A Combinatorial Interpretation of Ramp Schemes

Wen–Ai Jackson and Keith M. Martin*
Department of Pure Mathematics,
The University of Adelaide,
Adelaide SA 5005, Australia

Abstract

Ramp schemes are means by which a (large) secret can be shared among a group of participants in such a way that only sets of at least k participants can reconstruct the secret and the amount of information that sets of less than k participants can obtain is strictly controlled. This is a generalisation of the concept of a perfect threshold scheme. The current theory concerning ramp schemes will be concisely presented here alongside some new results. We consider the special class of strong ramp schemes and provide a combinatorial classification of optimal strong ramp schemes by showing their equivalence to ideal threshold schemes. A review of the previous literature will be presented.

1 Introduction

A *secret sharing scheme* is a method of distributing a *secret* among a group of *participants.* Each participant is issued with a *share* of the secret and only if certain pre-specified groups of participants pool their shares can the secret be completely reconstructed. The collection of groups that are permitted to reconstruct the secret is known as the *access structure.* Groups not in the access structure are said to be *unauthorised.* If there are n participants and the access structure consists of all the subsets of at least k of these participants ($k \leq n$) then the scheme is described as a (k, n)-*threshold scheme.* Secret sharing schemes have many potential applications, particularly to the area of cryptographic key distribution, and the interested reader is directed to [14] for further details. We note that the schemes under discussion here are all *unconditionally secure.* In other words, the security is independent of the amount of time and resources available to an opponent who is trying to break the scheme.

*This work was supported by the Australian Research Council

The first examples of secret sharing schemes [1], [13] appeared in the published literature in 1979. These were examples of threshold schemes. The former used polynomials over a finite field and the latter used hyperplanes of an affine geometry to construct their schemes. Secret sharing schemes are said to be *perfect* if no unauthorised group of participants can obtain any information-theoretic knowledge about the value of the secret. It is a simple exercise to verify that in any perfect secret sharing scheme the size of each participant's share must be at least the size of the secret. If the secret to be shared is very large then the constraint that the shares must be at least this large may be restrictive (in [12] schemes were discussed within the context of distributed computing where the secret could be a very large database). Hence the study of what have come to be known as *ramp* schemes comes from the need to consider threshold schemes for which there is a tradeoff between share size and security.

The rest of the paper is structured as follows. Firstly, a summary of the known results about ramp schemes is presented. We also prove some new results about linear ramp schemes. This will be followed by a discussion of the special class of ramp schemes known as *strong* ramp schemes. A classification of optimal strong ramp schemes in terms of ideal threshold schemes is given. We conclude with a short summary of the previous literature on ramp schemes.

2 The Theory of Ramp Schemes

Following the approaches of [3], [5] and [16], ramp schemes will be defined from an information theoretic viewpoint. Let $\mathcal{P}$ denote a collection of n participants, and let S denote the secret. For each $P \in \mathcal{P}$, let $\langle P \rangle$ be the finite set of shares which may be given to P, and let $\langle S \rangle$ be the finite set of values of the secret. Suppose there exists a probability measure ρ on Ω, the cartesian product of $\langle P \rangle$ (for all $P \in \mathcal{P}$) and $\langle S \rangle$. For each $\underline{w} \in \Omega$ we write $\underline{w} = (w_X)_{X \in \mathcal{P} \cup \{S\}}$ (where $w_X \in \langle X \rangle$). Let $A \subseteq \mathcal{P} \cup \{S\}$ and $\underline{w} \in \Omega$. Let $\underline{w}_A = (w_X)_{X \in A}$, let $\langle A \rangle = \{\underline{w}_A \,|\, \underline{w} \in \Omega\}$ and let $\chi(A)$ be the random variable defined by the projection $\chi(A) \colon \Omega \mapsto \langle A \rangle$. The measure ρ induces the probability mass function ρ_A of $\chi(A)$ on $\langle A \rangle$ such that for each $\underline{x} \in \langle A \rangle$,

$$\rho_A(\underline{x}) = \sum_{\{\underline{w} \in \Omega \,|\, \underline{w}_A = \underline{x}\}} \rho(\underline{w}).$$

The *entropy* of A is defined to be

$$H(A) = H(\chi(A)) = -\sum_{\underline{x} \in \langle A \rangle} \rho_A(\underline{x}) \log_2 \rho_A(\underline{x}).$$

Let $B \subseteq \mathcal{P} \cup \{S\}$. The measure ρ induces the conditional probability mass function $\rho_{A|B}$ such that for each $\underline{x} \in \langle A \rangle$ and $\underline{y} \in \langle B \rangle$,

$$\rho_{A|B}(\underline{x}, \underline{y}) = \frac{\sum_{\{\underline{w} \in \Omega \,|\, \underline{w}_A = \underline{x},\, \underline{w}_B = \underline{y}\}} \rho(\underline{w})}{\rho_B(\underline{y})}.$$

We define the *conditional entropy* of A given B as

$$H(A|B) = H(\chi(A)|\chi(B)) = -\sum_{\underline{y}\in\langle B\rangle}\sum_{\underline{x}\in\langle A\rangle} \rho_B(\underline{y})\rho_{A|B}(\underline{x},\underline{y})\log_2 \rho_{A|B}(\underline{x},\underline{y}).$$

Given $A, B \subseteq \mathcal{P}\cup\{S\}$ the following identity can be derived:

$$H(AB) \;=\; H(A) + H(B|A). \tag{1}$$

It can also be shown that for $C \subseteq \mathcal{P}\cup\{S\}$,

$$H(A|BC) \leq H(A|B). \tag{2}$$

For $A_1,\ldots,A_n, B \subseteq \mathcal{P}\cup\{S\}$ it follows from (1) that

$$H(A_1\ldots A_n|B) \;=\; H(A_1|B) + H(A_2|A_1B) + \cdots + H(A_n|A_1\ldots A_{n-1}B). \tag{3}$$

The following relation, derived from (2) and (3), is also useful:

$$H(A_1\ldots A_n) \;\leq\; H(A_1) + \cdots + H(A_n). \tag{4}$$

Note that we consider the string $A_1\ldots A_n$ with $n = 0$ to be empty and we let $H(\emptyset) = 0$. For a fuller explanation and description of the basic properties of entropy see [15, pp. 1–13]. Let $0 \leq c < k \leq n$. We say that $\mathcal{P}\cup\{S\}$ and ρ form a (c,k,n)-*ramp scheme* when the following conditions are satisfied:

1. If $A \subseteq \mathcal{P}$ and $|A| \geq k$ then $H(S|A) = 0$;
2. If $A \subseteq \mathcal{P}$ and $|A| \leq c$ then $H(S|A) = H(S)$.

A ramp scheme can thus be thought of as a collection of $(n+1)$-tuples from Ω. Each of these tuples is called a *distribution rule*. To implement the ramp scheme a distribution rule $\underline{w}$ is selected with probability $\rho(\underline{w})$ and participant P is given share w_P. The value of the secret under this distribution rule is w_S. For each participant P the quantity $H(P)$ is referred to as the *size* of P's share. $H(P)$ is an *approximation* of the average number of bits needed to represent P's share and satisfies $0 \leq H(P) \leq \log_2 |\langle P\rangle|$.

A perfect (k,n)-threshold scheme is a $(k-1,k,n)$-ramp scheme. Since the main reason for defining ramp schemes is to allow the size of shares to be reduced compared to perfect threshold schemes, it is worth determining how small the shares can be in a ramp scheme and whether optimal schemes can be constructed. We have the following result from [3]:

Result 1 *In a (c,k,n)-ramp scheme, for any set P^{k-c} of $k-c$ participants we have $H(P^{k-c}) \geq H(S)$.*

Result 1 says that the average size of the share that a participant holds is at least $H(S)/(k-c)$. By means of a counterexample, it is shown in [3] that the bound cannot be improved to say that $H(P) \geq H(S)/(k-c)$ for every participant $P \in \mathcal{P}$.

It is possible to approach this problem from the opposite angle. In other words, we first fix a bound on the size of a participant's share, and then determine a bound on the amount of information that an unauthorised set can obtain about the secret. This is the approach used in [5] where the following result was obtained:

Result 2 *Let $m \leq k$. Suppose a secret is shared among a set of participants in such a way that for each participant P, $H(P) \leq H(S)/m$, and for each set P^k of k participants, $H(S|P^k) = 0$. Then for each $0 \leq r \leq k$ and any set P^r of r participants we have that $H(S|P^r) \leq (k-r)H(S)/m$.*

Result 2 suggests that if we wish the security of a ramp scheme to be maximised with respect to a limit on the size of each share, then the information theoretic knowledge about the secret is likely to increase linearly with respect to the number of participants colluding in order to determine the secret. If we further wish any set P^c of c participants to obtain no information about the secret ($H(S|P^c) = H(S)$) then Result 2 suggests that we should consider schemes that meet the bound of Result 2 when $m = k - c$. Thus we define a (c, k, n)-ramp scheme to be *linear* if it has the extra property that:

3. If $A \subseteq \mathcal{P}$ and $|A| = r$ $(c \leq r \leq k)$ then $H(S|A) = \dfrac{k-r}{k-c}H(S)$.

The term *linear* was first used in this respect in [2]. If a ramp scheme is linear then it was shown in [5] that Result 1 can be strengthened. As the proof of this result in [5] was incomplete, we provide a full proof here.

Result 3 *Let $0 \leq r \leq k$. For any set P^r of r participants in a linear (c, k, n)-ramp scheme we have that $H(P^r) \geq rH(S)/(k-c)$.*

Proof. Let P^k be a set of k participants. Let $P \in P^k$ and let $P^{k-1} = P^k \setminus P$. By Property 3 we have that $H(S|P^{k-1}) - H(S|P^k) = H(S)/(k-c)$. Then from (1) it follows that $H(SP^{k-1}) - H(P^{k-1}) - H(SP^k) + H(P^k) = H(S)/(k-c)$. Rearranging, and applying (1), $H(P|P^{k-1}) = H(P|SP^{k-1}) + H(S)/(k-c)$, and thus

$$H(P|P^{k-1}) \geq \frac{1}{k-c}H(S). \tag{5}$$

Hence for $0 \leq r \leq k$ and any r participants $P_1, \ldots, P_r$, from (3) we see that $H(P_1 \ldots P_r) = H(P_1|P_2 \ldots P_r) + H(P_2|P_3 \ldots P_r) + \cdots + H(P_r) \geq rH(S)/(k-c)$, by (5). □

Thus we see that, for any participant P in a linear ramp scheme, $H(P) \geq H(S)/(k-c)$. We call a linear ramp scheme *optimal* if it has the property that $H(P) = H(S)/(k-c)$ for all $P \in \mathcal{P}$. An optimal $(k-1, k, n)$-ramp scheme is also known as an *ideal* (k, n)-threshold scheme. We now observe that if a (c, k, n)-ramp scheme is optimal then equality is obtained in the bound of Result 3.

Corollary 4 *Let $0 \leq r \leq k$. For any set P^r of r participants in an optimal (c, k, n)-ramp scheme we have that $H(P^r) = rH(S)/(k-c)$.*

Proof. Let $P^r = \{P_1, \ldots, P_r\}$. By (4) we have that $H(P^r) \leq \sum_{j=1}^{r} H(P_j) = rH(S)/(k-c)$. The corollary now follows from Result 3. □

We now prove a result which shows that any ramp scheme which meets the bound of Result 1 and in which the participants hold shares of size $H(S)/(k-c)$ is a linear (and hence optimal) ramp scheme.

Theorem 5 *A (c,k,n)-ramp scheme such that $H(P) = H(S)/(k-c)$ for all $P \in \mathcal{P}$ is linear.*

Proof. Let r be such that $c \leq r \leq k$. Let P^r be a set of r participants of $\mathcal{P}$ and let P^c be a c-subset of P^r. Let $P^r \setminus P^c = \{P_{c+1}, \ldots, P_r\}$. Then,

$$\begin{aligned} H(S|P^r) &= H(SP^r) - H(P^r) \quad (\text{ by } (1)\ ) \\ &\geq H(SP^c) - H(P^r) = H(S|P^c) + H(P^c) - H(P^r) \quad (\text{ by } (1)\ ) \\ &= H(S) + H(P^c) - H(P^r) \\ &\geq H(S) + H(P^c) - H(P^c) - \sum_{j=c+1}^{r} H(P_j) \quad (\text{ by } (4)\ ) \\ &= H(S) - \frac{r-c}{k-c}H(S) = \frac{k-r}{k-c}H(S). \end{aligned}$$

Further, by Result 2 it follows that $H(S|P^r) \leq (k-r)H(S)/(k-c)$, and so $H(S|P^r) = (k-r)H(S)/(k-c)$. Since the argument holds for all r $(c \leq r \leq k)$, the ramp scheme is linear. □

The following generalisation of Theorem 5 also holds:

Theorem 6 *Let r be such that $1 \leq r \leq k-c$. A (c,k,n)-ramp scheme such that for all sets P^r of r participants $H(P^r) = rH(S)/(k-c)$ is linear.*

Proof. If $r = 1$ then the result holds by Theorem 5. Now suppose $r > 1$. Let P^{k-c} be a set of $k-c$ participants. Let P^r be an r-subset of P^{k-c} and let P^{r-1} be an $(r-1)$-subset of P^r. For any participant $P \notin P^{r-1}$, we have $H(PP^{r-1}) = rH(S)/(k-c)$. Thus using (1), $H(P|P^{r-1}) = rH(S)/(k-c) - H(P^{r-1}) = \lambda H(S)$, for some fixed $\lambda > 0$. We show that $\lambda \geq 1/(k-c)$ and so for any $(r-1)$-set P^{r-1} and any participant $P \notin P^{r-1}$,

$$H(P|P^{r-1}) \geq \frac{1}{k-c}H(S). \tag{6}$$

Let $P^{k-c} \setminus P^r = \{P_1, \ldots, P_{k-c-r}\}$. Then,

$$\begin{aligned} H(S) &\leq H(P^{k-c}) \quad (\text{ by Result 1 }) \\ &= H(P^r) + H(P_1 \ldots P_{k-c-r}|P^r) \quad (\text{ by } (1)\ ) \\ &= \frac{r}{k-c}H(S) + H(P_1|P^r) + \cdots + H(P_{k-c-r}|P_1 \ldots P_{k-c-r-1}P^r) \quad (\text{ by } (3)\ ) \\ &\leq \frac{r}{k-c}H(S) + H(P_1|P^{r-1}) + \cdots + H(P_{k-c-r}|P^{r-1}) \quad (\text{ by } (2)\ ) \\ &= \frac{r}{k-c}H(S) + \lambda(k-c-r)H(S). \end{aligned} \tag{7}$$

Rearranging (7) we see that $\lambda \geq 1/(k-c)$, as required.

Now let $P^r = \{P_1, \dots, P_r\}$ be a set of r participants. Then by (3) and (6), $rH(S)/(k-c) = H(P^r) = H(P_1) + H(P_2|P_1) + \cdots + H(P_r|P_1 \dots P_{r-1}) \geq H(P_1|P^r \setminus P_1) + H(P_2|P^r \setminus P_2) + \cdots + H(P_r|P^r \setminus P_r) \geq rH(S)/(k-c)$. Thus equality holds throughout and so $H(P_1) = H(P_1|P^r \setminus P_1) = H(S)/(k-c)$. A similar argument shows that for any $P \in \mathcal{P}$ we have $H(P) = H(S)/(k-c)$ and so the result follows from Theorem 5. □

3 Strong Ramp Schemes

In this section we consider the further strengthening of the basic definition of a linear (c, k, n)-ramp scheme that was suggested in [16]. A linear (c, k, n)-ramp scheme is said to be *strong* if

1. There exist secret co-ordinates $S_1, \dots S_{k-c}$, taking values from the finite sets $\langle S_1 \rangle, \dots, \langle S_{k-c} \rangle$ respectively, such that there is a bijection $\alpha \colon \langle S \rangle \mapsto \langle S_1 \rangle \times \cdots \times \langle S_{k-c} \rangle$ and $\chi(S_1), \dots, \chi(S_{k-c})$ are independent (where for each i $(1 \leq i \leq k-c)$, $\chi(S_i)$ is the random variable representing S_i under the probability mass function induced by ρ_S);

2. Let r be such that $c \leq r \leq k$. For any set P^r of r participants and any $k-r$ co-ordinates S^{k-r} of the secret we have that
$$H(S^{k-r}|P^r) = \frac{k-r}{k-c} H(S). \tag{8}$$

Thus in a strong (c, k, n)-ramp scheme we can identify the secret S with the set $\{S_1, \dots, S_{k-c}\}$. From the independence of random variables $\chi(S_1), \dots, \chi(S_{k-c})$, we see that for any j $(1 \leq j \leq k-c)$,
$$H(S_j) = \frac{1}{k-c} H(S). \tag{9}$$

Ideal threshold schemes are well studied (for example [1, 8, 9, 11, 13]) and can be classified in terms of transversal designs. A *transversal design* $\mathcal{D}$ (denoted $\mathrm{TD}_\mu(t, r, q)$) is an incidence structure consisting of qr points and μq^t blocks. The points of $\mathcal{D}$ are partitioned into r classes of q points and each block of $\mathcal{D}$ intersects each point class in precisely one point. Further, every set of t points from distinct point classes is incident with precisely μ blocks. In [8] it was shown that an ideal (k, n)-threshold scheme for which $|\langle S \rangle| = q$ is equivalent to a $\mathrm{TD}_1(k, n+1, q)$.

It is relatively easy to show that an ideal threshold scheme can be used to construct a strong optimal ramp scheme. In fact the main result of this section shows that strong optimal ramp schemes are equivalent to ideal threshold schemes with certain parameters. We first need two lemmas.

Lemma 7 *Let P^k be a set of k participants and let $P \in \mathcal{P} \setminus P^k$. Then in an optimal (c, k, n)-ramp scheme we have that $H(P|P^k) = 0$.*

Proof. Let P^c be a c-subset of P^k. By repeated applications of (1) we see that $H(P^k \setminus P^c|SP^c) = H(SP^k) - H(SP^c) = H(S|P^k) + H(P^k) - H(S|P^c) - H(P^c) = H(P^k) - H(S) - H(P^c)$. Applying Corollary 4 gives $H(P^k \setminus P^c \mid SP^c) = 0$. Hence for any participant $P \notin P^c$ we have $H(P|SP^c) = 0$. By (1) we see that $H(P|P^k) = H(PP^k) - H(P^k) = H(SPP^k) - H(SP^k) = H(P|SP^k) \leq H(P|SP^c) = 0$. □

Lemma 8 *Let r be such that $0 \leq r \leq k-1$, and let P^r and P^{k-r-1} be disjoint sets of r and $k-r-1$ participants, respectively. Then in an ideal (k,n)-threshold scheme we have that $H(SP^{k-r-1}|P^r) = H(SP^{k-r-1})$.*

Proof. Let $P^{k-1} = P^{k-r-1} \cup P^r$. By (1) we have that $H(SP^{k-r-1}|P^r) = H(SP^{k-1}) - H(P^r) = H(S|P^{k-1}) + H(P^{k-1}) - H(P^r)$. Applying Corollary 4, $H(SP^{k-r-1}|P^r) = H(S) + (k-1)H(S) - rH(S) = (k-r)H(S)$. By applying (4) and Corollary 4, we see that $H(SP^{k-r-1}) \leq H(S) + H(P^{k-r-1}) = (k-r)H(S)$. So $(k-r)H(S) = H(SP^{k-r-1}|P^r) \leq H(SP^{k-r-1}) \leq (k-r)H(S)$. It follows that $H(SP^{k-r-1}|P^r) = H(SP^{k-r-1})$. □

Theorem 9 *There exists an ideal $(k, n+k-c-1)$-threshold scheme if and only if there exists a strong optimal (c,k,n)-ramp scheme.*

Proof. Let S' denote the secret of an ideal $(k, n+k-c-1)$-threshold scheme defined on participant set $\mathcal{P}$. Let $\mathcal{P}'$ be a subset of $k-c-1$ participants and let $S = \mathcal{P}' \cup S'$. Consider the scheme with secret S defined on participant set $\mathcal{P} \setminus \mathcal{P}'$. From Lemma 7 and the definition of a threshold scheme we see that for any k-subset P^k of $\mathcal{P} \setminus \mathcal{P}'$, we have $H(S|P^k) = 0$. Further, from Lemma 8 we see that for any c-subset P^c of $\mathcal{P} \setminus \mathcal{P}'$, we have $H(S|P^c) = H(S)$. Thus the new scheme is indeed a ramp scheme. Since each participant P in this ramp scheme is such that $H(P) = H(S') = H(S)/(k-c)$, it follows by Theorem 5 that the scheme is linear and hence optimal. To see that the scheme is strong, let S^{k-r} be a $k-r$ subset of S. If $S' \in S^{k-r}$ then the result follows directly from Lemma 8, and otherwise by a slight variation of this argument.

Conversely, suppose that we have an optimal strong (c,k,n)-ramp scheme defined on participants $\mathcal{P}$ with secret co-ordinates from set S. Let $S' \in S$ and let $\mathcal{P}' = \mathcal{P} \cup (S \setminus S')$. Let A be a k-subset of $\mathcal{P}'$ and let $r = |A \cap \mathcal{P}|$ $(r \leq k)$. By using (1), $H(A) = H(A \cap S|A \cap \mathcal{P}) + H(A \cap \mathcal{P}) = (k-r)H(S)/(k-c) + H(A \cap \mathcal{P})$. Thus by Corollary 4,

$$H(A) \quad = \quad \frac{k-r}{k-c}H(S) + \frac{r}{k-c}H(S) = \frac{k}{k-c}H(S). \tag{10}$$

Further, using (1), for a k-subset P^k of participants in $\mathcal{P}$, $H(S'\mathcal{P}') = H(S'\mathcal{P}'|P^k) + H(P^k)$. Then by Lemma 7 and Corollary 4, $H(S'\mathcal{P}') = kH(S)/(k-c)$. By (10) we see that $H(S'\mathcal{P}') = H(A)$. Thus by (1) we have that $H(S'\mathcal{P}'|A) = 0$, and in particular that $H(S'|A) = 0$.

Now let A be a $(k-1)$-subset of $\mathcal{P}'$ and let $r = |A \cap \mathcal{P}|$ $(r \leq k-1)$. By the same argument used for (10), we see that $H(S'A) = kH(S)/(k-c)$. From (4) we see that $H(A) \leq \sum_{X \in A} H(X) = (k-1)H(S)/(k-c)$. Then using (1),

$H(S'|A) = H(S'A) - H(A) \geq kH(S)/(k-c) - (k-1)H(S)/(k-c) = H(S)/(k-c)$. Thus by (9), $H(S'|A) \geq H(S')$. Hence from (2) we see that $H(S'|A) = H(S')$. Hence we have constructed an ideal (k, n)-threshold scheme and the correspondence is complete. □

Example 10 *Figure 1 illustrates how to apply Theorem 9 to an ideal* $(2,4)$*-threshold scheme* $\mathcal{M}$. *In this example* $\mathcal{M}$ *is such that the distribution rules are chosen using a uniform probability distribution and consequently* $H(P_i) = H(S) = \log_2 4 = 2$ *for each* i, $(1 \leq i \leq 4)$. *The resulting matrix* $\mathcal{M}'$ *represents an optimal* $(0,2,3)$*-ramp scheme whose distribution rules are also chosen uniformly.*

$$\mathcal{M} = \begin{array}{ccccc} P_1 & P_2 & P_3 & P_4 & S' \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 2 & 2 & 2 & 2 \\ 0 & 3 & 3 & 3 & 3 \\ 1 & 0 & 3 & 2 & 1 \\ 1 & 1 & 2 & 3 & 0 \\ 1 & 2 & 1 & 0 & 3 \\ 1 & 3 & 0 & 1 & 2 \\ 2 & 0 & 1 & 3 & 2 \\ 2 & 1 & 0 & 2 & 3 \\ 2 & 2 & 3 & 1 & 0 \\ 2 & 3 & 2 & 0 & 1 \\ 3 & 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 0 & 2 \\ 3 & 2 & 0 & 3 & 1 \\ 3 & 3 & 1 & 2 & 0 \end{array} \qquad \mathcal{M}' = \begin{array}{cccc} P_1 & P_2 & P_3 & S \\ 0 & 0 & 0 & (0,0) \\ 0 & 1 & 1 & (1,1) \\ 0 & 2 & 2 & (2,2) \\ 0 & 3 & 3 & (3,3) \\ 1 & 0 & 3 & (2,1) \\ 1 & 1 & 2 & (3,0) \\ 1 & 2 & 1 & (0,3) \\ 1 & 3 & 0 & (1,2) \\ 2 & 0 & 1 & (3,2) \\ 2 & 1 & 0 & (2,3) \\ 2 & 2 & 3 & (1,0) \\ 2 & 3 & 2 & (0,1) \\ 3 & 0 & 2 & (1,3) \\ 3 & 1 & 3 & (0,2) \\ 3 & 2 & 0 & (3,1) \\ 3 & 3 & 1 & (2,0) \end{array} \equiv \begin{array}{cccc} P_1 & P_2 & P_3 & S \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 5 \\ 0 & 2 & 2 & 10 \\ 0 & 3 & 3 & 15 \\ 1 & 0 & 3 & 9 \\ 1 & 1 & 2 & 12 \\ 1 & 2 & 1 & 3 \\ 1 & 3 & 0 & 6 \\ 2 & 0 & 1 & 14 \\ 2 & 1 & 0 & 11 \\ 2 & 2 & 3 & 4 \\ 2 & 3 & 2 & 1 \\ 3 & 0 & 2 & 7 \\ 3 & 1 & 3 & 2 \\ 3 & 2 & 0 & 13 \\ 3 & 3 & 1 & 8 \end{array}$$

Figure 1: Construction of an optimal $(0,2,3)$-ramp scheme.

4 Literature Review

The following is a summary, to the best of the authors' knowledge, of references in the literature to ramp schemes. The first comment regarding ramp schemes is an informal suggestion in 1981 by McEliece and Sarwate in [11]. They used Reed-Solomon codes to construct ideal threshold schemes and suggested an approach along the lines of that of Theorem 9 to convert their scheme into an optimal $(0, k, n)$-ramp scheme. A similar informal approach was also taken in 1983 by Karnin *et al* in [9]. They observed that a system which protected several secrets $s_1, s_2, \ldots, s_k$ could be considered to be a (linear) $(0, k, n)$-ramp scheme if the collection of separate secrets was interpreted as one large secret. Again this is a similar construction to that of Theorem 9.

The first real analysis of ramp schemes was provided by Blakley and Meadows in [2]. This paper was the one that first used the terms *ramp scheme* and *linear* *ramp scheme.* They first proposed a very general model for a ramp scheme and then discussed various interpretations of the security of such a scheme. However the schemes that they constructed were linear (c,k,n)-ramp schemes and were based on the threshold schemes proposed in [1]. Each of the known threshold scheme constructions was then considered and it was shown how to convert these to linear (c,k,n)-ramp schemes. Most of these modifications yielded linear ramp schemes which were in fact optimal and were again based on the approach taken in Theorem 9.

Yamamoto [16] was the first author to define ramp schemes in information theoretic terms. The ramp schemes in [16] were all linear and were constructed using matrices with special properties. Yamamoto introduced the definition of strong ramp schemes and gave conditions for when the schemes constructed in the paper were strong.

In 1989 Rabin [12] defined an *Information Dispersal Algorithm.* The problem that Rabin was trying to solve involved the need to reconstruct information from any k parties out of n in such a way that their shares were smaller than those in a perfect threshold scheme. It does not appear that Rabin needed restrictions on the amount of information that less than k parties could accumulate about the secret. Nonethless Rabin came up with a linear $(0,k,n)$ ramp scheme as the solution. Franklin and Yung in [6] also came up with a linear $(0,k,n)$-ramp scheme however they were also looking at the same problem as [9] as they were dealing with threshold schemes that protected several secrets.

The work on bounds for the share size of ramp schemes was looked at in Capocelli et al [5] and Blundo et al [3] in 1992 and 1993 respectively. Most of the cited results in this paper can be found in [5] with the exception of Result 1 which is from [3].

Generalising the concept of a ramp scheme to other monotone access structures has been studied in, for example, Kurosawa et al [10].

5 Conclusions

We have presented a survey of previous work on ramp schemes and have proved some further results about linear ramp schemes. Almost all the constructions for ramp schemes that have appeared in the published literature (under various definitions) have been for strong optimal schemes. We have classified such schemes by showing that they must have been constructed from ideal threshold schemes. We conclude with a couple of questions. Firstly are there any application driven reasons why an optimal ramp scheme would be desired to be strong? Secondly for which sets of parameters (c,k,n) do there exist optimal ramp schemes that are not strong and therefore have not been constructed by the general method used in proving Theorem 9?

References

[1] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS 1979 Natl. Computer Conf.*, New York, vol. 48, 1979, pp. 313–317, June 1979.

[2] G. R. Blakley and C. Meadows, "Security of Ramp Schemes," in *Lecture Notes in Comput. Sci. 196; Advances in Cryptology: Proc. Crypto '84*, G. R. Blakley and D. Chaum, Eds., pp. 242–268, Berlin: Springer-Verlag, 1985.

[3] C. Blundo, A. De Santis and U. Vaccaro, "Efficient Sharing of Many Secrets," in *Lecture Notes in Comput. Sci. 665; Proc. STACS '93*, P. Enjalbert, A. Finkel and K. W. Wagner, Eds., pp. 692–703, Berlin New York: Springer-Verlag, 1993.

[4] E. F. Brickell and D. M. Davenport, "On the Classification of Ideal Secret Sharing Schemes," *J. Cryptology*, vol. 2, pp. 123–134, 1991.

[5] R. M. Capocelli, A. De Santis, L. Gargano and U. Vaccaro, "A Note on Secret Sharing Schemes," in *Sequences II: Methods in Communications, Security and Computer Science*, pp. 335–344, Springer-Verlag, 1993.

[6] M. Franklin and M. Yung, "Communication Complexity of Secure Computation," in *Proc. of 24th ACM STOC*, pp. 699–710, 1992.

[7] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford: Clarendon Press, 1979.

[8] W.–A. Jackson and K. M. Martin, "Combinatorial Models for Perfect Secret Sharing Schemes," to appear in J. Combin. Math Combin. Comput.

[9] E. D. Karnin, J. W. Greene and M. E. Hellman, "On Secret Sharing Systems," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 1, pp. 35–41, 1983.

[10] K. Kurosawa, K. Ogada, K. Sakano, W. Ogata and S. Tsujii, "Nonperfect Secret Sharing Schemes and Matroids," in *Lecture Notes in Comput. Sci. 765; Advances in Cryptology: Proc. Eurocrypt '93*, pp. 231–241, 1994.

[11] R. J. McEliece and D. V. Sarwate, "On Sharing Secrets and Reed-Solomon Codes," *Comm. ACM*, vol. 24, no. 9, pp. 583–584, 1981.

[12] M. O. Rabin, "Efficient Dispersal of Information for Security, Load Balancing, and Fault Tolerance," *J. of the ACM*, vol. 36, no. 2, pp. 335–348, 1989.

[13] A. Shamir, "How to Share a Secret," *Comm. ACM*, vol. 22, no. 11, pp. 612–613, 1979.

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

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

[16] H. Yamamoto, "Secret Sharing Schemes using (k, L, n) Threshold Schemes," *Electronics and Communications in Japan*, part 1, vol. 69, no. 9, pp. 46–54, 1985.

(Received 11/7/95)