On Identification Secret Sharing Schemes

Ning Cai

Departmant of Information Engineering

The Chinese University of Hong Kong

Shatin, N. T., Hong Kong[1]

*e-mail:*ncai@ie.cuhk.edu.hk

Kwok Yan Lam

School of Computing

National University of Singapore

Lower Kent Ridge Road, Singapore 119260

e-mail: lamky@comp.nus.edu.sg

[1]The work was done when the author was with School of Computing, National University of Singapore.

Running head: **Identification Secret Sharing**

Corresponding Author:

Ning Cai

Departmant of Information Engineering

The Chinese University of Hong Kong

Shatin, N. T.,

Hong Kong

Abstract: Let $\mathcal{P}$ be a set of participants sharing a secret from a set of secrets. A secret sharing scheme is a protocol such that any qualified subset of $\mathcal{P}$ can determine the secret by pooling their shares, the messages which they receive, whereas non-qualified subsets of $\mathcal{P}$ cannot obtain any knowledge about the secret when they pooling what they receive. In (optimal) schemes, the sizes of shared secrets depend on the sizes of shares given to the participants. Namely the former is growing up exponentially as the latter is increasing exponentially.

In this paper, instead of determining the secret, we require the qualified subsets of participants to identify the secret. This changing allows us to share a set of secrets with double exponential sizes as the sizes of shares received by the participants are exponentially increasing. Thus much longer secret can be shared. We obtain the characterizations of their relations. Our idea originates from Ahlswede-Dueck's awarded work in 1989, where the identification codes via channels were introduced.

Index Terms: Identification, secret sharing, public message.

0 :	Zero
$\mathcal{A}$:	Script A
$\mathcal{P}$:	Script P
$\mathcal{Q}$:	Script Q
$\mathcal{S}$:	Script S
$\mathcal{X}$:	Script X
α :	Greek Alpha
δ :	Greek delta
ϵ :	Greek epsilon
θ :	Greek theta
λ :	Greek lambda
μ :	Greek mu
ϕ :	Greek phi

1 Introduction

A secret sharing scheme is a method of sharing a secret s from a finite set $\mathcal{S}$ of secrets among a finite set $\mathcal{P}$ of the paticipants in such a way that only so-called qualified subsets of $\mathcal{P}$ are able to reconstruct s whereas any other subsets of $\mathcal{P}$ should know absolutely nothing about s. To do this for a given $s \in \mathcal{S}$, the dealer, a special participant who is not in $\mathcal{P}$ and observes the secret s, distributes the "shares", messages chosen according to certain probability, to the paticipants in $\mathcal{P}$. A subset of the participants in $\mathcal{P}$ try to reconstruct s, by pooling their shares which they receive from the dealer. The subsets of $\mathcal{P}$ are distinguished to qualified and non-qualified subsets. The qualified subsets should be able to reconstruct s (without error) whereas the non-qualified subsets should have no knowledge about s. The collection of qualified susets is called access structure. Such a scheme usually called perfect secret sharing scheme. In this paper we only consider this kind of schemes and simply call them secret sharing schemes.

The first secret sharing schemes, (k, m) threshold schemes were introduced by G. R. Blakley [4] and A. Shamir [10] independently. They proved that to share a set of secrets with size q it is sufficient to give every participant $\log q$ bits, where q is a power of a prime not smaller than k, and here and throughout the paper the bases of all logarithms are 2. In a (k, m) threshold scheme, the cardinality of set $\mathcal{S}$ of participants is m and a subset A of participants is qualified iff $|A| \geq k$. The schemes are optimal in the sense that for fixed size $|\mathcal{S}|$, the information which each participant has to receive is the least possible. Actually it is easy to show in any secret sharing scheme, every participant must receive at least $\log |\mathcal{S}|$ bits share. Such a secret sharing scheme is called ideal.

The ideal secret sharing scheme does not always exist. (Please c. f. [5] for the conditions of existence of ideal secret sharing schemes in terms of matroids and [6] for examples where the ideal secret sharing scheme does not exist). However, for any access structure there exists a constant c such that it is sufficient to give each participant at most $c \log |\mathcal{S}|$ bits in an optimal scheme. That is, the sizes of shares given to the participants are exponentially increasing when the sizes of secrets shared are exponentially increasing.

The model of identification via channels was introduced by R. Ahlswede and G. Dueck [2] based on the following fact. In many cases, the receivers of channels only are interested in whether a special message was sent but not in which message was sent (and the senders do not know which message they are interested in). For example, a man was injured in an accident on a high way. The people whose relatives were driving on the high way only want to know if the poor man is their relatives. If not, they do not care who he is. The behaviour of transmission and identification via channels are very different. The well known Shannon Theorem [11] says that an optimal transmission code of length n carries asymptotically nC bits of information whereas it was shown in [2] that with an optimal identification code asymptotic 2^{nC} bits of information can be identified. Here C is the well known Shannon capacity. That means that the identification can be much faster done than transmission. So far the coding problem for the identification via channels has become a important and fruitful area in information theory. (For example, see [7] and [12]). A recent work by R. Ahlswede [1] provides many new ideas, problems, and results related identification. This opens a new area of the theory of information transfer.

We observe that similar things may happen in the secret sharing. Sometimes a subset of participants may be interested only in whether the dealer's secret is a special one but not what it is. In other words, instead to reconstruct it, they want to identify it. We represent such an example at the beginning of the Section 3. Similarly, a "secret sharing scheme" to require the qualified subsets to identify the secret, which will be called an identification secret sharing scheme, can "share" much more secrets than that to require to reconstruct it. We show that a set of secrets with double exponential size can be identified if the size of shares given to the participants exponentially increases. Thus much more secrets can be shared.

Our results are very similar to that in [3] in the following two points. (Please c. f. [3] or [1] for the details.)

-The (optimal) second order information rate for identification does not equal to the first order information rate for reconstruction.

-The rate of identification is equal to the size of common randomness.

In fact a hashing idea there is used by us to construct the identification secret sharing scheme.

We also consider the case in which the public message is allowed. That is the dealer's message divided to two parts, public message, which is broadcasted to all participants, and secret messages, or shares which are distributed to each participant privately. We show that the sizes of shares given by dealer are independent of the sizes of shared secrets if the quantity of public message is unlimited.

In the next section we present the necessary background of secret sharing schemes. Our model and results are stated in Section 3. The converse and direct theorems are proved in Sections 4 and 5, respectively.

2 Background

In this section, let us briefly review the definition of the secret sharing scheme. A few equivalent definitions have been given by the different authors. We present here a definition in terms of Shannon entropy [9], [6]. The other definitions, for example, can be found in [13].

Denote by $[J] := \{1, \dots, J\}$, for a positive integer J and $\mathcal{X}_A := \mathcal{X}_{j_1} \times \mathcal{X}_{j_2} \times \dots \times \mathcal{X}_{j_l}$ for $A := \{j_1, j_2, \dots j_l\} \subset [J]$ $(j_1 \leq j_2 \dots \leq j_l)$ and a given collection of finite sets $\mathcal{X}_1, \dots, \mathcal{X}_J$. Analogously we denote by $X_A := (X_{j_1}, \dots, X_{j_l})$ for a given sequence of random variables (RV) $(X_1, \dots, X_J)$. We also write a sequence in $\mathcal{X}_A$ as x_A, $\mathcal{X}^j := \mathcal{X}_{[j]}$, and $X^j := X_{[j]}$ and so on. Moreover the probability distribution of

RV Y and its conditional distribution under the condition that RV Z is given are denoted by P_Y and $P_{Y|Z}$ respectively. A collection $\mathcal{A}$ of subsets of a finite set $\mathcal{P}$ is monotone or an upset if $A \supset B \in \mathcal{P}$ implies $A \in \mathcal{A}$.

Let $\mathcal{S}$ be a finite set, the set of secrets. A set of participants sharing a secret from $\mathcal{S}$ is a finite set $\mathcal{P} := [J]$. In this paper for the simplicity of the notation, an integer $j \in [J]$, instead of P_j like to in the most other papers, stands for the jth participant in $\mathcal{P}$. An access structure $\mathcal{A}$ on $\mathcal{P}$ is a monotone collection of subsets in $\mathcal{P}$. A subset $A \subset \mathcal{P}$ is called qualified iff $A \in \mathcal{A}$ and otherwise A is non-qualified. A useful fact is that a monotone collection $\mathcal{A}$ of subsets is determined by the collection of its minimal subsets, $\mathcal{A}_0 := \{A : A \in \mathcal{A}$ and there is no $A' \in \mathcal{A}$ with $A' \subset A\}$. A secret sharing scheme is a way to distribute messages, the so-called shares, according to a secret $s \in \mathcal{S}$ such that the members of a qualified subset of $\mathcal{P}$ are able to reconstruct s by pooling the shares which they receive whereas the members of a non-qualified subsets have absolutely no knowledge about s when they pool what they receive. The distribution is done by a special participant, the dealer, who is not in $\mathcal{P}$. The secret sharing scheme can be defined in terms of Shannon entropy as follows.

For given a secret source, a RV S taking values in a finite set $\mathcal{S}$ of secrets, a set $\mathcal{P} = [J]$ of participants, and an access structure $\mathcal{A}$, a secret sharing scheme is specified by a stochastic matrix $W : \mathcal{S} \longrightarrow \mathcal{X}^J$ (a conditional probability distribution over a J-dimension cartesian product of finite sets $\mathcal{X}_j, j \in [J]$, under the condition that the secret $S = s$ is given) such that

i) For all $A \in \mathcal{A}$,

$$H(S|X_A) = 0, \tag{1}$$

ii) For all $A \notin \mathcal{A}$,

$$H(S|X_A) = H(S), \tag{2}$$

where $\mathcal{X}^J := \mathcal{X}_1 \times \ldots \times \mathcal{X}_J$ for any finite sets $\mathcal{X}_j, j = 1, \ldots, J$ and (say) $\mathcal{P} :=$ $[J]$, $H(.)$ and $H(.|.)$ are entropy and conditional entropy respectively, and $X^J :=$

$(X_1, \ldots, X_J)$ be the RV introduced by $P_S \times W$ i.e., for all $s \in \mathcal{S}$ and $x^J \in \mathcal{X}^J$, $P_{SX^J}(s, x^J) = P_S(s)W(x^J|s)$. Let us call $(\mathcal{X}_1, \ldots, \mathcal{X}_J)$ $(\mathcal{X}_j)$ the alphabet of $\mathcal{P}$ (the participant j) for W. Notice that the condition i) is equivalent to that the support sets $supp(P_{X_A|S}(.|s)) := \{x_A : P_{X_A|S}(x_A|s) > 0, x_A \in \mathcal{X}_A\}, s \in \mathcal{S}$ are pairwise disjoint or in other words for any $x_A \in \mathcal{X}_A$ there is at most one $s \in \mathcal{S}$ with $P_{X_A|S}(x_A|s) > 0$ for all $A \in \mathcal{A}$. The condition ii) is equivalent to that S and X_A are independent i. e., for all $A \notin \mathcal{A}, s \in \mathcal{S}$ and $x_A \in \mathcal{X}_A$

$$P_{S|X_A}(s|x_A) = P_S(s). \tag{3}$$

For given a W, the scheme works as follows. The dealer, who wants to share a secret $s \in \mathcal{S}$, chooses $x^J \in \mathcal{X}^J$ randomly according to the conditional distribution $W(.|s)$ and distributes the "shares", the message $x_j, j = 1, \ldots, J$ to the participant $j \in \mathcal{P}$ privately, (i.e. gives the participant j the message x_j). After receiving the shares, a subset A of participants pool their shares $x_j, j \in A$ to obtain a sequence $x_A \in \mathcal{X}_A$ and try to reconstruct s from x_A. In the case that $A \in \mathcal{A}$, there is unique $s' \in \mathcal{S}$ with $P_{X_A|S}(x_A|s') > 0$ and so they know with probability one that $s = s'$. On the other hand, (2) implies that x_A may not give any information about the secret if $A \notin \mathcal{A}$.

The assumption of montonicity of the access structure is necessary because the condition i) implies that for a "non-monotone access structure" secret sharing scheme nerve exists. On the other hand it was shown in [8] that for all (monotone) access structure the secret sharing schemes exist. Without loss of generality, we assume there is no participant $j \in \mathcal{P}$ with $\{j\} \in \mathcal{A}$ (since we can simply give such a participant the complete secret $S = s$) nor with $\{j\} \cup A \notin \mathcal{A}$ for all $A \subset \mathcal{P}$ (since in this case we can simply give nothing to such a j). We also assume that in the sequel all considered secret sources S have $P_S(s) > 0$ for all $s \in \mathcal{S}$ (since we can simply remove the secret of zero probability from $\mathcal{S}$). Then it is easy to show that for any secret source S , any $j \in \mathcal{P}$, and any secret scheme, $\log|\mathcal{X}_j| \geq \log|\mathcal{S}|$. On the other hand, one can always construct a secret sharing scheme with $\log |\mathcal{X}_j| \leq c \log |\mathcal{S}|$ (for all $j \in \mathcal{P}$) for a constant c depending only on the access structure $\mathcal{A}$ but not on $\mathcal{S}$ (please c. f. [8] or [14]). Usually we want that $\max_{j \in \mathcal{P}} |\mathcal{X}_j|$ as small as possible and call a scheme with minimum $\max_{j \in \mathcal{P}} |\mathcal{X}_j|$ optimal. Thus for any given access structure there is a constant c such that for all $\mathcal{S}$ (and any secret source S on it) and the optimal secret scheme for it,

$$\log |\mathcal{S}| \leq \log |\mathcal{X}_j| \leq c \log |\mathcal{S}|, \tag{4}$$

for all $j \in \mathcal{P}$.

3 The Models and the Results

Before defining our new model, the identification secret sharing(IDSS) scheme formally, let us consider an example. Suppose a company produces q kinds of products, which are labeled by $s = 0, 1, \ldots, q-1$, and has J potential customers. The company wants to sell a kind of products only when at least k customers intend to buy them. Otherwise for certain trade security reason, it even does not want the customers to know what it is going to sell. For this purpose, the company can apply a (k, J) threshold secret scheme for the set $\mathcal{S} := \{0, 1, \ldots, q-1\}$ of secrets when it is going to sell a kind of products labeled by $s \in \mathcal{S}$. If $l \geq k$ customers are interested in its products, they can pool their shares and determine the s, what the company is going to sell. However in the case that only $l < k$ customers intend to buy its products they have absolutely no idea about what it wants to sell even when they cooperate by pooling their shares. Here we assume the customers have to pay for using their sharing so that there is no reason for a customer who does not want to buy anything to contribute his/her share. According to the scheme, the company (or the dealer) has to give each potential customer (the participant) $\log q$ bits for the share. It may cost "a lot" when q is very large. Can it be done better? The answer seems "certainly" to be negative since the scheme that it uses is already optimal. However we notice that it often happens that a customer may only be interested in one kind of its products but not in all of them. In other words the customers only want to "identify" whether the products interesting for them will be sold and do not care what will be sold in the other case. This leaves a room for us to improve the protocol. It is clear that in the case, that only $l < k$ customers would like to buy $s_0 \in \mathcal{S}$, those customers never have a chance to buy them and so they can do nothing for their interests. In the case the number of customers interested in s_0 is not less than k they can identify whether s_0 will be sold by the cooperation among them and do not need the cooperation from the others. So we can assume only those who want to buy the same products may cooperate. This example leads us to the following model.

Given a finite set $\mathcal{S}$ of secrets (the sets of the indices of the products in the example), a set $\mathcal{P} = [J]$ of participants (the potential customers in the example), an access structure $\mathcal{A}$, or a collection of so-called qualified subsets of $\mathcal{P}$ (the collection of subsets of the customers with sizes at least k in the example). The dealer (the company in the example) chooses a conditional probability distribution over $\mathcal{X}^J$, a cartesian product of a sequence of finite sets $\mathcal{X}_1, \ldots, \mathcal{X}_J$, under the condition which $s \in \mathcal{S}$ is given. All participants know the conditional distribution.

a) For given $s \in \mathcal{S}$ (, which the company wants to sell in the example), the dealer chooses a sequence $x^J := (x_1, \ldots, x_J) \in \mathcal{X}^J$ according to the conditional distribution and gives the jth participant x_j as his/her share.

b) In the case that any qualified subset $A \in \mathcal{A}$ of participants want to know whether the s at the dealer's hands is a special $s_0 \in \mathcal{S}$, they can "identify" it by pooling their shares. (In the example, if at least k customers want to buy the s_0th products, they can check whether the company is going to sell them by pooling the shares which they received from the company.)

c)s and s_0 can be arbitrary secrets in $\mathcal{S}$ and the dealer (previously) has no idea about s_0. (In the example the company does not know what its customers want to buy.)

d) Any non-qualified subset of participants can obtain absolutely no information about the secret s at the dealer's hands. In particular they cannot identify whether it is a "special" s_0 by pooling their shares. (In the example if less k customers want to buy the same kind of products and cooperate to check whether the products are going to be sold or even try to obtain any information about what the company want to sell, they will fail to do it.)

Let us now define our scheme, the identification secret sharing (IDSS) scheme. Again suppose we are given a set $\mathcal{P} = [J]$ of participants, an access structure $\mathcal{A}$, and a secret source S, a RV taking values in the set $\mathcal{S}$ of secrets. Then a (λ_1, λ_2) IDSS scheme is specified by a stochastic matrix $W : \mathcal{S} \longrightarrow \mathcal{X}^J$ (for any sequence of finite sets $\mathcal{X}_j, j = 1, \ldots, J$) and a collection of subsets of $\mathcal{X}_A, A \in \mathcal{A}$ which we called decoding sets

$$\mathcal{D} := \{\mathcal{D}_s^A : \ A \in \mathcal{A}, \ s \in \mathcal{S}\} \tag{5}$$

such that for all $s \in \mathcal{S}$,

$$\mathcal{D}_s^A \subset \mathcal{X}_A \tag{6}$$

i') for all $A \in \mathcal{A}$ and $s, s' \in \mathcal{S}$ with $s \neq s'$,

$$P_{X_A|S}(\mathcal{D}_s^A|s) \geq 1 - \lambda_1, \tag{7}$$

and

$$P_{X_A|S}(\mathcal{D}_s^A|s') \leq \lambda_2, \tag{8}$$

and condition ii) hold. λ_1 and λ_2 are called probabilities of errors of the first kind and second kind respectively. The scheme works in a similar way. The dealer chooses the shares according to $W(.|s)$ for an $s \in \mathcal{S}$ (occurring with probability $P_S(s)$) and distribute them to the participants. A qualified subsets of participants, who are interested in whether s is equal to a "special" element s_0 in $\mathcal{S}$, pool their shares to obtain an $x_A \in \mathcal{X}_A$ and check whether x_A falls on $\mathcal{D}_{s_0}^A$. If so, they say "Yes(, the 's' at dealer's hands is s_0)." and otherwise they say "No(, it is not s_0)." By (7), with probability not smaller than $1-\lambda_1$ they say "Yes" and with probability not larger than λ_1 they make a mistake to say "No" when $s = s_0$. (This is known as the error of first kind in statistics.) By (8) they make a mistake to say "Yes" with probability not larger than λ_2 when $s \neq s_0$. (It is known as the error of the second kind in statistics.)

Notice in an IDSS scheme the errors are allowed. Let us assume the errors are not allowed i.e., $\lambda_1 = \lambda_2 = 0$. Then by (7), $\mathcal{D}_s^A \supset supp(P_{X_A|S}(.|s))$, for all $A \in \mathcal{A}, s \in \mathcal{S}$ and (8) yields that for all $A \in \mathcal{A}, s \neq s', \mathcal{D}_s^A \cap supp(P_{X_A|S}(.|s')) = \emptyset$. So for an IDSS scheme whose probabilities of errors of both kinds are zero, $supp(P_{X_A|S}(.|s)), s \in \mathcal{S}$ are pairwise disjoint for all $A \in \mathcal{A}$ and therefore the scheme actually is an (ordinary) secret sharing scheme. So we always assume that at least one of λ_1 and λ_2 is not 0. However as usual, like to in statistics and in the other models of identification, we assume that the error of first kind is more serious than that of the second kind. The assumption is reasonable. For example, in the above example an error of the first kind makes the company and its customers loose a chance for trade. They probably only waste time when an error of the second kind occurs. So we assume that $\lambda_1 \geq 0$ and $\lambda_2 > 0$. We shall see whether λ_1 is 0 asymptotically makes no difference. This suggests us to employ an IDSS scheme with $\lambda_1 = 0$ when the secret is sufficiently long.

For an IDSS scheme and an $A \in \mathcal{A}$, $\mathcal{D}_s^A$'s are not necessarily pairwise disjoint. Consequently a qualified subset A may identify s is s_0 or s_0' if they receive an $x_A \in \mathcal{D}_{s_0}^A \cap \mathcal{D}_{s_0'}^A$ for different s_0 and s_0'. Of course one of the identifications must be wrong but the probability to make wrong identification is always no larger than $\lambda_1 + \lambda_2$. The decoding sets' overlapping causes errors and so it seems to be a backward. But without the overlapping the size $|\mathcal{S}|$ of the shared secrets could not exceed $\mathcal{X}_A$ for all $A \in \mathcal{A}$ (in fact we have known that $|\mathcal{S}| \leq |\mathcal{X}_j|$ for all $j \in \mathcal{P}$) and we shall see that because of the overlapping, we identify secrets of double exponential sizes when the sizes of alphabets $\mathcal{X}_j$ are exponentially increasing. Paying a cost of the errors for gaining much longer shared secrets is exactly the key idea for IDSS scheme . This is simillar to in the case of identification codes for the channels.

We shall also discuss the case that the public message is allowed. In this case the dealer is allowed to braodcast a public message x_0 from a finite set $\mathcal{X}_0$, the alphabet of the public messages, and every participant in $\mathcal{P}$ receives not only his/her (private) share but also the public message. So instead of a stochastic matrix W from $\mathcal{S}$ to $\mathcal{X}^J$ the dealer uses a stochastic matrix W_0 from $\mathcal{S}$ to $(\mathcal{X}^n)^0 := \mathcal{X}^n \times \mathcal{X}_0$ to choose shares. A subset $A = \{j_1, \ldots, j_k\}$ (say) of participants obtain a sequence $(x^A)^0 := (x_{j_1}, \ldots, x_{j_k}, x_0) \in (\mathcal{X}_A)^0$ by pooling their shares. The decoding sets $(\mathcal{D}_s^A)^0 (\in (\mathcal{X}_A)^0$ for $A \in \mathcal{A}, s \in \mathcal{S})$ and the probabilities λ_1 and λ_2 of the errors of the first and the second kinds are defined analogously. For $A = \{j_1, \ldots, j_k\}$, the RV generated by an IDSS scheme with public message and the secret source S is denoted by $(X_A)^0 := (X_A, X_0) = (X_{j_1}, \ldots X_{j_k}, X_0)$ analogously.

For a given access structure $\mathcal{A}$ on a set $\mathcal{P}$ of participants, we denote by

$$a(\mathcal{A}; \mathcal{X}_1, \ldots, \mathcal{X}_J) := \min_{A \in \mathcal{A}} \prod_{j \in A} \mathcal{X}_j \tag{9}$$

The followings are our results:

Theorem 3.1 *1)For all $\epsilon, \lambda_2 > 0$, there exists a sufficiently large L such that for all access structure $\mathcal{A}$ on all $\mathcal{P}$, all S with $\log\log|\mathcal{S}| > L$ and all $\mathcal{X}_1, \ldots, \mathcal{X}_J$, with $|\mathcal{X}_j| \geq \theta_j$ for $j \in \mathcal{P}$, where $\theta_j, j \in \mathcal{P}$ are constants depending on λ_2 and $\mathcal{A}$ and*

$$\log a(\mathcal{A}; \mathcal{X}_1, \ldots, \mathcal{X}_J) > \log\log|\mathcal{S}|(1+\epsilon), \tag{10}$$

(where $a(.)$ is defined in (9),) there exists a $(0, \lambda_2)$ IDSS scheme (without public message and) with alphabet $(\mathcal{X}_1, \ldots, \mathcal{X}_J)$.

2)For all $\epsilon, \lambda_2 > 0, \lambda_1 \geq 0$ with $\lambda_1 + \lambda_2 < 1$, there exits a positive L such that for all access structure $\mathcal{A}$ on any $\mathcal{P}$ and all S with $\log\log|\mathcal{S}| > L$, there is no IDSS scheme (without public message and) with alphabet $(\mathcal{X}_1, \dots, \mathcal{X}_J)$ such that

$$\log a(\mathcal{A}; \mathcal{X}_1, \dots \mathcal{X}_J)) < \log\log|\mathcal{S}|(1-\epsilon). \tag{11}$$

Theorem 3.2 *1)For all $\epsilon, \lambda_2 > 0$ there exist a positive number L such that for all access structure $\mathcal{A}$ on all $\mathcal{P}$, all S with $\log\log|\mathcal{S}| > L$, and all $(\mathcal{X}_1, \dots, \mathcal{X}_J, \mathcal{X}_0)$ with $|\mathcal{X}_j| > \theta_j, j \in \mathcal{P}$, where $\theta_j, j \in \mathcal{P}$ are constants depending on λ_2 and $\mathcal{A}$, and*

$$\log a(\mathcal{A}; \mathcal{X}_1, \dots, \mathcal{X}_J) + \log|\mathcal{X}_0| > \log\log|\mathcal{S}|(1+\epsilon), \tag{12}$$

there exists a $(0, \lambda_2)$ IDSS scheme with public message and alphabet $(\mathcal{X}_1, \dots \mathcal{X}_J, \mathcal{X}_0)$.

2)For all $\epsilon, \lambda_2 > 0, \lambda_1 \geq 0$ with $\lambda_1 + \lambda_2 < 1$ there exists a positive L such that for all access structure $\mathcal{A}$ and all S with $\log\log|\mathcal{S}| > L$ there is no IDSS scheme with public message and alphabet $(\mathcal{X}_1, \dots, \mathcal{X}_J, \mathcal{X}_0)$ such that

$$\log A(\mathcal{A}, \mathcal{X}_1, \dots, \mathcal{X}_J) + \log|\mathcal{X}_0| < \log\log|\mathcal{S}|(1-\epsilon). \tag{13}$$

By Theorem 3.2 1) for fixed access structure and fixed probability of the error of the second kind, one can fix the sizes $|\mathcal{X}_j|, j \in \mathcal{P}$ of (private) alphabets to identify a set of secrets with arbitrarily large size by increasing the size of public alphabet. That means the majority of the message provided by the dealer may be broadcasted publicly. It follows from our observation that in the construction of IDSS scheme without public message in Section 5 the majorities of the shares given to the participants can be braodcasted publicly without changing the security. Thus a construction of IDSS with public message in Theorem 3.2 1) immediately follows.

4 The Converses

In this section we show the converse parts of Theorems 3.1 and 3.2 i.e., Theorem 3.1 2) and Theorem 3.2 2).

It is sufficient for us to show that for all $\epsilon, \delta > 0$ there exists an L such that for any access structure $\mathcal{A}$ and any secret source S with $\log\log|\mathcal{S}| > L$, that there exists a (λ_1, λ_2) IDSS scheme without public message and with alphabet $(\mathcal{X}_1, \dots, \mathcal{X}_J)$ such that (11) holds or a (λ_1, λ_2) IDSS with public message and alphabet $(\mathcal{X}_1, \dots, \mathcal{X}_J, \mathcal{X}_0)$ such that (13) holds implies that $\lambda_1 + \lambda_2 > 1 - \delta$.

Assume that we have such an IDSS scheme (with or without public message) and $A = \{j_1, \dots, j_l\}$ (say) achieves $a(\mathcal{A}; \mathcal{X}_1, \dots, \mathcal{X}_J)$ in (9). Let $\mathcal{X}_{j_l} := \{1, \dots, q\}$ and $\mathcal{Q}_K(\mathcal{X}_{j_l})$ be the set of probability distributions Q over $\mathcal{X}_{j_l}$ with $Q(j) = \frac{k}{K}, k \in \{0, 1, \dots, K\}$ for $j = 1, \dots, q$. Then a probability distribution P over $\mathcal{X}_{j_l}$ can be approximated by a probability distribution $Q \in \mathcal{Q}_K(\mathcal{X}_{j_l})$ in the sense that for all $x \in \mathcal{X}_{j_l}, |P(x) - Q(x)| < \frac{1}{K}$. Indeed for given a such P one can find a Q as follows. Choose $k_1 = \lfloor KP(1) \rfloor$ and $Q(1) = \frac{k_1}{K}$. Choose $k_i = \lfloor KP(i) \rfloor$ if $\sum_{x=1}^{i-1}[P(x) - Q(x)] \geq 0$ and otherwise $k_i = \lceil KP(i) \rceil$ and let $Q(i) = \frac{k_i}{K}$, having chosen $Q(1), \dots, Q(i-1)$. Thus $|P(x) - Q(x)| < \frac{1}{K}$ for all $x \in \mathcal{X}_{j_l}$ and $|\sum_{x=1}^{q} P(x) - \sum_{x=1}^{q} Q(x)| < \frac{1}{K}$, which and the definition of Q yield that $\sum_{x=1}^{q} Q(x) = \sum_{x=1}^{q} P(x) = 1$. Therefore Q is a probability distribution.

Let b be a sufficiently large integer specified later and $K := qb$. Then $|\mathcal{Q}_K(\mathcal{X}_{j_l})|$ is equal to the number of the integer solutions of the system $\sum_{k=1}^{q} z_k = K, 0 \leq z_k, k = 1, \dots, q$ (for $(z_1, \dots, z_q)$), and therefore

$$|\mathcal{Q}_K(\mathcal{X}_{j_l})| = \binom{K+q-1}{q-1} < 2^{K+q} = 2^{q(b+1)}. \tag{14}$$

Abbreviate $A \setminus \{j_l\} = \{j_1, \dots, j_{l-1}\} = A'$. Then by the definitions of $a(.)$ and $A = \{j_1, \dots, j_l\}$ we have

$$|\mathcal{X}_{A'}| = q^{-1} a(\mathcal{A}; \mathcal{X}_1, \dots, \mathcal{X}_J). \tag{15}$$

Next, for all $s \in \mathcal{S}$ we approximate $\{P_{X_{j_l}|X_{A'}S}(.|x_{A'}, s) : x_{A'} \in \mathcal{X}_{A'}\}$ by $\{Q(.|x_{A'}, s) : x_{A'} \in \mathcal{X}_{A'}\} \in (\mathcal{Q}_K(\mathcal{X}_{j_l}))^{|\mathcal{X}_{A'}|}$ (, where $(\mathcal{Q}_K(\mathcal{X}_{j_l}))^{|\mathcal{X}_{A'}|} := \{(Q_1, \dots, Q_{|\mathcal{X}_{A'}|}) : Q_i \in$

$\mathcal{Q}_K(\mathcal{X}_{j_l})\}$ is the $|\mathcal{X}_{A'}|$ dimension cartesian power of $\mathcal{Q}_K(\mathcal{X}_{j_l}))$ such that for all $s \in \mathcal{S}, x \in \mathcal{X}_{j_l}$, and $x_{A'} \in \mathcal{X}_{A'}$, $|P_{X_{j_l}|X_{A'}}(x|x_{A'}, s) - Q(x|x_{A'}, s)| < \frac{1}{K}$, or

$$\sum_{x \in \mathcal{X}_{j_l}} |P_{X_{j_l}|X_{A'},S}(x|x_{A'}, s) - Q(x|x_{A'}, s)| < q\frac{1}{K} = \frac{1}{b}, \tag{16}$$

as we have chosen $K = bq$. Let us choose L sufficiently large such that for all $\log\log|\mathcal{S}| > L$, $\frac{\log(b+1)+\log\log\log|\mathcal{S}|}{\log\log|\mathcal{S}|} < \epsilon$. Then (11) yields that

$$\begin{aligned} \log\log|\mathcal{S}| &> \log a(\mathcal{A}; \mathcal{X}_{j_1}, \ldots, \mathcal{X}_{j_l}) + \log(b+1) + \log\log\log|\mathcal{S}| \\ &> \log a(\mathcal{A}; \mathcal{X}_{j_1}, \ldots, \mathcal{X}_{j_l}) + \log(b+1) + \log\log a(\mathcal{A}; \mathcal{X}_{j_1}, \ldots, \mathcal{X}_{j_l}) \\ &= \log[a(\mathcal{A}; \mathcal{X}_{j_1}, \ldots, \mathcal{X}_{j_l})(b+1)\log a(\mathcal{A}; \mathcal{X}_{j_1}, \ldots, \mathcal{X}_{j_l})] \end{aligned}$$

Consequently, by (14) and (15) we have $|\mathcal{S}| > q^{(b+1)a(\mathcal{A};\mathcal{X}_{j_1},\ldots,\mathcal{X}_{j_l})} > |\mathcal{Q}_K(\mathcal{X}_{j_l})|^{|\mathcal{X}^{A'}|}$, which implies that there exist $s, s' \in \mathcal{S}$ with $s \neq s'$ and $Q(.|x_{A'}, s) = Q(.|x_{A'}, s')$ for all $x_{A'} \in \mathcal{X}_{A'}$. Thus, by (16), for all $x_{A'} \in \mathcal{X}_{A'}$,

$$\begin{aligned} &\sum_{x \in \mathcal{X}_{j_l}} |P_{X_{j_l}|X_{A'}S}(x|x_{A'}, s) - P_{X_{j_j}|X_{A'}S}(x|x_{A'}, s')| \\ \leq &\sum_{x \in \mathcal{X}_{j_l}} |P_{X_{j_l}|X_{A'}S}(x|x_{A'}, s) - Q(x|x_{A'}, s)| + \sum_{x \in \mathcal{X}_{j_l}} |Q(x|x_{A'}, s') - P_{X_{j_l}|X_{A'}S}(x|x_{A'}, s')| \\ < &\frac{2}{b}. \end{aligned} \tag{17}$$

On the other hand, by the definition of $a(.)$ in (9), $A' \notin \mathcal{A}$ and therefore (2) holds for A'. In other words, for all $s \in \mathcal{S}$, $P_{X_{A'}|S}(.|s) = P_{X_{A'}}(.)$. Thus for the pair of secrets s, s' in (17),

$$\begin{aligned} &\sum_{x_A \in \mathcal{X}_A} |P_{X_A|S}(x_A|s) - P_{X_A|S}(x_A|s')| \\ = &\sum_{x_{A'} \in \mathcal{X}_{A'}} \sum_{x \in \mathcal{X}_{j_l}} |P_{X_{A'}|S}(x_{A'}|s) P_{X_{j_l}|X_{A'}S}(x|x_{A'}, s) - P_{X_{A'}|S}(x_{A'}|s') P_{X_{j_l}|X_{A'}S}(x|x_{A'}, s')| \\ = &\sum_{x_{A'} \in \mathcal{X}_{A'}} P_{X_{A'}}(x_{A'}) \sum_{x \in \mathcal{X}_{j_l}} |P_{X_{j_l}|X_{A'}S}(x|x_{A'}, s) - P_{X_{j_l}|X_{A'}S}(x|x_{A'}, s')| \end{aligned}$$

$$
\begin{aligned}
&< \sum_{x_{A'} \in \mathcal{X}_{A'}} P_{X_{A'}}(x_{A'}) \frac{2}{b} \\
&= \frac{2}{b}. \qquad (18)
\end{aligned}
$$

We are ready to finish the proof of Theorem 3.1 2),

$$
\begin{aligned}
\lambda_1 + \lambda_2 &> 1 - P_{X_A|S}(\mathcal{D}_s^A|s) + P_{X_A|S}(\mathcal{D}_s^A|s') \\
&\geq 1 - \max_{\mathcal{D} \subset \mathcal{X}_A} (P_{X_A|S}(\mathcal{D}|s) - P_{X_A|S}(\mathcal{D}|s')) \\
&= 1 - \sum_{x_A : P_{X_A|S}(x_A|s) \geq P_{X_A|S}(x_A|s')} (P_{X_A|S}(x_A|s) - P_{X_A|S}(x_A|s')) \\
&= 1 - \frac{1}{2} \sum_{x_A \in \mathcal{X}_A} |P_{X_A|S}(x_A|s) - P_{X_A|S}(x_A|s')| > 1 - \frac{1}{b}.
\end{aligned}
$$

Thus the proof of Theorem 3.1 2) is completed by taking $b \geq \frac{1}{\delta}$.

One can show Theorem 3.2 2) in the same way but approximating $P_{X_{j_l}|X_{A''}S}(.|x_{A''}, s)$ for $A'' := A' \times \{\mathcal{X}_0\}$.

5 Constructions

In this section, we present constructive proof for the direct part, Theorem 3.1 1) through the well-known Gilbert-Varshamov bound in coding theory. An IDSS scheme with public message can be obtained by a slight modification from the IDSS scheme without public message. Therefore Theorem 3.2 1) is obtained. Let $\mathcal{Z} := \{0, \ldots, q-1\}$ and the Hamming distance between $z^n := (z_1, \ldots, z_n), z'^n := (z'_1, \ldots, z'_n) \in \mathcal{Z}^n, d_H(z^n, z'^n) := |\{j : z_j \neq z'_j\}|$

Theorem 5.1 (Gilbert-Varshamov Bound): *For all positive integers $d < n$, there exists a code $C \subset \mathcal{Z}^n$ of size $|C| = M$, such that for all $z^n, z'^n \in C, d_H(z^n, z'^n) > d$ (we say that the code has minimum (Hamming) distance larger than d) if M is an integer satisfying*

$$M < \frac{q^n}{\sum_{i=0}^{d} \binom{n}{i} (q-1)^i}. \tag{19}$$

Let us first describe the idea for the construction before presenting it formally. We first choose properly n, q, and d such that $\frac{d}{n}$ sufficiently close to one (depending on λ_2) and there exists a code over $\mathcal{Z}^n := \{0, 1, \ldots, q-1\}^n$ with minimum Hamming distance larger than d and size $|\mathcal{S}|$ by Gilbert-Varshamov bound. Then we map the secrets in $\mathcal{S}$ to the code by a bijector ϕ. All participants (including the dealer) know the code and ϕ. For a given $s \in \mathcal{S}$, the dealer randomly chooses an $i \in [n]$ with uniform distribution and then distributes the shares to the participants such that all qualified subsets can recover (i, c_i) if $\phi(s) = (c_1, \ldots c_n)$. After recovering (i, c_i) the members of a qualified subset, who want to identify if $s = s_0$ for an s_0 with $\phi(s_0) = (c_1^0, \ldots, c_n^0)$, check whether $c_i = c_i^0$. They say "Yes" if so and otherwise say "No". So the probability of the first kind is zero. On the other hand, the Hamming distance $d_H(\phi(s), \phi(s_0)) > d$ is sufficiently close to n and therefore the dealer chooses an i with probability sufficiently close to one such that $c_i \neq c_i^0$ if $s \neq s_0$. This implies the probability of the error of second kind is sufficiently close to zero since an error of the second kind occurs exactly when $s \neq s_0$ and the dealer chooses an i with $c_i = c_i^0$. This idea was first used in [3] to construct an identification code for a channel with feedback. Our observation is that the i chosen by the dealer can be publicly informed to the participants (and only c_i needs to be kept in secret). So the dealer may broadcast it when the public message is allowed. In the other case, he just informs it to the qualified sets via their shares but it is not necessary to keep it in secret from non-qualified subsets. The only part needed to be kept in secret is c_i, which can be "sent" to qualified subsets by an (ordinary) secret sharing scheme. This makes us identify more secret. We shall first construct a scheme and then show that it is an IDSS scheme satisfying the conditions of the theorem.

To construct the scheme, we first set up the parameters n, d, and q such that the desired code exists. For a given λ_2, let us fix $0 < \mu < \lambda_2$ and $\alpha > 1$. Choose an integer q such that

$$\frac{q^\mu}{2} \geq \alpha. \tag{20}$$

For a sufficiently large integer n (specified later) we choose a set $\mathcal{S}$ with cardinality

$$|\mathcal{S}| = \lfloor \frac{\alpha^n}{n} \rfloor \tag{21}$$

as the set of secrets and an integer d with $\mu \leq 1 - \frac{d}{n} < \lambda_2$. Since by (20)

$$|\mathcal{S}| \leq \frac{\alpha^n}{n} \leq \frac{q^{n\mu}}{n2^n} = \frac{q^n}{n2^n q^{n(1-\mu)}} \leq \frac{q^n}{n2^n q^d} < \frac{q^n}{\sum_{i=0}^d 2^n q^i} < \frac{q^n}{\sum_{i=0}^d \binom{n}{i}(q-1)^n},$$

by Gilbert-Varshamov bound, one can find a code C with minimum distance larger than d and cardinality $|C| = |\mathcal{S}|$ and therefore a bijector ϕ from $\mathcal{S}$ to C. The code and ϕ are known by the dealer and all participants in $\mathcal{P}$.

The dealer generates a RV U taking values in $[n]$ uniformly and distribute a share $x_j := (x'_j, x''_j)$ to the jth participant in $\mathcal{P}$ so that all qualified subsets can reconstruct (U, c_U) and all non-qualified subsets have no knowledge about c_U for a given $s \in \mathcal{S}$ with $\phi(s) = (c_1, \dots, c_n)$ (say). For an IDSS scheme without public message the dealer has to inform the qualified subsets the value of U through their (private) shares and he does it by the parts x'_j of the shares. For an IDSS with public message he does it through associating the public message $x_0 \in \mathcal{X}_0$ and the shares x'_j when the size $|\mathcal{X}_0|$ of public message is not sufficiently large (i. e., smaller than n) and otherwise through the public message (in this case the component x'_j in x_j is not necessary). Notice that we do not ask to keep the value of U in secret (from the non-qualified subsets). It can be sent in a public way. We only present the construction of IDSS schemes without public message. An IDSS schemes with public message can be obtained by a modification in an obvious way and we leave the details for the readers. Let $|\mathcal{A}| = I$ and denote by

$$\mathcal{A} = \{A_i : i = 1, \ldots, I\} \tag{22}$$

Because I and c in (4) are fixed for given $\mathcal{A}$, and by (21) $\log n < \log\log|\mathcal{S}|(1+\frac{\epsilon}{4})$ if $|\mathcal{S}|$ is sufficiently large, for any collection $(\mathcal{X}_1, \ldots, \mathcal{X}_J)$ of alphabets satisfying the conditions in Theorem 3.1 1), one can express $\mathcal{X}_j$'s (or their subsets) as $\mathcal{X}_j'^I \times \mathcal{X}_j''$, where $\mathcal{X}_j'^I$ is the I dimension cartesian power of $\mathcal{X}_j'$ and $\mathcal{X}_j''$ is a finite set with $|\mathcal{X}_j''| = q^c$ for c in (4) such that

$$\log a(\mathcal{A}; \mathcal{X}_1', \ldots, \mathcal{X}_J') > \log n(1 + \frac{\epsilon}{4}), \tag{23}$$

since by (9), (for $\mathcal{X} = \mathcal{X}_j'^I \times \mathcal{X}''$) $\log a(\mathcal{A}; \mathcal{X}_1, \ldots, \mathcal{X}_J) \leq \log a(\mathcal{A}; \mathcal{X}_1'^I, \ldots, \mathcal{X}_J'^I) + \max_{A\subset\mathcal{A}} \log \prod_{i\in A} |\mathcal{X}_i''| = \log a(\mathcal{A}; \mathcal{X}_1', \ldots, \mathcal{X}_J') + \log I + \max_{A\subset\mathcal{A}} \log \prod_{i\in A} |\mathcal{X}_i''|$ and

$$\log|\mathcal{X}_j''| = c \log q, \tag{24}$$

for all $j \in \mathcal{P}$ and c in (4). For each j, x_j' is a sequence in $\mathcal{X}'^I_j$ defined as follows. For $A_i, i = 1, \ldots, I = |\mathcal{A}|$ (please c. f. (22)) partition $\prod_{j\in A_i} \mathcal{X}_j'$ into n subsets of (nearly) equal sizes. Notice that by (23) the partition exists. The dealer chooses a sequence from the uth subset randomly and uniformly and gives its component in $\mathcal{X}_j'$ to participant $j \in A_i$ as the ith component of x_j' if $U = u(\in [n])$. The dealer arbitrarily chooses a letter in $\mathcal{X}_j'$ and gives it to $j \notin A_i$ as the ith component of x_j'. Thus for all A_i, the members $j \in A_i$ can recover the sequence chosen by the dealer for A_i by pooling the ith components of $x_j', j \in A_i$. So they know which subset the sequence falls on and therefore learn u, the value of RV U. Denote the introduced RV's by X_j', $j \in \mathcal{P}$. Then by the construction, X_j', $j \in \mathcal{P}$ are independent of S because they only depend on U and U is independent of S.

Next by (24) there exits a secret sharing scheme for the secret set $\mathcal{Z} := \{0, 1, \ldots, q-1\}$ with the alphabets $(\mathcal{X}_1'', \ldots, \mathcal{X}_J'')$. Thus in the case, that $S = s$ and $U = u$, the dealer chooses the shares x_j'', $j \in \mathcal{P}$ for the secret $s'' = c_u(\in \mathcal{Z})$, where

$\phi(s) = (c_1, \ldots, c_n)$, such that the qualified subsets are able to recover c_u and non-qualified subsets have no knowledge about c_u. Denote the corresponding RV's by S'' and $X''_j, j \in \mathcal{P}$ and (analogously $X''_A, A \subset \mathcal{P}$). Since $(X'^J S, S'', X''^J)$ forms a Markov chain and for $A \notin \mathcal{A}$ S'' is independent of X''_A, for non-qualified A, X''_A is independent of $X'^J S$. On the other hand S and X'^J are independent. So (X''_A, X'^J, S) is an independent triple. Consequently $X_A = (X'_A X''_A)$ and S are independent if $A \notin \mathcal{A}$ i.e., (2) or the condition ii) holds. We notice here that for $A \notin \mathcal{A}, H(S|X''_A, X'^J) = H(S)$ since X''_A, X'^J, S are independent. This means a non-qualified subset cannot obtain any information about the secret even if they know the value of X'^J. In other words, the dealer can inform the participants x'^J, the value of RV X'^J publically and this gives a construction of IDSS with public message. We leave the details to the readers. Finally we have to define the decoding sets $\mathcal{D}^A_s$ for all $A \in \mathcal{A}$ and $s \in \mathcal{S}$, and to show (7) (for $\lambda_1 = 0$) and (8). For fixed $A \in \mathcal{A}, s \in \mathcal{S}$ the decoding set $\mathcal{D}^A_s$ is defined as follows. Notice that for all $A \in \mathcal{A}$ the ith component of the value x'_A of X'_A falls on the uth subset for all i iff $U = u$. In this case, we say that x'_A falls on the uth subset of $\mathcal{X}'_A$. Let x'_A fall on the uth subset of $\mathcal{X}'_A$ and $\phi(s) = (c_1, \ldots, c_n)$. Then $x_A = (x'_A, x''_A) \in \mathcal{D}^A_s$ iff the secret s'' recovered by A via x''_A in the secret sharing scheme for S'' is c_u. Since A can recover $c_u (= s'')$ without error,

$$P_{X_A|S}(\mathcal{D}^A_s|s) = 1, \tag{25}$$

i. e., (7) hold for $\lambda_1 = 0$. Moreover X_A falls on $\mathcal{D}^A_s \cap \mathcal{D}^A_{s'}$ for $A \in \mathcal{A}, s \neq s'$ iff x'_A falls on a subset, say the uth subset such that $\phi(s)$ and $\phi(s')$ have the same component at the uth coordinate and the dealer chooses $U = u$. This with (25) yields that $P_{X_A|S}(\mathcal{D}^A_s|s') = P_{X_A|S}(\mathcal{D}^A_s \cap \mathcal{D}^A_{s'}|s') \leq 1 - \frac{d}{n} < \lambda_2$, i.e. (8) holds.

Acknowledgement: The authors would like to thank Dr. Huaxiong Wang for his helpful discussion and suggestion.

References

[1] Ahlswede, R. (1997), "Germerel theory of information trannsfer", Preprint 97-118, SFB 343 Diskrete Strukturen in der Mathematik, to appear in IEEE Trans. Inform. Theory.

[2] Ahlswede, R. and Dueck, G. (1989), "Identification via channels", IEEE Trans. Inform. Theory, V. 35, 15-29.

[3] Ahlswede, R. and Dueck, G. (1989), "Identification in presence of feedback-a discovery of new capacity formulas", IEEE Trans. Inform. Theory, V. 35, 30-39.

[4] Blakley, G. R. (1979), "Safeguading cryptographic keys", AFIPS Conference Procceding 48, 313-317.

[5] Brickell, E. F. and Davenport, D. M. (1991), "On the classification of ideal secret sharing schemes", J. Crytology 4, 123-134.

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

[7] Han, T. S. and Verdu, S. 1992, "New results in the theory and application of identification via channels", IEEE Trans. Inform. Theory, V.38, 14-25, 1992.

[8] Ito, M., Saito, A. and Nishizeki, T. (1987), "Secret sharing scheme realizing general access structure", Proc. IEEE Globecom'87, 99-102.

[9] Karnin, E. D., Greene, J. W., and Hellman, M. E. (1983), "On secret sharing schemes", IEEE Trans. Inform. Theory, V. 29, 35-41.

[10] Shamir, A. (1979), "How to share a secret", Commun. of the ACM 22, 612-613.

[11] Shannon, C. E. (1948), "A mathematics theory of communication", Bell Syst. Techn. J. 27, 339-425, 623-656.

[12] Steinberg, V. (1998), "New converses in the theory of identification via channels", IEEE Trans. Inform. Theory, 984-998.

[13] Stinson, D. R. (1992), "An explication of seccret sharing schemes", Design, Codes, and Cryptrograpghy 2 357-390.

[14] Stinson, D. R. (1998), "Decompsition constructions for secret-sharing schemes", IEEE Trans. Inform. Theory, 118-125.