ELSEVIER

Information Processing Letters 65 (1998) 25-32

Information Processing Letters

On secret sharing schemes

Carlo Blundo *, Alfredo De Santis [1], Ugo Vaccaro [2]

Dipartimento di Informatica ed Applicazioni, Università di Salerno, 84081 Baronissi (SA), Italy

Received 18 August 1997
Communicated by W.M. Turski

Abstract

A secret sharing scheme is a protocol to share a secret s among a set of participants $\mathcal{P}$ in such a way that only qualified subsets of $\mathcal{P}$ can reconstruct the value of s whereas any other subset of $\mathcal{P}$, non-qualified to know s, cannot determine anything about the value of the secret. In this paper we prove that the entropy of the shares of any non-qualified set is independent from the probability distribution according to which the secret is chosen. This result implies that several recent bounds on the shares' size and on the randomness required to construct secret sharing schemes can be strengthened. © 1998 Elsevier Science B.V.

Keywords: Cryptography; Safety/security in digital systems; Secret sharing

1. Introduction

A secret sharing scheme is a protocol to distribute shares of a secret s among a set of participants $\mathcal{P}$ in such a way that only qualified subsets of $\mathcal{P}$ can reconstruct the value of s whereas any other subset of $\mathcal{P}$, non-qualified to know s, cannot determine anything about the value of the secret.

The problem of establishing bounds on the size of the shares to be given to participants in secret sharing schemes is one of the basic problem in the area and has received considerable attention by several researchers (see [4-7,11,12,14,15,18,21,22]). The practical relevance of this issue is based on the following observations: Firstly, the security of any system tends to degrade as the amount of information that must be kept secret, i.e., the shares of the participants, increases. Secondly, if the shares given to participants are too long, the memory requirements for the participants will be too severe and, at the same time, the shares distribution algorithms will become inefficient. Therefore, it is important to derive significant upper and lower bounds on the shares' size for classes of access structures. (An access structure is a family of all subsets of $\mathcal{P}$ which are qualified to recover the secret.) It is well known that the shares' size of any non-qualified set of participants must be at least the entropy of the secret [12,17].

* Corresponding author. Email: carblu@dia.unisa.it.

[1] Email: ads@dia.unisa.it.

[2] Email: uv@dia.unisa.it.

PII S0020-0190(97)00194-4

The survey by Stinson [20] contains a unified description of results in the area of secret sharing schemes. The reader can also profitably see the book [23]. For an updated bibliography on secret sharing schemes we refer the reader to [24]; while, for different approaches to the study of secret sharing schemes, for schemes with "extended capabilities" such as disenrollment, fault tolerance, and pre-positioning we recommend the survey article by Simmons [19].

The first result we prove in this paper is that given an access structure $\mathcal{A}$, any secret sharing scheme for $\mathcal{A}$ with secret chosen in S according to a *fixed* probability distribution is also a secret sharing scheme for $\mathcal{A}$ for *any* probability distribution on S. Moreover, we prove that the entropy of the shares of any non-qualified set of participants is independent from the probability distribution according to which the secret is chosen. This has as immediate consequence that the shares' size of any non-qualified set of participants is at least $\log|S|$. Our results imply that the bounds on the share's size and on the randomness required to construct secret sharing schemes given in [2-6,8,9,12,14,15] can all be strengthened, as well as results on key distribution schemes such as the ones in [1]. Our results also imply an improvement over the main result of the recent paper [18].

2. Secret sharing schemes

A secret sharing scheme permits a secret to be shared among a set $\mathcal{P}$ of n participants in such a way that only qualified subsets of $\mathcal{P}$ can recover the secret, but any non-qualified subset has absolutely no information on the secret. An access structure $\mathcal{A}$ is the set of all subsets of $\mathcal{P}$ that can recover the secret.

Definition 1. Let $\mathcal{P}$ be a set of participants, a *monotone* access structure $\mathcal{A}$ on $\mathcal{P}$ is a subset $\mathcal{A} \subseteq 2^{\mathcal{P}} \setminus \{\emptyset\}$, such that $A \in \mathcal{A}$, $A \subseteq A' \subseteq P \Rightarrow A' \in \mathcal{A}$.

If $\mathcal{A}$ is an access structure on $\mathcal{P}$, then $B \in \mathcal{A}$ is a *minimal* qualified subset if $A \notin \mathcal{A}$ whenever $A \subset B$. The set of minimal qualified subsets of $\mathcal{A}$ is denoted by $\mathcal{A}^0$ and is called the *basis* of $\mathcal{A}$. A monotone access structure $\mathcal{A}$ is uniquely determined as a function of $\mathcal{A}^0$, since we have $\mathcal{A} = \{B \subseteq \mathcal{P} \mid A \subseteq B,\ A \in \mathcal{A}^0\}$. We say that $\mathcal{A}$ is the *closure* of $\mathcal{A}^0$ and write $\mathcal{A} = \mathrm{cl}(\mathcal{A}^0)$. All access structures considered in this paper are monotone.

A participant $P \in \mathcal{P}$ is an *essential* participant of $\mathcal{A}$ if there exists a set $X \in \mathcal{A}^0$ such that $P \in X$. If a participant P is not essential then we can construct a secret sharing scheme giving him nothing as his share. In fact, a non-essential participant does not need to participate "actively" in the reconstruction of the secret, since the information he has is not needed by any set in $\mathcal{P}$ in order to recover the shared secret. Therefore, we assume throughout this paper that all participants are essential, i.e., $\mathcal{P} = \bigcup_{A \in \mathcal{A}^0} A$.

In the following with S we denote the set of secrets; whereas, with $\mathbf{S}$ we denote the random variable taking values in S according to the probability distribution $\{\Pr_S(s)\}_{s\in S}$. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ and let a secret sharing scheme Σ for secrets in S be fixed. For any participant $P \in \mathcal{P}$, let us denote by $K(P)$ the set of all possible shares given to participant P. Suppose a *dealer* D wants to share the secret $s \in S$ among the participants in $\mathcal{P}$ (we will assume that $D \notin \mathcal{P}$). He does this by giving each participant $P \in \mathcal{P}$ a share from $K(P)$ chosen according to some, not necessarily uniform, probability distribution. A secret sharing scheme can be viewed as a collection of distribution rules, see [23] and [4] for details. Given a set of participants $A = \{P_{i_1}, \ldots, P_{i_r}\} \subseteq \mathcal{P}$, with $i_1 < \cdots < i_r$, let $K(A) = K(P_{i_1}) \times \cdots \times K(P_{i_r})$.

Any secret sharing scheme for secrets in S and a probability distribution $\{\Pr_S(s)\}_{s\in S}$ naturally induces a probability distribution on $K(A)$, for any $A \subseteq \mathcal{P}$. Denote this probability distribution by $\{\Pr_{K(A)}(a)\}_{a\in K(A)}$. With $\mathbf{A}$ we denote the random variable taking value on $K(A)$ according to $\{\Pr_{K(A)}(a)\}_{a\in K(A)}$. Finally, denote by $H(\mathbf{S}) = -\sum_{s\in S} \Pr_S(s) \log \Pr_S(s)$ the entropy of $\{\Pr_S(s)\}_{s\in S}$ and by $H(\mathbf{A})$ the entropy of $\{\Pr_{K(A)}(a)\}_{a\in K(A)}$, for any $A \subseteq \mathcal{P}$.

In terms of the probability distribution on the secrets and on the shares given to participants, we say that a secret sharing scheme is a *perfect* secret sharing scheme with secrets chosen according to $\mathbf{S}$, or simply a secret sharing scheme with secrets chosen according to S, for the access structure $\mathcal{A} \subseteq 2^{\mathcal{P}}$ if

(1) *Any subset $A \subseteq \mathcal{P}$ of participants enabled to recover the secret can compute the secret*: If $A \in \mathcal{A}$, then for all $a \in K(A)$ with $\Pr_{K(A)}(a) > 0$ there exists a unique secret $s \in S$ such that $\Pr(s \mid a) = 1$.

(2) *Any subset $A \subseteq \mathcal{P}$ of participants not enabled to recover the secret has no information on the secret value*: If $A \notin \mathcal{A}$, then for all $s \in S$ and for all $a \in K(A)$, it holds that $\Pr(s \mid a) = \Pr_S(s)$.

Property (1) means that the value of the shares held by $A \in \mathcal{A}$ completely determines the secret $s \in S$. Notice that property 2 means that the probability that the secret is equal to s given that the shares held by $A \notin \mathcal{A}$ are a, is the same as the a priori probability of the secret s. Therefore, no amount of knowledge of shares of participants not qualified to reconstruct the secret enables a Bayesian opponent to modify an a priori guess regarding which the secret is. Thus, property (2) means that random variables $\boldsymbol{S}$ and $\boldsymbol{A}$ are statistically independent.

Using Shannon's notion of entropy,[3] the above conditions can be restated as

(1′) for all $A \in \mathcal{A}$, $H(\boldsymbol{S} \mid \boldsymbol{A}) = 0$.

(2′) for all $A \notin \mathcal{A}$, $H(\boldsymbol{S} \mid \boldsymbol{A}) = H(\boldsymbol{S})$,

where

$$H(\boldsymbol{S} \mid \boldsymbol{A}) = -\sum_{a \in K(A)} \sum_{s \in S} \Pr_{K(A)}(a) \Pr(s \mid a) \log \Pr(s \mid a)$$

is the conditional entropy of $\boldsymbol{S}$ given $\boldsymbol{A}$.

3. The size of the shares

In this section we will prove that if Σ is a secret sharing scheme for a *fixed* probability distribution on the set of secrets S, then Σ is a secret sharing scheme for *any* probability distribution on S.

Intuitively, since property (2′) states that $\boldsymbol{A}$ and $\boldsymbol{S}$ are statistically independent then, any change in the probability distribution on S does not affect the conditional probability distribution of $\boldsymbol{S}$ given $\boldsymbol{A}$. Hence, properties (1′) and (2′) remain true independent of the probability distribution on S. We now formalize this intuition.

Let $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{S}$ be three random variables satisfying $H(\boldsymbol{S} \mid \boldsymbol{AB}) = 0$ and $H(\boldsymbol{S} \mid \boldsymbol{A}) = H(\boldsymbol{S} \mid \boldsymbol{B}) = H(\boldsymbol{S})$. Let $\boldsymbol{X}$ be a random variable taking values on X, with support$(\boldsymbol{X})$ we denote the set of values of X with positive probability, that is, support$(\boldsymbol{X}) = \{x \in X \mid \Pr(\boldsymbol{X} = x) > 0\}$. Assume for the rest of the paper that $\Pr(\boldsymbol{S} = s) > 0$ for all $s \in S$ (i.e., $S = \text{support}(\boldsymbol{S})$). Let $\boldsymbol{S}'$ be an arbitrary random variable defined on support$(\boldsymbol{S})$. Let $\boldsymbol{A}'$ and $\boldsymbol{B}'$ be the random variables taking values on the same supports as $\boldsymbol{A}$ and $\boldsymbol{B}$, respectively, with joint probability distribution

$$\Pr(\boldsymbol{A}' = a, \boldsymbol{B}' = b, \boldsymbol{S}' = s) = \Pr(\boldsymbol{A} = a, \boldsymbol{B} = b \mid \boldsymbol{S} = s) \Pr(\boldsymbol{S}' = s). \tag{1}$$

Clearly, support$(\boldsymbol{AB})$ = support$(\boldsymbol{A}'\boldsymbol{B}')$. The following lemma holds.

Lemma 2. *Let $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{S}$ be three random variables satisfying $H(\boldsymbol{S} \mid \boldsymbol{AB}) = 0$ and $H(\boldsymbol{S} \mid \boldsymbol{A}) = H(\boldsymbol{S} \mid \boldsymbol{B}) = H(\boldsymbol{S})$. The random variables $\boldsymbol{A}'$, $\boldsymbol{B}'$, and $\boldsymbol{S}'$ defined by* (1) *satisfy*

(1) $H(\boldsymbol{S}' \mid \boldsymbol{A}'\boldsymbol{B}') = 0$,

(2) $H(\boldsymbol{S}' \mid \boldsymbol{A}') = H(\boldsymbol{S}' \mid \boldsymbol{B}') = H(\boldsymbol{S}')$,

(3) $H(\boldsymbol{A}') = H(\boldsymbol{A})$ *and* $H(\boldsymbol{B}') = H(\boldsymbol{B})$,

(4) $H(\boldsymbol{A}' \mid \boldsymbol{B}'\boldsymbol{S}') = H(\boldsymbol{A} \mid \boldsymbol{BS})$ *and* $H(\boldsymbol{B}' \mid \boldsymbol{A}'\boldsymbol{S}') = H(\boldsymbol{B} \mid \boldsymbol{AS})$.

[3] For information-theoretic background we refer the reader to [13].

Proof. First, we prove that $H(\mathbf{S}' \mid \mathbf{A}'\mathbf{B}') = 0$. For arbitrary values of s, a, and b we have that

$$\begin{aligned}
&\Pr(\mathbf{A} = a, \mathbf{B} = b \mid \mathbf{S} = s) \cdot \Pr(\mathbf{S}' = s) \\
&\quad = \Pr(\mathbf{A}' = a, \mathbf{B}' = b, \mathbf{S}' = s) \\
&\quad = \Pr(\mathbf{S}' = s \mid \mathbf{A}' = a, \mathbf{B}' = b) \cdot \Pr(\mathbf{A}' = a, \mathbf{B}' = b) \\
&\quad = \Pr(\mathbf{S}' = s \mid \mathbf{A}' = a, \mathbf{B}' = b) \sum_{r \in S} \Pr(\mathbf{A}' = a, \mathbf{B}' = b \mid \mathbf{S}' = r) \cdot \Pr(\mathbf{S}' = r) \\
&\quad = \Pr(\mathbf{S}' = s \mid \mathbf{A}' = a, \mathbf{B}' = b) \sum_{r \in S} \Pr(\mathbf{A} = a, \mathbf{B} = b \mid \mathbf{S} = r) \cdot \Pr(\mathbf{S}' = r).
\end{aligned}$$

Since $H(\mathbf{S} \mid \mathbf{AB}) = 0$ then, for any pair $(a, b) \in A \times B$ satisfying $\Pr(\mathbf{A} = a, \mathbf{B} = b) > 0$, there exists a unique $s \in S$ such that $\Pr(\mathbf{A} = a, \mathbf{B} = b \mid \mathbf{S} = s) > 0$. Hence, for some function f such that $s = f(a, b)$, we get

$$\begin{aligned}
\Pr(\mathbf{S}' = s \mid \mathbf{A}' = a, \mathbf{B}' = b) &= \frac{\Pr(\mathbf{A} = a, \mathbf{B} = b \mid \mathbf{S} = s) \cdot \Pr(\mathbf{S}' = s)}{\Pr(\mathbf{A} = a, \mathbf{B} = b \mid \mathbf{S} = f(a,b)) \cdot \Pr(\mathbf{S}' = f(a,b))} \\
&= \begin{cases} 0 & \text{if } s \neq f(a,b), \\ 1 & \text{if } s = f(a,b). \end{cases}
\end{aligned}$$

Therefore, we obtain that $H(\mathbf{S}' \mid \mathbf{A}'\mathbf{B}') = 0$ which proves property (1) Now, we prove that property (2) is satisfied. Since $H(\mathbf{S} \mid \mathbf{A}) = H(\mathbf{S})$, we have $\Pr(\mathbf{A} = a \mid \mathbf{S} = s) = \Pr(\mathbf{A} = a)$ from which we obtain that

$$\begin{aligned}
\Pr(\mathbf{A}' = a \mid \mathbf{S}' = s) &= \sum_{b \in B'} \Pr(\mathbf{A}' \doteq a, \mathbf{B}' = b \mid \mathbf{S}' = s) \\
&= \sum_{b \in B} \Pr(\mathbf{A} = a, \mathbf{B} = b \mid \mathbf{S} = s) \\
&= \Pr(\mathbf{A} = a \mid \mathbf{S} = s) = \Pr(\mathbf{A} = a). \qquad (2)
\end{aligned}$$

This implies that $\Pr(\mathbf{A}' = a \mid \mathbf{S}' = s)$ does not depend on the value of s. Hence, $\mathbf{A}'$ and $\mathbf{S}'$ are independent (i.e., $H(\mathbf{S}' \mid \mathbf{A}') = H(\mathbf{S}')$). Thus, $\Pr(\mathbf{A}' = a \mid \mathbf{S}' = s) = \Pr(\mathbf{A} = a)$ and so we obtain that $\Pr(\mathbf{A}' = a) = \Pr(\mathbf{A} = a)$. Therefore, $H(\mathbf{A}') = H(\mathbf{A})$. Analogously, we can prove that $H(\mathbf{S}' \mid \mathbf{B}') = H(\mathbf{B}')$ and $H(\mathbf{B}') = H(\mathbf{B})$. Therefore, properties (2) and (3) hold. Property (4) follows from (2) by observing that

$$\begin{aligned}
&\Pr(\mathbf{B}' = b \mid \mathbf{A}' = a\ \mathbf{S}' = s) \cdot \Pr(\mathbf{A}' = a \mid \mathbf{S}' = s) \\
&\quad = \Pr(\mathbf{A}' = a, \mathbf{B}' = b \mid \mathbf{S}' = s) \\
&\quad = \Pr(\mathbf{A} = a, \mathbf{B} = b \mid \mathbf{S} = s) \\
&\quad = \Pr(\mathbf{B} = b \mid \mathbf{A} = a, \mathbf{S} = s) \cdot \Pr(\mathbf{A} = a \mid \mathbf{S} = s). \qquad \square
\end{aligned}$$

It is worthwhile to notice that in the proof of the above lemma we have also showed that $\mathbf{A} = \mathbf{A}'$ and $\mathbf{B} = \mathbf{B}'$, that is, they have the same support and the same probability distribution, which is indeed stronger than property (3) of Lemma 2.

Theorem 3. *Let $\mathcal{A}$ be an access structure on a set of participants $\mathcal{P}$. If Σ is a secret sharing scheme for $\mathcal{A}$ with secrets chosen according to $\mathbf{S}$, then Σ is a secret sharing scheme for $\mathcal{A}$ with secrets chosen according to $\mathbf{S}'$, where $\mathbf{S}'$ is any random variable defined on S.*

Proof. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the set of participants and let $\mathbf{P}'_1, \ldots, \mathbf{P}'_n$ be the random variables taking the same values as $\mathbf{P}_1, \ldots, \mathbf{P}_n$, respectively, and with joint probability distribution

$$\Pr(P'_1 = p_1, \ldots, P'_n = p_n, S' = s) = \Pr(P_1 = p_1, \ldots, P_n = p_n \mid S = s) \cdot \Pr(S' = s).$$

Clearly, for any $X = \{P_{i_1}, \ldots, P_{i_j}\} \subseteq \mathcal{P}$, we have that support$(X)$ = support(X'), where $X' = P'_{i_1} \ldots P'_{i_j}$. By Lemma 2 we have $H(S' \mid X') = 0$ if $X \in \mathcal{A}$ and $H(S' \mid X') = H(S')$ if $X \notin \mathcal{A}$. Therefore, the scheme Σ constitutes a secret sharing scheme for $\mathcal{A}$ with secrets chosen according to S' and the lemma is proved. □

The next two corollaries are immediate consequences of Lemma 2 and Theorem 3.

Corollary 4. *Let $\mathcal{A}$ be an access structure on a set of participants $\mathcal{P}$, let ϕ be a non-decreasing function, and let χ be a function. If there exist sets $X_1, \ldots, X_m \in 2^{\mathcal{P}} \setminus \mathcal{A}$ such that for any S and for any secret sharing scheme for $\mathcal{A}$ for secrets chosen according to S it holds that $\chi(H(X_1), \ldots, H(X_m)) \geqslant \phi(H(S))$, then for any S and for any secret sharing scheme for $\mathcal{A}$ for secrets chosen according to S we have $\chi(H(X_1), \ldots, H(X_m)) \geqslant \phi(\log|S|)$.*

Proof. Let $\mathcal{A}$ be an access structure on a set of participants $\mathcal{P}$ and let $X_1, \ldots, X_m \in 2^{\mathcal{P}} \setminus \mathcal{A}$. Let S' be an arbitrary random variable defined on support(S). As done in Theorem 3 define the random variables $P'_1, \ldots, P'_n$, taking the same values as $P_1, \ldots, P_n$, respectively, and with joint probability distribution

$$\Pr(P'_1 = p_1, \ldots, P'_n = p_n, S' = s) = \Pr(P_1 = p_1, \ldots, P_n = p_n \mid S = s) \cdot \Pr(S' = s).$$

Recall that if $X = \{P_{i_1}, \ldots, P_{i_j}\} \subseteq \mathcal{P}$, then with X' we denote the random variable $X' = P'_{i_1} \ldots P'_{i_j}$. From Lemma 2 we get $H(X_i) = H(X'_i)$, for $i = 1, \ldots, m$. Therefore,

$$\chi(H(X_1), \ldots, H(X_m)) = \chi(H(X'_1), \ldots, H(X'_m)) \geqslant \phi(H(S')).$$

The inequality $\chi(H(X_1), \ldots, H(X_m)) \geqslant \phi(H(S'))$ holds for any probability distribution on S' and in particular for the uniform one. Therefore, we get $\chi(H(X_1), \ldots, H(X_m)) \geqslant \phi(\log|S|)$ which proves the corollary. □

Corollary 4 implies that the results in [1,2,4,3,6,5,8,9,12,14,15] can all be strengthened. As an example consider the bound proved by Csirmaz [14]. He showed that for any integer $k \geqslant 2$, there exists an access structure $\mathcal{AS}$ on a set $\mathcal{P}$ of $k + 2^k - 2$ participants and k participants $P_1, \ldots, P_k \in 2^{\mathcal{P}} \setminus \mathcal{AS}$, such that $H(P_1) + \cdots + H(P_k) \geqslant (2^k - 1)H(S)$. In such a case, for a fixed k, the function χ is $\chi(z_1, \ldots, z_k) = z_1 + \cdots + z_k$, whereas, the function $\phi(z)$ is $\phi(z) = (2^k - 1)z$. From Corollary 4 we can improve on the above mentioned bound to $H(P_1) + \cdots + H(P_k) \geqslant (2^k - 1)\log|S|$. Therefore, there exists a $P \in \{P_1, \ldots, P_k\}$ such that $H(P) \geqslant \frac{2^k-1}{k}\log|S|$. As another example of the application of Corollary 4 consider the access structure $\mathcal{A} = \mathrm{cl}(\{\{P_1, P_2\}, \{P_2, P_3\}, \{P_3, P_4\}\})$. The main result of [18] is: If $|K(P_1)| = |K(P_4)| = |S|$, then $\log|K(P_2)| + \log|K(P_3)| \geqslant 3\log|S|$. From Corollary 4 we can improve on this bound to $H(P_2) + H(P_3) \geqslant 3\log|S|$. Such bound holds even if $|K(P_1)| \neq |S|$ or $|K(P_4)| \neq |S|$. In such a case the function χ is $\chi(z_1, z_2)) = z_1 + z_2$ and in [12] the inequality $H(P_2) + H(P_3) \geqslant 3H(S)$ was proved to hold for any S and for any secret sharing scheme for $\mathcal{A}$.

The next immediate corollary was profitably used in [9] to derive lower bounds on the amount of randomness needed by secret sharing schemes.

Corollary 5. *Let $\mathcal{A}$ be an access structure on a set of participants $\mathcal{P}$ and let ϕ be a non-decreasing function. If there exists a set $X \in 2^{\mathcal{P}} \setminus \mathcal{A}$ such that for any S and for any secret sharing scheme for $\mathcal{A}$ for secrets chosen according to S it holds that $H(X) \geqslant \phi(H(S))$, then the entropy $H(X)$ satisfies $H(X) \geqslant \phi(|S|)$.*

It is well known (see [12,17]) that $H(P) \geqslant H(S)$ for any $P \in \mathcal{P}$. This bound is tight if $\{P\} \in \mathcal{A}$. The following theorem shows an improvement whenever $\{P\} \notin \mathcal{A}$.

Theorem 6. *Let $\mathcal{A}$ be an access structure on a set of participants $\mathcal{P}$ and let Σ be a secret sharing scheme for $\mathcal{A}$ for secrets chosen according to $\boldsymbol{S}$. If there are $\{P\}, X \in 2^{\mathcal{P}} \setminus \mathcal{A}$ such that $\{P\} \cup X \in \mathcal{A}$, then*

$$H(\boldsymbol{P}) \geqslant \log|S| + H(\boldsymbol{P} \mid \boldsymbol{XS}).$$

Proof. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the set of participants. Let Σ be a secret sharing scheme for $\mathcal{A}$ with secrets chosen according to $\boldsymbol{S}$. From Theorem 3 it follows that Σ is a secret sharing scheme with secrets chosen according to $\boldsymbol{S}'$, where $\boldsymbol{S}'$ is any random variable defined on S. Let $\{P\}, X \notin \mathcal{A}$ be such that $\{P\} \cup X \in \mathcal{A}$. Then using the same notation as in Theorem 3, by Lemma 2 we get $H(\boldsymbol{P}) = H(\boldsymbol{P}')$, $H(\boldsymbol{S}' \mid \boldsymbol{X}') = H(\boldsymbol{S}')$, and $H(\boldsymbol{P}' \mid \boldsymbol{X}'\boldsymbol{S}') = H(\boldsymbol{P} \mid \boldsymbol{XS})$. Therefore,

$$\begin{aligned} H(\boldsymbol{P}) &= H(\boldsymbol{P}') \\ &\geqslant H(\boldsymbol{P}' \mid \boldsymbol{X}') \\ &= H(\boldsymbol{S}' \mid \boldsymbol{X}') - H(\boldsymbol{S}' \mid \boldsymbol{P}'\boldsymbol{X}') + H(\boldsymbol{P}' \mid \boldsymbol{X}'\boldsymbol{S}') \\ &\qquad (\text{as } H(\boldsymbol{S}' \mid \boldsymbol{X}') + H(\boldsymbol{P}' \mid \boldsymbol{X}'\boldsymbol{S}') = H(\boldsymbol{P}' \mid \boldsymbol{X}') + H(\boldsymbol{S}' \mid \boldsymbol{X}'\boldsymbol{P}')) \\ &= H(\boldsymbol{S}') + H(\boldsymbol{P}' \mid \boldsymbol{X}'\boldsymbol{S}') \\ &= H(\boldsymbol{S}') + H(\boldsymbol{P} \mid \boldsymbol{XS}). \end{aligned}$$

Then by choosing $\boldsymbol{S}'$ to be uniform, we have

$$H(\boldsymbol{P}) \geqslant \log|S'| + H(\boldsymbol{P} \mid \boldsymbol{XS}) = \log|S| + H(\boldsymbol{P} \mid \boldsymbol{XS})$$

which proves the theorem. □

It is well known that for any $P \in \mathcal{P}$, with $\{P\} \notin \mathcal{A}$, we have $|K(P)| \geqslant |S|$. This bound can be proved by counting arguments. The following theorem proves a better bound.

Theorem 7. *Let $\mathcal{A}$ be an access structure on a set of participants $\mathcal{P}$ and let Σ be a secret sharing scheme for $\mathcal{A}$ for secrets chosen according to $\boldsymbol{S}$. If there are $\{P\}, X \in 2^{\mathcal{P}} \setminus \mathcal{A}$ such that $\{P\} \cup X \in \mathcal{A}$, then*

$$H(\boldsymbol{P}) \geqslant \log|S|,$$

with equality if and only if $|K(P)| = |S|$.

Proof. From Theorem 6 we have that $H(\boldsymbol{P}) \geqslant \log|S|$. Hence, the first part of the theorem is proved. Suppose that $|K(P)| = |S|$. We have $\log|S| = \log|K(P)| \geqslant H(\boldsymbol{P}) \geqslant \log|S|$. Hence, $H(\boldsymbol{P}) = \log|S|$. Now, we prove that $H(\boldsymbol{P}) = \log|S|$ implies $|K(P)| = |S|$. Theorem 3 implies that a secret sharing scheme with secret chosen in S according to a fixed probability distribution is also a secret sharing scheme with secret chosen according to $\boldsymbol{S}'$, where $\boldsymbol{S}'$ is a uniformly distributed random variable with the same sample space as $\boldsymbol{S}$. This implies that the size of the set $K(P)$ does not change when the secret is chosen according to $\boldsymbol{S}'$. Therefore, without loss of generality we assume that $H(\boldsymbol{S}) = \log|S|$, that is, the secret is uniformly chosen. From Theorem 6 and from $H(\boldsymbol{P}) = \log|S|$ we get $H(\boldsymbol{P} \mid \boldsymbol{XS}) = 0$; whereas from $H(\boldsymbol{P} \mid \boldsymbol{X}) = H(\boldsymbol{S}) + H(\boldsymbol{P} \mid \boldsymbol{XS})$ and from $H(\boldsymbol{P} \mid \boldsymbol{XS}) = 0$ we obtain $H(\boldsymbol{P} \mid \boldsymbol{X}) = H(\boldsymbol{S})$. From $H(\boldsymbol{P}) = \log|S|$ and $H(\boldsymbol{P} \mid \boldsymbol{X}) = H(\boldsymbol{S}) = \log|S|$ we derive that $H(\boldsymbol{P} \mid \boldsymbol{X}) = H(\boldsymbol{P})$. Hence $\boldsymbol{P}$ and $\boldsymbol{X}$ are independent. Now, fix an $x \in K(X)$. From the independence of $\boldsymbol{X}$ and $\boldsymbol{P}$ and from $H(\boldsymbol{S} \mid \boldsymbol{XP}) = H(\boldsymbol{P} \mid \boldsymbol{XS}) = 0$ we derive that for any $p \in K(P)$ there exists an unique $s \in S$ such that $\Pr(\boldsymbol{P} = p, \boldsymbol{S} = s \mid \boldsymbol{X} = x) > 0$ and vice versa. Thus, $|K(P)| = |S|$ which proves the theorem. □

Theorem 6 states that for any access structure $\mathcal{A}$ the relation $H(\boldsymbol{P}) \geqslant \log|S| + H(\boldsymbol{P} \mid \boldsymbol{XS})$ holds for any $\{P\}, X \in 2^{\mathcal{P}} \setminus \mathcal{A}$ such that $\{P\} \cup X \in \mathcal{A}$. Since $H(\boldsymbol{P}) = \log|S|$, for any $P \in \mathcal{P}$, is the optimal situation we refer to such a scheme as an *ideal* scheme. Theorem 7 implies that in any ideal scheme the probability distribution on the shares given to participants is uniform.

Recent work on definitions of ideal scheme in [16] showed (in their notation) that secret sharing schemes as defined in [10] (so-called BD-schemes), [11] (BS schemes) and information theoretically defined schemes (IT schemes) had a hierarchical relationship with BD most general and BS most specialised. However under the definitions of ideal for these models the hierarchy paradoxically altered to put BD at the top and IT at the bottom. Under this new definition of ideal for IT schemes (i.e., $H(\boldsymbol{P}) = \log|S|$, for any $P \in \mathcal{P}$), the expected hierarchy is restored for the ideal case, namely BD at the top and BS at the bottom.

In [12] the authors showed how to construct secret sharing schemes for the access structure $\mathcal{T} = \{\{A, B\}\}$, such that $H(\boldsymbol{A}) = H(\boldsymbol{B}) = H(\boldsymbol{S})$, where support$(\boldsymbol{S}) = \{0, 1\}$ and $\Pr(\boldsymbol{S} = 0) = p$ and $\Pr(\boldsymbol{S} = 1) = 1 - p$, $p \leqslant 1/2$. According to Theorem 7 their construction is correct only in the case $p = 1/2$. Moreover, Theorem 4.3 in [12] has to be modified as follows.

Theorem 8. *Let $\mathcal{A}$ be an access structure on a set of participants $\mathcal{P}$. If there are $\{P\}, X \in 2^{\mathcal{P}} \setminus \mathcal{A}$ such that $\{P\} \cup X \in \mathcal{A}$, then there exists a secret sharing scheme for $\mathcal{A}$ with secret chosen according to $\boldsymbol{S}$ such that $H(\boldsymbol{P}) = \log|S|$.*

Clearly, the previous theorem holds also when $\{P\} \in \mathcal{A}$, but it is immediate to see that if $\{P\} \in \mathcal{A}$, then we can easily construct a secret sharing scheme in which $H(\boldsymbol{P}) = H(\boldsymbol{S})$.

References

[1] C. Blundo, A. Cresti, Space requirements for broadcast encryption, in: EUROCRYPT 94, Lecture Notes in Computer Science, vol. 950, Springer, Berlin, 1995, pp. 287-298.

[2] C. Blundo, A. Cresti, A. De Santis, U. Vaccaro, Fully dynamic secret sharing schemes, Theoret. Comput. Sci. 165 (1996) 407-440.

[3] C. Blundo, A. Giorgio Gaggia, D.R. Stinson, On the dealer's randomness required in secret sharing schemes, Designs, Codes and Cryptography 11 (2) (1997) 107-122.

[4] C. Blundo, A. De Santis, R. De Simone, U. Vaccaro, Tight bounds on the information rate of secret sharing schemes, Designs, Codes and Cryptography 11 (1) (1997) 1-25.

[5] C. Blundo, A. De Santis, L. Gargano, U. Vaccaro, On the information rate of secret sharing schemes, Theoret. Comput. Sci. 154 (1996) 283-306.

[6] C. Blundo, A. De Santis, A. Giorgio Gaggia, U. Vaccaro, New bounds on the information rate of secret sharing schemes, IEEE Trans. Inform. Theory 41 (1995) 549-554.

[7] C. Blundo, A. De Santis, D.R. Stinson, U. Vaccaro, Graph decomposition and secret sharing schemes, J. Cryptology 8 (1995) 39-64.

[8] C. Blundo, A. De Santis, U. Vaccaro, Efficient sharing of many secrets, in: STACS 93, Lecture Notes in Computer Science, vol. 665, Springer, Berlin, 1993, pp. 692-703.

[9] C. Blundo, A. De Santis, U. Vaccaro, Randomness in distribution protocols, Inform. and Comput. 131 (2) (1996) 111-139.

[10] E.F. Brickell, D.M. Davenport, On the classification of ideal secret sharing schemes, J. Cryptology 4 (2) (1991) 123-124.

[11] E.F. Brickell, D.R. Stinson, Some improved bounds on the information rate of perfect secret sharing schemes, J. Cryptology 5 (3) (1992) 153-166.

[12] R.M. Capocelli, A. De Santis, L. Gargano, U. Vaccaro, On the size of shares for secret sharing schemes, J. Cryptology 6 (3) (1993) 157-169.

[13] T.M. Cover, J.A. Thomas, Elements of Information Theory, John Wiley & Sons, New York, 1991.

[14] L. Csirmaz, The size of a share must be large, in: A. De Santis (Ed.), Advances in Cryptology - Eurocrypt'94, Lecture Notes in Computer Science, vol. 950, Springer, Berlin, 1995, pp. 13-22.

[15] M. van Dijk, On the information rate of perfect secret sharing schemes, Design, Codes and Cryptography 6 (1995) 143-169.

[16] W.A. Jackson, K.M. Martin, Combinatorial models for perfect secret sharing schemes, J. Combin. Math. Combin. Comput. (to appear).

[17] E.D. Karnin, J.W. Greene, M.E. Hellman, On secret sharing systems, IEEE Trans. Inform. Theory 29 (1) (1983) 35-41.

[18] K. Kurosawa, K. Okada, Combinatorial lower bounds for secret sharing schemes, Inform. Process. Lett. 60 (1996) 301-304.

[19] G.J. Simmons, An introduction to shared secret and/or shared control schemes and their application, in: Contemporary Cryptology, IEEE Press, 1991, pp. 441-497.

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

[21] D.R. Stinson, New general lower bounds on the information rate of secret sharing schemes, in: CRYPTO 92, Lecture Notes in Computer Science, vol. 740, Springer, Berlin, 1993, pp. 170–184.

[22] D.R. Stinson, Decomposition constructions for secret sharing schemes, IEEE Trans. Inform. Theory 40 (1994) 118–125.

[23] D.R. Stinson, Cryptography Theory and Practice, CRC Press, Inc., Boca Raton, FL, 1995.

[24] D.R. Stinson, Bibliography on secret sharing, available on-line as http://bibd.unl.edu/~stinson/ssbib.html.