\overline{x} \in ker(A)$ we have $\overline{z}^t\overline{x} = 0$ then $\overline{z} \in im(A^t)$.*

Lemma 3 *Let $\overline{z} \in span(\mathcal{B} \cup \mathcal{C})$ and suppose that for all $\overline{x} \in im(A^t)$ we have $\overline{z}^t\overline{x} = 0$ then $\overline{z} \in ker(A)$.*

3.1 Smith-normal form

An important tool will be the reducing a matrix to Smith-normal form (for more information see [1, 23, 25]).
Let $A \in \mathbf{Z}^{\mu,\mathcal{T}}$. Suppose we reduce A to Smith-normal form, then there exists $U \in GL(\mu, \mathbf{Z})$ and $V \in GL(\mathcal{T}, \mathbf{Z})$ such that $U\,A\,V = D$ with

$$D = \begin{bmatrix} D_l & 0 \\ 0 & 0 \end{bmatrix},$$

where D_l is a diagonal $l \times l$ matrix with nonzero integer entries d_i along the diagonal, called invariant factors, and satisfy $d_i|d_{i+1}$. U and V are nonsingular matrices which have integer entries. Let l denote the rank of A. Observe that U can be interpreted as a series of row operations of types I and/or III, and V can be interpreted as a series of column operations of type I and/or III that are performed on A to reduce it to D. Since the ring $\mathbf{Z}$ is a principal ideal domain, the invariant factors of A are unique, up to sign, we assume without loss of generality that all invariant factors are positive.
Note that $ker(D) = \{(0, 0, \ldots, 0, x_{l+1}, x_{l+2}, \ldots, x_{\mathcal{T}})^t : x_i \in \mathbf{Z}\}$ and
that $im(D^t) = \{(d_1x_1, d_2x_2, \ldots d_lx_l, 0, 0, \ldots, 0)^t : x_i \in \mathbf{Z}\}$.
We now observe that $ker(A)$ and $im(A^t)$ can be computed by using the Smith-normal form of A. Reduce A to Smith-normal form. Thus $UAV = D$. It follows then that $U^{-1}DV^{-1} = A$. Now consider $\overline{x}$ such that $A\overline{x} = \overline{0}$. Then $UAVV^{-1}\overline{x} = \overline{0}$. Thus $DV^{-1}\overline{x} = \overline{0}$. Consequently $ker(D) = V^{-1} \cdot ker(A)$ and so $ker(A) = V \cdot ker(D)$. Now consider $\overline{y} \in im(A^t)$, then there exists $\overline{x}$ such that $\overline{y} = A^t\overline{x}$. Observe then that $V^t\overline{y} = V^tA^tU^t(U^t)^{-1}\overline{x}$. Hence $V^t\overline{y} = D^t(U^t)^{-1}\overline{x}$. Thus $V^t \cdot im(A^t) = im(D^t)$, which implies that $im(A^t) = (V^{-1})^t \cdot im(D^t)$.

Lemma 4 *Consider the equation $A\overline{x} = \overline{b}$ for fixed matrix $A \in \mathbf{Z}^{\mu,\mathcal{T}}$ and fixed column matrix $\overline{b} \in \mathbf{Z}^{\mu}$. Suppose $UAV = D$, reduces A to Smith-normal form, and that $d_1, \ldots, d_l$ represents the invariant factors of A. Then $A\overline{x} = \overline{b}$ has a solution iff for $i = 1, \ldots, l$, invariant factor d_i divides $\sum_{j=1}^{\mathcal{T}} u_{ij} b_i$ and for all $i = l+1, \ldots, \mu$ we have $\sum_j u_{ij} b_i = 0$, where u_{ij} is the ij term of the matrix U.*

Due to limited space we omit the proof.
Suppose we have reduced $A \in \mathbf{Z}^{\mu,\mathcal{T}}$ to Smith-normal form and we have derived

$$DV^{-1}\overline{x} = U\overline{b}. \tag{1}$$

In light of Lemma 4, we make the following observations. Observe that $l \leq min(\mu, \mathcal{T})$, and that $U \in \mathbf{Z}^{\mu,\mu}$ and $V \in \mathbf{Z}^{\mathcal{T},\mathcal{T}}$. Also note that $D \in \mathbf{Z}^{\mu,\mathcal{T}}$ and $U\bar{b} \in \mathbf{Z}^{\mu}$, where the $l+1^{st}$ through the μ^{th} rows of D and $U\bar{b}$ consists of zeros. Therefore we can delete a suitable number of zero rows (or add zero rows if appropriate) of D and $U\bar{b}$, respectively, without altering the equality of the left and right hand sides of equation (1) until we form matrices with $\mathcal{T}$ rows. We will denote these two matrices by D_{del} and $(U\bar{b})_{del}$, respectively (now note that $D_{del} \in \mathbf{Z}^{\mathcal{T},\mathcal{T}}$ and $(U\bar{b})_{del} \in \mathbf{Z}^{\mathcal{T}}$). Also note that we will still have $D_{del}V^{-1}\overline{x} = (U\bar{b})_{del}$.
Let U' denote the product of elementary matrices which will normalize the nonzero diagonal entries of D_{del} (i.e. divide the diagonal entries by the invariant factors). Then $U' \in \mathbf{Q}^{\mathcal{T},\mathcal{T}}$, where $\mathbf{Q}$ denotes the set of rational numbers. Note that $(U')^{-1} \in \mathbf{Z}^{\mathcal{T},\mathcal{T}}$ and that

$$U'D_{del}V^{-1}\overline{x} = U'(U\bar{b})_{del} \text{ where } U'(U\bar{b})_{del} \in \mathbf{Z}^{\mathcal{T}}.$$

Lastly note that since U' does not modify rows $l+1$ through $\mathcal{T}$, and that the $l+1^{st}$ row through the $\mathcal{T}^{th}$ row of $U'(U\bar{b})_{del}$ will still consist of zeros. Let $X' = U'(U\bar{b})_{del}$.

Lemma 5 *$\overline{x}$ is a solution to the equation $A\overline{x} = \overline{b}$ (provided a solution exists) iff there exist integers $z_{l+1}, \ldots, z_{\mathcal{T}}$ such that $\overline{x} = V\left(X' + [0, \ldots, 0, z_{l+1}, \ldots, z_{\mathcal{T}}]^t\right)$*

Again, due to limited space we omit the proof.
We define $||\cdot||$ to be a function $||\cdot|| : \mathbf{Z}^{\tau} \longrightarrow \mathbf{Z}$, such that $||\cdot||$ is additive, that is, $||\overline{x} + \overline{y}|| = ||\overline{x}|| + ||\overline{y}||$. [3] Then for all integers a, $||a\overline{x}|| = a||\overline{x}||$. Throughout this paper we will use $||\overline{x}|| = \sum_{i=1}^{\tau} x_i$ where $\overline{x} = [x_1, \ldots, x_\tau]^t$. However one could make several different choices for $||\cdot||$ (the choice of $||\cdot||$ will be dependent on the target vector used in the integer span program).

4 GILTS and Black-box secret sharing

4.1 Definition of a t out of n group independent linear threshold sharing scheme

As introduced in [26], a group independent linear threshold sharing scheme is defined as:

Definition 1 *[26] Let $\mathbf{K} = \{\mathcal{K} | \mathcal{K}$ is a finite abelian group$\}$. A group independent t out of n linear threshold scheme or GILTS is an ordered pair $(\Psi, \mathcal{S})$ such that:*
(1) For each $\mathcal{K} \in \mathbf{K}$ and for each $i = 1, \ldots, n$ there corresponds a sharespace $S_{i,\mathcal{K}}$. We write $\mathcal{S}_i = \{S_{i,\mathcal{K}} : \mathcal{K} \in \mathbf{K}\}$ and $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_n)$.
(2) For all $B \in \Gamma_0$ and for all i there exists a function $\psi_{B,i}$ such that for all $\mathcal{K} \in \mathbf{K}$, $\psi_{B,i} : S_{i,\mathcal{K}} \longrightarrow \mathcal{K}$ is a homomorphism. Further, for all $k \in \mathcal{K}$, shares $\overline{s}_i$ belonging to $S_{i,\mathcal{K}}$ are distributed to participant P_i such that $\forall B \in \Gamma_0$, $k = \sum_{i \in B} \psi_{B,i}(\overline{s}_i)$ (here k is the secret that owuld be shared out),
(i) (privacy) $Prob(\mathbf{k} = k | \overline{\mathbf{s}}_{i_1} = \overline{s}_{i_1}, \ldots, \overline{\mathbf{s}}_{i_{t-1}} = \overline{s}_{i_{t-1}}) = Prob(\mathbf{k} = k)$, and
(ii) (completeness) $Prob(\mathbf{k} = k | \overline{\mathbf{s}}_{i_1} = \overline{s}_{i_1}, \ldots, \overline{\mathbf{s}}_{i_t} = \overline{s}_{i_t}) = 1$.

[3] We are abusing the traditional use of $||\cdot||$ notation since norms are nonnegative, whereas in our definition there will be $\overline{x}$ such that $||\overline{x}|| < 0$.

Thus in a GILTS $(\Psi, \mathcal{S})$, the Ψ refers to a collections of group independent functions which map sharespaces to the secret space (group), and $\mathcal{S}$ refers to a collection of sharespaces. We now make a series of assumptions. The same assumptions were made in [26], they are:

- We assume that $S_{i,\mathcal{K}}$ is the direct product $\mathcal{K}^{a_i}$ (since this is the only method known to achieve group independent sharing). Here $S_{i,\mathcal{K}}$ denotes participant P_i's share space, $\mathcal{K}$ is the keyspace (group), and a_i is some positive integer which will denote the number of subshares given to participant P_i.
- It is assumed that $\psi_{B,i}$ is a row matrix (with a_i columns) of integers (i.e. P_i possesses subshares which belong to the keyspace), such that $\psi_{B,i}(\overline{s}_i) = \psi_{B,i} \cdot \overline{s}_i$ where the latter is the scalar dot product between an integer vector and a vector containing group entries.
- When we use Ψ to describe a group independent t out of n threshold scheme, then Ψ will denote an integer matrix, i.e. $\Psi \in \mathbf{Z}^{\mu,\mathcal{T}}$ where $\mathcal{T} = \sum_{i=1}^{n} a_i$. We assume that Ψ has a partition into n submatrices. i.e. $\Psi = [A_1|\cdots|A_n]$. Shares are distributed to the n participants (which we collectively represent by $\overline{s}$) such that

$$\Psi \overline{s} = \overline{k} \text{ where } \overline{k} = [k, k, \ldots, k]^T. \tag{2}$$

Suppose that Ψ is reduced to Smith-normal form. Then there exists $U \in GL(\mu, \mathbf{Z})$ and $V \in GL(\mathcal{T}, \mathbf{Z})$ such that $U\Psi V = D$. Let l denote the rank of Ψ.

Then $U\Psi VV^{-1}\overline{s} = U\overline{k}$. Hence $DV^{-1}\overline{s} = U\Psi VV^{-1}\overline{s} = U\overline{k}$. Consider the first l rows of the column matrix $U\overline{k}$. Each row can be interpreted as an integer $\sum_j \alpha_j u_{ij}$ applied to k. It follows then that $d_i|(\sum_j \alpha_j u_{ij})$. Since $d_i|\sum_{j=1}^{\mu} \alpha_j u_{ij}$ (for $i = 1, \ldots, l$), we can divide each of the first l rows by the corresponding d_i and still retain the form of an integer matrix. It follows then that we have

$$\begin{bmatrix} I_{l\times l} & 0_{l\times(\mathcal{T}-l)} \\ 0_{(\mu-l)\times l} & 0_{(\mu-l)\times(\mathcal{T}-l)} \end{bmatrix} V^{-1}\overline{s}$$
$$= [k\frac{\sum_{i=1}^{\mu}\alpha_i u_{1i}}{d_1}, \ldots, k\frac{\sum_{i=1}^{\mu}\alpha_i u_{li}}{d_l}, 0, \ldots, 0]^T.$$

Let $R = \mathcal{T} - l$, and let $r_1, \ldots, r_R$ be chosen uniformly at random from $\mathcal{K}$. Then

$$V^{-1}\overline{s} = [k\frac{\sum_{i=1}^{\mu}\alpha_i u_{1i}}{d_1}, \ldots, k\frac{\sum_{i=1}^{\mu}\alpha_i u_{li}}{d_l}, r_1, \ldots, r_R]^T.$$

Therefore

$$\overline{s} = V[\frac{\sum_{i=1}^{\mu}\alpha_i u_{1i}}{d_1}k, \ldots \frac{\sum_{i=1}^{\mu}\alpha_i u_{li}}{d_l}k, r_1, \ldots, r_R]^T. \tag{3}$$

Represent V as $V = [X|Y]$, where X is a $\mathcal{T} \times l$ matrix (which is formed by using the first l columns of V). Then $\overline{s}$ can be represented as

$$\overline{s} = C[k, r_1, \ldots, r_R]^T, \tag{4}$$

where $C = \left[X \cdot [\frac{\sum_{i=1}^{\mu}\alpha_i u_{1i}}{d_1}, \ldots, \frac{\sum_{i=1}^{\mu}\alpha_i u_{li}}{d_l}]^T | Y\right]$. Consequently the application of Smith-normal form on an integer matrix that describes how the shareholders reconstruct the secret will provide the distributor's matrix C as to how to construct the shares. Further, the total number of subshares $\mathcal{T} = \sum a_i$ can be expressed as $R + l$. R is the number of random elements required, and l is the rank of Ψ.

In [17] the following necessary privacy condition was established. Because it is integral to an argument made in a later proof we provide an outline of the proof in the appendix.

Theorem 1 *[17, 27] For all $B \subset \{P_1, \ldots, P_n\}$ with $B \notin \Gamma$, there exist matrices $Y_B \in \mathbf{Z}^{\mathcal{T}_B, R}$ and $Z_B \in \mathbf{Z}^R$ such that $\overline{s}_B = Y_B(Z_B k + \overline{r})$ where $\mathcal{T}_B = \sum_{i\in B} a_i$ and $\overline{r} = [r_1, \ldots r_R]^t$.*

Remark: Because one only needs to use a basis for the row span of Ψ, we will assume from now on that Ψ consists of l rows where l is the rank of Ψ and that $\Psi\overline{s} = [k, k, \ldots, k]^t$. If Ψ did not conform to this assumption one could perform row operations on Ψ to zero out the unneeded rows and drop these zeroed rows to form a new Ψ' which does conform to this assumption. Second, note that $\Psi \cdot C = [\overline{1}, \overline{0}, \ldots, \overline{0}]$ where $\overline{1} = [1, 1, ..., 1]^t$ and $\overline{0} = [0, 0, ..., 0]^t$.

4.2 Black-box secret sharing and integer span programs

At Crypto 2002 Cramer and Fehr [10] introduced what they called Black-box secret sharing. An important tool that was utilized in the development of black-box secret sharing scheme was their generalization of the Karchmer and Widgerson monotone span program [24]. Monotone span programs have been shown to be equivalent to linear secret sharing [2, 21, 24, 31]. Here Cramer and Fehr generalized the monotone span program over arbitrary rings. Of particular interest to group independent threshold sharing schemes would be span programs over the set of integers, i.e. integer span programs.
Let S denotes a (not necessarily finite) commutative ring with 1. Let Γ be a monotone access structure on $\{1, ..., n\}$, and let $M \in S^{d,e}$ be a matrix whose d rows are labelled by a surjective function $\rho : \{1, ..., d\} \rightarrow \{1, ..., n\}$.

Definition 2 *[10] $\epsilon = (1, 0, ..., 0)^t \in S^e$ is called the target vector. $\mathcal{M} = (S, M, \rho, \epsilon)$ is called a monotone span program (over the ring S). If $S = \mathbf{Z}$, it is called an integer span program, or ISP, for short. The size of the ISP is defined as $size(M) = d$, where d is the number of rows of M .*

Definition 3 *[10] Let Γ be a monotone access structure and let $\mathcal{M} = (S, M, \rho, \epsilon)$ be a monotone span program over S. Then M is a monotone span program for Γ, if for all $A \subset \{1, ..., n\}$ the following holds.*
(i) (completeness) If $A \in \Gamma$, then $\epsilon \in im(M_A^t)$.
(ii) (privacy) If $A \notin \Gamma$, then there exists $\kappa = (\kappa_1, ..., \kappa_e)^t \in ker(M_A)$ with $\kappa_1 = 1$.

One says that M computes Γ.

Definition 4 *[10] Let Γ be a monotone access structure on $\{1, ..., n\}$, let $M = \mathbf{Z}^{d,e}$ matrix, ρ be a surjective labeling of the rows of M to $\{1, ..., n\}$. For each $A \in \Gamma$ let $\lambda(A) \in \mathbf{Z}^{d_A}$. Let E be the collection of all $\lambda(A)$. Then (M, ρ, E) is called an integer Γscheme*

Formally the definition of Blackbox secret sharing is:

Definition 5 *[10] Let Γ be a monotone access structure on $\{1, ..., n\}$ and let $\mathcal{B} = (M, \rho, E)$ be an integer Γscheme. Then $\mathcal{B}$ is a blackbox secret sharing scheme for Γ if the following holds. Let G be an arbitrary finite Abelian group G, and let $A \subset \{1, ..., n\}$ be an arbitrary nonempty set. For arbitrarily distributed $s \in G$, let $\overline{g} = (g_1, ..., g_e)^t \in G^e$ be drawn uniformly at random, subject to $g_1 = s$. Define $\overline{s} = M\overline{g}$. Then:*
(Completeness) If $A \in \Gamma$, then $\overline{s}_A^t \lambda(A) = s$ with probability 1, where $\lambda(A) \in E$ is the reconstruction vector for A.
(Privacy) If $A \notin \Gamma$, then $\overline{s}_A$ contains no Shannon information on s.

Theorem 2 *[10] Let Γ be a monotone access structure on $\{1, ..., n\}$, and let $\mathcal{B} = (M, \rho, E)$ be an integer Γscheme. Then $\mathcal{B}$ is a blackbox secret sharing scheme for Γ if and only if $\mathcal{M} = (S, M, \rho, \epsilon)$ is an ISP for Γ and for all $A \in \Gamma$, its reconstruction vector $\lambda(A) \in E$ satisfies $M_A^t \lambda(A) = \epsilon$.*

5 Some observations concerning a GILTS and an ISP

We modify the definition of integer span program (ISP) using a different completeness and privacy condition. This definition will be equivalent to the definition of an ISP as given in [10], but we use the target vector $\overline{1} = [1, 1, ..., 1]^t$ rather than ϵ. Due to this choice, we need to make other modifications to the definition of an ISP. As a side remark, we note that there are numerous equivalent versions of ISP using different target vectors. Our choice of this target vector is strategic in that the target vector $\overline{1}$ is a target vector that best illustrates the construction of the reconstruction matrix for the dual scheme.

Definition 6 *We say that $(M, \Gamma, \rho, \overline{1})$ is an integer span program over Γ provided*
(i)(completeness) for all $A \in \Gamma$ there exists $\overline{1} \in im(M_A^t)$ i.e. there exists $\overline{x}$ such that $\overline{1} = M_A^t \overline{x}$
(ii) (privacy) for all $A \notin \Gamma$, there exists a $\overline{x}$ with $\sum x_i = 1$ such that $\overline{x} \in ker(M_A)$.

Here ρ is the labeling of the rows of M (we will assume that M^t is an n-partitioned matrix). If $(M, \Gamma, \rho, \overline{1})$ is an ISP over Γ where Γ is the collection of all sets of participants that contain t or more members, then we will say that $(M, \Gamma, \rho, \overline{1})$ computes T_t^n (so T_t^n implies an ISP which computes a t out of n threshold). If $(M, \Gamma, \rho, \overline{1})$ is an ISP that computes T_t^n, then we will say that M is an ISP that computes T_t^n with target vector $\overline{1}$. This definition is equivalent to Cramer and Fehr's.
Suppose Ψ is a t out of n GILTS, we construct a integer span program M in the following way. Recall that the representation of $\overline{s}$ given by (4), $\overline{s} = C[k, r_1, \ldots, r_R]^t$. We define the $\mathcal{T} \times (R+1)$ matrix M by $M = C \cdot F$ where F and F^{-1} are respectively

$$F = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \quad F^{-1} = \begin{bmatrix} 1 & -1 & -1 & \cdots & -1 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}. \tag{5}$$

For $i = 1, .., R+1$, let $\vec{e}_i \in \mathbf{Z}^{1,R+1}$ be the row vector with a 1 in the i^{th} column and zeros elsewhere. Then $\vec{e}_1 \cdot F = [1, 1, ..., 1]$ and for $2 \leq i \leq R+1$, $\vec{e}_i \cdot F = \vec{e}_i$. Lastly note that if $\overline{x}$ is such that $\sum x_i = 1$ then the first coordinate of $F \cdot \overline{x}$ is 1.
Now note that $\overline{s}$, which is defined by equation (4), can be expressed as

$$\overline{s} = M \cdot F^{-1} \cdot [k, r_1, \cdots, r_R]^t \tag{6}$$

In [10], the following result was established using the target vector ϵ. We establish this result for the target vector $\overline{1}$ and our definition of an ISP. This result demonstrates that our use of the target vector $\overline{1}$ in the definition is appropriate. In addition, this proof will merge several ideas from [10] with [26] and [16]. However due to space consideration we have moved the proof to the appendix.

Theorem 3 *[10] M is an integer span program which computes T_t^n with target vector $\overline{1} = [1, 1, \ldots, 1]$ iff Ψ is a t out of n GILTS.*

6 The dual

If Γ is an access structure for a secret sharing scheme, then the dual of this secret sharing scheme is a secret sharing scheme whose access structure is $\{B \subset \{P_1, ..., P_n\} : B \notin \widetilde{\Gamma}\}$. The dual of the t out of n threshold sharing scheme is a $n - t + 1$ out of n threshold sharing scheme (and vice versa). The dual of t out of n threshold scheme has been discussed thoroughly in literature [2, 21, 18, 31], however all of these have been limited to sharing over finite fields. At Crypto 2002, Cramer and Fehr [10] established

that for each ISP which computes T_t^n there exists an ISP, of equal size, which computes T_{n-t+1}^n. Their proof was a constructive proof in that they constructed the T_{n-t+1}^n ISP from the ISP which computed T_t^n. Our contribution here shows how to construct the dual from a t out of n GILTS. It will become apparent how to construct a $n-t+1$ out of n GILTS from a t out of n GILTS. Again recall that we are using an target vector different than the one use in [10]. Our construction of the dual will demonstrate why we choose to use the target vector equal to $\overline{1}$.

Suppose Ψ is a t out of n GILTS, such that shares $\overline{s}$ are distributed to participants so that $\Psi\overline{s} = \overline{k}$ where $\overline{k}^t = [k, k, \ldots, k]$. Let M represent the integer span program derived from Ψ which computes T_t^n. Thus $\Psi \cdot M = [\overline{1}, \ldots, \overline{1}]$. Let $M_{dual} = \Psi^t$ and let $\Psi_{dual} = M^t$. We claim that M_{dual} is a an integer span program which can compute T_{n-t+1}^n, and that Ψ_{dual} is a $n-t+1$ out of n GILTS.

Theorem 4 *[10] M_{dual} is a an integer span program which computes T_{n-t+1}^n.*

Proof. We first consider the privacy condition. Let A be a set of participants satisfying $|A| < n-t+1$. Let $\tilde{A} = 2^{\mathcal{P}} \setminus A$, then $|\tilde{A}| \geq t$. Since $|\tilde{A}| \geq t$, there exists a subset of $\tilde{A}$ which contains t or more participants. Fix some set $B \subseteq \tilde{A}$ of t participants. Observe that $\Psi_B M_B = [\overline{1}, ...\overline{1}]$. Therefore there exist integers $w_1, \ldots, w_l$ with $\sum w_i = 1$ such that the linear combination $\sum w_i\vec{\psi}_i$ describes how the participants in B compute the secret k, using the t out of n GILTS Ψ. Observe that $B \cap A = \emptyset$. Thus $\sum w_i\vec{\psi}_i$ has zeroed all entries in Ψ whose columns belong to A. i.e. $\sum w_i\vec{\psi}_{A,i} = \vec{0}$. Here $\vec{\psi}_{A,i}$ refers to those entries in the i^{th} row of Ψ_A, where Ψ_A is those columns of Ψ which pertain to the members in A. Let $\overline{w} = [w_1, \ldots, w_l]^t$. Then $\Psi_A^t\overline{w} = \overline{0}$. i.e. $M_{dual}\overline{w} = \overline{0}$. Consequently $\overline{w} \in ker(M_{dual})$ and $||\overline{w}|| = 1$.

Now suppose A is a subset such that $|A| \geq n-t+1$. We will assume without loss of generality $|A| = n-t+1$ We will now establish that $\overline{1} \in im(M_{A,dual}^t)$. Observe that $\tilde{A} = 2^{\mathcal{P}} \setminus A$ is such that $|\tilde{A}| = t-1$. Thus there exists $\overline{x} \in \mathbf{Z}^{R+1}$ such that $M_{\tilde{A}}\overline{x} = \overline{0}$ and $||\overline{x}|| = 1$. Now $\Psi \cdot M = [\overline{1}, ..., \overline{1}]$. Also observe that $\Psi \cdot M \cdot \overline{x} = [\overline{1}, ..., \overline{1}] \cdot \overline{x} = \overline{1}$. The last statement is true because $||x|| = 1$. Since $M_{\tilde{A}}\overline{x} = \overline{0}$ we see that $\Psi_{\tilde{A}}M_{\tilde{A}}\overline{x} = \overline{0}$. Now $\Psi \cdot M \cdot \overline{x} = \Psi_{\tilde{A}}M_{\tilde{A}}\overline{x} + \Psi_A M_A\overline{x} = \overline{1}$ and so $\Psi_A M_A\overline{x} = \overline{1}$. Let $\overline{z} = M_A\overline{x}$. Then $M_{A,dual}^t\overline{z} = \Psi_A\overline{z} = \Psi_A M_A\overline{x} = \overline{1}$. Hence $\overline{1} \in im(M_{A,dual}^t)$ and so the proof is complete. □

Corollary 1 *Ψ_{dual} is a $n-t+1$ out of n GILTS.*

If Ψ is a t out of n GILTS, then we will use an $*$ to refer to the corresponding dual GILTS. Thus $\Psi^* = M^t$, $M^* = \Psi^t$ and $C^* = M^* \cdot F^{-1}$ (where F^{-1} represents the $l \times l$ matrix described by (5)). That is the transpose of the ISP is the reconstruction matrix of the dual. A result which is very ironic, that is, the shareholders reconstruction matrix can be used to develop the distributor sharing matrix for the dual. Let R^* denote the number of random elements needed to generate the GILTS Ψ^*, and let l^* denote the rank of Ψ^*. Then $R^* = l - 1$ and $l^* = R + 1$.

Example 1 *Consider the following 2 out of 3 GILTS. Suppose k is the secret and two random elements r_1, r_2 are selected uniformly random from the group. Now suppose that the dealer deals the following shares to the 3 participants: $\overline{s}_1 = (k - r_1, r_2)$, $\overline{s}_2 = k - r_2$ and $\overline{s}_3 = (r_1, r_2)$. Then*

$$\Psi = \left[\begin{array}{cc|c|cc} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right].$$

It can be shown that

$$C = \left[\begin{array}{ccc} 1 & -1 & 0 \\ 0 & 0 & 1 \\ \hline 1 & 0 & -1 \\ \hline 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right] \qquad \text{where } \overline{s} = \left[\begin{array}{c} s_{11} \\ s_{12} \\ s_{21} \\ s_{31} \\ s_{32} \end{array}\right]$$

where

$$M = \left[\begin{array}{ccc} 1 & 0 & 1 \\ 0 & 0 & 1 \\ \hline 1 & 1 & 0 \\ \hline 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right]$$

here $M = C \cdot F$ where F is a 3×3 matrix. Observe that $\overline{s} = [\overline{s}_1, \overline{s}_2, \overline{s}_3]^t = C \cdot [k, r_1, r_2]^t$. Now $\Psi^* = M^t$ describes a $3 - 2 + 1 = 2$ out of 3 GILTS.

For another example of the construction of the dual given a Ψ (GILTS), we refer the reader Example 2 in the appendix. We now summarize how to construct the dual. The algorithm is based on equation (3) and equation (4).

Algorithm 1 *(Input = Ψ; Output = Ψ^*)*
Let Ψ be a t out of n GILTS. Assume that $\Psi \in \mathbf{Z}^{l,\mathcal{T}}$ where l= rank of Ψ. Observe that to determine $\overline{s}$ such that $\Psi\overline{s} = \overline{k}$ is comparable to solving $\Psi\overline{x} = \overline{1}$.

(i) Reduce Ψ to Smith-normal form. i.e. $U\Psi V = D$. (Then $U\Psi VV^{-1}\overline{x} = U\overline{1}$.)

(ii) Let $U'\overline{1}$ denote the column matrix generated by dividing each row of $U\overline{1}$ by the invariant factor d_i of D.

(iii) Represent V by $V = [X|Y]$ where X denoted the first l columns of V and Y denotes the remaining R columns of V.

(iv) Let

$$C = \left[X \cdot U'\overline{1} \,|\, Y\right]$$

(iv) Set $M = C * F$ where F is given by equation (5).

(v) Lastly, let $\Psi^* = M^t$.

Observe that this algorithm can be used as well to output the ISP M, since $M = (\Psi^*)^t$. Further this algorithm can be used to determine C, since C is computed in step (iv) of the algorithm. If the reader is interested in an algorithm which can compute a Ψ, there are several in literature including [15, 16]. Some of the methods defined to compute secret sharing schemes over fields can be modified to generate group independent sharing schemes. For example one can modify the monotone circuit construction algorithm in [30] to generate a group independent sharing scheme.

7 An ISP M implies the reconstruction matrix Ψ

In [10], the authors constructed a ISP of size $O(n \log_2 n)$ which computed T_t^n with a target vector $\epsilon = [1, 0, \ldots, 0]$. The authors then suggested that the corresponding Blackbox secret sharing could be generated using techniques in [16]. We point out that by utilizing the Smith-normal form technique on the dual, we can generate the reconstruction matrix Ψ. Let us denote the ISP developed [10] which computes T_t^n and has target vector ϵ by W. Then set $M = W \cdot F$ where F is given by (5). It follows that M is an ISP which computes T_t^n with target vector $\overline{1}$. Given M, we know that $\Psi^* = M^t$ is a $n - t + 1$ out of n GILTS. Using the Smith-normal form derivation method, given Ψ^* we can compute C^* by using equation (4). We then can compute $M^* = C^* \cdot F$. Now set $\Psi = (M^*)^t$. Thus we have constructed the reconstruction function Ψ for the secret sharing scheme implied by the ISP W.

From the above remark we see that by starting with an ISP M, we can construct Ψ, by utilizing the dual. We now ask if we go in a complete circle will we derive M. That is, will M^{**} always be equivalent[4]

[4]Here equivalent $im(M^{**})^t) = im(M^t)$

to M. We can ask the analogous question will Ψ^{**} always be equivalent[5] to Ψ. The answer to both of these questions is no, the proof is by example.

Theorem 5 *There exists a Ψ, a t out of n GILTS, such that $im(\Psi^{**}) \neq im(\Psi)$. Similarly there exists an ISP M which computes T_t^n such that $im((M^{**})^t) \neq im(M^t)$.*

The proof is given by Example 3 in the appendix.

8 Randomness required to generate a GILTS

Because one needs to seed a sharing scheme with truly random elements, it is important for the distributor to know the randomness requirement needed to generate a secret sharing scheme. Considerable amount of work has been done on generating bounds on randomness in secret sharing schemes, see [5, 6, 7, 8, 11, 12]. In the cases of [6, 11] it was to develop randomness bounds for secret sharing schemes, that were not necessarily threshold sharing schemes. In [7, 8], bounds were developed for multisecret sharing scheme and/or dynamic threshold scheme. Bounds on the amount of randomness in group independent sharing schemes have been discussed in [26].

Theorem 6 *[26] For a t out of n GILTS, the number R of random elements needed to generate a GILTS satisfies $R+1 \geq \sqrt{1+\log_2 \binom{n}{t-1}}$.*

The bound $R+1 \geq 1+\log_2 \binom{n}{t-1}$ can be established under certain conditions[6]. We now find that we can improve upon all the bounds as a consequence of the following result and Theorem 4.
From [27] the following was established.

Theorem 7 *[27] If Ψ is a t out of n GILTS then the rank l of Ψ is bounded by $l \geq 1+\log_2 \binom{n}{t}$.*

We now observe that the rank l^* of a $n-t+1$ out of n GILTS Ψ^* must satisfy $l^* \geq 1+\log_2 \binom{n}{n-t+1}$. Since $l^* = R+1$, we find that the following is true.

Theorem 8 *If Ψ is a t out of n GILTS then the number R of random elements needed to generate a GILTS is bounded by $R \geq \log_2 \binom{n}{n-t+1}$.*

Since the bound in Theorem 7 is tight in the case $n-t+1 = n-1$, it immediately follows that the bound Theorem 8 is tight when $t=2$. Observe that $\binom{n}{t-1} = \binom{n}{n-t+1}$ and so this new randomness bound has improved upon Theorem 6, no longer requiring the square root.
The following result was established in [10]. We restate it using our notation.

Theorem 9 *[10] Let Ψ denote a t out of n GILTS then the size of Ψ, denoted by $\mathcal{T} = \sum_{i=1}^{n} a_i$ is bounded by $\Omega(n \log n)$.*

Using the above bound, the bounds on rank and randomness can be improved upon. First we need to state a result from [26].

[5] By equivalent we are referring to the condition that the row spans of each matrix are equal to each other. $im(\Psi^{**}) = im(\Psi)$.

[6] If any set of t participants can not only compute k but possess enough information that they can compute all shares distributed to the n participants.

Theorem 10 *[26] For each $i = 1, \ldots, n$, either the rank of A_i equals the size of $\overline{s}_i$ or participant P_i can reduce his share size to the rank of A_i. Thus one can assume that the rank of A_i is equal to a_i (the number of columns of A_i).*

Theorem 11 *Let Ψ be a t out of n GILTS and l the rank of Ψ, then $l \geq 1 + \log_2(n \cdot (n-1) \cdots (t+1))$.*

Proof. We provide a sketch of the proof. Recall $\Psi = [A_1 | \cdots | A_n]$ where A_i is a $l \times a_i$ matrix. Since the size of a ISP which computes T_t^n is $\Omega(n \log_2 n)$, we have $\sum_{i=1}^{n} a_i \geq n \log_2 n$. Therefore there exists an i such that $a_i \geq \log_2 n$. We will assume without loss of generality that $i = 1$ (otherwise we would interchange submatrices until we have interchanged A_i with A_1). By Theorem 10, each A_i has rank a_i. To establish the lower bound on rank we reduce Ψ to a triangular form (we do not require the leading entry to be a one) and make an argument about the number of rows remaining in the triangularized Ψ. Since A_1 has rank $a_1 \geq \log_2 n$, if U_1 is the product of elementary row operations that triangularize the first a_1 columns, then $U_1\Psi$ will have at least a_1 nonzero rows. Now consider the GILTS where we remove participant P_1, this is a t out of $n-1$ scheme. By Theorem 9 this requires $\Omega((n-1)\log_2(n-1))$ shares, so there exists a submatrix for which has at least $\log_2(n-1)$ column entries in the rows where participant P_1 does not participate that were not affected by row operations U_1. We assume without loss of generality that this is submatrix A_2. We continue the process of triangularizing, however we now use $U_1\Psi$. Since U_1 has not modified at least $\log_2(n-1)$ columns of A_2, if we let U_2 be the product of elementary row operations that triangularize the columns $a_1 + 1$ through a_2, then $U_2U_1\Psi$ has at least $\log_2 n + \log_2(n-1)$ nonzero rows. So far we see that $l \geq \log_2 n + \log_2(n-1)$. We continue this process. At the $n-t-1$ stage we have triangularized the first $\sum_{i=1}^{n-t-1} a_i$ columns od Ψ, we have computed $U_{n-t-1} \cdots U_2U_1\Psi$ and we have established $l \geq \log_2 n + \log_2(n-1) + \cdots + \log_2(n-(n-t-1)+1)$. At this stage we can see that by removing participants $P_1, \ldots, P_{n-t-1}$ we still have a t out of $t+1$ scheme. By Theorem 9 we see that the number of shares is $\Omega((t+1)\log_2(t+1))$. Thus there exists a submatrix for which at least $\log_2(t+1)$ columns entries in the rows for which participants $P_1, \ldots, P_{n-t-1}$ do not participate that were not affected by $U_{n-t-1} \cdots U_2U_1$. We assume without loss of generality this is submatrix A_{n-t}. We now continue the triangularization process focusing on columns $\sum_{i=1}^{n-t-1} a_i + 1$ though $\sum_{i=1}^{n-t} a_i$. Again the matrix product $U_{n-t-1} \cdots U_2U_1$ has not modified at least $\log_2(t+1)$ of these columns. Let U_{n-t} be the product of elementary row matrices which triangularize these columns, then $l \geq \log_2 n + \log_2(n-1) + \cdots + \log_2(t+2) + \log_2(t+1)$. Now consider the removal of participant $P_1, \ldots, P_{n-t}$, what remains is a t out of t scheme, thus each participant must be given at least one subshare. As we continue to triangularize we see that in columns $\sum_{i=1}^{n-t} a_i + 1$ though $\sum_{i=1}^{n-t+1} a_i$ there must be at least one column entry in the rows for which participants $P_1, \ldots, P_{n-t}$ do not participate which has not been modified by the product $U_{n-t} \cdots U_2U_1$. Hence $l \geq 1 + \log_2 n + \log_2(n-1) + \cdots + \log_2(t+2) + \log_2(t+1)$ Thus $l \geq 1 + \log_2(n \cdot (n-1) \cdots (t+2) \cdot (t+1))$, and so the proof is complete. □

Theorem 12 *If Ψ is a t out of n GILTS then the number R of random elements needed to generate the GILTS is bounded by $R \geq \log_2(n \cdot (n-1) \cdots (n-t+3) \cdot (n-t+2))$.*

Proof. Let Ψ be a t out of n GILTS. Let M denote the ISP which computes T_t^n. Then $\Psi^* = M^t$ is a $n-t+1$ out of n GILTS. Therefore by Theorem 11, $l^* \geq 1 + \log_2(n \cdot (n-1) \cdots (n-t+1+1))$. Since $1 + R = l^*$, we have $R \geq \log_2(n \cdot (n-1) \cdots (n-t+2))$. □

This bound on randomness, as well as the bound on the rank of Ψ, is a significant improvement on all previous bounds on rank and randomness of group independent threshold sharing schemes. These bounds most definitely reflect (not necessarily tightly in all cases) known values for rank and randomness of GILTS constructed with minimal number of subshares. For example we know of a 7 out of 8 GILTS which requires the minimal number of subshares 24 and has minimal rank of 4 hence $R = 20$. Previous randomness bounds did not explain why R needed to be so close to 24. The randomness bound described

in Theorem 12 clearly demonstrates that if $n-t$ is small then R will be asymptotically close to $\log_2 n!$. Lastly, Cramer and Fehr have established that $\mathcal{T} = \sum_{i=1}^{n} a_i$ has an asymptotic bound of $\Omega(n \log n)$. Notice that $\mathcal{T} = l + R \geq 1 + \log_2(n \cdot (n-1) \cdots (t+2) \cdot (t+1)) + \log_2(n \cdot (n-1) \cdots (n-t+3) \cdot (n-t+2)) \geq \log_2(n!)$. Asymptotically $O(\log_2(n!)) = O(n \log_2 n)$, and so it does not appear that one could make any improvements on these bounds from an asymptotic sense.

9 Necessary and sufficient conditions for a GILTS

Let $\Psi \in \mathbf{Z}^{l,\mathcal{T}}$ be a $l \times \mathcal{T}$ integer matrix. Suppose that there exists a function ρ which assigns to each column of Ψ a member of $\{1, 2, ..., n\}$. To this end, by rearranging columns we can just assume that ρ implies a partition of Ψ such that $\Psi = [A_1|A_2|\cdots|A_n]$. We will assume that the column rank of A_i is equal to the number of columns of A_i. And lastly we will assume that the rank of Ψ is l.

We now ask what are the necessary conditions for Ψ to define a t out of n GILTS. That is, what are the formal requirements for Ψ to satisfy Definition 1?

The necessary and sufficient conditions for Ψ to be a t out of n GILTS can be summarized as follows

(i) The integer matrix equation $\Psi\overline{x} = [1, 1, \ldots 1]^t$ must be solvable. Thus Ψ must satisfy Lemma 4.

(ii) For each $B \in \Gamma$ there exists integers $x_1, \ldots x_\mu$ where $\sum x_i = 1$ such that the linear combination $\sum_{i=1}^{\mu} x_i \vec{\psi}_i$ reduces to a row vector whose column entries that correspond to participants in $\tilde{B}$ are zero.

(iii) Theorem 1 must be satisfied for all $B \subset \{P_1, ..., P_n\}$ with $B \notin \Gamma$.

In light of recent work in [10] and our observations we can revise the necessary and sufficient conditions to a set of criteria that only Ψ needs to satisfy. That is, we have the following.

Theorem 13 *The necessary and sufficient conditions for Ψ to be a t out of n GILTS is:*

(i) for all $B \subset \{P_1, \ldots, P_n\}$ with $|B| \geq n - t + 1$ there exists $\overline{x}$ such that

$$\overline{1} = \Psi_B \overline{x}, \text{ and}$$

(ii) for all $B \subset \{P_1, \ldots, P_n\}$ with $|B| \leq n - t$ there exists $\overline{x}$ with $||x|| = \sum x_i = 1$ such that

$$\overline{0} = \Psi_B^t \overline{x}.$$

Proof.

First we establish that these conditions are necessary. Suppose Ψ is a t out of n GILTS. Then we can construct the ISP M with target vector $\overline{1}$. By Theorem 4, the dual ISP $M^* = \Psi^t$ where M^* computes T^n_{n-t+1}. Now consider the completeness condition. Thus for each B with $|B| \geq n - t + 1$ there exists $\overline{x}$ such that $\overline{1} = (M^*_B)^t \overline{x} = \Psi_B \overline{x}$. Now consider the privacy condition. Let B be a set of participants with $|B| \leq n - t$. Then there exists $\overline{x} \in ker(M^*_B)$ with $||x|| = 1$. Since $M^*_B = \Psi^t_B$ we have $\Psi_B \overline{x} = \overline{0}$, and so we have established the necessary condition.

We now consider the sufficient condition. Let $\Psi \in \mathbf{Z}^{l,\mathcal{T}}$ be a partitioned integer matrix $\Psi = [A_1|\cdots|A_n]$, where the column rank A_i is equal to the number of columns of A_i, the rank of Ψ is l, and suppose that Ψ satisfies both (i) and (ii) of the Theorem. Thus by (i), we see that the matrix equation $\Psi\overline{x} = \overline{1}$ is solvable. Reduce Ψ to Smith-normal form, and compute M. That is, we determine U, V such that $U\Psi V = D$, then compute C, lastly compute $M = C \cdot F$. To establish that Ψ is a t out of n GILTS we could show that M is an ISP which computes T^n_t. Note that $M^t \cdot \Psi^t = [\overline{1}, \ldots, \overline{1}]$ such that Ψ^t is an ISP that computes T^n_{n-t+1}. By Theorem 4 M^t is a $n - t + 1$ out of n GILTS. Therefore by Theorem 4 $(M^t)^t = M$ is an ISP which computes T^n_t. As $\Psi \cdot M = (M^t \cdot \Psi^t)^t = [\overline{1}, \ldots, \overline{1}]^t = [\overline{1}, \ldots, \overline{1}]$ we have established that Ψ is a t out of n GILTS. □

10 Conclusion

This work has merged several works. Our contributions include: we have demonstrated how to construct the dual of a t out of n GILTS from the shareholders reconstruction matrix Ψ. In the appendix we have provided an example. Also, using results by Cramer and Fehr, we have developed new bounds on the rank of the reconstruction matrix and the amount of randomness needed to generate a t out of n GILTS. These bounds are significant improvements to any other existing bounds for group independent sharing and their asymptotic sum equals the minimal size GILTS (Block-box sharing scheme). Thus these bounds cannot be improved upon asymptotically. Since one requires truly random elements to be generated to develop a group independent scheme, the amount of randomness required does place a computational burden on the distributor. Consequently these bounds are important. Bounds on rank are important due to the nature that the dual of a t out of n GILTS is a $n-t+1$ out of n GILTS. Lastly we have developed a new set of criteria to determine if a n-partitioned integer matrix is a t out of n GILTS.
Let the term *optimal GILTS* refer to a GILTS which uses a minimal number of subshares. We do raise a few questions.

(1) In our attempt to describe group independent linear sharing we assumed that each homomorphism $\psi_{B,i}$ was a row of integers. All known group independent schemes are of this form. Does there exist a group independent scheme not of this form?

(2) Do all optimal group independent t out of n threshold scheme have invariant factors equal to 1?

(3) All optimal schemes discussed in previous works are such that the integer entries of Ψ is 0,1, or -1. Is this true in general for all optimal schemes? That is, is it a requirement? (Here we are not referring to schemes that are asymptotically optimal.)

References

[1] W. Adkins and S. Weintrab. *Algebra, an approach via module theory.* Springer-Verlag, NY, 1992.

[2] A. Beimel. "Secure schemes for secret sharing and key distribution". Ph.D.thesis, Technion, Haifa, June 1996.

[3] J. Benaloh and J. Leichter. "Generalized secret sharing and monotone functions". In *Proc. CRYPTO '88*, Springer LNCS, vol. 765, pp. 274–285, 1988.

[4] S. Blackburn, M. Burmester, Y. Desmedt, and P. Wild. "Efficient Multiplicative Sharing schemes". In *Advances in Cryptology - Eurocrypt '96, LNCS 1070*, pp. 107-118, Springer-Verlag, 1996.

[5] C. Blundo, A. De Santis, and U. Vaccaro. "Randomness in Distribution Protocols". *Inform. Comput.* pp. 111-139, 1996.

[6] C. Blundo, A.G. Gaggia, and D. R. Stinson. "On the Dealer's randomness Required in Secret Sharing Schemes". In *Design, Codes and Cryptography*, 11, pp. 235-259, 1997.

[7] C. Blundo and B. Masucci. "Randomness in Multi-Secret Sharing Schemes". In *Journal of Universal Computer Science,* Vol. 5, No. 7, 1999, pp. 367–389.

[8] C. Blundo and B. Masucci. "A note on the Randomness in Dynamic Threshold Scheme". In *Journal of Computer Security*, Vol. 7, No. 1, 1999, pp. 73–85.

[9] C. Boyd. "Digital Multisignatures", *Cryptography and coding*, Clarendon Press, 1989, pp 241-246.

[10] R. Cramer and S. Fehr. "Optimal Black-box secret sharing over arbitrary abelian groups". In *CRYPTO 2002.*

[11] L. Csirmaz. "The dealer's random bits in perfect sharing schemes" In *Studia Sci. Math. Hungar.* 32(1996) pp.429-437.

[12] A. De Santis, and B. Masucucci. "Multiple Ramp Schemes". In *IEEE Transns. on Inform. Theory*, 45, no. 5, pp. 1720-1728, 1999.

[13] A. De Santis, Y. Desmedt, Y. Frankel, and M. Yung. "How to share a function". In *Proceedings of the twenty-sixth annual ACM Symp. Theory of Computing (STOC)*, pp. 522-533, 1994.

[14] Y. Desmedt. Society and group oriented cryptography: a new concept. In *Advances of Cryptology-Crypto '87*

[15] Y. Desmedt, G. Di Crescenzo, and M. Burmester. "Multiplicative non-Abelian sharing schemes and their application to threshold cryptography". In *Advances in Cryptology - Asiacrypt '94, LNCS 917.* pp. 21-32, Springer-Verlag, 1995.

[16] Y. Desmedt and Y. Frankel. "Homomorphic zero-knowledge threshold schemes over any finite Abelian group". In *Siam J. Disc. Math. vol 7, no. 4* pp. 667-679, SIAM, 1994.

[17] Y. Desmedt and S. Jajodia. "Redistributing secret shares to new access structures and its applications". Tech. Report ISSE-TR-97-01, George Mason University, July 1997 ftp://isse.gmu.edu/pub/techrep/97.01.jajodia.ps.gz

[18] S. Fehr. "Efficient Construction of the Dual Span Program". May 1999, Manuscript, ETH Zurich.

[19] Y. Frankel, P. Gemmel, P. Mackenzie, and M. Yung. "Proactive RSA". In *Advances of Cryptology-Crypto '97*, 1997, LNCS 1294, Springer Verlag, 1997, p. 440-454.

[20] Y. Frankel, P. Gemmel, P. Mackenzie, and M. Yung. "Optimal-Resilience Proactive Public-key Cryptosystems". In *Proc. 38th FOCS*, IEEE, 1997, p. 384-393.

[21] A. Gal. "Combinatorial methods in boolean function complexity". Ph.D.thesis, University of Chicago, 1995.

[22] R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin. "Robust and efficient sharing of RSA functions". In *Advances of Cryptology-Crypto '96,* LNCS 1109, Springer Verlag, 1996, p. 157-172.

[23] T. Hungerford. *Algebra.* Springer-Verlag, NY, 1974.

[24] M. Karchmer and A. Wigderson. "On span programs" In *Proc. of* 8^{th} *annual Complexity Theory Conference,* pp 102-111, 1993.

[25] H.L. Keng. *Introduction to Number Theory.* Springer Verlag, NY 1982

[26] B. King. "Randomness Required for Linear Threshold Sharing Schemes Defined over Any Finite Abelian Group". In *ACISP 2001.* pp. 376-391.

[27] B. King. "Some results in linear secret sharing". Ph.D. thesis, University of Wisconsin Milwaukee, 2001.

[28] A. Shamir. "How to share a secret", *Comm. ACM*, 22(1979), pp 612-613.

[29] V. Shoup. "Practical Threshold Signatures". In *Advances in Cryptology - EUROCRYPT 2000*, LNCS 1807, Springer Verlag 2000, p. 207-220.

[30] D. Stinson. *Cryptography, Theory and Practice.* CRC Press, NY, 1995

[31] M. van Dijk. "A Linear Construction of Secret Sharing Schemes". In *Design, Codes and Cryptography* 12, pp. 161-201, 1997.

11 Appendix

Lemma 1 For all $\overline{x} \in ker(A)$ and $\overline{y} \in im(A^t)$, $\overline{y}^t\overline{x} = \overline{x}^t\overline{y} = 0$.
Proof. Let $\overline{x} \in ker(A)$ and $\overline{y} \in im(A^t)$. Then there exists a $\overline{z}$ such that $\overline{y} = A^t\overline{z}$. Consider $\overline{y}^t\overline{x}$. $\overline{y}^t\overline{x} = (A^t\overline{z})^t\overline{x} = \overline{z}^tA\overline{x} = \overline{z}^t\overline{0} = 0$. □
Lemma 2 Let $\overline{z} \in span(\mathcal{B} \cup \mathcal{C})$ and suppose that for all $\overline{x} \in ker(A)$ we have $\overline{z}^t\overline{x} = 0$ then $\overline{z} \in im(A^t)$.
Proof. Let $\overline{z} \in span(\mathcal{B} \cup \mathcal{C})$. Then $\overline{z} = \sum_{i=1}^{\beta} u_i\overline{b}_i + \sum_{i=1}^{\gamma} v_i\overline{c}_i$ for some integers $u_1, \ldots, u_\beta, v_1, \ldots, v_\gamma$. Consider $\overline{z}^t\overline{x}$ which must equal 0.

$$\begin{aligned}
\overline{z}^t\overline{x} &= \overline{x}^t\overline{z} = \overline{x}^t(\sum_{i=1}^{\beta} u_i\overline{b}_i + \sum_{i=1}^{\gamma} v_i\overline{c}_i) \\
&= \overline{x}^t\sum_{i=1}^{\beta} u_i\overline{b}_i + \overline{x}^t\sum_{i=1}^{\gamma} v_i\overline{c}_i = \overline{x}^t\sum_{i=1}^{\beta} u_i\overline{b}_i + \sum_{i=1}^{\gamma} v_i(\overline{x}^t\overline{c}_i) \\
&= \overline{x}^t\sum_{i=1}^{\beta} u_i\overline{b}_i + \sum_{i=1}^{\gamma} v_i \cdot 0 = \overline{x}^t\sum_{i=1}^{\beta} u_i\overline{b}_i.
\end{aligned}$$

Therefore for all $\overline{x} \in ker(A)$ we have $\overline{x}^t\sum_{i=1}^{\beta} u_i\overline{b}_i = 0$. However $\sum_{i=1}^{\beta} u_i\overline{b}_i \in ker(A)$, let $\overline{x} = \sum_{i=1}^{\beta} u_i\overline{b}_i$. Then $\overline{x}^t\overline{x} = 0$ implies $\overline{x} = \overline{0}$. Therefore $u_i = 0$ for all i. Consequently $\overline{z} \in im(A^t)$. □
Lemma 3 Let $\overline{z} \in span(\mathcal{B} \cup \mathcal{C})$ and suppose that for all $\overline{x} \in im(A^t)$ we have $\overline{z}^t\overline{x} = 0$ then $\overline{z} \in ker(A)$.
The proof is similar to the proof of Lemma 2 and is left as an exercise.
Theorem 1 [17, 27] For all $B \subset \{P_1, \ldots, P_n\}$ with $B \notin \Gamma$, there exists matrices $Y_B \in \mathbf{Z}^{\mathcal{T}_B, R}$ and $Z_B \in \mathbf{Z}^R$ such that $\overline{s}_B = Y_B(Z_Bk + \overline{r})$ where $\mathcal{T}_B = \sum_{i \in B} a_i$ and $\overline{r} = [r_1, \ldots r_R]^t$.
Proof. Let B' be a set of participants such that $|B'| < t$ and let the rank of $C_{B'}$ be $l_{B'}$. We express $C_{B'}$ as $C_{B'} = [X_{B'}|Y_{B'}]$ where $X_{B'}$ denotes the first column of $C_{B'}$ and $Y_{B'}$ denotes the remaining R columns. Then $\overline{s}_{B'} = X_{B'}k + Y_{B'}[r_1, \ldots, r_R]^t$. Consider matrices $U_{B'}$ and $V_{B'}$ which reduce $Y_{B'}$ to Smith normal form. Thus

$$U_{B'}Y_{B'}V_{B'} = \begin{bmatrix}
d_{Y_{B'},1} & 0 & \cdots & & 0 & \cdots & 0 \\
0 & d_{Y_{B'},2} & & & \vdots & & \vdots \\
 & & \ddots & & \vdots & & \vdots \\
0 & \cdots & & d_{Y_{B'},l_{B'}} & 0 & \cdots & 0 \\
0 & \cdots & & & 0 & \cdots & 0 \\
\vdots & & & & \vdots & & \vdots \\
0 & \cdots & & & 0 & \cdots & 0
\end{bmatrix}.$$

We will denote this matrix by $D_{Y_{B'}}$. Apply matrix $U_{B'}$ to $\overline{s}_{B'}$, we get

$$U_{B'}\overline{s}_{B'} = U_{B'}X_{B'}k + U_{B'}Y_{B'}[r_1, \ldots, r_R]^t.$$

So

$$U_{B'}\overline{s}_{B'} = U_{B'}X_{B'}k + D_{Y_{B'}}V_{B'}^{-1}[r_1, \ldots, r_R]^t.$$

It follows then that for $i = 1, \ldots, l_{B'}$, $d_{Y_{B'},i}$ divides the integer in the i^{th} row of $U_{B'}X_{B'}$. Further, all rows i of $U_{B'}X_{B'}$, where $i > l_{B'}$, are zero. Hence

$$U_{B'}X_{B'} = \left[d_{Y_{B'},1}x_1, d_{Y_{B'},2}x_2, \ldots, d_{Y_{B'},l_{B'}}x_{l_{B'}}, 0, \ldots, 0\right]^t.$$

Consequently,

$$U_{B'}\overline{s}_{B'} = D_{Y_{B'}}[x_1, \ldots, x_{l_{B'}}, 0, \ldots, 0]^t k + D_{Y_{B'}}V_{B'}^{-1}[r_1, \ldots, r_R]^t.$$

Even though the number of rows of $U_{B'}X_{B'}$ (which equals the number of rows of $C_{B'}$), does not necessarily equal the number of columns of $C_{B'}$, which is $R+1$, we have the following.
$U_{B'}\overline{s}_{B'} = D_{Y_{B'}}V_{B'}^{-1}V_{B'}[x_1, \ldots, x_{l_{B'}}, 0, \ldots, 0]^t k$

$$+D_{Y_{B'}}V_{B'}^{-1}[r_1, \ldots, r_R]^t.$$

This can be formed because $l_{B'} \leq R$, and so we can add sufficient number of zeros or delete sufficient number of zeros in $[x_1, \ldots, x_{l_{B'}}, 0, \ldots, 0]^t$, whichever is needed, which allows us to insert $V_{B'}^{-1}V_{B'}$ into the previous equation. Hence

$$U_{B'}\overline{s}_{B'} = D_{Y_{B'}}V_{B'}^{-1}(V_{B'}[x_1, \ldots, x_{l_{B'}}, 0, \ldots, 0]^t k + [r_1, \ldots, r_R]^t).$$

Therefore

$$\overline{s}_{B'} = U_{B'}^{-1}D_{Y_{B'}}V_{B'}^{-1}(V_{B'}[x_1, \ldots, x_{l_{B'}}, 0, \ldots, 0]^t k + [r_1, \ldots, r_R]^t),$$

which implies

$$\overline{s}_{B'} = Y_{B'}(V_{B'}[x_1, \ldots, x_{l_{B'}}, 0, \ldots, 0]^t k + [r_1, \ldots, r_R]^t. \quad (7)$$

Let us denote $V_{B'}\left[x_1, \ldots, x_{l_{B'}}, 0, \ldots, 0\right]^t$ by $Z_{B'}$. Then $\overline{s}_{B'} = Y_{B'}(Z_{B'}k + \overline{r})$. □

Proof of Theorem 3

Proof. Let us assume that Ψ is a t out of n GILTS. First we consider the completeness condition. Let A denote any set of t participants . Then there exists a linear combination of the rows of Ψ that determines how the participants in A compute the secret k. Let $x_1, \ldots, x_l$ denote the integer coefficients. Thus $\sum_i x_i\vec{\psi}_i\overline{s} = \sum_i x_i k = k$. Hence $\sum x_i = 1$. Since $\overline{s} = C[k, r_1, \ldots, r_R]^t$

$$\begin{aligned}\sum_i x_i\vec{\psi}_i M &= \sum_i x_i\vec{\psi}_i C \cdot F = \sum_i x_i[1, 0, \ldots, 0] \cdot F \\ &= [1, 0, \ldots, 0] \cdot F = [1, 1, \ldots, 1].\end{aligned}$$

Observe that $\sum_i(x_i\vec{\psi}_i M) = (\sum_i x_i\vec{\psi}_i)M$. Thus $M^t \cdot (\sum_i x_i\vec{\psi}_i)^t = [1, 1, \ldots, 1]^t$. Further the coefficients $x_1, \ldots, x_l$ describe the linear combination of the rows of Ψ that determine how the participants in A compute the secret k. Thus the rows of column matrix $(\sum_i x_i\vec{\psi}_i)^t$ which correspond to participants P, where $P \notin A$, will be zero. Let $\overline{z}$ be the column matrix consisting of the entries in $(\sum_i x_i\vec{\psi}_i)^t$ which correspond to participants in A. Consequently $M_A^t \cdot \overline{z} = M^t \cdot (\sum_i x_i\vec{\psi}_i)^t = [1, 1, \ldots, 1]^t$. Hence $\overline{1} \in im(M_A^t)$.

We now consider the privacy condition. We utilize an argument similar to the one in [10]. The basis for the argument is due to Theorem 1 which was first established in [17]. Consider a set of participants A such that $|A| < t$. We will assume without loss of generality that $|A| = t-1$. We need to show that there exists an $\overline{y} \in \mathbf{Z}^{R+1}$ such that $M_A\overline{y} = \overline{0}$ and $\sum_i y_i = 1$. Now $\overline{s}_A = C_A \cdot [k, r_1, \ldots, r_R]^t$. By Theorem 1, there exist matrices Y_A and Z_A such that $\overline{s}_A = Y_A(Z_A k + [r_1, \ldots, r_R]^t)$. Thus $\overline{s}_A = Y_A([Z_A|I_{R\times R}]) \cdot [k, r_1, \ldots, r_R]^t$ where $I_{R\times R}$ is the $R \times R$ identity matrix. Consequently we can express C_A as $C_A = Y_A([Z_A|I_{R\times R}])$. Utilizing the fact that $Y_A \cdot \overline{0} = \overline{0}$, we can find an $\overline{x} = [x_1, \ldots, x_{R+1}]^t$ such that $C_A \cdot \overline{x} = \overline{0}$ and $x_1 = 1$. (Simply let $\overline{x} = [1, -z_1, -z_2, \ldots, -z_R]^t$ where $Z_A = [z_1, z_2, \ldots, z_R]^t$.) Since $M_A = C_A \cdot F$, we see that

$F^{-1} \cdot \overline{x} \in ker(M_A)$. By equation (5), $F^{-1} \cdot \overline{x} = [1 + \sum_{i=1}^{R} z_i, -z_1, -z_2, \ldots, -z_R]^t$. Thus $||F^{-1} \cdot \overline{x}|| = 1$, and so we have established the privacy condition.

Now assume M is an integer span program which computes T_t^n with target vector $\overline{1} = [1, 1, \ldots, 1]$. We construct the GILTS as follows. Let $\mathcal{F} = \{\vec{z} : \vec{z} \cdot M = [1, 1, \ldots, 1]\}$. Then $\mathcal{F} \neq \emptyset$, since for all $A \in \Gamma$ there exists $\overline{x}$ such that $\overline{1} = M_A^t \overline{x}$. This implies $[1, 1, \ldots, 1] = \overline{x}^t M_A = \vec{x} M_A$. One can easily construct a $\vec{z}$ from $\vec{x}$, by inserting column entries of $\vec{x}$ into $\vec{z}$ which correspond to columns which belong to members of A and inserting 0's into columns of $\vec{z}$ which belong to members not in A.

Let $\vec{b}_1, \ldots, \vec{b}_\beta$ be a basis for $\mathcal{F}$ and then let Ψ be the matrix whose rows consist of the row vectors $\vec{b}_1, \ldots, \vec{b}_\beta$. Lastly , let $\overline{s} = C \cdot [k, r_1, \ldots, r_R]^t = M \cdot F^{-1} \cdot [k, r_1, \ldots, r_R]$ where k is the secret and $r_1, \ldots, r_R$ will be elements selected uniformly random from the group. We partition Ψ in the same manner as M was partitioned.

Let $A \in \Gamma$, then there exists $\overline{x}'$ such that $\overline{1} = M_A^t \overline{x}'$. Let $\vec{x}$ be the row matrix consisting of entries equal to the corresponding entry of $\overline{x}'$ in columns which correspond to members in A and 0's in columns which corresponds to members not in A. Thus $\vec{x} \cdot M = [1, 1, \ldots, 1]$. Of course there must exist $w_1, w_2, \ldots, w_\beta$ such that $\vec{x} = \sum w_i \vec{b}_i$. Since $\vec{x} \cdot M = \vec{b}_1 \cdot M = \cdots = \vec{b}_1 \cdot M = [1, 1, ..., 1]$, it follows that $\sum w_i = 1$. Therefore $\sum w_i \vec{b}_i \overline{s} = k$. Hence the completeness property of Definition 1 is satisfied.

We now consider the privacy condition of Definition 1. Let B be a set of participants where $|B| < t$. Then there exists $\overline{x}$ such that $M_B \overline{x} = \overline{0}$ and $\sum x_i = 1$. Let $\overline{y} = F \cdot \overline{x}$. As $C_B = M_B \cdot F^{-1}$, we have $C_B \overline{y} = M_B \cdot F^{-1} \cdot F \cdot \overline{x} = \overline{0}$. Now observe that $\overline{y} = [y_1, \ldots, y_{R+1}]^t$ is such that $y_1 = 1$, this follows from the fact that $\overline{y} = F \cdot \overline{x}$, $||\overline{x}|| = \sum x_i = 1$, and by equation (5). Since $C_B \cdot [1, y_2, \ldots, y_{R+1}]^t = \overline{0}$, we can infer that the first column of C_B is a linear combination of columns 2 through $R+1$. Express $C_B = [X_B | Y_B]$ where X_B is the first column of C_B. Then $X_B = Y_B \cdot [-y_2, \ldots, -y_{R+1}]^t$. Let $Z_B = [-y_2, \ldots, -y_{R+1}]^t$. Then $C_B = [X_B | Y_B] = [Y_B \cdot Z_B | Y_B] = Y_B [Z_B | I_{R \times R}]$. Thus $\overline{s}_B = Y_B [Z_B | I_{R \times R}] \cdot [k, r_1, \ldots, r_R]^t = Y_B [Z_B k | \overline{r}]$ where $\overline{r} = [r_1, \ldots, r_R]^t$ (here Z_B times scalar k means "multiply" every element in the column matrix by k). Since $\overline{r}$ is selected uniformly random, due to the one-time pad we can infer that the privacy condition of Definition 1 is satisfied. Observe that we have reconstructed the necessary result for a GILTS, Theorem 1. □

Example 2 *The following is an example of a 2 out of 5 GILTS $\Psi \overline{s} = \overline{k}$. Ψ was hand computed and verified to be a 2 out of 5 GILTS. M was computed using the Smith-normal form technique. That is we first computed C using equation (4), and then computed $M = C \cdot F$. The computations were done using PARI/GP.*

$$\Psi = \left[\begin{array}{cc|c|ccc|ccc|cccc} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

$$M = \left[\begin{array}{ccccc} 1 & 1 & 1 & 1 & 2 \\ -1 & -1 & -1 & -2 & -2 \\ \hline 0 & 0 & 0 & 0 & -1 \\ \hline 1 & 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 3 & 3 \\ 0 & -1 & 0 & 0 & 0 \\ \hline 1 & 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 3 & 3 \\ 1 & 2 & 1 & 1 & 1 \\ 1 & 1 & 2 & 1 & 1 \\ \hline 1 & 1 & 1 & 1 & 2 \\ 1 & 1 & 1 & 2 & 1 \\ 1 & 2 & 1 & 1 & 1 \\ 0 & 1 & -1 & 0 & 0 \end{array}\right]$$

Thus $\Psi^* = M^t$ describes a 5-2+1=4 out of 5 GILTS. The shares $\overline{s}^*$ for this GILTS can be computed as $\overline{s}^* = M^* \cdot F \cdot [k, r_1, \ldots r_{l-1}]^t = \Psi^t \cdot F \cdot [k, r_1, \ldots r_{l-1}]^t$ where k denotes the secret and $r_1, \ldots, r_{l-1}$ are selected uniformly random from the group by the distributor (here l is the rank of Ψ and F is the $l \times l$ matrix described by (5)).

In this example $\sum a_i = 14$, $l = 10$ and $R = 4$. Thus for the dual we have 14 shares dealt to the 5 participants so that $a_1 = 2, a_2 = 1, a_3 = 3$, and $a_4 = a_5 = 4$, where $R^* = 10$ and $l^* = 4$.

Example 3 *The following 2 out of 4 GILTS example illustrates that Ψ^{**} does not necessarily equal Ψ.*

Consider the following 2 out of 4 GILTS satisfying $\Psi\overline{s} = \overline{k}$ where Ψ is 6×8 matrix (partitioning is described below). The last row of Ψ implicitly describes a relation between s_{22} and s_{32}, the relation is that $2s_{22} + 2s_{32} = 0$. The invariant factors of Ψ are: $d_1 = \cdots d_5 = 1$ and $d_6 = 2$. By applying the techniques that we have described (i.e. reducing Ψ to Smith-normal form we derive the M matrix to be:

$$\Psi = \left[\begin{array}{cc|cc|cc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 3 & 0 & 2 & 0 & 0 \end{array}\right]$$

$$M = \left[\begin{array}{ccc} 0 & -1 & 0 \\ 1 & 1 & 2 \\ \hline 0 & -1 & 0 \\ 0 & 0 & -1 \\ \hline 1 & 2 & 1 \\ 0 & 0 & 1 \\ \hline 1 & 2 & 1 \\ 1 & 1 & 0 \end{array}\right]$$

As we have illustrated $\Psi^* = M^t$, where Ψ^* will be a $4 - 2 + 1$out of 4 GILTS, i.e. 3 out of 4 GILTS.

Now we apply that same techniques (reduce Ψ^* to Smith-normal form) The result is that

$$M^* = \left[\begin{array}{cccccc} 0 & -2 & -1 & 0 & -1 & 1 \\ 0 & 1 & 0 & 0 & 0 & -1 \\ \hline 1 & 1 & 2 & 1 & 3 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ \hline 1 & 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ \hline 0 & -2 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & -1 & 0 \end{array}\right]$$

Now $\Psi^{**} = (M^*)^t$, we claim that $\Psi^{**} \neq \Psi$. This can be seen by the fact that $[0,0,0,1,0,1,0,0]^t \notin im(\Psi^t)$.[7] *Now observe that $[0,0,0,1,0,1,0,0]^t = (\Psi^{**})^t \cdot [-1,0,0,1,0,0]^t$*

[7] It is true that $[0,0,0,2,0,2,0,0]^t \in im(\Psi^t)$.