J. Cryptology (1998) 11: 75–86

Journal of
CRYPTOLOGY

On Matroid Characterization of Ideal Secret Sharing Schemes*

Jovan Dj. Golić
School of Electrical Engineering, University of Belgrade,
Bulevar Revolucije 73, 11001 Belgrade, Yugoslavia
golic@galeb.etf.bg.ac.yu

Communicated by Ernest F. Brickell

Received 16 April 1993 and revised 10 October 1996

Abstract. A characterization of ideal secret sharing schemes with an arbitrary number of keys is derived in terms of balanced maximum-order correlation immune functions. In particular, it is proved that a matroid is an associated matroid for a binary ideal secret sharing scheme if and only if it is representable over the binary field. Access structure characterization of connected binary ideal schemes is established and a general method for their construction is pointed out.

Key words. Ideal secret sharing schemes, Matroids, Access structures.

1. Introduction

A *secret sharing scheme* is a procedure of sharing a secret key k from a finite set $\mathcal{K}$ among a finite set $\mathcal{P}$ of participants in a random way such that certain specified subsets of participants, from the so-called *access structure* Γ, can compute the key by pooling their shares picked from a finite set $\mathcal{S}$ and given to participants by a dealer D, $D \notin \mathcal{P}$. A natural requirement is that Γ be *monotone*, that is, if $A \in \Gamma$ and $A \subseteq B \subseteq \mathcal{P}$, then $B \in \Gamma$. Let the set of minimal elements of Γ be called the *minimal access structure* and be denoted as Γ_m. A secret sharing scheme is said to be *connected* if every participant $p \in \mathcal{P}$ is contained in some subset in Γ_m. A secret sharing scheme is called *perfect* if any subset of participants $P \notin \Gamma$ cannot gain any information about the key. The *information rate* for a secret sharing scheme can be defined as $\log_2|\mathcal{K}|/\log_2|\mathcal{S}|$. A perfect secret sharing scheme is said to be *ideal* if it has maximum information rate 1. Note that the first secret

* This research was supported in part by the Science Fund of Serbia, Grant #04M02, through the Mathematical Institute, Serbian Academy of Science and Arts. As independent work, this paper was submitted before the appearance of [1]. Part of this work was carried out while the author was with the Information Security Research Centre, Queensland University of Technology, Brisbane, Queensland, Australia.

sharing schemes introduced by Blakley [3] and Shamir [13] were the so-called threshold schemes, where Γ_m consists of all the subsets of $\mathcal{P}$ of a specified cardinality.

A comprehensive survey of secret sharing schemes and the corresponding literature can be found in [16], [4], and [15]. Ideal secret sharing schemes were first defined by Brickell [5]. In [10] and [2] it is shown how to realize perfect secret sharing schemes for arbitrary monotone access structures. In [2] it is also proved that a certain access structure cannot be realized by ideal secret schemes, and the corresponding upper bound on the information rate was then improved in [7] and later in [8], where the tight bound was found. Brickell and Davenport [6] established a connection between ideal secret sharing schemes and matroids and Martin [11] showed how to specify the associated matroid in terms of the access structure only. An interesting result was obtained by Seymour [12] who discovered a matroid (Vamos) that cannot be associated with any ideal secret sharing scheme. However, the characterization of the associated matroids and the achievable access structures as well as a general method for the construction of ideal secret sharing schemes are still open problems.

In this paper we first obtain a characterization of ideal secret sharing schemes for an arbitrary key size in terms of balanced maximum-order correlation immune functions [14]. For the binary key, we show that the associated matroids are binary and then characterize the achievable access structures and give a general construction method as well. Preliminaries are given in Section 2, the general case is studied in Section 3, and the binary one is analyzed in Section 4. Conclusions and open problems are given in Section 5.

2. Preliminaries

In this section we first review the basic definitions regarding perfect and ideal secret sharing schemes and then present and briefly discuss the main results from [6]. Let a finite set of secret keys be denoted as $\mathcal{K}$, a finite set of shares as $\mathcal{S}$, a finite set of participants as $\mathcal{P}$, a dealer as D, $D \notin \mathcal{P}$, the extended set of participants as $\mathcal{P}^* = \mathcal{P} \cup D$ where for simplicity $\{D\} = D$, and a finite randomizing set as $\mathcal{R}$. The total number of participants $|\mathcal{P}^*|$ is denoted as N. Further, for any function $F\colon \mathcal{R} \times \mathcal{P}^* \to \mathcal{K} \cup \mathcal{S}$ and arbitrary subsets $R \subseteq \mathcal{R}$ and $P \subseteq \mathcal{P}^*$, let, for any $r \in \mathcal{R}$, $F(r, P)$ denote the ordered set $\{F(r, p)\}_{p \in P}$ and let $F(R, P) = \{F(r, P) : r \in R\}$. Then a secret sharing scheme is defined in terms of a function F such that $F(\mathcal{R}, D) = \mathcal{K}$ and $F(\mathcal{R}, \mathcal{P}) \subseteq \mathcal{S}^{|\mathcal{P}|}$. For any $r \in \mathcal{R}$, the function $F(r, p)$, $p \in \mathcal{P}^*$, is usually called [16] a distribution rule. The distribution function F can be depicted as a matrix whose rows are indexed by $r \in \mathcal{R}$ and columns by $p \in \mathcal{P}^*$, see [6].

Let $\mathcal{R}_k = \{r : r \in \mathcal{R}, F(r, D) = k\}$, for any $k \in \mathcal{K}$. When the dealer D wants to distribute shares corresponding to a secret key, D first picks a key k at random according to an *arbitrary* prior probability distribution on $\mathcal{K}$, randomly chooses a value r such that $F(r, D) = k$ according to a *given* conditional probability distribution π_k on $\mathcal{R}_k$, and then distributes the share $F(r, p)$ to a participant p, for every $p \in \mathcal{P}$. A secret sharing scheme is then generally defined as an ordered set $\mathcal{F} = (F, \{\pi_k\}_{k \in \mathcal{K}})$ which besides the distribution matrix F also contains the conditional probability distributions as well. Without loss of generality, we assume that the conditional probability distributions are all strictly positive. Equivalently, $\mathcal{F}$ can be regarded as an ordered set of discrete random variables corresponding to individual participants including the dealer where the probability distribution associated with the dealer may be arbitrary. In a special case, if one assumes that the conditional probability distributions are all uniform, then a secret sharing scheme $\mathcal{F}$ can be expressed solely in terms of a distribution matrix F, see [6], [7], and [16]. For simplicity, such schemes are here denoted by F instead of $\mathcal{F}$. If, in addition, no two rows of F are identical, then a scheme is called *canonic*.

A secret sharing scheme $\mathcal{F}$ is called *perfect* with a monotone access structure Γ if for every prior probability distribution of secret keys: (1) for any qualified subset of participants $P \in \Gamma$, $H(D|P) = 0$ and (2) for any unqualified subset of participants $P \notin \Gamma$, $P \subseteq \mathcal{P}$, $H(D|P) = H(D)$, where H is the entropy operator, see [8]. Equivalently, $F(r, D)$ is a function of $F(r, P)$ for a qualified P and is (probabilistically) independent of $F(r, P)$ for an unqualified P. Clearly, $\mathcal{F}$ is perfect if it is perfect for any particular strictly positive prior probability distribution of secret keys. For secret sharing schemes with uniform conditional probability distributions, some combinatorial sufficient conditions for a scheme to be perfect in terms of the distribution matrix F only are given in [7] and [6]. We note that these conditions are easily generalized into the following *necessary and sufficient* conditions:

(1) If $P \in \Gamma$, then $F(r, P) = F(r', P) \Rightarrow F(r, D) = F(r', D)$.
(2) If $P \notin \Gamma$, $P \subseteq \mathcal{P}$, then for any secret key k and any achievable vector value v of $F(r, P)$, $|\{r : r \in \mathcal{R}_k, F(r, P) = v\}|/|\mathcal{R}_k|$ is independent of k.

Conditions (1) and (2) characterize functional dependence and probabilistic independence of $F(r, D)$ and $F(r, P)$, respectively. As was suggested in [6] and [7], condition (2) can be replaced by a weaker one which describes what can be called possibilistic independence:

(2′) If $P \notin \Gamma$, $P \subseteq \mathcal{P}$, then, for any secret key k and any achievable vector value v of $F(r, P)$, $|\{r : r \in \mathcal{R}_k, F(r, P) = v\}| > 0$.

Any secret sharing scheme $\mathcal{F}$, with not necessarily uniform conditional probability distributions, can then be called *weakly perfect* with a monotone access structure Γ if its distribution matrix F satisfies conditions (1) and (2′). This notion was introduced in [6] and [7], but only for secret sharing schemes with uniform conditional probability distributions. To summarize, a secret sharing scheme with uniform conditional probability distributions is perfect if and only if its distribution matrix satisfies (1) and (2), and any secret sharing scheme is weakly perfect if and only if its distribution matrix satisfies (1) and (2′). Since the conditional probability distributions are generally assumed to be strictly positive, it follows that a perfect secret sharing scheme must also be weakly perfect with the same access structure. While the converse is clearly not true in general, it may be true that every weakly perfect secret sharing scheme can be transformed into a perfect one with the same access structure.

Perfect and weakly perfect secret sharing schemes such that $|\mathcal{S}| = |\mathcal{K}|$ are called *ideal* and *weakly ideal*, respectively. Without loss of generality, one can assume that $\mathcal{S} = \mathcal{K}$, so that $F \colon \mathcal{R} \times \mathcal{P}^* \to \mathcal{K}$. Let $|\mathcal{K}| = q$. An ideal or weakly ideal (secret sharing) scheme is called *connected* if every participant $p \in \mathcal{P}$ is contained in some subset from its minimal access structure Γ_m. Brickell and Davenport [6] have studied canonic ideal and weakly ideal schemes, in which the conditional probability distributions are uniform and the distribution matrix has no repeated rows.

In order to outline the main results from [6], we need some basic notions from matroid theory, see [17]. A matroid $M = (E, \mathcal{E})$ is a finite set E and a collection $\mathcal{E}$ of subsets of E, called *independent* sets, such that (1) every subset of an independent set is independent and (2) for every $X \subseteq E$, every maximal independent subset of X has the same cardinality, called the *rank* of X (an empty set $\emptyset$ is considered independent and has rank zero). A *dependent* set of M is a subset of E that is not independent. A minimal dependent set is called a *circuit*, whereas a maximal independent set is called a *base*. A matroid is said to be *connected* if, for any two elements of E, there is a circuit containing both of them. A *loop* is a single element circuit.

The main effort of Brickell and Davenport was to prove [6, Proposition 1] that in any canonic connected weakly ideal scheme with q keys and $N \geq 2$ participants, for every $P \subseteq \mathcal{P}^*$, $\#P$ defined as $|F(\mathcal{R}, P)|$ is a positive integer power of q. As a consequence, they have then obtained two interesting properties: first [6, Theorem 3], that in such schemes every participant can be taken as a dealer and, second [6, Theorem 1], that $\rho(P) = \log_q \#P$, $P \subseteq \mathcal{P}^*$, together with $\rho(\emptyset) = 0$ defines a rank function of a connected matroid, which is called the *associated matroid* [16] and denoted by $M(F)$ (for canonic schemes, $\mathcal{F}$ reduces to F). The first property means that any subset of participants $P \subseteq \mathcal{P}^*$ is either independent or dependent where in independent subsets the participant shares are possibilistically independent according to condition (2′), and in dependent subsets the share of each participant is a function of the shares of the others according to condition (1). It then also follows [6, Theorem 1] that the independent/dependent sets of the associated matroid $M(F)$ coincide with the independent/dependent subsets of participants. Note that Proposition 1 of [6] easily follows if one initially assumes that a scheme, not necessarily connected, is weakly ideal with respect to each participant as a dealer, see [12]. So, the main result of [6] is in fact to prove that other connected weakly ideal schemes do not exist.

Another interesting result of Brickell and Davenport, again obtained as a consequence of Proposition 1 of [6], is Theorem 9 of [6] which shows that every canonic connected weakly ideal scheme is necessarily ideal with the same access structure, with respect to any participant as a dealer. This means that in independent subsets of participants the shares are not only possibilistically, but also probabilistically independent according to condition (2). Conditions (2) and (2′) are thus mutually equivalent for connected secret sharing schemes with information rate 1, with uniform conditional probability distributions, and with distinct rows of the distribution matrix. Let $H(D)$ denote the entropy of the dealer depending on the prior probability distribution of the keys, and let $H(P)$ denote the joint entropy of a subset of participants $P \subseteq \mathcal{P}^*$. Then in canonic connected ideal schemes $H(P)/H(D) = \log_q \#P$ is the rank function of the associated matroid, which is connected. It is interesting to note that this result also follows from polymatroidal properties of the entropy function corresponding to an ordered set of discrete random variables [9], under the assumption that a canonic scheme, not necessarily connected, is ideal with respect to each participant as a dealer.

Finally, for an arbitrary connected matroid M representable over a field with q elements, q being a prime power, Brickell and Davenport gave a construction of a canonic connected ideal scheme with q keys and the associated matroid M, see Theorem 2 of [6]. Martin [11] later showed how to construct the set of circuits of the associated matroid based on the access structure only, see also Lehman's result [17, Theorem 5.4.1], which means that the associated matroid does not depend on the particular ideal scheme realizing the access structure as long as the scheme is connected. If the collection of subsets of participants obtained by the construction [11] does not satisfy the circuit axioms [17], then (but not only then) the given access structure cannot be realized by any ideal scheme. By using graph-theoretic arguments, Seymour [12] proved that the well-known Vamos matroid on a set of eight elements cannot be associated with any ideal scheme.

3. General Ideal Schemes

The main results from [6] regarding the characterization of ideal secret sharing schemes can be interpreted by the following theorems. The theorems as such are actually not given in an explicit form in [6], but are easily derived in light of the discussion from the previous section. As we have already pointed out, the result contained in the following Theorem 1 [6] is actually the most difficult one to prove. Note that as far as weakly ideal schemes are concerned, the canonic property is in fact not necessary. Also, instead of connected weakly ideal schemes only, we more generally deal with schemes weakly ideal with respect to every participant as a dealer. Such schemes are composed of a number of distinct connected components. If a connected component consists of a single participant only, then such a participant is called *degenerate*.

Theorem 1 [6]. *A connected secret sharing scheme is weakly ideal with respect to any particular participant as a dealer if and only if it is weakly ideal with respect to every participant as a dealer.*

Theorem 2 [6]. *A secret sharing scheme with q keys is weakly ideal with respect to every participant as a dealer if and only if, for every $P \subseteq \mathcal{P}^*$, $|F(\mathcal{R}, P)| = q^{\rho(P)}$ where ρ is a nonnegative integer function. It then follows that ρ extended by $\rho(\emptyset) = 0$ is the rank function of a matroid on $\mathcal{P}^*$.* (*For a degenerate participant p, $\rho(p) = 0$ and hence p is a loop.*)

Theorem 3 [6]. *A canonic secret sharing scheme F is ideal with respect to any particular participant as a dealer if and only if it is weakly ideal with respect to the same participant as a dealer. The corresponding access structures are the same. Moreover, a canonic secret sharing scheme with q keys is ideal with respect to every participant as a dealer if and only if, for every $P \subseteq \mathcal{P}^*$ and each achievable vector value v of $F(r, P)$, $|\{r : r \in \mathcal{R}, F(r, P) = v\}| = q^{\rho'(P)}$ where ρ' is a nonnegative integer function.*

Theorem 4 [6], [11]. *Given a weakly ideal secret sharing scheme with a participant p_0 as a dealer, the set of circuits of the associated matroid containing p_0 is equal to $\{p_0 \cup P : P \in \Gamma_m\}$ where Γ_m is the the corresponding minimal access structure with respect to p_0. If the scheme is in addition connected, then the associated matroid is uniquely determined by Γ_m.*

Note that Theorems 1 [6], 2 [6], and 3 [6] directly imply that canonic ideal threshold schemes are equivalent to orthogonal arrays of index one. Our objective in this section is to obtain a more specific characteriziation of ideal secret sharing schemes with an arbitrary number q of keys. We first point out that every ideal, not necessarily canonic, scheme can be reduced to a canonic form.

Theorem 5. *Every ideal secret sharing scheme with any particular participant as a dealer can be transformed into a canonic ideal secret sharing scheme with the same participant as a dealer and with the same access structure. The transformation consists in reducing the repeated rows in the distribution matrix to the single ones and in assuming the uniform conditional probability distributions of the rows.*

Proof. Consider an arbitrary ideal secret sharing scheme $\mathcal{F} = (F, \{\pi_k\}_{k\in\mathcal{K}})$ where the distribution matrix F may have repeated rows and the conditional probability distributions $\{\pi_k\}_{k\in\mathcal{K}}$ are positive. From conditions (1), (2), and (2′) it then follows that $\mathcal{F}$ is weakly ideal too, with the same participant as a dealer and with the same access structure. The same holds for the transformed scheme as well. Since the transformed scheme is canonic, it is also ideal by Theorem 3 [6]. □

Theorem 5 means that canonic ideal schemes as introduced by Brickell and Davenport in [6] are essentially the most general ones as far as the access structure is concerned. Their distribution matrix F is characterized by Theorem 2 [6] or, more precisely, by Theorem 3 [6]. We now prove that one can be even more specific about the distribution matrix of such schemes using the notion of *balanced maximum-order correlation immune* functions [14]. A surjective function $f\colon \mathcal{A} \to \mathcal{B}$, where $\mathcal{A}$ and $\mathcal{B}$ are finite sets, is called balanced if every value from $\mathcal{B}$ is assumed an equal number of times by f. A balanced function $f\colon \mathcal{K}^m \to \mathcal{K}$ is called maximum-order correlation immune if it is balanced for each fixed value of every proper subset of its m input variables (it suffices to consider proper subsets of maximum cardinality only). Since the columns of the distribution matrix corresponding to degenerate participants in ideal schemes are single-valued, see Theorem 2 [6], without loss of generality we assume that the participants are all nondegenerate.

Theorem 6. *A canonic secret sharing scheme F with a set $\mathcal{K}$ of q keys and a set $\mathcal{P}^*$ of $N \geq 2$ nondegenerate participants is ideal with respect to every participant as a dealer if and only if for every $P \subseteq \mathcal{P}^*$ either the values of $F(r, P)$, $r \in \mathcal{R}$, are uniformly distributed over $\mathcal{K}^{|P|}$ or there exist a nonempty proper subset $P' \subset P$ and a participant $p \in P\backslash P'$ such that $F(\mathcal{R}, P') = \mathcal{K}^{|P'|}$ and that $F(r, p) = f(F(r, P'))$, $r \in \mathcal{R}$, where f is a balanced maximum-order correlation immune function over $\mathcal{K}^{|P'|}$.*

The total number of rows in F is then a positive integer power of q, whereas the subsets P such that $F(r, P)$ is uniformly distributed coincide with the independent sets of the associated matroid $M(F)$.

Proof. We first prove the necessity. From Theorem 2 [6] it follows that $|F(\mathcal{R}, P)| = q^t$ where t is the cardinality of maximal independent subsets of P, $P \subseteq \mathcal{P}^*$, and, in particular, $|F(\mathcal{R}, \mathcal{P}^*)| = q^n$ where n is the rank of the associated matroid $M(F)$. Moreover, from Theorem 3 [6] it follows that $|\{r : r \in \mathcal{R}, F(r, P) = v\}| = q^{n-t}$ for each achievable vector value v of $F(r, P)$. So, if P is an independent set in $M(F)$, then $t = |P|$ and $F(r, P)$ is uniformly distributed over $\mathcal{K}^{|P|}$.

On the other hand, if P is a dependent set in $M(F)$, then it contains a (minimal dependent set) circuit C of $M(F)$ as a subset, where $|C| \geq 2$ holds necessarily, because there are no degenerate participants. It then follows that $|F(\mathcal{R}, C)| = q^m$ where $m = |C| - 1$. For an arbitrary participant p in C, both p and $C \backslash p$ are independent, so that $|F(\mathcal{R}, C \backslash p)| = q^m$ and $|F(\mathcal{R}, p)| = q$. Also, each value of $F(r, C \backslash p)$ and each value of $F(r, p)$ appear exactly q^{n-m} and q^{n-1} times in the functions $F(r, C \backslash p)$ and $F(r, p)$, $r \in \mathcal{R}$, respectively. Since the share $F(r, p)$ is a function f of the shares $F(r, C \backslash p)$, $r \in \mathcal{R}$, for each value k of $F(r, p)$ there must be exactly q^{m-1} values of $F(r, C \backslash p)$ such that $f(F(r, C \backslash p)) = k$. Hence f is a balanced function $\mathcal{K}^m \to \mathcal{K}$.

If $m = 1$, then, trivially, f is maximum-order correlation immune too. If $m \geq 2$, then let p' be an arbitrary participant in $C \backslash p$. Since p and p' are arbitrary distinct participants in C, they can change places, and the above argument then shows that the share $F(r, p')$ is also a function of the shares $F(r, C \backslash p')$, $r \in \mathcal{R}$. Therefore, for any fixed value of $F(r, C \backslash p \backslash p')$, the value of $F(r, p')$ uniquely determines the value of $F(r, p)$ and vice versa. As p' is arbitrary, it follows that f achieves all q values for each fixed subset of $m - 1$ out of m input variables. Hence f is maximum-order correlation immune.

Assume now that the distribution matrix F of a canonic secret sharing scheme satisfies the required conditions. First note that the condition for a dependent set is clearly equivalent to a stronger one that there exists a subset $P' \subseteq P$, $|P'| \geq 2$, such that, for each $p \in P'$, $F(\mathcal{R}, P' \backslash p) = \mathcal{K}^{|P'|-1}$ and that $F(r, p) = f(F(r, P' \backslash p))$, $r \in \mathcal{R}$, where f is a balanced maximum-order correlation immune function over $\mathcal{K}^{|P'|-1}$. In fact, this is why balanced maximum-order correlation immunity is required. If the values of $F(r, P)$ are uniformly distributed, then call a subset $P \subseteq \mathcal{P}^*$ independent, and if not, then call it dependent. It follows that every subset of an independent set is independent. Accordingly, if P is independent, then $|F(\mathcal{R}, P)| = q^{|P|}$. We now show that, for any dependent P, $|F(\mathcal{R}, P)|$ is also a positive integer power of q. Namely, if P is dependent, then consider any maximal independent subset $\hat{P}$ of P and any participant $p \in P \backslash \hat{P}$. By the assumed maximality of $\hat{P}$, the set $\hat{P} \cup p$ must be dependent. Since $\hat{P}$ itself is independent, it follows that there exists a subset $P' \subseteq \hat{P}$ such that $F(r, p)$ is a function of $F(r, P')$, $r \in \mathcal{R}$. Hence $F(r, p)$ is a function of $F(r, \hat{P})$ too. Therefore, $|F(\mathcal{R}, \hat{P} \cup p)| = q^{|\hat{P}|}$. Furthermore, since p is an arbitrary participant from $P \backslash \hat{P}$, we also have that $|F(\mathcal{R}, P)| = q^{|\hat{P}|}$. Theorem 2 [6] then implies that the secret sharing scheme is weakly ideal. Since the scheme is canonic, Theorem 3 [6] yields that it is ideal too.

The last part of the theorem follows trivially. □

Let $\mathcal{M}_{q,N}$ denote the class of matroids associated with ideal secret sharing schemes with q keys and N participants including the dealer. If a scheme is connected, then the associated matroid is connected too. If a scheme does not have degenerate participants, then the associated matroid has no loops. Theorem 6 shows that for any particular q, the structure of $\mathcal{M}_{q,N}$ is determined by q-ary balanced maximum-order correlation immune functions. According to the construction from [6] it follows that, for q a prime power, $\mathcal{M}_{q,N}$ contains all the matroids representable over a field (nearfield) with q elements.

In the next section we prove that in the binary case, $q = 2$, $\mathcal{M}_{2,N}$ is exactly the class of matroids representable over the binary field.

4. Binary Ideal Schemes

In this section we consider ideal secret sharing schemes with $q = |\mathcal{K}| = |\mathcal{S}| = 2$ keys, which we call binary ideal schemes. Recall [17] that a matroid M on E is called representable over a field F if there exists a rank-preserving function (not necessarily an injection) φ: $E \to V$ where V is a vector space over F. In particular, a matroid M is binary if it is representable over the binary field GF(2). There are many equivalent characterizations of binary matroids, see [17]. For example, we use the following circuit characterization: a collection $\mathcal{C}$ of nonempty subsets of a finite set E is the set of circuits of a binary matroid on E if and only if for every two distinct members of $\mathcal{C}$, C_1 and C_2, it is true that $C_1 \not\subseteq C_2$ and that the symmetric difference $C_1 \Delta C_2$ contains a member C of $\mathcal{C}$. Equivalently, a collection $\mathcal{C}$ of nonempty subsets of E is the set of circuits of a binary matroid on E if and only if the members of $\mathcal{C}$ are minimal and the symmetric difference of any collection of distinct members of $\mathcal{C}$ is the union of disjoint members of $\mathcal{C}$, see [17]. Combining this characterization with the fact proved in [14] that the only maximum-order correlation immune and balanced boolean functions are nonconstant affine functions, and also using the construction [6] of canonic ideal schemes whose associated matroids are representable over a field, we now prove that $\mathcal{M}_{2,N}$ is the class of binary matroids.

Theorem 7. *A matroid is the associated matroid for a binary ideal secret sharing scheme if and only if it is representable over the binary field.*

Proof. If a matroid M is binary, then the construction from the proof of Theorem 2 of [6] described at the end of this section gives a canonic ideal scheme whose associated matroid is M. Conversely, let F be the distribution matrix of a canonic ideal scheme and let $M(F)$ be the associated matroid. By Theorem 6, for any circuit C of $M(F)$ such that $|C| = m \geq 2$ there exists a balanced maximum-order correlation immune boolean function f: $\{0, 1\}^m \to \{0, 1\}$ such that $f(F(r, C)) = 0$ for every $r \in \mathcal{R}$. Siegenthaler [14] has proved that the only balanced maximum-order correlation immune boolean functions are nonconstant affine functions in GF(2), that is, every such function f: $\{0, 1\}^m \to \{0, 1\}$ has the algebraic normal form $f(x_1, \ldots, x_m) = c + \sum_{i=1}^{m} x_i$, where the addition is modulo 2 and c is a binary constant. Consequently, if C_1 and C_2 are any two distinct circuits of $M(F)$ whose cardinalities are both greater than 1, then there exist binary constants c_1 and c_2 such that

$$c_1 + \sum_{p \in C_1} F(r, p) = c_2 + \sum_{p \in C_2} F(r, p) = 0, \qquad r \in \mathcal{R}. \tag{1}$$

Since the common variables in (1) cancel out, we have

$$c_1 + c_2 + \sum_{p \in C_1 \Delta C_2} F(r, p) = 0, \qquad r \in \mathcal{R}. \tag{2}$$

By Theorem 6 we then get that $C_1 \Delta C_2$ is a dependent set of $M(F)$ and hence must contain a circuit of $M(F)$ as a subset. On the other hand, if at least one of the circuits C_1 and C_2 is a loop (of cardinality 1), then their symmetric difference clearly contains this loop as a subset. The circuit characterization of binary matroids then yields that $M(F)$ is binary. □

Our next objective is to characterize the access structures achievable by connected binary ideal schemes. A direct consequence of Theorems 4 [6], [11] and 7 is the following implicit characterization of the achievable minimal access structures.

Lemma 1. *Let $\mathcal{P}^* = \mathcal{P} \cup p_0$ be a set of participants where $p_0 \notin \mathcal{P}$. A minimal collection Γ_m of subsets of $\mathcal{P}$ is the minimal access structure of a connected binary ideal secret sharing scheme with p_0 as a dealer if and only if a connected binary matroid on $\mathcal{P}^*$ exists whose set of circuits containing p_0 is given as $\{p_0 \cup A : A \in \Gamma_m\}$.*

In order to derive an explicit characterization of the achievable minimal access structures, we need an additional lemma about the binary matroids.

Lemma 2. *Let M be a connected binary matroid on a finite set E and let x be an arbitrary element of E. Let $\mathcal{C}$ denote the set of circuits of M and let $\mathcal{C}_x$ denote the set of circuits of M containing x. Then $\mathcal{C} \backslash \mathcal{C}_x$ is equal to the set $\Delta(\mathcal{C}_x)$ of minimal elements of the collection $\{C_1 \Delta C_2 : C_1, C_2 \in \mathcal{C}_x, C_1 \neq C_2\}$.*

Proof. Since no element of $\Delta(\mathcal{C}_x)$ contains x and, due to the circuit characterization of binary matroids, every element of $\Delta(\mathcal{C}_x)$ contains a circuit of M, it follows that every element of $\Delta(\mathcal{C}_x)$ belongs to $\mathcal{C} \backslash \mathcal{C}_x$.

On the other hand, suppose that C is any circuit from $\mathcal{C} \backslash \mathcal{C}_x$. Since M is connected, there exists a circuit of M containing both x and any element of C, that is, a circuit C_1 from $\mathcal{C}_x$ that has a nonempty intersection with C. Choose any C_1 so that $C \cup C_1$ is minimal over all such C_1. According to the circuit characterization of binary matroids, the symmetric difference of any set of distinct circuits is the union of disjoint circuits. As both C and C_1 are circuits, their symmetric difference $C \Delta C_1$ then contains a circuit C_2 from $\mathcal{C}_x$. Since $C_2 \nsubseteq C_1$, it follows that $C_2 \cap C \neq \emptyset$. Now, suppose that C_2 is a proper subset of $C \Delta C_1$. Then C_2 is also a proper subset of $C \cup C_1$ and hence $C \cup C_1$ is not minimal. Thus, C_2 must be equal to $C \Delta C_1$. This means that $C = C_1 \Delta C_2$, where both C_1 and C_2 belong to $\mathcal{C}_x$. Equivalently, every circuit from $\mathcal{C} \backslash \mathcal{C}_x$ is an element of $\Delta(\mathcal{C}_x)$. □

The desired explicit characterization of the minimal access structures achievable by connected binary ideal schemes is then given by the following theorem.

Theorem 8. *Let $\mathcal{P}^* = \mathcal{P} \cup p_0$ be a set of participants where $p_0 \notin \mathcal{P}$ and let Γ_m be a minimal collection of subsets of $\mathcal{P}$ whose union is equal to $\mathcal{P}$. Let $\Delta(\Gamma_m)$ denote the set of minimal elements of the collection $\{A_1 \Delta A_2 : A_1, A_2 \in \Gamma_m, A_1 \neq A_2\}$. Further, let Γ'_m and Γ''_m denote the sets of minimal elements of the collections $\{A_1 \Delta A_2 : A_1 \in \Delta(\Gamma_m), A_2 \in \Gamma_m, A_1 \neq A_2\}$ and $\{A_1 \Delta A_2 : A_1, A_2 \in \Delta(\Gamma_m), A_1 \neq A_2\}$, respectively.*

Then Γ_m is the minimal access structure of a connected binary ideal secret sharing scheme with p_0 as a dealer if and only if a connected binary matroid on $\mathcal{P}^*$ exists whose set of circuits is given as $\mathcal{C}(\Gamma_m) = \Delta(\Gamma_m) \cup \{p_0 \cup A : A \in \Gamma_m\}$. Such a matroid exists if and only if:

(1°) *no element of $\Delta(\Gamma_m)$ is contained in any element of Γ_m,*
(2°) *for every element of Γ'_m there exists an element of Γ_m or $\Delta(\Gamma_m)$ contained in it, and*
(3°) *for every element of Γ''_m there exists an element of $\Delta(\Gamma_m)$ contained in it.*

Proof. The first part of the theorem is a direct consequence of Lemmas 1 and 2 combined. As for the second part, the required matroid exists if and only if the collection $\mathcal{C}(\Gamma_m)$ is minimal and the symmetric difference of every two distinct elements of $\mathcal{C}(\Gamma_m)$ contains an element of $\mathcal{C}(\Gamma_m)$. Since no element of $\{p_0 \cup A : A \in \Gamma_m\}$ is contained in any element of $\Delta(\Gamma_m)$, the collection $\mathcal{C}(\Gamma_m)$ is minimal if and only if condition (1°) is satisfied. Now, by the definition of $\Delta(\Gamma_m)$, the symmetric difference of every two distinct elements of $\{p_0 \cup A : A \in \Gamma_m\}$ contains an element of $\Delta(\Gamma_m)$. It then remains to check the mutual symmetric differences of elements of $\Delta(\Gamma_m)$ and $\{p_0 \cup A : A \in \Gamma_m\}$, respectively, and the symmetric differences of distinct elements of $\Delta(\Gamma_m)$. Clearly, the symmetric difference of any element of $\{p_0 \cup A : A \in \Gamma_m\}$ and any element of $\Delta(\Gamma_m)$ contains an element of $\mathcal{C}(\Gamma_m)$ if and only if condition (2°) is true. Similarly, the symmetric difference of any two distinct elements of $\Delta(\Gamma_m)$ contains an element of $\mathcal{C}(\Gamma_m)$ if and only if condition (3°) is satisfied. □

The achievability conditions from Theorem 8 can be checked in computational time quadratic in the cardinality of Γ_m. Moreover, any minimal collection Γ_m can in principle be iteratively modified by removing or adding certain elements so that conditions (1°), (2°), and (3°) be gradually met. If Γ_m is achievable, then it suffices to check the symmetric differences of no more than four distinct elements of Γ_m. If Γ_m has to be modified, then higher order symmetric differences have to be tested as well. For an achievable Γ_m, Theorem 8 specifies a way of determining the set of circuits of the connected binary matroid associated with a binary ideal scheme that can realize Γ_m. The scheme itself can then be constructed by first deriving a standard representation of the associated binary matroid from the set of its circuits and then by using the construction from [6]. More precisely, a standard representation of the binary matroid M on $\mathcal{P}^*$ with $\mathcal{C}(\Gamma_m)$ as the set of its circuits is obtained by the technique described in [17]. Starting from $\mathcal{C}(\Gamma_m)$ first find a base $B = \{b_1, \ldots, b_n\}$ of M such that $b_1 = p_0$, where n is the rank of M, which is easy. Let $\mathcal{P}^* \backslash B = \{e_1, \ldots, e_m\}$, $n + m = |\mathcal{P}| + 1$, and let C_j be the fundamental circuit of e_j in the base B, that is, the unique circuit such that $e_j \in C_j \subset B \cup e_j$, see [17]. Then a standard representation of M over GF(2) is given by the columns of the binary matrix

$$\begin{array}{cc} b_1 \cdots b_n & e_1 \cdots e_m \\ A' = [\quad I_n & A \quad], \end{array} \tag{3}$$

where I_n is the identity matrix of dimensions $n \times n$ and $A = [A_{ij}]_{n,m}$ with $A_{ij} = 1$ if b_i belongs to C_j and $A_{ij} = 0$ otherwise.

So, the columns of A' define an ordered set of binary vectors of dimension n, $\{\varphi(p)\}_{p\in\mathcal{P}^*}$. According to [6], the corresponding canonic binary ideal scheme is then defined by $F(r, p) = r \cdot \varphi(p)$, $p \in \mathcal{P}^*$, $r \in \mathrm{GF}(2)^n$, where "·" denotes the dot product. Let $r = (r_1, \ldots, r_n)$, where $r_1 = k$ is the secret bit to be shared. When the dealer $p_0 = b_1$ wants to distribute shares corresponding to a secret bit k, he first picks $r_1 = k$ at random according to a prior probability distribution, chooses uniformly at random the binary vector $(r_2, \ldots, r_n)$, and then distributes the share $r \cdot \varphi(p)$ to a participant p, for every $p \in \mathcal{P}$.

5. Conclusion

In this paper we continue the study of Brickell and Davenport [6] and Martin [11] regarding the matroid characterization of connected ideal secret sharing schemes. We first provide some additional insight into the results from [6] and then obtain a characterization of ideal schemes with an arbitrary number q of keys in terms of q-ary balanced maximum-order correlation immune functions. For $q = 2$, we prove that a necessary and sufficient condition for a matroid to be associated with such a scheme is that it is representable over the binary field. We also derive a characterization of the access structures achievable by connected binary ideal schemes and describe an efficient method for their construction. Clearly, the same access structures are also achievable by connected ideal schemes with $q = 2^n$ keys.

An interesting open problem is to extend our results regarding the matroid and access structure characterizations as well as the construction of binary ideal schemes to ideal schemes with an arbitrary number q of keys. A possible way of approaching this problem is by studying the properties of balanced maximum-order correlation immune functions over arbitrary finite sets. The structure of the associated matroids is expected to be constrained by such properties, which is in accordance with the intriguing Seymour's result [12] that there exists a matroid (Vamos) that cannot be associated with any ideal scheme. We believe that the reason for this is in the strict definitions of the information rate and the entropy structure of ideal schemes. So, we make the following:

Conjecture. *Let ρ be the rank function of an arbitrary matroid on a set of participants $\mathcal{P}^*$ such that $\rho(p) = 1$, $p \in \mathcal{P}^*$ (nondegenerate participants). Then, for every $\varepsilon > 0$, there exists a canonic secret sharing scheme F on $\mathcal{P}^*$ such that, for any participant $p \in \mathcal{P}^*$, $|H(P)/H(p) - \rho(P)| < \varepsilon$ for every $P \subseteq \mathcal{P}^*$, where H is the entropy operator.*

Acknowledgment

The author is grateful to an anonymous referee for helpful comments.

References

[1] A. Beimel and B. Chor, Universally ideal secret sharing schemes, *Advances in Cryptology - Crypto '92*, Lecture Notes in Computer Science, vol. 740, E. F. Brickell, ed., Springer-Verlag, Berlin, 1993, pp. 183–195.

[2] J. Benaloh and J. Leichter, Generalized secret sharing and monotone functions, *Advances in Cryptology - Crypto* '88, Lecture Notes in Computer Science, vol. 403, S. Goldwasser, ed., Springer-Verlag, Berlin, 1990, pp. 27–35.

[3] G. R. Blakley, Safeguarding cryptographic keys, *Proc. AFIPS* 1979, NCC, vol. 48, New York, 1979, pp. 313–317.

[4] C. Blundo, A. De Santis, D. P. Stinson, and U. Vaccaro, Graph decompositions and secret sharing schemes, *J. Cryptology*, vol. 8 (1995), pp. 39–64.

[5] E. F. Brickell, Some ideal secret sharing schemes, *J. Combin. Math. Combin. Comput.*, vol. 6 (1989), pp. 105–113.

[6] E. F. Brickell and D. M. Davenport, On the classification of ideal secret sharing schemes, *J. Cryptology*, vol. 4 (1991), pp. 123–134.

[7] E. F. Brickell and D. R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, *J. Cryptology*, vol. 5 (1992), pp. 153–166.

[8] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, On the size of shares for secret sharing schemes, *J. Cryptology*, vol. 6 (1993), pp. 157–168.

[9] S. Fujishige, Polymatroidal dependence structure of a set of random variables, *Inform. and Control*, vol. 39 (1978), pp. 55–72.

[10] M. Ito, A. Saito, and T. Nishizeki, Secret sharing scheme realizing general access structure, *Proc. IEEE Globecom* '87, Tokyo, 1987, pp. 99–102.

[11] K. M. Martin, Discrete Structures in the Theory of Secret Sharing, Ph.D. thesis, University of London, 1991.

[12] P. D. Seymour, On secret-sharing matroids, *J. Combin. Theory Ser. B*, vol. 56 (1992), pp. 69–73.

[13] A. Shamir, How to share a secret, *Comm. ACM*, vol. 22 (1979), pp. 612–613.

[14] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, *IEEE Trans. Inform. Theory*, vol. 30 (1984), pp. 776–780.

[15] G. J. Simmons, An introduction to shared secret and/or shared control schemes and their applications, *Contemporary Cryptology*: *the Science of Information Integrity*, G. J. Simmons, ed., IEEE Press, New York, 1992, pp. 441–497.

[16] D. R. Stinson, An explication of secret sharing schemes, *Designs, Codes and Cryptography*, vol. 2 (1992), pp. 357–390.

[17] D. J. A. Welsh, *Matroid Theory*, Academic Press, London, 1976.