Efficient Constructions for One Sharing of Many Secrets*

Wen-Ai Jackson and Keith M. Martin†
Department of Pure Mathematics,
The University of Adelaide,
Adelaide 5005, Australia

Abstract

A secret sharing scheme is a system whereby some secret data can be protected among a set of participants in such a way that only certain pre-specified groups of participants can reconstruct the secret. Most secret sharing schemes are designed with the intent that once the secret has been recovered there must be a further redistribution of information to participants before the scheme can be used again to protect a new secret. In this paper the secret sharing schemes under consideration can be used more than once, at the expense of a possible reduction in security as the scheme is repeatedly used. A bound on the amount of information held by each participant in such schemes is known. Constructions for secret sharing schemes that are optimal with respect to this bound are now provided.

1 Introduction

A *secret sharing scheme* is a way of protecting a *secret* among a group of *participants*. This is done by distributing to each participant some information known as a *share*. The secret sharing scheme is designed so that only certain pre-specified groups of participants will be able to pool their shares and reconstruct the secret. This collection of groups of participants is known as the *access structure* of the secret sharing scheme. Secret sharing schemes were first proposed in [3] and [12] which both discussed the case of (k, m)-*threshold schemes*, where the access structure consists of all subsets of an m-set of at least some fixed cardinality k. For a good introduction to the theory of secret sharing schemes see [14] and for applications of secret sharing schemes see [13].

*A preliminary version of this paper was presented at Asiacrypt'94, Wollongong, Australia
†This work was supported by the Australian Research Council

We consider the situation where a secret sharing scheme is to be used several times. We assume that throughout the lifetime of a secret sharing scheme the integrity of the shares is preserved but the value of a reconstructed secret becomes public knowledge. For instance, let the participants be members of a military unit and the secrets be a set of one-time use passwords to be issued only in emergency situations. In the event of such an emergency an authorised set of members of the unit can use their shares to determine a password which can then be broadcast to the whole unit. During a subsequent alert a new password will be needed. The design of the secret sharing scheme must take into consideration the fact that the old password is now known by all the participants. In most traditional models it is necessary to redistribute fresh shares to each participant once a particular secret has been reconstructed. This can be a costly process with respect to both time and resources. We would like to extend the potential lifetime of a particular set of shares by allowing them to be used in the recovery of more than one secret.

The secret sharing schemes that we study offer *unconditional security*. This means that their security is independent of the time and resources available to any opponent who is trying to interfere with the procedure. Threshold schemes that permitted shares to be re-used several times were studied in [7]. The security of these schemes was not unconditional since it relied on the difficulty of computing discrete logarithms modulo a large prime (we say that secret sharing schemes of this type offer *conditional security*). Conditionally secure secret sharing schemes with re-usable shares for the more general class of *monotone* access structures (see Section 2) were studied in [8]. Unconditionally secure threshold schemes that protected more than one secret were first discussed in [10]. These schemes were not optimal in the sense that we will discuss later. Unconditionally secure secret sharing schemes for general monotone access structures were studied in [4] and some lower bounds on the size of share that each participant holds in such schemes were shown. The size of a participant's share in a secret sharing scheme reflects the efficiency of the scheme as larger shares are more costly to store and process. In Section 2 we formalise the problem and in Section 3 we present two constructions for secret sharing schemes that meet the main lower bound given in [4].

2 Modelling schemes to share many secrets

We call a secret sharing scheme that is to be used up to n times an *n-secret sharing scheme*. We begin by defining a model for an n-secret sharing scheme. Let $\mathcal{P} = \{P_1, \ldots, P_m\}$ index a collection of participants and let $\mathcal{S} = \{S_1, \ldots, S_n\}$ index a set of secrets (these secrets will be accessed sequentially and in any order). For each $1 \leq i \leq m$ let $\langle P_i \rangle$ be the finite set of all possible shares for participant P_i, and for each $1 \leq i \leq n$ let $\langle S_i \rangle$ be the finite set of all possible values of the secret S_i. For each $\mathcal{Z} = \{Z_1, \ldots, Z_r\} \subseteq \mathcal{P} \cup \mathcal{S}$ let $\langle \mathcal{Z} \rangle = \langle Z_1 \rangle \times \cdots \times \langle Z_r \rangle$ (the collection of r-tuples with component i from set $\langle Z_i \rangle$).

An n-secret sharing scheme consists of a publicly known subset $\mathcal{F}$ of $\langle \mathcal{P} \cup \mathcal{S} \rangle$ and a probability measure p defined on $\mathcal{F}$. Each $f \in \mathcal{F}$ is known as a *distribution rule*. We

label the components of $f \in \mathcal{F}$ such that $f = (f(P_1), \ldots, f(P_m), f(S_1), \ldots, f(S_n))$. For each $\mathcal{Z} = \{Z_1, \ldots, Z_r\} \subseteq \mathcal{P} \cup \mathcal{S}$ we let $f(\mathcal{Z}) = (f(Z_1), \ldots, f(Z_r))$. To implement an n-secret sharing scheme a distribution rule f is selected (with probability $p(f)$) from $\mathcal{F}$. For each $1 \leq i \leq m$ the share given to P_i is $f(P_i)$ and for each $1 \leq i \leq n$ the value of secret S_i is $f(S_i)$. Note that the secret values can be *explicit* (the values $z_1, \ldots, z_n$ of the secrets are predetermined and an f is chosen such that $f(\mathcal{S}) = (z_1, \ldots, z_n)$), or be *implicit* ($f$ is chosen first and the secret values implicitly become $f(S_1), \ldots, f(S_n)$). An n-secret sharing scheme is designed mainly for implicit secrets, suitable for uses such as when the secret values correspond to cryptographic keys. As an n-secret sharing scheme does not guarantee to have a distribution rule f that has $f(\mathcal{S}) = (z_1, \ldots, z_n)$ for all possible choices of $z_1, \ldots, z_n$, such a scheme may not always be suitable for use with explicit secrets.

An *access structure* Γ, defined on $\mathcal{P}$, is a collection of subsets of $\mathcal{P}$. We assume that Γ is *monotone*, hence it has the property that for all $\mathcal{A} \subseteq \mathcal{A}' \subseteq \mathcal{P}$, if $\mathcal{A} \in \Gamma$ then $\mathcal{A}' \in \Gamma$. We assume that Γ is *connected* (for all $P \in \mathcal{P}$ there exists $\mathcal{A} \subseteq \mathcal{P}$ such that $P \in \mathcal{A} \in \Gamma$ but $\mathcal{A} \setminus \{P\} \notin \Gamma$).

The model for n-secret sharing in [4] was defined in terms of the entropy function (see for example [15] for an introduction to entropy). For any $\mathcal{Z} \subseteq \mathcal{P} \cup \mathcal{S}$ and any $z \in \langle \mathcal{Z} \rangle$ let $p(z) = \sum_{\{f \in \langle \mathcal{P} \cup \mathcal{S} \rangle \mid f(\mathcal{Z}) = z\}} p(f)$. We let $[\mathcal{Z}] = \{z \in \langle \mathcal{Z} \rangle \mid p(z) > 0\}$. Then let

$$H(\mathbf{Z}) = -\sum_{z \in [\mathcal{Z}]} p(z) \log_2 p(z).$$

Similarly, for any $\mathcal{Y}, \mathcal{Z} \subseteq \langle \mathcal{P} \cup \mathcal{S} \rangle$ we let

$$H(\mathbf{Z}|\mathbf{Y}) = -\sum_{y \in [\mathcal{Y}]} \sum_{z \in [\mathcal{Z}]} p(y) p(z, y) \log_2 p(z, y).$$

Let Γ be an access structure defined on $\mathcal{P}$ and let $\mathcal{S}$,$\mathcal{F}$ and p be as previously defined.

> $\mathcal{F}$ and p form an *n-secret sharing scheme* for Γ if the following conditions are satisfied:
>
> [N1] For all $\mathcal{A} \in \Gamma$ and all $S_i \in \mathcal{S}$ we have that $H(\mathbf{S_i}|\mathbf{A}) = 0$.
>
> [N2] There exists a non-negative non-increasing sequence $(1 = \alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ with the property that for all $\mathcal{A} \notin \Gamma$, for all $0 \leq k \leq n-1$, and for all $\{S_{i_1}, \ldots, S_{i_k}, S_{i_{k+1}}\} \subseteq \mathcal{S}$,
>
> $$H(\mathbf{S_{i_{k+1}}}|\mathbf{S_{i_1}}, \ldots, \mathbf{S_{i_k}}, \mathbf{A}) = \alpha_j H(\mathbf{S_{i_{k+1}}}).$$

Thus an n-secret sharing scheme has the following properties. If a set of participants $\mathcal{A}$ is in the access structure then their collective shares can be used to uniquely determine the value of any secret S_i. If $\mathcal{A}$ is not in the access structure then by pooling their shares the participants of $\mathcal{A}$ obtain no more information about any of the

secret values (other than the publicly known information obtained from knowledge of $\mathcal{F}$). Further for each $1 \leq k \leq n-1$ there is a predetermined limit on the amount of information that the pooled shares of $\mathcal{A}$ and knowledge of k previous secret values give away about any other secret value. Where appropriate we refer to such a scheme as an n-secret sharing scheme *with respect to* $(1, \alpha_1, \ldots, \alpha_{n-1})$. A 2-secret sharing scheme is exhibited in Example 2.

Note that in [4] an n-secret sharing scheme was referred to as a *multisecret sharing scheme*. We also note that in [8] the secrets were ordered and necessarily accessed in sequence. In our model (and that of [4]) the order of reconstruction of the secrets is not important.

For each $1 \leq i \leq m$, $H(\mathbf{P_i})$ is referred to as the *size* of P_i's share. To be precise, $H(\mathbf{P_i})$ is an *approximation* of the average number of bits needed to represent P_i's share and takes a value in the range $0 \leq H(\mathbf{P_i}) \leq \log_2 |[P_i]|$. Similarly, for each $1 \leq i \leq n$, $H(\mathbf{S_i})$ is the *size* of secret S_i. In [4] the following result was proved.

Result 1 *In an n-secret sharing scheme for Γ with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$, for any ordering $S_{i_0}, \ldots, S_{i_{n-1}}$ of $\mathcal{S}$, and for each $P_i \in \mathcal{P}$,*

$$H(\mathbf{P_i}) \geq \sum_{j=0}^{n-1} \alpha_j H(\mathbf{S_{i_j}}). \tag{1}$$

For reasons relating to storage cost and efficiency, it is desirable to minimise the size of shares in any n-secret sharing scheme. Hence we would like to construct n-secret sharing schemes that meet (1) with equality for each $P_i \in \mathcal{P}$. We refer to such secret sharing schemes as *n-optimal*. An advantage of establishing n-secret sharing schemes with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$ where $\alpha_i < 1$ for some $1 \leq i \leq n-1$, is that (1) suggests that in theory it is possible to trade-off a reduction in share size against a reduction in security (compared to n-secret sharing schemes with respect to $(1, 1, \ldots, 1)$).

Note that 1-optimal secret sharing schemes have the property that for each $P_i \in \mathcal{P}$, the size of the share of P_i is the same as the size of the secret. Such schemes have been studied extensively in the literature and are referred to as *ideal* secret sharing schemes (see for example [5]). We say that a monotone access structure is *ideal* if there exists an ideal secret sharing scheme with access structure Γ. We refer to an ideal secret sharing scheme $\mathcal{F}$ such that p is uniform on $[\mathcal{P} \cup \mathcal{S}]$ and $[\mathcal{S}]$, and such that $|[\mathcal{S}]| = q$, as a *uniform* ideal secret sharing scheme for Γ with *secret length* q.

For the rest of the paper we assume that each secret S_i has the same size.

Example 2 *The following set of distribution rules $\mathcal{F}$ form a 2-optimal secret sharing scheme with respect to $(1,1)$ for $\Gamma = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_2, P_3\}\}$. In our examples we use an array representation for a set of tuples, where the entry in the row indexed by i and the column indexed by j is the component indexed by j in the*

tuple labelled by i.

	P_1	P_2	P_3	S_1	S_2
f_1	0	0	0	0	0
f_2	0	1	1	0	1
f_3	0	2	2	1	0
f_4	0	3	3	1	1
f_5	1	0	0	0	1
f_6	1	1	1	1	0
f_7	1	2	2	1	1
f_8	1	3	3	0	0
f_9	2	0	0	1	0
f_{10}	2	1	1	1	1
f_{11}	2	2	2	0	0
f_{12}	2	3	3	0	1
f_{13}	3	0	0	1	1
f_{14}	3	1	1	0	0
f_{15}	3	2	2	0	1
f_{16}	3	3	3	1	0

In the above a distribution rule is chosen uniformly. If f_6 is chosen then each participant receives the share 1. *If P_1 and P_2 pool their shares then it is clear that f_6 is the chosen distribution rule and hence they can deduce that the secret value of S_1 is 1 and S_2 is 0. If P_1 acts alone then they can only deduce that the distribution rule is one of f_5, f_6, f_7, f_8. Hence the secret values of S_1 and S_2 are equally likely to be 0 or 1. Even if the value of S_1 is already known (in this case to be 1) then P_1 can only deduce that the distribution rule is f_6 or f_7, and again the value of S_2 is equally likely to be 0 or 1. This is also true if only the value of S_2 is known and P_1 tries to determine the value of S_1. Finally, $H(\mathbf{P_1}) = H(\mathbf{P_2}) = \log_2 4 = 2$ and $H(\mathbf{S_1}) = H(\mathbf{S_2}) = \log_2 2 = 1$ and hence $\mathcal{F}$ satisfies (1).*

Note that in Example 2 there are only two possible values for each secret. In practical examples the number of possible secret values will normally be very large.

3 Constructing n-optimal secret sharing schemes

In this section we present two constructions for n-optimal secret sharing schemes. The first construction is for an n-optimal secret sharing scheme for any ideal Γ with respect to any non-negative non-increasing rational sequence $(1, \alpha_1, \cdots, \alpha_{n-1})$. The second construction has an important advantage, but only works for a more restricted range of sequences $(1, \alpha_1, \ldots, \alpha_{n-1})$. Both constructions use the same general technique, which we now describe.

Firstly we define an *n-secret distribution.* An n-secret distribution is essentially an n-secret sharing scheme without any shares. In other words it is a collection of distribution rules that consist of secret values only. More formally, let $\mathcal{S} = \{S_1, \ldots, S_n\}$

index a set of secrets and for each $1 \leq i \leq n$ let S_i take a secret value from the finite set $\langle S_i \rangle$. We will assume that $\langle S_1 \rangle = \cdots = \langle S_n \rangle$. Let $(1, \alpha_1, \ldots, \alpha_{n-1})$ be a non-negative non-increasing sequence. Using the notation from the last section, let $\mathcal{G}$ be a subset of $\langle \mathcal{S} \rangle$ and let p be a probability measure such that p is uniform on $[\mathcal{S}]$. Then $\mathcal{G}$ is an *n-secret distribution with respect to* $(1, \alpha_1, \ldots, \alpha_{n-1})$ if for all $0 \leq k \leq n-1$, and for all $\{S_{i_1}, \ldots, S_{i_k}, S_{i_{k+1}}\} \subseteq \mathcal{S}$,

$$H(\mathbf{S_{i_{k+1}}} | \mathbf{S_{i_1}}, \ldots, \mathbf{S_{i_k}}) = \alpha_j H(\mathbf{S_{i_{k+1}}}).$$

We say that $\lambda = |[\mathcal{S}]|$ is the *length* of the n-secret distribution. Our general construction technique is as follows:

Secret Distribution Technique

We start with the following objects:

- $\mathcal{F}$ a uniform ideal secret sharing scheme for Γ with secret length λ.
- $\mathcal{G}$ an n-secret distribution with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$ of length λ.

Now form an n-optimal secret sharing scheme $\mathcal{H}$ for Γ with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$ by defining a bijection between the secret values of $\mathcal{F}$ and the distribution rules of $\mathcal{G}$ and replacing each secret value of $\mathcal{F}$ with its corresponding distribution rule of $\mathcal{G}$.

Thus the above technique results in each secret value of $\mathcal{F}$ being replaced by an n-tuple of secret values of $\mathcal{G}$. The proof that $\mathcal{H}$ is n-optimal is straightforward.

Example 3 *We show how to use the Secret Distribution Technique to construct the 2-optimal secret sharing scheme exhibited in Example 2. Let Γ be the ideal access structure in Example 2. Let $\mathcal{F}'$ be the uniform ideal secret sharing scheme for Γ obtained from $\mathcal{F}$ in Example 2 by treating the components indexed by S_1, S_2 as a binary ordered pair, indexed by S. Hence, for example, the distribution rule f_4 in $\mathcal{F}$ becomes the distribution rule f_4' in $\mathcal{F}'$ given by*

	P_1	P_2	P_3	S
f_4'	0	3	3	$(1,1)$.

Let $\mathcal{G} = \{(0,0),(0,1),(1,0),(1,1)\}$ be a 2-secret distribution with respect to $(1,1)$. Then by applying the Secret Distribution Technique to $\mathcal{F}'$ and $\mathcal{G}$, using the identity mapping between secret values of $\mathcal{F}'$ and distribution rules of $\mathcal{G}$, we reconstruct $\mathcal{F}$.

3.1 The Tranversal Product Construction

We now provide our first construction. We will construct an n-secret distribution and then use the Secret Distribution Technique to convert it to an n-optimal secret sharing

scheme. We build our n-secret distribution using the following structures. Let q, n be positive integers and let j be an integer such that $1 \leq j \leq n$. Let $\mathcal{X} = \{X_1, \ldots, X_n\}$ be a set of indices and let Q be a finite set of size q. We say that a set $\mathcal{T}$ of n-tuples (indexed by $\mathcal{X}$), with elements from Q, is a (j, n, q)-*transversal system* if for every subset $\{X_{i_1}, \ldots, X_{i_j}\}$ of $\mathcal{X}$ and every j-tuple $(z_1, \ldots, z_j) \in Q^j$ there is a unique $h \in \mathcal{T}$ such that $h(X_{i_1}) = z_1, \ldots, h(X_{i_j}) = z_j$. Note that $\mathcal{T}$ is a (j, n, q)-transversal system if and only if the tuples in $\mathcal{T}$ form the rows of a combinatorial structure known as an *orthogonal array* [2].

Example 4 *Let $Q = \{0, 1\}$. Then the tuples $\mathcal{T}_1 = \{(0,0), (1,1)\}$ form a $(1, 2, 2)$-transversal system. The tuples $\mathcal{T}_2 = \{(0,0), (1,1), (0,1), (1,0)\}$ form a $(2, 2, 2)$-transversal system.*

Let Γ be a monotone access structure and let $(1, \alpha_1, \ldots, \alpha_{n-1})$ be a sequence of non-negative non-increasing rationals, where for each $0 \leq i \leq n-1$, $\alpha_i = u_i/u_0$ (for some positive integers $u_0, u_1, \ldots, u_{n-1}$). For each $1 \leq i \leq n$ let $d_i = u_{i-1} - u_i$ ($u_n = 0$) and let $\delta = \sum_{i=1}^{n} i d_i$.

Transversal Product Construction

To construct an n-optimal secret sharing scheme $\mathcal{H}$ for Γ with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$ proceed as follows:

- Let $\mathcal{S} = \{S_1, \ldots, S_n\}$ index a set of secrets.
- Let $q \geq n - 1$ be a prime power such that there exists a uniform ideal secret sharing scheme $\mathcal{F}$ for Γ with secret length q^δ.
- For each $1 \leq j \leq n$ and each $1 \leq k \leq d_j$, let $\mathcal{T}_{jk}$ be a (j, n, q)-transversal system, indexed by $\mathcal{S}$.
- Define an n-secret distribution $\mathcal{G}$ with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$ as follows. For each set $\{h_{jk} \in \mathcal{T}_{jk} \mid 1 \leq j \leq n, 1 \leq k \leq d_j\}$, define a distribution rule $g \in \mathcal{G}$ such that for each $1 \leq l \leq n$, $g(S_l) = (h_{11}(S_l), \ldots, h_{1d_1}(S_l), \ldots\ldots, h_{n1}(S_l), \ldots, h_{nd_n}(S_l))$.
- Apply the Secret Distribution Technique to $\mathcal{F}$ and $\mathcal{G}$.

Note that the existence of a uniform ideal secret sharing scheme for Γ with secret length q is sufficient to guarantee the existence of one with secret length q^δ (see [6]). Note also that for any $1 \leq j \leq n$ and prime power $q \geq n - 1$ there exists a (j, n, q)-transversal system (see for example [2]). The Transversal Product Construction is so named because we effectively 'multiply' together a sequence of transversal systems, where this sequence consists of d_j copies of a (j, n, q)-transversal system for each $1 \leq j \leq n$. It is straightforward to verify that $\mathcal{G}$ is an n-secret distribution with

respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$ of length q^δ and hence that we can apply the Secret Distribution Technique. Finally we note that for every access structure currently known to be ideal, it is possible to find a prime power q for which there exists an ideal secret sharing scheme for that access structure with secret length q (see [5] for an example of such constructions).

Example 5 *Let $n = 2$ and $\alpha_1 = 1/3$. Let $u_0 = 3$, $u_1 = 1$, $(u_2 = 0)$ and thus $d_1 = 2$, $d_2 = 1$. Choosing $q = 2$ we need two copies of a $(1, 2, 2)$-transversal system and one copy of a $(2, 2, 2)$-transversal system. Thus let $\mathcal{T}_{11} = \mathcal{T}_{12} = \mathcal{T}_1$ (of Example 4) and let $\mathcal{T}_{21} = \mathcal{T}_2$ (of Example 4). The distribution rules of $\mathcal{G}$, a 2-secret distribution with respect to $(1, 1/3)$, are thus given as follows, where $[S_1] = [S_2] = \mathbf{Z}_2^3$ (the set of binary 3-tuples):*

	S_1	S_2		S_1	S_2
g_1	$(0,0,0)$	$(0,0,0)$	g_9	$(1,0,0)$	$(1,0,0)$
g_2	$(0,0,1)$	$(0,0,1)$	g_{10}	$(1,0,1)$	$(1,0,1)$
g_3	$(0,0,0)$	$(0,0,1)$	g_{11}	$(1,0,0)$	$(1,0,1)$
g_4	$(0,0,1)$	$(0,0,0)$	g_{12}	$(1,0,1)$	$(1,0,0)$
g_5	$(0,1,0)$	$(0,1,0)$	g_{13}	$(1,1,0)$	$(1,1,0)$
g_6	$(0,1,1)$	$(0,1,1)$	g_{14}	$(1,1,1)$	$(1,1,1)$
g_7	$(0,1,0)$	$(0,1,1)$	g_{15}	$(1,1,0)$	$(1,1,1)$
g_8	$(0,1,1)$	$(0,1,0)$	g_{16}	$(1,1,1)$	$(1,1,0)$

For example, rule g_2 was constructed using tuple $(0,0)$ of $\mathcal{T}_{11}$, tuple $(0,0)$ of $\mathcal{T}_{12}$ and tuple $(1,1)$ of $\mathcal{T}_{21}$. It is easily checked that $H(\mathbf{S_1}) = H(\mathbf{S_2}) = \log_2 8 = 3$ and $H(\mathbf{S_1}|\mathbf{S_2}) = H(\mathbf{S_2}|\mathbf{S_1}) = \log_2 2 = 1$. In order to construct a 2-optimal secret sharing scheme for any ideal access structure Γ with respect to $(1, 1/3)$ we take a uniform ideal secret sharing scheme $\mathcal{F}$ for Γ with secret length 16 and then replace the secret values of $\mathcal{F}$ with the 16 elements of $\mathcal{G}$.

The Transversal Product Construction is extremely useful since it applies to any sequence of non-negative non-increasing rationals $(1, \alpha_1, \ldots, \alpha_{n-1})$. We note that generally the resulting n-optimal secret sharing schemes will have very large secret lengths. This is highly desirable in most practical applications, however for many sequences the resulting secret length may be even larger than that required for the security of the application. We now describe an alternative construction for an n-secret mapping which only works for certain sequences $(1, \alpha_1, \ldots, \alpha_{n-1})$, but which can result in smaller secret lengths.

3.2 The Intersection Mapping Construction

The Tranversal Product Construction creates a secret distribution from smaller objects (tranversal systems). In contrast, the Intersection Mapping Construction produces a secret distribution mapping by dividing a large object into smaller objects. This construction starts with a set of tuples that form $[\mathcal{S}]$ and then associates certain sets of components with each secret S_i in such a way that the result is a secret distribution mapping.

Let Γ, n, $\mathcal{S}$ and $(1, \alpha_1, \ldots, \alpha_{n-1})$ be as in Section 3.1 (hence $\alpha_i = u_i/u_0$ where u_i, u_0 are positive integers). An *intersection mapping with respect to* $(1, \alpha_1, \ldots, \alpha_{n-1})$ is a pair (ω, ϕ), where ω is a positive integer, W is the collection of u_0-subsets of the set $\{1, \ldots, \omega\}$, and $\phi: \mathcal{S} \to W$ is such that for every $1 \leq k \leq n-1$ and every subset $\{S_{i_1}, \ldots, S_{i_k}, S_{i_{k+1}}\} \subseteq \mathcal{S}$,

$$|\phi(S_{i_{k+1}}) \setminus (\phi(S_{i_1}) \cup \cdots \cup \phi(S_{i_k}))| = u_j. \tag{2}$$

Example 6 *Let* $\mathcal{P} = \{P_1, P_2\}$, $\Gamma = \{\mathcal{P}\}$, $n = 3$ *and* $\mathcal{S} = \{S_1, S_2, S_3\}$. *Let* $\alpha_1 = 2/4$ *and* $\alpha_2 = 1/4$. *Let* $\omega = 7$ *and let* $\phi: \mathcal{S} \to W$ *be given by*

$$\phi(S_1) = \{1, 4, 5, 7\}, \qquad \phi(S_2) = \{2, 4, 6, 7\}, \qquad \phi(S_3) = \{3, 5, 6, 7\}.$$

It is easily verified that (ω, ϕ) *is an intersection mapping with respect to* $(1, 2/4, 1/4)$.

Intersection Mapping Construction

To construct an n-optimal secret sharing scheme $\mathcal{H}$ for Γ with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$ proceed as follows:

- Let $\mathcal{S} = \{S_1, \ldots, S_n\}$ index a set of secrets.
- Let (ω, ϕ) be an intersection mapping with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$.
- Let $q \geq 2$ be an integer such that there exists a uniform ideal secret sharing scheme $\mathcal{F}$ for Γ with secret length q^ω.
- Define an n-secret distribution $\mathcal{G}$ with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$ as follows. For every ω-tuple $(x_1, \ldots, x_\omega)$ with elements from $\{0, 1, \ldots, q-1\}$, define a distribution rule $g \in \mathcal{G}$ such that for each $1 \leq l \leq n$, if $\phi(S_l) = \{i_1, \ldots, i_r\}$ then $g(S_l) = (x_{i_1}, \ldots, x_{i_r})$.
- Apply the Secret Distribution Technique to $\mathcal{F}$ and $\mathcal{G}$.

It is straightforward to verify that the mapping $\mathcal{G}$ defined in the Intersection Mapping Construction is a secret distribution with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$.

Example 7 *Let* $\Gamma = \{\{P_1, P_2\}, \{P_1, P_3\}, \{P_1, P_2, P_3\}\}$. *We show how to use the Intersection Mapping Construction to construct a 3-optimal secret sharing scheme with respect to* $(1, 2/4, 1/4)$. *The following distribution rules* $\mathcal{F}$ *form a uniform ideal secret sharing scheme for* Γ *with secret length 2:*

	P_1	P_2	P_3	S
f_1	0	0	0	0
f_2	0	1	1	1
f_3	1	0	0	1
f_4	1	1	1	0

We convert $\mathcal{F}$ to a uniform ideal secret sharing scheme $\mathcal{F}^7$ for Γ with secret length 2^7 by 'multiplying' $\mathcal{F}$ by itself seven times (see [6] for details). Each distribution rule of $\mathcal{F}^7$ is formed by concatenating component-wise a 7-tuple of rules from $\mathcal{F}$. For example the rule f in $\mathcal{F}^7$ formed from the 7-tuple $(f_2, f_3, f_2, f_2, f_4, f_1, f_3)$ is

$$\begin{array}{cccccc} & P_1 & & P_2 & & P_3 & & S \\ f & (0,1,0,0,1,0,1) & & (1,0,1,1,1,0,0) & & (1,0,1,1,1,0,0) & & (1,1,1,1,0,0,1). \end{array}$$

Now define a 3-secret distribution $\mathcal{G}$ with respect to $(1, 2/4, 1/4)$ using the intersection mapping $(7, \phi)$ of Example 6. Hence, for example, the distribution rule $g \in \mathcal{G}$ arising from the binary 7-tuple $(1,1,1,1,0,0,1)$ is

$$\begin{array}{cccccc} & S_1 & & S_2 & & S_3 \\ g & (1,1,0,1) & & (1,1,0,1) & & (1,0,0,1). \end{array}$$

Finally, in applying the Secret Distribution Technique to $\mathcal{F}$ and $\mathcal{G}$, the most natural bijection between the binary 7-tuple secret values of $\mathcal{F}$ and the distribution rules of $\mathcal{G}$ is the one that maps the secret value $(z_1, \ldots, z_7)$ onto the distribution rule of $\mathcal{G}$ arising from $(z_1, \ldots, z_7)$. Hence under this mapping the distribution rule f results in a distribution rule h of a 3-optimal secret sharing scheme with respect to $(1, 2/4, 1/4)$ given by

$$\begin{array}{cccccc} P_1 & P_2 & P_3 & S_1 & S_2 & S_3 \\ (0,1,0,0,1,0,1) & (1,0,1,1,1,0,0) & (1,0,1,1,1,0,0) & (1,1,0,1) & (1,1,0,1) & (1,0,0,1). \end{array}$$

Although the Intersection Mapping Construction is both intuitive and simple, the main difficulty with using it is that an intersection mapping must first be found. We now present a sufficient condition for the existence of an intersection mapping. Once again let $(1, \alpha_1, \ldots, \alpha_{n-1})$ be a non-increasing sequence of non-negative rationals (where $\alpha_i = u_i/u_0$). We say that $(1, \alpha_1, \ldots, \alpha_{n-1})$ is *suitable* if for each $1 \leq i \leq n$ we have $\beta_i \geq 0$, where

$$\beta_i = \sum_{j=n-i}^{n-1} (-1)^{j-n+i} \binom{i-1}{n-j-1} u_j. \tag{3}$$

We need $\beta_i \geq 0$ in order to apply our construction of an intersection mapping (Theorem 9). Firstly we give a useful expression for the integers u_i in terms of the integers β_i.

Lemma 8 *With β_i $(1 \leq i \leq n)$ as defined in (3), for each $0 \leq k \leq n-1$ we have that*

$$u_k = \sum_{i=1}^{n-k} \binom{n-k-1}{i-1} \beta_i. \tag{4}$$

Proof. Let k be such that $0 \leq k \leq n-1$. To prove that (4) is the correct expression for u_k in terms of the variables β_i $(1 \leq i \leq n)$, we let γ be the result of substituting (3) into the right-hand side of (4) and then show that $\gamma = u_k$. Thus

$$\begin{aligned}
\gamma &= \sum_{i=1}^{n-k} \sum_{j=n-i}^{n-1} (-1)^{j-n+i} \binom{n-k-1}{i-1} \binom{i-1}{n-j-1} u_j \\
&= \sum_{j=k}^{n-1} \sum_{i=n-j}^{n-k} (-1)^{j-n+i} \binom{n-k-1}{i-1} \binom{i-1}{n-j-1} u_j \\
&= \sum_{j=k}^{n-1} \sum_{l=0}^{j-k} (-1)^l \binom{n-k-1}{n-j-1+l} \binom{n-j-1+l}{n-j-1} u_j, \qquad (5)
\end{aligned}$$

by substituting $l = i - n + j$. Then by substituting $a = n-k-1$ and $b = n-j-1$ and using a well-known combinatorial identity (see for example [1]) we see that for $j > k$ the coefficient of u_j in (5) is given by

$$\sum_{l=0}^{a-b} (-1)^l \binom{a}{b+l} \binom{b+l}{b} = \binom{a}{b} \sum_{l=0}^{a-b} (-1)^l \binom{a-b}{l} = 0.$$

Thus the only non-zero coefficient in (5) corresponds to $j = k$ and thus we see that $\gamma = u_k$, as required. □

Theorem 9 *Let $n \geq 1$ and let $(1, \alpha_1, \ldots, \alpha_{n-1})$ be a suitable sequence of non-increasing non-negative rationals. Then there exists a secret allocation mapping with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$.*

Proof. Let $N = \{1, \ldots, n\}$ and for $1 \leq i \leq n$ let β_i be calculated using (3) (where $\alpha_i = u_i/u_0$). Let $\mathcal{D}$ be a collection of subsets of N consisting of β_k copies of all the distinct k-subsets of N, for each $1 \leq k \leq n$. We construct the intersection mapping (ω, ϕ) as follows:

- Let $\omega = |\mathcal{D}| = \sum_{i=1}^{n} \beta_i \binom{n}{i}$.
- Let the subsets in $\mathcal{D}$ be ordered $D_1, \ldots, D_\omega$.
- For $1 \leq l \leq n$ let $\phi(S_l) = \{i \mid l \in D_i\}$.

It follows that for each $1 \leq l \leq n$, $|\phi(S_l)| = \sum_{i=1}^{n} \binom{n-1}{i-1} \beta_i = u_0$ (by (4)). Let k be such that $1 \leq k \leq n$ and let $\{S_{i_1}, \ldots, S_{i_k}, S_{i_{k+1}}\} \subseteq \mathcal{S}$. Let $I = \{i_1, \ldots, i_k\}$. Notice that

$$\phi(S_{i_{k+1}}) \setminus \cup_{j \in I} \phi(S_j) = \bigcup_{\{J \subseteq N \setminus I \mid i_{k+1} \in J\}} (\cap_{l \in J} \phi(S_l)) \setminus (\cup_{l \notin J} \phi(S_l)). \qquad (6)$$

For each $1 \leq j \leq n-k$ there are $\binom{n-k-1}{j-1}$ j-subsets J of $N \setminus I$ such that $i_{k+1} \in J$. Further, $|(\cap_{l \in J} \phi(S_l)) \setminus (\cup_{l \notin J} \phi(S_l))|$ is the number of subsets in $\mathcal{D}$ that equal J, which is β_j. Thus using (6) and (4) we see that

$$|\phi(S_{i_{k+1}}) \setminus \cup_{j \in I} \phi(S_j)| = \sum_{j=1}^{n-i} \binom{n-i-1}{j-1} \beta_j = u_i.$$

Thus (ω, ϕ) is an intersection mapping with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$. □

Example 10 *Let $n = 3$, $\alpha_1 = 2/4$ and $\alpha_2 = 1/4$. From (3) we see that $\beta_1 = \beta_2 = \beta_3 = 1$ and hence that $(1, 2/4, 1/4)$ is suitable. Thus we form the structure $\mathcal{D}$ which consists of the sets $D_1 = \{1\}$, $D_2 = \{2\}$, $D_3 = \{3\}$, $D_4 = \{1, 2\}$, $D_5 = \{1, 3\}$, $D_6 = \{2, 3\}$, $D_7 = \{1, 2, 3\}$. Thus $\omega = 7$ and $\phi(S_1) = \{1, 4, 5, 7\}$, $\phi(S_2) = \{2, 4, 6, 7\}$, $\phi(S_3) = \{3, 5, 6, 7\}$. The secret allocation mapping (ω, ϕ) with respect to $(1, 2/4, 1/4)$ is the one exhibited in Example 6.*

3.3 Comparison of constructions

We now compare the two constructions described in Sections 3.1 and 3.2. First note that with δ and d_i as defined in Section 3.1 and ω as defined in the proof of Theorem 9 we have that

$$\begin{aligned} \delta &= \sum_{i=1}^{n} id_i = \sum_{k=0}^{n-1} u_k = \sum_{k=0}^{n-1} \sum_{i=1}^{n-k} \binom{n-k-1}{i-1} \beta_i \qquad (\text{by (3)}) \\ &= \sum_{i=1}^{n} \sum_{k=0}^{n-i} \binom{n-k-1}{i-1} \beta_i = \sum_{i=1}^{n} \binom{n}{i} \beta_i = \omega. \end{aligned}$$

The penultimate equality comes from repeated application of the fact that $\binom{m}{j} = \binom{m-1}{j-1} + \binom{m-1}{j}$ (see for example [1]). Thus if $(1, \alpha_1, \ldots, \alpha_{n-1})$ is suitable and a prime power q is chosen such that $q \geq n - 1$ then the secret length of the n-optimal secret sharing scheme constructed using either construction is the same. The significant advantage of the Intersection Mapping Construction is that it can be used to construct a scheme for *any* integer $q \geq 2$ as long as $(1, \alpha_1, \ldots, \alpha_{n-1})$ is suitable and there exists a uniform ideal secret sharing scheme for Γ of length q^ω.

For instance let $n = 6$ and $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = (13/22, 8/22, 5/22, 3/22, 1/22)$. Setting $u_0 = 22$ we get $\delta = 52$. The smallest known q for which there exists a $(2, 6, q)$-transversal system is $q = 5$ (see [2]) and thus for this particular example we would need to base any construction on a uniform ideal secret sharing scheme for Γ with secret length at least $\lambda = 5^{52} \simeq 2.22 \times 10^{36}$. However, we have $(\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6) = (1, 2, 0, 1, 0, 1)$ and hence $(1, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5)$ is suitable. Thus for any ideal access structure for which there exists a uniform ideal secret sharing scheme with secret length 2^{52}, there exists a 6-optimal secret sharing scheme for Γ with respect to $(1, 13/22, 8/22, 5/22, 3/22, 1/22)$ with secret length $2^{52} \simeq 4.50 \times 10^{15}$.

An alternative method of reducing the secret length is simply to choose the α_i carefully so that extra large secret lengths are avoided. Hence in the above example, if we choose instead to approximate the stated values of α_i by $(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = (1/2, 1/3, 1/4, 1/6, 1/12)$ then using the Transversal Product Construction results in a secret length of $\lambda = 5^{28} \simeq 3.72 \times 10^{19}$ and, since $(1, 1/2, 1/3, 1/4, 1/6, 1/12)$ is suitable, using the Intersection Mapping Construction results in a secret length of $\lambda = 2^{28} \simeq 2.68 \times 10^8$.

4 Conclusions

We have described a construction method for n-optimal secret sharing schemes with respect to any non-negative rational non-increasing sequence $(1, \alpha_1, \ldots, \alpha_{n-1})$ for any ideal access structure Γ. An interesting open question is to determine whether every n-optimal secret sharing scheme necessarily has an ideal access structure. We also described a process that constructs n-optimal secret sharing schemes for certain special sequences $(1, \alpha_1, \ldots, \alpha_{n-1})$ and can result in schemes with smaller secret lengths. Both constructions use an ideal secret sharing scheme for Γ to generate the n-optimal secret sharing scheme. The same construction methods can be used for non-ideal access structures by replacing the ideal secret sharing scheme with any perfect secret sharing scheme for Γ. The resulting set of distribution rules form an n-secret sharing scheme for Γ with respect to $(1, \alpha_1, \ldots, \alpha_{n-1})$, but the scheme is not n-optimal.

References

[1] I. Anderson, *A first course in combinatorial mathematics*, Clarendon Press, Oxford, 1989.

[2] Th. Beth, D. Jungnickel and H. Lenz, *Design Theory*, Bibliographisches Institut, Mannheim, 1985.

[3] G. R. Blakley, *Safeguarding cryptographic keys*, in Proceedings of AFIPS 1979 National Computer Conference, 48, 1979, pp.313–317.

[4] C. Blundo, A. De Santis and U. Vaccaro, *Efficient Sharing of Many Secrets*, in Proceedings of STACS '93, Lecture Notes in Comput. Sci., 665, 1993, pp.692–703.

[5] E. F. Brickell and D. M. Davenport, *On the Classification of Ideal Secret Sharing Schemes*, J. Cryptology, 2, (1991), pp.123–124.

[6] E. F. Brickell and D. R. Stinson, *Some Improved Bounds on the Information Rate of Perfect Secret Sharing Schemes*, J. Cryptology, 2, (1992), pp.153–166.

[7] R. A. Croft and S. P. Harris, *Public-Key Cryptography and Re-usable Shared Secrets*, in Cryptography and Coding, H. J. Beker and F. C. Piper, eds., Clarendon Press, 1989, pp.255–268.

[8] L. Harn and H.-Y. Lin, *An l-Span Generalized Secret Sharing Scheme*, in Proceedings of Crypto '92, Lecture Notes in Comput. Sci., 740, 1993, pp.558–565.

[9] W.-A. Jackson and K. M. Martin, *Combinatorial Models for Perfect Secret Sharing Schemes*, J. Comb. Math. Comb. Comput., to appear.

[10] E. D. Karnin, J. W. Greene and M. E. Hellman, *On Secret Sharing Systems*, IEEE Trans. Inf. Theory, Vol IT-29, 1, (1983), pp.35–41.

[11] K. M. Martin, *New Secret Sharing Schemes from Old*, J. Comb. Math. Comb. Comput., 14, (1993), pp.65–77.

[12] A. Shamir, *How to Share a Secret*, Comm. ACM, Vol 22, 11, (1979), pp.612–613.

[13] G. J. Simmons, *An Introduction to Shared Secret and/or Shared Control Schemes and their Application*, in Contemporary Cryptology: The Science of Information Integrity, IEEE Press, 1992, pp.441–497.

[14] D. R. Stinson, *An Explication of Secret Sharing Schemes*, Des. Codes Cryptogr., 2, (1992), pp.357–390.

[15] D. Welsh, *Codes and Cryptography*, Clarendon Press, Oxford, 1988.

(Received 16/2/96)