J. Cryptology (1993) 6: 87–95

Journal of
CRYPTOLOGY

# Secret Sharing Over Infinite Domains*

Benny Chor and Eyal Kushilevitz**
Department of Computer Science,
Technion, Haifa 32000, Israel
benny@techsel.bitnet

Communicated by Ernest F. Brickell

Received 30 November 1990 and revised 11 May 1992

**Abstract.** Let $\mathscr{F}_n$ be a monotone, nontrivial family of sets over $\{1, 2, \ldots, n\}$. An $\mathscr{F}_n$ perfect secret-sharing scheme is a probabilistic mapping of a secret to $n$ shares, such that:

- The secret can be reconstructed from any set $T$ of shares such that $T \in \mathscr{F}_n$.
- No subset $T \notin \mathscr{F}_n$ of shares reveals any partial information about the secret.

Various secret-sharing schemes have been proposed, and applications in diverse contexts were found. In all these cases the set of secrets and the set of shares are finite.

In this paper we study the possibility of secret-sharing schemes over *infinite* domains. The major case of interest is when the secrets and the shares are taken from a *countable* set, for example all binary strings. We show that no $\mathscr{F}_n$ secret-sharing scheme over any countable domain exists (for any $n \geq 2$).

One consequence of this impossibility result is that no *perfect private-key encryption schemes*, over the set of all strings, exist. Stated informally, this means that there is no way to encrypt all strings perfectly without revealing information about their length. These impossibility results are stated and proved not only for perfect secret-sharing and private-key encryption schemes, but also for wider classes—*weak* secret-sharing and private-key encryption schemes.

We constrast these results with the case where both the secrets and the shares are real numbers. Simple perfect secret-sharing schemes (and perfect private-key encryption schemes) are presented. Thus, infinity alone does not rule out the possibility of secret sharing.

**Key words.** Secret sharing, Perfect private-key encryption.

* This research was supported by Technion V.P.R. Fund 120-722, New York Metropolitan research fund, and by US–Israel BSF Grant 88-00282. An early version of this paper appeared in *Advances in Cryptology, Proceedings of Crypto '89*, G. Brassard, ed., pp. 299–306, Lecture Notes in Computer Science, Vol. 435, Springer-Verlag, Berlin, 1990.

** Present address: Aiken Computation Laboratory, Harvard University, 33 Oxford Street, Cambridge, MA 02138, U.S.A. eyalk@das.harvard. edu.

## 1. Introduction

The topic of this paper is the existence of secret-sharing schemes over infinite domains. A *generalized secret-sharing scheme* is a way of distributing a secret among $n$ parties in a way that "legal" sets of parties will be able to reconstruct the secret, while "illegal" sets of parties will not get information about the secrets. This is formalized by the following definitions:

**Definition 1.** Let $\mathscr{F}_n$ be a family of subsets of $\{1, 2, \ldots, n\}$ (intuitively, $\mathscr{F}_n$ will be the family of all sets of parties which are allowed to reconstruct the secret). The family $\mathscr{F}_n$ is called *good* if it satisfies the following properties:

- *Monotonicity*: if $T \in \mathscr{F}_n$ and $T \subset T'$, then $T' \in \mathscr{F}_n$. (Intuitively, we want that if a set $T$ is allowed to reconstruct the secret then any set $T'$ that contains $T$ is also allowed to reconstruct the secret.)
- *Nontriviality*: there is a set $T \in \mathscr{F}_n$ which is not a singleton, and is minimal with respect to membership in $F_n$. That is, $|T| \geq 2$ and, for every proper subset $D$ of $T$, $D \notin \mathscr{F}_n$. (Intuitively, if $\mathscr{F}_n$ does not have this property, then it is trivially determined by a set of singletons $C \subset \{1, 2, \ldots, n\}$: if $i \in C$, then the $i$th party gets the secret, while if $i \notin C$, the $i$th party gets a useless share.)

**Definition 2.** Let $A$ be an arbitrary set of possible secrets, let $\mathscr{F}_n$ be a good family of sets, and let $\alpha \geq 1$ be a constant. An $(\mathscr{F}_n, \alpha)$ *secret-sharing scheme* over $A$ is a probabilistic mapping $\Pi$: $A \to B_1 \times B_2 \times \cdots \times B_n$ from the set of secrets to a set of $n$-tuples (the shares) such that:

1. The secret $a$ can be reconstructed from any "legal" set of shares. That is, for any subset $T \in \mathscr{F}_n$, there exists a function $h_T$: $\bigtimes_{i \in T} B_i \to A$ such that, for every possible set of shares $(s_1, \ldots, s_n) = \Pi(a)$, the secret can be found by $h_T(\{s_i\}_{i \in T}) = a$.
2. No "illegal" set of shares reveals "too much" partial information about the secret (in the information-theoretic sense). Formally, for any subset $T \notin \mathscr{F}_n$, for every two secrets $a_1, a_2 \in A$ and for every possible shares $\{s_i\}_{i \in T}$:

$$\frac{1}{\alpha} \cdot \Pr(\{s_i\}_{i \in T} | a_2) \leq \Pr(\{s_i\}_{i \in T} | a_1) \leq \alpha \cdot \Pr(\{s_i\}_{i \in T} | a_2).$$

We remark here that in this definition no specific probability distribution is associated with the secrets. Each secret determines a probability measure over the space of secrets. Some special cases of the above definition are of particular interest:

- For $\alpha = 1$, a $(\mathscr{F}_n, \alpha)$ *secret-sharing scheme* is called *perfect*. In a perfect secret-sharing scheme, no illegal set of shares reveals *any* partial information about the secret.
- The case where $\mathscr{F}_n$ contains all the subsets of size at least $k$. These schemes are usually called $(k, n, \alpha)$ *threshold* schemes.

Perfect threshold schemes were first introduced by Blakley [7] and Shamir [14]. Since then, other constructions were given (see [12]), properties of these schemes were studied [4], [16], and various applications were found (e.g., [13], [10], and [3]). Generalized (perfect) schemes were introduced and constructed in [11] and [5].

In all the above-mentioned works, the set of secrets and the set of shares are finite. In this paper we investigate the possibility of secret sharing over infinite domains. The main motivation for studying the question comes from infinite countable domains where each member has a finite description (over a finite alphabet). Typical examples are the set of all integers and the set of all binary strings. Can we share any secret string using only strings as shares? More generally, can we share a secret from any infinite set, using only elements of this set as shares? It turns out that the possibility (or impossibility) of secret-sharing schemes is not based on infinity alone. The cardinality of the domain has to be examined. In particular we show:

1. If the sets of secrets and shares are *countable* (that is, of the same cardinality as the integers), then no $(\mathscr{F}_n, \alpha)$ secret-sharing schemes exist for any $n \geq 2$, a good family $\mathscr{F}_n$, and $\alpha \geq 1$.
2. If the sets of secrets and shares have cardinality $\aleph$ (the cardinality of the reals), then $\mathscr{F}_n$ *perfect* secret-sharing schemes exist for any good family $\mathscr{F}_n$.

As we deal with infinite domains, we require that the probability measure defined over these spaces satisfies $\sigma$-additivity [6, p. 19]. That is, if $A_1, A_2, \ldots$ is a sequence of disjoint measurable sets, then $\Pr(\bigcup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \Pr(A_i)$. In particular, if $\Pr(A_i) = 0$ for all $i$, then the probability of their union is also 0.

A *perfect private-key encrption scheme* [15] is an encryption scheme where an eavesdropper gets no partial information about the plaintext by examining the ciphertext. Again, the notions used are not complexity-based but rather information theoretic. The classical example of a perfect private-key encryption scheme is the Vernam "one-time pad." This scheme is perfect provided all messages are of equal length. Otherwise ciphertexts encrypting different length plaintexts could be distinguished merely by observing the length of the ciphertext. A simple counting argument would show that it is not possible to have a perfect private-key encryption scheme over all strings and still bound the length of all possible ciphertexts of any individual string. Here, we show that even if no such bound is assumed, perfect private-key encryption over a countable domain is not possible. This holds even for schemes where a key is used just once, to encrypt a single plaintext. Interestingly, the proof is by a reduction to the problem of secret sharing and is thus valid for an appropriately defined notion of a *weak* private-key encryption scheme. Again, we complement this result by giving a perfect private-key encryption scheme over the reals.

The remainder of this paper is organized as follows: in Section 2 we discuss secret-sharing schemes over countable domains. Section 3 deals with private-key encryption schemes over countable domains. Finally, in Section 4 we treat the case of real domain.

*Chronological Remark.* Results which are closely related to ours have appeared in two papers by Blakley and Swanson [8], [9]. Our results are more general, as they apply to *weak*, *generalized* secret-sharing and *weak* encryption schemes, while those of [8] only apply to *perfect*, *threshold* schemes and *perfect* encryption schemes.

Our proofs are entirely different and substantially simpler than those in [8] and [9]. In addition, the statement of the main impossibility result (our Theorem 1) seems to require fewer conditions than the statement appearing in Theorem 5.1 of [8].

## 2. Secret Sharing over Countable Sets

In this section we deal with secret-sharing schemes in which both the secrets and the shares are taken from countable sets. We prove that such schemes do not exist.

Clearly, if the set of secrets is infinite, then the set of shares must be infinite too. Otherwise, if there are only $m$ possible shares, they can encode at most $m^n$ secrets. Therefore if we are interested in countable sets of secrets (such as the set of all integers or the set of all strings), then the set of shares must be at least countable too. It is also easy to see that no secret-sharing scheme can map every $n$ bit long secret $s$ into shares of length less than or equal to $f(n)$ for any function $f(n)$. (This observation is used, in a different context, in Theorem 4.2 of [1].) However, in this section we show that a countable set of shares is not enough even if there is no bound on the length of possible shares.

The first lemma claims that if there exists a $(\mathscr{F}_n, \alpha)$ secret-sharing scheme over a set $A$, then there also exists a $(2, 2, \alpha)$ secret-sharing scheme (that is, a 2 out of 2 threshold scheme) over the set $A$. This can be considered as a complementary result to a result of Benaloh and Leichter [5] which shows how to use a (2, 2) perfect threshold scheme in order to construct $\mathscr{F}_n$ perfect secret-sharing schemes for any good $\mathscr{F}_n$.

**Lemma 1.** *Let $A$ be a set of secrets. Let $n \geq 2$ and $\alpha \geq 1$. Let $\mathscr{F}_n$ be a good family. If there exists a $(\mathscr{F}_n, \alpha)$ secret-sharing scheme over the set $A$, then there exists a $(2, 2, \alpha)$ threshold scheme over the set $A$.*

**Proof.** By the assumption that $\mathscr{F}_n$ is good there exists a set $T \in \mathscr{F}_n$, such that $|T| \geq 2$ and such that every $D \subsetneq T$ satisfy $D \notin \mathscr{F}_n$. Let $\varnothing \neq D_1 \subsetneq T$, and let $D_2 = T \backslash D_1$. Clearly, $D_1, D_2 \notin \mathscr{F}_n$, and $D_2 \neq \varnothing$.

The $(2, 2, \alpha)$ threshold scheme will work by generating the $n$ shares $s_1, \ldots, s_n$ as in the $(\mathscr{F}_n, \alpha)$ secret-sharing scheme. The first share in the new scheme will be all the shares corresponding to parties in $D_1$ in the original scheme (i.e., $\{s_i\}_{i \in D_1}$). The second share in the new scheme will be all the shares corresponding to parties in $D_2$ in the original scheme (i.e., $\{s_i\}_{i \in D_2}$). The two new shares determine what the secret is. This is because these shares carry the same information that the shares of $D_1 \cup D_2 = T$ have in the original $(\mathscr{F}_n, \alpha)$ scheme, and $T$ is a "legal" set (that is, $T \in \mathscr{F}_n$). On the other hand, for every secret $a \in A$ and for every possible shares $\{s_i\}_{i \in D_1}$ the probability $\Pr(\{s_i\}_{i \in D_1} | a)$ in the new scheme is exactly the same as in the original scheme, and therefore the condition

$$\frac{1}{\alpha} \cdot \Pr(\{s_i\}_{i \in D_1} | a_2) \leq \Pr(\{s_i\}_{i \in D_1} | a_1) \leq \alpha \cdot \Pr(\{s_i\}_{i \in D_1} | a_2)$$

still holds for every two secrets $a_1, a_2 \in A$. This implies that the first share of the new scheme does not reveal "too much" information about the secret, since it carries the same amount of information as the shares of $D_1$ have in the original scheme. A similar argument holds for the second share (consists of the shares of $D_2$ in the original scheme). Therefore the new scheme is a (2, 2, $\alpha$) threshold scheme. □

It is also important to note that if the set of shares in the original scheme is infinite, then the set of shares in the new (2, 2) threshold scheme has the same cardinality.

**Theorem 1.** *Let $A$ be a countable set. Let $n \geq 2$, $\alpha \geq 1$, and $\mathscr{F}_n$ be a good family of sets. Then there is no $(\mathscr{F}_n, \alpha)$ secret-sharing scheme distributing secrets taken from $A$ using shares taken from a countable set.*

**Proof.** Assume, toward a contradiction, that for some $n$, $\alpha$, and $\mathscr{F}_n$ as above there exists a $(\mathscr{F}_n, \alpha)$ secret-sharing scheme. By Lemma 1, this implies the existence of a (2, 2, $\alpha$) threshold scheme. Denote by $h$ the function which reconstructs the secret from the two shares ($h$: $B_1 \times B_2 \to A$). Recall that a (2, 2, $\alpha$) threshold scheme on the set $A$ is a probability distribution $\Pi$ which defines, for every secret $a$ and every pair of "shares" $(s_1, s_2)$, the probability $\Pr((s_1, s_2)|a)$ in a way that:

(1) If $h(s_1, s_2) \neq a$, then $\Pr((s_1, s_2)|a) = 0$.

(2) Any two secrets $a_1$ and $a_2$, and any share $s_2 \in B_2$, satisfy

$$\Pr(s_2|a_1) = \sum_{s_1 \in B_1} \Pr((s_1, s_2)|a_1) \leq \sum_{s_1 \in B_1} \alpha \cdot \Pr((s_1, s_2)|a_2) = \alpha \cdot \Pr(s_2|a_2).$$

(3) Any two secrets $a_1$ and $a_2$, and any share $s_1 \in B_1$, satisfy

$$\Pr(s_1|a_1) = \sum_{s_2 \in B_2} \Pr((s_1, s_2)|a_1) \leq \sum_{s_2 \in B_2} \alpha \cdot \Pr((s_1, s_2)|a_2) = \alpha \cdot \Pr(s_1|a_2).$$

Let $a_0 \in A$ be an arbitrary secret. Since $B_1$ and $B_2$ are countable (and so is $B_1 \times B_2$) there must be a pair of shares $(s_1', s_2')$ such that $\Pr((s_1', s_2')|a_0) > 0$ (otherwise as $B_1 \times B_2$ is countable then by $\sigma$-additivity the secret $a_0$ could not be shared). Let $\varepsilon$ denote $\Pr(s_1'|a_0) > 0$. From (3), for every $a \in A$ we have $\Pr(s_1'|a) \geq \varepsilon/\alpha$. Given any secret $a \in A$, we define

$$B_2^a = \{s_2 | h(s_1', s_2) = a\}.$$

Then

$$\begin{aligned}\sum_{s_2 \in B_2^a} \Pr(s_2|a) &= \sum_{s_2 \in B_2^a} \sum_{s_1 \in B_1} \Pr((s_1, s_2)|a) \\ &\geq \sum_{s_2 \in B_2^a} \Pr((s_1', s_2)|a) \\ &= \Pr(s_1'|a) \qquad \text{(by the } B_2^a \text{ definition)} \\ &\geq \frac{\varepsilon}{\alpha}.\end{aligned}$$

That is,

$$\sum_{s_2 \in B_2^a} \Pr(s_2|a) \geq \frac{\varepsilon}{\alpha}. \qquad (*)$$

Also note that by the $B_2^a$ definition the sets $B_2^{a_1}$ and $B_2^{a_2}$ are disjoint for any two secrets $a_1 \neq a_2$, and furthermore

$$\bigcup_{a \in A} B_2^a = B_2. \tag{$**$}$$

Thus

$$\begin{aligned}
1 &= \sum_{s_2 \in B_2} \Pr(s_2 | a_0) \\
&= \sum_{a \in A} \sum_{s_2 \in B_2^a} \Pr(s_2 | a_0) \qquad \text{(by ($**$) and $\sigma$-additivity)} \\
&\geq \sum_{a \in A} \sum_{s_2 \in B_2^a} \frac{1}{\alpha} \cdot \Pr(s_2 | a) \qquad \text{(by (2))} \\
&= \sum_{a \in A} \frac{1}{\alpha} \cdot \sum_{s_2 \in B_2^a} \Pr(s_2 | a) \\
&\geq \sum_{a \in A} \frac{\varepsilon}{\alpha^2} \qquad \text{(by ($*$))} \\
&= \infty \qquad \text{(since $A$ is infinite).}
\end{aligned}$$

Contradiction. □

The intuition behind the proof is that over the Cartesian product of two countable domains, it is not possible to assign any probability distribution where a countable number of points get nonzero mass and the projection on any single coordinate is "almost" uniform.

## 3. Perfect Encryption over Countable Sets

In this section we deal with perfect and "almost-perfect" private-key encryption schemes. We show that there is no such scheme which encrypts an arbitrary string using a string. We start with the formal definitions:

A *private-key encryption scheme* consists of three parts:

(1) A way of choosing keys from a set $K$. This way is expressed by a probability distribution $\Pi$ over the set $K$.

(2) A private-key encryption function $E$ that takes a plaintext $p$ and a key $k$ and produces a ciphertext $c$ (that is, $E(p, k) = c$).

(3) A decryption function $D$ that takes a ciphertext $c$ and a key $k$ and produces the original plaintext $p$ (that is, $D(E(p, k), k) = p$).

Let $\alpha \geq 1$. An encryption scheme is called *$\alpha$-weak* if it also satisfies:

(4) For every two possible plaintexts $p_1$ and $p_2$ and every ciphertext $c$, an eavesdropper does not learn from the ciphertext "too much" information about which of the two is the plaintext that was sent. Formally:

$$\frac{1}{\alpha} \cdot \Pr(c | p_2) \leq \Pr(c | p_1) \leq \alpha \cdot \Pr(c | p_2).$$

For $\alpha = 1$ an $\alpha$-weak encryption scheme is called *perfect*. Intuitively, in such a case an eavesdropper does not learn from the ciphertext *any* information about which is the plaintext that was sent.

We stress again that this definition is valid even if no probability distrubition on plaintexts is assumed. In case such a probability distribution exists, then (4) with $\alpha = 1$ is equivalent to Shannon's definition [15] stating that every plaintext $p$ and every ciphertext $c$ satisfies $\Pr(p|c) = \Pr(p)$. That is, the *a priori* probability of the plaintext equals the *a posteriori* probability of the plaintext after seeing the ciphertext.

The most famous perfect private-key encryption scheme is the "one-time pad" system which enables a user A to send any plaintext (of the same length as the key) to a user B in a way that an eavesdropper cannot get any information about the plaintext. The claim of our theorem is that there is no perfect private-key encryption scheme for encrypting arbitrary strings. We emphasize that this is true even though ciphertexts corresponding to a single plaintext can have unbounded length.

**Theorem 2.** *Let $\alpha \geq 1$ and let $K$, $P$, and $C$ be countable sets of possible keys, plaintexts, and ciphertexts (respectively). Then there is no $\alpha$-weak private-key encryption scheme encrypting plaintext taken from $P$ using keys from $K$ and ciphertext from $C$.*

**Proof.** The idea is to show that if an $\alpha$-weak encryption scheme exists, then a $(2, 2, \alpha)$ secret-sharing over countable sets of secrets and shares exists. This is done by observing that an $\alpha$-weak private-key encryption scheme is a special case of a $(2, 2, \alpha)$ secret-sharing scheme, in which one of the shares (the key) is chosen before the secret is known.

We assume the existence of an $\alpha$-weak encryption scheme and we construct the following $(2, 2, \alpha)$ secret-sharing scheme for distributing a secret $p$ taken from the countable set $P$: the share of the first participant, $P_1$, will be a $k \in K$ chosen according to the probability distribution $\Pi$, and the share of the second participant, $P_2$, will be $c = E(p, k)$. Clearly, $P_1$ and $P_2$ together can reconstruct $p$, since $D(c, k) = p$. The participant $P_1$ does not learn anything about $p$ since $k$ is chosen independently from $p$. That is, $\Pr(k|p_1) = \Pr(k|p_2)$. In addition, $P_2$ does not learn "too much" about $p$ since according to condition (4) of $\alpha$-weak encryption schemes $1/\alpha \cdot \Pr(c|p_2) \leq \Pr(c|p_1) \leq \alpha \cdot \Pr(c|p_2)$. □

## 4. Secret Sharing over the Reals

In this section we deal with secret-sharing schemes over the real numbers. Although it has no practical implications, it is interesting to ask the question whether secret-sharing schemes do not exist over every infinite set, or maybe some properties of countable sets are the cause of the results of Section 2.

We introduce a simple secret-sharing scheme using real numbers. Since there is a 1–1 and onto transformation from the real numbers to the unit interval $[0, 1)$, it is more convenient to use this interval as the set of secrets. We use the same interval as the set of shares, as it allows us to use the uniform probability distribution.

We first have to define what we mean by a secret-sharing scheme over the reals. More specifically, we have to define what we mean by saying that no "illegal" set (i.e., $T \notin \mathscr{F}_n$) of shares reveals any information about the secret. All the schemes we present in this section are *perfect* ($\alpha = 1$), and therefore $\alpha$ is omitted from the notations. The following natural definition is used:

For every two secrets $a_1, a_2 \in A$, for any set of indices $T \notin \mathscr{F}_n$, and for any $|T|$-tuple of measurable sets $\{C_i\}_{i \in T} \subseteq [0, 1)$ the following holds:

$$\Pr(\forall i \in T: s_i \in C_i | a_1) = \Pr(\forall i \in T: s_i \in C_i | a_2).$$

We can now present a secret-sharing scheme for every good family of sets $\mathscr{F}_n$ $(n \geq 2)$, using ideas that were used in the finite case [4], [5]. We first introduce a $(k, k)$ secret-sharing scheme which distributions a secret $a$ taken from the interval $[0, 1)$. We use the Legesgue measure on $[0, 1)$.

1. Choose independently, with a uniform distribution, $k - 1$ real numbers, $s_1, \ldots, s_{k-1}$, in the interval $[0, 1)$.
2. Choose $s_k \in [0, 1)$ which satisfies $s_1 + \cdots + s_{k-1} + s_k = a \pmod 1$.

The proof that this is indeed a secret-sharing scheme is similar to the proof of its analogue in the finite case.

For introducing an $\mathscr{F}_n$ secret-sharing scheme for every good family of sets $\mathscr{F}_n$, we observe that the same technique described in [5] works here as well.

**Corollary 3.** *Let $\mathscr{F}_n$ be a good family of sets $(n \geq 2)$. There is an $\mathscr{F}_n$ (perfect) secret-sharing scheme for distributing secrets taken from a countable set using shares which are real numbers.*

We can arbitrarily embed the countable set of secrets in the interval $[0, 1)$, and distribute the result according to the above scheme. It is easy to see that the result is a secret-sharing scheme. (Note that the shares in this scheme are real numbers, thus this does not contradict the results of Section 2.) Similarly, it is possible to construct perfect private-key encryption schemes with keys uniformly distributed in $[0, 1)$.

The difference between the case of countable sets and the case of the real numbers stems from different properties of the cardinalities $\aleph_0$ and $\aleph$. Our results were generalized to other infinite cardinalities by Ben-David [2].

## Acknowledgments

We would like to thank Shai Ben-David, Oded Goldreich, and Hugo Krawczyk for helpful discussions on the topics of this paper. We would also like to thank Bob Blakley for acquainting us with his work [8], [9].

## References

[1] Abadi, M., J. Feigenbaum, and J. Kilian, On Hiding Information from an Oracle, *J. Comput. System Sci.*, Vol. 39, No. 1, pp. 21–50, 1989.

[2] Ben-David, S., Private communication.

[3] Ben-or, M., S. Goldwasser, and A. Wigderson, Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation, *Proc. 20th Symp. on Theory of Computing*, pp. 1–10, 1988.

[4] Benaloh (Cohen), J. D., Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret, *Advances in Cryptography—Crypto 86 (Proceedings)*, A. M. Odlyzko (ed.), pp. 251–260, Lecture Notes in Computer Science, Vol. 263, Springer-Verlag, Berlin, 1987.

[5] Benaloh, J., and J. Leichter, Generalized Secret Sharing and Monotone Functions, *Advances in Cryptography—Crypto 86 (Proceedings)*, A. M. Odlyzko (ed.), pp. 213–222, Lecture Notes in Computer Science, Vol. 263, Springer-Verlag, Berlin, 1987.

[6] P. Billingsley, *Probability and Measure*, Wiley, New York, 1979.

[7] Blakley, G. R., Safeguarding Cryptographic Keys, *Proc. NCC AFIPS 1979*, pp. 313–317, 1979.

[8] Blakley, G. R., and L. Swanson, Security Proofs for Information Protection Systems, *Proc. IEEE Symp. on Security and Privacy*, 1981, pp. 75–88.

[9] Blakley, G. R., and L. Swanson, Infinite Structures in Information Theory, *Proc. Crypto 82*, pp. 39–50.

[10] Goldreich, O., S. Micali, and A. Wigderson, How To Play Any Mental Game, *Proc 19th Symp. on Theory of Computing*, pp. 218–229, 1987.

[11] Ito, M., A. Saito, and T. Nishizeki. Secret Sharing Schemes Realizing General Access Structure, *Proc. IEEE Global Telecommunication Conf., Globecom 87*, pp. 99–102, 1987.

[12] Kothari, S. C., Generalized Linear Threshold Scheme, *Advances in Cryptography—Crypto 84 (Proceedings)*, G. R. Blakey and D. Chaum (ed.), pp. 231–241, Lecture Notes in Computer Science, Vol. 196, Springer-Verlag, Berlin, 1985.

[13] Rabin, M. O., Randomized Byzantine Generals, *Proc. 24th Symp. on Foundations of Computer Science*, pp. 403–409, 1983.

[14] Shamir, A., How To Share a Secret, *Comm. ACM*, Vol. 22, 1979, pp. 612–613.

[15] Shannon, C. E., Communication Theory of Secrecy Systems, *Bell System Tech. J.*, Vol. 28, 1949, pp. 657–715.

[16] Stinson, D. R., and S. A. Vanstone, A Combinatorial Approach to Threshold Schemes, *SIAM J. Discrete Math.*, Vol. 1, 1988, pp. 230–236.