REDUCED ACCESS STRUCTURES WITH FOUR MINIMAL QUALIFIED SUBSETS ON SIX PARTICIPANTS

MOTAHHAREH GHARAH AND SHAHRAM KHAZAEI

Department of Mathematical Sciences
Sharif University of Technology
P.O. Box 11155-9415, Tehran, Iran

(Communicated by Claude Carlet)

Abstract. In this paper, we discuss a point about applying known decomposition techniques in their most general form. Three versions of these methods, which are useful for obtaining upper bounds on the optimal information ratios of access structures, are known as: Stinson’s $\lambda$-decomposition, $(\lambda, \omega)$-decomposition and $\lambda$-weighted-decomposition, where the latter two are generalizations of the first one. We continue by considering the problem of determining the exact values of the optimal information ratios of the reduced access structures with exactly four minimal qualified subsets on six participants, which remained unsolved in Martí-Farré et al.’s paper [Des. Codes Cryptogr. 61 (2011), 167-186]. We improve the known upper bounds for all the access structures, except four cases, determining the exact values of the optimal information ratios. All three decomposition techniques are used while some cases are handled by taking full advantage of the generality of decompositions.

1. Introduction

A secret sharing scheme is a method that allows a secret to be shared among a set of participants and it was independently proposed by Shamir [27] and Blakley [3] in 1979. Their method, known as threshold secret sharing, is performed in a way that any subset of participants of size more than a certain threshold can recover the secret while any other subset of participants learn nothing about the secret. A natural generalization of threshold secret sharing was proposed by Itô et al. [16] to allow more general structures of subsets to learn the secret, while keeping the secret information theoretically hidden from all other subsets. The collection of qualified subsets is called an access structure, which is supposed to be monotone increasing, i.e., any superset of a qualified subset must be qualified.

One of the major problems in secret sharing is to minimize the ratio of the largest share size to the secret size, known as the information ratio, initially introduced in [6, 4, 23]. This measure is also referred to as complexity and its inverse is called information rate in the literature. The optimal information ratio of an access structure is defined as the infimum information ratios of all secret sharing schemes realizing it. Despite the long history of the subject, there are significant gaps between known lower and upper bounds on the optimal information ratio of many access structures (for example, see [32, 18, 8]), with very few ones settled (see [10, 9] for two notable examples).

2010 Mathematics Subject Classification: 94A62.

Key words and phrases: Secret sharing scheme, optimal information ratio, decomposition techniques.
The optimal information ratio for some concrete access structures have been studied in several papers (for example, see [32, 18, 20, 21, 24, 13, 9]). Lower bounds on the optimal information ratios of the access structures can be derived by using the entropy method as initially described in [7]. This method can be automated using linear programming (LP) technique [26] and, very recently has enjoyed substantial improvements [12]. The common approach for finding upper bounds on the optimal information ratio of such access structures is to utilize the so-called decomposition techniques, initially introduced by Stinson under the name of λ-decomposition [29]. Later, two generalizations of the technique were introduced, called (λ, ω)-decomposition [33] and λ-weighted-decomposition [30].

We highlight the contributions of the paper below:

• On taking full advantage of the generality of decomposition techniques. Most of the papers in the literature have worked with a restricted and less general variant of the definition of λ-decomposition. Going a little bit ahead, the λ-decomposition allows sub-access structures to be subsets of the original access structure. We were able to identify only three papers ([29, 25, 22]) in the literature that provided a definition of λ-decomposition in its most general form. All other papers, e.g., see [18, 30, 20, 21, 31], have presented a definition in which the minimal sub-access structures are considered to be subsets of the original minimal access structure. Actually, the former three papers have actually applied the technique in its less general variant. Consequently, this limited view on the method has resulted in devising less efficient secret sharing schemes in several cases, including reduced access structures with four minimal subsets [22]. We discuss this issue in further details in Section 3. Similar remarks about (λ, ω) and λ-weighted-decomposition techniques are also argued in the same section.

• Results on reduced access structures on 6 participants with 4 minimal subsets. In [22], Martí-Farré et al. have studied the optimal information ratio of the access structures with four minimal qualified subsets. Although the exact values of the optimal information ratio were determined in several cases, for some other ones, an upper and a lower bounds were only obtained. In particular, among the all 77 non-isomorphic such access structures on six participants, only 44 cases were fully resolved and the other 33 were remained unsolved. Fourteen cases are immediately resolved by taking the currently known results into account and using a simple observation: if there is a linear secret sharing scheme for an access structure with a certain information ratio, then there is a linear scheme for its dual (to be defined later) with the same information ratio [17]. All three decomposition techniques are used for handling the remaining access structures: 7 cases are resolved using the Stinson’s λ-decomposition technique [29], 4 cases are tackled by applying (λ, ω)-decomposition [33] and 4 other cases are resolved using the λ-weighted-decomposition [30]. Four access structures remains unsolved, two of which are duals of two renowned open graph access structures with six participants [32]. We point out that some of our decompositions are achieved by taking full advantage of decomposition techniques, which were discussed above.

• (λ, ω)-decomposition and duality. A theorem—which relates the dual of a (λ, ω)-decomposition for a given access structure to a (λ', ω')-decomposition for the dual of the decomposed access structure—is discussed in Section 3.2, which might be interesting on its own.
2. Definitions and preliminaries

2.1. Secret sharing schemes. In this section, we introduce the basic notations and definitions. We refer the reader to [28] for an old survey and further details on the topic and to [1] for a more recent one.

Access structures. Let \( \mathcal{P} = \{p_1, \ldots, p_n\} \) be a set of participants. A collection of subsets \( \Gamma \subseteq 2^\mathcal{P} \) is called an access structure on \( \mathcal{P} \) if it is monotone increasing, i.e., for every \( A \in \Gamma \) and \( A \subseteq B \) it holds that \( B \in \Gamma \). The sets in \( \Gamma \) and \( \Gamma^c = 2^\mathcal{P} \setminus \Gamma \) are, respectively, called qualified and forbidden sets. A qualified set \( A \in \Gamma \) is called minimal if any proper subset of it is a forbidden set. A forbidden set \( B \in \Gamma^c \) is called maximal if any proper superset of it is a qualified set. The collection of all minimal qualified subsets and that of all maximal forbidden sets are denoted by \( \Gamma_\text{min} \) and \( \Gamma_\text{max} \), respectively. We refer to \( \Gamma_\text{min} \) as the minimal access structure of \( \Gamma \).

Notation. In this paper, a subset \( A = \{p_{i_1}, \ldots, p_{i_m}\} \) of participants is represented by \( [A] = \{i_1, \ldots, i_m\} \), and a collection \( \mathcal{A} = \{A_1, \ldots, A_m\} \) of subsets of participants is represented by \( [\mathcal{A}] = [A_1] + \ldots + [A_m] \). For example, \( [\Gamma^-] = 1359 + 23 + 5C + 9C \) is a representation of the minimal access structure \( \Gamma^- = \{(1,3,5,9), (2,3), (5,C), (9,C)\} \) on \( \mathcal{P} = \{1,2,3,5,9,C\} \).

Random variables. Let \( X \) be a random variable with support \( \mathcal{X} = \{x_1, \ldots, x_m\} \) (i.e., the set of values that it accepts with positive probability) and let \( p_i = \Pr[X = x_i] \). The Shannon entropy of \( X \) is defined as \( H(X) = - \sum_{i=1}^{m} p_i \log_2 p_i \), where 0 \( \log_2 0 \) is considered to be 0. The entropy of \( X \) conditioned on \( Y \) is defined as \( H(X|Y) = \sum_{y \in \mathcal{Y}} \Pr[Y = y] H(X|Y = y) \), where \( \mathcal{Y} \) is the support of \( Y \) and \( H(X|Y = y) = \sum_{x_i \in \mathcal{X}} \Pr[X = x_i|Y = y] \log_2 \Pr[X = x_i|Y = y] \).

Formal definition. Initial steps towards formalizing the definition of a secret sharing scheme and its security was taken in [19, 6, 7, 5]. Below, we present a definition which captures the information theoretical security.

Definition 1 (secret sharing scheme). A secret sharing scheme on \( \mathcal{P} \), is a triplet \( \Sigma = (S, R, \Pi) \), where \( S \) and \( R \) are independent random variables with supports \( S \) and \( R \), respectively, satisfying \( H(S) > 0 \), and \( \Pi : S \times R \to S_1 \times \ldots \times S_n \) is a map, in which \( S_\ell \) is the support of the random variable \( S_\ell \) induced by \( \Pi(S, R) = (S_1, \ldots, S_n) \). We refer to \( \Pi \), \( S \) and \( R \) as the sharing map, secret space and randomness space.

To share a secret \( s \in S \), presumably sampled from \( S \), a randomness \( r \) is sampled from \( R \) and the vector of shares \( \Pi(s,r) = (s_1, \ldots, s_n) \) is computed. Then, each share \( s_j \) is privately transmitted to the participant \( p_j \). For a set \( A \subseteq \mathcal{P} \), we denote the random variable \( S_A \) as the restriction of \( \Pi(S, R) \) to the entries that correspond to the members of \( A \).

Definition 2 (realization of an access structure). Let \( \Sigma \) be a secret sharing scheme and let \( \Gamma \) be an access structure both defined on \( \mathcal{P} \). We say that \( \Sigma \) is a secret sharing scheme for \( \Gamma \), or \( \Gamma \) realizes \( \Sigma \), if the following two hold:

1. The secret can be reconstructed by qualified sets; that is, for all \( A \in \Gamma \), it holds that \( H(S|S_A) = 0 \).
2. The secret is remained perfectly hidden from the forbidden sets; that is, for all \( B \notin \Gamma \), it holds that \( H(S|S_B) = H(S) \).

Information ratio. Let \( \Sigma \) be a secret sharing scheme on \( \mathcal{P} \). The information ratio of a participant \( p_i \in \mathcal{P} \) in \( \Sigma \), denoted by \( \sigma_p(\Sigma) \), is defined by \( \sigma_p(\Sigma) = H(S_i)/H(S) \).
and the information ratio of the scheme Σ is defined by \( \sigma(\Sigma) = \max_{p \in P} \sigma_p(\Sigma) \). We refer to the vector \( \mathbf{\sigma}(\Sigma) = (\sigma_p(\Sigma))_{p \in P} \) as the contribution vector or, following [18], convec for short. Let \( \Gamma \) be an access structure on \( P \). The optimal information ratio of the access structure \( \Gamma \) is defined by \( \sigma(\Gamma) = \inf \sigma(\Sigma) \), where the infimum is taken over all secret sharing schemes \( \Sigma \) for \( \Gamma \).

**Ideal and linear schemes, and dual access structures.** A secret sharing scheme \( \Sigma \) with \( \sigma(\Sigma) = 1 \) is called ideal. An access structure \( \Gamma \) is called ideal, if there is an ideal scheme for it. A secret sharing scheme is said to be linear if the sets \( S, R, S_1, \ldots, S_n \) are all vector spaces of finite dimension over a finite field \( F \) and the sharing map is linear on \( F \). In some papers (e.g., [2]), if the dimension of the secret space of a linear secret sharing scheme is larger than one, the scheme is referred to as multi-linear.

We do not make such a distinction in this paper. The dual access structure of an access structure \( \Gamma \) on \( P \), denoted by \( \Gamma^* \), is defined by \( \Gamma^* = \{ A \subseteq P : P \setminus A \in \Gamma^c \} \). It is proved in [17] that if \( \Sigma \) is a linear secret sharing scheme for \( \Gamma \), then there exists a linear secret sharing scheme \( \Sigma^* \) for \( \Gamma^* \) with the same convec, and consequently \( \sigma(\Sigma) = \sigma(\Sigma^*) \).

### 2.2. Decomposition Constructions

In this section, we review three decomposition techniques for constructing secret sharing schemes from [29, 33, 30]. These techniques are useful for constructing a new secret sharing scheme from a number of given schemes, under some specified conditions.

**2.2.1. \( \lambda \)-decomposition.** We present a definition of the \( \lambda \)-decomposition technique [29] which can be found in several papers and we believe it should be considered as the standard definition. We refer to Section 3 for further discussion.

**Definition 3 (\( \lambda \)-decomposition).** Let \( \Gamma \) be an access structure on \( P \) and let \( \lambda \) be a positive integer. The collection \( \{\Gamma^1, \ldots, \Gamma^\ell\} \) of access structures is called a \( \lambda \)-decomposition of \( \Gamma \) if the following two hold:

1. \( \Gamma^j \subseteq \Gamma \) for every \( j \in [\ell] \).
2. If \( A \in \Gamma^j \), then it holds that \( A \in \Gamma^j \) for at least \( \lambda \) distinct values of \( j \in [\ell] \).

When all the sub-access structures \( \Gamma^j \) are ideal, we call the decomposition ideal; otherwise, it is referred to as non-ideal.

**Theorem 1 ([29]).** Let \( \{\Gamma^1, \ldots, \Gamma^\ell\} \) be a \( \lambda \)-decomposition of \( \Gamma \) on \( P \). Suppose that there exists a finite field \( F \) such that for every \( \Gamma^j, j \in [\ell] \), there exist a (not necessarily linear) secret sharing scheme with secret space \( F \) and convec \( \mathbf{\sigma}^j = (\sigma^j_p)_{p \in P} \). Then, there exist a secret sharing scheme \( \Sigma \) for \( \Gamma \) with convec \( \sum_{j=1}^{\ell} \mathbf{\sigma}^j \) over the secret space \( F^\lambda \).

**2.2.2. \((\lambda, \omega)\)-decomposition.** An interesting generalization of the \( \lambda \)-decomposition technique is called \( \lambda \)-\( \omega \)-decomposition method [33], formalized below.

**Definition 4 ((\( \lambda, \omega \))-decomposition).** Let \( \Gamma \) be an access structure on \( P \), and let \( \lambda, \omega \) be positive integers such that \( \lambda > \omega \). A \((\lambda, \omega)\)-decomposition of \( \Gamma \) consists of a collection \( \{\Gamma^1, \ldots, \Gamma^\ell\} \) of access structures on \( P \) such that the following requirements are satisfied:

1. If \( A \in \Gamma^j \), then it holds that \( A \in \Gamma^j \) for at most \( \omega \) distinct values of \( j \in [\ell] \).
2. If \( A \in \Gamma^j \), then it holds that \( A \in \Gamma^j \) for at least \( \lambda \) distinct values of \( j \in [\ell] \).

When all the sub-access structures \( \Gamma^j \) are ideal, we call the decomposition ideal; otherwise, it is referred to as non-ideal.
2.2.3. $\lambda$-weighted-decomposition. A second interesting extension of the $\lambda$-decomposition technique is the $\lambda$-weighted-decomposition method [30]. Instead of defining a weighted access structure as it was originally presented in [30], we present a simpler definition, similar to the notion of an access function in [11]. Even though it might be more suitable to call a weighted access structure an unnormalized rational-value access function, we stick to the original terminology.

Definition 5 (weighted access structure). A weighted access structure on $\mathcal{P}$ is a map $W : 2^\mathcal{P} \rightarrow \mathbb{Z}^\geq 0$ such that $W(\emptyset) = 0$ and for every $A, B \subseteq \mathcal{P}$, if $A \subseteq B$, then it holds that $W(A) \leq W(B)$. For every $A \subseteq \mathcal{P}$, $W(A)$ is called the weight of $A$ in $W$. We refer to $W(\mathcal{P})$ as the weight of $W$.

Let us describe how a weighted access structure $W$ on the participants set $\mathcal{P}$ can be represented minimally. Let $w = W(\mathcal{P})$ and, for every $0 \leq i \leq w$, let $W_i$ denote the collection of all subsets of $\mathcal{P}$ of weight $i$. For every $1 \leq i \leq w$, let $W_i^-$ denote the set of all minimal subsets in $W_i$, where a subset $A \in W_i$ is called minimal if none of its proper subsets belongs to $W_i$. We refer to $W^- = (W_1^-, \ldots, W_w^-)$ as the minimal weighted access structure of $W$. In this paper, the minimal weighted access structure is symbolically represented by $[W^-] = \sum_{i=1}^w i \times ([W_i^-])$.

Definition 6 (realization of a weighted access structure). Let $\Sigma$ be a secret sharing scheme and let $W$ be a weighted access structure, both defined on $\mathcal{P}$. We say that $\Sigma$ is a secret sharing scheme for $W$, or $\Sigma$ realizes $W$, if for every subset $A \subseteq \mathcal{P}$, it holds that $H(S|S_A) = (1 - \frac{W(A)}{W(\mathcal{P})})H(S)$.

Definition 7 ($\lambda$-weighted-decomposition). Let $\Gamma$ be an access structure on $\mathcal{P}$ and $\lambda$ be a positive integer. A $\lambda$-weighted-decomposition of $\Gamma$ consists of a collection $\{W_1, \ldots, W^\prime\}$ of weighted access structures such that the following requirements are satisfied:

1. If $A \in \Gamma^+$, then it holds that $W^j(A) = 0$, for every $j \in [t]$ (equivalently, $\Gamma^+ \subseteq W_0^\prime$, where $W_0^\prime$ is the set of all subsets of weight 0).
2. If $A \in \Gamma^-$, then it holds that $\sum_{j=1}^t W^j(A) \geq \lambda$

Theorem 3 ([30]). Let $\Gamma$ be an access structure on $\mathcal{P}$, and $\{W_1, \ldots, W^\prime\}$ be a $\lambda$-weighted-decomposition of $\Gamma$. Assume that there exists a finite field $\mathbb{F}$ such that each weighted sub-access structure $W^j$, of weight $w^j$, $j \in [t]$, is realized by a (not necessarily linear) secret sharing scheme with convex $\sigma^j = (\sigma^j_p)_{p \in \mathcal{P}}$ over the secret space $\mathbb{F}^{w^j}$. Moreover, suppose that in the $j$th scheme, any subset $A \subseteq \mathcal{P}$ can obtain $W^j(A)$ out of the $w^j$ secrets (of course, without gaining any information about the remaining $w^\prime - W^j(A)$ secrets). Then, there exist a secret sharing scheme $\Sigma$ for $\Gamma$ with convex $\frac{1}{\lambda} \sum_{j=1}^t w^j \sigma^j$ over the secret space $\mathbb{F}^\lambda$.

2.3. Reduced access structures. In this section, we explain the reduction procedure for access structures, with a certain number of minimal subsets, as it has been introduced in [22]. The optimal information ratio of such access structures is invariant under this reduction.
2.3.1. Notations. In the following, we restate some notation from [22]. For every positive integer \( k \), let \( \mathcal{U}_k = \{0, 1\}^k - \{0^k, 1^k\} \) and, for \( i = 0, \ldots, k - 1 \), let \( \mathcal{U}_k^i = \{ b_{k-1} \ldots b_1 b_0 \in \mathcal{U}_k : b_i = 1 \} \). For a subset \( \mathcal{Q} \subseteq \mathcal{U}_k \) of participants, define the access structure \( \Gamma_k(\mathcal{Q}) \) on \( \mathcal{Q} \) as
\[
\Gamma_k(\mathcal{Q}) = \{ A \subseteq \mathcal{Q} : \mathcal{Q} \cap \mathcal{U}_k^i \subseteq A \text{ for some } i = 0, \ldots, k - 1 \}.
\]
In other words, each of the minimal qualified subsets of \( \Gamma_k(\mathcal{Q}) \) is of the form \( \mathcal{Q} \cap \mathcal{U}_k^i \) for some \( i = 0, \ldots, k - 1 \).

**Example 1.** For \( k = 4 \), we have
\[
\mathcal{U}_4 = \{0001, \ldots, 1110\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E\},
\]
where hexadecimal representation of length-4 binary strings has been used. The subsets \( \mathcal{U}_4^i \) are
\[
\begin{align*}
\mathcal{U}_4^0 &= \{1, 3, 5, 7, 9, B, D\}, \\
\mathcal{U}_4^1 &= \{2, 3, 6, 7, A, B, E\}, \\
\mathcal{U}_4^2 &= \{4, 5, 6, 7, C, D, E\}, \\
\mathcal{U}_4^3 &= \{8, 9, A, B, C, D, E\}.
\end{align*}
\]
It can be verified that for the participant set \( \mathcal{Q} = \{1, 2, 3, 5, 9, C\} \), we have \([\Gamma_4(\mathcal{Q})^-] = 1359 + 23 + 5C + 9C\).

2.3.2. Reduction procedure for access structures. For determining the optimal information ratio of the access structures with at most \( k \) minimal qualified subsets, studying the optimal information ratio of access structures \( \Gamma_k(\mathcal{Q}) \) with \( \mathcal{Q} \subseteq \mathcal{U}_k \) is sufficient [22].

**Definition 8.** Let \( \Gamma \) be an access structure on a set \( \mathcal{Q} \) of participants with exactly \( k \) minimal qualified subsets \( \Gamma^- = \{A_0, A_1, \ldots, A_{k-1}\} \). Consider the set
\[
\mathcal{P} = \{X(p, \Gamma) : p \in \mathcal{Q}\} - \{0^k, 1^k\} \subseteq \mathcal{U}_k,
\]
in which \( X(p, \Gamma) = b_{k-1} \ldots b_1 b_0 \), where \( b_i = 1 \) if \( p \in A_i \), and \( b_i = 0 \) otherwise. The access structure \( \Gamma' = \Gamma_k(\mathcal{P}) \) on the set \( \mathcal{P} \) is called the reduced form of \( \Gamma \). The access structure \( \Gamma' \) is called a reduced access structure if \( \Gamma' \) is isomorphic to \( \Gamma \).

**Proposition 1.** Let \( \Gamma \) be an access structure on a set \( \mathcal{Q} \) with exactly \( k \) minimal qualified subsets and let \( \Gamma' = \Gamma_k(\mathcal{P}) \) be its reduced form. Then, \( \sigma(\Gamma') = \sigma(\Gamma) \).

3. Some remarks on decomposition techniques

In this section, we first draw the reader’s attention to a closer look at the definitions of different decompositions, which to the best of our knowledge, has not been discerned in the literature. Then, we provide a theorem concerning the dual of \((\lambda, \omega)\)-decomposition constructions.

3.1. On using decompositions in their most general form. Most of the papers in the literature refer to a variant of Definition 3 as \( \lambda \)-decomposition, in which the first condition is considered to be \( \Gamma^{j^-} \subseteq \Gamma^- \) instead of \( \Gamma^j \subseteq \Gamma \). Obviously, this variant of the definition is less general and more restrictive. We were only able to spot three papers ([29, 25, 22]) in the literature which had provided the more general definition of the \( \lambda \)-decomposition. Peculiarly, even these papers have restricted themselves to decompositions conforming with the less general definition, when applying the technique in practice. For ease of our reference, we highlight the following observation.
Reduced access structures with four minimal ...

Table 1. An ideal 2-decomposition for $\Gamma = \Gamma_4(\{1, 2, 3, 5, 9, C\})$

| $[\Gamma^-]$ | $\sigma^j$ = $(\sigma^j_p)_{p \in P}$ |
|----------------|---------------------------------|
| $23 + 5C + 9C + 1359$ | $(0, 1, 1, 0, 0, 0)$ |
| $5C + 9C$ | $(0, 0, 0, 1, 1, 1)$ |
| $5C + 1359$ | $(1, 0, 1, 1, 1, 1)$ |
| $23 + 9C + 1359 + 125C$ | $(1, 1, 1, 1, 1, 1)$ |

Observation 1. Applying $\lambda$-decomposition technique by considering the first condition as $\Gamma^j \subseteq \Gamma$ instead of $\Gamma^j^- \subseteq \Gamma^-$ may be beneficial in some cases.

We remark that in practice, instead of checking the condition $\Gamma^j \subseteq \Gamma$, the equivalent condition $\Gamma^j^- \subseteq \Gamma$ is verified. In the following example, we see how Observation 1 leads to finding the optimal information ratio of an access structure using ideal $\lambda$-decomposition, while the restricted definition provably fails to do so.

Example 2 (ideal $\lambda$-decomposition). Consider $\Gamma = \Gamma_4(\{1, 2, 3, 5, 9, C\})$, with minimal access structure $[\Gamma^-] = 1359 + 23 + 5C + 9C$. The best known lower and upper bounds are 3/2 and 5/3, respectively [22]. There are only 15 sub-access structures $\Gamma^j$ with the property that $\Gamma^j^- \subseteq \Gamma^-$, among which only 10 are ideal. By solving a simple linear programming problem, one can verify that the best ideal $\lambda$-decomposition, restricted to using these 10 ideal access sub-structures, leads to optimal information ratio 5/3. This matches with the upper bound reported in [22]. The collection $\{\Gamma^1, \ldots, \Gamma^4\}$, given in Table 1, is an ideal 2-decomposition for $\Gamma$, resulting in an upper bound 3/2 on the optimal information ratio. Notice that $\Gamma^4^- \subseteq \Gamma$ but $\Gamma^4^- \not\subseteq \Gamma^-$, since it includes the non-minimal qualified subset $125C \notin \Gamma^-$. Fortunately, the situation for $(\lambda, \omega)$-decomposition and $\lambda$-weighted-decomposition is more satisfactory. The original papers [33, 30], which have introduced the techniques, as well as the very few papers which have applied them (for example, see [34]), provide consistent definitions (i.e., equivalent to the ones given in Section 2.2). Nevertheless, it seems that a limited view on the definition has been present while applying the technique to actual access structures under study. Further explanation follows.

The definition of $(\lambda, \omega)$-decomposition allows to choose any $\Gamma^j \subseteq 2^P$ as a sub-access structure when decomposing a given access structure $\Gamma$ on $P$. However, in actual applications, the sub-access structures have been chosen as subsets of $\Gamma^- \cup \Gamma^c$. That is, every subset $A \in \Gamma^j$ is included either in $\Gamma^-$ or $\Gamma^c$. Consequently, in most of the cases, many subsets (i.e., those in $\Gamma \setminus \Gamma^-$) have missed the chance to be included in sub-access structures.

Similarly, when decomposing an access structure $\Gamma$ using the weighted-decomposition technique, the definition authorizes any “well-formed” minimal weighted sub-access structure $W^j^- = (W^j_1, \ldots, W^j_n)$ as long as the first condition in Definition 7 is satisfied. Equivalently, $W^j_i$'s are disjoint subsets of $\Gamma$ such that for every $A, B \in \Gamma$, if $A \subseteq B$, $A \in W^j_1$ and $B \in W^j_\ell$, then $\ell > k$. However, in the very few examples of the applications of this technique, $W^j_i$'s have been restricted to be disjoint subsets of $\Gamma^-$. That is, every subset in $\Gamma \setminus \Gamma^-$ is discarded to be included in $W^j_i$'s.
Table 2. An ideal (3,1)-decomposition for \( \Gamma = \Gamma_4(\{1,3,5,A,B,C\}) \)

\[
\begin{array}{c|cc|c}
\hline
\Gamma^- & a_1 \ldots a_4 & b_1 \ldots b_5 & \sigma^j = (\sigma^j_p)_{p \in P} \\
\hline
5C & 1000 & 00000 & (0,0,1,0,0,0) \\
5 + AB & 1111 & 00111 & (0,0,1,1,1,0) \\
C + 3AB + 13B & 1111 & 11000 & (1,1,0,1,1,1) \\
3AB + ABC + 135B + 15BC & 0111 & 00000 & (1,1,1,1,1,1) \\
\hline
\end{array}
\]

Note. Consider an access structure \( \Gamma \) with \( \Gamma^- = \{A_1, \ldots, A_m\} \) and \( \Gamma^+ = \{B_1, \ldots, B_M\} \). Each bit \( a_i \) of binary string \( a_1 \ldots a_m \) in the second column indicates if \( A_i \) is a qualified subset of \( \Gamma_i \); that is, \( a_i = 1 \) iff \( A_i \in \Gamma_i \). Similarly, each bit \( b_j \) of binary string \( b_1 \ldots b_M \) in third column indicates if \( B_j \) is a qualified subset of \( \Gamma^+ \); that is, \( b_j = 1 \) iff \( B_j \in \Gamma^+ \).

Table 3. A 2-weighted-decomposition for \( \Gamma = \Gamma_4(\{3,5,6,9,A,D\}) \)

\[
\begin{array}{c|cc|c}
\hline
\Gamma^- & \Sigma^j & \sigma^j = (\sigma^j_p)_{p \in P} \\
\hline
5C + 3AB + ABC + 135B & \text{Note.} & \text{In } \Sigma^2, \text{the shares of participants are assigned as follows: } s_1 = (r_2 + r_5 - s_1, r_9), \quad s_5 = r_3 + r_4, \quad s_6 = (r_4, r_6), \quad s_8 = r_1 + r_2, \quad s_A = (r_2, r_5 + r_6 + s_2), \quad s_D = (r_3 + s_1, r_1 + s_1). \\
\hline
\end{array}
\]

Of course, the intention of imposing such restrictions in the actual examples of \((\lambda, \omega)\)-decomposition and \(\lambda\)-weighted-decomposition is arguable. Our point is to highlight that considering the more general definition would be more promising. Even though we do not currently have any proof for the superiority of the more general definitions, we have the feeling that the more general definitions could be much more advantageous.

The following two examples illustrate the above points about taking full advantage of the generality of the \((\lambda, \omega)\)-decomposition and \(\lambda\)-weighted-decomposition techniques.

Example 3 (ideal \((\lambda, \omega)\)-decomposition). Consider \( \Gamma = \Gamma_4(\{1,3,5,A,B,C\}) \), with minimal access structure \( \Gamma^- = 5C + 3AB + ABC + 135B \). The best known lower and upper bounds are 3/2 and 5/3, respectively [22]. The collection \( \{\Gamma^1, \ldots, \Gamma^4\} \), given in Table 2, is an ideal \((3,1)\)-decomposition for \( \Gamma \), resulting in an upper bound 3/2 on the optimal information ratio. Notice that \( \Gamma^4 \not\subseteq \Gamma^- \cup \Gamma^+ \) since it includes the non-minimal qualified subset \( 15BC \in \Gamma \setminus \Gamma^- \). We remark that this access structure has an optimal (4,2)-decomposition which conforms to the limited definition.

Example 4 (\(\lambda\)-weighted-decomposition). Consider \( \Gamma = \Gamma_4(\{3,5,6,9,A,D\}) \), with minimal access structure \( \Gamma^- = 359D + 36A + 56D + 9AD \). The best known lower and upper bounds are 3/2 and 5/3, respectively [22]. The collection \( \{W^1, W^2\} \), given in Table 3, is a 2-weighted-decomposition for \( \Gamma \), resulting in an upper bound 3/2 on the optimal information ratio. Let \( W^1 = 1 \times ([W^1^-]) \), where \( [W^1^-] = 359D + 36AD + 56D + 9AD \). Notice that \( W^1^- \not\subseteq \Gamma^- \) since it includes the non-minimal qualified subset \( 36AD \in \Gamma \setminus \Gamma^- \).
3.2. \((\lambda, \omega)\)-decomposition and duality. In this section, we show that the collection of the duals of a \((\lambda, \omega)\)-decomposition for a given access structure \(\Gamma\) renders a \((\lambda', \omega')\)-decomposition for \(\Gamma^*\), which in some cases, it turns out to be a \(\lambda'\)-decomposition.

**Theorem 4.** Let \(\Gamma\) be an access structure on \(\mathcal{P}\) and suppose that \(\{\Gamma^1, \ldots, \Gamma^t\}\) is a \((\lambda, \omega)\)-decomposition of \(\Gamma\). Then, \(\{\Gamma^{1*}, \ldots, \Gamma^{t*}\}\) is a \((t - \omega, t - \lambda)\)-decomposition of \(\Gamma^*\).

**Proof.** Let \(\mathbb{I}(B \in \mathcal{A})\) be the indicator function of the predicate \(B \in \mathcal{A}\); i.e., \(\mathbb{I}(B \in \mathcal{A}) = 1\) if \(B \in \mathcal{A}\), and \(\mathbb{I}(B \in \mathcal{A}) = 0\) otherwise. Since \(\{\Gamma^1, \ldots, \Gamma^t\}\) is a \((\lambda, \omega)\)-decomposition of \(\Gamma\), it holds that: 1) if \(A \in \Gamma^{-}\), then \(\sum_{j=1}^{t} \mathbb{I}(A \in \Gamma^j) \geq \lambda\) and, 2) if \(B \in \Gamma^{+}\), then \(\sum_{j=1}^{t} \mathbb{I}(B \in \Gamma^j) \leq \omega\). To prove the claim, we show that 1) if \(A \in \Gamma^{*-}\), then \(\sum_{j=1}^{t} \mathbb{I}(A \in \Gamma^{j*}) \geq t - \omega\) and, 2) if \(B \in \Gamma^{*+}\), then \(\sum_{j=1}^{t} \mathbb{I}(B \in \Gamma^{j*}) \leq t - \lambda\). We prove the first one. The second one is proved similarly. Let \(A \in \Gamma^{*-}\) and define \(B = \mathcal{P} - A\). Notice that \(B \in \Gamma^{+}\). We have

\[
\sum_{j=1}^{t} \mathbb{I}(A \in \Gamma^{j*}) = \sum_{j=1}^{t} \mathbb{I}(B \in 2^\mathcal{P} \setminus \Gamma^j) = \sum_{j=1}^{t} (1 - \mathbb{I}(B \notin 2^\mathcal{P} \setminus \Gamma^j))
\]

\[
= t - \sum_{j=1}^{t} \mathbb{I}(B \in \Gamma^j) \geq t - \omega. \quad \square
\]

**Corollary 1.** If \(\{\Gamma^1, \ldots, \Gamma^{\lambda}\}\) is a \((\lambda, \omega)\)-decomposition of \(\Gamma\), then \(\{\Gamma^{1*}, \ldots, \Gamma^{\lambda*}\}\) is a \(\lambda'\)-decomposition of \(\Gamma^*\) with \(\lambda' = \lambda - \omega\).

**Corollary 2.** Let \(\Gamma\) be an access structure on \(\mathcal{P}\) and suppose that \(\{\Gamma^1, \ldots, \Gamma^t\}\) is a \((\lambda, \omega)\)-decomposition of \(\Gamma\). Assume that for every \(\Gamma^j, j \in [t]\), there exist a linear secret sharing scheme, based on which, one can construct a secret sharing scheme with convec \(\sigma\) for \(\Gamma\). Then, there exist a \((t - \omega, t - \lambda)\)-decomposition construction for \(\Gamma^*\) with the same convec.

4. Upper bounds on the optimal information ratio

Martí-Farré et al. [22] considered the optimal information ratio of the access structures with four minimal qualified subsets. From Proposition 1, they only consider the optimal information ratio of the reduced access structures of the form \(\Gamma_{4}(\mathcal{P})\) with \(\mathcal{P} \subseteq \mathcal{U}_4\). For several cases, they obtained the exact values of the optimal information ratios, and in the remaining ones, they gave upper and lower bounds. In particular, for the cases of access structures with six participants, the problem was resolved for 44 out of the total 77 non-isomorphic reduced form access structures. In this section, we resolve the problem for all the remaining reduced access structures with six participants, except four cases. More precisely, 14 access structures, appearing in Table 8, correspond to the dual access structures of graph access structures on six participants, except four cases. Additionally, for each of the other 15 access structures we present a secret sharing scheme, using a suitable decomposition technique, with an optimal information ratio matching the lower bounds reported in [22]. The cases that have been resolved by taking Observation 1 into account will be pointed out.

The details of decompositions for \(\mathcal{A}_1, \mathcal{A}_8\) and \(\mathcal{A}_{12}\) have been explained in Example 2, Example 3 and Example 4, respectively, and that of the other access structures can be found in Appendix A.
Table 4. Results obtained by ideal $\lambda$-decomposition

| $P$ | Access Structure | $\sigma$ from [22] | $\sigma$ |
|-----|------------------|---------------------|---------|
| $A_1$ | $12359C$ | $23 + 5C + 9C + 1359$ |          |
| $A_2$ | $12569C$ | $26 + 9C + 159 + 56C$ |          |
| $A_3$ | $13569A$ | $56 + 9A + 36A + 1359$ |          |
| $A_4$ | $1356AC$ | $AC + 135 + 56C + 36A$ |          |
| $A_5$ | $35679A$ | $9A + 567 + 367 + 3579$ |          |
| $A_6$ | $127BCD$ | $17BD + 27B + 7CD + BCD$ | $[5/3,11/6]$ | $5/3$ |

Note. Details of decompositions can be found in Appendix A.1.

Table 5. Result obtained by non-ideal $\lambda$-decomposition

| $P$ | Access Structure | $\sigma$ from [22] | $\sigma$ |
|-----|------------------|---------------------|---------|
| $A_7$ | $167ABD$ | $17BD + 67AB + 67D + ABD$ | $[3/2,5/3]$ | $3/2$ |

Note. Details of decompositions can be found in Appendix A.2.

Table 6. Results obtained by ideal $(\lambda, \omega)$-decomposition

| $P$ | Access Structure | $\sigma$ from [22] | $\sigma$ |
|-----|------------------|---------------------|---------|
| $A_8$ | $135ABC$ | $5C + 3AB + ABC + 135B$ |          |
| $A_9$ | $125ACD$ | $2A + 15D + 5CD + ACD$ |          |
| $A_{10}$ | $136ACE$ | $13 + ACE + 6CE + 36AE$ | $[3/2,5/3]$ | $3/2$ |
| $A_{11}$ | $167ABC$ | $17B + 67C + ABC + 67AB$ |          |

Note. Details of decompositions can be found in Appendix A.3.

**Result 1.** We obtain new upper bounds on the optimal information ratios of each of the access structures, presented in Table 4, using ideal $\lambda$-decomposition technique by considering Observation 1. The access structure $A_5$ and $A_6$ have been handled by applying the technique to their corresponding dual access structures.

**Result 2.** The result for access structure $A_7$ in Table 5 is obtained by applying $\lambda$-decomposition technique to its corresponding dual access structure.

**Result 3.** For each of the access structures in Table 6, the known upper bound on the optimal information ratio is improved by using the $(\lambda, \omega)$-decomposition technique.

**Result 4.** We derive new upper bound on the optimal information ratio of each of the access structures in Table 7, by using $\lambda$-weighted-decomposition technique. The presented results for access structures $A_{14}$ and $A_{15}$ are obtained by applying the technique to their corresponding dual access structures.

**Remark 1.** As it was mentioned above, the results on the access structures $A_5$ - $A_7$ have been obtained by applying a $\lambda$-decomposition technique to their corresponding dual access structures. According to Theorem 4, our decompositions can be translated into $(\lambda, \omega)$-decompositions for the original access structures. Consequently, the translated decompositions fulfill the conditions of Corollary 1.
Table 7. Results obtained by \( \lambda \)-weighted decomposition

| \( \mathcal{P} \) | Access Structure | \( \sigma \) from [22] | \( \sigma \) |
|-----------------|------------------|----------------------|-----|
| \( A_{12} \)    | \( 3569AD \)     | \( 359D + 36A + 56D + 9AD \) |     |
| \( A_{13} \)    | \( 1249AC \)     | \( 19 + 2A + 4C + 9AC \) | \( 3/2, 5/3 \) |
| \( A_{14} \)    | \( 35679E \)     | \( 3579 + 367E + 567E + 9E \) | \( 3/2 \) |
| \( A_{15} \)    | \( 3569BE \)     | \( 359B + 36BE + 56E + 9BE \) | \( 3/2, 7/4 \) |

Note. Details of decompositions can be found in Appendix A.4.

Table 8. Results obtained from the corresponding dual graph access structures

| \( \mathcal{P} \) | Access Structure | \( \cong \Gamma^* \) | \( \sigma \) from [22] | \( \sigma \) |
|-----------------|------------------|----------------------|----------------------|-----|
| \( 167BDE \)    | \( 17BD + 67BE + 6D + 7BE + BDE \) | \( \cong \Gamma_{14}^* \) | \( 3/2 , 5/3 \) | \( 14, 32 \) |
| \( 356BDE \)    | \( 35BD + 36BE + 56DE + BDE \) | \( \cong \Gamma_{10}^* \) | \( 3/2, 7/4 \) | \( 139 \) |
| \( 357AC \)     | \( 357 + 37AB + 57C + ABC \) | \( \cong \Gamma_{13}^* \) | \( 3/2, 11/6 \) | \( 139 \) |
| \( 37BCDE \)    | \( 37BD + 37BE + 7CDE + BCDE \) | \( \cong \Gamma_{10}^* \) | \( 3/2, 11/6 \) | \( 139 \) |
| \( 125ADE \)    | \( 15D + 2AE + 5DE + ADE \) | \( \cong \Gamma_{12}^* \) | \( 5/3, 7/4 \) | \( 139 \) |
| \( 135ADE \)    | \( 135D + 3AE + 5DE + ADE \) | \( \cong \Gamma_{16}^* \) | \( 5/3, 11/6 \) | \( 139 \) |
| \( 137BCE \)    | \( 137B + 37BE + 7C + BCE \) | \( \cong \Gamma_{16}^* \) | \( 5/3, 11/6 \) | \( 139 \) |
| \( 124BDE \)    | \( 1BD + 2BE + 4DE + BDE \) | \( \cong \Gamma_{12}^* \) | \( 7/4, 11/6 \) | \( 139 \) |
| \( 125BDE \)    | \( 1BD + 2BE + 5DE + BDE \) | \( \cong \Gamma_{12}^* \) | \( 7/4, 11/6 \) | \( 139 \) |
| \( 135BDE \)    | \( 135BD + 3BE + 5DE + BDE \) | \( \cong \Gamma_{12}^* \) | \( 7/4, 11/6 \) | \( 139 \) |
| \( 136BDE \)    | \( 13BD + 36BE + 6DE + BDE \) | \( \cong \Gamma_{12}^* \) | \( 7/4, 11/6 \) | \( 139 \) |
| \( 137BDE \)    | \( 137BD + 37BE + 7DE + BDE \) | \( \cong \Gamma_{12}^* \) | \( 7/4, 11/6 \) | \( 139 \) |

Note 1. For all the 14 access structures given in Table 8, the corresponding dual access structures are graph access structures on six participants. The reported upper bounds in Table 8 have been presented in [32, 30, 15, 14].

5. Conclusion

Stinson’s \( \lambda \)-decomposition, and its variants, are powerful methods to compute an upper bound on the optimal information ratio of an access structure, using some sub-access structures with known secret sharing schemes. Two variants of the Stinson’s definition can be found in the literature based on the property that sub-access structures must fulfill: 1) each sub-access structure must be a subset of the given access structure 2) each minimal sub-access structure must be a subset of the given minimal access structure. Despite the fact that the former variant is more general than the latter one, to the best of our knowledge, all known examples of decompositions are applications of the second variant. Surprisingly, the first definition can be found only in very few references.
We argued that regarding the extensions of Stinson’s method, i.e., \((\lambda, \omega)\)-decomposition and \(\lambda\)-weighted-decomposition, even though the definitions are consistent in the literature — capturing the most general form —, a similar restriction might have been in mind when applying these techniques in practice as well.

In this paper, we showed that the more general definitions are probably much more advantageous than their restricted counterparts, by considering the access structures with exactly four minimal qualified subsets on six participants. Some of these access structures had remained unsolved in [22]. We have resolved all of them, except four cases, given in Table 9.

We remark that two of the four unsolved access structures are duals of two graph access structures on six participants which have been left open for a long time [32]. Moreover by using improved LP-technique in [12], for each of them, the known lower bound on optimal information ratio over all linear schemes has been improved to \(8/5\).

**ACKNOWLEDGMENTS**

The authors would like to thank the anonymous reviewers for their constructive and valuable comments that greatly contributed to improving the quality and presentation of the paper. The first author has been supported by Iranian National Science Foundation (INSF) under postdoc program contract no. 94027246. The second author has been supported by Sharif Industrial Relation Office (SIRO) under grant no. G931223.

**REFERENCES**

[1] A. Beimel, Secret-sharing schemes: a survey, in *Int. Conf. Coding Crypt.*, Springer, 2011, 11–46.

[2] A. Beimel, A. Ben-Efraim, C. Padró and I. Tyomkin, Multi-linear secret-sharing schemes, in *Theory of Cryptography Conference*, Springer, Berlin, 2014, 394–418.

[3] G. R. Blakley, Safeguarding cryptographic keys, in *Proceedings of the 1979 AFIPS National Computer Conference*, Monval, NJ, USA, AFIPS Press, 1979, 313–317.

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

[5] C. Blundo, A. De Santis, R. D. Simone and U. Vaccaro, Tight bounds on the information rate of secret sharing schemes, *Des. Codes Crypt.*, 11 (1997), 107–122.

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

[7] R. M. Capocelli, A. D. Santis, L. Gargano and U. Vaccaro, On the size of shares for secret sharing schemes, *J. Cryptology*, 6 (1993), 157–167.

[8] L. Csirmaz, An impossibility result on graph secret sharing, *Des. Codes Crypt.*, 53 (2009), 195–209.

[9] L. Csirmaz, Secret sharing on the d-dimensional cube, *Des. Codes Crypt.*, 74 (2015), 719–729.
Reduced access structures with four minimal subsets

[10] L. Csirmaz and G. Tardos, Optimal information rate of secret sharing schemes on trees, *IEEE Trans. Inf. Theory*, 59 (2013), 2527–2530.

[11] O. Farràs, T. B. Hansen, T. Kaced and C. Padró, Optimal non-perfect uniform secret sharing schemes, in *Int. Crypt. Conf.*, Springer, Berlin, 2014, 217–234.

[12] O. Farràs, T. Kaced, S. Martin and C. Padro, Improving the linear programming technique in the search for lower bounds in secret sharing, Cryptology ePrint Archive, Report 2017/919, 2017; available at https://eprint.iacr.org/2017/919.

[13] O. Farràs, J. R. Metcalf-Burton, C. Padró and L. Vázquez, On the optimization of bipartite secret sharing schemes, *Des. Codes Crypt.*, 63 (2012), 255–271.

[14] M. Gharahi and M. H. Dehkordi, Perfect secret sharing schemes for graph access structures on six participants, *J. Math. Crypt.*, 7 (2013), 143–146.

[15] M. Gharahi and M. H. Dehkordi, The complexity of the graph access structures on six participants, *Des. Codes Crypt.*, 67 (2013), 169–173.

[16] M. Ito, A. Saito and T. Nishizeki, Secret sharing scheme realizing general access structure, *Electr. Commun. Japan (Part III: Fandam. Electr. Sci.)*, 72 (1989), 56–64.

[17] W.-A. Jackson and K. M. Martin, Geometric secret sharing schemes and their duals, *Des. Codes Crypt.*, 4 (1994), 83–95.

[18] W.-A. Jackson and K. M. Martin, Perfect secret sharing schemes on five participants, *Des. Codes Crypt.*, 9 (1996), 267–286.

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

[20] J. Martí-Farré and C. Padró, Secret sharing schemes with three or four minimal qualified subsets, *Des. Codes Crypt.*, 34 (2005), 17–34.

[21] J. Martí-Farré and C. Padró, Secret sharing schemes on access structures with intersection number equal to one, *Discrete Appl. Math.*, 154 (2006), 552–563.

[22] J. Martí-Farré, C. Padró and L. Vázquez, Optimal complexity of secret sharing schemes with four minimal qualified subsets, *Des. Codes Crypt.*, 61 (2011), 167–186.

[23] K. M. Martin, New secret sharing schemes from old, *J. Combin. Math. Combin. Comp.*, 14 (1993), 65–77.

[24] C. Padró and G. Sáez, Secret sharing schemes with bipartite access structure, *IEEE Trans. Inf. Theory*, 46 (2000), 2596–2604.

[25] C. Padró and G. Sáez, Lower bounds on the information rate of secret sharing schemes with homogeneous access structure, *Inf. Process. Lett.*, 83 (2002), 345–351.

[26] C. Padró, L. Vázquez and A. Yang, Finding lower bounds on the complexity of secret sharing schemes by linear programming, *Discrete Appl. Math.*, 161 (2013), 1072–1084.

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

[28] D. R. Stinson, An explication of secret sharing schemes, *Des. Codes Crypt.*, 2 (1992), 357–390.

[29] D. R. Stinson, Decomposition constructions for secret-sharing schemes, *IEEE Trans. Inf. Theory*, 40 (1994), 118–125.

[30] H.-M. Sun and B.-L. Chen, Weighted decomposition construction for perfect secret sharing schemes, *Comp. Math. Appl.*, 43 (2002), 877–887.

[31] H.-M. Sun, H. Wang, B.-H. Ku and J. Pieprzyk, Decomposition construction for secret sharing schemes with graph access structures in polynomial time, *SIAM J. Discrete Math.*, 24 (2010), 617–638.

[32] M. Van Dijk, On the information rate of perfect secret sharing schemes, *Des. Codes Crypt.*, 6 (1995), 143–169.

[33] M. Van Dijk, W.-A. Jackson and K. M. Martin, A general decomposition construction for incomplete secret sharing schemes, *Des. Codes Crypt.*, 15 (1998), 301–321.

[34] M. Van Dijk, T. Kevenaar, G.-J. Schrijen and P. Tuyls, Improved constructions of secret sharing schemes by applying ($\lambda$, $\omega$)-decompositions, *Inf. Process. Lett.*, 99 (2006), 154–157.

Received March 2017; revised August 2017.

E-mail address: gharahi.motahhareh@gmail.com
E-mail address: shahram.khazaei@sharif.ir
Appendix A. Details of decomposition constructions

A.1. Ideal λ-decompositions. We provide the details of our decomposition for the access structure in Table 4.

- \( \mathcal{A}_2 = \Gamma_4(\{1, 2, 5, 6, 9, C\}) \)

| \([\Gamma^-]\) | \(\sigma' = (\sigma'_p)_{p \in P}\) |
|----------------|-----------------|
| 26             | (0, 1, 0, 1, 0, 0) |
| 159 + 9C       | (1, 0, 1, 0, 1, 1) |
| 56C + 9C       | (0, 0, 1, 1, 1, 1) |
| 159 + 26 + 56C + 129C | (1, 1, 1, 1, 1, 1) |

- \( \mathcal{A}_3 = \Gamma_4(\{1, 3, 5, 6, 9, A\}) \)

| \([\Gamma^-]\) | \(\sigma' = (\sigma'_p)_{p \in P}\) |
|----------------|-----------------|
| 36A + 56       | (0, 1, 1, 1, 0, 1) |
| 1359 + 36A + 9A + 156 | (1, 1, 1, 1, 1, 1) |
| 1359 + 56 + 9A + 136A | (1, 1, 1, 1, 1, 1) |

- \( \mathcal{A}_4 = \Gamma_4(\{1, 3, 5, 6, 9, A, C\}) \)

| \([\Gamma^-]\) | \(\sigma' = (\sigma'_p)_{p \in P}\) |
|----------------|-----------------|
| 36A + AC       | (0, 1, 0, 1, 1, 1) |
| 135 + 36A + 56C + 1AC | (1, 1, 1, 1, 1, 1) |
| 135 + 56C + AC + 136A | (1, 1, 1, 1, 1, 1) |

- \( \mathcal{A}_5 = \Gamma_4(\{3, 5, 6, 7, 9, A\}) \)

| \([\Gamma^-]\) | \(\sigma' = (\sigma'_p)_{p \in P}\) |
|----------------|-----------------|
| 5A             | (0, 1, 0, 0, 0, 1) |
| 69 + 79        | (0, 0, 1, 1, 1, 0) |
| 69 + 5A + 7A + 359 + 36A + 379 | (1, 1, 1, 1, 1, 1) |
| 79 + 7A + 359 + 36A + 35A + 369 | (1, 1, 1, 1, 1, 1) |

- \( \mathcal{A}_6 = \Gamma_4(\{1, 2, 7, B, C, D\}) \)

| \([\Gamma^-]\) | \(\sigma' = (\sigma'_p)_{p \in P}\) |
|----------------|-----------------|
| 7B             | (0, 0, 1, 1, 0, 0) |
| 12C            | (1, 1, 0, 0, 1, 0) |
| 7D + 2D        | (0, 1, 1, 0, 0, 1) |
| 2D + BD        | (0, 1, 0, 1, 0, 1) |
| 7C + 12C       | (1, 1, 1, 0, 1, 0) |
| 2D + BC + 12C + 1BD | (1, 1, 0, 1, 1, 1) |
| 7B + 7C + 7D + BC + BD | (0, 0, 1, 1, 1, 1) |
| 7B + 7C + 7D + BC + BD | (0, 0, 1, 1, 1, 1) |
A.2. Non-ideal $\lambda$-decompositions. We provide the details of our decomposition for the access structure in Table 5.

- $A_7 = \Gamma_4(\{1, 6, 7, A, B, D\})$

\[
[A_7^-] = 7A + 7B + 7D + 6B + BD + 6D + AD + 16A
\]

| $[\Gamma^-]$ | $\Sigma^1$ | $\sigma^1 = (\sigma^1_p)_{p \in \mathcal{P}}$ |
|-------------|-------------|----------------------------------|
| $6D + AD$   | (0, 1, 0, 1, 0, 1) |
| $7A + 7B + 7D + 6B + BD + 6D + 16A + 1AD$ | (1, 1, 2, 1, 1, 1) |
| $7A + 7B + 7D + 6B + BD + AD + 16A + 16D$ | (1, 1, 1, 1, 1, 1) |

Note. In $\Sigma^2$, the shares of participants are assigned as follows: $s_1 = r_1 + r_2$, $s_0 = r_2$, $s_7 = (r_1, r_2), s_A = r_1 + s, s_B = r_2 - s, s_D = r_2 + s$. We point out that $\Gamma^2 \not\equiv \Gamma^3$.

A.3. Ideal $(\Lambda, \omega)$-decompositions. We provide the details of our decompositions for each of the access structures in Table 6.

- $A_9 = \Gamma_4(\{1, 2, 5, A, C, D\})$

\[
[A_9^-] = 2A + 15D + 5CD + ACD
\]

| $[\Gamma^-]$ | $a_1 \ldots a_4$ | $b_1 \ldots b_6$ | $\sigma^1 = (\sigma^1_p)_{p \in \mathcal{P}}$ |
|-------------|----------------|----------------|----------------------------------|
| $2A$        | 1000           | 000000         | (0, 1, 0, 1, 0)                   |
| $5 + A$     | 1111           | 111101         | (0, 0, 1, 1, 0, 0)                |
| $15D + CD$  | 0111           | 000010         | (1, 0, 1, 0, 1, 1)                |
| $2A + ACD$  | 1001           | 000000         | (0, 1, 0, 1, 1, 1)                |
| $15D + 5CD$ | 0110           | 000000         | (1, 0, 1, 0, 1, 1)                |

- $A_{10} = \Gamma_4(\{1, 3, 6, A, C, E\})$

\[
[A_{10}^-] = 13 + ACE + 6CE + 36AE
\]

| $[\Gamma^-]$ | $a_1 \ldots a_4$ | $b_1 \ldots b_7$ | $\sigma^1 = (\sigma^1_p)_{p \in \mathcal{P}}$ |
|-------------|----------------|----------------|----------------------------------|
| $13$        | 1000           | 00000000       | (1, 1, 0, 0, 0, 0)                |
| $3 + C$     | 1111           | 1111011        | (0, 1, 0, 1, 1, 0)                |
| $13 + 36AE$ | 1001           | 00000000       | (1, 1, 1, 0, 1)                   |
| $ACE + 6CE$ | 0110           | 00000000       | (0, 0, 1, 1, 1, 1)                |
| $ACE + 6CE + 6AE$ | 0111 | 00000000 | (0, 0, 1, 1, 1, 1)                |

- $A_{11} = \Gamma_4(\{1, 6, 7, A, B, C\})$

\[
[A_{11}^-] = 17B + 67C + ABC + 67AB
\]

| $[\Gamma^-]$ | $a_1 \ldots a_4$ | $b_1 \ldots b_8$ | $\sigma^1 = (\sigma^1_p)_{p \in \mathcal{P}}$ |
|-------------|----------------|----------------|----------------------------------|
| $17 + 76$   | 1101           | 11000001       | (1, 1, 1, 0, 0, 0)                |
| $17B + ABC$ | 1010           | 00000000       | (1, 1, 0, 1, 1, 1)                |
| $1B + AB + 6C$ | 1111 | 00111010 | (1, 1, 0, 1, 1) |
| $67C + ABC + 67AB$ | 0111 | 00000000 | (0, 1, 1, 1, 1, 1) |
A.4. Weighted $\lambda$-decompositions. We provide the details of our decompositions for each of the access structures in Table 7.

- $A_{13} = \Gamma_4(\{1, 2, 4, 9, A, C\})$

| $[A_{13}^+] = 19 + 2A + 4C + 9AC$ | $\Sigma^j$ | $\sigma^j = (\sigma^j_p)_{p \in P}$ |
|-----------------------------------|---------|---------------------------------|
| $1 \times (2A)$                   | $\Sigma^1$ | $(0, 1, 0, 1, 0)$               |
| $1 \times (4C)$                   |          | $(0, 0, 1, 0, 1)$               |
| $1 \times (2A + 4C) + 2 \times (19 + 9AC)$ | $\Sigma^3$ | $(2, 1, 1, 3, 2, 2)$            |

**Note.** In $\Sigma^3$, the shares of participants are assigned as follows: $s_1 = (r_1 + r_2 + r_3 + r_4, r_5)$, $s_2 = r_4 + s_1$, $s_4 = r_1 + s_2$, $s_0 = (r_1 + r_3 + s_2, r_2 + r_4 + s_1, r_5 + s_2)$, $s_A = (r_3, r_4)$, $s_C = (r_1, r_2)$.

- $A_{14} = \Gamma_4(\{3, 5, 6, 7, 9, E\})$

| $[A_{14}^+] = 69 + 79 + 3E + 5E + 7E + 9E + 359$ | $\Sigma^j$ | $\sigma^j = (\sigma^j_p)_{p \in P}$ |
|-----------------------------------------------|---------|---------------------------------|
| $1 \times (69 + 79 + 359)$                   | $\Sigma^1$ | $(1, 1, 1, 1, 1, 0)$             |
| $1 \times (69 + 79 + 359) + 2 \times (3E + 5E + 7E + 9E)$ | $\Sigma^2$ | $(2, 2, 1, 2, 3)$               |

**Note.** In $\Sigma^2$ the shares of participants are assigned as follows: $s_1 = (r_1, r_2 + r_3)$, $s_5 = (r_1, r_3)$, $s_6 = r_2, s_7 = (r_1 + r_2, r_3), s_9 = (r_1, r_2 + s_1), s_E = (r_1 + s_1, r_2 + r_3 + s_2)$.

- $A_{15} = \Gamma_4(\{3, 5, 6, 9, B, E\})$

| $[A_{15}^+] = 69 + 5B + 6B + 3E + 5E + 9E + BE + 359$ | $\Sigma^j$ | $\sigma^j = (\sigma^j_p)_{p \in P}$ |
|-----------------------------------------------|---------|---------------------------------|
| $1 \times (3E + 5E + 9E)$                   | $\Sigma^1$ | $(1, 1, 0, 1, 0, 1)$             |
| $1 \times (69 + 5B + 6B + 359)$             | $\Sigma^2$ | $(1, 1, 2, 1, 0)$               |
| $1 \times (69 + 5B + 6B + 3E + 5E + 9E + 359) + 2 \times (BE)$ | $\Sigma^3$ | $(1, 1, 1, 1, 2, 2)$            |

**Note.** The shares of participants in $\Sigma^2$ are assigned as follows: $s_3 = r_1 + r_2 + s$, $s_5 = r_3, s_6 = (r_1 + s, r_2), s_9 = r_1, s_B = r_2 + s$, and in $\Sigma^3$, they are assigned as follows: $s_3 = r_1 + r_2 - s_1, s_5 = r_2, s_6 = r_1 - s_1, s_9 = r_1, s_B = (r_1, r_2 - s_1), s_E = (r_1 - s_1, r_2 + s_2)$. 