Linear Threshold Multisecret Sharing Schemes[☆]

Oriol Farràs[a], Ignacio Gracia[b], Sebastià Martín[b], Carles Padró[c]

[a]*Dept. d'Eng. Informàtica i Matemàtiques, Universitat Rovira i Virgili, Tarragona, Spain*
[b]*Dept. de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya, Barcelona, Spain*
[c]*School of Mathematical Sciences, Nanyang Technological University, Singapore*

Abstract

In a multisecret sharing scheme, several secret values are distributed among a set of n users, and each secret may have a different associated access structure. We consider here information-theoretic secure schemes with multithreshold access structures. Namely, for every subset P of k users there is a secret key that can only be computed when at least t of them put together their secret information. Coalitions with at most w users with less than t of them in P cannot obtain any information about the secret associated to P. The main parameters to optimize are the length of the shares and the amount of random bits that are needed to set up the distribution of shares, both in relation to the length of the secret. In this paper, we provide lower bounds on this parameters. Moreover, we present an optimal construction for $t = 2$ and $k = 3$.

Keywords: cryptography, information-theoretic security, multisecret sharing schemes, threshold access structures.

1. Introduction

There are several different kinds of cryptographic protocols with information-theoretic security that have some common features. Namely, they can be described as collections of random variables satisfying certain properties, which in general can be stated in terms of their joint Shannon entropies. Secret sharing schemes form the best known class of such protocols, and also the one that has been most extensively studied. Other examples are key predistribution schemes, broadcast encryption schemes, and multisecret sharing schemes.

In a *secret sharing scheme* some secret value is distributed into shares among a set of users in such a way that only the *authorized sets* of users can reconstruct the secret from their shares, while the participants in a *forbidden set* cannot obtain any information at all about the secret value. The family of the authorized sets together with the family of the forbidden sets form the *access structure* of the secret sharing scheme. In a *multisecret sharing scheme* several secret values are distributed, every one of them with a different access structure. In this paper, only *threshold multisecret sharing schemes*, that is, those having a *multithreshold access structure*, are considered. In such a scheme, the distributed secrets are in one-to-one correspondence with the sets of k-out-of-n users. The qualified sets for the secret corresponding to a set P are those with at least t users in P, while every set with at most w users with less than t of them in P is forbidden. Observe that the particular case $k = n$ correspond to the threshold secret sharing schemes introduced by Shamir [19] and Blakley [2], while the case $t = 1$ correspond to the key predistribution schemes considered in [3, 4].

The length of the shares and the amount of required randomness, in relation to the length of the secret values, are usually considered as a measure for the efficiency of multisecret sharing schemes. These

[☆]A preliminary version of this paper appeared in the *Proceedings of the Fourth International Conference on Information Theoretic Security, ICITS 2009*, and it was published in its proceedings, *Lecture Notes in Comput. Sci.* **5973** (2010) 110–126. The authors' work was partially supported by the Spanish Ministry of Education and Science under projects TSI2006-02731 and MTM2009-07694. The first author's work was partially supported by the Spanish Government through projects TIN201127076-C03-01 and Consolider Ingenio 2010 CSD2007-00004, and by the Government of Catalonia under Grant 2009 SGR 1135. The fourth author's work was partially supported by the Singapore National Research Foundation under Research Grant NRF-CRP2-2007-03.
Email addresses: oriol.farras@urv.cat, ignacio@ma4.upc.edu, sebasm@ma4.upc.edu, carlespl@ntu.edu.sg.

parameters are called, respectively, *information ratio* and *randomness*. Their optimization for threshold multisecret sharing schemes is the problem considered in this paper.

General lower bounds for the information ratio of threshold multisecret sharing schemes were given in [12, 16]. The threshold secret sharing schemes from [2, 19] attain the lower bound for the particular case $k = n$ and $w = t - 1$. The same applies to the key predistribution schemes from [4] for the case $t = 1$. Optimal constructions have been presented as well for the cases $t = 2$ and $w = n - k + 1$ [13], and $t = 2$, $k = 3$ and $1 \leq w \leq n - 2$ [1]. The existence of optimal threshold multisecret sharing schemes for other values of the parameters (w, t, k, n) is unknown.

In this paper we apply to multisecret sharing schemes two techniques that have been developed for secret sharing and, in a lesser degree, also for key predistribution schemes and broadcast encryption schemes. First, the use of polymatroids, which is derived from the fact that the joint Shannon entropies of a collection of random variables define a polymatroid [9, 10] The reader is referred to [15] and its references for more information about the use of polymatroids in secret sharing. And second, the use of constructions based on linear algebra, in which the involved random variables are defined by linear maps. Linear secret sharing schemes have been extensively studied since its introduction by Karnin, Greene, and Hellman [14] and Brickell [6]. In a similar development as in secret sharing, linear and multilinear algebra have been used to construct key predistribution schemes [17] and broadcast encryption schemes [18].

By using polymatroids, we present a new general lower bound for the randomness of threshold multisecret sharing schemes, and also a new proof for the lower bound on the information ratio that was given in [12]. By using similar linear algebra techniques as in [17], we present a linear construction of optimal threshold multisecret sharing schemes for the case $t = 2$, $k = 3$ and $1 \leq w \leq n - 2$. An optimal construction for this case was previously presented in [1]. Nevertheless our construction is much simpler, and the proof is shorter. Finally, in Section 6, we present a general construction of multithreshold schemes for all possible values of the parameters (w, t, k, n). In general, these are not optimal schemes, but it is the best known general construction.

2. The Tools

2.1. Shannon Entropies and Polymatroids

Given a finite collection of random variables $(S_i)_{i \in Q}$ and a subset $A = \{i_1, \ldots, i_r\} \subseteq Q$, we use S_A to denote the random variable $S_{i_1} \times \cdots \times S_{i_r}$, and $H(S_A)$ will denote its Shannon entropy. The reader is referred to [7] for more information about Shannon entropy, but all properties that are used in the paper are presented in the following.

For every positive real number $c > 0$, the mapping $h \colon 2^Q \to \mathbb{R}$ defined by $h(A) = cH(S_A)$ satisfies the following properties.

- $h(\emptyset) = 0$.
- h is *monotone increasing*: if $A \subseteq B \subseteq Q$, then $h(A) \leq h(B)$.
- h is *submodular*: $h(A \cup B) + h(A \cap B) \leq h(A) + h(B)$ for every $A, B \subseteq Q$.

That is, h is the *rank function* of a *polymatroid* with *ground set* Q. This connection between Shannon entropy and polymatroids was found out by Fujishige [9, 10]. By analogy to the conditional entropy, we use the notation $h(A|B) = h(A \cup B) - h(B)$. Clearly,

$$h(A_1 \cup \cdots \cup A_r) = \sum_{i=1}^{r} h(A_i | A_1 \cup \cdots \cup A_{i-1}). \tag{1}$$

In particular, submodularity implies that $h(X|Y) \geq h(X|Y \cup Z)$ for all $X, Y, Z \subseteq Q$.

Lemma 2.1. *The following properties are satisfied for every $X, Y, Z \subseteq Q$.*

1. *If $h(Y|Z) = 0$, then $h(X|Z) = h(X|Y \cup Z)$.*
2. *If $h(X|Y) = h(X)$ and $h(X|Y \cup Z) = 0$, then $h(Z) \geq h(X)$.*

Proof. The first property is a consequence of the equality $h(Y|Z) + h(X|Y \cup Z) = h(X|Z) + h(Y|X \cup Z)$, which is itself derived from (1). For the second property we use that $h(Z) + h(Y|Z) + h(X|Y \cup Z) = h(Y) + h(X|Y) + h(Z|X \cup Y)$, and hence $h(Z) = h(X) + h(Z|X \cup Y) + h(Y) - h(Y|Z) \geq h(X)$. □

2.2. Linear Random Variables

Consider a finite field $\mathbb{K}$, a $\mathbb{K}$-vector space E with finite dimension and a finite family of $\mathbb{K}$-linear maps $(\phi_i)_{i\in Q}$, where $\phi_i\colon E \to E_i$. These linear maps define a family of random variables $(S_i)_{i\in Q}$ by taking the uniform probability distribution on E. A family of random variables that can be defined in this way is said to be $\mathbb{K}$-*linear*. For every $A \subseteq U$, consider the linear map $\phi_A\colon E \to \prod_{i\in A} E_i$ defined by $\phi_A(x) = (\phi_i(x))_{i\in A}$. Then it is clear that $H(S_A) = \log|\mathbb{K}| \cdot \operatorname{rank}\phi_A$. Take $h(A) = H(S_A)/\log|\mathbb{K}| = \operatorname{rank}\phi_A = \dim E - \dim\ker\phi_A$.

Lemma 2.2. *For every $A, B \subseteq Q$,*

1. *$h(A|B) = 0$ if and only if $\ker\phi_B \subseteq \ker\phi_A$,*
2. *$h(A|B) = h(A)$ if and only if $\ker\phi_A + \ker\phi_B = E$.*

Proof. Observe that $\ker\phi_{A\cup B} = \ker\phi_A \cap \ker\phi_B$, and hence $h(A|B) = h(A\cup B) - h(B) = \dim\ker\phi_B - \dim(\ker\phi_A \cap \ker\phi_B)$. Therefore, $h(A|B) = 0$ if and only if $\ker\phi_B \subseteq \ker\phi_A$, and $h(A|B) = h(A)$ if and only if $\dim E = \dim\ker\phi_A + \dim\ker\phi_B - \dim(\ker\phi_A \cap \ker\phi_B) = \dim(\ker\phi_A + \ker\phi_B)$. □

2.3. Multilinear Algebra

Given a vector space E with finite dimension over a field $\mathbb{K}$, the *dual space* E^* is the set of the *linear forms* on E, that is, the linear maps from E to $\mathbb{K}$. Clearly, E^* is a vector space over $\mathbb{K}$. Moreover, $\dim E = \dim E^*$ if E has finite dimension. For a vector subspace $F \subseteq E$, the *orthogonal subspace* $F^\perp \subseteq E^*$ is given by $F^\perp = \{\alpha \in E^* : \alpha(v) = 0 \text{ for every } v \in F\}$.

An *r-linear form* on E is a map from E^r to $\mathbb{K}$ that is separately linear in each variable. A multilinear form $T\colon E^r \to \mathbb{K}$ is said to be *symmetric* if it is invariant under permutation of its variables, that is, $T(v_1,\ldots,v_r) = T(v_{\sigma 1},\ldots,v_{\sigma r})$ for every permutation σ on $\{1,\ldots,r\}$ and for every $(v_1,\ldots,v_r) \in E^r$. The set $S_r(E)$ of the symmetric r-linear forms on E is a $\mathbb{K}$-vector space with dimension $\binom{m+r-1}{r}$, where $\dim E = m$.

Finally, we need the following technical result, which can be seen as a variant of the Schwartz-Zippel Lemma. A proof for it can be found in [8, Lemma 6.2].

Lemma 2.3. *Let $p \in \mathbb{K}[X_1,\ldots,X_N]$ be a nonzero polynomial on N variables of degree at most $d < |\mathbb{K}|$ on each variable. Then, there exists $(x_1,\ldots,x_N)$ in $\mathbb{K}^N$ such that $p(x_1,\ldots,x_N) \neq 0$.*

3. Multisecret Sharing Schemes

Before formally defining multisecret sharing schemes, we introduce, following [12], some nomenclature and notation for their access structures. In a multisecret sharing scheme a number of secret values, which are indexed by a finite set $\mathcal{J}$, are distributed into shares among a set U of users. For every $j \in \mathcal{J}$, consider the families Γ_j and Δ_j of, respectively, the authorized and forbidden sets of users for the corresponding secret value. Naturally, Γ_j is monotone increasing, Δ_j is monotone decreasing and $\Gamma_j \cap \Delta_j = \emptyset$ for every $j \in \mathcal{J}$. The tuple $(\Gamma_j, \Delta_j)_{j\in\mathcal{J}}$ is called the *access structure* of the multisecret sharing scheme. Such an access structure is said to be *complete* if $\Gamma_j \cup \Delta_j = 2^U$ for every $j \in \mathcal{J}$.

A *multisecret sharing scheme* $\Sigma = ((K_j)_{j\in\mathcal{J}}, (S_i)_{i\in U})$ consists of two collections of random variables. The random variables $(K_j)_{j\in\mathcal{J}}$ correspond to the secret values. The elements in U are the *users* of the scheme and the random variables $(S_i)_{i\in U}$ correspond to the *shares*. Given a positive constant $c > 0$, consider the polymatroid with ground set $Q = \mathcal{J} \cup U$ and rank function h defined by $h(X) = c\,H((K_j)_{j\in X\cap\mathcal{J}}, (S_i)_{i\in X\cap U}) = c\,H(K_{X\cap\mathcal{J}}, S_{X\cap U})$ for every $X \subseteq Q$. We say that the multisecret sharing scheme Σ has access structure $(\Gamma_j, \Delta_j)_{j\in\mathcal{J}}$ if the following conditions are satisfied.

1. If $A \subseteq U$ is in Γ_j, then $h(\{j\}|A) = 0$.
2. If $B \subseteq U$ is in Δ_j, then $h(\{j\}|B) = h(\{j\})$.

By the first condition, the secret value K_j can be recovered from the shares of the users in a qualified set $A \in \Gamma_j$. By the second condition, the users in a forbidden set $B \in \Delta_j$ cannot obtain any information about the value of K_j. Observe that, with this definition, we require the schemes to have information-theoretic security.

The efficiency of a multisecret sharing scheme is usually measured by the length of the shares and the total number of random bits required to distribute the shares, both in relation to the length of the secret values. Specifically, the *information ratio* σ and the *randomness* σ_T of a multisecret sharing scheme are defined by

$$\sigma = \frac{\max_{i\in U} h(\{i\})}{\min_{j\in\mathcal{J}} h(\{j\})}, \qquad \sigma_T = \frac{h(\mathcal{J}\cup U)}{\min_{j\in\mathcal{J}} h(\{j\})}.$$

For a finite field $\mathbb{K}$, a multisecret sharing scheme Σ is said to be $\mathbb{K}$-*linear* if the family of random variables $((K_j)_{j\in\mathcal{J}}, (S_i)_{i\in U})$ is $\mathbb{K}$-linear, that is, these random variables are defined by $\mathbb{K}$-linear maps $(\pi_j)_{j\in\mathcal{J}}$ and $(\phi_i)_{i\in U}$, respectively, defined on a $\mathbb{K}$-vector space E. Because of Lemma 2.2, such a collection of linear random variables defines a linear multisecret sharing scheme if and only if the following conditions are satisfied.

1. If $A \in \Gamma_j$, then $\ker\phi_A \subseteq \ker\pi_j$.
2. If $B \in \Delta_j$, then $\ker\phi_B + \ker\pi_j = E$.

Moreover, the information ratio and the randomness are in this case

$$\sigma = \frac{\max_{i\in U} \operatorname{rank}\phi_i}{\min_{j\in\mathcal{J}} \operatorname{rank}\pi_j}, \qquad \sigma_T = \frac{\dim E}{\min_{j\in\mathcal{J}} \operatorname{rank}\pi_j}.$$

In this paper, we focus on *threshold multisecret sharing schemes*, or *multithreshold schemes* for short, which are the ones having a *threshold access structure*. Such an access structure is determined by four positive integers w, t, k and n such that

- $1 \le t \le k \le n$ and
- $t-1 \le w \le n-k+t-1$.

Secret values are in one-to-one correspondence with the k subsets of a set U of n users, that is,

$$\mathcal{J} = \{P \subseteq U \,:\, |P| = k\}.$$

The qualified and forbidden sets corresponding to $P \in \mathcal{J}$ are determined in terms of the total number of elements and the number of elements in P. Specifically,

$$\Gamma_P = \{A \subseteq U : |A\cap P| \ge t\} \text{ and } \Delta_P = \{B \subseteq U : |B| \le w, |B\cap P| \le t-1\}.$$

A scheme with this access structure is called a *w-secure (t,k,n)-multithreshold sharing scheme*. Observe that a threshold access structure is complete if and only if $w = n-k+t-1$. In this situation we have a *complete (t,k,n)-multithreshold sharing scheme*. If a multithreshold scheme is complete, for every $P \in \mathcal{J}$ and $B \subseteq U$ with $|B\cap P| < t$, the subset B is in Δ_P. The particular cases $k = n$ and $t = 1$ correspond, respectively, to secret sharing schemes and key predistribution schemes.

The problem that we consider in this work is to optimize the information ratio and the randomness of multithreshold sharing schemes. Given integers w, t, k, n in the above conditions, we define $\sigma(w,t,k,n)$ as the infimum of the information rates of all w-secure (t,k,n)-multithreshold schemes, and $\sigma_T(w,t,k,n)$ is defined analogously. Then the problem we consider here is to determine the values of $\sigma(w,t,k,n)$ and $\sigma_T(w,t,k,n)$ for all possible values of the parameters w,t,k,n. Due to the symmetry of the access structure, it is easy to see that the search of optimal schemes can be restricted to the ones with $h(j_1) = h(j_2)$ for all $j_1, j_2 \in \mathcal{J}$ and $h(i_1) = h(i_2)$ for all $i_1, i_2 \in U$.

4. Lower Bounds on the Information Ratio and Randomness

This section is devoted to prove Theorem 4.1, which provides lower bounds on the information ratio and randomness of multithreshold schemes. The proof uses the technical results presented in Section 2.1. The lower bound on $\sigma(w,t,k,n)$ was given in [12, Theorem 5] with another proof. No lower bound on $\sigma_T(w,t,k,n)$ was previously known.

Theorem 4.1. *The following lower bounds for the optimal information ratio and the optimal randomness of multithreshold sharing schemes apply for every positive integers w,t,k,n with $1 \le t \le k \le n$ and $t-1 \le w \le n-k+t-1$.*

- $\sigma(w,t,k,n) \geq \binom{w+k-2t+1}{k-t}$.
- $\sigma_T(w,t,k,n) \geq \binom{w+k-2t+2}{k-t+1} + (t-1)\binom{w+k-2t+1}{k-t}$.

Proof. Consider subsets $A \subseteq U' \subseteq U$ such that $|A| = t-1$ and $|U'| = w+k-(t-1)$, and consider the family $\mathcal{A} = \{P \in \mathcal{J} : A \subseteq P \subseteq U'\}$. Take $P \in \mathcal{A}$ and $C = (U' \setminus P) \cup A$. Then $C \in \Delta_P$ because $|C| = w$ and $|C \cap P| = t-1$. On the other hand, $|C \cap P'| \geq t$ if $P' \in \mathcal{A} \setminus \{P\}$, and hence $C \in \Gamma_{P'}$. Then $h(\mathcal{A} \setminus \{P\}|C) = 0$, and this implies that $h(\{P\}|\mathcal{A} \setminus \{P\}) \geq h(\{P\}|C) = 1$. Therefore, $h(\{P\}|\mathcal{A} \setminus \{P\}) = 1$ for every $P \in \mathcal{A}$. As a consequence,

$$|\mathcal{A}| = \sum_{P \in \mathcal{A}} h(\{P\}) \geq h(\mathcal{A}) \geq \sum_{P \in \mathcal{A}} h(\{P\}|\mathcal{A} \setminus \{P\}) = |\mathcal{A}|$$

and $h(\mathcal{A}) = |\mathcal{A}|$. Consider now a participant $i \in U' \setminus A$ and the set $B = A \cup \{i\}$. Consider as well the family $\mathcal{B} = \{P \in \mathcal{A} : B \subseteq P\}$. Since $\mathcal{B} \subseteq \mathcal{A}$, it follows that $h(\mathcal{B}) = |\mathcal{B}|$. We affirm that $h(\mathcal{B}|A) = h(\mathcal{B})$. For every $P \in \mathcal{A}$, we take $C_P = (U' \setminus P) \cup A$. As before, $C_P \in \Delta_P$ and $C_P \in \Gamma_{P'}$ for every $P' \in \mathcal{A} \setminus \{P\}$. Now,

$$h(\mathcal{B}|A) \geq \sum_{P \in \mathcal{B}} h(\{P\}|A \cup (\mathcal{B} \setminus \{P\})) \geq \sum_{P \in \mathcal{B}} h(\{P\}|C_P \cup (\mathcal{B} \setminus \{P\})) = \sum_{P \in \mathcal{B}} h(\{P\}|C_P) = |\mathcal{B}|,$$

which proves our affirmation. We have used that $h(\mathcal{B} \setminus \{P\}|C_P) = 0$. Since $h(\mathcal{B}|A \cup \{i\}) = h(\mathcal{B}|B) = 0$ and $h(\mathcal{B}|A) = h(\mathcal{B})$, we obtain that $h(\{i\}) \geq h(\mathcal{B}) = |\mathcal{B}|$. This proves the lower bound on the optimal information ratio $\sigma(w,t,k,n)$.

Our next step is to prove that $h(\mathcal{A}|B) \geq |\mathcal{A} \setminus \mathcal{B}|$. Indeed,

$$\begin{aligned} h(\mathcal{A}|B) &\geq \sum_{P \in \mathcal{A}} h(\{P\}|B \cup (\mathcal{A} \setminus \{P\})) = \sum_{P \in \mathcal{A} \setminus \mathcal{B}} h(\{P\}|B \cup (\mathcal{A} \setminus \{P\})) \\ &= \sum_{P \in \mathcal{A} \setminus \mathcal{B}} h(\{P\}|B) = |\mathcal{A} \setminus \mathcal{B}|. \end{aligned}$$

Clearly, $h(\{P\}|B) = 0$ if $P \in \mathcal{B}$. We have used as well that $h(\mathcal{A} \setminus \{P\}|B) = 0$ if $P \in \mathcal{A} \setminus \mathcal{B}$. Observe that $h(U \cup \mathcal{J}) = h(U)$. Moreover, $h(U) = h(B) + h(U|B)$. First, we are going to find a bound on $h(B)$. Since $h(\mathcal{B}|A) = h(\mathcal{B})$ and $h(\mathcal{B}|B) = h(\mathcal{B}|A \cup \{i\}) = 0$, we have that $h(\{i\}|A) \geq h(\mathcal{B})$. Therefore, $h(B) \geq t \cdot h(\mathcal{B}) = t \cdot |\mathcal{B}|$. And second, we find a bound on $h(U|B)$. Since $h(\mathcal{A}|U) = 0$, we have $h(U|B) \geq h(\mathcal{A}|B) \geq |\mathcal{A} \setminus \mathcal{B}|$, and the desired lower bound on $\sigma_T(w,t,k,n)$ is obtained. □

If $w = t-1$, the lower bounds in Theorem 4.1 are $\sigma(t-1,t,k,n) \geq 1$ and $\sigma_T(t-1,t,k,n) \geq t$. It is not difficult to check that an ideal (t,n)-threshold secret sharing scheme as, for instance, the one proposed by Shamir [19], is a $(t-1)$-secure (t,k,n)-multithreshold scheme attaining these bounds. Observe that $w = t-1$ if $k = n$. If $t = 1$, then we have the lower bounds

- $\sigma(w,1,k,n) \geq \binom{w+k-1}{k-1}$ and
- $\sigma_T(w,1,k,n) \geq \binom{w+k}{k}$.

In this case, the key predistribution schemes presented in [4] are optimal w-secure $(1,k,n)$-multithreshold schemes.

5. Optimal w-Secure $(2,3,n)$-Multithreshold Schemes

In this section we present a construction of linear w-secure $(2,3,n)$ multithreshold schemes, where $1 \leq w \leq n-2$, whose information ratio and randomness attain the lower bounds in Theorem 4.1. We define next a linear family of random variables and then we prove in Theorem 5.3 that, under certain conditions, they define a multithreshold scheme with the required properties.

Definition 5.1. Consider integers w, n with $n \geq 3$ and $1 \leq w \leq n-2$, a finite field $\mathbb{K}$ with $|\mathbb{K}| \geq n+1$, the sets $U = \{1, \ldots, n\}$ and $\mathcal{J} = \{P \subseteq U : |P| = 3\}$, and two n-tuples $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$ of distinct values in, respectively, $\mathbb{K} \setminus \{0\}$ and $\mathbb{K}$. Observe that there may be $i, j \in U$ with $x_i = y_j$. For every $i \in U$, take $\lambda_i = -x_i^w$ and the vector $v_i = (1, x_i, x_i^2, \ldots, x_i^{w-1}) \in \mathbb{K}^w$. Consider as well the vector spaces $E = S_2(\mathbb{K}^w) \times (\mathbb{K}^w)^*$ and $F = (\mathbb{K}^w)^*$. Finally, consider the linear maps $(\phi_i)_{i \in U}$ and $(\pi_P)_{P \in \mathcal{J}}$ defined as follows.

- For every $i \in U$, take $\phi_i \colon E \to F$ with $\phi_i(T, S) = T(v_i, \cdot) + \lambda_i S$.
- If $P = \{i, j, k\} \in \mathcal{J}$ with $i < j < k$, then $\pi_P \colon E \to \mathbb{K}$ with

$$\pi_P(T, S) = y_i \cdot \phi_i(T, S)(\lambda_k v_j - \lambda_j v_k) + y_j \cdot \phi_j(T, S)(\lambda_i v_k - \lambda_k v_i) + y_k \cdot \phi_k(T, S)(\lambda_j v_i - \lambda_i v_j).$$

We define $\Sigma(n, w, \mathbb{K}, \mathbf{x}, \mathbf{y})$ as the family of linear random variables defined by the linear maps $((\phi_i)_{i \in U}, (\pi_P)_{P \in \mathcal{J}})$.

Some technicalities are needed in order to prove in Theorem 5.3 that, if the finite field $\mathbb{K}$ is large enough, there exist n-tuples $\mathbf{x}, \mathbf{y} \in \mathbb{K}^n$ such that $\Sigma(n, w, \mathbb{K}, \mathbf{x}, \mathbf{y})$ is a w-secure $(2, 3, n)$ multithreshold scheme. Consider the rational function $L \in \mathbb{K}(Z_0, Z_1, \ldots, Z_w)$ given by

$$L = \sum_{i=1}^{w} \left(Z_i^w \cdot \prod_{1 \leq j \leq w, j \neq i} \frac{Z_0 - Z_j}{Z_i - Z_j} \right).$$

Observe that $L(z_i, z_1, \ldots, z_w) = z_i^w$ for every w-tuple $(z_1, \ldots, z_w)$ of distinct values in $\mathbb{K}$ and for every $i = 1, \ldots, w$. Given $B = \{i_1, \ldots, i_w\} \subseteq U$ with $i_1 < i_2 < \cdots < i_w$ and an n-tuple $X = (X_1, \ldots, X_n)$, we notate $X_B = (X_{i_1}, \ldots, X_{i_w})$.

Lemma 5.2. *If $|\mathbb{K}| \geq \binom{n}{2}\binom{n-2}{w}(2w-1)+2$, there exists an n-tuple $\mathbf{x}$ of distinct values in $\mathbb{K} \setminus \{0\}$ such that $x_j^w L(x_i, \mathbf{x}_B) - x_i^w L(x_j, \mathbf{x}_B) \neq 0$ for every $B \subseteq U$ with $|B| = w$ and for every $i, j \in U \setminus B$ with $i \neq j$.*

Proof. For $B \subseteq U$ and $i, j \in U \setminus B$ with $|B| = w$ and $i < j$, consider

$$G_{B,i,j} = \left(\prod_{r,s \in B,\, r<s} (X_s - X_r) \right) \cdot \left(X_j^w L(X_i, X_B) - X_i^w L(X_j, X_B) \right).$$

Observe that the denominator of the rational function $X_j^w L(X_i, X_B) - X_i^w L(X_j, X_B)$ is canceled by the product of the terms $X_s - X_r$, and hence $G_{B,i,j}$ is a polynomial in $\mathbb{K}[X_1, \ldots, X_n]$. Moreover, $G_{B,i,j}$ is a nonzero polynomial because monomials of the form $X_j^w X_i^\ell M(X_B)$, where $0 \leq \ell \leq w-1$, appear only from $X_j^w L(X_i, X_B)$, and at least one of them is nonzero. Finally, observe that $G_{B,i,j}$ has degree at most $2w-1$ on each variable. Consider the polynomial $G \in \mathbb{K}[X_1, \ldots, X_n]$ defined by

$$G = X_1 \cdots X_n \cdot \left(\prod G_{B,i,j} \right),$$

where the last product runs over all $B \subseteq U$ and $i, j \in U - B$ with $|B| = w$ and $i < j$. Clearly, G is a nonzero polynomial with degree at most $d = \binom{n}{2}\binom{n-2}{w}(2w-1)+1$ on each variable. Since $|\mathbb{K}| \geq d+1$, there exists $\mathbf{x} \in \mathbb{K}^n$ with $G(\mathbf{x}) \neq 0$ by Lemma 2.3. Clearly, the n-tuple $\mathbf{x}$ satisfies the required conditions. □

Theorem 5.3. *If $w < n-2$ and $|\mathbb{K}| \geq \max\left\{ \binom{n}{2}\binom{n-2}{w}(2w-1)+2, \binom{n-1}{w}\binom{n-w-1}{2} + n \right\}$, or $w = n-2$ and $|\mathbb{K}| \geq n+1$, then there exist n-tuples $\mathbf{x}, \mathbf{y}$ such that $\Sigma(n, w, \mathbb{K}, \mathbf{x}, \mathbf{y})$ is an optimal w-secure $(2, 3, n)$ multithreshold scheme.*

Proof. We have to prove first that $\ker \phi_A \subseteq \ker \pi_P$ for every $A \subseteq P \subseteq U$ with $|A| = 2$ and $|P| = 3$. We can suppose without loss of generality that $A = \{1, 2\}$ and $P = \{1, 2, 3\}$. It is not difficult to check that, for every $(T, S) \in E$,

$$\phi_1(T, S)(\lambda_3 v_2 - \lambda_2 v_3) + \phi_2(T, S)(\lambda_1 v_3 - \lambda_3 v_1) + \phi_3(T, S)(\lambda_2 v_1 - \lambda_1 v_2) = 0.$$

Therefore, $\pi_P(T,S)=0$ if $\phi_1(T,S)=\phi_2(T,S)=0$.

Now we have to prove that $\ker\phi_B+\ker\pi_P=E$ if $B\subseteq U$ is such that $|B|=w$ and $|B\cap P|\leq 1$. Since $\dim\ker\pi_P=\dim E-1$, it is enough to prove that $\ker\phi_B\not\subseteq\ker\pi_P$.

For a set $B\subseteq U$ with $|B|=w$, consider the only linear form $S_B\in(\mathbb{K}^w)^*$ such that $S_B(v_i)=-\lambda_i=x_i^w$ for every $i\in B$. Consider as well the symmetric bilinear form $T_B\in S_2(\mathbb{K}^w)$ defined by $T_B(u,v)=S_B(u)S_B(v)$ for every $(u,v)\in\mathbb{K}^w\times\mathbb{K}^w$. Clearly, $(T_B,S_B)\in\ker\phi_B$.

Let $f_B\in\mathbb{K}[X]$ be the polynomial of degree $w-1$ defined by $f_B=\alpha_1+\alpha_2X+\cdots+\alpha_wX^{w-1}$, where $S_B=\sum_{i=1}^w\alpha_ie^i$, that is, $(\alpha_1,\ldots,\alpha_w)$ are the components of the linear form $S_B\in(\mathbb{K}^w)^*$ in the canonical basis of $(\mathbb{K}^w)^*$. Observe that $f_B(x_i)=S_B(v_i)$ for every $i\in U$.

Suppose that $|B\cap P|=1$. We can assume that $P=\{1,2,3\}$ and $P\cap B=\{3\}$. It is straightforward to check that $\pi_P(T_B,S_B)=(y_1-y_2)\lambda_3(S_B(v_1)+\lambda_1)(S_B(v_2)+\lambda_2)$. Observe that $f_B(x_i)=x_i^w$ for all $i\in B$. If $S_B(v_1)+\lambda_1=0$, then $f_B(x_1)=x_1^w$, and hence X^w-f_B would be a polynomial of degree w with $w+1$ zeroes, a contradiction. Similarly, $S_B(v_2)+\lambda_2\neq 0$, and hence $(T_B,S_B)\notin\ker\pi_P$.

At this point we have proved that $\Sigma(n,w,\mathbb{K},\mathbf{x},\mathbf{y})$ is a w-secure $(2,3,n)$ multithreshold scheme if $w=n-2$. Observe that we only required that $\mathbf{x},\mathbf{y}$ are n-tuples of distinct values in, respectively, $\mathbb{K}-\{0\}$ and $\mathbb{K}$, and hence it is enough that $|\mathbb{K}|\geq n+1$.

Things are more complicated if $w<n-2$. In this situation we have to prove as well that $(T_B,S_B)\notin\ker\pi_P$ when $B\cap P=\emptyset$. Specifically, we prove that, given any n-tuple $\mathbf{x}$ whose existence is given by Lemma 5.2, there exists an n-tuple $\mathbf{y}$ of distinct values in $\mathbb{K}$ for which that condition is satisfied. If $P=\{i,j,k\}$ and $B\subseteq U$ is such that $|B|=w$ and $B\cap P=\emptyset$, then

$$\begin{aligned}\pi_P(T_B,S_B) &= y_i(f_B(x_i)+\lambda_i)(\lambda_kf_B(x_j)-\lambda_jf_B(x_k))\\ &\quad +y_j(f_B(x_j)+\lambda_j)(\lambda_if_B(x_k)-\lambda_kf_B(x_i))\\ &\quad +y_k(f_B(x_k)+\lambda_k)(\lambda_if_B(x_j)-\lambda_jf_B(x_i)).\end{aligned}$$

Therefore, there is a polynomial $g_{P,B}\in\mathbb{K}[Y_1,\ldots,Y_n]$ such that $\pi_P(T_B,S_B)=g_{P,B}(\mathbf{y})$. We prove next that $g_{P,B}$ is nonzero by checking the coefficient of Y_k in this polynomial, which is equal to

$$(f_B(x_k)+\lambda_k)(\lambda_if_B(x_j)-\lambda_jf_B(x_i))=(f_B(x_k)+\lambda_k)(x_j^wL(x_i,\mathbf{x}_B)-x_i^wL(x_j,\mathbf{x}_B))\neq 0.$$

We have applied here Lemma 5.2 and the fact that $f_B=L(X,\mathbf{x}_B)$. At this point, it is enough to prove that there exists an n-tuple $\mathbf{y}$ of distinct values in $\mathbb{K}$ such that $g_{P,B}(\mathbf{y})\neq 0$ for every $P\in\mathcal{J}$ and $B\subseteq U$ with $|B|=w$ and $B\cap P=\emptyset$. Consider the nonzero polynomial $g\in\mathbb{K}[Y_1,\ldots,Y_n]$ defined by

$$g=\left(\prod_{1\leq i<j\leq n}(Y_j-Y_i)\right)\cdot\left(\prod g_{P,B}\right)$$

where the second product runs over all pairs (P,B) of sets in the conditions above. Observe that the polynomial g has degree $d=\binom{n-1}{w}\binom{n-w-1}{2}+n-1$ on each variable. Since $|\mathbb{K}|\geq d+1$, there exists $\mathbf{y}\in\mathbb{K}^n$ with $g(\mathbf{y})\neq 0$ by Lemma 2.3. Clearly, the n-tuple $\mathbf{y}$ satisfies the required conditions.

Observe that the information ratio of the scheme $\Sigma(n,w,\mathbb{K},\mathbf{x},\mathbf{y})$ is $\sigma=\operatorname{rank}\phi_i=\dim F=w$ and its randomness is $\sigma_T=\dim E=\binom{w+1}{2}+w$. Therefore, the lower bounds in Theorem 4.1 are attained. □

6. A General Construction

We present in this section a construction of w-secure (t,k,n)-multithreshold schemes for all possible values of the parameters (w,t,k,n). The information ratio and the randomness of these schemes do not attain the lower bounds in Theorem 4.1, but no general construction with better values for these parameters has been presented before. As we did in previous section, we define next a family of linear maps that will be proved to determine a multithreshold scheme.

Definition 6.1. Consider integers w,t,k,n with $1\leq t\leq k\leq n$ and $t-1\leq w\leq n-k+t-1$, a finite field $\mathbb{K}$ with $|\mathbb{K}|\geq n+1$, the sets $U=\{1,\ldots,n\}$ and $\mathcal{J}=\{P\subseteq U\,:\,|P|=k\}$, and n distinct values $x_1,\ldots,x_n\in\mathbb{K}\setminus\{0\}$. Take $m=w-t+2$ and, for every $i\in U$, the vector $v_i=(1,x_i,x_i^2,\ldots,x_i^{m-1})\in\mathbb{K}^m$. Consider as well the vector spaces $E=(S_k(\mathbb{K}^m))^t$ and $F=S_{k-1}(\mathbb{K}^m)$, and the linear maps $(\phi_i)_{i\in U}$ and $(\pi_P)_{P\in\mathcal{J}}$ defined as follows.

- For every $i \in U$, the linear map $\phi_i \colon E \to F$ is given by

$$\phi_i(T_1, \ldots, T_t) = T_1(v_i, \ldots) + x_i \cdot T_2(v_i, \ldots) + \cdots + x_i^{t-1} \cdot T_t(v_i, \ldots).$$

- If $P = \{i_1, \ldots, i_k\} \in \mathcal{J}$, consider $\pi_P \colon E \to \mathbb{K}$ with $\pi_P(T_1, \ldots, T_t) = T_1(v_{i_1}, \ldots, v_{i_k})$.

Theorem 6.2. *The linear family of random variables determined by the linear maps introduced in Definition 6.1 forms a w-secure (t, k, n)-multithreshold scheme with information ratio and randomness*

$$\sigma = \binom{w+k-t}{k-1} \text{ and } \sigma_T = t \cdot \binom{w+k-t+1}{k},$$

respectively.

Proof. Let P be a set in $\mathcal{J}$. Without loss of generality, we can suppose that $P = \{1, \ldots, k\}$. Every user $i \in P$ can compute

$$\begin{aligned} s_{i,P} &= [\phi_i(T_1, \ldots, T_t)](v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_k) = \\ &= T_1(v_1, \ldots, v_k) + x_i \cdot T_2(v_1, \ldots, v_k) + \cdots + x_i^{t-1} \cdot T_t(v_1, \ldots, v_k). \end{aligned}$$

Clearly, the values $s_{i,P}$ are shares for the secret value $k_P = T_1(v_1, \ldots, v_k)$ in a (t, k)-threshold secret sharing scheme. Because of that, the participants in every t-subset A of P can recover the secret value k_P. In particular, this implies that $\bigcap_{i \in A} \ker \phi_i \subseteq \ker \pi_P$ for every $A \in \Gamma_P$.

We prove next that $\bigcap_{i \in B} \ker \phi_i + \ker \pi_P = E$ for every $B \in \Delta_P$. Since $\dim \ker \pi_P = \dim E - 1$, it is enough to find a vector in $\bigcap_{i \in B} \ker \phi_i$ that is not in $\ker \pi_P$. Take $B \in \Delta_P$ with $|B| = w$ and a subset $C \subseteq B \setminus P$ with $|C| = w - t + 1 = m - 1$. Let F be the vector subspace of $\mathbb{K}^m$ spanned by the vectors $(v_i)_{i \in C}$. Clearly, the dimension of F is equal to $m - 1$. Moreover, $v_i \notin F$ if $i \in U \setminus C$. Take a nonzero linear form $\alpha \in F^\perp \subseteq (\mathbb{K}^m)^*$. Observe that $\alpha(v_i) = 0$ if and only if $i \in C$. Consider as well the symmetric k-linear form $T \in S_k(\mathbb{K}^m)$ defined by $T(u_1, \ldots, u_k) = \alpha(u_1) \cdots \alpha(u_k)$. Since $T(v_1, \ldots, v_k) \neq 0$, the proof is completed by finding values $\mu_1, \ldots, \mu_t \in \mathbb{K}$ such that $\mu_1 \neq 0$ and $\widehat{T} = (\mu_1 T, \ldots, \mu_t T) \in \bigcap_{i \in B} \ker \phi_i$. Obviously, $\phi_i(\widehat{T}) = 0$ for every $i \in C$. On the other hand, $\phi_i(\widehat{T}) = (\mu_1 + \mu_2 x_i + \cdots + \mu_t x_i^{t-1}) \cdot T(v_i, \ldots)$ for every $i \in B \setminus C$. The required values $\mu_j \in \mathbb{K}$ are obtained from $\prod_{i \in B \setminus C}(X - x_i) = \mu_1 + \mu_2 X + \cdots + \mu_t X^{t-1}$. □

7. Conclusions

Summarizing the results presented in this paper are the following.

- We obtain a new general lower bound for the randomness of threshold multisecret sharing schemes.
- We provide a new proof for the lower bound on the information ratio that was given in [12].
- We present a linear construction of optimal threshold multisecret sharing schemes for the case $t = 2$, $k = 3$ and $1 \leq w \leq n - 2$. Although an optimal construction for this case was previously presented in [1], ours is much simpler, and the proof is shorter.
- We present a general construction of multithreshold schemes for all possible values of the parameters (w, t, k, n). In general, these are not optimal schemes, but it is the best known general construction.

References

[1] S.G. Barwick, W.-A. Jackson. An Optimal Multisecret Threshold Scheme Construction. *Des. Codes Cryptogr.* **37** (2005) 67–389.

[2] G.R. Blakley. Safeguarding cryptographic keys. *AFIPS Conference Proceedings* **48** (1979) 313–317.

[3] R. Blom. An Optimal Class of Symmetric Key Generation Systems. *Advances in Cryptology, Eurocrypt '84, Lecture Notes in Comput. Sci.* **209** (1984) 335–338.

[4] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung. Perfectly secure key distribution for dynamic conferences. *Advances in Cryptology, Crypto '92, Lecture Notes in Comput. Sci.* **740** (1993) 471–486.

[5] C. Blundo, P. D'Arco, V. Daza, C. Padró. Bounds and constructions for unconditionally secure distributed key distribution schemes for general access structures. *Theoret. Comput. Sci.* **320** (2004) 269–291.

[6] E.F. Brickell. Some ideal secret sharing schemes. *J. Combin. Math. and Combin. Comput.* **9** (1989) 105–113.

[7] T.M. Cover, J.A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 1991.

[8] O. Farràs, J. Martí-Farré, C. Padró. Ideal Multipartite Secret Sharing Schemes. *J. Cryptology* **25** (2012) 434–463.

[9] S. Fujishige. Polymatroidal Dependence Structure of a Set of Random Variables. *Information and Control* **39** (1978) 55–72.

[10] S. Fujishige. Entropy functions and polymatroids—combinatorial structures in information theory. *Electron. Comm. Japan* **61** (1978) 14–18.

[11] S. Fujishige. *Submodular Functions and Optimization*. Annals of Discrete Mathematics **47**, North-Holland Elsevier, Amsterdam, 1991.

[12] W.-A. Jackson, K.M. Martin, C.M. O'Keefe. Multisecret threshold schemes. *Advances in Cryptology, Crypto '93, Lecture Notes in Comput. Sci.* **773** (1994) 126–135.

[13] W.-A. Jackson, K.M. Martin, C.M. O'Keefe. A Construction for Multisecret Threshold Schemes. *Des. Codes Cryptogr.* **9** (1996) 287–303.

[14] E.D. Karnin, J.W. Greene, M.E. Hellman. On secret sharing systems. *IEEE Trans. Inform. Theory* **29** (1983) 35–41.

[15] J. Martí-Farré, C. Padró. On Secret Sharing Schemes, Matroids and Polymatroids. *J. Math. Cryptol.* **4** (2010) 95–120.

[16] B. Masucci. Sharing Multiple Secrets: Models, Schemes and Analysis. *Des. Codes Cryptogr.* **39** (2006) 89–111.

[17] C. Padró, I. Gracia, S. Martín Molleví, P. Morillo. Linear Key Predistribution Schemes. *Des. Codes Cryptogr.* **25** (2002) 281–298.

[18] C. Padró, I. Gracia, S. Martín, P. Morillo. Linear broadcast encryption schemes. *Discrete Appl. Math.* **128** (2003) 223–238.

[19] A. Shamir. How to share a secret. *Commun. of the ACM.* **22** (1979) 612–613.

[20] G. J. Simmons. How to (Really) Share a Secret. *Advances in Cryptology – CRYPTO '88, Lecture Notes in Comput. Sci.* **403** (1990) 390–448.

[21] D.R. Stinson. On some methods for unconditionally secure key distribution and broadcast encryption. *Des. Codes Cryptogr.* **12** (1997) 215–243.