SECURITY OF RAMP SCHEMES

G. R. Blakley and Catherine Meadows

Department of Mathematics
Texas A&M University
College Station, Texas 77843-3368

1. OVERVIEW.

A k out of n p/s/r process [AS81] is a very efficient way to convey information (k words suffice to reclaim k words). But it provides virtually no cryptographic security for the information it deals with.

A k out of n threshold scheme [DE81, p. 179-187] is very inefficient as a conveyor of information (k words are necessary to reclaim 1 word). But the linear threshold schemes provide Shannon perfect security [BL81a] up to threshold k. Examples of linear threshold schemes are Blakley projective [BL79], Blakley affine [BL73], Shamir [SH79], Bloom [BL81b], McEliece/Sarwate [MC81], some versions of Asmuth/Bloom [AS83] and some versions of Karnin/Greene/Hellman [KE83]. In addition to the linear threshold schemes there are the threshold schemes due to Davida/DeMillo/Lipton [DA80], some Asmuth/Bloom schemes, and some Karnin/Green/Hellman schemes.

For many practical purposes, Shannon perfect security is too much security if it is bought with k-fold (or more) bandwidth expansion. A magazine wanting to use a 4 out of 6 threshold scheme to store a mailing list occupying 12 rolls of magnetic tape might balk at the need to write, store and manipulate 72 rolls of mag tape to gain Shannon perfect security against opponents whose cryptanalytic expertise is unimpressive. But it might be willing to write, store and handle 24 rolls to get a specified -- more modest -- level of security, the reasoning being much the same as what leads people to put locks on glass doors. You balance level of security against the amenities which less security provides, in an environment in which the opponents are viewed as troublesome but not too threatening.

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, pp. 242-268, 1985.

We will follow a suggestion of Bloom's [BL81b] and explore the properties of various versions of what we will call a "k out of n to yield d ramp scheme" (or, more briefly, a (d,k,n) ramp scheme). Figures 1.1, 1.2 and 1.3 will make clear why we chose the ramp terminology for the generalization of the notion of threshold scheme.

One of the most important types of ramp scheme, the linear ramp scheme does the following. It takes d pieces of input information (i.e. members of a finite field F). From these d inputs (and using k - d other predetermined types of inputs, perhaps some of them random) it produces n outputs in such a fashion that the d inputs can easily be reconstructed from any k outputs. But there is a predetermined level of uncertainty (perhaps the level is zero, and there is an absolute upper bound dependent on j) regarding the inputs if only j outputs are known -- given that $j < k$. It should be obvious from the description above that the assumption

$$1 \leq d \leq k \leq n$$

is implicit in this definition.

The magazine mentioned above could use a (3,4,6) ramp scheme to turn its 12 input rolls of mag tape into 6 boxes (each containing four output rolls). This ramp scheme would have the property that it is easy to get the contents of all 12 input rolls back from any 4 boxes of four output rolls. A competitor of the magazine who gained access to only 3 of these boxes of four tapes each would have some knowledge of the contents of the 12 original mag tape rolls, but likely not enough to be useful.

The basic security consideration in a linear k out of n threshold scheme is all-or-none, i.e. Shannon perfect security [BL81b; SH79]. For every word w belonging to the field F we have

Probability (w is the word conveyed by the scheme | given that k-1 (or fewer) shadows are known)

= Probability (w is the word conveyed by the scheme)

In other words, no amount of knowledge of shadows [BL79] (coded words) below the threshold level k enables a Bayesian opponent [KO81, p. 31] to modify an a priori guess regarding what information the scheme conveys.

A k out of n threshold scheme is the extreme (1,k,n) case of the notion of ramp scheme. See Figure 1.2 below for a description

of a linear (1,k,n) ramp scheme. A k out of n p/s/r process is the opposite extreme, the (k,k,n) case of the notion of ramp scheme. See Figure 1.3 below for a description of a linear (k,k,n) ramp scheme). Here there is a small measure of security. If you intercept only k-1 shadows you can know at most (k-1)/100k per cent of the k pieces of information that were to be conveyed. And you may know less than that, depending on circumstances. We will address this point more fully below.

The basic security consideration in a (d,k,n) ramp scheme is Shannon relative security. This generalization of the notion of Shannon perfect security goes as follows. Consider the d dimensional vector space T consisting of all lists

$$(f(1), f(2), \ldots, f(d))$$

of d words (i.e. members of the finite field F in question). Somebody who knows how the linear ramp scheme in question has been designed and implemented can do no better than the following. Given knowledge of z shadows of the information there is an affine subspace U of T. The dimensionality dim (U) of this affine subspace U is

$$\dim(U) = \min\{d, \max\{0, k-z\}\}$$

(see Figure 1). The subspace U has the property that for every list

$$\xi = (\xi(1), \xi(2), \ldots, \xi(d))$$

of elements of the field F in question we have

Probability (the list ξ to be conveyed does not belong to U) = 0,

Probability (the list ξ to be conveyed is equal to $w \in U$ | given the knowledge of z intercepted shadows)

$$= \frac{\text{Probability (the list } \xi \text{ to be conveyed is equal to } w \in U)}{\text{Probability (the list } \xi \text{ belongs to U)}}$$

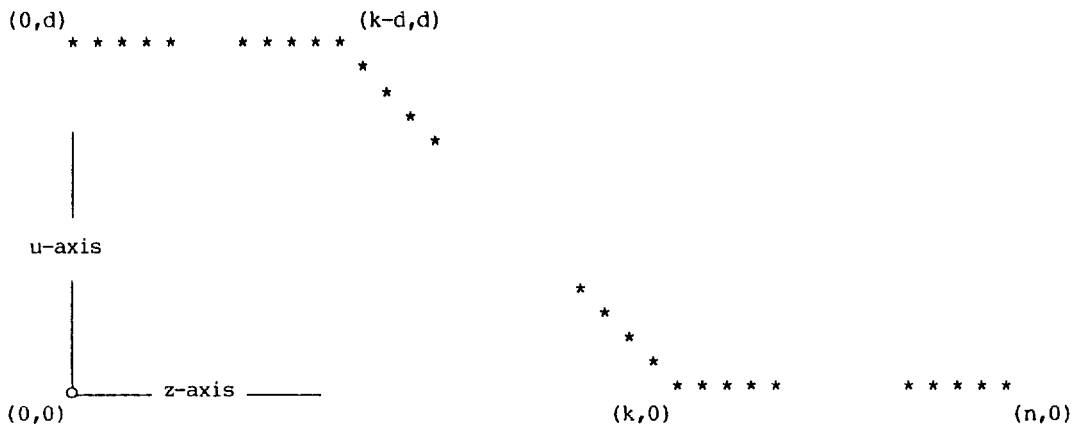
In brief, a Bayesian opponent in possession of z shadows from a (d,k,n) linear ramp scheme now knows that the desired list ξ belongs to U. This is a considerable increase over the amount of information he had at the outset, before he knew any shadows. But, as to where it is within U, he knows no more than he did before he had acquired any shadows. Thus suppose that $1 \leq d \leq k \leq n$. With z shadows

available, an opponent knows of a subspace U whose dimension is given in the Figure 1.1 below.

The concept of linear ramp scheme can also be extended to more general (nonlinear) ramp schemes (such as some versions of the Asmuth/Bloom ramp scheme) by associating a subset U of T to each set of z shadows, where T is merely a set of lists of d words instead of a vector space. Of course in this case we cannot put dimensionality requirements on U, since U will in general not be a linear space. We can, however put degree-of-freedom requirements on U, namely, that if U the subset of T corresponding to k-d+s shadows then knowledge of U leaves us with exactly d-s degrees of freedom. In other words, knowledge of U should not give us any information about any d-s member sublist of $\xi = (\xi(1),\xi(2),\ldots,\xi(d))$ but knowledge of U and any d-member sublist should give us knowledge of the whole list.

We will follow, to some extent, a recent view of threshold schemes due to S. Kothari [KO85]. In addition to its unifying properties, his formulation neatly uncouples the probabilistic considerations from the algebra. This makes it possible for him to give simple elegant proofs of Shannon perfect security for many heretofore seemingly different threshold schemes. Also, he makes explicit the notion that Shamir's [SH79] threshold scheme is a special case of Bloom's [BL81b]. We wish to point out that the converse statement also holds, in a sense. The first mention of this converse to Kothari's observation can be found in [KA83]. Thus it might be more appropriate to speak of a Shamir/Bloom scheme--or of the Bloom approach to a Shamir threshold scheme--henceforward, rather than of separate threshold schemes. Kothari also shows that the Bloom threshold scheme [KO85] is dual to the Blakley affine [BL83] geometric threshold scheme. So all the known Shannon perfectly secure threshold schemes are linear algebraic, and are to all mathematical intents and purposes identical. A corollary of this is that there are rigid [BL83] Blakley schemes and nonrigid versions of the other schemes.

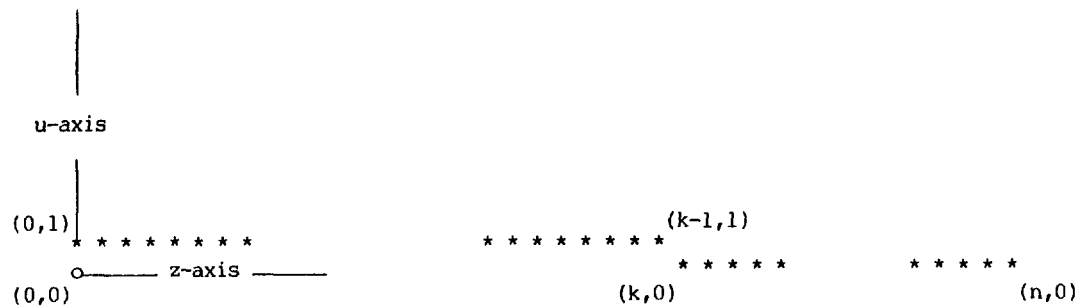
Since the theory of threshold schemes and ramp schemes seems to be maturing, we have collected all the papers touching it known to us in the references at the end of this paper. It is worth noting that Chaum also enunciated ideas [CH79; CH82] along the lines of threshold schemes and suggested implementations making use of cryptosystems.



z	min{d, max{0,k-z}}
0	d
1	d
2	d
...	d
k-d-2	d
k-d-1	d
k-d	d
k-d+1	d-1
k-d+2	d-2
...	...
k-2	2
k-1	1
k	0
k+1	0
k+2	0
...	0
n-2	0
n-1	0
n	0

Figure 1.1

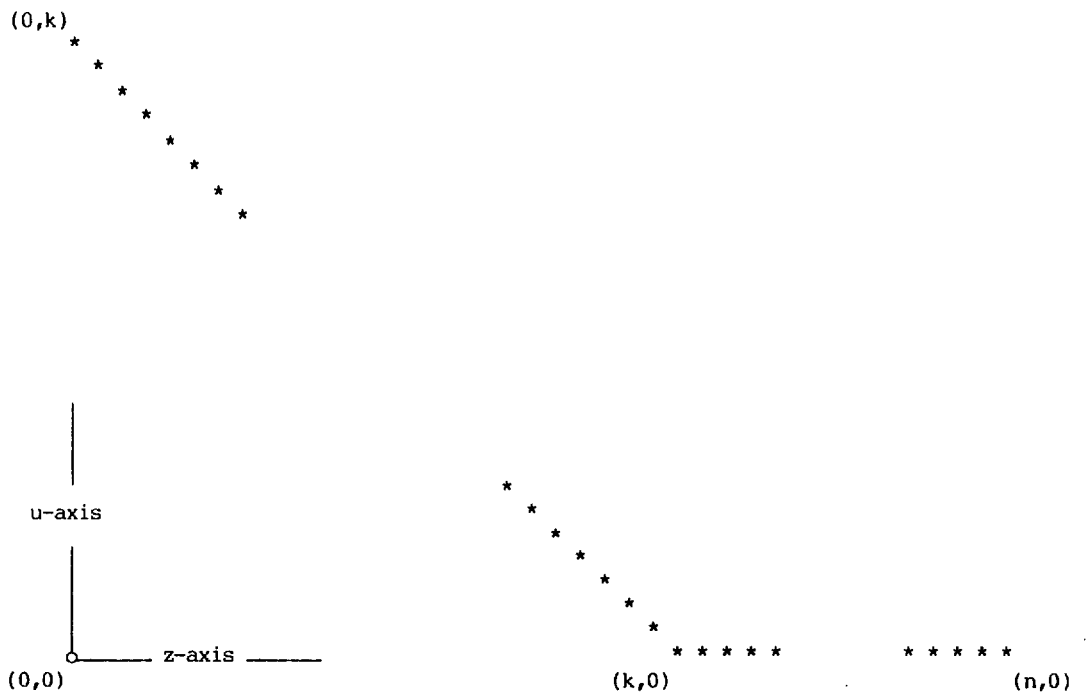
Graph of number u of degrees of uncertainty (i.e. of the dimension u of the subspace U) versus number z of known shadows in the general (d,k,n) linear ramp scheme. The ramp falls at a 45 degree angle from (z,u) = (k-d,d) to (z,u) = (k,0).



z	min{1, max{0,k-z}}
0	1
1	1
2	1
...	1
k-2	1
k-1	1
k	0
k+1	0
k+2	0
...	0
n-2	0
n-1	0
n	0

Figure 1.2

Graph of number u degrees of uncertainty (i.e. of the dimension u of the subspace U) versus number z of known shadows in a (1,k,n) linear ramp scheme, i.e. a k out of n linear threshold scheme. The ramp falls at a 45° angle from (z,u) = (k-1,1) to (z,u) = (k,0).



z	min{k, max{0,k-z}}
0	k
1	k-1
2	k-2
...	...
k-2	2
k-1	1
k	0
k+1	0
k+2	0
...	0
n-2	0
n-1	0
n	0

Figure 1.3

Graph of number u degrees of uncertainty (i.e. of the dimension u of the subspace U) versus number z of known shadows in a (k,k,n) linear ramp scheme, i.e. a k out of n linear p/s/r process. The ramp falls at a 45° angle from (z,u) = (0,k) to (z,u) = (k,0).

2. GENERALIZED RAMP SCHEMES

In this section we develop a general definition of ramp scheme. This definition is actually more general than needed for the examples in this paper, but we state it in as much generality as possible in order that it can be made to fit any future examples of ramp schemes.

(2.1) Definition. A (d,k,n) ramp scheme is defined as follows. We start with a concealing set V and a key set W such that

$$\frac{\log |V|}{\log |W|} \approx \frac{k}{d}$$

where $|\ |$ denotes cardinality. Let π be a surjective map from V to W, that is let π be a map such that for every $w \in W$, there is at least one $v \in V$ such that $\pi(V) = w$. We will call π the revealing map. Given a key element w in W we choose point y in $\pi^{-1}(w)$ called the concealing point. To this point y we associate a set of n shadows

$$\{H(1), H(2), \ldots, H(n)\}$$

where each shadow $H(i)$ is a subset of V such that

a) The intersection of any k shadows is $\{y\}$.

b) There exists an integer ℓ dependent upon d and k such that

i) $1 \leq \ell \leq k$

ii) The restriction of π to the intersection of any ℓ shadows is surjective.

iii) Knowledge about $w = \pi(y)$ increases in some regular way with knowledge of each shadow after ℓ shadows.

As an example of what we mean by the last part of this definition, suppose that W is a vector space of dimension s over a finite field. We could require that, if H is the intersection of $\ell+i < k$ shadows, then $\pi(H)$ is a vector space of dimension $s-i$.

In the threshold scheme case $(1,k,n)$ we can require a scheme to be Shannon perfectly secure. We define a threshold scheme to be Shannon perfectly secure if it satisfies the following criterion.

Whenever the intersection H of less than k shadows is known, then the probability that the image of x under π is w is equal to the a priori probability of w (in other words, $p(\pi^{-1}(w)\,|\,H) = p(w)$). Since some probabilities go to zero in the general ramp scheme case, and the remaining ones usually increase, Shannon perfect security is of course impossible. However, we can still require that no probability which remains positive increases any faster than any other which remains positive, i.e. that the ratios of the remaining positive probabilities remain the same. If this is not possible we can at least require that the ratios do not vary too much from the original. The following definition makes these ideas precise.

(2.2) Definition. A (d,k,n) ramp scheme R is <u>Shannon relatively secure</u> if, whenever the intersection H of less than k shadows is known, then

$$\frac{p(\pi^{-1}(w)\,|\,H)}{p(\pi^{-1}(w^*)\,|\,H)} = \frac{p(w)}{p(w^*)} \tag{2.3}$$

for every pair of elements w and w^* in $\pi(H)$. A (d,k,n) ramp scheme R is <u>Shannon t-relatively secure</u> if, whenever the intersection H of less than k shadows is known, then

$$\frac{p(q)}{(1+t)\,p(w^*)} < \frac{p(\pi^{-1}(w)\,|\,H)}{p(\pi^{-1}(w^*)\,|\,H)} < \frac{(1+t)\,p(w)}{p(w^*)} \quad . \tag{2.4}$$

We say that a ramp scheme is <u>t-relatively secure with knowledge of r shadows</u> if the above inequality holds whenever H is the intersection of r shadows.

In the following lemma we show that the definition of Shannon relative security arises naturally from Shannon perfect security.

(2.5) Lemma. Let R be a (d,k,n) ramp scheme. Then R is Shannon relatively secure if and only if whenever the intersection H of less than k shadows is known, then

$$p(\pi^{-1}(w)\,|\,H) = p(w\,|\,\pi(H)).$$

In particular, a threshold scheme is Shannon relatively secure if and only if it is Shannon perfectly secure, and a Shannon relatively secure ramp scheme is Shannon perfectly secure up to and including

knowledge of $k - d$ shadows.

Proof: Let H be the intersection of no more than k shadows. If

$$p(\pi^{-1}(w)\,|\,H) = p(w\,|\,\pi(H))$$

then for all $w \in \pi(H)$

$$\begin{aligned} p(\pi^{-1}(w)\,|\,H) &= p(w)/w(H) \\ &= p(\{w\} \cap \pi(H))/p(\pi(H)) \\ &= p(w)/p(\pi(H)). \end{aligned}$$

Thus, for all w and w^* in $\pi(H)$ we have

$$\frac{\pi(\pi^{-1}(w)\,|\,H)}{p(\pi^{-1}(w^*)\,|\,H)} = \frac{p(w)/p(\pi(H))}{p(w^*)/p(\pi(H))} = \frac{p(w)}{p(w^*)}$$

and so R is Shannon relatively secure.

Conversely, suppose that R is Shannon relatively secure. If $w \in \pi(H)$ then both $p(\pi^{-1}(w)\,|\,H)$ and $p(w\,|\,\pi(H))$ are zero. Now let $\pi(H) = \{w(0),w(1),\ldots,w(m)\}$. Then

$$p(\pi^{-1}(w(0))\,|\,H)/p(\pi^{-1}(w(i))\,|\,H) = p(w(0))/p(w(i))$$

for $1 \leq i \leq m$. Moreover

$$p(\pi^{-1}(w(0))\,|\,H) + \ldots + p(\pi^{-1}(w(m))\,|\,H) = 1.$$

This gives us a nondegenerate system of $m + 1$ linear equations in $m + 1$ unknowns $p(\pi^{-1}(w(0))\,|\,H)$ through $p(\pi^{-1}(w(m))\,|\,H)$ for which

$$\begin{aligned} p(\pi^{-1}(w(0)\,|\,H) &= p(w(0)\,|\,\pi H), \\ &\vdots \\ p(\pi^{-1}(w(m)\,|\,H) &= p(w(m)\,|\,\pi(H)) \end{aligned}$$

is the unique solution.

The last statement of the lemma follows from the fact that $\pi(H) = W$ when no more than $k - d$ shadows are known.

The major advantage of the above definition of ramp schemes is that, as in the case of Kothari's [KO85] definition of linear threshold scheme, it allows us to characterize Shannon relative security solely in terms of the cardinalities of $\pi^{-1}(w)$ and $\pi^{-1}(w) \cap H$.

(2.6) Lemma. Let R be a (d,k,n) ramp scheme. Then R is Shannon relatively secure if and only if, whenever the intersection H of fewer than k shadows is known, the equality

$$\frac{\left|\pi^{-1}(w) \cap H\right|}{\left|\pi^{-1}(w^*) \cap H\right|} = \frac{\left|\pi^{-1}(w)\right|}{\left|\pi^{-1}(w^*)\right|} \tag{2.7}$$

holds for all w, w^* in $\pi(H)$. R is Shannon t-relatively secure if and only if, whenever the intersection H of fewer than k shadows is known, the inequalities

$$\frac{\left|\pi^{-1}(w)\right|}{(1+t)\left|\pi^{-1}(w^*)\right|} < \frac{\left|\pi^{-1}(w) \cap H\right|}{\left|\pi^{-1}(w^*) \cap H\right|} < \frac{(1+t)\left|\pi^{-1}(w)\right|}{\left|\pi^{-1}(w^*)\right|} \tag{2.8}$$

hold for all w, w^* in $\pi(H)$.

Proof. R is Shannon relatively secure if and only if

$$p(w|H)/p(w^*|H) = p(w)/p(w^*).$$

But

$$p(w|H) = p(\pi^{-1}(w) \cap H)/p(H).$$

Since the point y in $\pi^{-1}(w)$ is chosen at random the distribution on $\pi^{-1}(w)$ is uniform and so

$$p(\pi^{-1}(w) \cap H) = \frac{p(w)\left|\pi^{-1}(w) \cap H\right|}{\left|\pi^{-1}(w)\right|}$$

Thus equation (2.3) in the definition of Shannon relative security becomes

$$\frac{p(w)}{p(w^*)} \frac{\left|\pi^{-1}(w) \cap H\right|}{\left|\pi^{-1}(w^*) \cap H\right|} \frac{\left|\pi^{-1}(w^*)\right|}{\left|\pi^{-1}(w)\right|} = \frac{p(w)}{p(w^*)}$$

which reduces to equation (2.7). Similarly, inequality (2.4) in the definition of Shannon t-relative security becomes

$$\frac{p(w)}{(1+t)\,p(w^*)} < \frac{\left|\pi^{-1}(w) \cap H\right|}{\left|\pi^{-1}(w^*) \cap H\right|} \frac{\left|\pi^{-1}(w^*)\right|}{\left|\pi^{-1}(w)\right|} \frac{p(w)}{p(w^*)} < \frac{(1+t)\,p(w)}{p(w^*)}$$

which reduces to inequality (2.8). □

In the remaining sections of this paper we examine several examples of (d,k,n) ramp schemes, along with their security proofs.

3. RIGID LINEAR SCHEMES

In this section we develop a general linear ramp scheme within the general framework set forth by Kothari in [KO85]. Namely, let V be a vector space of dimension k over a finite field F, let y be a point of V hiding the key vector in some way, and let the $H(i)$s be hyperplanes in general position with respect to y. (This is actually less general then Kothari's scheme, which also includes projective and affine spaces.) We let W be F^d and we let the map $\pi: V \to W$ be a linear transformation. It turns out that if the $H(i)$s are oriented so that the intersection of any ℓ of them with a certain translation of the kernel of π is a linear variety of dimension $\min(k-\ell-d,0)$ then any such scheme is Shannon relatively secure. We make this requirement precise below.

(3.1) Definition. We define a (d,k,n) linear ramp scheme in the following way. Let F be a finite field, let $V = F^k$ and let $W = F^d$. Let $\pi: F^k \to F^d$ be a linear transformation. Choose hyperplanes $T(1), T(2), \ldots, T(d)$ through the origin such that $T(1) \ldots T(d)$ is the kernel of π. For $1 \leq i \leq d$, let $t(i)$ be the vector such that

$$T(i) = \{x \in F^k \mid t(i) \cdot x = 0\}.$$

Next choose hyperplanes through the origin $S(1), \ldots, S(n)$ such that the set

$$\{T(1), \ldots, T(d), S(1), \ldots, S(n)\}$$

is in general position, with respect to the origin, that is, such that the intersection of any k members of the set is the origin. For $1 \leq i \leq n$ let $s(i)$ be the vector such that

$$S(i) = \{x \in F^k \mid s(i) \cdot x = 0\}.$$

(Thus the set of vectors $\{t(1), \ldots, t(d), s(1), \ldots, s(n)\}$ is in general position.) For a given w in F^d we choose shadows by picking a point y at random in $\pi^{-1}(w)$ and then picking field elements $c(1)$ through $c(n)$ such that the intersection of any k of the hyperplanes

$$H(i) = \{x \in F^k \mid x \cdot s(i) = c(i)\}$$

is $\{y\}$. Since the hyperplanes $S(i)$ are in general position, this can be done by choosing $c(i)$ such that y is an element f each $H(i)$. Since y is also an element of each $T(i)$, the set

$$\{T(1), \ldots, T(d), H(1), \ldots, H(n)\}$$

is also in general position with respect to y.

(3.2) Proposition. The linear scheme is a (d,k,n) ramp scheme with $\ell = k-d$. Moreover, if $k-d+s$ shadows are known, then all that is known about the key element w is that it lies in a vector subspace of W of dimension $d-i$.

Proof: That linear schemes satisfy condition (a) of Definition (2.1) is clear from their definition.

In order to prove the rest of the proposition, let H be the intersection of r shadows, where $1 \leq r \leq r$. Thus

$$H = H(i_1) \cap \ldots \cap H(i_r).$$

Let

$$S = S(i_1) \cap \ldots \cap S(i_r).$$

Then $H = S+a$, where $a \in F^k$. It follows that $\dim(\pi(H)) = \dim(\pi(S))$, and so it remains to show that $\pi(S) = F^d$ when $r \leq d-k$ and $\dim(\pi(S)) = d-s$ when $r = d-k+s$.

Since the $S(i)$s and the $T(i)$s are in general position, we have

$$\begin{aligned}\dim(S \cap T) &= \min(0, \dim(S) + \dim(T) - k)\\ &= \min(0, k-r+k-d-k)\\ &= \min(0, k-(d+r)).\end{aligned}$$

It follows that, if $r = k-d-s$ where $0 \leq s < k-d$, then

$$\begin{aligned}\dim(\pi(S)) &= \dim(S) - \dim(S \cap T)\\ &= k-r-(k-(d+r))\\ &= d\end{aligned}$$

Thus $\pi(S))$, and hence $\pi(H)$, is all of F^d. If $r = k-d+s$, where $1 \leq s \leq d$, then

$$\begin{aligned}\dim(\pi(S)) &= \dim(S) - \dim(S \cap T)\\ &= k-r-0\\ &= k-(k-d+s)\\ &= d-s.\end{aligned}$$

Hence $\dim(\pi(H)) = d-s$. □

(3.3) Remark. We note that if the subspaces $S(i), \ldots, S(n)$ are fixed beforehand and made known to the general public, no information about the key element w is given away. Moreover, we are saved the trouble of calculating the orientations of the $H(i)$s anew each time, and economy is gained since each shadow holder only has to guard a single field element instead of the equation of a hyperplane. It follows that any efficient ramp scheme will have this property. However, as we see, this property can be built into any linear ramp scheme.

Schemes in which the $S(i)$s are fixed beforehand are known as rigid schemes since the choice of the shadows $H(i)$ is fixed by the choice of the point $y \in \pi^{-1}(w)$.

(3.4) Remark: It we think of the key element w as a single random key, then the above construction of rigid linear ramp scheme suffices. However, if we think of w as a vector of d keys, or as a word that could possibly be deduced if we knew a small part of it, we need to put further conditions on the scheme. For example, we want to avoid such instances as

$$\pi(H(i_1) \cap \ldots \cap \pi(H(i_{k-d+s})) = \{w_1\} \times \ldots \times \{w_s\} \times F^{d-s}$$

since this would give away s of the keys. In other words, if

$$\rho_j : F^d \to F$$

is the projection defined by $\rho((f_1,\ldots,f_d)) = f_j$ we never want $\rho_j(\pi(H))$ to be a single point of H if H is the intersection of less than k shadows. But since $\pi(H)$ is a translation of $\pi(S)$, where S is the intersection of the $S(i)$s corresponding to the $H(i)$s whose intersection is H, it is enough to require that $\rho_j(\pi(S)) \neq \{0\}$. This can be done easily by first setting the subspaces $T(j)$ equal to $\ker(\rho_j \circ \pi)$. Now suppose in such a case that $\rho_j(\pi(S)) = \{0\}$. Then $S \subseteq \mathrm{Ker}(\rho_j \circ \pi) = T(j)$. But this contradicts the fact that the $S(i)$s will have been chosen such that the $S(i)$s and the $T(j)$s are in general position.

(3.5) Theorem. The (d,k,n) linear ramp scheme is Shannon relatively secure.

Proof: By Lemma (2.6) it is enough to show that given H the intersection of ℓ shadows, then

$$\frac{\left|\pi^{-1}(w) \cap H\right|}{\left|\pi^{-1}(w^*) \cap H\right|} = \frac{\left|\pi^{-1}(w)\right|}{\left|\pi^{-1}(w^*)\right|}$$

for all w and w^* in $\pi(H)$. Since π is a linear transformation, we know that

$$\left|\pi^{-1}(w)\right| = \left|\pi^{-1}(w^*)\right|$$

for all w in F^d, so it is enough to show that

$$\left|\pi^{-1}(w) \cap H\right| = \left|\pi^{-1}(w^*) \cap H\right|$$

for all w and w^* in $\pi(H)$.

Since $\pi^{-1}(w)$ is a translation of the kernel of π, $\pi^{-1}(w)$ and H are translations of two vector subspaces in general position. Thus, if the sum of their dimensions is less than k (that is, if H is the intersection of more than $k-d$ shadows) their intersection is either empty or a single point, and $\left|\pi^{-1}(w) \cap H\right| = 1$ whenever

$w \in \pi(H)$. If the sum of the dimensions of $\pi^{-1}(w)$ and H is greater than k, then

$$\dim(\pi^{-1}(w) \cap H) = \dim(\pi^{-1}(w)) + \dim(H) - k$$

for all w, so $|\pi^{-1}(w) \cap H|$ is the same for all w.

Next we look at some examples of ramp schemes.

A. Blakley Scheme

The Blakley scheme is the scheme of Definition (3.1) with π taken to be a projection to a d-dimensional subspace of F^k such that kernel of π satisfies the conditions of Definition (3.1). This is essentially a rigid version of the Blakley scheme described in [BL79].

B. Bloom Scheme

In this scheme [BL81b] we let V be $(F^k)^*$, the space of linear functionals [HO71, p. 97] from F^k to F. (Of course $(F^k)^*$ is isomorphic to F^k.) Let $t_1, \ldots, t_d$ be linearly independent vectors in F^k. The map $\pi: (F^k)^* \to F^d$ is given by

$$\pi(L) = (L(t_1), \ldots, L(t_d)).$$

Choose vectors $\{s_1, \ldots, s_n\}$ in F^k such that the set

$$\{t_1, \ldots, t_d, s_1, \ldots, s_n\}$$

is in general position. let

$$S(i) = \{L \in (F^k)^* \mid L(s_i) = 0\}$$

and let

$$T(i) = \{L \in (F^k)^* \mid L(t_i) = 0\}.$$

Then if we let $T = T(1) \cap \ldots \cap T(d)$, we have $T = \ker(\pi)$. Let w be a point in F. Pick a linear functional G at random in $\pi^{-1}(w)$. The shadows $H(i)$ associated to w are

$$H(i) = \{L \in (F^k)^* \mid L(s_i) = G(s_i))\}.$$

Clearly H(i) is a translation of S(i), and so the Bloom scheme satisfies all the criteria for a linear ramp scheme. Moreover, it follows from the way we have defined the T(i)s that the Bloom scheme clearly satisfies the criteria of Remark (3.3).

C. Shamir Scheme

The Shamir threshold scheme [SH79] is defined as follows. Let f(x) be a polynomial of degree k-1 in F[x], where F is a finite field. Choose elements c_1, b_1, ..., b_n. Let $f(c_1)$ be the key and let $f(b_1)$ through $f(b_1)$. If we know k shadows then we can use Lagrange interpolation to find f(x) and hence the key $f(c_1)$. In [KO84] Kothari points out that the Shamir scheme is a special case of Bloom's scheme. Suppose that

$$f(x) = a_0 + a_1x + \ldots + a_nx^{k-1}.$$

We let the linear functional L we are hiding be defined by

$$L(v) = (a_0,a_1, \ldots, a_n) \cdot V,$$

we let the n vectors s_i in general position be

$$s_i = (1, b_i, (b_i)^2, \ldots, (b_i)^{k-1})$$

and let t_1 be $(1, b_0, (b_0)^2, \ldots, (b_0)^{k-1})$. The key is $L \cdot v_1$. This This is clearly equivalent to Shamir's scheme. Moreover, since these vectors (which make up the Vandermonde matrix) are usually the ones chosen for the Bloom scheme anyway this means that Bloom's and Shamir's schemes are essentially equivalent. We point out that we can make Shamir's scheme into a ramp scheme by letting the key element be the vector $(f(c_1), \ldots, f(c_d))$ where $c_1, \ldots, c_d$ are elements of F.

D. Karnin/Greene/Hellman Scheme.

In this scheme [KA83] the vector space F^d is replaced by $(F^e)^d$ and F^k by $(F^e)^k$, where e is a positive integer. Let A(1) through A(d) be k•e by e matrices such that the k-e by d-e matrix formed by A(1) through A(d) is of maximal rank. Next choose matrices B(1) through B(n) such that any k member subset of

$$\{(A(1), \ldots, A(d), B(1), \ldots, B(n)\}$$

gives a k-e by k-e matrix of full rank. The map

$$\pi: (F^e)^k \to (F^e)^d$$

is given by

$$\pi(x) = (A(1)\cdot x, \ldots, A(d)\cdot x).$$

Let

$$T(i) = \{u \in (F^e)^k \mid A(i)\cdot u = 0\}.$$

Let

$$S(j) = \{x \in (F^e)^k \mid B(j)\cdot x = 0\}.$$

Clearly the $S(j)$s and the $T(j)$s are in general position and the intersection of the $T(i)$s is the kernel of π. If w is a vector in $(F^e)^d$ choose a random member u of $\pi^{-1}(w)$. We let the ith shadow associated with w be

$$H(i) = \{x \in (F^e)^k \mid B(i)\cdot x = B(i)\cdot u\}.$$

The conditions of the Karnin/Greene/Hellman scheme are similar to those of Definition (3.1) and similar security proofs may be obtained. In particular, the Karnin/Greene/Hellman scheme reduces to Bloom's scheme if $e = 1$. Simply replace F^k by $(F^k)^*$ and the random vector u in $\pi^{-1}(w)$ by $u^* \in (F^k)^*$, where $u^*(x) = u \cdot x$ for every $x \in F^k$. Then $\pi: F^k \to F^d$ becomes

$$\pi(u^*) = (u^*(A(1)), .., u^*(A(d)),$$

$S(i)$ becomes $\{u^* \mid u^*(A(i)) = 0\}$ and so forth.

4. FIELD SIZES

We have paid little attention to the field F underlying the vector spaces above. But with general (d,k,n) ramp scheme, as with its special case the k out of n threshold scheme and the k out of n p/s/r process it is necessary that the underlying field contain at least n members. The reason for this is that otherwise it is not possible to find the necessary hyperplanes (or points, as the case may

be) in general position as required by the formulation given in Section 3.

Actually the cardinality of the field can drop as low as $n-2$ in some rather exceptional cases. There is, for example a Bloom 3 out of 6 p/s/r process (i.e. a Bloom (3,3,6) ramp scheme) whose underlying field is GF(4). The reason for this is that the six vectors

$$[1,0,0]$$
$$[0,1,0]$$
$$[0,0,1]$$
$$[1,1,1]$$
$$[1,a,b]$$
$$[1,b,a]$$

are in general position in $GF(4)^3$, where the members of GF(4) are $0,1,a$ and $b = a^2$.

But the $n-2$ bound is seldom attained, and it is an open question [MA67] to characterize all the cases in which this happens.

For many purposes there is no advantage to be gained by using large field in building a threshold scheme (i.e. a (1,k,n) ramp scheme) if a smaller field would suffice. The latter, which could be implemented more cheaply and quickly, would provide as much security--Shannon perfect security--as the former.

But, when it comes to more general ramp schemes, there are many occasions on which use of a large underlying field might be desirable. Only Shannon relative security (or even merely Shannon t t-relative security) is available to the user of a (d,k,n) ramp scheme when $d \geq 2$. So it might be desirable to have a large haystack of shadows in which to hide the message needle. Somebody who used $GF(2^{32})$ as the underlying field for let us say, a (2,5,9) ramp scheme would have the consolation of knowing that an opponent who had obtained four shadows corresponding to a single test of two 32-bit words would still have nothing other than his a priori guess as to which of 4 billion possibilities was the correct value of the 64 bit string in question. The opponent would, of course, be better off for knowing the four shadows, having thereby eliminated more than 18 billion billion possibilities.

Contrast this state of affairs with 8 successive applications of a (2,5,9) ramp scheme over GF(16) to the same 64 bits of information. Each successive 8-bit substring would be narrowed down to one of 16 possibilities. The total possible number of values of the 64 bit string would again be some what over 4 billion to an opponent who had intercepted four shadows of everything. But, though

the opponents recovery problems in the two cases at hand thus look mathematically equivalent, they are not cryptographically equivalent. Suppose for example, that the original 64 bit string were eight latin letters ASCII coded, and each of the successive two-halbyte lists were the ASCII code for a single letter. The 16 possibilities for each symbol would be narrowed down to 1 or 2 by the requirement that it be one of only 26 bytes among all 256 possible bytes. The opponent would thus recover the message without machine assistance if the underlying field were GF(16). No such cheap approach is available when $GF(2^{32})$ is employed.

The question of infinite fields is a different matter, as noted in [BL83]. However the duality relationship between Blakley schemes and Shamir/Bloom scemes enables us to give a satisfactory solution to some of the problems raised in [BL83]. We can now produce Shannon perfectly secure rigid Blakley projective geometric (d,k,n) ramp schemes which amount to natural, and very efficient, generalizations of infinite one-time pads [BL83]. This development will be described in full elsewhere.

5. ASMUTH/BLOOM SCHEMES

In this section we look at an example of a ramp scheme based on the Asmuth/Bloom threshold scheme [AS83].

Choose prime numbers $p(1)$ through $p(d)$ and integers $m(1)$ through $m(k+n)$ such that the following properties hold:

(i) $p(1) < p(2) < \ldots < p(d) < m(1) < \ldots < m(k+n)$

(ii) All of the numbers in (i) are pairwise relatively prime.

(iii) $\prod_{i=1}^{k} m(i) > p(d) \prod_{i=1}^{k-1} m(k+n+1-i)$

(iv) $\prod_{i=1}^{k} m(i) < \prod_{j=1}^{d} p(j) \prod_{i=1}^{k-d+1} m(k+i)$

Denote the product of the $p(i)$s by P and the product of the k smallest $m(i)$s by M. Let V be the collection of all integers y such that $0 \leq y < M$. Let W be Z/PZ. Let the revealing map π be the evaluation mod P. We choose the shadows in the following way. Let w be an element of Z/PZ. Choose a random number A such that $0 \leq y = x+AP < M$. The ith shadow $H(i)$ is the set of all integers z between zero and M such that $y \equiv z \bmod m(i+i)$. The intersection of any r shadows $H(i_1), \ldots, H(i_r)$ is, by the Chinese Remainder

Theorem, the set of all z between zero and M such that $y \equiv z$ modulo the product of $m(k+i_1)$ through $m(k+i_r)$.

(5.1) Proposition: The Asmuth-Bloom scheme is a (d,k,n) ramp scheme with $\ell = d-k$. Knowledge is gained in a regular way with knowledge of each shadow after $d-k$ shadows in the sense that

a) Knowledge of $k-d$ shadows and knowledge of y modulo $d-s+1$ of the $p(i)$s gives us knowledge of w.

b) Knowledge of $k-d+s$ shadows does not give us knowledge of y modulo any $d-s$ of the $P(i)$s.

Proof: First we note that if the $m(i)$s are relatively close to the $p(i)$s (which is guaranteed by part (iii) of the definition) then

$$\log \frac{|V|}{|W|} \approx \frac{k}{d}.$$

Now suppose we know k shadows, that is, suppose we know y modulo k of the $m(k+i)$s. Denote their product by B. By the Chinese Remainder Theorem, we know y mod B. Since $B \geq M$, there is only one number z such that $0 \leq Z < M$ and $y \equiv Z \bmod B$, namely y. Thus the intersection of k shadows is a single point in $\pi^{-1}(w)$, and so the Asmuth-Bloom scheme satisfies part a) of Definition (2.1).

Next suppose that we know no more than $k-d$ shadows, that is, that we know y modulo no more than $k-d$ of the $m(k+i)$s. Denote their product by B. By the Chinese Remainder Theorem, we know y modulo B. By (iii) and (i) $M/B > P$, and since P is relatively prime to all the $m(i)$s, this means that the set of all integers z $z \equiv y \bmod B$ and $z < M$ covers all congruence classes modulo P. Thus the restriction of π to the intersection of no more than $k-d$ shadows is surjective, and so the Asmuth-Bloom scheme satisfies part (b) of Definition (2.1).

Next, suppose we know $k-d+s$ shadows, where $1 \leq s < d$. Let B denote the product of the corresponding $m(k+i)$s. Let C denote the product of any $d-s$ of the $p(i)$s. By (i) and (iii) $M/B > C$. From this fact and the fact that C and B are relatively prime, we can conclude that the set of all integers z such that $z \equiv y \bmod B$ and $z < M$ covers all congruence classes mod C. Thus, if we let ρ denote the projection from Z/PZ to Z/CZ, the restriction of $\rho \circ \pi$

to the intersection of the shadows is surjective, giving us part b) of the proposition.

Finally, suppose that we know y modulo k-d-s of the primes and d-s+1 of the m(k+i)s. Denote the product of the primes by C and the product of the m(k+i)s by B. By (i) and (iv) M < BC. Thus knowledge of y modulo BC gives us y, giving us part a) of the proposition.

We note that conditions (iii) and (iv) of the definition of the Asmuth/Bloom ramp scheme can be changed by requiring that

$$\prod_{i=1}^{k} m(i) > p(d) \cdot \prod_{i=1}^{k-1+t} m(k+n+1-i)$$

and

$$\prod_{i=1}^{k} m(i) < \prod_{j=1}^{d} p(j) \cdot \prod_{i=1}^{k-d+t} m(k+i)$$

for some positive integer $t < d$. This would lessen the amount of information gained with each shadow. Knowledge of k-d+s shadows and d-s+t of the p(i)s would be required for knowledge of w. Or we could leave part (iii) of the definition unchanged: this would have the advantage of allowing us more leeway in choosing the m(i)s, and would mean that knowledge of k-d+s shadows and d-s+t of the p(i)s would always give us knowledge of w, while knowledge of fewer of the p(i)s sometimes would and sometimes would not, depending on the shadows. However, in both cases efficiency would be lost. The change in part (iii) of the definition would require the ratio m(1)/p(d) to be larger, while the change in part (iv) would allow the ratio to be larger.

(5.2) Theorem. Let R be a (d,k,n) Asmuth/Bloom ramp scheme. Let P denote the product of the p(i)s, let M denote the product of the k smallest m(i)s, and, for $1 \leq r \leq d-k$, let M_r denote the product of the r largest m(i)s. If $r \leq k-d$ then R is Shannon t-relatively secure with knowledge of r shadows if and only if

$$([M/M_r P] - 1/t)([M/P] - 1/t) > (1+t)/t^2 .$$

If $r > k-d$ then R is t-relatively secure if and only if

$$[M/P] - 1/t > 0$$

Proof: By Lemma (2.6) it is enough to show that, if H is the intersection of r shadows, then

$$(5.3) \qquad \frac{\left|\pi^{-1}(w)\right|}{(1+t)\left|\pi^{-1}(w^*)\right|} < \frac{\left|\pi^{-1}(w) \cap H\right|}{\left|\pi^{-1}(w^*) \cap H\right|} < \frac{(1+t)\left|\pi^{-1}(w)\right|}{\left|\pi^{-1}(w^*)\right|}$$

for all w and w^* in $\pi(H)$. Let H be the intersection of r shadows. Then H is the set of all z between zero and M such that $z \equiv y \bmod B$, where B is the product of the r $m(k+i)$s corresponding to the ℓ shadows. The cardinality of $\pi^{-1}(w)$ for a given w in Z/PZ is either $[M/P]$ or $[M/P] + 1$, and the cardinality of $\pi^{-1}(w) \cap H$ is either $[M/BP]$ or $[M/BP] + 1$, where $[\ ]$ denotes the greatest integer function. We consider the two cases:

A: $r \leq k-d$ (in which case $[M/BP] > 0$), and

B: $r > k-d$ (in which case $[M/BP] = 0$).

Case A. Suppose that $\ell \leq k-d$. Then $[M/BP] > 0$. The worst possible case as far as the right half of inequality (5.3) is concerned is

$$\left|\pi^{-1}(w)\right| = [M/P],$$

$$\left|\pi^{-1}(w^*)\right| = [M/P] + 1$$

$$\left|\pi^{-1}(w) \cap H\right| = [M/BP] + 1, \text{ and}$$

$$\left|\pi^{-1}(w^*) \cap H\right| = [M/BP].$$

We are thus reduced to proving the inequality

$$([M/BP] + 1)/[M/BP] < (1+t)[M/P]/[M/P] + 1.$$

This is equivalent to

$$([M/BP] - 1/t)([M/P] - 1/t) > (1+t)/t^2.$$

Since $B \leq N_r$ and can be equal to N_r it is thus necessary and sufficient to have

$$([M/N_rP] - 1/t)([M/P] - 1/t) > (1+t)/t^2.$$

The proof of the left-hand side of inequality (5.3) is similar.

Case B. Suppose that $\ell > k-d$. By conditions (i) and (iv) of the definition of the Asmuth/Bloom scheme we then have $[M/BP] = 0$. Thus the cardinality of $\pi^{-1}(w) \cap H$ is either 0 or 1. Since we are only interested in proving the inequality for w and w^* in $\pi(H)$, the worst possible case as far as the right half of inequality (4.3) is

$$\left|\pi^{-1}(w)\right| = [M/P],$$

$$\left|\pi^{-1}(w^*)\right| = [M/P] + 1,$$

$$\left|\pi^{-1}(w) \cap H\right| = 1,$$

and

$$\left|[\pi^{-1}(w^*) \cap H\right| = 1.$$

We thus have to prove the inequality

$$\frac{1}{[M/P]} < \frac{(1-t)}{[M/P] + 1}$$

This is equivalent to $[M/P] - 1/t > 0$.

There are two apparent contradictions here that need to be resolved. First we might ask the question: what if we choose t such that $[M/P] - 1/t < 0$? Then would it be possible that

$$([M/N_rP - 1/t)([M/P] - 1/t) < (1+t)/t^2 \tag{4.4}$$

thus giving Shannon t-relative security for small t but not possibly for larger t? The answer is no. For suppose that $[M/P] - 1/t < 0$ and that equation (4.4) holds. Then we have

$$([M/N_rP] - 1/t)([M/P] - 1/t) = t^2[M/N_rP][M/P] - t([M/N_rP] + [M/P] + 1$$

$$> (t+1)/t^2$$

Hence

$$t^2[M/N_rP][M/P] > t([M/N_rP] + [M/P] + 1)$$

and so

$$\frac{1}{t} < \frac{[M/N_rP][M/P]}{[M/N_rP] + [M/P] + 1}$$

But

$$[M/N_rP] - \frac{[M/N_rP][M/P]}{[M/N_rP] + [MP] + 1} = \frac{[M/N_rP]^2 + [M/N_rP]}{[M/N_rP] + [MP] + 1} > 0 .$$

Thus $[M/N_rP] - 1/t > 0$, and so $[M/P] - 1/t > 0$.

The other apparent contradiction is that the requirements for t-relative security after knowledge of k-d shadows is less stringent than the requirement before, making it seem that we lose information as we gain knowledge of the shadows. But this contradiction appears only if we forget the fact that after k-d shadows some probabilities, which are not figured in the computations of t-relative security, go to zero. Thus, in spite of appearances, we still have more information than before.

Note that Shannon t-relative security and Condition (iii) of the definition of the Asmuth/Bloom scheme require that M be large in comparison to PN_r, while Condition (iv) requires that M be relatively small. If d is large then Shannon t-relative security and Condition (iii) become relatively easy to obtain, while Condition (iv) becomes harder. The reverse is true if d is small.

The difficulty seems to lie in the inequality in Condition (iii). If this inequality could be replaced by an equality, then it and the first two conditions would suffice to give us a ramp scheme. Condition (iv). This indeed can be done in certain cases of the generalized Asmuth/Bloom scheme, in which the integers are replaced by a Euclidean domain and the p(i)s and m(i)s can be replaced by relatively prime elements of the same degree. However, since the only known practical example of such a scheme is Shamir's scheme [SH79], which was discussed in Section 3, we refrain from discussing generalized Asmuth-Bloom schemes here.

This work was supported in part by NSA Grant MDA-83-H-0002.

REFERENCES

AS81 C. A. Asmuth and G. R. Blakley, An efficient algorithm for constructing a cryptosystem which is harder to break than two other cryptosystems, Computers and Mathematics with Applications, Vol. 7 (1981), pp. 447-450.

AS82 C. A. Asmuth and G. R. Blakley, Pooling, splitting and restituting information to overcome total failure of some channels of communication, Proceedings of the 1982 Symposium on Security and Privacy, IEEE Computer Society, Los Angeles, (1982), pp. 156-169.

AS83 C. Asmuth and J. Bloom, A modular approach to key safeguarding. IEEE Transactions on Information Theory, Vol. IT-30 (1983), pp. 208-210.

BL79 G. R. Blakley, Safeguarding cryptographic keys, Proceedings of the National Computer Conference, 1979, American Federation of Information Processing Societies -- Conference Proceedings, Vol. 48 (1979), AFIPS Press, Montvale, New Jersey (1979), pp. 313-317.

BL80 G. R. Blakley, One-time pads are key safeguarding schemes, not cryptosystems. Fast key safeguarding schemes (threshold schemes) exist, Proceedings of the 1980 Symposium on Security and Privacy, IEEE Computer Society, New York (1980), pp. 108-113.

BL81a G. R. Blakley and Laif Swanson, Security proofs for information protection systems, Proceedings of the 1981 Symposium on Security and Privacy, IEEE, Computer Society, New York (1981), pp. 75-88.

BL81b J. Bloom, A note on superfast threshold schemes, Preprint, Texas A&M University, Department of Mathematics (1981)

and

Threshold schemes and error correcting codes, Abstracts of Papers Presented to the American Mathematical Society, Vol. 2 (1981), p. 230.

BL82 G. R. Blakley, Protecting information against both destruction and unauthorized disclosure, Proceedings of the 1982 Carnahan Conference on Security Technology, University of Kentucky Press, (1982), pp. 123-133.

BL83 G. R. Blakley and L. Swanson, Infinite structures in information theory, in D. Chaum, R. L. Rivest and A. T. Sherman, Advances in Cryptology, Proceeding of Crypto '82, Plenum Press, New York (1983), pp. 39-50.

CH79 D. Chaum, Computer systems established, maintained, and trusted by mutually suspicious groups, Memorandum No. UCB/ERL/M79/10, UC Berkeley ERL (1979).

CH82 D. Chaum, Computer systems established, maintained and trusted by mutually suspicious groups, Ph.D. dissertation in Computer Science, UC Berkeley (1982).

DA80 G. I. Davida, R. A. DeMillo and R. J. Lipton, Protecting shared cryptographic keys, Proceedings of the 1980 Symposium on Security and Privacy, IEEE Computer Society, New York (1980), pp. 100-102.

DE82 D. E. R. Denning, Cryptography and Data Security, Addison-Wesley, Reading, Massachusetts (1980).

HA83 S. Harari, Secret sharing systems, in Secure Digital Communications, Edited by G. Longo, Springer-Verlag, Wien (1983), pp. 105-110.

HO71 K. Hoffman and R. Kunze, Linear Algebra, Second Edition, Prentice Hall, Englewood Cliffs, New Jersey (1971).

KA83 E. D. Karnin, J. W. Greene and M. E. Hellman, On secret sharing systems, Verbal presentation, Session B3 (Cryptography), 1981 IEEE International Symposium on Information Theory, Santa Monica, California, February 9-12 (1981),

and

On secret sharing systems, IEEE Transactions on Information Theory. Vol. IT-29 (1983), pp. 35-41.

KO81 A. G. Konheim, Cryptography: A Primer, Wiley-Interscience, New York (1981).

KO85 S. Kothari, On a Generalized Threshold Scheme, Proceedings of Crypto '84, Springer-Verlag, New York (1985).

LI83 R. Lidl and H. Niederreiter, Finite Fields, Vol. 20 of the Encyclopedia of Mathematics and its Applications, Addison-Wesley, Reading, Massachusetts (1983).

MA67 S. MacLane and G. Birkhoff, Algebra, MacMillan, New York, (1967).

MA78 F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam (1978).

MC81 R. J. McEliece and D. V. Sarwate, On sharing secrets and Reed-Solomon codes, communications of the ACM, Vol. 24 (1981), pp. 583-584.

MI87 M. Mignotte, How to share a secret, in Cryptography, Edited by T. Beth, Springer-Verlag, Berlin (1983), pp. 371-375.

OZ84 L. H. Ozarow and A. D. Wyner, Wire-tap channel, II, AT&T Bell Labs Technical Journal, vol. 63 (1984), to appear.

SH79 A. Shamir, How to share a secret, Communications of the ACM, Vol. 22 (1979), pp. 612-613.