On General Perfect Secret Sharing Schemes

G. R. Blakley[1] and G. A. Kabatianski[2]

[1] Department of Mathematics, Texas A&M University, USA
blakley@math.tamu.edu
[2] IPPI, Moscow, Russia, on leave at Department of Mathematics, Texas A&M University
kaba@ippi.ac.msk.su

Abstract. The purpose of this paper is to provide a general information-theoretic framework extensible to arbitrary access structures and to establish the correspondence between ideal SSS and matroids without invoking the more restrictive combinatorial definition of ideal scheme.

1 Introduction

The history of secret sharing schemes (SSS) began in 1979 when this problem was introduced and partially solved for the case of (n, τ)-threshold schemes (see [1], [2]). R. McEliece and D. Sarwate pointed out [3] a relationship between threshold schemes and codes in 1981. In 1983, E. Karnin, J. Greene, and M. Hellman [4] gave an information-theoretic (IT) approach to SSS. Later this approach was developed in [5]. In our opinion the most important step in the classification of ideal perfect SSS was taken by E. F. Brickell and D. M. Davenport [6] by establishing the relationship between *combinatorial ideal* (*i.e.* such that secret and shadows belong to the same alphabet) schemes and matroids. To do this they used not only combinatorial techniques but also combinatorial definitions. Recently K. Kurosawa *et al.* [11], following the ideas of [6], have shown that this relationship is also true for the case of IT ideal perfect SSS, but only under the restrictive assumption of uniform distribution of secrets.

In this paper we treat SSS by information-theoretic tools, in continuation of the approach of [4], [5]. We prove a new bound on the "cardinality" of a perfect SSS which shows, in particular, that such a scheme should have properties similar to the properties of a well-known combinatorial object—an orthogonal array. For ideal SSS we generalize the result of Brickell and Davenport under a general definition of ideal scheme based on information-theoretic notions. Our paper is self-contained and it seems to us that our proof is not only simpler than [6], [11], but sheds a different light on this problem.

2 Definitions

The problem of SSS can be formulated in the following way. There is a secret s_0 chosen from the set $\mathcal{S}_0$ of all possible secrets with probability $p(s_0)$. And there is a dealer who provides information to n participants in a such a way that some

D. Coppersmith (Ed.): Advances in Cryptology - CRYPTO '95, LNCS 963, pp. 367-371, 1995.

sets of participants, called allowed coalitions, can recover the secret exactly, but participants forming any other set cannot get additional information beyond their *a priori* information about the value of the secret. To do this, the dealer uses some (finite) alphabets $\mathcal{S}_1, \ldots, \mathcal{S}_n$, whose elements are called "shares" (or "shadows"). For a given s_0, the dealer distributes shares $s_1, \ldots, s_n$ (the i-th participant receives share s_i, and has no information about the values of other shares) chosen by him with probability $P_{s_0}(s_1, \ldots, s_n)$. We define the probability distribution P on a set $\mathcal{S} = \mathcal{S}_0 \times \cdots \times \mathcal{S}_n$, where $P(s) = P(s_0, s_1, \ldots, s_n) = p(s_0)P_{s_0}(s_1, \ldots, s_n)$. Equivalently one can start from some distribution P on a set $\mathcal{S} = \mathcal{S}_0 \times \cdots \times \mathcal{S}_n$. Any such a pair $(P, \mathcal{S})$ can be considered to be an SSS. We call a point $(s_0, s_1, \ldots, s_n)$ a "sharing rule". P is called the distribution of sharing rules. We regard the share values s_i as random variables with joint distribution P, and denote them S_i.

Let Γ be some access structure, *i.e.* let Γ be a set of subsets of $\{1, \ldots, n\}$ with the monotonic property ($A \in \Gamma, A \subset B$ imply $B \in \Gamma$). W.l.o.g. one can restrict consideration to Γ containing neither "negligible" participants (*i.e.* j such that $j \in A \in \Gamma$ always implies $A \backslash \{j\} \in \Gamma$) or "super" participants (*i.e.* j such that $\{j\} \in \Gamma$). We call a pair $(P, \mathcal{S})$ a perfect SSS, realizing the access structure Γ, if

1. $P(S_0 = c_0 \mid S_i = c_i, i \in A) \in \{0, 1\}$ if $A \in \Gamma$
2. $P(S_0 = c_0 \mid S_i = c_i, i \in A) = P(S_0 = c_o)$ if $A \notin \Gamma$

Following [4] we reformulate the above definition in the language of entropy, *i.e.*

1. $H(S_0 \mid S_i, i \in A) = 0$ if $A \in \Gamma$
2. $H(S_0 \mid S_i, i \in A) = H(S_0)$ if $A \notin \Gamma$

Define a set $V = \{s \in \mathcal{S} \mid P(s) > 0\}$ and call it the "array" (or the "code") of the SSS $(P, \mathcal{S})$. Roughly speaking, combinatorial treatments of SSS deal with an array V whose rows are uniformly distributed, *i.e.* ***only*** with a uniform distribution of sharing rules (or, if one allows repetitions of row, probabilities have to be only rational numbers). Then the definition of the perfect SSS can be reformulated in "cardinality" language (see [8]). E. F. Brickell and D. M. Davenport gave [6] another definition of "perfect scheme" which is weaker than the usual one(s) given above. In fact, they replaced Property 2 by the following property. If the set of rows of V having given entries c_i in positions belonging to a set A, $A \notin \Gamma$, is not empty then any value of s_0 (*i.e.* "0"-entry) occurs among these rows. The usual combinatorial definition demands that all values of s_0 occur equally often. It is easy to see that the array of any perfect SSS is perfect according to the definition of [6], but there are examples of arrays which generate perfect SSS in the sense defined in [6] and which do not give rise to any perfect SSS in the usual sense of "perfect". Luckily, for the case of *combinatorial ideal* SSS, these notions coincide [6].

As we mentioned above, the combinatorial(C) definition of *ideal* is that $|\mathcal{S}_i| = |\mathcal{S}_0|$ for all $i = 1, \ldots, n$. The information-theoretic (IT) definition is based on the

amount of information which the dealer should send through a channel to the i-th participant. It equals $H(S_i)$. It is known (see [5]) that for any perfect SSS, $H(S_i) \geq H(S_0)$ for all $i = 1, \ldots, n$. Therefore we call a perfect SSS IT-ideal (or C-ideal) if $H(S_i) = H(S_0)$ (or, $|\mathcal{S}_i| = |\mathcal{S}_0|$, correspondingly) for all $i = 1, \ldots, n$.

3 New bound for the cardinality of general perfect SSS

Instead of considering a pair $(P, \mathcal{S})$ we will consider only a pair (P, V), because $P(s) = 0$ for $s \notin V$. We call $|V|$ the cardinality of the SSS. We do not know to whom to attribute the following simple result.

Lemma 1 *If a pair (P, V) is a perfect SSS for some access structure Γ and some probability distribution p on the set of secrets $\mathcal{S}_0$ then the pair (P', V) perfectly realizes the same Γ and a distribution p', where $P'(s_0, \ldots, s_n) = \frac{p'(s_0)}{p(s_0)} P(s_0, \ldots, s_n)$.*

Denote by $\Gamma_{\min}$ the set of minimal subsets of Γ. The following lemma (see [5]) is very useful.

Lemma 2 $H(S_j \mid S_i, i \in A \backslash \{j\}) \geq H(S_0)$ *for any* $A \in \Gamma_{\min}$ *and any* $j \in A$.

Corollary 1 $H(S_i, i \in A) \geq |A| \cdot H(S_0)$ *for any* $A \in \Gamma_{\min}$.

Denote by V_A the minor of the array V whose columns belong to the set $A \subseteq \{1, \ldots, n\}$ and by $\|V_A\|$ the number of different rows of this minor. Consider any perfect SSS (P, V) with corresponding access structure Γ. According to Lemma 1, there is a perfect realization of the same access structure Γ with uniform distribution of secrets and with the same array V. Hence, for the new SSS, $H(S_0) = \log q$, where $q = |\mathcal{S}_0|$ is the number of secrets. On the other hand, $H(S_i, i \in A) \leq \log \|V_A\|$, with equality if and only if different rows of V_A occur equally often. Therefore the following result is true:

Theorem 1. $\|V_A\| \geq q^{|A|}$ *for any perfect SSS (P, V) and any $A \in \Gamma_{\min}$ with equality only if different rows of V_A occur equally often.*

Corollary 2 *For any perfect SSS, the cardinality of its array satisfies the inequality $|V| \geq q^{\gamma}$, where $\gamma = \max\{|A|, A \in \Gamma_{\min}\}$.*

4 Ideal schemes and matroids

We will distinguish between two definitions of an ideal SSS. For the combinatorial definition, Theorem 1 guarantees that the array of any C-ideal perfect SSS has the property that all possible rows occur equally often within the "subarray" V_A. Such a property (similar to a corresponding property of an orthogonal array) already provides enough power to give a new proof of the result of [6] for the particular case of perfect C-ideal SSS. But we will do more. We will prove it for the more general information-theoretic definition of an ideal SSS.

Let us recall the definition of matroid (see [10]). A matroid is a finite set X and a collection $\mathcal{I}$ of subsets of X (called independent sets) such that the following properties hold.

1. $\varnothing \in \mathcal{I}$
2. If $A \in \mathcal{I}$ and $B \subseteq A$ then $B \in \mathcal{I}$
3. If $A, B \in \mathcal{I}$ and $|A| = |B|+1$ then there exists $a \in A \setminus B$ such that $a \cup B \in \mathcal{I}$

There are other equivalent definitions of matroid. One is based on the *rank* function, and another on minimal dependent sets, called *circuits*. Let (P, V) be an IT-ideal SSS for the access structure Γ. Define a function h on subsets A of the set $\{0, \ldots, n\}$ in the following way: $h(A) = H(S_i, i \in A)$. W.l.o.g. let $h(0) = 1$. Then well known properties of entropy assure us that the following properties of a rank function of matroid hold (see [10]):

1. $h(\varnothing) = 0$
2. $h(A) \leq h(b \cup A) \leq h(A) + 1$
3. If $h(A \cup b) = h(A \cup c) = h(A)$ then $h(A \cup b \cup c) = h(A)$

The entropy is not always an integer-valued function, unfortunately. Otherwise we could immediately conclude that our definition produces a matroid. The main point of the proof of [6] was to prove that $\log_q |V_A|$ is an integer-valued function. It is clear that, if one assigns uniform probability distribution to rows of V, then $\log_q |V_A|$ is exactly the above-defined function $h(A)$. K. Kurosawa *et al.* [11] applied this approach to IT-ideal SSS and proved that, under the assumption of uniformly distributed secrets, $h(A)$ is an integer-valued function, and hence serves as the rank function of the matroid. We use another, simpler, way to provide a proof without appealing to a uniform distribution on secrets. We replace the desired "integer-valued" property by a weaker one, which is much simpler to prove for general IT-ideal perfect SSS.

Lemma 3 *If $h(A) = |A|$, then $h(A \cup b)$ equals either $|A|$ or $|A| + 1$ for any b.*

Based on this lemma, the following generalization of result of E. F. Brickell and D. M. Davenport [6] can be proved.

Theorem 2. *For any IT-ideal perfect SSS the independent sets A such that $h(A) = |A|$ define a matroid. All circuits of this matroid which contain the point 0 are of the form $0 \cup A, A \in \Gamma_{\min}$.*

The second part of the statement of Theorem 2 is very important (see[9]), because all circuits of a matroid can be uniquely (and rather simply, see [10]) determined by all its circuits containing a given point. Hence, a matroid's structure can be derived directly from the access structure Γ. This fact provides a tool for proving that some access structures cannot be realized by IT-ideal SSS.

5 Acknowledgment

Shortly after submitting this paper, we received a preprint of the forthcoming [7] by W.-A. Jackson and K. M. Martin. Among its numerous results, it already provided a different sort of proof of Theorem 2, very much in the spirit of [6]. We are indebted to Keith Martin for thoughtful commentary and criticism in the ensuing discussions.

References

1. G. R. Blakley, Safeguarding cryptographic keys, *Proceedings of AFIPS 1979 National Computer Conference*, vol.48, N. Y., 1979,pp. 313–317.
2. A. Shamir, How to share a secret, *Communications of the ACM*, vol.22,no.1, 1979, pp. 612–613.
3. R. J. McEliece and D. V. Sarwate, On secret sharing and Reed-Solomon codes, *Communications of the ACM*, vol. 24, 1981, pp. 583–584.
4. E. D. Karnin, J. W. Greene, and M. E. Hellman, On secret sharing systems, *IEEE Transactions on Informatiom Theory*, vol. 29,no. 1, 1983, pp. 231–241.
5. R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, On the size of shares for secret sharing schemes, *Journal of Cryptology*, vol. 6, 1993, pp. 157–167.
6. E. F. Brickell and D. M. Davenport, On the classification of ideal secret sharing schemes, *Journal of Cryptology*, vol. 4, 1991, pp. 123–134.
7. W.-A. Jackson and K. M. Martin, Combinatorial models for perfect secret sharing schemes, Submitted to *Journal of Combinatorial Mathematics and Combinatorial Computing*
8. D. R. Stinson, An explication of secret sharing schemes, *Designs,Codes and Cryptography*, vol.2, 1992, pp. 357–390.
9. K. M. Martin, Discrete structures in the theory of secret sharing, Ph. D. thesis, University of London, 1991.
10. D. J. A. Welsh, *Matroid Theory*, Academic Press, 1976.
11. K. Kurosawa, K. Okada, K. Sakano, W. Ogata and S. Tsujii, Nonperfect secret sharing schemes and matroids, Advances in Cryptology—EUROCRYPT'93, Lect. Notes in Comput. Sci. vol. 765, 1993, pp. 126–141.