On Secret Reconstruction in Secret Sharing Schemes

Huaxiong Wang and Duncan S. Wong

***Abstract*—A secret sharing scheme typically requires secure communications in each of two distribution phases: 1) a dealer distributes shares to participants (share distribution phase); and later 2) the participants in some authorised subset send their share information to a combiner (secret reconstruction phase). While problems on storage required for participants, for example, the size of shares, have been well studied, problems regarding the communication complexity of the two distribution phases seem to have been mostly neglected in the literature so far. In this correspondence, we deal with several communication related problems in the secret reconstruction phase. Firstly, we show that there is a tradeoff between the communication costs and the number of participants involved in the secret reconstruction. We introduce the communication rate as the ratio of the secret size and the total number of communication bits transmitted from the participants to the combiner in the secret reconstruction phase. We derive a lower bound on the communication rate and give constructions that meet the bound. Secondly, we show that the point-to-point secure communication channels for participants to send share information to the combiner can be replaced with partial broadcast channels. We formulate partial broadcast channels as set systems and show that they are equivalent to the well-known combinatorial objects of cover-free family. Surprisingly, we find that the number of partial broadcast channels can be significantly reduced from the number of point-to-point secure channels. Precisely, in its optimal form, the number of channels can be reduced from n to $O(\log n)$, where n is the number of participants in a secret sharing scheme. We also study the communication rates of partial broadcast channels for the secret reconstruction.**

***Index Terms*—Cover-free family, cryptography, information-theoretic security, multicast communication, secret sharing.**

I. Introduction

A *secret sharing scheme* is a method of sharing a *secret* among a group of *participants* (or *shareholders*) in such a way that only certain specified subsets of participants (those belonging to an *access structure*) can reconstruct the secret whereas subsets of participants not belonging to the access structure cannot learn anything about the secret. A secret sharing scheme realizing an access structure which consists of all subsets of at least t out of n participants is called a (t, n)*threshold secret sharing scheme* [3], [19]. The secret is chosen by a special entity called the *dealer*. In a conventional secret sharing scheme, shares are generated and securely distributed to the participants by the dealer. To recover the secret, participants in an *authorised subset* (those in the access structure) securely send their shares to a *combiner* who uses a public algorithm to reconstruct the secret.

It is important to keep the share size of each participant as small as possible. One of the basic problems in the theory of secret sharing scheme is to establish bounds on the size of shares given to participants (see [5], [6], [22]). It is well known that the share size for a secret must be at least the size of the secret itself. When this lower bound is met, that is, the share of each participant is of the same size as the secret, the scheme is said to be *ideal*. The realization of an ideal scheme strongly depends on the underlying access structure and the secret size. It is known that not every (monotone) access structure can be realized by an ideal scheme and the classification problem of ideal monotone access structures remains open. Regarding the impact of secret size on ideal schemes, it is proved by Karnin *et al.* [14] that there exists an ideal (t, n)-threshold scheme such that $2 \leq t \leq n-1$ if and only if the size of the secret is at least $n - t + 2$.

Informally, a secret sharing scheme consists of two phases: *share distribution phase* and *secret reconstruction phase*. In the share distribution phase, a trusted *dealer* chooses a secret, runs a distribution algorithm to generate shares, and then distributes the shares to participants through some secure point-to-point communication channels. In the secret reconstruction phase, a *combiner* collects the shares of participants from an *authorised set* and applies a reconstruction algorithm to recover the secret. For collecting the shares in this phase, the participants from the authorised set send their shares to the combiner through some secure point-to-point communication channels.

There is another set of problems that has mostly been neglected in literature. These problems are concerning about the complexity of secure communications for the dealer to distribute shares to participants and the participants from an authorised set to send shares to the combiner. In this correspondence, we focus on the following two questions that are related to the communication complexity of the secret reconstruction phase:

1) Whether or not the communication cost can be reduced if more participants are involved in the secret reconstruction phase?
2) Whether or not the secure point-to-point communication channels between the participants and the combiner are necessary or can be replaced with some multicast communication channels while still maintaining the perfectness of the secret?

For the first question, let us look at a simple example. Let $\mathcal{P} = \{P_1, \ldots, P_n\}$ be the set of participants of a secret sharing scheme. Assume that participants in an authorised set B want to reconstruct the secret, typically they choose a *minimal* authorised subset A such that $A \subseteq B$ and only participants in A reveal their shares to the combiner. In other words, participants in $B \setminus A$ do not need to give their shares to the combiner. In this case, the total communication cost for participants in A to send shares to the combiner using secure point-to-point communication channels is at least $|A|H(S)$, where $H(S)$ is the size of the secret. One may ask if participants in $B \setminus A$ also contribute their shares or some information of their shares in the secret reconstruction phase, is it possible that the total communication cost can further be reduced?

For the second question, we study secret sharing schemes where no secure point-to-point communication channel exists and the communication between participants and the combiner is through some *partial broadcast* channels. A partial broadcast channel is a point-to-multipoint channel that allows a sender to send a message *simultaneously and privately* to a set of receivers, who are some other participants and the combiner of the secret sharing scheme in this case. Many conventional communication technologies naturally support point-to-multipoint communication. Examples are local area networks, using Ethernet buses or token rings, and transmission over radio networks and IP multicasting. In these examples, a partial broadcast channel can be established by sharing a common key among the sender and the recipients, and using an encryption algorithm to encipher the data in transmission.

Our results. We give affirmative answers to both of the questions above. First, we show that for a (t, n)-threshold secret sharing scheme,

Manuscript received March 2, 2006; revised July 17, 2007. The work of H. Wang was supported in part by Australian Research Council Discovery Grants DP0558773 and DP0665035, and Singapore Ministry of Education through the Grant T206B2204.

H. Wang is with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, and also with the Centre for Advanced Computing—Algorithms and Cryptography, Department of Computing, Macquarie University, Sydney NSW 2109, Australia (e-mail: hxwang@ntu.edu.sg; hwang@ics.mq.edu.au).

D. S. Wong is with the Department of Computer Science, City University of Hong Kong, Hong Kong, China (e-mail: duncan@cityu.edu.hk).

Communicated by E. Okamoto, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2007.911179

if the secret reconstruction phase has ℓ participants involved, where $\ell > t$, then it is possible to reduce the total number of communication bits from $tH(S)$ to $\frac{\ell}{\ell-t+1}H(S)$, where $tH(S)$ is the minimal number of bits to send if only t participants are involved in the secret reconstruction phase. This shows that there is a trade-off between the communication cost and the number of participants involved in the secret reconstruction phase. We also propose a polynomial-based construction of secret sharing scheme that facilitates communication cost saving for secret reconstruction with adjustable value of ℓ. The scheme is also easy to implement and has minimal share size (i.e., our scheme is ideal).

Second, we consider the use of partial broadcast communication channels for secret reconstruction. We show that the number of communication channels can be significantly reduced if partial broadcast channels are used. In its optimal case, this approach reduces the number of channels used to $O(\log n)$ partial broadcast channels from n point-to-point channels as required in a conventional secret sharing scheme. In particular, we model the partial channel setting as a set system and show that a (t, n)-threshold secret sharing scheme with partial broadcast channels for secret reconstruction exists if and only if the latter is a cover-free family, a well-studied combinatorial object. We also show that the communication cost for secret reconstruction increases while gradually changing the partial broadcast channels to secure point-to-point channels, which indicates another trade-off between communication cost and channel privacy for secret reconstruction. In addition, we propose a generic construction technique for building a communication-efficient scheme using partial broadcast channels.

Related work. The problem concerning secret reconstruction with more than minimal number of participants involved was first investigated by Martin *et al.* [16]. They studied various techniques to do secret reconstruction for (t, n)-threshold secret sharing schemes where ℓ $(\ell > t)$ participants are involved and each of them reveals only partial information of the share. Such schemes are called *threshold changeable secret sharing schemes*. The focus of [16] was on the security of these schemes. By allowing the threshold changeable, it enables the possible update and change of the security structure of a scheme. For example, higher threshold may be needed when the degree of trust among participants decreases over time, due to organizational issues or security incidents. In [16], a general model for threshold-changeable secret sharing schemes was developed and two constructions were given. Among the two constructions, one is based on polynomials using the Shamir approach and the other is geometrical in nature and is optimal in terms of the size of shares. Recently, Steinfeld *et al.* [20], [21] applied lattice reduction techniques to the construction of threshold changeable schemes. The techniques support more flexible choice of ℓ. However, the schemes in [20], [21] are probabilistic in the sense that the security and perfectness of the schemes are only probabilistically guaranteed. In [1], Barwick *et al.* considered the communication cost of updating parameters of a threshold scheme when broadcast communication channels are used. The first problem we will address in this correspondence is closely related to threshold-changeable secret sharing schemes. Although the motivation of our work is to reduce the communication cost of secret reconstruction, the techniques used in threshold changeable secret sharing schemes may also be applied and/or modified for building secret sharing schemes with communication-efficient secret reconstruction.

The second problem we are concerning with is related to secure communication in multicast network.[1] Secure communication in multicast networks has attracted a lot of attention in recent years. Franklin and Yung [10] gave a necessary and sufficient condition for individuals to exchange private messages in multicast models in the presence of passive adversaries. Franklin and Wright [11], Desmedt and Wang [8] obtained several results for the case of having active Byzantine adversaries. In addition, Goldreich *et al.* [12] studied fault-tolerant computation in the multicast model. Obviously, if one treats the communication between the participants and the combiner as a multicast network, then the previous results of secure transmission protocols in multicast networks can be applied directly to simulate point-to-point communication channels, and the second problem we are concerning with can be tackled using conventional secret sharing schemes. However, such an approach relies on the efficiency of the transmission protocols developed for secure multicast networks and also requires interaction in general, and so is not efficient for our purpose.

In [18], Safavi-Naini and Wang studied secret sharing schemes with partial broadcast channels for share distribution. That is, shares are distributed from the dealer to participants through partial broadcast channels. They showed that the number of channels and the total number of communication bits can both be reduced when using partial broadcast channels, when compared with the conventional approach of using secure point-to-point communication channels. Our work in this correspondence is to study the communication complexity of secret reconstruction, that is, when participants send their shares to the combiner for recovering the secret. Similar to the results of share distribution [18], the number of partial broadcast communication channels for secret reconstruction can significantly be less, while the total number of communication bits transmitted can, however, be higher than that of using conventional point-to-point communication channels.

Beimel and Chor [2] proposed some secret sharing schemes which use public (rather than secret/secure) communication channels to do secret reconstruction. In their schemes, it is assumed that the combiner is one of the participants (shareholders), and in secret reconstruction phase, participants broadcast partial information of their shares so that a particular participant (i.e., the combiner) is able to reconstruct the secret. In our work, we consider that the combiner can be anyone who simply applies a publicly known algorithm to reconstruct the secret once sufficient share information has been collected, and we also assume that the participants involved in the secret reconstruction have already known the set (or the size of the set) of participants involved in the reconstruction.

Paper organization. In Section II, both perfect and nonperfect secret sharing schemes are introduced. Section III introduces communication rate for secret reconstruction in the secure point-to-point communication model. In the section, we also derive bounds and give constructions for communication-efficient threshold schemes. Section IV introduces a model for secret sharing schemes with partial broadcast channels to do secret reconstruction. It also gives the necessary and sufficient condition of using partial broadcast channels. In addition, bounds on channel efficiency and communication complexity under the new model are derived, and a generic construction approach for such type of schemes is proposed. We conclude the correspondence in Section V.

II. Preliminaries

Let $\mathcal{P} = P_1, \ldots, P_n$ be a group of n participants and let $2^{\mathcal{P}}$ denote the family of all subsets of $\mathcal{P}$. An *authorized set* is a subset of participants who are authorised to access a secret. An *access structure* $\Gamma \subseteq 2^{\mathcal{P}}$ is the collection of all possible authorised sets. An access structure with the property that if $A \in \Gamma$ and $A \subseteq A'$ then $A' \in \Gamma$ is called *monotone increasing*.

Let S be a finite set of secrets to share and S_i be the set of all possible values of shares given to P_i, $1 \leq i \leq n$. Let R be the set of all possible random inputs and $H(X)$ denote the entropy of a random variable X

[1]Sometimes, partial broadcast channels are called multicast channels.

(for information-theoretic background we refer readers to [7]). For a finite set X we will abuse the notation and denote by X a random variable with domain X. For $A = \{P_{i_1}, \ldots, P_{i_j}\} \subseteq \mathcal{P}$, where $i_1 < i_2 < \cdots < i_j$, we denote $S_A = S_{i_1} \times \cdots \times S_{i_j}$.

Definition: A **secret sharing scheme** Π, which realizes an access structure Γ, consists of a mapping $\mathcal{D} : S \times R \to S_1 \times \cdots \times S_n$, from the cross product of secrets and random strings to a set of n-tuples (shares), such that the following two conditions hold:

1) The secret can be reconstructed by any subset in Γ. That is, for every secret $s \in S$ and authorised set $A \in \Gamma$, where A is denoted as $\{P_{i_1}, \ldots, P_{i_{|A|}}\}$, there exists a set of mappings $\mathcal{C}_A = (\boldsymbol{c}_{i_1}, \ldots, \boldsymbol{c}_{i_{|A|}})$, where $\boldsymbol{c}_{i_j} : S_{i_j} \to C_{i_j}$, for $1 \le j \le |A|$ and a function $h_A : C_{i_1} \times \cdots \times C_{i_{|A|}} \to S$ such that for every random string $r \in R$, if $\mathcal{D}(s, r) = \{s_1, \ldots, s_n\}$ then $h_A(\boldsymbol{c}_{i_1}(s_{i_1}), \ldots, \boldsymbol{C}_{i_{|A|}}(s_{i_{|A|}})) = s$.
2) Every subset not in Γ reveals no information as to the value of the secret (in the information theoretic sense). Formally, for any subset $I \notin \Gamma$, for every secret $a \in S$, and for every possible collection of shares $\{s_i\}_{\{i:P_i \in I\}}$

$$p\left(a \mid \{s_i\}_{\{i:P_i \in I\}}\right) = p(a)$$

where the probability is taken over the random string r.

We call $\mathcal{D}$, $\mathcal{C}_A$ and h_A as the *dealer algorithm*, the *channel share redistribution for* A and the *combiner algorithm for* A, respectively. Intuitively, a secret sharing scheme realizing an access structure Γ has two properties: 1) given the shares of participants in an authorised set $A \in \Gamma$, *the secret can be uniquely determined*, while 2) given the shares of participants in a set $I \notin \Gamma$, *nothing new about the secret can be learnt*. That is,

1) If $A \subseteq \mathcal{P}$ and $A \in \Gamma$, then $H(S|S_A) = 0$.
2) If $I \subseteq \mathcal{P}$ and $I \notin \Gamma$, then $H(S|S_I) = H(S)$.

The quantity $H(S)$ measures the 'uncertainty' of the secret and can be interpreted as the average number of bits required to represent a secret $s \in S$, and so represents the 'size' of the secret. Similarly, the value $H(S_i)$ represents the size of the share given to P_i. In practice, it is desirable to minimize the size of each share.

A secret sharing scheme is called *perfect* if the second property above is satisfied. A weaker version of the second property is to require that the secret cannot be uniquely determined if shares of participants in $A \notin \Gamma$ are pulled up. In this correspondence, unless otherwise stated, we will assume that the secret sharing scheme in study is perfect. It is known [6], [22] that in any perfect secret sharing scheme, $H(S_i) \ge H(S)$, for all $1 \le i \le n$. When $H(S_i) = H(S)$, for all $1 \le i \le n$, we refer to such a scheme an *ideal* scheme.

A subset Σ of $2^{\mathcal{P}}$ is called *monotone decreasing* if for any $A, B \subseteq \mathcal{P}$, whenever $A \in \Sigma$ and $B \subseteq A$, $B \in \Sigma$. (Γ, Σ) is called a *double* access structure [18] if Γ is monotone increasing, Σ is monotone decreasing and $\Gamma \cap \Sigma = \emptyset$.

A secret sharing scheme realizing a double access structure (Γ, Σ) is a pair of dealer algorithm $\mathcal{D}$ and combiner algorithm $\{h_A\}_{A \in \Gamma}$, such that

1) $H(S|S_A) = 0$ for any $A \in \Gamma$ (that is, A can recover the secret); and
2) $H(S|S_B) = H(S)$ for any $B \in \Sigma$ (that is, B has no information about the secret).

Note that in a secret sharing scheme realizing a double access structure (Γ, Σ), given the shares of participants in $\mathcal{C} \in 2^{\mathcal{P}} \setminus (\Gamma \cup \Sigma)$, some information about the secret may be revealed. Also note that a perfect secret sharing scheme realizing a monotone access structure Γ is a secret sharing scheme realizing a double access structure (Γ, Σ) where $\Sigma = 2^{\mathcal{P}} \setminus \Gamma$. We call the secret sharing scheme realizing access structure (Γ, Σ) *nonperfect* if $2^{\mathcal{P}} \setminus (\Gamma \cup \Sigma) \neq \emptyset$ and $0 < H(S|S_C) < H(S)$ for some $C \in 2^{\mathcal{P}} \setminus (\Gamma \cup \Sigma)$. This is to distinguish it from an ordinary perfect secret sharing scheme.

An interesting property of nonperfect secret sharing schemes is that the efficiency bound on perfect secret sharing schemes, that is $H(S_i) \ge H(S)$ for all $1 \le i \le n$, can be violated. It is proved in [17] that for any nonperfect secret sharing scheme, the following bound holds

$$\max\{H(S_i) : 1 \le i \le n\} \ge H(S) \min |A\ B|\} \tag{1}$$

where $A \in \Gamma$ and $B \in \Sigma$.

A well studied type of nonperfect secret sharing schemes is (d, t, n)-*ramp* schemes [4], [13], where $d < t$, $\Gamma = \{A \subseteq \mathcal{P} || A| \ge t\}$ and $\Sigma = \{B \subseteq \mathcal{P} || B| \le d\}$. It should be noted that the bound in (1) can be met with equality. A (d, t, n)-ramp scheme is called *optimal* if $H(S|S_A) = ((t - r)/(t - d))H(S)$ for any subset $A \subseteq \mathcal{P}$ where $|A| = r, d \le r \le t$ and the shares held by participants are of minimal size. In [13], it is shown that a (d, t, n)-ramp scheme with the property that $H(S_i) = H(S)/(t - d)$, for all $1 \le i \le n$, is optimal.

III. Communication Rate for Secret Reconstruction

In this section, we define a term called communication rate and use it as a measure of communication cost for participants to send their shares to the combiner for secret reconstruction in a secret sharing scheme using point-to-point communication channels. We also propose a construction of such a (t, n)-threshold secret sharing scheme and show that it achieves high communication rate.

A. Communication Rate

Observe that in the secret reconstruction phase, a participant P_i in the authorized set A may not send the plain share s_i to the combiner. Instead, he may send an 'encoded' version of s_i (encoded in an unconditional secure way), denoted as $c_i = \boldsymbol{c}_i(s_i)$ in the definition above, to the combiner. That is, c_i is actually transmitted through a secure point-to-point communication channel from P_i to the combiner. Therefore, the total communication complexity for the combiner to pull up shares of all the participants in A is the sum of c_i's length, rather than merely that of s_i's, for $P_i \in A$.

Definition 3.1: Let S be a finite set of secrets. We define the communication rates of a secret sharing scheme for an access structure Γ as follows.

- Given a secret sharing scheme Π for an access structure Γ, the communication rate for $A \in \Gamma$ is defined as

$$\rho_{(A,\Pi)} = \frac{H(S)}{\sum_{\mathcal{P}_i \in A} H(C_i)}.$$

- Given a secret sharing scheme Π for an access structure Γ, the communication rate for Π is defined as

$$\rho_{\Pi} = \min_{A \in \Gamma} \rho_{(A,\Pi)}.$$

- Given an access structure Γ, the communication rate for Γ is defined as

$$\rho_{\Gamma} = \sup_{\Pi \in \mathcal{S}} \rho_{\Pi}$$

where $\mathcal{S}$ is the space of all secret sharing schemes for the access structure Γ.

Theorem 3.1: Let Π be a (t, n)-threshold secret sharing scheme. For any $A \subseteq \mathcal{P}$ and $|A| \ge t$, we have

$$\rho_{(A,\Pi)} \le \frac{|A| - t + 1}{|A|}.$$

Furthermore, there exist secret sharing schemes such that the above bound is tight for any A with $|A| \ge t$.

Proof: Let $I(X;Y)$ denote the mutual information between X and Y.[2] Assume that $A = \{P_{i_1}, \ldots, P_{i_\ell}\} \subseteq \mathcal{P}$ and $\ell \geq t$. For any $(t-1)$-subset $I \subset A$, we have

$$\begin{aligned} I(S; C_{A\setminus I}|C_I) &= H(S|C_I) - H(S|C_{A\setminus I}, C_I) \\ &= H(S|C_I) - H(S|C_A) \\ &= H(S). \end{aligned} \tag{2}$$

On the other hand

$$\begin{aligned} I(S; C_{A\setminus I}|C_I) &= H(C_{A\setminus I}|C_I) - H(C_{A\setminus I}|C_I, S) \\ &\leq H(C_{A\setminus I}) \\ &\leq \sum_{\{i:P_i \in A\setminus I\}} H(C_i). \end{aligned} \tag{3}$$

From (2) and (3), it follows that $\sum_{\{i:P_i\in A\setminus I\}} H(C_i) \geq H(S)$.

Now let $\mathcal{I}$ be the collection of all $(t-1)$-subsets of A. We show that

$$\binom{\ell-1}{t-1} \sum_{\{i:P_i\in A\}} H(C_i) = \sum_{I\in\mathcal{I}} \sum_{\{j:P_j\in A\setminus I\}} H(C_j). \tag{4}$$

To see this, for each $P_i \in A$, set $\mathcal{I}_i = \{B \in \mathcal{I}; i \notin B\}$. Then for each $1 \leq i \leq n$, $H(C_i)$ appears $|\mathcal{I}_i| = \binom{\ell-1}{t-1}$ times at the right-hand side of (4). It follows that

$$\begin{aligned} \binom{\ell-1}{t-1} \sum_{\{i:P_i\in A\}} H(C_i) &= \sum_{B\in\mathcal{I}} \sum_{\{j:P_j\in A\setminus B\}} H(C_j) \\ &\geq \binom{\ell}{t-1} H(S) \end{aligned}$$

and we obtain $\sum_{\{i:P_i\in A\}} H(C_i) \geq \frac{\ell}{\ell-t+1} H(S)$. It follows that $\rho_{(A,\Pi)} = \frac{H(S)}{\sum_{j=1}^{\ell} H(C_{i_j})} \leq \frac{\ell-t+1}{\ell}$ for any Π.

Next, we show that there exists a secret sharing scheme Π such that the lower bound of $\rho_{(A,\Pi)}$ is tight for any A with $|A| > t$. To this end, we apply optimal ramp secret sharing schemes and give an explicit construction that meets the bound. Recall that in an optimal $(t-1,\ell,n)$-ramp scheme, $t \leq \ell \leq n$, we have $H(S_i') = H(S)/(\ell-t+1)$, where S_i' is the share space of P_i (such schemes can easily be constructed, see [13] for details). For $A \subseteq \mathcal{P}$ with $|A| = \ell$ for $t \leq \ell \leq n$, we simply impose an optimal $(t-1,\ell,\ell)$-ramp scheme for the same secret to those participants in A, and in the secret reconstruction phase, each participant in A submits his share (of $H(S)/(\ell-t+1)$ bits) to the combiner. Therefore, the total number of communication bits from participants in A is $\frac{\ell}{\ell-t+1}H(S)$ and the result follows. □

Corollary: Let Σ be the (t,n) access structure and Π be a secret sharing scheme over Σ. Then we have

1) $\rho_{(A,\Pi)} \leq \frac{\ell-t+1}{\ell}$ for any A with $|A| = \ell \geq t$.
2) $\rho_\Sigma \leq \frac{n-t+1}{n}$.

Proof: Part 1 follows from Theorem 3.1 directly. For Part 2, it is easy to see that the function $f(x) = \frac{x}{x-t+1}$ is monotone increasing for $x \geq t$. Thus if we take $A = \mathcal{P}$, it gives rise to the minimal value, that is $\frac{n}{n-t+1}$. Therefore, $\rho \leq \frac{n-t+1}{n}$. □

B. Constructions

In this subsection, we apply techniques of ramp secret sharing scheme and threshold changeable secret sharing scheme onto the construction of (t,n)-threshold scheme so that the resulting scheme can achieve high communication rate for secret reconstruction.

As we have already seen in the proof of Theorem 3.1, a straightforward approach is to apply multiple $(t-1,\ell,n)$-ramp schemes, $t \leq \ell \leq n$, to the generation and distribution of shares to the n participants in $\mathcal{P}$. In the secret reconstruction phase, the involved participants only reveal the shares of the associated ramp scheme, rather than their full shares. However, the problem with this approach is that the size of share for each participant is prohibitively large. Suppose that the construction is based on the optimal $(t-1,\ell,n)$ ramp schemes, for all $t \leq \ell \leq n$, then the size of each share will be $\sum_{\ell=t}^{n} \frac{1}{\ell-t+1} = \sum_{i=1}^{n-t+1} \frac{1}{i}$ times the size of the secret, while we note that in an ideal threshold secret sharing scheme, the size of each share is the same as the size of the secret. Thus the implied question is how to construct a (t,n)-threshold scheme with smaller shares (ideally having the size of each share be the same as that of the secret) and higher communication rate for secret reconstruction.

Another related technique is threshold changeable secret sharing scheme. Martin *et al.* [16] considered the following questions: in a (t,n)-threshold secret sharing scheme, ℓ participants, $\ell > t$, want to work jointly to reconstruct the secret by revealing only partial information of their shares. In particular, they considered functions $\boldsymbol{c}_i : S_i \to C_i$, $1 \leq i \leq n$, such that (1) for any $|A| \geq \ell$, $H(S|C_A) = 0$; and (2) for any $|A| < \ell$, $H(S|C_A) \neq 0$. Thus, their main focus in [16] is the security of the threshold parameter. In this correspondence, we are interested in constructing (t,n)-threshold secret sharing schemes that satisfy condition (1) and another condition (2') $\sum_{\{i:P_i\in A\}} H(C_i) < tH(S)$, rather than (2).

Now we propose constructions of ideal (t,n)-threshold schemes in which the threshold value can be adjusted for achieving better communication complexity in the secret reconstruction phase.

Let the set of secrets be $S = GF(q) \times GF(q)$ for some prime power q. We construct an ideal $(2,n)$-threshold scheme as follows. Let $q > n+2$ and $x_1, \ldots, x_n$ be n public distinct elements in GF$(q)\setminus\{0,1\}$. To share a secret $s = (r_0, r_1) \in$ GF$(q) \times$ GF(q), in the share distribution phase, the dealer chooses two polynomials $f(x), g(x)$ of degree at most 1 and 2, respectively, such that

$$\begin{aligned} f(x) &= r_0 + ax \\ g(x) &= r_0 + b_1 x + b_2 x^2 \text{ and } g(1) \\ &= r_1. \end{aligned}$$

The share given to participant P_i, for $1 \leq i \leq n$, is $(f(x_i), g(x_i))$. We show that the scheme is an ideal $(2,n)$-threshold scheme. First, each individual participant has no information about the secret. To see this, equivalently $f(x)$ and $g(x)$ can be selected as follows. The dealer randomly chooses two values $a, b_2 \in$ GF(q) and constructs two polynomials $f(x) = r_0 + ax$ and $g(x) = r_0 + (r_1 - r_0 - b_2)x + b_2x^2$ for the secret (r_0, r_1). Such choice of polynomials guarantees that the values a and b_2 are independent random values in GF(q). Given the share of participant P_i, that is $(f(x_i), g(x_i)) = (\alpha, \beta)$, we obtain

$$\begin{cases} \alpha = r_0 + ax_i \\ \beta = r_0 + (r_1 - r_0 - b_2)x_i + b_2 x_i^2. \end{cases}$$

Rewrite the equations above, we have

$$\begin{cases} r_0 = -x_i a + \alpha \\ r_1 = (1-x_i)a + (1-x_i)b_2 + \frac{\beta}{x_i} - \frac{\alpha}{x_i} + \alpha. \end{cases}$$

Since x_i, α, β are known and the coefficient matrix of the above equations $\begin{pmatrix} -x_i & 0 \\ (1-x_i) & (1-x_i) \end{pmatrix}$ is invertible, it follows that there exists one-to-one mapping between (r_0, r_1) and (a, b_2). Since a and b_2 are independently and randomly chosen, it follows that P_i has no information about (r_0, r_1).

To see that any two participants, say P_1 and P_2, can recover the secret, first note that P_1 and P_2 can recover $f(0)$ using their *partial* shares $f(x_1)$ and $f(x_2)$. Then, because $f(0) = g(0) = r_0$, P_1 and P_2 can use $g(0), g(x_1), g(x_2)$ to uniquely determine $g(x)$ and recover $r_1 = g(1)$. But now if three participants, say P_1, P_2, and P_3, want to recover

[2]For more information-theoretic background we refer readers to [7].

the secret, they need to reveal their partial shares: that is, P_i reveals $g(x_i)$ for $i = 1, 2, 3$. By using $g(x_1), g(x_2)$ and $g(x_3)$, the polynomial $g(x)$ can be uniquely determined and then the secret $(g(0), g(1))$ can be recovered. Observe that in this case, the total information (messages) needed in recovering the secret is $H(g(x_1)) + H(g(x_2)) + H(g(x_3)) = \frac{3}{2}H(S)$ (notation abused). However, if two participants are involved in the secret reconstruction phase, it is not hard to show that each participant needs to send his full share to the combiner (otherwise it will violate the well-known result that the share of each participant is at least the size of the secret). The total information required is $H(S_1) + H(S_2) = H(f(x_1), g(x_1)) + H(f(x_2), g(x_2)) = 2H(S)$. Thus, we save $\frac{1}{2}H(S)$ bits of communication between the participants and the combiner if three participants are involved in the secret reconstruction phase.

Now we can generalize the construction technique above to build a generic (t, n)-threshold scheme. Assume that the set of secrets is $S = \text{GF}(q)^v$ for some integer v and prime power $q > n + v$. Let $x_1, \ldots, x_n$ be n public distinct elements in $\text{GF}(q) \setminus \{1, 2, \ldots, v\}$. The dealer algorithm proceeds as follows. To share a secret $s = (r_1, r_2, \ldots, r_v) \in \text{GF}(q)^v$, the dealer randomly selects a set of polynomials $(f_1, f_2, \ldots, f_v)$ with the following property: for each $1 \leq i \leq v$

$$f_i(1) = r_1, f_i(2) = r_2, \ldots, f_i(v) = r_i$$

and the degree of f_i is $t+i-2$. The share of participant $P_j, 1 \leq j \leq n$, is $\alpha_j = (f_1(x_j), f_2(x_j) \ldots, f_v(x_j)) \in GF(q)^v$.

Lemma 3.1: The dealer algorithm above gives rise to an ideal (t, n)-threshold secret sharing scheme.

Proof: First of all, we show that shares of any t participants are sufficient for secret reconstruction. Without loss of generality, assume that the t participants are $P_1, \ldots, P_t$ and each participant has share $(f_1(x_i), \ldots, f_v(x_i)), 1 \leq i \leq n$. The secret reconstruction is based on an iterative process: the participants reveal the first component of their shares and recover $r_1 = f_1(1)$ as the degree of f_1 is at most $t - 1$; then they use the second component of their shares, together with $r_1 = f_2(1)$, to recover $r_2 = f_2(2)$, and so on. Next, we show that for any $t - 1$ participants, there is no information about the secret can be recovered from pooling their shares. Without loss of generality, we assume that $P_1, \ldots, P_{t-1}$ are the $t-1$ participants and their shares are $\alpha_1, \ldots, \alpha_{t-1} \in \text{GF}(q)^v$. Set $\mathcal{F}$ as shown in the equation at the bottom of the page. We define $\phi : \mathcal{F} \longrightarrow \text{GF}(q)^v$ by

$$\phi(F(x)) = (f_1(1), \ldots, f_v(v)).$$

It is straightforward to verify that ϕ is one-to-one mapping from $\mathcal{F}$ to $\text{GF}(q)^v$, which yields that $P_1, \ldots, P_{t-1}$ has no information about the secret. □

Now we consider the secret reconstruction for the scheme above. Suppose there are ℓ participants, $A = \{P_1, \ldots, P_\ell\}$, want to reconstruct the secret. Instead of transmitting t full shares to the combiner, each of them sends only a portion of the full share. There are two cases to consider.

Case 1: $\ell > t+v-1$. Select $t+v-1$ participants from A and each of them sends the last component of his share which is a point on $f_v(x)$. Since the degree of $f_v(x)$ is at most $t + v - 2$, $f_v(x)$ can be reconstructed and the secret $s = (f_v(1), \ldots, f_v(v))$ can be recovered. In this case, the secret reconstruction communication rate for A is $\rho = \frac{v}{v+t-1}$, and is greater than $\frac{1}{t}$. Note that since $n \geq t + v - 1$ and the value $\frac{v}{v+t-1}$ is bounded by the optimal value of $\frac{n-t+1}{n}$ according to Theorem 3.1.

Case 2: $\ell \leq t + v - 1$. In this case, instead of revealing the full share, *all* participants P_i from A only reveal their partial shares $(f_{\ell-t+1}(x_i), \ldots, f_v(x_i))$. Using the same strategy for secret reconstruction as described in Lemma 3.1, the secret can be recovered by first reconstructing $f_{\ell-t+1}(x)$, and then $f_{\ell-t+2}(x)$, and so on, until $f_v(x)$ is reconstructed. In this case, the communication rate for A is $\rho = \frac{v}{(v-\ell+t)\ell}$. So, to obtain a better information rate we require $\frac{v}{(v-\ell+t)\ell} > \frac{1}{t}$, a simple calculation implies that $v < l$. Note that the above reconstruction algorithm is the worst-case algorithm, one may improve the communication rate by revealing other parts of the partial shares, rather than all participants from A reveal $(f_{\ell-t+1}(x_i), \ldots, f_v(x_i))$. However, it remains open to optimize the information rate with this approach.

IV. Secret Reconstruction With Partial Broadcast Channels

A *partial broadcast channel* is a communication channel that enables a message to be sent from a sender a to a collection B of receivers such that only members of B can learn the sent message and those outside $B \cup \{a\}$ learn nothing about the message.

We consider the scenario that in the secret reconstruction, participants transmit their shares to the combiner by partial broadcast channels. Assume that there are m partial broadcast channels $X = \{x_1, \ldots, x_m\}$. Each channel x_i is associated with a subset $A_i \subseteq \mathcal{P}$ such that a message sent by one of the participants in A_i to the combiner through x_i can be heard by all other members of A_i. Each participant P_i is a recipient of some channels in X. We use B_i, $B_i \subseteq X$, to denote the channels that are allocated to P_i. Let $\mathcal{B} = \{B_1, \ldots, B_n\}$. We call the set system $(X, \mathcal{B})$ the partial broadcast channels for $\mathcal{P}$.

We assume that the share distribution of a secret sharing scheme has been implemented, that is, each participant P_i already holds a share $s_i \in S_i$. In a conventional secret sharing secret, if an authorised subset A wishes to reconstruct the secret, each participant $P_i \in A$ sends his share s_i (or a related value determined by s_i to the combiner by a *single* point-to-point secure channel). In the partial broadcast channels scenario, the message transmitted through a partial broadcast channel may be heard by other participants. However, each participant P_i has access to *multiple* partial broadcast channels from B_i, intuitively secret reconstruction is possible if P_i can send s_i to the combiner using all the channels from B_i that simulate a single point-to-point secure channel.

$$\mathcal{F} = \left\{ F(x) = (f_1(x), \ldots, f_v(x)) \;\middle|\; \begin{array}{c} f_1(1) = f_2(1) = \cdots = f_v(1) \\ f_2(2) = f_3(2) = \cdots = f_v(2) \\ \vdots \\ f_{v-1}(v-1) = f_v(v-1) \\ F(x_i) = \alpha_i, i = 1, 2, \ldots t-1 \\ \deg(f_j) \leq t + j - 2, \\ j = 1, 2, \ldots, v. \end{array} \right\}.$$

We can generalize *channel share redistribution* in the previous section as follows. Let $A \subseteq \mathcal{P}$ and $A \in \Gamma$. For $P_i \in A$, let $B_i = \{x_{i_1}, \ldots, x_{i_{m_i}}\}$ be the partial broadcast channels allocated to P_i. We define a probabilistic mapping

$$\mathcal{C}_{i,A} : S_i \to C_{i_1,A} \times \ldots \times C_{i_{m_i},A}.$$

We call $\mathcal{C}_{i,A}$ the *channel share redistribution* associated to P_i and A and $\mathcal{C}_A = \{\mathcal{C}_{i,A}; P_i \in A\}$ the channel share redistribution for A. We denote $\mathcal{C}_{i,A} = \mathcal{C}_{i,A}(S_i)$ and $\mathcal{C}_A = \prod_{P_i \in A} \mathcal{C}_{i,A}(S_i)$. That is, on input a share held by P_i, $\mathcal{C}_{i,A}$ outputs a sequence of messages $(c_{i_1,A}, \ldots, c_{i_{m_i},A})$, and then P_i transmits $c_{i_j,A}$ to the combiner using the partial broadcast channel x_{i_j}, for $1 \le j \le m_i$. To guarantee the perfect security, any unauthorised subset of participants should not learn anything about the secret even after getting some secret reconstruction transmissions from the partial broadcast channels. Since the channels are not point-to-point secure channels, the messages transmitted by a participant may be heard by some other participants. We define the additional view of a participant P_i, after participants in A have engaged in secret reconstruction, as follows.

$$\text{View}_{i;A} = \{c_{j_k,A} : x_{j_k} \in B_i \cap B_j, P_j \in A\}.$$

and for a set of participant I, we define

$$\text{View}_{I;A} = \cup_{\{i;P_i \in I\}} \text{View}_{i;A}.$$

Definition 4.1: Let S be a finite set of secrets. A *secret sharing scheme* $\widehat{\Pi}$ for access structure Γ and with partial broadcast channels for secret reconstruction consists of a mapping $\mathcal{D} : S \times R \to S_1 \times \cdots \times S_n$, from the cross product of secrets and random strings to a set of n-tuples (shares) such that the following two conditions hold.

1) The secret can be reconstructed by any authorised set of participants. That is, for every secret $s \in S$ and set $A \in \Gamma$, there exists a channel share redistribution $\mathcal{C}_A : S_A \to C_A$ and a combiner algorithm $h_A : C_A \to S$ such that for every random string r, if $\mathcal{D}(s, r) = \{s_1, \ldots, s_n\}$ then $h_A(\{\mathcal{C}_{i,A}(s_i)\}_{P_i \in A}) = s$.
2) Every unauthorised subset of participants cannot obtain any partial information about the secret (in the information theoretic sense), even after the secret reconstruction. Formally, for any subset $I, A \subseteq \mathcal{P}$ with $A \in \Gamma$ and $I \notin \Gamma$, for every secret $a \in S$, and for every possible collection of shares $\{s_i\}_{P_i \in I}$ and any channel share redistribution $\mathcal{C}_A$

$$p(a|\{s_i\}_{P_i \in I}, \text{View}_{I;A}) = p(a)$$

where the probability is taken over the random string r.

That is, a secret sharing scheme $\widehat{\Pi}$ for access structure Γ with partial broadcast channels has the following properties:

1) $H(S|C_A) = 0$, for any $A \in \Gamma$.
2) $H(S|S_I, \text{View}_{I;A}) = H(S)$, for all $A \in \Gamma$ and $I \notin \Gamma$.

We consider two efficiency measures for the secret construction of the secret sharing schemes with partial broadcast channels:

1) *Channel efficiency:* the number of required partial broadcast channels;
2) *Communication efficiency:* the total number of bits transmitted from the participants to the combiner in the secret reconstruction.

Note that in a conventional secret sharing scheme, the number of private point-to-point channels for n participants is n; and the number of bits transmitted from a t-set of participants is $tH(S)$.

A. Channel Efficiency

It is well known that in a conventional secret sharing scheme, for any set of secrets S ($|S| \ge 2$) there exists a (t, n)-threshold secret sharing scheme. It is natural to ask: given partial broadcast channels $(X, \mathcal{B})$, does there exist a (t, n)-threshold secret sharing scheme that uses $(X, \mathcal{B})$ for secret reconstruction?

We first recall the notion of cover-free families [9].

Definition 4.2: A set system $(X, \mathcal{B})$ with $X = \{x_1, \ldots, x_m\}$ and $\mathcal{B} = \{B_i \subseteq X | i = 1, \ldots, n\}$ is called an (n, m, t)-*cover-free family* (or (n, m, t)-CFF for short) if for any subset $\Delta \subseteq \{1, \ldots, n\}$ with $|\Delta| = t$ and any $i \notin \Delta$

$$|B_i \backslash \cup_{j \in \Delta} B_j| \ge 1.$$

The elements of X are called *points* and elements of $\mathcal{B}$ are called *blocks*. In other words, in an (n, m, t)-CFF $(X, \mathcal{B})$, the union of any t blocks in $\mathcal{B}$ cannot cover any other remaining ones. The following theorem gives a characterization for the channel requirements of (t, n)-threshold secret sharing schemes using partial broadcast channels for secret reconstruction.

Theorem 4.1: Let $(X, \mathcal{B})$ be the partial broadcast channels and let S ($|S| \ge 2$) be the set of secrets. There exists a (t, n)-threshold sharing scheme using partial broadcast channels $(X, \mathcal{B})$ for secret reconstruction if and only if $(X, \mathcal{B})$ is an $(n, m, t-1)$

Proof: First we show the sufficiency. Assume that Π is a conventional (t, n)-threshold secret sharing scheme. Without loss of generality, we assume that the share space S_i for participant P_i is an additive group. Also assume that the set of partial broadcast channels allocated to P_i is $B_i = \{x_{i_1}, \ldots, x_{i_{m_i}}\}$. Let $A \subseteq \mathcal{P}$ and $|A| \ge t$. For each $P_i \in A$, define the channel share redistribution mapping

$$\mathcal{C}_{i,A} : S_i \to C_{i_1,A} \times \cdots \times C_{i_{m_i},A},$$

by $\mathcal{C}_{i,A}(s_i) = (s_i - \sum_{j=2}^{m_i} r_{i_j}, r_{i_2}, \ldots, r_{i_{m_i}})$, where $C_{i_j} = S_i$, for $1 \le j \le m_i$, and r_{i_j}'s are randomly chosen from C_{i_j}, for $2 \le j \le m_i$. It is easy to see the combiner after receiving all the transmitted messages from the participants in A can reconstruct the secret by applying the combiner algorithm specified in Π. That is, $H(S|C_A) = 0$. It is left to show that $H(S|S_I, \text{View}_{I;A}) = H(S)$, for all $|I| < t$ and $|A| \ge t$. Indeed, for each $P_j \notin I$, since $(X, \mathcal{B})$ is an $(n, m, t-1)$-cover-free family, we have $|B_j \setminus \cup_{\{k:P_k \in I\}} B_k| \ge 1$. That means there exists at least one channel from B_j that is secure against all the participants from I. Since the share s_j is split into m_j shares (note that $\mathcal{C}_{j,A}$ gives rise to an (m_j, m_j)-threshold secret sharing scheme). Thus, all participants from I cannot get at least one share and so they have no information about the share s_i. That is, $H(S_j|S_I, \text{View}_{I;A}) = H(S_j)$ for all $P_j \in A$ and $P_j \notin I$. It follows that $H(S|S_I, \text{View}_{I;A}) = H(S|S_I) = H(S)$.

Conversely, assume that the set system of partial broadcast channels $(X, \mathcal{B})$ is not an $(n, m, t-1)$-cover-free family. Then there exists a participant P_i and a set $A \subseteq \mathcal{P}$ such that $P_i \in A, |A| = t$ and $B_i \subseteq \cup_{\{j;P_j \in A \setminus \{P_i\}\}} B_j$. It follows that any information transmitted by P_i will also be learnt by the coalition of participants from $A \setminus \{P_i\}$, and therefore, $H(S|S_I, \text{View}_{I;A}) = H(S|S_A) = 0$, where $I = A \setminus \{P_i\}$, which contradicts the assumption that any $t-1$ participants should not be able to obtain any information about the secret. □

Cover-free families were first studied in terms of superimposed binary codes by Kautz and Singleton [15]. Erdös, Frankl, and Füredi [9] studied cover-free families as combinatorial objects that generalize the Sperner systems. Cover-free families have been discussed by numerous researchers in the subjects of information theory, combinatorics, communication and cryptography.

In [9], Erdös, Frankl and Füredi derived the following upper bound on n for k-uniform cover-free families (that is $|B_i| = k$ for all k). That is, in any k-uniform (n, m, t)-CFF

$$n \leq \binom{m}{\lceil \frac{k}{t} \rceil} \Big/ \binom{k}{\lceil \frac{k}{t} - 1 \rceil}.$$

The above bound can be reached for some special cases. For example, there exists a probabilistic construction in [9] for a $2t$-uniform (n, m, t)-CFF with $n = (m^2/4t) - o(m^2)$. In the general case, the best lower bound on m is given in [24] as follows. For any (n, m, t)-CFF with $t \geq 2$, $m \geq c\frac{t^2}{\log t} \log n$ for some constant $c \approx 1/2$.

Using a probabilistic method, Erdös, Frankl and Füredi [9] proved the existence of (n, m, t)-CFF with $m = O(t^2 \log n)$ and $|B_i| = O(t \log n)$ for any $t \geq 2$.

By applying the previous results on cover-free families, the following result can be obtained.

Corollary 4.1: There exists a (t, n)-threshold secret sharing scheme using $O(\log n)$ partial broadcast channels for secret reconstruction.

B. Communication Rates for Partial Broadcast Channels

We generalize the communication rate for the secret construction using partial broadcast channels.

Definition 4.3: Let S be a finite set of secrets. We define the communication rates for a secret sharing scheme with partial broadcast channels as follows.

- Given a secret sharing scheme $\widehat{\Pi}$ for access structure Γ with partial broadcast channels $(X, \mathcal{B})$ for secret reconstruction, where $B_i = \{x_{i_1}, \ldots, x_{i_{m_i}}\}$, $i = 1, 2, \ldots, n$. The communication rate for $A \in \Gamma$ is defined as

$$\widehat{\rho}_{(A,\widehat{\Pi})} = \frac{H(S)}{\sum_{\{i:P_i \in A\}} \sum_{j=1}^{m_i} H(C_{i_j})}.$$

- Given a secret sharing scheme $\widehat{\Pi}$ for an access structure Γ, the communication rate for $\widehat{\Pi}$ is defined as

$$\rho_{\widehat{\Pi}} = \min_{A \in \Gamma} \rho_{(A,\widehat{\Pi})}.$$

- Given an access structure Γ, the communication rate for Γ is defined as

$$\rho_{\Gamma} = \sup_{\widehat{\Pi} \in \mathcal{S}} \rho_{\widehat{\Pi}}$$

where $\mathcal{S}$ is the space of all secret sharing schemes for the access structure Γ with the partial broadcast channels.

We say a cover-free family $(X, \mathcal{B})$ is a *minimal* (n, m, t)-cover-free family if the size of each block $B_i \in \mathcal{B}$ is minimal. In other words, for any $B_i \in \mathcal{B}$ and any $a \in B_i$, $(X, \mathcal{B}')$ is no longer an (n, m, t)-cover-free family, where $\mathcal{B}' = \{B_1, \ldots, B_{i-1}, B_i', B_{i+1}, \ldots, B_n\}$ and $B_i' = B_i \setminus \{a\}$. It is easy to see that given an (n, m, t)-cover-free family $(X, \mathcal{B})$ one can always remove some elements from each block, if necessary, until it becomes a minimal (n, m, t)-cover-free family.

Theorem 4.2: Let $(X, \mathcal{B})$ be a minimal $(n, m, t-1)$-cover-free family. Let S be a finite set of secrets and $\widehat{\Pi}$ be a (t, n)-threshold secret sharing scheme with partial broadcast channels $(X, \mathcal{B})$. Then for any $A \subseteq \mathcal{P}$ and $|A| \geq t$,

$$\widehat{\rho}_{(A,\widehat{\Pi})} \leq \frac{|A| - t + 1}{|A|}.$$

Moreover, if there exists $P_j \in A$ such that $|B_j| \geq 1$, then the above strict inequality holds.

Proof: Let $A \subseteq \mathcal{P}$ with $|A| = \ell \geq t$ be the set of participants who want to reconstruct the secret. We assume that the combiner receives the transmitted data $c_i \in C_i$ from participant P_i. Then using an identical argument from Theorem 3.1, we can show that $\sum_{\{i:P_i \in A\}} \sum_{j=1}^{m_i} H(C_{i_j}) \geq \sum_{\{i:P_i \in A\}} H(C_i) \geq \frac{\ell}{\ell - t + 1} H(S)$.

We show the second part of the theorem. Since there exists P_j such that $|B_j| = m_j > 1$. That is, P_j needs to use the partial broadcast channels from B_j to securely transmit at least $\frac{1}{\ell - t + 1} H(S)$ bits to the combiner. Assume that the channel share redistribution mapping is $\mathcal{C}_{j,A} : S_j \to C_{j_1} \times \cdots \times C_{j_{m_j}}$, we show that

$$\sum_{k=1}^{m_j} H(C_{j_k}) > \frac{1}{\ell - t + 1} H(S) \tag{5}$$

Indeed, we may assume that $H(C_j | C_{j_1}, \ldots, C_{j_m}) = 0$ and $H(C_j | C_{j_i}) = H(C_j)$. It follows that the mapping $\mathcal{C}_{i,A}$ gives rise to a $(1, r, m_j)$-ramp scheme for some $2 \leq r \leq m_j$. Hence we have

$$\sum_{k=1}^{m_j} H(C_{j_k}) \geq \frac{m_j}{m_j - r + 1} H(C_j) > \frac{1}{\ell - t + 1} H(S).$$

The strict inequality of the theorem then follows the last inequality from above and the result follows. □

Similar to the case of using point-to-point communication channels, we have the following strict bounds on the communication rate in the model of partial broadcast channels.

Corollary 4.2: Let $(X, \mathcal{B})$ be a minimal $(n, m, t-1)$-cover-free family and $m < n$. Let S be a finite set of secrets and $\widehat{\Pi}$ be a (t, n)-threshold secret sharing scheme with partial broadcast channels $(X, \mathcal{B})$. Then $\widehat{\rho}_{\Pi} < \frac{n - t + 1}{n}$.

Note that the bound in Theorem 4.2 depends on the underlying partial broadcast channels $(X, \mathcal{B})$. It also indicates that there is a tradeoff between the channel efficiency and the communication complexity when using partial broadcast channels.

C. Constructions

It is tempted to construct a (t, n)-threshold secret sharing scheme with partial broadcast channels that achieves both good channel efficiency and high communication rate. We suggest the following generic approach:

Step 1) apply a (t, n)-threshold secret sharing scheme with high communication rate (in the conventional point-to-point communication setting) to generate and distribute shares to participants;

Step 2) apply techniques of ramp secret sharing schemes to the channel share redistribution in secret reconstruction.

Techniques developed in Section III-B can be applied to Step 1) directly. We suggest to use ramp schemes to construct the channel share redistribution in Step 2).

Assume that $A \subseteq \mathcal{P}$, $|A| \geq \ell$, is the set of participants who want to reconstruct the secret. Let c_i be the output of the channel share redistribution algorithm in Step 1) for participant $P_i \in A$. To guarantee the perfectness of the scheme, it is sufficient for P_i to transmit c_i to the combiner using partial broadcast channels $B_i = \{x_{i_1}, \ldots, x_{i_{m_i}}\}$ in a secure way that protects against coalition of any other $t - 1$ participants. The channel share redistribution algorithm given in Theorem 4.1 splits c_i to m_i shares using an (m_i, m_i)-threshold secret sharing scheme, and each share is then transmitted by a partial broadcast channel. Thus, the communication cost is about m_i times of that in the secure point-to-point communication setting. The communication cost can be improved, depending on the structure of the underlying broadcast channels $(X, \mathcal{B})$.

Let

$$u_i = \min\{|B_i \setminus \cup_{j\in\Delta} B_j|; i \notin \Delta \subseteq \{1,2,\ldots,n\}, |\Delta| = t-1\}.$$

Now, instead of using an (m_i, m_i)-threshold secret sharing scheme, we split c_i using an $(m_i - u_i - 1, m_i, m_i)$-ramp scheme. If an optimal ramp scheme can be adopted, then communication cost of sending c_i will become $\frac{m_i}{u_i} H(C_i)$, which yields an improving factor of $1/u_i$.

V. Conclusion

In this correspondence, we study the communication efficiency problems of secret reconstruction in secret sharing schemes. We showed that there exists a tradeoff between the communication cost and the number of participants involved in secret reconstruction. We also relaxed the requirement of having secure point-to-point communication channels as in conventional secret sharing schemes and showed that certain partial broadcast channels are sufficient to do secret reconstruction. Secret sharing schemes are known to be playing important roles in building distributed security systems and secure multiparty computation. An interesting research topic that can be worked on in the future is to apply the results of this correspondence to the construction of more efficient secure multiparty cryptographic protocols. Another interesting problem is to find some more efficient constructions with optimal or suboptimal communication complexity.

References

[1] S. Barwick, W.-A. Jackson, and K. Martin, "Updating the parameters of a threshold scheme by minimal broadcast," *IEEE Trans. Inf. Theory*, vol. 51, pp. 620–633, 2005.

[2] A. Beimel and B. Chor, "Secret sharing with public reconstruction," *IEEE Trans. Inf. Theory*, vol. 44, no. (5, pp. 1887–1896, 1998.

[3] G. R. Blakey, "Safeguarding cryptographic keys," in *Proc. AFIPS 1979 Nat. Comput. Conf.*, 1979, vol. 48, pp. 313–317.

[4] G. R. Blakely and C. Meadows, "Security of ramp schemes," *Adv. Crypt.: Crypto'84*, vol. 196, pp. 242–268, 1984.

[5] C. Blundo, A. De Santi, D. R. Stinson, and U. Vaccaro, "Graph decompositions and secret sharing schemes," *J. Crypt.*, vol. 8, pp. 39–64, 1995.

[6] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, "On the size of shares for secret sharing schemes," *J. Crypt.*, vol. 6, pp. 157–169, 1993.

[7] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[8] Y. Desmedt and Y. Wang, "Perfectly secure message transmission revisited," in *Proc. EuroCrypt'02*, Lecture Notes in Computer Science 2332, pp. 502–517.

[9] P. Erdös, P. Frankl, and Z. Furedi, "Families of finite sets in which no set is covered by the union of r others," *Israel J. Math.*, vol. 51, pp. 79–89, 1985.

[10] M. Franklin and M. Yung, "Secure hypergraphs: Privacy from partial broadcast," in *Proc. ACM STOC'95*, 1995, pp. 36–44, ACM Press.

[11] M. Franklin and R. Wright, "Secure communication in minimal connectivity models," *J. Crypt.*, vol. 13, no. 1, pp. 9–30, 2000.

[12] O. Goldreich, S. Goldwasser, and N. Linial, "Fault-tolerant computation in the full information model," *SIAM J. Comput.*, vol. 27, no. 2, pp. 506–544, 1998.

[13] W. A. Jackson and K. M. Martin, "A combinatorial interpretation of ramp schemes," *Australasian J. Combin.*, vol. 14, pp. 51–60, 1996.

[14] E. Karnin, J. Greene, and M. Hellman, "On secret sharing systems," *IEEE Trans. Inf. Theory*, vol. 29, pp. 35–41, 1983.

[15] W. H. Kautz and R. C. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inf. Theory*, vol. IT-10, pp. 363–377, 1964.

[16] K. Martin, J. Pieprzyk, R. Safavi-Naini, and H. Wang, "Changing thresholds in the absence of secure channels," *Australian Comput. J.*, vol. 31, pp. 34–43, 1999.

[17] W. Ogata and K. Kurosawa, "Some basic properties of general nonperfect secret sharing schemes," *J. Universal Comput. Sci.*, vol. 4, no. 8, pp. 690–704, 1998.

[18] R. Safavi-Naini and H. Wang, "Secret sharing schemes with partial broadcast channels, manuscript," *Des. Codes Cryptogr.*, vol. 41, pp. 5–22, 2006.

[19] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, 1979.

[20] R. Steinfeld, H. Wang, and J. Pieprzyk, "Lattice-based threshold changeability for standard Shamir secret-sharing schemes," *Adv. Crypt—Asiacrypt 2004, Lecture Notes in Computer Science*, vol. 3329, pp. 170–186, 2004.

[21] R. Steinfeld, J. Pieprzyk, and H. Wang, "Dealer-free threshold changeability for standard CRT secret-sharing schemes," *Finite Fields and Their Applications*, vol. 12, pp. 653–680, 2006.

[22] D. R. Stinson, "An explication of secret sharing schemes," *Des. Codes Cryptogr.*, vol. 2, pp. 357–390, 1992.

[23] D. R. Stinson, T. Trung van, and R. Wei, "Secure frameproof codes, key distribution patterns, group testing algorithms and related structures," *J. Stat. Plan. Infer.*, vol. 86, pp. 595–617, 2000.

[24] D. R. Stinson, R. Wei, and L. Zhu, "Some new bounds for cover-free families," *J. Combin. Theory, A*, vol. 90, pp. 224–234, 2000.

Minimum Pseudoweight and Minimum Pseudocodewords of LDPC Codes

Shu-Tao Xia and Fang-Wei Fu

***Abstract*—In this correspondence, we study the minimum pseudoweight and minimum pseudocodewords of low-density parity-check (LDPC) codes under linear programming (LP) decoding. First, we show that the lower bound of Kelley, Sridhara, Xu, and Rosenthal on the pseudoweight of a nonzero pseudocodeword of an LDPC code whose Tanner graph has girth greater than 4 is tight if and only if this pseudocodeword is a real multiple of a codeword. Then, the lower bound of Kashyap and Vardy on the stopping distance of an LDPC code is proved to be also a lower bound on the pseudoweight of a nonzero pseudocodeword of an LDPC code whose Tanner graph has girth 4, and this lower bound is tight if and only if this pseudocodeword is a real multiple of a codeword. Using these results we further obtain that for some LDPC codes, there are no other minimum pseudocodewords except the real multiples of minimum weight codewords. This means that the LP decoding for these LDPC codes is asymptotically optimal in the sense that the ratio of the probabilities of decoding errors of LP decoding and maximum-likelihood decoding approaches 1 as the signal-to-noise ratio (SNR) tends to infinity. Finally, some LDPC codes are listed to illustrate these results.**

***Index Terms*—Fundamental cone, linear programming (LP) decoding, low-density parity-check (LDPC) codes, pseudocodewords, pseudoweight, stopping sets.**

I. Introduction

While studying iterative decoding of low-density parity-check (LDPC) codes, Wiberg [28] and Koetter and Vontobel [12] showed that pseudocodewords play an important role when characterizing the performance of LDPC codes. Koetter and Vontobel [12] presented an explanation for the relevance of pseudocodewords in iterative decoding

Manuscript received June 8, 2006; revised November 11, 2006. This research is supported in part by the NSFC-GDSF Joint Fund under Grant U0675001, the Major State Basic Research Development Program of China (973 Program) under Grant 2003CB314801, and the open research fund of National Mobile Communications Research Laboratory, Southeast University, China. The material in this correspondence was presented in part at the 2006 IEEE Information Theory Workshop, Chengdu, China, October 2006.

S.-T. Xia is with the Graduate School at Shenzhen of Tsinghua University, Shenzhen, Guangdong 518055, China, and also with the National Mobile Communications Research Laboratory, Southeast University, Nanjing 210096, China (e-mail: xiast@sz.tsinghua.edu.cn).

F.-W. Fu is with the Chern Institute of Mathematics and the Key Laboratory of Pure Mathematics and Combinatorics, Nankai University, Tianjin 300071, China (e-mail: fwfu@nankai.edu.cn).

Communicated by M. P. Fossorier, Associate Editor for Coding Techniques.
Digital Object Identifier 10.1109/TIT.2007.911177