Secret Sharing Over Infinite Domains* (extended abstract)

Benny Chor†
Eyal Kushilevitz‡

Department of Computer Science
Technion, Haifa 32000, Israel

Abstract: A (k, n) secret sharing scheme is a probabilistic mapping of a secret to n shares, such that

- The secret can be reconstructed from any k shares.
- No subset of $k-1$ 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 (k, n) secret sharing scheme over any countable domain exists (for any $2 \leq k \leq n$).

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 perfectly encrypt all strings without revealing information about their length.

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

*Supported by Technion V.P.R. fund 120-722 – New York Metropolitan research fund.
†benny@techsel.bitnet
‡eyalk@techunix.bitnet

G. Brassard (Ed.): Advances in Cryptology - CRYPTO '89, LNCS 435, pp. 299-306, 1990.

1. INTRODUCTION

Let A be an arbitrary set of possible secrets. A *(k,n)-secret-sharing scheme* 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 k shares. That is, for any subset $T \subseteq \{1,2,...,n\}$ of size $|T| = k$, there exists a function $h_T: B_{i_1} \times \cdots \times B_{i_k} \to A$ such that $h_T(\{s_i\}_{i \in T}) = a$.
2) No subset of less than k shares reveals any partial information about the secret (in the information theoretic sense). Formally, for any subset $T \subseteq \{1,2,...,n\}$ of size $|T| \leq k-1$, for every two secrets $a_1, a_2 \in A$ and for every possible shares $\{s_i\}_{i \in T}$:

$$Pr(\{s_i\}_{i \in T} \mid a_1) = Pr(\{s_i\}_{i \in T} \mid a_2)$$

We remark here that this definition is valid even if no specific probability distribution is associated with the secrets.

Secret-sharing schemes were first introduced by Blakley [Bl] and Shamir [Sh]. Since then, other constructions were given (see [Ko]), the characteristics of these schemes were studied [Bh,SV], and various applications were found (e.g. [Ra , GMW , BGW]).

In all the abovementioned 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 domains where every 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. One has to examine the cardinality of the domain. 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 (k,n) secret-sharing schemes exist for any $2 \leq k \leq n$.
2) If the sets of secrets and shares has cardinality $\aleph$ (the cardinality of the reals), then (k,n) secret-sharing schemes exist for any $1 \leq k \leq n$.

A *perfect private-key encryption scheme* [Shannon] 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 perfect private-key encryption scheme is Vernam "one time pad". This scheme is perfect provided all messages are of equal length. Otherwise one could distinguish between ciphertexts encrypting different length plaintexts 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 one removes this restriction, 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. Again, we complement this result by giving a perfect private-key encryption scheme over the reals.

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

Note added in proof: The same results have appeared in works of Blakley and Swanson [BS1,BS2]. The main difference between these works and ours is in the proof methods.

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 or equal $f(n)$, for any function $f(n)$ (This observation is used, in a different context, in [AFK, Theorem 4.2]). 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.

Lemma 1: Let $2 \le k \le n$. If there exists a (k,n) secret-sharing scheme then there exists a (k,k) secret-sharing scheme.

Proof: The (k,k) scheme will work by generating the n shares as in the (k,n) scheme and then distributing only k of them. The k shares enable the reconstruction of the secret since they enable it in the original scheme. On the other hand any $k-1$ shares do not reveal any information about the secret since they do not reveal such information in the original scheme. Therefore the new scheme is a (k,k) secret-sharing scheme. □

Lemma 2: Let $2 \le k$. If there exists a (k,k) secret-sharing scheme then there exists a (2,2) secret-sharing scheme.

Proof: The (2,2) scheme will work by generating the k shares as in the (k,k) scheme. $k-1$ of the shares will be the first share in the new scheme and the last share will be the second share in the new scheme. The two new shares determine what is the secret since they carry the same information as the k shares have in the original (k,k) scheme. On the other hand each of the two new shares do not reveal any information about the secret

since any set of less than k shares does not reveal any information in the original scheme. Therefore the new scheme is a (2,2) secret-sharing scheme □

Theorem 1: Let A be a countable set. For every $2 \le k \le n$ there is no secret-sharing scheme distributing secrets taken from A using shares taken from a countable set.

Proof: Using the two lemmas above it is enough to show that a (2,2) secret-sharing scheme does not exist in order to prove that for every $2 \le k \le n$ a (k,n) secret-sharing scheme does not exist. Denote by h the function which reconstruct the secret from the two shares ($h: B_1 \times B_2 \to A$). Recall that a (2,2) secret sharing-scheme on the set A is a probability distribution Π which defines for every secret a and every pair of "shares" (s_1,s_2), the probability $Pr((s_1,s_2) \mid a)$ in a way that:

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

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

$$Pr(s_2 \mid a_1) = \sum_{s_1 \in B_1} Pr((s_1,s_2) \mid a_1) = \sum_{s_1 \in B_1} Pr((s_1,s_2) \mid a_2) = Pr(s_2 \mid a_2)$$

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

$$Pr(s_1 \mid a_1) = \sum_{s_2 \in B_2} Pr((s_1,s_2) \mid a_1) = \sum_{s_2 \in B_2} Pr((s_1,s_2) \mid a_2) = Pr(s_1 \mid a_2)$$

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 $Pr((s'_1,s'_2) \mid a_0) > 0$ (otherwise the secret a_0 could not be shared). Let $\varepsilon > 0$ denote $Pr(s'_1 \mid a_0)$. From (3), for every $a \in A$ we have $Pr(s'_1 \mid a)=\varepsilon$. Given any secret $a \in A$, we define

$$B_2^a = \{ s_2 \mid h(s'_1,s_2)=a \}.$$

Then

$$\begin{aligned} \sum_{s_2 \in B_2^a} Pr(s_2 \mid a) &= \sum_{s_2 \in B_2^a} \sum_{s_1 \in B_1} Pr((s_1,s_2) \mid a) \\ &\ge \sum_{s_2 \in B_2^a} Pr((s'_1,s_2) \mid a) \\ &= Pr(s'_1 \mid a) \qquad \text{by } B_2^a \text{ definition} \\ &= \varepsilon. \end{aligned}$$

That is

$$\sum_{s_2 \in B_2^a} Pr(s_2 \mid a) \ge \varepsilon \qquad (*)$$

Also note that by B_2^a definition the sets B_2^{a1} and B_2^{a2} are disjoint for any two secrets

$a_1 \neq a_2$, and furthermore

$$\bigcup_{a \in A} B_2^a = B_2. \qquad (**)$$

Thus

$$\begin{aligned}
1 &= \sum_{s_2 \in B_2} Pr(s_2 | a_0) \\
&= \sum_{a \in A} \sum_{s_2 \in B_2^a} Pr(s_2 | a_0) && \text{by (**)} \\
&= \sum_{a \in A} \sum_{s_2 \in B_2^a} Pr(s_2 | a) && \text{by (2)} \\
&\geq \sum_{a \in A} \varepsilon && \text{by (*)} \\
&= \infty && \text{since } A \text{ is infinite}
\end{aligned}$$

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 countable number of points get non-zero mass and the projection on any single coordinate is uniform.

3. PERFECT ENCRYPTION OVER COUNTABLE SETS

In this section we deal with 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 Π 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 $D(E(p,k),k)=p$).

An encryption scheme is called *perfect* 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 any information which of the two is the plaintext which was sent. Formally:

$$Pr(c | p_1) = Pr(c | p_2)$$

We stress again that this definition is valid even if no probability distribution on plaintexts is assumed. In case that such probability distribution exists, then (4) is equivalent to Shannon's definition [Shannon] stating that every plaintext p and every ciphertext c satisfy $Pr(p \mid c)=Pr(p)$. 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 such a scheme does not exist 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 K,P,C be countable sets of possible keys, plaintexts and ciphertexts (respectively). Then there is no perfect 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 a perfect encryption scheme exists then a (2,2) secret-sharing scheme over countable sets of secrets and shares exists. This is done by observing that a perfect private-key encryption scheme is a special case of a (2,2) secret-sharing scheme, in which one of the shares (the key) is chosen before the secret is known.

We assume the existence of perfect encryption scheme and we construct the following (2,2) 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 Π, 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 $D(c,k)=p$. P_1 does not learn anything about p since k is chosen independently from p. P_2 does not learn anything about p since according to condition (4) of perfect encryption schemes $Pr(c \mid p_1)=Pr(c \mid p_2)$. □

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 specificly, we have to define what we mean by saying that no set of at most $k-1$ shares reveals any information about the secret. The following natural definition is used:

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

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

We can now present a secret-sharing scheme for every $2 \leq k \leq n$, using ideas that were used in the finite case [Bh,BL]. We first introduce a (k,k) secret-sharing scheme which distributes a secret a taken from the interval [0,1). We use the Lebesgue measure on [0,1).

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

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

For introducing a (k,n) secret-sharing scheme for every $k \leq n$, we observe that the same technique described in [BL] works here as well.

Corollary: There is a (k,n) secret-sharing scheme for distributing secrets taken from a countable set usings 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. 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 Shai Ben-David [Be].

ACKNOWLEDGEMENTS

We would like to thank Shai Ben-David, Oded Goldreich and Hugo Krawczyk for helpful discussions on the topics of this paper.

REFERENCES

[AFK] Abadi, M., J. Feigenbaum, and J. Kilian, "On Hiding Information from an Oracle", *JCSS*, Vol. 39, No. 1, pp. 21-50, 1989.

[Be] Ben-David, S., Private Communication.

[BGW] Ben-or M., S. Goldwasser, and A. Wigderson, "Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation" *Proc. of 20th STOC*, pp. 1-10, 1988.

[Bh] Benaloh, (Cohen), J.D., "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", *Advances in Cryptography - Crypto86 (proceedings)*, A.M. Odlyzko (ed.), Springer-Verlag, Lecture Notes in Computer Science, Vol. 263, pp. 251-260, 1987.

[BL] Benaloh, J., and J. Leichter, "Generalized Secret Sharing and Monotone Functions", *Advances in Cryptography - Crypto86 (proceedings)*, A.M. Odlyzko (ed.), Springer-Verlag, Lecture Notes in Computer Science, Vol. 263, pp. 213-222, 1987.

[Bl] Blakley, G.R., "Safeguarding Cryptographic Keys", *Proc. NCC AFIPS 1979* , pp. 313-317, 1979.

[BS1] Blakley, G.R., and L. Swanson, "Security Proof for Information Protection Systems", *Proc. IEEE Symposium on Security and Privacy*, 1981, pp. 75-88.

[BS2] Blakley, G.R., and L. Swanson, "Infinite Structures in Information Theory", *Proc. Crypto82*, pp. 39-50.

[GMW] Goldreich, O., S. Micali, and A. Wigderson, "How to Play Any Mental Game", *Proc. of 19th STOC*, pp. 218-229, 1987.

[Ko] Kothari, S. C., "Generalized Linear Threshold Scheme", *Advances in Cryptography - Crypto84 (proceedings)*, G.R. Blakely and D. Chaum (ed.), Springer-Verlag, Lecture Notes in Computer Science, Vol. 196, pp. 231-241, 1985.

[Ra] Rabin M.O., "Randomized Byzantine Generals " *Proc. of 24th FOCS*, pp. 403-409, 1983.

[Sh] Shamir, A., "How to Share a Secret", *Comm. ACM* , Vol. 22, 1979, pp. 612-613.

[Shannon] Shannon, C.E., "Communication Theory of Secrecy Systems", *Bell System Technical Jour.*, Vol. 28, 1949, pp. 657-715.

[SV] Stinson, D. R., and S. A. Vanstone, "A Combinatorial Approach to Threshold Schemes", *SIAM Jour. on Disc. Math.*, Vol. 1, 1988, pp. 230-236.