On the Secure Conditions for Distributed Storage Systems

Rui Zhu and Wangmei Guo
State Key Lab. of ISN, Xidian University, Xian 710071, China
Email: rzhu@stu.xidian.edu.cn, wangmeiguo@mail.xidian.edu.cn

***Abstract*—The problem of secure distributed storage systems (DSS) with regenerating codes is concerned in this paper. We consider an eavesdropper model where an eavesdropper wiretaps a subset of storage nodes, and either their repairing data or stored data can be wiretapped. We focus on two typical and special cases, the Minimum Bandwidth Repair (MBR) and the Minimum Storage Repair (MSR). Our main contribution is to draw a connection between this problem and secure network coding theory introduced by Cai and Yeung, and the secrecy capacity can be determined in this method. We prove that for both MBR and MSR cases, if the maximal wiretapped information rate can be determined, the secrecy capacity can be achieved by linear secure network coding. Particularly, a static exact regenerating code can be transformed into a secure regenerating code for the MBR and MSR cases.**

I. Introduction

The demand for huge volumes' data, driven by distributed (cloud) computing, social networks, data sharing, etc., has increased in the past decades. These applications call for a reliable and secure storage system, and then distributed storage systems are becoming the de-facto mechanism for large scale data storage systems. In a distributed storage system (DSS), the massive source data should be dispersed and/or encoded into many smaller components to be stored in a storage node. The storage systems are vulnerable to security breaches for node failure and potential eavesdroppers, and coding approaches can improve the resilience to these threats.

Recent years have witnessed the development of network coding theory and techniques for distributed storage systems. The paradigm of network coding [1], [2] has provided rich source of new problems that generalize traditional problems in communications, followed by a large body of further work in the literature. In [3], Dimakis et al. introduced the theory of regenerating codes. Formally, consider a DSS with n storage nodes. The user then downloads the source data by connecting to any k storage nodes and decoding the received data. Such property is also called (n, k) MDS property and will be introduced formally in the subsequent section. If the user (or Data Collector, DC) directly connects to these n nodes to download a file, any node failure would cause the breakdown of the DSS. Thus, redundancy is introduced into the system to improve reliability against node failures and coding technique can improve the performance.

With the increasing awareness of data security and privacy protection, developing secure distributed storage systems have attracted attentions of researchers and engineers. The main threats to a DSS are potential eavesdroppers and adversarial attacks. Cai and Yeung proposed their pioneer work on secure network coding in [4] and later published in [5]. Their work shows that the maximum achievable rate (i.e. the *secrecy capacity*) for this problem is given by $n-r$ packets if the field size q is sufficiently large, where r is the maximal edges the eavesdroppers can access. When the collection of wiretapping sets is arbitrary, Cui et al. presented the cutset bound in [6] and proposed that this upper bound is unachievable for some cases. They also proved the NP-hardness of deriving the secrecy capacity for arbitrary wiretapping set eavesdroppers.

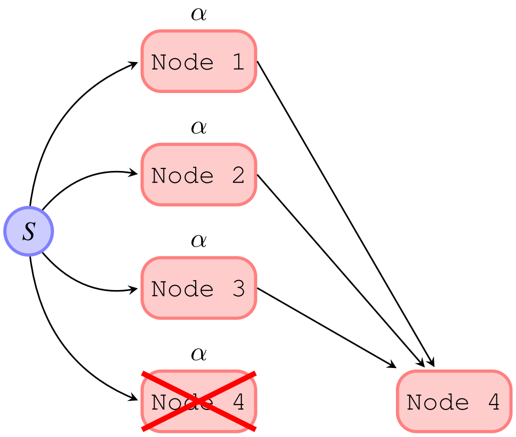

Fig. 1: A simple model for DSS

The secure distributed storage system against eavesdroppers with the read-access to any $l(< k)$ storage nodes has been studied in detail by Pawar et al. [7]. They proposed an upper bound of secrecy capacity for this model and proved that for a special regime called bandwidth-limited regime, their bound is tight by providing an explicit coding scheme. Later in [8], Shah et al. proposed a generalized type of eavesdroppers, called (l, l') eavesdroppers, with the read-access of l storage nodes and l' of these nodes are wiretapped during repairing. They also designed secure distributed storage codes at the *Minimum Bandwidth Repair* (MBR) point and the *Minimum Storage Repair* (MSR) point. For the MBR point, their code can prevent any eavesdroppers with $l < k$ and $l' \leq l$ for all (n, k, d). For the MSR point, their code can be constructed at $(n, k, d \geq 2k-2)$ for all (l, l'), but the secure optimality is only proved for $l' = 0$ in their paper. The recent unpublised work [9] by Rawat et al. derived a new upper bound for secrecy capacity, which proved the optimality of Shah's code for $l' = 1$. Their work also included a new type of secure regenerating codes for MSR, achieving the capacity when $d = n - 1$ and $l' \leq 2$ motivated by Maximal Rank Distance codes [10] and Zigzag codes [11].

In this paper, we address the problem of secure distributed storage systems using regenerating codes. Our main contribution is to prove that the upper bound in [9] is tight at the MSR point for all (n, k, d) and any (l, l') eavesdroppers, making the secrecy capacity be determined. We firstly present the DSS model and the eavesdroppers model under information-theoretic framework. For practical consideration, we focus on two special cases: the systems at the MBR and MSR points. There have been increasing attention on these two cases for their optimality and many good exact repair codes have been found, facilitating the study of secure distributed storage codes.

This paper is organized as follows. In Section II we describe the system and the eavesdroppers model. We present our main general approach in Section III. In Section IV, we study the secure distributed storage systems for MBR and MSR systems. The paper is concluded in Section V.

II. Models and notations

In this section, we propose a formal description of distributed storage system with regenerating codes. A DSS consists of a source file M, n storage nodes (we call them *Storage Node Set* $\mathcal{N}$) and some potential user nodes (or Data Collector, DC). Each of the storage node has a storage capacity of α. With entropy functions we rewrite it as

$$H(Y_i) = \alpha$$

where Y_i denotes the data stored in node i. A DC can reconstruct the source file M by connecting to any k storage nodes and this property is called (n, k) *MDS Property*. Under the information theory framework, we have:

$$H(M|Y_{\mathcal{K}}) = 0, \quad \text{for all } \mathcal{K} \subseteq \mathcal{N}, |\mathcal{K}| = k, \tag{1}$$

where $|\mathcal{K}|$ indicates the cardinality of the set $\mathcal{K}$, and we call $\mathcal{K}$ as the *Download Node Set*.

If a storage node i is failed, the newcomer i' will connect to any other $d(\geq k)$ nodes to recover the failed data. We focus on single node repairing. (For multi-node repairing, we refer readers to literature about *Coordinated Repairing* [12], or *Cooperative Repairing* [13]). The set of nodes participating in repairing node i is denoted as $\mathcal{D}_i$ (we call $\mathcal{D}_i$ the *Helper Node Set*) and we may drop the lower index i without ambiguity in some cases. We denote $\hat{Y}_i$ as data after repairing node i. If $\hat{Y}_i$ is always identical with Y_i, we call *Exact Repair*; otherwise, we call the repairing as *Functional Repair*. During the repairing procedure, node j transmits data S_j^i to node i and the communication bandwidth is denoted as β:

$$H(S_j^i) = \beta.$$

We denote $S_{\mathcal{A}}^i$ as the set of data from a set of storage nodes $\mathcal{A}$ to storage node i and $S_j^{\mathcal{A}}$ as the set of data from j to $\mathcal{A}$ as follows:

$$\begin{aligned} S_{\mathcal{A}}^i &\triangleq \{S_m^i\}_{m \in \mathcal{A}}, \\ S_j^{\mathcal{A}} &\triangleq \{S_j^m\}_{m \in \mathcal{A}}. \end{aligned}$$

From the network coding perspective, $S_{\mathcal{A}}^i$ consists of information symbols on incoming edges of i from node set $\mathcal{A}$ and $S_j^{\mathcal{A}}$ consists of symbols on outcoming edges of j to the node set $\mathcal{A}$. If the repairing symbols $S_{\mathcal{D}}^i$ is irrelevant with the choice of helper node set $\mathcal{D}$ for all node i at any time, we call this special regenerating code as *Static Regenerating Code*. Under the information theory framework, the symbols S_m^i from node m should be a function of Y_m, and the recovering data $\hat{Y}_i$ should be a function of all helping symbols $S_{\mathcal{D}}^i$. That is,

$$H(S_m^i|Y_m) = 0, \tag{2}$$

$$H(\hat{Y}_i|S_{\mathcal{D}_i}^i) = 0. \tag{3}$$

A. The Properties for MBR and MSR

Both the work of [3] and [14] explained the cutset bound(or min-cut analysis) for the distributed storage model. The cutset bound is as follows:

$$\mathcal{M} \leq \sum_{i=1}^{k} \min\{\alpha, (d - i + 1)\beta\}. \tag{4}$$

And [3] showed that this bound is achievable by functional repair codes based on random network coding. Based on this bound, they found a storage-bandwidth tradeoff curve given the maximal file size $\mathcal{M}$. A tradeoff curve can be established from the cutset bound (4). For the optimal repairing scheme, the storage capacity α ranges from $(d - k + 1)\beta$ to $d\beta$:

$$(d - k + 1)\beta \leq \alpha \leq d\beta$$

Two edge points in the tradeoff curve indicate optimality in storage capacity and repair bandwidth. For $\alpha = d\beta$, the repairing bandwidth $\gamma = d\beta$ meets the smallest value α, and it is the MBR case; for $\alpha = (d-k+1)\beta$, the storage capacity is $\mathcal{M}/k$ and this is the minimum storage per node, the MSR case. Both of these definitions were proposed in [3].

For the sake of convenience, we may call a DSS as an MBR system if the parameters α, β are at the MBR point of the storage-capacity tradeoff curve. The MSR system is similarly defined as the MBR system. Also, the MBR case and the MSR case refer to storage systems at the MBR and MSR point, respectively.

B. Eavesdropper Model

In this paper, we consider the (l, l') eavesdropper proposed by Shah et al. in [8]. Their definition is generalized from Pawar et al. in [7], which defined an eavesdropper with the read-access of $l(< k)$ storage nodes at any time. The eavesdropper can wiretap them among the initial n storage nodes, or to wait for failures and eavesdrop on their repairing data. For an (l, l') eavesdropper, he/she can wiretap l storage data and access both the storage and repairing data at l' nodes of them. In the subsequent sections, we always denote the set of l storage nodes as $\mathcal{E}$ and the set of wiretapped l' storage nodes during repairing as $\mathcal{E}'$, i.e. $\mathcal{E}' \subseteq \mathcal{E}$. The symbols $Z_{\mathcal{E}}$ denote the data received by the eavesdropper when he/she wiretaps the storage node set $\mathcal{E}$.

To protect storage data against eavesdroppers, the source data M should be randomized by a random key K, which is independent of the message. The stored data Y_i is encoded and distributed by both M and K:

$$H(Y_i|M,K) = 0, \quad i \in \mathcal{N}. \tag{5}$$

Our target is to store the source file M under *Perfect Secrecy* conditon, i.e.

$$H(M|Z_{\mathcal{E}}) = H(M). \tag{6}$$

Given a distributed storage system with parameter (n, k, d) and an (l, l')-eavesdropper, its secrecy capacity, denoted as C^s, is defined as the maximum amount of stored data such that the reconstruction, repairable and secure property are simutaneously satisfied for all possible data collectors and eavesdroppers. The secrecy condition is defined as follows (similar definition from [7])

$$C^s(\alpha, \beta) \triangleq \sup_{\mathcal{K},\mathcal{E}:(1),(6)\text{hold}} H(M). \tag{7}$$

For the sake of convenience, we may denote C^s instead of $C^s(\alpha, \beta)$ in most cases.

III. Approach

In this section, we propose our main framework in studying the security problem of distributed storage systems. According to the study of secure network coding by Tao et al. in [6], the problem to determine the secrecy capacity of arbitrary wiretapping set is NP hard. The eavesdropper model in this paper can be equivalent with a node-wise wiretapper in the information flow graph in [3] as follows: a wiretapped storage node during its repairing can be regarded as the eavesdropper wiretaps the "in" node; otherwise, for stored data, it is equivalent with wiretapping "out" node. Yet few results for this node-wise eavesdropper model have been found in the literature. However, the following theorem indicates that, if all information on edges in a wiretapping set is a function (or combination) of that on edges in a minimum cut, the problem can be equivalent with linear secure network against r-eavesdropper [5], which can wiretap any r edges in a network.

Theorem 1. *Suppose the eavesdropper wiretaps a subset of nodes denoted as $\mathcal{E}$. If $H(Z_{\mathcal{E}}|Y_{\mathcal{K}}) = 0$, i.e. all wiretapping data are a function of stored data in any k storage nodes, then the secrecy capacity can be derived as follows:*

$$C^s = \mathcal{M} - \max_{\mathcal{E}} H(Z_{\mathcal{E}}) \tag{8}$$

where $\mathcal{M}$ is the storage capacity from the cutset bound in Eq. (4).

Proof:
Direct part: Since an r-secure network coding can prevent the collection of all subsets of channels with cardinality not exceeding r, the transformation can be obtained if $H(Z_{\mathcal{E}})$ is determined.
Converse part: Suppose the eavesdropper wiretaps the set $\mathcal{E}$ of survival nodes. Let $\mathcal{K}$ be any k nodes out of n storage nodes in the system. Thus, we can derive the secrecy rate by

$$\begin{aligned}
H(M) &= H(M|Z_{\mathcal{E}}) - H(M|Z_{\mathcal{E}}, Y_{\mathcal{K}}) && (9)\\
&= I(M; Y_{\mathcal{K}}|Z_{\mathcal{E}}) && (10)\\
&\leq H(Y_{\mathcal{K}}|Z_{\mathcal{E}}) && (11)\\
&= H(Z_{\mathcal{E}}|Y_{\mathcal{K}}) + H(Y_{\mathcal{K}}) - H(Z_{\mathcal{E}}) && (12)\\
&= H(Y_{\mathcal{K}}) - H(Z_{\mathcal{E}}) && (13)\\
&= \mathcal{M} - H(Z_{\mathcal{E}}). && (14)
\end{aligned}$$

By expanding $H(Y_{\mathcal{K}}, Z_{\mathcal{E}})$ in two ways, Eq.(12) can be derived. Eq. (13) is from the condition $H(Z_{\mathcal{E}}|Y_{\mathcal{K}}) = 0$. The converse part then can be directly proved by Eq. (14). ■

Here we indicate the relationship between Theorem 1 and linear secure network coding by Cai and Yeung. If the eavesdropper wiretaps r edges, he/she can wiretap at most r symbols in the network. Denoted as $H(Z_{\mathcal{W}})$, where $\mathcal{W}$ is representing the wiretapped edges and $Z_{\mathcal{W}}$ is a collection of wiretapped symbols, we have $H(Z_{\mathcal{W}}) \leq r$ and the identity holds when edges in $\mathcal{W}$ are all included in a minimum cut and thus r random keys are necessary to prevent it. In Theorem 1, $Z_{\mathcal{E}}$ plays the same role of r wiretapped edges, and thus the secure network coding can work with r random keys mixed in the source node.

In [15] and later in [7], Pawar et al. proposed an upper bound against eavesdropper if no more than l nodes are wiretapped. The upper bound is as follows:

$$C^s \leq \sum_{i=l+1}^{k} \min\{\alpha, (d-i+1)\beta\} \tag{15}$$

This upper bound is achievable for MBR by Shah et al. in [8], but it seems hard to find a proper code to achieve this upper bound for the MSR point. We will analyze this phenomenon in the next section. The key step is to evaluate whether the condition $H(Z_{\mathcal{E}}|Y_{\mathcal{K}}) = 0$ holds for these two cases. If so, the secrecy capacity is only associated with the accurate value of $H(Z_{\mathcal{E}})$.

IV. Two Special Cases: MBR and MSR

In this section, we study the security problem for two special distributed storage systems, MBR and MSR. These two cases are optimal in repairing bandwidth and storage, respectively, and then attract most attention to study. In the subsequent analysis of these two cases, the wiretapped data can be proved to be a function of information on edges in a minimum cut. The problem of secrecy capacity is then directly reduced into determining the wiretapped information rate $H(Z_{\mathcal{E}})$.

With the knowledge of $H(Z_{\mathcal{E}})$, the secrecy capacity approach code can be established by precoding at the source node along with "proper" exact regenerating codes. The "proper" regenerating codes are defined for those exact repair codes, which the repairing data for a particular node i, $S^i_{\mathcal{D}}$, is independent with the choice of helper node set. This property is motivated by secure regenerating codes designed in [8], where both MBR and MSR codes are exact repair codes and information downloaded by the replacement node is designed to be independent of the helper node set.

A. The MBR Case

Next, we attempt to study the secrecy rate for the MBR systems. For the MBR case, we have

$$H(Y_{\mathcal{K}}) = \sum_{i=1}^{k}(d-i+1)\beta \geq H(S_{\mathcal{D}}^{\mathcal{K}}). \tag{16}$$

And, from 2, we have

$$\begin{aligned} H(Y_{\mathcal{K}}|S_{\mathcal{D}}^{\mathcal{K}}) &= 0, & (17)\\ H(Y_{\mathcal{K}}) \leq H(Y_{\mathcal{K}}, S_{\mathcal{D}}^{\mathcal{K}}) &= H(S_{\mathcal{D}}^{\mathcal{K}}). & (18)\end{aligned}$$

Combining (16), (17) and (18), it suffices to imply that storage data $Y_{\mathcal{K}}$ are identical with their repairing data under some invertible transformations, i.e., $H(Y_{\mathcal{K}}|S_{\mathcal{D}}^{\mathcal{K}}) = 0$ and $H(S_{\mathcal{D}}^{\mathcal{K}}|Y_{\mathcal{K}}) = 0$. Thus, we have

$$\begin{aligned} H(Z_{\mathcal{E}}|Y_{\mathcal{K}}) &\leq H(Z_{\mathcal{E}}|S_{\mathcal{D}}^{\mathcal{K}}) & (19)\\ &= 0. & (20)\end{aligned}$$

Here we can find that for MBR systems, any static exact MBR code can be linearly transformed into a secure MBR code. For each MBR exact repair code, the storage data of node l and the repairing data $S_{\mathcal{D}}^{l}$ can be linearly transformed by invertible linear transformation. It implies that repairing data for exact MBR can be independent with the choice of $\mathcal{D}$. Thus, an exact MBR code is actually a static MBR code, and the following theorem can be proved.

Theorem 2. *Any MBR exact repair code can be linearly transformed into a secure MBR code for all (l, l') eavesdropper, and it is a static regenerating code.*

B. The MSR Case

Theorem 2 and a practical code proposed by Shah et al. in [8] can solve the security problems for MBR cases. For MSR cases, the minimum cuts in the information flow graph are all storage edges. Then, when the eavesdropper wiretaps the repairing symbols, he/she can receive more symbols than a storage node and lead to worse situation. In this case, we cannot directly find the characterization of secrecy capacity by the cutset bound.

In this subsection, we solve this problem in the following way. Firstly, we revisited the upper bound in [9] by Rawat et al. This upper bound has an very intuitive description motivating us to prove its tightness. Then, we prove that repairing data must be the function of storage data in any k nodes. This is equivalent to check whether $H(Z_{\mathcal{E}}|Y_{\mathcal{K}}) = 0$. At last, by Theorem 1, the upper bound can be achieved with randomness mixture at the source node and employing the static regenerating code. For $d = n-1$, the exact repair code is static since the only choice for the helper node set is to choose all other surviving nodes. For $d < n-1$, the existence of such exact code can be found in [8], although their code is not optimal for $l' \geq 2$.

In recent unpublished work [9], the authors presented a new upper bound for $H(M)$ and designed a Interference-Alignment based code to achieve such upper bound when $d = n-1$. Here we denote the l wiretapped nodes as the set $\mathcal{E}$ and the set of l' node, whose repairing data were wiretapped, is denoted as $\mathcal{E}'$. The proposed upper bound is as follows:

Theorem 3. *[9] For a bandwidth efficient repairable (n, k) MDS code, we have*

$$C^s \leq \sum_{i \in \mathcal{K}\backslash\mathcal{E}} \left(\alpha - H(S_i^{\mathcal{E}'})\right). \tag{21}$$

This upper bound can be intuitively interpreted in the following way. For those secure nodes (which is not wiretapped) in $\mathcal{K}$, denoted as $\mathcal{K}\backslash\mathcal{E}$, each of them can contribute to secure rate by $H(Y_i|S_i^{\mathcal{E}'})$, which equals to $\alpha - H(S_i^{\mathcal{E}'})$. Note that their bound can be derived under functional repair.

Theorem 4. *For a MSR distributed storage system under exact repair, any collection $\mathcal{K}$ of k storage nodes, repairing symbols S_m^i is a function of stored data in $\mathcal{K}$, where $i \in \mathcal{K}$ and $m \neq i$.*

Note that the proof seems to be trival since any k storage nodes can reconstruct the source file. However, as Cui et al. proposed in their paper [6], the terminal node in a wiretapped network is not necessarily to receive all random keys, and key cancellation can enhance secrecy rate in some cases. The essential is that secure multicast problem is equivalent to broadcasting rather than multicasting, since the source message M can be equivalent with the common message and random keys are sort of private messages. Before the proof of this theorem, we need to recall a varied version of the data processing inequality to facilitate the proof.

Lemma 1. *If Z is a function of U and V, then $H(U, V) \geq H(V, Z)$.*

Proof: The condition is equivalent to $H(Z|U, V) = 0$ and thus we have $H(U, V, Z) = H(Z|U, V) + H(U, V) = H(U, V)$. Since $H(U, V, Z) \geq H(V, Z)$, we then have $H(U, V) \geq H(V, Z)$. ■

Proof of Theorem 4: Let i be the failed node and m be an arbitrary helper node of i. Choose another $k-1$ storage nodes with i to be the set $\mathcal{K}$. We assume that $m \notin \mathcal{K}$, since $H(S_m^i|Y_{\mathcal{K}}) = 0$ for $m \in \mathcal{K}$. Let $\mathcal{B}$ be another $d-k$ helper nodes except those in $\mathcal{K}$ and the node m. Then we have:

$$\begin{aligned} & H(S_m^i, Y_{\mathcal{K}}) & \\ = \; & H(S_m^i, Y_i, Y_{\mathcal{K}\backslash i}) & (22)\\ \leq \; & H(S_m^i, S_{\mathcal{B}}^i, S_{\mathcal{K}\backslash i}^i, Y_{\mathcal{K}\backslash i}) & (23)\\ = \; & H(S_m^i, S_{\mathcal{B}}^i, Y_{\mathcal{K}\backslash i}) & (24)\\ \leq \; & H(S_{m\cup\mathcal{B}}^i) + H(Y_{\mathcal{K}\backslash i}) & (25)\\ \leq \; & (d-k+1)\beta + (k-1)\alpha & (26)\\ = \; & k\alpha. & (27)\end{aligned}$$

Eq. (23) follows by the repairing equation $H(Y_i|S^i_m, S^i_{\mathcal{B}}, S^i_{\mathcal{K}\backslash i}) = 0$ and substituting variables $U = (S^i_{\mathcal{B}}, S^i_{\mathcal{K}\backslash i})$,$V = S^i_m$ and $Z = Y_i$ into Lemma 1. Eq. (24) follows from $H(S^i_{\mathcal{K}\backslash i}|Y_{\mathcal{K}\backslash i}) = 0$, and Eq. (25) follows from the Independence bound on entropy, or the chain rule of joint entropy. On the other hand, we also have

$$\begin{aligned} H(S^i_m, Y_{\mathcal{K}}) &\geq H(Y_{\mathcal{K}}) \quad (28)\\ &= k\alpha. \quad (29)\end{aligned}$$

Then it must be that $H(S^i_m, Y_{\mathcal{K}}) = H(Y_{\mathcal{K}})$, which leads to $H(S^i_m|Y_{\mathcal{K}}) = 0$. ■

Along with Theorem 1, we can conclude that for MSR under exact repair, the secrecy capacity is only associate with the minimum $H(Z_{\mathcal{E}})$, the rate of wiretapped information. Thus, for (l, l') eavesdropper, we can estimate a lower bound for $H(Z_{\mathcal{E}})$:

$$\max_{\mathcal{E}} H(Z_{\mathcal{E}}) \geq l\alpha + H(S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}). \quad (30)$$

If the upper bound could be achieved, Eq. (30) should attain the identity and it is the target for the following part of this subsection.

Lemma 2. *For a (n, k, d) MSR distributed storage system, if the node i is failed and the helper node set is $\mathcal{D}$. Let $\mathcal{A}$ be a subset of $\mathcal{D}$ with the cardinality of $k-1$, and $\mathcal{B}$ be the complement of $\mathcal{A}$ in $\mathcal{D}$. Thus we have*

$$H(S^i_{\mathcal{B}}|Y_i, S^i_{\mathcal{A}}) = 0. \quad (31)$$

Proof: As the lemma stated, we separate $\mathcal{D}$ as two sets:$\mathcal{A}$ and $\mathcal{B}$ and $|\mathcal{A}| = k-1, |\mathcal{B}| = d-k+1$. Then, we have:

$$\begin{aligned} I(S^i_{\mathcal{B}}; Y_i, S^i_{\mathcal{A}}) &= I(S^i_{\mathcal{B}}; S^i_{\mathcal{A}}) + I(S^i_{\mathcal{B}}; Y_i|S^i_{\mathcal{A}}) \quad (32)\\ &\geq I(S^i_{\mathcal{B}}; Y_i|S^i_{\mathcal{A}}) \quad (33)\\ &= H(Y_i|S^i_{\mathcal{A}}). \quad (34)\end{aligned}$$

For the MSR system, storage data in any k storage nodes are mutually independent, which leads to the mutual independence of elements in $Y_{\mathcal{A}}$ and Y_i [1] (and also for $S^i_{\mathcal{A}}$ and Y_i [2]). Thus we have:

$$\begin{aligned} H(Y_i|S^i_{\mathcal{A}}) &= H(Y_i) \quad (35)\\ &= (d-k+1)\beta \quad (36)\end{aligned}$$

and

$$I(S^i_{\mathcal{B}}; Y_i, S^i_{\mathcal{A}}) \geq \alpha = (d-k+1)\beta. \quad (37)$$

On the other hand, we have

$$\begin{aligned} &I(S^i_{\mathcal{B}}; Y_i, S^i_{\mathcal{A}})\\ \leq\ &H(S^i_{\mathcal{B}}) \quad (38)\\ \leq\ &(d-k+1)\beta. \quad (39)\end{aligned}$$

Then, it must be that $I(S^i_{\mathcal{B}}; Y_i, S^i_{\mathcal{A}}) = (d-k+1)\beta = H(S^i_{\mathcal{B}})$, which leads to

$$\begin{aligned} H(S^i_{\mathcal{B}}|Y_i, S^i_{\mathcal{A}}) &= H(S^i_{\mathcal{B}}) - I(S^i_{\mathcal{B}}; Y_i, S^i_{\mathcal{A}}) \quad (40)\\ &= 0. \quad (41)\end{aligned}$$

Then Lemma 2 can be directly derived by Eq. (41). ■

Lemma 3. *For a secure MSR regenerating code against (l, l') eavesdropper, if it is an exact repair code and the repairing data for each node is independent of the helper node set, the maximal wiretapped information rate $H(Z_{\mathcal{E}})$ is given by*

$$\max_{\mathcal{E}} H(Z_{\mathcal{E}}) = l\alpha + H(S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}). \quad (42)$$

Proof: From Eq. (30), we only need to prove the converse part:

$$H(Z_{\mathcal{E}}) \leq l\alpha + H(S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}).$$

Without loss of generality, let $\mathcal{K}$ be the first k storage nodes: $1, 2, \dots, k$; let $\mathcal{E}$ denote the first l storage nodes: $1, 2, \dots, l$; and let $\mathcal{E}'$ denote the first l' storage nodes: $1, 2, \dots, l'$, i.e., $\mathcal{E}' \subseteq \mathcal{E}$. According to the statement, the secrecy capacity approach code should satisfy that $S^i_{\mathcal{D}}$ are independent with $\mathcal{D}$. Thus, we assume that for each node i, $k-1$ of helper nodes are from $\mathcal{K}\backslash i$, and the rest $d-k+1$ nodes are from the same set $\mathcal{B}$. We thus have

$$\begin{aligned} &H(Z_{\mathcal{E}})\\ \leq\ &H(S^{\mathcal{E}'}_{\mathcal{D}}, Y_{\mathcal{E}\backslash\mathcal{E}'}) \quad (43)\\ =\ &H(S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}, S^{\mathcal{E}'}_{\mathcal{E}}, S^{\mathcal{E}'}_{\mathcal{D}\backslash\mathcal{K}}, Y_{\mathcal{E}\backslash\mathcal{E}'}) \quad (44)\\ =\ &H(S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}, S^{\mathcal{E}'}_{\mathcal{E}}, S^{\mathcal{E}'}_{\mathcal{D}\backslash\mathcal{K}}, Y_{\mathcal{E}\backslash\mathcal{E}'}, Y_{\mathcal{E}'}) \quad (45)\\ =\ &H(S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}, S^{\mathcal{E}'}_{\mathcal{D}\backslash\mathcal{K}}, Y_{\mathcal{E}}) \quad (46)\\ =\ &H(S^{\mathcal{E}'}_{\mathcal{D}\backslash\mathcal{K}}|S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}, Y_{\mathcal{E}}) + H(S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}, Y_{\mathcal{E}}). \quad (47)\end{aligned}$$

Eq. (44) follows from separating the helper node set $\mathcal{D}$ into three parts $\mathcal{E}, \mathcal{K}\backslash\mathcal{E}, \mathcal{D}\backslash\mathcal{K}$. Eq. (45) follows from the repairing procedure $H(Y_{\mathcal{E}'}|S^{\mathcal{E}'}_{\mathcal{D}}) = 0$ and Eq. (46) follows from $H(S^{\mathcal{E}'}_{\mathcal{E}}|Y_{\mathcal{E}}) = 0$. Now we focus on the first term of Eq. (47). By Lemma 2, for each $i \in \mathcal{E}'$, we have

$$\begin{aligned} &H(S^i_{\mathcal{D}\backslash\mathcal{K}}|Y_{\mathcal{E}}, S^i_{\mathcal{K}\backslash\mathcal{E}}) \quad (48)\\ =\ &H(S^i_{\mathcal{D}\backslash\mathcal{K}}|Y_i, Y_{\mathcal{E}\backslash i}, S^i_{\mathcal{K}\backslash\mathcal{E}}) \quad (49)\\ \leq\ &H(S^i_{\mathcal{D}\backslash\mathcal{K}}|Y_i, S^i_{\mathcal{E}\backslash i}, S^i_{\mathcal{K}\backslash\mathcal{E}}) = 0. \quad (50)\end{aligned}$$

That is, $H(S^i_{\mathcal{D}\backslash\mathcal{K}}|Y_{\mathcal{E}}, S^i_{\mathcal{K}\backslash\mathcal{E}}) = 0$. Thus, we have

$$\begin{aligned} H(S^{\mathcal{E}'}_{\mathcal{D}\backslash\mathcal{K}}|Y_{\mathcal{E}}, S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}) &\leq \sum_{i\in\mathcal{E}'} H(S^i_{\mathcal{D}\backslash\mathcal{K}}|Y_{\mathcal{E}}, S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}) \quad (51)\\ &\leq \sum_{i\in\mathcal{E}'} H(S^i_{\mathcal{D}\backslash\mathcal{K}}|Y_{\mathcal{E}}, S^i_{\mathcal{K}\backslash\mathcal{E}}) \quad (52)\\ &= 0. \quad (53)\end{aligned}$$

Substituting Eq. (53) into Eq. (47), we have

$$\begin{aligned} H(Z_{\mathcal{E}}) &\leq H(S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}, Y_{\mathcal{E}}) \quad (54)\\ &\leq H(S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}) + H(Y_{\mathcal{E}}) \quad (55)\\ &= l\alpha + H(S^{\mathcal{E}'}_{\mathcal{K}\backslash\mathcal{E}}). \quad (56)\end{aligned}$$

[1] For a subset of k storage nodes in an MSR system, we have $H(Y_{\mathcal{K}}) = k\alpha = \sum_{i\in\mathcal{K}} H(Y_i)$. Thus, for any $i, j \in \mathcal{K}$, Y_i and Y_j are independent. It also holds for Y_i and $Y_{\mathcal{A}}$ if $|\mathcal{A}| < k$.

[2] If $I(Y_i; Y_{\mathcal{A}}) = 0$, since $H(S^i_{\mathcal{A}}|Y_{\mathcal{A}}) = 0$, we have $I(S^i_{\mathcal{A}}; Y_i) \leq I(Y_{\mathcal{A}}; Y_j) = 0$ by data processing inequality, which implies the independence between $S^i_{\mathcal{A}}$ and Y_i.

The lemma then directly holds from Eq. (56). ■

From Lemma 3, we can conclude that for each secure exact repair code with the independence of identities of helper nodes, the maximal wiretapped rate can be estimated. We can give an alternative form of MSR secrecy capacity by the following theorem.

Theorem 5. *For a bandwidth efficient repairable (n, k) MDS code at MSR point, the upper bound (21) is tight and the secrecy capacity can be found if for any node i and $\mathcal{E}'$, $H(S_i^{\mathcal{E}'})$ is minimized.*

C. Discussions

Functional repair and exact repair are two typical repairing types for regenerating codes. In the pioneer work by Dimakis et al., their bound is derived by functional repair, which can be equivalent with a multicast problem. However, Shah et al. proved in [14] that only MBR and MSR points in storage-bandwidth tradeoff curve can be met for exact repair. Most exact repair codes are algebraic constructed with explicit structures, and have advantages over random network coding based funtional repair. The exact repair codes also transcend the limitations of random network coding based functional code in a secure DSS. This phenomena is described in [15] and later in [7] by giving an example. Their idea can be illustrated as the following fact: if a node fails frequently, for example, t times, the eavesdropper can receive $t\gamma = td\beta$ symbols and they are mutually linearly independent with high probability for systems using random network coding. It motivates us to answer such question: is the secrecy capacity for functional repair as same as that of exact repair?

From our analysis of two special cases, MBR and MSR, we can conclude that for those two cases, the answer is yes. For MBR, we prove that any exact MBR code can be transformed into a secure code; for MSR, we prove that the static exact repair code can achieve the secrecy capacity. Since the exact repair can be regarded as a special case of functional case, if an exact repair code can achieve the secrecy capacity under functional repair, the equality of secrecy capacity for both functional repair and exact repair is proved. Thus, for practical consideration, designing a proper exact repairing code is the main objective for secure distributed storage systems.

V. Conclusion

In this paper we consider secure regenerating codes for dynamic distributed storage systems. Our main objective is to investigate characteristics and conditions for secure regenerating codes, and focuses on two special cases: MBR and MSR. We draw a connection between secure regenerating codes and secure network codes by Cai and Yeung in [5] to determine the secrecy capacity. For MBR, the exact MBR code is static since repairing data is identical with storage data, which also implies that wiretapped data are always a function of storage data in any k storage nodes. For MSR, we prove that a new upper bound proposed in [9] is tight for MSR codes. Our proof is based on the analysis of static exact regenerating codes, in which repairing data for a particular node is independent with the choice of helper node set $\mathcal{D}$. With randomness mixture before storage encoding, the upper bound is achievable and it implies that the biggest challenge in secure MSR code constructing is to minimize the rate of repairing data from any node i to any other l' node.

Acknowledgement

This work was partially supported by a grant from the National Natural Science Foundation of China (Ref. No. 61271174).

References

[1] R. Ahlswede, N. Cai, S. Li, and R. Yeung, "Network information flow," *Information Theory, IEEE Transactions on*, vol. 46, no. 4, pp. 1204–1216, 2000.

[2] S. Li, R. Yeung, and N. Cai, "Linear network coding," *Information Theory, IEEE Transactions on*, vol. 49, no. 2, pp. 371–381, 2003.

[3] A. Dimakis, P. Godfrey, Y. Wu, M. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *Information Theory, IEEE Transactions on*, vol. 56, no. 9, pp. 4539–4551, 2010.

[4] N. Cai and R. Yeung, "Secure network coding," in *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*. IEEE, 2002, p. 323.

[5] ——, "Secure network coding on a wiretap network," *Information Theory, IEEE Transactions on*, vol. 57, no. 1, pp. 424–435, 2011.

[6] T. Cui, T. Ho, and J. Kliewer, "On secure network coding with unequal link capacities and restricted wiretapping sets," in *IEEE Information Theory Workshop (ITW)*, 2010.

[7] S. Pawar, S. El Rouayheb, and K. Ramchandran, "Securing dynamic distributed storage systems against eavesdropping and adversarial attacks," *Information Theory, IEEE Transactions on*, vol. 57, no. 10, pp. 6734–6753, 2011.

[8] N. Shah, K. Rashmi, and P. Kumar, "Information-theoretically secure regenerating codes for distributed storage," in *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*. IEEE, 2011, pp. 1–5.

[9] A. Rawat, O. Koyluoglu, N. Silberstein, and S. Vishwanath, "Optimal locally repairable and secure codes for distributed storage systems," *arXiv preprint arXiv:1210.6954*, 2012.

[10] D. Silva and F. Kschischang, "Universal secure network coding via rank-metric codes," *Information Theory, IEEE Transactions on*, vol. 57, no. 2, pp. 1124–1135, 2011.

[11] I. Tamo, Z. Wang, and J. Bruck, "Zigzag codes: Mds array codes with optimal rebuilding," *Information Theory, IEEE Transactions on*, vol. 59, no. 3, pp. 1597 –1616, march 2013.

[12] A.-M. Kermarrec, N. Le Scouarnec, and G. Straub, "Repairing multiple failures with coordinated and adaptive regenerating codes," in *Network Coding (NetCod), 2011 International Symposium on*. IEEE, 2011, pp. 1–6.

[13] K. W. Shum, "Cooperative regenerating codes for distributed storage systems," in *Communications (ICC), 2011 IEEE International Conference on*. IEEE, 2011, pp. 1–5.

[14] N. Shah, K. Rashmi, P. Kumar, and K. Ramchandran, "Distributed storage codes with repair-by-transfer and non-achievability of interior points on the storage-bandwidth tradeoff," *Information Theory, IEEE Transactions on*, no. 3, pp. 1837–1852, 2012.

[15] S. Pawar, S. El Rouayheb, and K. Ramchandran, "On secure distributed data storage under repair dynamics," in *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*. IEEE, 2010, pp. 2543–2547.