On Secret Sharing Systems

EHUD D.KARNIN, JONATHAN W.GREENE,
MARTIN E.HELLMAN
IEEE TRANSACTIONS ON INFORMATION THEORY,
VOL IT-29, PP. 35-41, JANUARY 1983

Prepared by
Chao-yu Chen

Department of Institute of Communications Engineering
National Tsing Hua University, Taiwan 300, R.O.C.

DEC 27, 2000

Outline

- Introduction
- Requirements for a secret sharing system
- Goal
- Bounds on the maximum value of n

Introduction

Cryptography is extremely useful for making data files unintelligible to any one who does not possess the secret key.

- There is a need for providing a backup copy of the key to protect against losing the secret key. To guard against simultaneous destruction, these copies should be stored in separated parts.
  Letting v_i denote the information stored in the ith deposit box and letting s denote the secret key,

  $$v_1 = v_2 = \ldots = v_n = s.$$

  But theft of even one piece compromises the secret.

Introduction

A approach protects against the threat of theft.
Dividing the secret key s into n pieces. Letting v_1 to v_{n-1} be independent random variables, uniformly distributed over S, and letting

$$v_n = s + (v_1 + v_2 + \cdots + v_{n-1})(mod\ q),$$

where $q = |S|$ is the cardinality of S.
But if even one of the v_i is destroyed, the user is unable to reconstruct the secret key.

Goal

Dividing a secret s into n pieces $v_1, v_2, \cdots, v_n$, each chosen from a set V, such that the following conditions are satisfied.

C1) The secret s is recoverable from any k pieces ($k \le n$).

C2) Knowledge of $k - 1$ or fewer pieces provides absolutely no information about s.

If the system is not to involve data expansion we also require:

C3) $|V| \le |S|$. That is, each pieces v_i is to be no longer than s.

Any such system will be referred to as a "$k - out - of - n$ secret sharing system."

Restating these requirements using the notation of information theory we have for any set of k indices $\{i_1, i_2, \cdots, i_k\}$:

$$H(s|v_{i_1}, v_{i_2}, \cdots, v_{i_k}) = 0$$

and

$$H(s|v_{i_1}, v_{i_2}, \cdots, v_{i_{k-1}}) = H(s).$$

Theorem 1: For conditions C1) and C2) to hold it is necessary that

$$H(v_i) \geq H(s), \quad i = 1, 2, \cdots, n.$$

Note: If s is uniformly distributed over S then C3) can be represented as $H(v_i) \leq H(s)$. Then theorem 1 implies that

$$H(v_1) = H(s), \quad i = 1, 2, \cdots, n.$$

Requirements for a Secret Sharing System

Theorem 2: Associating s with v_0, and generating from $GF(2)$ to any finite field $GF(q)$, the problem of finding a secret sharing system of the form

$$v_i = uA_i$$

is equivalent to the following.

Requirements for a Secret Sharing System

Find a set of $n+1$ matrices over $GF(q), \{A_0, A_1, A_2, \cdots, A_n\}$, each of dimension km-by-m, such that every set of k of the A_i has full rank, km.
(m is the secret size and k is the number of pieces required to reconstruct the secret. The dimension of u is km.)

Requirements for a Secret Sharing System

Example: Here is a 2-out-of-4 system with a 2-bit secret s:

$$A_0 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} A_1 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} A_2 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} A_3 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix} A_4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

, where u is (u_1, u_2, u_3, u_4).

In this example

$$s = uA_0 = (u_1, u_2),$$

$$v_1 = uA_1 = (u_3, u_4),$$

$$v_2 = uA_2 = (u_1 + u_2 + u_3, u_2 + u_4),$$

$$v_3 = uA_3 = (u_2 + u_3, u_1 + u_4),$$

$$v_4 = uA_4 = (u_1 + u_3, u_2 + u_3 + u_4).$$

It can be shown that any single piece knows nothing about s and that any two pieces can solve for $s = (u_1, u_2)$.

Requirements for a Secret Sharing System

Theorem 3: The secret s can be taken to be the first m components of u without loss of generality. Further, v_1 can be taken to be the next m components of u, v_2 can be taken to be the next m components of $u, \cdots$, and v_{k-1} can be taken to be the last m components of u.

Bounds On the Maximum Value of n

Theorem 4: Given $|S| = q^m$ and k, a one component secret sharing system of the form $v = uG$ has

$$\begin{aligned} q^m \leq n_{max} \leq q^m + k - 2, &\quad q^m > k \\ n_{max} = k, &\quad q^m \leq k \end{aligned}$$