New Bounds for Distributed Storage Systems with Secure Repair

Ravi Tandon[1] and Soheil Mohajer[2]

[1]Discovery Analytics Center & Department of Computer Science, Virginia Tech, Blacksburg, VA
[2]Department of Electrical and Computer Engineering, University of Minnesota, Twin Cities, MN

***Abstract*— In this paper, we consider exact-repair distributed storage systems. Characterizing the optimal storage-vs-repair bandwidth tradeoff for such systems remains an open problem, in general with results available in the literature for very specific instances. We characterize the optimal tradeoff between storage and repair bandwidth if in addition to exact-repair requirements, an additional requirement of pair-wise symmetry on the repair process is imposed. The optimal tradeoff surprisingly consists of only one efficient point, namely the minimum bandwidth regenerating (MBR) point. These results are also extended to the case in which the stored data (or repair data) must be secure from an external wiretapper, and the correspondingly optimal secure tradeoffs are also characterized. The main technical tool used in the converse proofs is a use of Han's inequality for sub-sets of random variables. Finally, we also present results in which the pair-wise symmetry constraint is relaxed and a new converse bound is obtained for the case of exact repair in which an external adversary can access the repair data of any one node. This bound improves upon the existing best known results for the secure and exact repair problem.**

I. Introduction

Contemporary distributed storage systems store massive amounts of data over a set of distributed nodes. Besides the traditional goals of achieving reliability by introducing redundancy, new aspects such as efficient repair of failed storage nodes make their design even more challenging. To overcome these issues, the concept of regenerating codes for distributed storage systems was introduced by Dimakis *et al.* [3]. A distributed storage system (DSS) consists of n storage nodes each with a storage capacity of α units of data such that the entire file of size $\mathcal{B}$ can be recovered by accessing any $k < n$ nodes. This is called as the reconstruction property of the DSS. Whenever a node fails, d nodes (where $k \leq d \leq n-1$) participate in the repair process by sending β units of data each. This procedure is termed as the regeneration of a failed node and β is referred to as the per-node repair bandwidth.

In [3], by using the concepts of network coding [4], the authors show that the parameters of a DSS must satisfy

$$\mathcal{B} \leq \sum_{i=0}^{k-1} \min\left(\alpha, (d-i)\beta\right). \tag{1}$$

Thus, in order to store a file of size $\mathcal{B}$, there exists a fundamental tradeoff between α (storage) and $d\beta$ (total repair bandwidth). However, this tradeoff is in general achievable only for the functional-repair case [3]. In functional repair, a failed node is replaced by a new node such that the resulting DSS has the same reconstruction and regeneration capabilities as before. In particular, the contents of the repaired node may not necessarily be identical to the failed node even though the desirable properties of the DSS are preserved.

In contrast to functional repair, exact repair regeneration requires the repair process to replace a failed node with an identical new node. Exact repair is a practically appealing property specially when it is desirable that the stored contents remain intact over time. Furthermore, the file recovery process is also easier in this case as the reconstruction procedure need not change whenever a failed node is replaced. While characterizing the storage-vs-bandwidth tradeoff for the case of exact repair remains a challenging open problem in general, two extreme points of this tradeoff (depending on whether α or β is minimized first) namely, the minimum storage regenerating case (MSR) and the minimum bandwidth regenerating (MBR) case have been studied extensively (see [5], [6] and references therein). Beyond these points, the optimal exact-repair tradeoff for the $(4,3,3)$-DSS was characterized in [7] where it has been shown that the optimal tradeoffs for functional and exact repair are different. There have been several recent works in this regard, namely new outer bounds (converse results beyond $(4,3,3)$) in [14], as well as novel achievable schemes in [15] and [16], and new results for secure and exact repair in [17]–[19]. Even though these recent advances have brought forth new insights on the fundamental problem of exact repair, the general problem of characterizing the optimal tradeoff for the exact repair problem remains open till date.

Besides the requirements of exact repair, another important design concern for such systems is that of data security. Pawar et.al [9] introduced the notion of information theoretic security for such systems where various models for the adversary are introduced and investigated. In one of those models (which we refer to as Type-I model), the adversary can access the data stored in any $\ell < k$ nodes. In another model (referred to as the Type-II model), the adversary is more powerful and can access not only the content of the nodes but the repair data of any $\ell < k$ nodes sent by other nodes to repair. The focus of this paper is on the exact repair problem with such security constraints and the main contributions of this paper are two fold:

- For the distributed storage system with an external

E-mail: tandonr@vt.edu, soheil@umn.edu

adversary, we obtain new outer bounds for the exact and secure repair problem. In particular, we consider the general (n, k, d) DSS operating in the presence of an eavesdropper which can read the repair data of any ℓ nodes. The goal is to find the maximum size of data which can be stored while being information theoretically secure from such adversary. An upper bound on the admissible file size for this general problem was obtained in [9] together with some optimality results; however the general problem still remains open. We develop a new bound for this problem for general parameters (n, k, d) and for $\ell = 1$ and show that it outperforms the bounds of [9].

- We also focus on the exact repair problem with an additional condition of pair-wise symmetric repair. The pair-wise symmetric repair condition refers to the following: consider any two storage nodes, for example, nodes i and j and a set of other $(d-1)$ helper nodes which we denote collectively as $\mathcal{H}$. Now, consider the repair of node i from node j and the fixed $(d-1)$ helper nodes and denote the repair data send by node j as $S_{j\to i}$. Similarly, considering the repair of node j from node i and the same set of fixed helper nodes, we define the repair data sent from node i to node j as $S_{i\to j}$. Then, the pair-wise symmetric repair condition enforces that $S_{i\to j} = S_{j\to i}$. In other words, it means that given the fixed set of $(d-1)$ helper nodes, the data which node i sends to repair node j must be the same as the data which node j must send to repair node i. Through a novel converse proof, we characterize the optimal tradeoff of the exact repair problem along with the pair-wise symmetry condition. Interestingly, the tradeoff only has one efficient point (namely the minimum bandwidth regenerating (MBR)) point, the achievability for which has been established in [11]. The pair-wise symmetry restriction also presents an operation interpretation of the MBR point and shows that there exists no other (more efficient) exact repair point satisfying such a condition.

Notation: We denote the set $\{1, 2, \ldots, m\}$ by $[m]$ for $m \in \mathbb{Z}^+$. For any set $\mathcal{A} \subseteq [n]$ we define $W_{\mathcal{A}} = \{W_i : i \in \mathcal{A}\}$. For sets $\mathcal{A}, \mathcal{B} \subseteq [n]$, we define $S_{\mathcal{A}\to\mathcal{B}} = \{S_{i\to j} : i \in A, j \in B\}$. Finally we use $S_{\mathcal{A}\leftrightarrow\mathcal{B}}$ to denote the union of repair data in both directions, i.e, $(S_{\mathcal{A}\to\mathcal{B}}, S_{\mathcal{B}\to\mathcal{A}})$.

II. System Model

A (n, k, d, ℓ) DSS consists of n storage nodes that store a file F of size $\mathcal{B}$ across n nodes, with each node storing up to α units of data. A data collector connects to any $k < n$ nodes in order to reconstruct the file F. This is known as the MDS property of the DSS [3]. We focus on single node failures in which at any given point only one node in the system could fail. For the repair of a failed node, any d out of the remaining $(n-1)$ *alive* nodes send $\beta \leq \alpha$ units of data in order to aid the repair process. The parameter $d\beta$ is referred to as the total repair bandwidth. From an information theoretic perspective, the goal is to store a file F, whose entropy is $\mathcal{B}$, i.e., $H(F) = \mathcal{B}$. Let W_i denote the storage content at node i, for $i = 1, 2 \ldots, n$. Hence,

$$H(W_i) \leq \alpha, \quad \forall\ i = 1, 2, \ldots, n. \tag{2}$$

Due to the MDS property we also have

$$H\left(F|W_{\mathcal{K}}\right) = 0, \quad \forall \mathcal{K} \subset [n] \text{ with } |\mathcal{K}| = k. \tag{3}$$

Let $S_{i\to j}$ denote the data sent by node i to repair node j. Due to the repair bandwidth constraint, we have

$$H(S_{i\to j}) \leq \beta, \quad \forall i, j \in [n] \tag{4}$$

and for *exact repair* of node j from d nodes, we also have

$$H(W_j|S_{\mathcal{D}\to j}) = 0, \quad j \notin \mathcal{D} \subset [n], |\mathcal{D}| = d. \tag{5}$$

Since $S_{i\to j}$ is a function of the data stored in node i, we have $H(S_{i\to j}|W_i) = 0$.

Secrecy Constraints: We also have another parameter $\ell < k$, which signifies the number of nodes an adversary can wiretap. In particular, we consider two types of adversaries:

- Type-I: adversary can wiretap only the stored data on any ℓ nodes. For any $\ell < k$ nodes to be secure, we require

$$I\left(F; W_{\mathcal{L}}\right) = 0, \quad \forall \mathcal{L} \subset [n] \text{ with } |\mathcal{L}| \leq \ell \tag{6}$$

  where $W_{\mathcal{L}}$ is the data stored on nodes whose index belong to $\mathcal{L}$.
- Type-II: adversary can wiretap the repair data of any ℓ nodes. For the repair of any $\ell < k$ nodes to be secure, we require

$$I\left(F; S_{n_1}, S_{n_2} \ldots, S_{n_\ell}\right) = 0, \tag{7}$$

  where S_{n_i} is the repair data downloaded from any other d nodes to repair node n_i. Note that the d nodes repairing n_i might be different from those helping to repair n_j.

We first note that the Type-I adversary is in general weaker than Type-II adversary since the constraint (7) implies (6) but not the other way around. Finally, we note that by setting $\ell = 0$, we recover the original problem with no security constraints.

III. Main Results & Discussion

Theorem 1 *The secrecy capacity of an (n, k, d) storage system with Type-II secrecy against an eavesdropper who observes the repair data for any $\ell = 1$ node is upper bounded by*

$$\mathcal{B}^S \leq \frac{k-1}{4}\alpha + \frac{(k-1)(3d-2k)}{4}\beta. \tag{8}$$

The best existing results for the Type-II secrecy problem with general parameters are in [9] which shows that

$$\mathcal{B}^S \leq \sum_{i=l}^{k-1} \min\left(\alpha, (d-i)\beta\right). \tag{9}$$

The result of Theorem 1 improves upon the above bound in general. We next illustrate our bound in (8) together with the

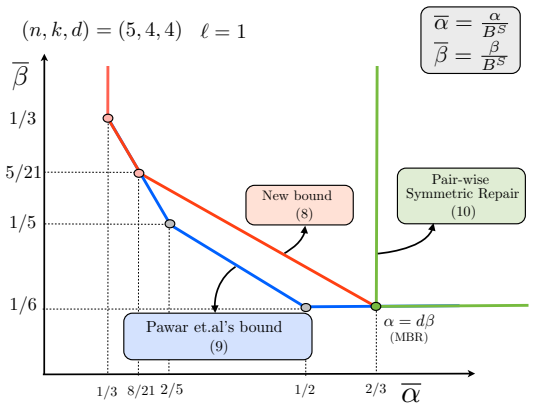

Fig. 1: Bounds for $(n,k,d)=(5,4,4)$ and $\ell=1$.

bound in (9) for the case of $(n,k,d)=(5,4,4)$ and $\ell=1$ in Figure 1.

We strongly believe that even being tighter, the bound in Theorem 1 is not achievable. We in fact conjecture that the secrecy capacity for a general (n,k,d,ℓ) system with strong secrecy constraint is upper bounded by

$$\mathcal{B}^S \leq \left[(k-l)d - \left(\binom{k}{2} - \binom{\ell}{2}\right)\right] \min\left(\frac{\alpha}{d}, \beta\right) \quad (10)$$

In particular, this conjecture suggests that the MBR point in the only efficient point on the optimum trade-off for the strong secrecy capacity of DSSs.

Specific scenarios for which the Type-II secrecy problem has been completely solved are in [17]–[19], and correspond to the following cases:

- All (n,k,d,ℓ), $d \leq 3$
- $(n,k,d)=(n,n-1,n-1)$ and $\ell=n-2$.

For all these cases, this conjecture has been proved to be true.

Even though we are unable to prove this conjecture under the general setting, we next consider a constrained version of this problem with a *pair-wise symmetric repair* condition and prove that the optimal trade-off for this restricted problem is indeed given by the above bound.

The pair-wise symmetric repair condition refers to the following: consider any two storage nodes, for example, nodes i and j and a set of other $(d-1)$ helper nodes which we denote collectively as $\mathcal{H}$. Now, consider the repair of node i from node j and nodes in $\mathcal{H}$ and denote the repair data send by node j as $S_{j\to i}$. Similarly, considering the repair of node j from node i and the same set of fixed helper nodes $\mathcal{H}$, we define the repair data sent from node i to node j as $S_{i\to j}$. Then, the pair wise symmetric repair condition enforces that $S_{i\to j}=S_{j\to i}$. In other words, it means that given the fixed set of $(d-1)$ helper nodes, the data which node i sends to repair node j must be the same as the data which node j must send to repair node i and hence the name pair-wise symmetric repair.

Theorem 2 *The optimal (α,β) trade-off for an (n,k,d,ℓ) distributed storage system with exact and pair-wise symmetric repair is given by*

$$\mathcal{B}^S \leq \left[(k-l)d - \left(\binom{k}{2} - \binom{\ell}{2}\right)\right] \min\left(\frac{\alpha}{d}, \beta\right) \quad (11)$$

for both Type-I and Type-II secrecy.

This result shows that with the symmetric pair-wise repair constraint, the only efficient point in the storage-bandwidth tradeoff is the MBR point. This also provides another operational interpretation of the MBR point.

The proofs for Theorems 1 and 2 are presented next.

IV. Proof of Theorem 1

In this section we focus on the case of Type-II secrecy with $\ell=1$, and present the proof of Theorem 1.

Let $\mathcal{A}\subseteq[d+1]$ be an arbitrary set with $|\mathcal{A}|=k-1$, and $i\in[d+1]\setminus\mathcal{A}$ be an index not in $\mathcal{A}$. We have

$$\begin{aligned}
\mathcal{B}^S &= H(F) = H(F|S_{[d+1]\setminus\{i\}\to i}) \\
&= H(F, S_{[d+1]\to i}) - H(S_{[d+1]\to i}) \qquad (12)\\
&\leq H(F, W_{\mathcal{A}}, S_{[d+1]\to i}) - H(S_{[d+1]\to i}) \\
&= H(W_{\mathcal{A}}, S_{[d+1]\to i}) - H(S_{[d+1]\to i}) \\
&= H(W_{\mathcal{A}}) + H(S_{[d+1]\to i}|W_{\mathcal{A}}) - H(S_{[d+1]\to i}) \\
&\leq H(W_{\mathcal{A}}) + H(S_{[d+1]\to i}|S_{\mathcal{A}\to i}) - H(S_{[d+1]\to i}) \\
&= H(W_{\mathcal{A}}) - H(S_{\mathcal{A}\to i}). \qquad (13)
\end{aligned}$$

where in (12) we just added $S_{i\to i}$ to what the eavesdropper observes, and set $S_{i\to i}$ to be a dummy variable with zero entropy.

In order to bound $H(S_{\mathcal{A}\to i})$ we can write

$$\begin{aligned}
H(S_{\mathcal{A}\to i}) &= \frac{1}{\binom{d}{k-1}} \sum_{\substack{\mathcal{A}\subset[d+1]\setminus\{i\}\\|\mathcal{A}|=k-1}} H(S_{\mathcal{A}\to i}) \qquad (14)\\
&\geq \frac{k-1}{d}\frac{1}{\binom{d}{d}} \sum_{\substack{\mathcal{A}'\subset[d+1]\setminus\{i\}\\|\mathcal{A}'|=d}} H(S_{\mathcal{A}'\to i}) \qquad (15)\\
&\geq \frac{k-1}{d} H(W_i). \qquad (16)
\end{aligned}$$

where (14) follows from the symmetry of the repair variables, that is, $H(S_{\mathcal{A}\to i})$ is invariant w.r.t. the choice of $\mathcal{A}\subset[d+1]\setminus\{i\}$ provided that $|\mathcal{A}|=k-1$; (15) follows from Han's inequality [13]; and inequality in (16) holds since the content of node i can be reconstructed from repair data downloaded from nodes in $\mathcal{A}'$ with $|\mathcal{A}'|=d$.

In order to upper bound $H(W_{\mathcal{A}})$, we can write

$$\begin{aligned}
H(W_{\mathcal{A}}) &= \sum_{i=1}^{k-1} H(W_i|W_{[i-1]}) \\
&= \sum_{i=1}^{k-1} \left[H(W_i) - I(W_i; W_{[i-1]})\right], \qquad (17)
\end{aligned}$$

and bound the mutual information above by

$$\begin{aligned} I(W_i; W_{[i-1]}) &\geq I(S_{i\to[i-1]}; S_{[i-1]\to i}) \\ &= I(S_{i\to[i]}; S_{[i]\to i}) \quad (18) \\ &= H(S_{i\to[i]}) + H(S_{[i]\to i}) - H(S_{i\leftrightarrow[i]}) \quad (19) \end{aligned}$$

where in (18) we just added $S_{i\to i}$ which is a dummy random variable, with zero entropy.

Next we bound terms in (19) individually. First note that

$$\begin{aligned} &\sum_{i=1}^{k-1} H(S_{i\to[i]}) + H(S_{[k:d+1]\to[1:k-1]}) \\ &\qquad \geq H\left(\bigcup_{i=1}^{k-1}\bigcup_{j=1}^{i} S_{i\to j}, \bigcup_{j=1}^{k-1}\bigcup_{i=k}^{d+1} S_{i\to j}\right) \\ &\qquad \geq H\left(\bigcup_{j=1}^{k-1}\bigcup_{i=j}^{k-1} S_{i\to j}, \bigcup_{j=1}^{k-1}\bigcup_{i=k}^{d+1} S_{i\to j}\right) \\ &\qquad = H\left(\bigcup_{j=1}^{k-1}\bigcup_{i=j}^{d+1} S_{i\to j}\right) \\ &\qquad = H\left(\bigcup_{j=1}^{k-1}\bigcup_{i=j}^{d+1} S_{i\to j}, \bigcup_{j=1}^{k-1} W_j\right) \quad (20) \\ &\qquad \geq H(W_{\mathcal{A}}). \quad (21) \end{aligned}$$

Note that in order to get (20), we can argue that W_1 can be recovered from $\bigcup_{j=1}^{d+1} S_{j\to 1}$. Once W_1 is available, we can construct $S_{1\to 2}$, which together with $\bigcup_{j=2}^{d+1} S_{j\to 2}$ can reconstruct W_2. Now, from W_1 and W_2, we find $S_{1\to 3}$ and $S_{2\to 3}$, respectively, and then with the help of $\bigcup_{j=3}^{d+1} S_{j\to 3}$ we recover W_3. Continuing this procedure, all the content of all discs in $[k-1]$ can be recovered.

Similarly,

$$\begin{aligned} &\sum_{i=1}^{k-1} H(S_{[i]\to i}) + H(S_{[k:d+1]\to[1:k-1]}) \\ &\qquad \geq H\left(\bigcup_{i=1}^{k-1}\bigcup_{j=1}^{i} S_{j\to i}, \bigcup_{i=1}^{k-1}\bigcup_{j=k}^{d+1} S_{j\to i}\right) \\ &\qquad \geq H\left(\bigcup_{j=1}^{k-1}\bigcup_{i=j+1}^{k-1} S_{j\to i}, \bigcup_{j=1}^{k-1}\bigcup_{i=k}^{d+1} S_{i\to j}\right) \\ &\qquad = H\left(\bigcup_{j=1}^{k-1}\bigcup_{i=j+1}^{k-1} S_{j\to i}, \bigcup_{j=1}^{k-1}\bigcup_{i=k}^{d+1} S_{i\to j}, \bigcup_{i=1}^{k-1} W_i\right) \\ &\qquad \geq H(W_{\mathcal{A}}). \quad (22) \end{aligned}$$

Finally we can bound the last term in (19) using the following lemma. The proof of lemma is presented in Appendix I.

Lemma 1 *For the (n, k, d) distributed storage system with exact repair requirements, we have*

$$\begin{aligned} \sum_{i=1}^{k-1} H(S_{i\leftrightarrow[i]}) &\leq \sum_{i=1}^{k-1} H(S_{[d+1]\to i}) - H(S_{[d+1]\to[k-1]}) \\ &\leq \sum_{i=1}^{k-1} H(S_{[d+1]\to i}) - H(W_{\mathcal{A}}). \quad (23) \end{aligned}$$

Plugging (19), (21), (22), and (23) in (17), we get

$$\begin{aligned} 4H(W_{\mathcal{A}}) \leq &\sum_{i=1}^{k-1} H(W_i) + 2H(S_{[k:d+1]\to[1:k-1]}) \\ &+ \sum_{i=1}^{k-1} H(S_{[d+1]\to i}) \quad (24) \end{aligned}$$

which together with (16) imply

$$\begin{aligned} \mathcal{B}^S &\leq \frac{1}{4}\sum_{i=1}^{k-1} H(W_i) + \frac{1}{2} H(S_{[k:d+1]\to[1:k-1]}) \\ &\quad + \left(\frac{k-1}{4} - \frac{k-1}{d}\right) H(S_{[d+1]\to i}) \\ &\leq \frac{k-1}{4}\alpha + \left(\frac{(k-1)(d+2-k)}{2} + \frac{(k-1)(d-4)}{4}\right)\beta \\ &= \frac{k-1}{4}\alpha + \frac{(k-1)(3d-2k)}{4}\beta, \end{aligned}$$

which is the desired bound. Note that this bound is a valid one for $d \geq 4$. For $d < 4$, the problem has been completely solved from the results in [17]–[19].

V. Proof of Theorem 2

We prove the bound for Type-I secrecy. Validity of the bound for Type-II secrecy is just an immediate consequence of the fact that Type-II secrecy is stronger than Type-I.

We bound the entropy of the file, F as follows

$$\begin{aligned} \mathcal{B}^S &= H(F) \\ &= H(F|W_1, \ldots, W_\ell) \quad (25) \\ &\leq H(F, W_{\ell+1}, \ldots, W_k | W_1, \ldots, W_\ell) \\ &= H(W_{\ell+1}, \ldots, W_k | W_1, \ldots, W_\ell) \\ &\quad + H(F|W_1, \ldots, W_\ell, W_{\ell+1}, \ldots, W_k) \\ &= H(W_{\ell+1}, \ldots, W_k | W_1, \ldots, W_\ell) \quad (26) \\ &= \sum_{i=\ell+1}^{k} H(W_i | W_1, \ldots, W_{i-1}) \quad (27) \end{aligned}$$

where (25) follows from the Type-I (weaker) secrecy constraint, and (26) follows from the property that the file F must be recoverable from the data stored in any k nodes. Next, the rest of the proof is devoted to upper bounding the terms appearing in the summation. In particular, there are two ways to upper bound the terms. The first one is rather

straightforward and is as follows:

$$\begin{aligned}\mathcal{B}^S &\leq \sum_{i=\ell+1}^{k} H(W_i|W_1,\ldots,W_{i-1}) \\ &\leq \sum_{i=\ell+1}^{k} H(S_{[d+1]\to i}|S_{[i-1]\to i}) \\ &\leq \sum_{i=\ell+1}^{k} (d-i+1)\beta \end{aligned} \tag{28}$$

to obtain one of the terms in Theorem 2 and has the dependence on the repair bandwidth, β.

We next prove the other bound (which depends on the storage parameter α). To this end, we rewrite the summation in (27) as

$$\mathcal{B}^S \leq \sum_{i=\ell+1}^{k} H(W_i|W_1,\ldots,W_{i-1}) \tag{29}$$

$$= \sum_{i=\ell+1}^{k} \Big[H(W_i) - I(W_i; W_{[i-1]})\Big] \tag{30}$$

In order to further upper bound the above expression, we state the following Lemma which is central to the proof. We present the proof of Lemma 2 in Appendix II. Intuitively, this lemma states that with exact and pair-wise symmetric repair constraint, the mutual information between the content on a node W_{s+1} and the data stored at s other nodes is lower bounded as a fraction of the entropy of the node W_{s+1}.

Lemma 2 *For the (n,k,d) distributed storage system with exact and pair-wise symmetric repair requirements, we have*

$$I(W_{s+1}; W_1,\ldots,W_s) \geq \left(\frac{s}{d}\right) H(W_{s+1}) \tag{31}$$

for any $1 \leq s \leq d$.

Using Lemma 2, we further upper bound (30) as follows:

$$\begin{aligned}\mathcal{B}^S &= \sum_{i=\ell+1}^{k} \Big[H(W_i) - I(W_i; W_{[i-1]})\Big] \\ &\leq \sum_{i=\ell+1}^{k} \left[H(W_i) - \left(\frac{i-1}{d}\right) H(W_i)\right] \\ &= \sum_{i=\ell+1}^{k} \left(\frac{d-i+1}{d}\right) H(W_i) \\ &\leq \sum_{i=\ell+1}^{k} \left(\frac{d-i+1}{d}\right) \alpha \end{aligned} \tag{32}$$

Hence, from (28) and (32), we arrive at

$$\begin{aligned}\mathcal{B}^S &\leq \sum_{i=\ell+1}^{k} (d-i+1) \min\left(\frac{\alpha}{d}, \beta\right) \\ &= \left[(k-\ell)d - \left(\binom{k}{2} - \binom{\ell}{2}\right)\right] \min\left(\frac{\alpha}{d}, \beta\right) \end{aligned} \tag{33}$$

thus completing the proof of Theorem 2.

VI. Conclusions

We considered the distributed storage problem with exact repair and information theoretic secrecy constraints. We developed a novel outer bound on the storage and repair bandwidth tradeoff. Our results for the general problem improve upon the best known outer bounds for this problem for all (n,k,d) parameters when the eavesdropper can access the repair data of any one node. Furthermore, under a more restrictive scenario of pair-wise symmetric repair, we completely characterize the corresponding tradeoff and show that it corresponds to the MBR point. The key technical element in the proofs of these results involves a novel use of Han's inequality. Future work includes extensions of this technique for tightening of the bounds for $\ell \geq 1$.

Appendix I
Proof of Lemma 1

We can prove a stronger claim, that is, for any $\tau \leq d$, we have

$$\sum_{i=1}^{\tau} H(S_{[d+1]\to i}) \geq \sum_{i=1}^{\tau} H(S_{i\leftrightarrow[i]}) + H(S_{[d+1]\to[\tau]}). \tag{34}$$

This can be proved by induction on τ. It is clear that for $\tau = 1$, the summation in the RHS reduces to the entropy of a dummy variable $S_{1\to 1}$, which is zero. The remaining terms are just identical, and so the inequality holds with equality.

Now, assume the claim holds for $\tau - 1$. Then we have

$$\begin{aligned}&\sum_{i=1}^{\tau} H(S_{[d+1]\to i}) = \sum_{i=1}^{\tau-1} H(S_{[d+1]\to i}) + H(S_{[d+1]\to\tau}) \\ &\geq \left[\sum_{i=1}^{\tau-1} H(S_{i\leftrightarrow[i]}) + H(S_{[d+1]\to[\tau-1]})\right] + H(S_{[d+1]\to\tau}) \end{aligned} \tag{35}$$

$$\begin{aligned}&= \sum_{i=1}^{\tau-1} H(S_{i\leftrightarrow[i]}) + H(S_{[d+1]\to[\tau-1]}, S_{[\tau-1]\to\tau}) \\ &\quad + H(S_{[d+1]\to\tau}, S_{\tau\to[\tau-1]}) \end{aligned} \tag{36}$$

$$\begin{aligned}&= \sum_{i=1}^{\tau-1} H(S_{i\leftrightarrow[i]}) + H(S_{[d+1]\to[\tau-1]}, S_{\tau\leftrightarrow[\tau]}) \\ &\quad + H(S_{[d+1]\to\tau}, S_{\tau\leftrightarrow[\tau]}) \end{aligned} \tag{37}$$

$$\begin{aligned}&\geq \sum_{i=1}^{\tau-1} H(S_{i\leftrightarrow[i]}) + H(S_{\tau\leftrightarrow[\tau]}) \\ &\quad + H(S_{[d+1]\to[\tau-1]}, S_{[d+1]\to\tau}, S_{\tau\leftrightarrow[\tau]}) \end{aligned} \tag{38}$$

$$\geq \sum_{i=1}^{\tau} H(S_{i\leftrightarrow[i]}) + H(S_{[d+1]\to[\tau]}). \tag{39}$$

Note that

- (35) holds because of the induction assumption for $\tau-1$.
- in (36) we used the fact that for any $1 \leq j \leq \tau$, having repair data from $(d+1)$ (from d nodes excluding itself) one can recover W_j, and hence $S_{j\to i}$, for any i. In particular, $S_{i\to[i-1]}$ is a function of the repair data;

- in (37) we just used the definition of $S_{\tau\leftrightarrow[\tau]}$, and the fact that $S_{\tau\to\tau}$ is a dummy variable;
- and (38) follows from inequality

$$H(XZ)+H(YZ)\geq H(XYZ)+H(Z).$$

This completes the proof. ■

APPENDIX II
PROOF OF LEMMA 2

First note that

$$H(S_{s+1\to[s]}|W_{s+1})=0 \tag{40}$$

due to the fact that $S_{s+1\to i}$ is the repair data sent by the node $s+1$ in the repair of node i, for $i=1,\ldots,s$. Furthermore, we also note that

$$H(S_{[s]\to s+1}|W_{[s]})=0 \tag{41}$$

since $S_{i\to s+1}$ is the repair data sent by node i in the repair of node $s+1$. We can thus lower bound the mutual information $I(W_{s+1};W_{[s]})$ as

$$\begin{aligned} I(W_{s+1};W_{[s]}) &\geq I(S_{s+1\to[s]};S_{[s]\to s+1}) \\ &= I(S_{[s]\to s+1};S_{[s]\to s+1}) \qquad (42)\\ &= H(S_{[s]\to s+1}). \qquad (43)\end{aligned}$$

In (42), we invoked the pair-wise symmetric repair constraint, i.e., $S_{i\to j}=S_{j\to i}$ and replaced $S_{s+1\to i}$ by $S_{i\to s+1}$ for $i=1,\ldots,s$. To complete the proof of the lemma, we next show the following

$$H(S_{[s]\to s+1})\geq\frac{s}{d}H(W_{s+1}). \tag{44}$$

To prove (44), we can write

$$\begin{aligned} H(S_{[s]\to s+1}) &= \frac{1}{\binom{d}{s}}\sum_{\substack{\mathcal{A}\subset[d+1]\setminus\{s+1\}\\|\mathcal{A}|=s}} H(S_{\mathcal{A}\to s+1}) \qquad (45)\\ &\geq \frac{s}{d}\frac{1}{\binom{d}{d}}\sum_{\substack{\mathcal{A}'\subset[d+1]\setminus\{s+1\}\\|\mathcal{A}|=d}} H(S_{\mathcal{A}'\to s+1}) \qquad (46)\\ &\geq \frac{s}{d}H(W_{s+1}) \qquad (47)\end{aligned}$$

where (45) follows from the fact that the system is symmetric, and $H(S_{\mathcal{A}\to s+1})$ is the same for all $\mathcal{A}$ with $|\mathcal{A}|=s$; in (46) we have used Han's inequality [13] for random variables $X_i=S_{i\to s+1}$, for $i\in[d+1]\setminus\{s+1\}$, which is

$$\frac{1}{\binom{d}{s}}\sum_{\mathcal{A}:|\mathcal{A}|=s}\frac{H(X(\mathcal{A}))}{s}\geq\frac{1}{\binom{d}{d}}\sum_{\mathcal{A}':|\mathcal{A}'|=d}\frac{H(X(\mathcal{A}'))}{d}.$$

Finally, (47) follows from the fact that W_{s+1} must be recoverable from the repair data coming in from d nodes. Substituting (47) in (43) we get the desired bound. ■

REFERENCES

[1] K. V. Rashmi, N. B. Shah, D. Gu, H. Kuang, D. Borthakur and K. Ramchandran, "A Solution to the Network Challenges of Data Recovery in Erasure-coded Distributed Storage Systems: A Study on the Facebook Warehouse Cluster", in arXiv:1309.0186, Sept. 2013.

[2] K. V. Rashmi, N. B. Shah and P. V. Kumar, "Enabling node repair in any erasure code for distributed storage", in arXiv:1101.0133, Jun. 2011.

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

[4] R. Ahlswede, N. Cai, S.-Y. R. Li and R. W. Yeung, "Network information flow," *IEEE Trans. Inf. Theory,* vol. 46, pp. 1204–1216, Jul. 2000.

[5] N. B. Shah, K. V. Rashmi, P. V. Kumar and K. Ramchandran, "Distributed storage codes with repair-by-transfer and non-achievability of interior points on the storage-bandwidth tradeoff," *IEEE Trans. Inf. Theory,* vol. 58, no. 3, pp. 1837–1852, Mar. 2012.

[6] V. Cadambe, S. Jafar, H. Maleki, K. Ramchandran and C. Suh, "Asymptotic interference alignment for optimal repair of MDS codes in distributed storage," *IEEE Trans Inf. Theory,* vol. 59, no. 5, pp. 2974–2987, May. 2013.

[7] C. Tian, "Rate region of the (4,3,3) exact-repair regenerating codes," in *Proc. Intern. Symp. Inf Theory, ISIT*, Istanbul, Turkey, Jun. 2013.

[8] A. S. Rawat, O. O. Koyluoglu, N. Silberstein, and S. Vishwanath, "Optimal locally repairable and secure codes for distributed storage systems," in arXiv:1210.6954, Aug. 2013.

[9] S. Pawar, S. El Rouayheb, and K. Ramchandran, "Securing dynamic distributed storage systems against eavesdropping and adversarial attacks," *IEEE Trans. Inf. Theory,* vol. 58, pp. 6734–6753, Mar. 2012.

[10] O. O. Koyluoglu, A. S. Rawat, and S. Vishwanath, " Secure Cooperative Regenerating Codes for Distributed Storage Systems,", in arXiv:1210.3664, Oct. 2012.

[11] N. B. Shah, K. V. Rashmi, and P. V. Kumar, "Information-theoretically secure regenerating codes for distributed storage," in *Proc. IEEE Global Commun. Conf., GLOBECOM*, Houston, TX, Dec. 2011.

[12] S. Goparaju, S. El Rouayheb, R. Calderbank and H. Vincent Poor, "Data Secrecy in Distributed Storage Systems under Exact Repair," in *Proc. IEEE International Symposium on Network Coding, NETCOD*, Calgary, Canada, Jun. 2013.

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

[14] B. Sasidharan, K. Senthoor, P. V. Kumar , "An Improved Outer Bound on the Storage-Repair-Bandwidth Tradeoff of Exact-Repair Regenerating Codes", in arXiv:1312.6079, Dec. 2013.

[15] C. Tian, B. Sasidharan, V. Aggarwal, V. A. Vaishampayan, P. V. Kumar, "Layered, Exact-Repair Regenerating Codes Via Embedded Error Correction and Block Designs", in arXiv:1408.0377, Aug. 2014.

[16] S. Goparaju, S. El Rouayheb, R. Calderbank , "New Codes and Inner Bounds for Exact Repair in Distributed Storage Systems ", in arXiv:1402.2343, Feb. 2014.

[17] R. Tandon, S. Amuru, T. C. Clancy and R. M. Buehrer, "Towards Optimal Secure Distributed Storage Systems with Exact Repair", in arXiv:1310.0054, Oct. 2013.

[18] R. Tandon, S. Amuru, T. C. Clancy and R. M. Buehrer, "On Secure Distributed Storage Systems with Exact Repair", in *Proc. IEEE International Conference on Communications (ICC)*, Sydney, Australia, June. 2014.

[19] R. Tandon, S. Amuru, T. C. Clancy and R. M. Buehrer, "Distributed Storage Systems with Secure and Exact Repair - New Results", in *Proc. Information Theory and Applications Workshop (ITA)*, San Diego, CA, Feb. 2014.