Quantifying the Cost of Privately Storing Data in Distributed Storage Systems

Rémi A. Chou

Abstract—Consider a user who wishes to store a file in multiple servers such that at least t servers are needed to reconstruct the file, and z colluding servers cannot learn any information about the file. Unlike traditional secret-sharing models, where perfectly secure channels are assumed to be available at no cost between the user and each server, we assume that the user can only send data to the servers via a public channel, and that the user and each server share an individual secret key with length n. For a given n, we determine the maximal length of the file that the user can store, and thus quantify the necessary cost to store a file of a certain length, in terms of the length of the secret keys that the user needs to share with the servers. Additionally, for this maximal file length, we determine (i) the optimal amount of local randomness needed at the user, (ii) the optimal amount of public communication from the user to the servers, and (iii) the optimal amount of storage requirement at the servers.

Index Terms—Secret sharing, information-theoretic security, secure distributed storage.

I. INTRODUCTION

CENTRALIZED data storage of sensitive information could mean compromising the entirety of the data in the case of a data breach. By contrast, a decentralized storage strategy can offer resilience against data breaches and avoid having a single point of entry for hackers. Well-known decentralized strategies are able to ensure that if a file is stored in L servers, then any $t \leq L$ servers that pool their information can reconstruct the file, whereas any $t - 1$ compromised servers do not leak any information about the file in an information-theoretic sense. For instance, secret sharing [2], [3] solves this problem with the optimal storage size requirement at each server. Specifically, to store F bits over L servers, the best possible storage strategy, that allows reconstruction of the information from $t \leq L$ servers and is resilient against data breaches at $t - 1$ servers, requires storing LF bits over the L servers. In secret sharing models, the user who wishes to store a file in the servers corresponds to the dealer, the file corresponds to a secret, and the information stored at a given server is called a share of the secret. Applications of secret

sharing to secure distributed storage have been extensively studied for a wide range of settings, e.g., [4]–[12]. Note that, as motivated in [13]–[16], the servers could also correspond to independent cloud storage providers, as it is often less costly for businesses and organizations to outsource data storage but cloud storage providers lack reliable security guarantees and may be the victims of data breaches.

Since the user and the servers are not physically collocated, a standard assumption in secret sharing models [2], [3], [17]–[20] is the availability of individual and information-theoretically secure channels between the user and each server, that allow the user to securely communicate a share of the secret to each server. In this paper, we propose to quantify the cost associated with this assumption. Specifically, instead of assuming the availability at no cost of such information-theoretically secure channels, we assume that the user can communicate over a one-way public channel with each server, and that the user and each server share a secret key, which is a sequence of n bits uniformly distributed over $\{0, 1\}^n$. Then, for a given n, we determine the maximal length of the file that the user can store. Given this relationship between n and the maximal length of the file, one can thus determine the necessary cost to store a file of a given length, in terms of the length of the secret keys that the user needs to share with the servers. Furthermore, we are also interested in minimizing (i) the amount of additional resource locally needed at the user, i.e., local randomness needed by the user to form the shares that will be stored at the servers, (ii) the amount of public communication between the user and the servers, and (iii) the cost of file storage, i.e., the amount of information that needs to be stored at the servers.

The most challenging part of this study is proving the converse results on the maximal length of the file that the user can store, the optimal amount of local randomness needed at the user, and the optimal amount of public communication between the user and the servers. Unlike in traditional secret-sharing models, in our converse, we need to account for the presence of shared secret keys, public communication available to all parties, and the fact that the creation phase of the shares and the secure communication phase of the shares to the servers are allowed to be jointly designed in our model. Note that these two phases are *independent* in traditional secret-sharing models, which only focus on the creation phase of the shares since the secure communication phase of the shares relies on the assumption that information-theoretically secure channels are available at no cost. Finally, we establish achievability results that match our converse results using
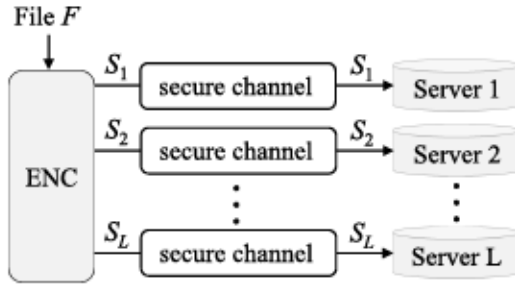
Fig. 1.   Traditional secret sharing settings rely on the assumption that individual and information-theoretically secure channels between each server and the user are available at no cost.

ramp secret sharing schemes [21], [22]. Specifically, we prove the optimality of an achievability scheme that separates the creation of the shares using ramp secret sharing schemes and the secure communication of the shares to the servers via one-time pads.

The remainder of the paper is organized as follows. In Section II, we describe in an informal manner our setting and the objectives of our study. This section also compares our setting to traditional secret sharing settings and reviews some known results. In Section III, we formally state the problem. In Section IV, we present our main results. In Section V, we extend our setting and results to a multi-user setting. Finally, in Section VI, we provide concluding remarks.

II. PROBLEM MOTIVATION AND COMPARISON WITH TRADITIONAL SECRET SHARING

Consider one user who wishes to store a file F in L servers, indexed in $\mathcal{L} \triangleq \{1, \ldots, L\}$, such that any t servers that pool their information can reconstruct F and any z colluding servers cannot learn any information about F, where t and z are chosen in $\{1, \ldots, L\}$ and $\{1, \ldots, t-1\}$, respectively.

In a traditional secret sharing setting, the user encodes the file F into L shares $(S_1, \ldots, S_L)$ and transmits the share S_l to Server $l \in \mathcal{L}$ via individual secure channels (available at no cost) between the user and each server. The setting is depicted in Figure 1 and the requirements are formalized as

$$\forall T \subseteq \mathcal{L}, |T| \geq t \implies H(F|S_T) = 0 \text{ (Recoverability)},$$
$$\forall \mathcal{U} \subseteq \mathcal{L}, |\mathcal{U}| \leq z \implies I(F; S_{\mathcal{U}}) = 0 \text{ (Security)},$$

where we have defined $S_T \triangleq (S_l)_{l \in T}, \forall T \subseteq \mathcal{L}$. In this setting, the following questions arise.

1) What is the minimum size of an individual share S_l, $l \in \mathcal{L}$?
2) What is the minimum size of all the shares $(S_l)_{l \in \mathcal{L}}$ considered jointly?
3) What is the minimum amount of local randomness needed at the encoder to obtain shares with minimum size?

These questions have all been studied in the literature. It is well known, e.g., [23], [24], that designing shares that satisfy $\sum_{l \in \mathcal{L}} H(S_l) = \frac{L}{t-z}H(F)$ is optimal, and the minimum amount of local randomness needed to achieve this optimal
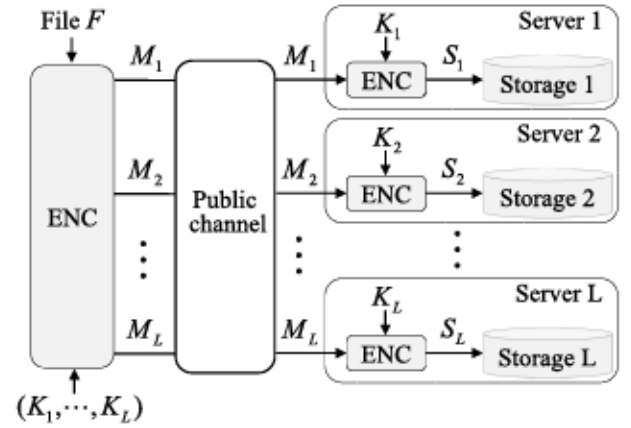

Fig. 2.   In our setting, individual and information-theoretically secure channels between each server and the user are replaced by a public communication channel and pairs of secret keys between the user and the servers. One of our main objectives is to characterize the minimum key lengths needed for a given file size.

bound is $\frac{z}{t-z}H(F)$. Moreover, under the additional assumption that

$$\forall T \subset \mathcal{L}, z < |T| < t \implies H(F|S_T) = \frac{t-|T|}{t-z}H(F),$$

then [24] showed that, for individual shares, having $H(S_l) = \frac{1}{t-z}H(F)$, $l \in \mathcal{L}$, is optimal.

In this paper, we wish to quantify the cost associated with the assumption that individual secure channels are available between the user and each server. To this end, we replace these individual secure channels by a public channel between the user and the servers and assume that the user shares with Server $l \in \mathcal{L}$ a key K_l with length n. The key length n aims to quantify the aforementioned cost. Let M_l be the public communication of the user to Server l, $M \triangleq (M_l)_{l \in \mathcal{L}}$ be the overall public communication, and S_l be the information stored at Server l after the public communication happened. Our setting is depicted in Figure 2 and the requirements are formalized as

$$\forall T \subseteq \mathcal{L}, |T| \geq t \implies H(F|S_T) = 0 \text{ (Recoverability)},$$
$$\forall \mathcal{U} \subseteq \mathcal{L}, |\mathcal{U}| \leq z \implies I(F; M, K_{\mathcal{U}}) = 0 \text{ (Security)},$$

where we have defined $S_T \triangleq (S_l)_{l \in T}$, $K_T \triangleq (K_l)_{l \in T}$, $\forall T \subseteq \mathcal{L}$. Note that the servers may only store a function of the public communication. Additionally, the creation phase of the shares and the secure communication phase of the shares to the servers are allowed to be jointly designed, unlike in traditional secret sharing, where the creation of the shares is independent of their secure communication to the servers due to the availability of secure channels. Note also that the public communication M now needs to be accounted for information leakage about the file F in the security constraint. In our study we ask the following questions.

1) What is the maximal length for the file F that the user can store for a given key length n? Let us denote this maximal length by $r_\star^{(F)}$.
2) What is the minimal amount of local randomness needed at the user to achieve $r_\star^{(F)}$?

3) For a given $l \in \mathcal{L}$, what is the minimal storage size needed at Server l for the user to achieve $r_\star^{(F)}$? In other words, what is the minimal size for S_l?
4) For a given $l \in \mathcal{L}$, what is the minimal amount of public communication M_l to Server l needed for the user to achieve $r_\star^{(F)}$?
5) What is the minimal amount of overall public communication $(M_l)_{l \in \mathcal{L}}$ needed for the user to achieve $r_\star^{(F)}$?

III. PROBLEM STATEMENT

Notation: For any $a, b \in \mathbb{N}^*$, define $[a, b] \triangleq [a, b] \cap \mathbb{N}$. For any $x \in \mathbb{R}$, define $[x]^+ \triangleq \max(0, x)$. For a given set $\mathcal{S}$, let $2^{\mathcal{S}}$ denote the power set of $\mathcal{S}$. Finally, let $\times$ denote the Cartesian product.

Consider L servers indexed in $\mathcal{L} \triangleq [1, L]$ and one user. Assume that Server $l \in \mathcal{L}$ and the user share a secret key $K_l \in \mathcal{K} \triangleq \{0, 1\}^n$, which is a sequence of n bits uniformly distributed over $\{0, 1\}^n$. The L keys are assumed to be jointly independent. For any $\mathcal{Y} \subseteq \mathcal{L}$, we use the notation $K_{\mathcal{Y}} \triangleq (K_y)_{y \in \mathcal{Y}}$.

Definition 1: A $\left(2^{r^{(F)}}, 2^{r^{(R)}}, \left(2^{r_l^{(M)}}\right)_{l \in \mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l \in \mathcal{L}}\right)$ private file storage strategy consists of

- A file F owned by the user, which is uniformly distributed over $\mathcal{F} \triangleq \{0, 1\}^{r^{(F)}}$ and independent from the keys $K_{\mathcal{L}}$ (the superscript (F) stands for File);
- A sequence of local randomness R owned by the user, which is uniformly distributed over $\mathcal{R} \triangleq \{0, 1\}^{r^{(R)}}$ and independent from all the other random variables (the superscript (R) stands for Randomness);
- L encoding functions $h_l : \mathcal{R} \times \mathcal{K} \times \mathcal{F} \to \mathcal{M}_l$, where $l \in \mathcal{L}$, and $\mathcal{M}_l \triangleq \{0, 1\}^{r_l^{(M)}}$ (the superscript (M) stands for Message);
- L servers with storage space $r_l^{(S)}$ bits for Server $l \in \mathcal{L}$ (the superscript (S) stands for Server);
- L encoding functions $g_l : \mathcal{M}_l \times \mathcal{K} \to \mathcal{S}_l$, where $l \in \mathcal{L}$, and $\mathcal{S}_l \triangleq \{0, 1\}^{r_l^{(S)}}$;
- 2^L decoding functions $f_{\mathcal{A}} : \times_{l \in \mathcal{A}} \mathcal{S}_l \to \mathcal{F}$, where $\mathcal{A} \subseteq \mathcal{L}$;

and operates as follows:

1) The user publicly sends to Server $l \in \mathcal{L}$ the message $M_l \triangleq h_l(R, K_l, F)$. For $\mathcal{Y} \subseteq \mathcal{L}$, we define $M_{\mathcal{Y}} \triangleq (M_l)_{l \in \mathcal{Y}}$. For convenience, we also write $M \triangleq M_{\mathcal{L}}$.
2) Server $l \in \mathcal{L}$ stores $S_l \triangleq g_l(M_l, K_l)$.
3) Any subset of servers $\mathcal{A} \subseteq \mathcal{L}$ can compute $\widehat{F}(\mathcal{A}) \triangleq f_{\mathcal{A}}(S_{\mathcal{A}})$, an estimate of F, where $S_{\mathcal{A}} \triangleq (S_l)_{l \in \mathcal{A}}$.

The setting is depicted in Figure 2.

Definition 2: Fix $t \in [1, L]$, $z \in [1, t - 1]$. Then, $r^{(F)}$ is (t, z)-achievable if there exists a $\left(2^{r^{(F)}}, 2^{r^{(R)}}, \left(2^{r_l^{(M)}}\right)_{l \in \mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l \in \mathcal{L}}\right)$ private file storage strategy such that

$$\forall \mathcal{A} \subseteq \mathcal{L}, |\mathcal{A}| \geq t \implies H(F|\widehat{F}(\mathcal{A})) = 0 \text{ (Recoverability)}, \tag{1}$$

$$\forall \mathcal{U} \subseteq \mathcal{L}, |\mathcal{U}| \leq z \implies I(F; M, K_{\mathcal{U}}) = 0 \text{ (Security)}. \tag{2}$$

The set of all achievable lengths $r^{(F)}$ is denoted by $\mathcal{C}_F(t, z)$.

(1) means that any subset of servers with size larger than or equal to t is able to perfectly recover the files F, and (2) means that any subset of servers with size smaller than or equal to z is unable to learn any information about the file. Note that (2) accounts for the fact that colluding servers have access to the entire public communication M.

Our main objective is to determine, under the constraints (1) and (2), the maximal file length that the user can store in the servers given that the secret keys shared with the servers have length n. Next, another of our objectives is to determine (i) the minimum amount of local randomness needed at the user, (ii) the minimum storage requirement at the servers, and (iii) the minimum amount of public communication from the user to the servers that are needed to achieve the largest file rate in $\mathcal{C}_F(t, z)$. To this end, we introduce the following definition.

Definition 3: Fix $t \in [1, L]$, $z \in [1, t - 1]$. For $r^{(F)}$ in $\mathcal{C}_F(t, z)$, let $\mathcal{Q}(r^{(F)})$ be the set of tuples $T \triangleq \left(r^{(R)}, (r_l^{(M)})_{l \in \mathcal{L}}, (r_l^{(S)})_{l \in \mathcal{L}}\right)$ such that there exists a $\left(2^{r^{(F)}}, 2^{r^{(R)}}, \left(2^{r_l^{(M)}}\right)_{l \in \mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l \in \mathcal{L}}\right)$ private file storage strategy that (t, z)-achieves $r^{(F)}$. Then, define

$$r_\star^{(F)}(t, z) \triangleq \sup_{r^{(F)} \in \mathcal{C}_F(t, z)} r^{(F)},$$

$$r_{l,\star}^{(M)}(t, z) \triangleq \inf_{T \in \mathcal{Q}(r_\star^{(F)}(t,z))} r_l^{(M)}, l \in \mathcal{L},$$

$$r_{\Sigma,\star}^{(M)}(t, z) \triangleq \inf_{T \in \mathcal{Q}(r_\star^{(F)}(t,z))} \sum_{l \in \mathcal{L}} r_l^{(M)},$$

$$r_\star^{(R)}(t, z) \triangleq \inf_{T \in \mathcal{Q}(r_\star^{(F)}(t,z))} r^{(R)},$$

$$r_{l,\star}^{(S)}(t, z) \triangleq \inf_{T \in \mathcal{Q}(r_\star^{(F)}(t,z))} r_l^{(S)}, l \in \mathcal{L}.$$

$r_\star^{(F)}(t, z)$ is the largest file size that the user can privately store under the constraints (1) and (2). Then, $r_\star^{(R)}(t, z)$, $r_{l,\star}^{(M)}(t, z)$, $r_{\Sigma,\star}^{(M)}(t, z)$, and $r_{l,\star}^{(S)}(t, z)$, $l \in \mathcal{L}$, are the minimum amount of local randomness, the minimum amount of public communication to Server l, the minimum amount of public communication to all the servers, and the minimum storage size required at Server l, respectively, needed for the user to achieve $r_\star^{(F)}(t, z)$. Remark that, a priori, it is unclear whether all these quantities can be achieved simultaneously, i.e., whether there exists a $\left(2^{r_\star^{(F)}(t,z)}, 2^{r_\star^{(R)}(t,z)}, \left(2^{r_{l,\star}^{(M)}(t,z)}\right)_{l \in \mathcal{L}}, \left(2^{r_{l,\star}^{(S)}(t,z)}\right)_{l \in \mathcal{L}}\right)$ file storage strategy that (t, z)-achieves $r_\star^{(F)}(t, z)$.

IV. MAIN RESULTS

In Section IV-A, we prove impossibility results. Specifically, we first derive an upper bound on the maximum file length $r_\star^{(F)}(t, z)$. Then, assuming that the user stores a file of length $r_\star^{(F)}(t, z)$, we derive lower bounds on the minimum amount of local randomness $r_\star^{(R)}(t, z)$ needed at the user, the minimum amount of public communication needed to each individual server from the user, i.e., $r_{l,\star}^{(M)}(t, z)$, $l \in \mathcal{L}$, the minimum

amount of public communication needed to all the servers from the user, i.e., $r_{\Sigma,\star}^{(M)}(t,z)$, and the minimum storage size needed at Server $l \in \mathcal{L}$, i.e., $r_{l,\star}^{(S)}(t,z)$. In Section IV-B, we prove an achievability result that matches all the bounds found in Section IV-A.

A. Impossibility Results

Theorem 1 (Converse on the File Length): Let $t \in [\![1, L]\!]$ and $z \in [\![1, t-1]\!]$. Then, we have

$$r_{\star}^{(F)}(t,z) \le n(t-z).$$

Proof: Set $D = 1$ in Appendix A. ∎

Theorem 1 means that it is impossible for the user to store a file of length larger than $n(t-z)$ bits. The proof of Theorem 1 is obtained by first upper bounding the file length by $I(K_{\mathcal{A}}; K_{\mathcal{L}}|K_{\mathcal{U}})$ for any $\mathcal{A}, \mathcal{U} \subseteq \mathcal{L}$ such that $|\mathcal{A}| = t$, $|\mathcal{U}| = z$, and $\mathcal{U} \subset \mathcal{A}$ using Definition 1 and the constraints (1) and (2). Theorem 1 is then obtained from this upper bound by leveraging the independence of the secret keys.

Theorem 2 (Converse on Storage Size Requirement at the Servers): Let $t \in [\![1, L]\!]$ and $z \in [\![1, t-1]\!]$. Then, we have

$$r_{l,\star}^{(S)}(t,z) \ge n, \forall l \in \mathcal{L}.$$

Proof: Set $D = 1$ in Appendix B. ∎

Theorem 2 means that Server $l \in \mathcal{L}$ needs a storage capacity of at least n bits, and is obtained by considering the fact that, at the beginning of the protocol, each server needs to store its secret key.

Theorem 3 (Converse on the Total Amount of Public Communication to the Servers): Let $t \in [\![1, L]\!]$ and $z \in [\![1, t-1]\!]$. Then, we have

$$r_{\Sigma,\star}^{(M)}(t,z) \ge \frac{L}{t-z} r_{\star}^{(F)}(t,z).$$

Proof: Set $D = 1$ in Appendix C. ∎

Theorem 3 means that it is impossible for the user to store a file of length $r_{\star}^{(F)}(t,z)$ if the public communication sum-length to the servers is smaller than $\frac{L}{t-z} r_{\star}^{(F)}(t,z)$ bits. The proof of Theorem 3 is obtained by first showing that for $\mathcal{T} \subseteq \mathcal{L}$ and $\mathcal{S} \subseteq \mathcal{L} \backslash \mathcal{T}$ such that $|\mathcal{T}| = z$ and $|\mathcal{S}| = t - z$, the sum of the message sizes for the servers in $\mathcal{S}$ is lower bounded by $H(F)$. Then, Theorem 3 is obtained by a combinatorial argument that consists in summing this bound over all possible sets of servers $\mathcal{S}$ and $\mathcal{T}$ as above.

Theorem 4 (Converse on the Amount of Public Communication to an Individual Server): Let $t \in [\![1, L]\!]$ and $z \in [\![1, t-1]\!]$. Consider the following condition

$$\forall \mathcal{U}, \mathcal{V} \subseteq \mathcal{L}, |\mathcal{U}| = |\mathcal{V}| \implies I(F; M_{\mathcal{U}}, K_{\mathcal{U}}) = I(F; M_{\mathcal{V}}, K_{\mathcal{V}}). \tag{3}$$

(3) indicates that any two sets of colluding servers that have the same size have the same amount of information about the file F. If (3) holds, then we have

$$r_{l,\star}^{(M)}(t,z) \ge \frac{1}{t-z} r_{\star}^{(F)}(t,z), \forall l \in \mathcal{L}.$$

Proof: Set $D = 1$ in Appendix D. ∎

Note that (3) is always true for sets with cardinality smaller than or equal to z by (2), and for sets with cardinality larger than or equal to t by (1). Note that the concept of leakage symmetry also exists in the context of secret sharing under the denomination uniform secret sharing [25].

Under the leakage symmetry condition (3), Theorem 4 means that it is impossible for the user to store a file of length $r_{\star}^{(F)}(t,z)$ if the public communication length to Server $l \in \mathcal{L}$ is smaller than $\frac{1}{t-z} r_{\star}^{(F)}(t,z)$ bits. Theorem 4 is obtained by first proving a lower bound on individual public message size that depends on the leakages associated with some sets of servers, specifically, we prove that the public message size for Server $l \in \mathcal{L}$ is lower bounded by $\sum_{i=z}^{t-1} [2\alpha_{i+1} - \alpha_i - \alpha_{i+2}]^+$, where for $i \in \mathcal{L}$ and $\mathcal{S} \subseteq \mathcal{L}$ such that $|\mathcal{S}| = i$, we have defined $\alpha_i \triangleq I(F; M_{\mathcal{S}}, K_{\mathcal{S}})$ and $\alpha_{L+1} \triangleq \alpha_L$. Then, we perform an optimization over all possible values of $(\alpha_i)_{[\![1, L+1]\!]}$ to minimize this bound and obtain Theorem 4.

Theorem 5 (Converse on the Amount of Required Local Randomness at the Users): Let $t \in [\![1, L]\!]$ and $z \in [\![1, t-1]\!]$. Then, we have

$$r_{\star}^{(R)}(t,z) \ge \frac{z}{t-z} r_{\star}^{(F)}(t,z).$$

Proof: Set $D = 1$ in Appendix E. ∎

Theorem 5 means that it is impossible for the user to store a file of length $r_{\star}^{(F)}(t,z)$ if the amount of its local randomness is smaller than $\frac{z}{t-z} r_{\star}^{(F)}(t,z)$ bits. The proof of Theorem 5 is obtained by first proving the bound $\sum_{l \in \mathcal{S}} H(M_l, K_l | M_{\mathcal{V}}, K_{\mathcal{V}}) \ge H(F) + \sum_{l \in \mathcal{S}} H(K_l)$ for $\mathcal{S} \subseteq \mathcal{L} \backslash (\mathcal{T} \cup \mathcal{V})$ such that $|\mathcal{S}| = t - z$ with $\mathcal{V} \subseteq \mathcal{L}$ such that $|\mathcal{V}| < z$ and $\mathcal{T} \subseteq \mathcal{L} \backslash \mathcal{V}$ such that $|\mathcal{T}| = z - |\mathcal{V}|$. Then, by a combinatorial argument that consists in summing this bound over all possible sets $\mathcal{S}$ and $\mathcal{T}$ as above, we obtain Theorem 5.

B. Capacity Results

We first derive an achievability result with a private file storage strategy that separates the creation of the shares, which is done via ramp secret sharing [21], [22], and the secure distribution of the shares, which is done via a one-time pad. We will then compare the bounds achieved by this coding strategy with the impossibility results of Section IV-A, to prove their optimality.

Theorem 6: Let $t \in [\![1, L]\!]$ and $z \in [\![1, t-1]\!]$. There exists a $\left(2^{r^{(F)}}, 2^{r^{(R)}}, \left(2^{r_l^{(M)}}\right)_{l \in \mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l \in \mathcal{L}}\right)$ private file storage strategy that (t,z)-achieves $r^{(F)}$ such that

$$r^{(F)} = n(t-z),$$
$$r^{(R)} = nz,$$
$$r_l^{(S)} = n, \forall l \in \mathcal{L},$$
$$r_l^{(M)} = n, \forall l \in \mathcal{L}.$$

Proof: Set $D = 1$ in Appendix F. ∎

From Theorem 6 and the impossibility results of Section IV-A, we obtain a characterization of the quantities introduced in Definition 3 as follows.

Theorem 7: Let $t \in [1, L]$ and $z \in [1, t-1]$. We have

$$r_\star^{(F)}(t,z) = n(t-z),$$
$$r_\star^{(R)}(t,z) = nz,$$
$$r_{l,\star}^{(S)}(t,z) = n, \forall l \in \mathcal{L},$$
$$r_{\Sigma,\star}^{(M)}(t,z) = Ln,$$
$$(3) \implies \left(r_{l,\star}^{(M)}(t,z) = n, \forall l \in \mathcal{L}\right).$$

Proof: Set $D = 1$ in Appendix G. ∎

Note that from Theorem 6 and Theorem 7, we immediately have Corollary 1, which states that the optimal quantities of Definition 3 can be obtained simultaneously by a single private file storage strategy.

Corollary 1: Let $t \in [1, L]$ and $z \in [1, t-1]$. There exists a $\left(2^{r^{(F)}}, 2^{r^{(R)}}, \left(2^{r_l^{(M)}}\right)_{l\in\mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l\in\mathcal{L}}\right)$ private file storage strategy that (t,z)-achieves $r^{(F)}$ such that

$$r^{(F)} = r_\star^{(F)}(t,z),$$
$$r^{(R)} = r_\star^{(R)}(t,z),$$
$$r_l^{(S)} = r_{l,\star}^{(S)}(t,z), \forall l \in \mathcal{L},$$
$$\sum_{l\in\mathcal{L}} r_l^{(M)} = r_{\Sigma,\star}^{(M)}(t,z),$$
$$r_l^{(M)} = r_{l,\star}^{(M)}(t,z), \forall l \in \mathcal{L}, \text{ when (3) holds.}$$

Results interpretation: Consider, $t \in \mathcal{L}$, and $z \in [1, t-1]$. Assume that the user shares an individual key with length n bits with each server. Then, the user can store a file of size at most $n(t-z)$ bits such that any set of servers larger than or equal to t can reconstruct the file, and any set of servers smaller than or equal to z cannot learn anything about the file. Moreover, if the user stores a file of length $n(t-z)$ bits, then the optimal storage capacity at each server is n bits, the optimal amount of local randomness needed at the user is $n \times z$ bits, and the optimal amount of public communication from the user to all the servers is $L \times n$ bits. If one assumes that the leakage about the file must be symmetric among the servers, i.e., (3) holds, then the optimal amount of public communication from the user to Server $l \in \mathcal{L}$ is n bits.

Note that Corollary 1 shows that there is a linear relationship between the maximal length of the file that can be stored and the three resources key length, local randomness, and public communication. This relationship is represented in Figure 3.

V. EXTENSION TO MULTIPLE USERS

In this section, we generalize the problem statement and results of Sections III and IV, respectively, to the case where $D \geq 1$ users wish to store files in the servers.

A. Problem Statement

Consider L servers indexed by $\mathcal{L} \triangleq [1, L]$ and D users indexed by $\mathcal{D} \triangleq [1, D]$. Assume that Server $l \in \mathcal{L}$ and User $d \in \mathcal{D}$ share a secret key $K_{d,l} \in \mathcal{K}_d \triangleq \{0,1\}^{n_d}$, which is a sequence of n_d bits uniformly distributed over $\{0,1\}^{n_d}$. All the $D \times L$ keys are assumed to be jointly independent. For any

Four-dimensional space
(file length, key length, local randomness, public communication)

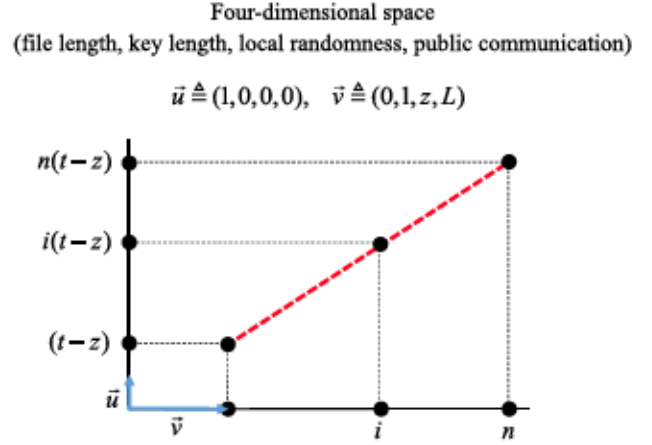$$\vec{u} \triangleq (1,0,0,0), \quad \vec{v} \triangleq (0,1,z,L)$$

Fig. 3. Linear relationship between the maximal length of the file that can be stored and the three resources key length, local randomness, and public communication. For instance, for $i \in \mathbb{N}$, storing a file of $i(t-z)$ bits requires i-bit keys, $i \times z$ bits of local randomness, and $i \times L$ bits of public communication.

$\mathcal{X} \subseteq \mathcal{D}$, $\mathcal{Y} \subseteq \mathcal{L}$, we define $K_{\mathcal{X},\mathcal{Y}} \triangleq (K_{x,y})_{x\in\mathcal{X},y\in\mathcal{Y}}$ and, for convenience, we also write $K_{d,\mathcal{Y}} \triangleq K_{\{d\},\mathcal{Y}}$ for any $d \in \mathcal{D}$.

Definition 4: A $\left(\left(2^{r_d^{(F)}}\right)_{d\in\mathcal{D}}, \left(2^{r_d^{(R)}}\right)_{d\in\mathcal{D}}, \left(2^{r_{d,l}^{(M)}}\right)_{d\in\mathcal{D},l\in\mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l\in\mathcal{L}}\right)$ private file storage strategy consists of

- D independent files F_d, $d \in \mathcal{D}$, where File F_d is owned by User d and is uniformly distributed over $\mathcal{F}_d \triangleq \{0,1\}^{r_d^{(F)}}$. The files $(F_d)_{d\in\mathcal{D}}$ are assumed independent of the keys $K_{\mathcal{D},\mathcal{L}}$;
- D independent sequences of local randomness R_d, $d \in \mathcal{D}$, where Sequence R_d is owned by User d and is uniformly distributed over $\mathcal{R}_d \triangleq \{0,1\}^{r_d^{(R)}}$. The sequences $(R_d)_{d\in\mathcal{D}}$ are assumed independent of all the other random variables;
- $D \times L$ encoding functions $h_{d,l} : \mathcal{R}_d \times \mathcal{K}_d \times \mathcal{F}_d \to \mathcal{M}_{d,l}$, where $d \in \mathcal{D}$, $l \in \mathcal{L}$, and $\mathcal{M}_{d,l} \triangleq \{0,1\}^{r_{d,l}^{(M)}}$;
- L servers with storage capacities $r_l^{(S)}$ bits for Server $l \in \mathcal{L}$;
- $L \times D$ encoding functions $g_{l,d} : \mathcal{M}_{d,l} \times \mathcal{K}_d \to \mathcal{S}_{l,d}$, where $l \in \mathcal{L}$, $d \in \mathcal{D}$, and the $\mathcal{S}_{l,d}$ are such that $\times_{d\in\mathcal{D}}\mathcal{S}_{l,d} = \{0,1\}^{r_l^{(S)}}$;
- $2^L \times D$ decoding functions $f_{\mathcal{A},d} : \times_{l\in\mathcal{A}}\mathcal{S}_{l,d} \to \mathcal{F}_d$, where $\mathcal{A} \subseteq \mathcal{L}$, $d \in \mathcal{D}$;

and operates as follows:

1) User $d \in \mathcal{D}$ publicly sends to Server $l \in \mathcal{L}$ the message $M_{d,l} \triangleq h_{d,l}(R_d, K_{d,l}, F_d)$. For $\mathcal{X} \subseteq \mathcal{D}$, $\mathcal{Y} \subseteq \mathcal{L}$, we define $M_{\mathcal{X},\mathcal{Y}} \triangleq (M_{d,l})_{d\in\mathcal{X},l\in\mathcal{Y}}$ and, for convenience, we also write $M_{\mathcal{X}} \triangleq M_{\mathcal{X},\mathcal{L}}$ and $M_d \triangleq M_{\{d\},\mathcal{L}}$, $d \in \mathcal{D}$.
2) Server $l \in \mathcal{L}$ stores $(S_{l,d})_{d\in\mathcal{D}}$ where for $d \in \mathcal{D}$, $S_{l,d} \triangleq g_{l,d}(M_{d,l}, K_{d,l})$.
3) Any subset of servers $\mathcal{A} \subseteq \mathcal{L}$ can compute $\hat{F}_d(\mathcal{A}) \triangleq f_{\mathcal{A},d}(S_{\mathcal{A},d})$, an estimate of F_d, where $d \in \mathcal{D}$ and $S_{\mathcal{A},d} \triangleq (S_{l,d})_{l\in\mathcal{A}}$.

Definition 5: Let $\mathbf{t} \triangleq (t_d)_{d\in\mathcal{D}} \in [1, L]^D$ and $\mathbf{z} \triangleq (z_d)_{d\in\mathcal{D}} \in \times_{d\in\mathcal{D}}[1, t_d - 1]$. A length-tuple

$\left(r_d^{(F)}\right)_{d\in\mathcal{D}}$ is $(\mathbf{t},\mathbf{z})$-achievable if there exists a $\left(\left(2^{r_d^{(F)}}\right)_{d\in\mathcal{D}}, \left(2^{r_d^{(R)}}\right)_{d\in\mathcal{D}}, \left(2^{r_{d,l}^{(M)}}\right)_{d\in\mathcal{D},l\in\mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l\in\mathcal{L}}\right)$ private file storage strategy such that

$$\forall d\in\mathcal{D},\left(\forall\mathcal{A}\subseteq\mathcal{L},|\mathcal{A}|\geq t_d \implies H(F_d|\widehat{F}_d(\mathcal{A}))=0\right), \quad (4)$$

$$\forall d\in\mathcal{D},\left(\forall\mathcal{U}\subseteq\mathcal{L},|\mathcal{U}|\leq z_d \implies I(F_{\mathcal{Z}_d};M_{\mathcal{D}},K_{\mathcal{D},\mathcal{U}})=0\right), \quad (5)$$

where for $d\in\mathcal{D}$, we have defined $\mathcal{Z}_d\triangleq\{i\in\mathcal{D}:z_i\geq z_d\}$ and $F_{\mathcal{Z}_d}\triangleq(F_i)_{i\in\mathcal{Z}_d}$. The set of all achievable length-tuples is denoted by $\mathcal{C}_F(\mathbf{t},\mathbf{z})$.

(4) means that any subset of servers with size larger than or equal to t_d is able to perfectly recover the file F_d, $d\in\mathcal{D}$, and (5) means that any subset of servers with size smaller than or equal to z_d is unable to learn any information about the files $\{F_i : i\in\mathcal{D}, z_i\geq z_d\}$. Similar to the case $D=1$ in Section III, we have the following counterpart to Definition 3.

Definition 6: Let $\mathbf{t}\triangleq(t_d)_{d\in\mathcal{D}}\in[1,L]^D$ and $\mathbf{z}\triangleq(z_d)_{d\in\mathcal{D}}\in\bigtimes_{d\in\mathcal{D}}[1,t_d-1]$. For $\mathbf{r}^{(F)}\triangleq\left(r_d^{(F)}\right)_{d\in\mathcal{D}}$ in $\mathcal{C}_F(\mathbf{t},\mathbf{z})$, let $\mathcal{Q}(\mathbf{r}^{(F)})$ be the set of tuples $T\triangleq\left((r_d^{(R)})_{d\in\mathcal{D}},(r_{d,l}^{(M)})_{d\in\mathcal{D},l\in\mathcal{L}},(r_l^{(S)})_{l\in\mathcal{L}}\right)$ such that there exists a $\left(\left(2^{r_d^{(F)}}\right)_{d\in\mathcal{D}}, \left(2^{r_d^{(R)}}\right)_{d\in\mathcal{D}}, \left(2^{r_{d,l}^{(M)}}\right)_{d\in\mathcal{D},l\in\mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l\in\mathcal{L}}\right)$ private file storage strategy that $(\mathbf{t},\mathbf{z})$-achieves $\mathbf{r}^{(F)}$. Then, for any $d\in\mathcal{D}$, we define the following quantities:

$$r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})\triangleq\sup_{\mathbf{r}^{(F)}\in\mathcal{C}_F(\mathbf{t},\mathbf{z})}r_d^{(F)},$$

$$r_{d,l,\star}^{(M)}(\mathbf{t},\mathbf{z})\triangleq\inf_{\substack{T\in\mathcal{Q}(\mathbf{r}^{(F)})\\:r_d^{(F)}=r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})}}r_{d,l}^{(M)},l\in\mathcal{L},$$

$$r_{d,\Sigma,\star}^{(M)}(\mathbf{t},\mathbf{z})\triangleq\inf_{\substack{T\in\mathcal{Q}(\mathbf{r}^{(F)})\\:r_d^{(F)}=r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})}}\sum_{l\in\mathcal{L}}r_{d,l}^{(M)},$$

$$r_{d,\star}^{(R)}(\mathbf{t},\mathbf{z})\triangleq\inf_{\substack{T\in\mathcal{Q}(\mathbf{r}^{(F)})\\:r_d^{(F)}=r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})}}r_d^{(R)},$$

$$r_{d,l,\star}^{(S)}(\mathbf{t},\mathbf{z})\triangleq\inf_{\substack{T\in\mathcal{Q}(\mathbf{r}^{(F)})\\:r_d^{(F)}=r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})}}r_l^{(S)},l\in\mathcal{L}.$$

$r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})$ is the largest file size that User $d\in\mathcal{D}$ can privately store under the constraints (4) and (5). Then, $r_{d,\star}^{(R)}(\mathbf{t},\mathbf{z})$, $r_{d,l,\star}^{(M)}(\mathbf{t},\mathbf{z})$, $r_{d,\Sigma,\star}^{(M)}(\mathbf{t},\mathbf{z})$, and $r_{d,l,\star}^{(S)}(\mathbf{t},\mathbf{z})$, $l\in\mathcal{L}$, are the minimum amount of local randomness, the minimum amount of public communication to Server l, the minimum amount of public communication to all the servers, and the minimum storage size required at Server l, respectively, needed for User d to obtain $r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})$. A priori, it is unclear whether it is possible to simultaneously obtain $\left(r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})\right)_{d\in\mathcal{D}}$, i.e., whether $\left(r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})\right)_{d\in\mathcal{D}}\in\mathcal{C}_F(\mathbf{t},\mathbf{z})$. We will show that it is actually possible. We will then study whether $r_{d,\star}^{(R)}(\mathbf{t},\mathbf{z})$, $r_{d,l,\star}^{(M)}(\mathbf{t},\mathbf{z})$, and $r_{d,l,\star}^{(S)}(\mathbf{t},\mathbf{z})$, $d\in\mathcal{D}$, $l\in\mathcal{L}$, can be

simultaneously obtained in the achievability of $\left(r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})\right)_{d\in\mathcal{D}}$ with a single coding scheme.

B. Results

In the following theorem, we state impossibility results that are counterpart to the results in Section IV-A for the case $D=1$.

Theorem 8: Let $\mathbf{t}\triangleq(t_d)_{d\in\mathcal{D}}\in[1,L]^D$ and $\mathbf{z}\triangleq(z_d)_{d\in\mathcal{D}}\in\bigtimes_{d\in\mathcal{D}}[1,t_d-1]$. Consider the following leakage symmetry condition

$$\forall d\in\mathcal{D},(\forall\mathcal{U},\mathcal{V}\subseteq\mathcal{L},$$
$$|\mathcal{U}|=|\mathcal{V}|\implies I(F_d;M_{d,\mathcal{U}},K_{d,\mathcal{U}})=I(F_d;M_{d,\mathcal{V}},K_{d,\mathcal{V}})). \quad (6)$$

Then, for any $d\in\mathcal{D}$, we have

$$r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})\leq n_d(t_d-z_d), \quad (7)$$

$$r_{d,l,\star}^{(S)}(\mathbf{t},\mathbf{z})\geq\sum_{d\in\mathcal{D}}n_d,\forall l\in\mathcal{L}, \quad (8)$$

$$r_{d,\Sigma,\star}^{(M)}(\mathbf{t},\mathbf{z})\geq\frac{L}{t_d-z_d}r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z}), \quad (9)$$

$$(6)\implies r_{d,l,\star}^{(M)}(\mathbf{t},\mathbf{z})\geq\frac{1}{t_d-z_d}r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z}),\forall l\in\mathcal{L}, \quad (10)$$

$$r_{d,\star}^{(R)}(\mathbf{t},\mathbf{z})\geq\frac{z_d}{t_d-z_d}r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z}). \quad (11)$$

(7) is proved in Appendix A and means that it is impossible for User $d\in\mathcal{D}$ to store a file of length larger than $n_d(t_d-z_d)$ bits. (8) is proved in Appendix B and means that Server $l\in\mathcal{L}$ needs a storage capacity of at least $\sum_{d\in\mathcal{D}}n_d$ bits. (9) is proved in Appendix C and means that it is impossible for User $d\in\mathcal{D}$ to store a file of length $r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})$ if the public communication sum-length to the servers is smaller than $\frac{L}{t_d-z_d}r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})$ bits. (10) is proved in Appendix D and means that, under the leakage symmetry condition (6), it is impossible for User $d\in\mathcal{D}$ to store a file of length $r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})$ if the public communication length to Server $l\in\mathcal{L}$ is smaller than $\frac{1}{t_d-z_d}r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})$ bits. (11) is proved in Appendix E and means that it is impossible for User $d\in\mathcal{D}$ to store a file of length $r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})$ if the amount of its local randomness is smaller than $\frac{z_d}{t_d-z_d}r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})$ bits.

We now give a counterpart to Theorem 6 for the case $D=1$ with the following achievability result.

Theorem 9: Let $\mathbf{t}\triangleq(t_d)_{d\in\mathcal{D}}\in[1,L]^D$ and $\mathbf{z}\triangleq(z_d)_{d\in\mathcal{D}}\in\bigtimes_{d\in\mathcal{D}}[1,t_d-1]$. There exists a $\left(\left(2^{r_d^{(F)}}\right)_{d\in\mathcal{D}}, \left(2^{r_d^{(R)}}\right)_{d\in\mathcal{D}}, \left(2^{r_{d,l}^{(M)}}\right)_{d\in\mathcal{D},l\in\mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l\in\mathcal{L}}\right)$ private file storage strategy that $(\mathbf{t},\mathbf{z})$-achieves $\left(r_d^{(F)}\right)_{d\in\mathcal{D}}$ such that, for any $d\in\mathcal{D}$,

$$r_d^{(F)}=n_d(t_d-z_d),$$
$$r_d^{(R)}=n_dz_d,$$
$$r_l^{(S)}=\sum_{d\in\mathcal{D}}n_d,\forall l\in\mathcal{L},$$
$$r_{d,l}^{(M)}=n_d,\forall l\in\mathcal{L}.$$

Proof: See Appendix F. ∎

Then, similar to Theorem 7 and Corollary 1 for the case $D = 1$, we deduce the following results. Theorem 10 provides a characterization of the quantities introduced in Definition 6, and Corollary 2 shows that the optimal quantities of Definition 6 (defined for each individual user) can be obtained simultaneously by a single private file storage strategy.

Theorem 10: Let $\mathbf{t} \triangleq (t_d)_{d \in \mathcal{D}} \in [1, L]^D$ and $\mathbf{z} \triangleq (z_d)_{d \in \mathcal{D}} \in \bigtimes_{d \in \mathcal{D}}[1, t_d - 1]$. For any $d \in \mathcal{D}$, we have

$$r_{d,\star}^{(F)}(\mathbf{t}, \mathbf{z}) = n_d(t_d - z_d),$$
$$r_{d,\star}^{(R)}(\mathbf{t}, \mathbf{z}) = n_d z_d,$$
$$r_{d,l,\star}^{(S)}(\mathbf{t}, \mathbf{z}) = \sum_{d \in \mathcal{D}} n_d, \forall l \in \mathcal{L},$$
$$r_{d,\Sigma,\star}^{(M)}(\mathbf{t}, \mathbf{z}) = L n_d,$$
$$(6) \implies \left(r_{d,l,\star}^{(M)}(\mathbf{t}, \mathbf{z}) = n_d, \forall l \in \mathcal{L} \right).$$

Proof: See Appendix G. ∎

Corollary 2: Let $\mathbf{t} \triangleq (t_d)_{d \in \mathcal{D}} \in [1, L]^D$ and $\mathbf{z} \triangleq (z_d)_{d \in \mathcal{D}} \in \bigtimes_{d \in \mathcal{D}}[1, t_d - 1]$. There exists a $\left(\left(2^{r_d^{(F)}} \right)_{d \in \mathcal{D}}, \left(2^{r_d^{(R)}} \right)_{d \in \mathcal{D}}, \left(2^{r_{d,l}^{(M)}} \right)_{d \in \mathcal{D}, l \in \mathcal{L}}, \left(2^{r_l^{(S)}} \right)_{l \in \mathcal{L}} \right)$ private file storage strategy that $(\mathbf{t}, \mathbf{z})$-achieves $\left(r_d^{(F)} \right)_{d \in \mathcal{D}}$ such that, for any $d \in \mathcal{D}$,

$$r_d^{(F)} = r_{d,\star}^{(F)}(\mathbf{t}, \mathbf{z}),$$
$$r_d^{(R)} = r_{d,\star}^{(R)}(\mathbf{t}, \mathbf{z}),$$
$$r_l^{(S)} = r_{d,l,\star}^{(S)}(\mathbf{t}, \mathbf{z}), \forall l \in \mathcal{L},$$
$$\sum_{l \in \mathcal{L}} r_{d,l}^{(M)} = r_{d,\Sigma,\star}^{(M)}(\mathbf{t}, \mathbf{z}),$$
$$r_{d,l}^{(M)} = r_{d,l,\star}^{(M)}(\mathbf{t}, \mathbf{z}), \forall l \in \mathcal{L}, \text{ when (6) holds.}$$

VI. CONCLUDING REMARKS

We considered the problem of storing a file in L servers such that any $t \leq L$ servers can reconstruct the file, and any subset of $z < t$ colluding servers cannot learn any information about the file. Unlike solutions that rely on traditional secret sharing models, we developed a new model that does not make the assumption that individual and information-theoretically secure channels between the user and each server are available at no cost. Instead, we assume that the user can communicate with the servers over a one-way public channel, and share with each server a secret key with length n, which is meant to quantify the cost of privately storing the file. For a given secret-key length n and parameters t and z, we established the maximal length of the file that the user can store. Additionally, we determine in this case the minimum amount of local randomness needed at the user, the minimum amount of public communication between the user and the servers, and the minimum amount of storage space required at the servers. While our model allows a joint design of the creation phase of the shares and the secure distribution phase of the shares, our results prove the optimality of an achievability scheme that separates the creation of the shares using ramp secret sharing schemes and the secure distribution of the shares via one-time pads. Finally, we discussed an extension of our results to a multi-user setting.

At least two generalizations of the problem setting can be considered and remain open. In the first generalization, the user and the servers communicate over noisy, instead of noiseless, channels; partial results have been obtained in [26] for this setting and constructive coding schemes have been proposed in [27], [28]. In the second generalization, the user and the servers have access to arbitrarily correlated random variables instead of independent and uniformly distributed secret keys; partial results have been obtained in this direction in [29]–[32] and constructive coding schemes have been proposed in [33].

APPENDIX A
PROOF OF EQUATION (7)

Consider an arbitrary $\left(\left(2^{r_d^{(F)}} \right)_{d \in \mathcal{D}}, \left(2^{r_d^{(R)}} \right)_{d \in \mathcal{D}}, \left(2^{r_{d,l}^{(M)}} \right)_{d \in \mathcal{D}, l \in \mathcal{L}}, \left(2^{r_l^{(S)}} \right)_{l \in \mathcal{L}} \right)$ private file storage strategy that $(\mathbf{t}, \mathbf{z})$-achieves $\left(r_d^{(F)} \right)_{d \in \mathcal{D}}$. Fix $d \in \mathcal{D}$. Define $\{d\}^c \triangleq \mathcal{D} \backslash \{d\}$. In the following lemma, using Definition 4 and the reliability and security constraints (4) and (5) from Definition 5, we first give an upper bound on $r_d^{(F)}$ that only depends on the secret keys.

Lemma 1: Let $\mathcal{A}, \mathcal{U} \subseteq \mathcal{L}$ such that $|\mathcal{A}| = t_d$, $|\mathcal{U}| = z_d$, and $\mathcal{U} \subset \mathcal{A}$. We have

$$r_d^{(F)} \leq I(K_{\mathcal{D},\mathcal{A}}, K_{\{d\}^c, \mathcal{L}}; K_{d, \mathcal{L}} | K_{\mathcal{D}, \mathcal{U}}).$$

Proof: We have

$$r_d^{(F)}$$
$$\overset{(a)}{=} H(F_d)$$
$$= H(F_d | M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}}) + I(F_d; M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}})$$
$$\overset{(b)}{\leq} H(F_d | M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}}) + I(F_{\mathcal{Z}_d}; M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}})$$
$$\overset{(c)}{=} H(F_d | M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}})$$
$$= I(\widehat{F}_d(\mathcal{A}); F_d | M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}}) + H(F_d | M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}}, \widehat{F}_d(\mathcal{A}))$$
$$\overset{(d)}{\leq} I(\widehat{F}_d(\mathcal{A}); F_d | M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}}) + H(F_d | \widehat{F}_d(\mathcal{A}))$$
$$\overset{(e)}{=} I(\widehat{F}_d(\mathcal{A}); F_d | M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}})$$
$$\overset{(f)}{\leq} I(M_\mathcal{D}, K_{\mathcal{D}, \mathcal{A}}; F_d | M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}})$$
$$\overset{(g)}{=} I(K_{\mathcal{D}, \mathcal{A}}; F_d | M_\mathcal{D}, K_{\mathcal{D}, \mathcal{U}})$$
$$\overset{(h)}{\leq} I(K_{\mathcal{D}, \mathcal{A}}, M_{\{d\}^c}; F_d, M_d | K_{\mathcal{D}, \mathcal{U}})$$
$$\overset{(i)}{\leq} I(K_{\mathcal{D}, \mathcal{A}}, F_{\{d\}^c}, K_{\{d\}^c, \mathcal{L}}, R_{\{d\}^c}; K_{d, \mathcal{L}}, F_d, R_d | K_{\mathcal{D}, \mathcal{U}})$$
$$\overset{(j)}{=} I(K_{\mathcal{D}, \mathcal{A}}, F_{\{d\}^c}, K_{\{d\}^c, \mathcal{L}}; K_{d, \mathcal{L}}, F_d | K_{\mathcal{D}, \mathcal{U}})$$
$$\quad + I(K_{\mathcal{D}, \mathcal{A}}, F_{\{d\}^c}, K_{\{d\}^c, \mathcal{L}}; R_d | K_{\mathcal{D}, \mathcal{U}}, K_{d, \mathcal{L}}, F_d)$$
$$\quad + I(R_{\{d\}^c}; K_{d, \mathcal{L}}, F_d, R_d | K_{\mathcal{D}, \mathcal{U}}, K_{\mathcal{D}, \mathcal{A}}, F_{\{d\}^c}, K_{\{d\}^c, \mathcal{L}})$$
$$\overset{(k)}{=} I(K_{\mathcal{D}, \mathcal{A}}, F_{\{d\}^c}, K_{\{d\}^c, \mathcal{L}}; K_{d, \mathcal{L}}, F_d | K_{\mathcal{D}, \mathcal{U}})$$
$$\overset{(l)}{\leq} I(K_{\mathcal{D}, \mathcal{A}}, K_{\{d\}^c, \mathcal{L}}; K_{d, \mathcal{L}} | K_{\mathcal{D}, \mathcal{U}}),$$

where (a) holds by uniformity of the files $(F_d)_{d \in \mathcal{D}}$, (b) holds by the chain rule and non-negativity of the

mutual information, (c) holds by (5) because $|\mathcal{U}| = z_d$, (d) holds because conditioning reduces entropy, (e) holds by (4) because $|\mathcal{A}| = t_d$, (f) holds because $\hat{F}_d(\mathcal{A})$ is a function of $S_{\mathcal{A},d}$, which is itself a function of $(M_\mathcal{D}, K_{\mathcal{D},\mathcal{A}})$, (g) holds because $I(M_\mathcal{D}; F_d | M_\mathcal{D}, K_{\mathcal{D},\mathcal{U}}, K_{\mathcal{D},\mathcal{A}}) = 0$, (h) holds by the chain rule applied twice and non-negativity of the mutual information, (i) holds because $M_{\{d\}^c}$ is a function of $(F_{\{d\}^c}, K_{\{d\}^c,\mathcal{L}}, R_{\{d\}^c})$ (with the notation $F_\mathcal{S} \triangleq (F_d)_{d \in \mathcal{S}}$ and $R_\mathcal{S} \triangleq (R_d)_{d \in \mathcal{S}}$ for any $\mathcal{S} \subseteq \mathcal{D}$), and M_d is a function of $(F_d, K_{d,\mathcal{L}}, R_d)$, (j) holds by the chain rule applied twice, (k) holds by independence between $R_{\{d\}^c}$ and $(K_{\mathcal{D},\mathcal{A}}, F_{\{d\}^c}, K_{\{d\}^c,\mathcal{L}}, K_{d,\mathcal{L}}, F_d, R_d, K_{\mathcal{D},\mathcal{U}})$ and by independence between R_d and $(K_{\mathcal{D},\mathcal{A}}, F_{\{d\}^c}, K_{\{d\}^c,\mathcal{L}}, K_{d,\mathcal{L}}, F_d, K_{\mathcal{D},\mathcal{U}})$, (l) holds by applying twice the chain rule, independence between $F_{\{d\}^c}$ and $(K_{\mathcal{D},\mathcal{A}}, K_{\{d\}^c,\mathcal{L}}, K_{d,\mathcal{L}}, F_d, K_{\mathcal{D},\mathcal{U}})$, and independence between F_d and $(K_{\mathcal{D},\mathcal{A}}, K_{\{d\}^c,\mathcal{L}}, K_{d,\mathcal{L}}, K_{\mathcal{D},\mathcal{U}})$ similar to (j) and (k). ∎

Next, we simplify the upper bound of Lemma 1 using the independence of the secret keys as follows.

Lemma 2: Let $\mathcal{A}, \mathcal{U} \subseteq \mathcal{L}$ such that $|\mathcal{A}| = t_d$, $|\mathcal{U}| = z_d$, and $\mathcal{U} \subset \mathcal{A}$. We have

$$I(K_{\mathcal{D},\mathcal{A}}, K_{\{d\}^c,\mathcal{L}}; K_{d,\mathcal{L}} | K_{\mathcal{D},\mathcal{U}}) \leq n_d(t_d - z_d).$$

Proof: We have

$$
\begin{aligned}
&I(K_{\mathcal{D},\mathcal{A}}, K_{\{d\}^c,\mathcal{L}}; K_{d,\mathcal{L}} | K_{\mathcal{D},\mathcal{U}}) \\
&= I(K_{\mathcal{D},\mathcal{A}}; K_{d,\mathcal{L}} | K_{\mathcal{D},\mathcal{U}}) + I(K_{\{d\}^c,\mathcal{L}}; K_{d,\mathcal{L}} | K_{\mathcal{D},\mathcal{A}} K_{\mathcal{D},\mathcal{U}}) \\
&\overset{(a)}{\leq} I(K_{\mathcal{D},\mathcal{A}}; K_{d,\mathcal{L}} | K_{\mathcal{D},\mathcal{U}}) \\
&\quad + I(K_{\{d\}^c,\mathcal{L}}, K_{\{d\}^c,\mathcal{A}}, K_{\{d\}^c,\mathcal{U}}; K_{d,\mathcal{L}}, K_{d,\mathcal{A}}, K_{d,\mathcal{U}}) \\
&= I(K_{\mathcal{D},\mathcal{A}}; K_{d,\mathcal{L}} | K_{\mathcal{D},\mathcal{U}}) + I(K_{\{d\}^c,\mathcal{L}}; K_{d,\mathcal{L}}) \\
&\overset{(b)}{=} I(K_{\mathcal{D},\mathcal{A}}; K_{d,\mathcal{L}} | K_{\mathcal{D},\mathcal{U}}) \\
&\overset{(c)}{\leq} I(K_{\mathcal{D},\mathcal{A}}, K_{\{d\}^c,\mathcal{U}}; K_{d,\mathcal{L}} | K_{d,\mathcal{U}}) \\
&= I(K_{d,\mathcal{A}}; K_{d,\mathcal{L}} | K_{d,\mathcal{U}}) \\
&\quad + I(K_{\{d\}^c,\mathcal{A}}, K_{\{d\}^c,\mathcal{U}}; K_{d,\mathcal{L}} | K_{d,\mathcal{U}}, K_{d,\mathcal{A}}) \\
&\leq I(K_{d,\mathcal{A}}; K_{d,\mathcal{L}} | K_{d,\mathcal{U}}) \\
&\quad + I(K_{\{d\}^c,\mathcal{A}}, K_{\{d\}^c,\mathcal{U}}; K_{d,\mathcal{L}}, K_{d,\mathcal{U}}, K_{d,\mathcal{A}}) \\
&\overset{(d)}{=} I(K_{d,\mathcal{A}}; K_{d,\mathcal{L}} | K_{d,\mathcal{U}}) \\
&\overset{(e)}{=} H(K_{d,\mathcal{A}} | K_{d,\mathcal{U}}) \\
&\overset{(f)}{=} H(K_{d,\mathcal{A} \setminus \mathcal{U}}) \\
&\overset{(g)}{=} n_d(t_d - z_d),
\end{aligned}
$$

where (a) holds by the chain rule applied twice and non-negativity of the mutual information, (b) holds by independence between the keys $K_{\{d\}^c,\mathcal{L}}$ and $K_{d,\mathcal{L}}$, (c) holds by the chain rule and non-negativity of the mutual information, (d) holds by independence between $(K_{\{d\}^c,\mathcal{A}}, K_{\{d\}^c,\mathcal{U}})$ and $(K_{d,\mathcal{L}}, K_{d,\mathcal{U}}, K_{d,\mathcal{A}})$, (e) holds because $\mathcal{A} \subseteq \mathcal{L}$, (f) holds because $\mathcal{U} \subset \mathcal{A}$, (g) holds because the keys $K_{d,l}$, $l \in \mathcal{A} \setminus \mathcal{U}$, are independent and each uniformly distributed over $\{0,1\}^{n_d}$ and $|\mathcal{A} \setminus \mathcal{U}| = t_d - z_d$. ∎

Next, by combining Lemmas 1 and 2, we have

$$r_d^{(F)} \leq n_d(t_d - z_d). \tag{12}$$

Finally, note that (12) is valid for any private file storage strategy that $(\mathbf{t}, \mathbf{z})$-achieves $\left(r_d^{(F)}\right)_{d \in \mathcal{D}} \in \mathcal{C}_F(\mathbf{t}, \mathbf{z})$, so, in particular, (12) is valid for a file storage strategy that $(\mathbf{t}, \mathbf{z})$-achieves $\left(\bar{r}_d^{(F)}\right)_{d \in \mathcal{D}}$, where $\left(\bar{r}_d^{(F)}\right)_{d \in \mathcal{D}} \in \mathcal{C}_F(\mathbf{t}, \mathbf{z})$ is such that $\bar{r}_d^{(F)} = r_{d,\star}^{(F)}(\mathbf{t}, \mathbf{z})$.

APPENDIX B
PROOF OF EQUATION (8)

Server $l \in \mathcal{L}$ must store the keys $K_{\mathcal{D},l}$ at the beginning of the protocol. Hence, for any $d \in \mathcal{D}$, $l \in \mathcal{L}$, we must have

$$
\begin{aligned}
r_{d,l,\star}^{(S)}(\mathbf{t}, \mathbf{z}) &\geq |K_{\mathcal{D},l}| \\
&= \sum_{d \in \mathcal{D}} |K_{d,l}| \\
&= \sum_{d \in \mathcal{D}} n_d.
\end{aligned}
$$

APPENDIX C
PROOF OF EQUATION (9)

Consider an arbitrary $\left(\left(2^{r_d^{(F)}} \right)_{d \in \mathcal{D}}, \left(2^{r_d^{(R)}} \right)_{d \in \mathcal{D}}, \left(2^{r_{d,l}^{(M)}} \right)_{d \in \mathcal{D}, l \in \mathcal{L}}, \left(2^{r_l^{(S)}} \right)_{l \in \mathcal{L}} \right)$ private file storage strategy that $(\mathbf{t}, \mathbf{z})$-achieves $\left(r_d^{(F)}\right)_{d \in \mathcal{D}}$. Fix $d \in \mathcal{D}$. In the following lemma, using Definition 4 and the reliability and security constraints (4) and (5) from Definition 5, we first give a lower bound on the sum of the entropy of the message $(M_{d,l})_{l \in \mathcal{S}}$ for sets $\mathcal{S} \subset \mathcal{L}$ with cardinality $|\mathcal{S}| = t_d - z_d$.

Lemma 3: For $\mathcal{T} \subseteq \mathcal{L}$ and $\mathcal{S} \subseteq \mathcal{L} \setminus \mathcal{T}$ such that $|\mathcal{T}| = z_d$ and $|\mathcal{S}| = t_d - z_d$, we have

$$\sum_{l \in \mathcal{S}} H(M_{d,l}) \geq H(F_d).$$

Proof: We have

$$
\begin{aligned}
&\sum_{l \in \mathcal{S}} H(M_{d,l}) + \sum_{l \in \mathcal{S}} H(K_{d,l}) \\
&\overset{(a)}{\geq} \sum_{l \in \mathcal{S}} H(M_{d,l} | K_{d,l}) + \sum_{l \in \mathcal{S}} H(K_{d,l}) \\
&= \sum_{l \in \mathcal{S}} H(M_{d,l}, K_{d,l}) \\
&\overset{(b)}{\geq} H(M_{d,\mathcal{S}}, K_{d,\mathcal{S}}) \\
&\overset{(c)}{\geq} H(M_{d,\mathcal{S}}, K_{d,\mathcal{S}} | M_{d,\mathcal{T}}, K_{d,\mathcal{T}}) \\
&= I(M_{d,\mathcal{S}}, K_{d,\mathcal{S}}; F_d | M_{d,\mathcal{T}}, K_{d,\mathcal{T}}) \\
&\quad + H(M_{d,\mathcal{S}}, K_{d,\mathcal{S}} | F_d, M_{d,\mathcal{T}}, K_{d,\mathcal{T}}) \\
&= H(F_d | M_{d,\mathcal{T}}, K_{d,\mathcal{T}}) - H(F_d | M_{d,\mathcal{S}}, K_{d,\mathcal{S}}, M_{d,\mathcal{T}}, K_{d,\mathcal{T}}) \\
&\quad + H(M_{d,\mathcal{S}}, K_{d,\mathcal{S}} | F_d, M_{d,\mathcal{T}}, K_{d,\mathcal{T}}) \\
&\overset{(d)}{\geq} H(F_d | M_{d,\mathcal{T}}, K_{d,\mathcal{T}}) - H(F_d | S_{\mathcal{S} \cup \mathcal{T}, d}) \\
&\quad + H(M_{d,\mathcal{S}}, K_{d,\mathcal{S}} | F_d, M_{d,\mathcal{T}}, K_{d,\mathcal{T}})
\end{aligned}
$$

$$\overset{(e)}{\geq} H(F_d|M_{d,T}, K_{d,T}) - H(F_d|\widehat{F}_d(\mathcal{S} \cup T))$$
$$+ H(M_{d,\mathcal{S}}, K_{d,\mathcal{S}}|F_d, M_{d,T}, K_{d,T})$$
$$= H(F_d) - I(F_d; M_{d,T}, K_{d,T}) - H(F_d|\widehat{F}_d(\mathcal{S} \cup T))$$
$$+ H(M_{d,\mathcal{S}}, K_{d,\mathcal{S}}|F_d, M_{d,T}, K_{d,T})$$
$$\overset{(f)}{\geq} H(F_d) - I(F_{Z_d}; M_{\mathcal{D}}, K_{\mathcal{D},T}) - H(F_d|\widehat{F}_d(\mathcal{S} \cup T))$$
$$+ H(M_{d,\mathcal{S}}, K_{d,\mathcal{S}}|F_d, M_{d,T}, K_{d,T})$$
$$\overset{(g)}{=} H(F_d) + H(M_{d,\mathcal{S}}, K_{d,\mathcal{S}}|F_d, M_{d,T}, K_{d,T})$$
$$\overset{(h)}{\geq} H(F_d) + H(M_{d,\mathcal{S}}, K_{d,\mathcal{S}}|F_d, R_d, K_{d,T})$$
$$\overset{(i)}{\geq} H(F_d) + H(K_{d,\mathcal{S}}|F_d, R_d, K_{d,T})$$
$$\overset{(j)}{=} H(F_d) + \sum_{l \in \mathcal{S}} H(K_{d,l}),$$

where (a) and (c) hold because conditioning reduces entropy, (b) holds by the chain rule and because conditioning reduces entropy, (d) holds because $S_{\mathcal{S},d}$ is a function of $(M_{d,\mathcal{S}}, K_{d,\mathcal{S}})$ and $S_{T,d}$ is a function of $(M_{d,T}, K_{d,T})$, (e) holds because $\widehat{F}_d(\mathcal{S} \cup T)$ is a function of $S_{\mathcal{S} \cup T, d}$, (f) holds by the chain rule and non-negativity of the mutual information, (g) holds by (5) because $|T| = z_d$ and by (4) because $|\mathcal{S} \cup T| = t_d$, (h) holds because $M_{d,T}$ is a function of $(F_d, R_d, K_{d,T})$, (i) holds by the chain rule and non-negativity of the entropy, (j) holds because $K_{d,\mathcal{S}}$ is independent from $(F_d, R_d, K_{d,T})$ (since $\mathcal{S} \cap T = \emptyset$) and because the keys $(K_{d,l})_{l \in \mathcal{S}}$ are independent. ∎

Next, by summing both sides of the equation of Lemma 3 over all possible sets $T \subseteq \mathcal{L}$ and $\mathcal{S} \subseteq \mathcal{L} \backslash T$ such that $|T| = z_d$ and $|\mathcal{S}| = t_d - z_d$, we obtain a lower bound on the sum of the entropy of all the message $(M_{d,l})_{l \in \mathcal{L}}$.

Lemma 4: We have

$$\sum_{l \in \mathcal{L}} H(M_{d,l}) \geq \frac{L}{t_d - z_d} H(F_d).$$

Proof: We have

$$\frac{L}{t_d - z_d} H(F_d)$$
$$\overset{(a)}{=} \frac{L}{t_d - z_d} \Upsilon_d \sum_{\substack{T \subseteq \mathcal{L} \\ |T| = z_d}} \sum_{\substack{\mathcal{S} \subseteq T^c \\ |\mathcal{S}| = t_d - z_d}} H(F_d)$$
$$\overset{(b)}{\leq} \frac{L}{t_d - z_d} \Upsilon_d \sum_{\substack{T \subseteq \mathcal{L} \\ |T| = z_d}} \sum_{\substack{\mathcal{S} \subseteq T^c \\ |\mathcal{S}| = t_d - z_d}} \sum_{l \in \mathcal{S}} H(M_{d,l})$$
$$\overset{(c)}{=} \frac{L}{t_d - z_d} \Upsilon_d \sum_{\substack{T \subseteq \mathcal{L} \\ |T| = z_d}} \binom{L - z_d - 1}{t_d - z_d - 1} \sum_{l \in T^c} H(M_{d,l})$$
$$\overset{(d)}{=} \frac{L}{t_d - z_d} \Upsilon_d \binom{L - z_d - 1}{t_d - z_d - 1} \sum_{\substack{T \subseteq \mathcal{L} \\ |T| = L - z_d}} \sum_{l \in T} H(M_{d,l})$$
$$\overset{(e)}{=} \frac{L}{t_d - z_d} \Upsilon_d \binom{L - z_d - 1}{t_d - z_d - 1} \binom{L - 1}{L - z_d - 1} \sum_{l \in \mathcal{L}} H(M_{d,l})$$

$$= \sum_{l \in \mathcal{L}} H(M_{d,l}),$$

where (a) holds with $\Upsilon_d \triangleq \binom{L}{z_d}^{-1} \binom{L - z_d}{t_d - z_d}^{-1}$, (b) holds by Lemma 3, (c) holds because for any $l \in T^c$, $H(M_{d,l})$ appears exactly $\binom{L - z_d - 1}{t_d - z_d - 1}$ times in the term $\sum_{\substack{\mathcal{S} \subseteq T^c \\ |\mathcal{S}| = t_d - z_d}} \sum_{l \in \mathcal{S}} H(M_{d,l})$ (note that this observation was also made in [34, Lemma 3.2]), (d) holds by a change of variables in the sums, (e) holds because for any $l \in \mathcal{L}$, $H(M_{d,l})$ appears exactly $\binom{L - 1}{L - z_d - 1}$ times in the term $\sum_{\substack{T \subseteq \mathcal{L} \\ |T| = L - z_d}} \sum_{l \in T} H(M_{d,l})$. ∎

Finally, we have

$$\frac{L}{t_d - z_d} r_d^{(F)} \overset{(a)}{=} \frac{L}{t_d - z_d} H(F_d)$$
$$\overset{(b)}{\leq} \sum_{l \in \mathcal{L}} H(M_{d,l})$$
$$\leq \sum_{l \in \mathcal{L}} r_{d,l}^{(M)}, \tag{13}$$

where (a) holds by uniformity of F_d, (b) holds by Lemma 4. Since (13) is valid for any private file storage strategy, (13) is also valid for a $\left(\left(2^{\tilde{r}_d^{(F)}} \right)_{d \in \mathcal{D}}, \left(2^{\tilde{r}_d^{(R)}} \right)_{d \in \mathcal{D}}, \left(2^{\tilde{r}_{d,l}^{(M)}} \right)_{d \in \mathcal{D}, l \in \mathcal{L}}, \left(2^{\tilde{r}_l^{(S)}} \right)_{l \in \mathcal{L}} \right)$ file storage strategy that $(\mathbf{t}, \mathbf{z})$-achieves $\left(\tilde{r}_d^{(F)} \right)_{d \in \mathcal{D}}$, where $\left(\tilde{r}_d^{(F)} \right)_{d \in \mathcal{D}} \in \mathcal{C}_F(\mathbf{t}, \mathbf{z})$ is such that $\tilde{r}_d^{(F)} = r_{d,\star}^{(F)}(\mathbf{t}, \mathbf{z})$ and $\sum_{l \in \mathcal{L}} \tilde{r}_{d,l}^{(M)} = r_{d,\Sigma,\star}^{(M)}(\mathbf{t}, \mathbf{z})$.

APPENDIX D
PROOF OF EQUATION (10)

Consider an arbitrary $\left(\left(2^{r_d^{(F)}} \right)_{d \in \mathcal{D}}, \left(2^{r_d^{(R)}} \right)_{d \in \mathcal{D}}, \left(2^{r_{d,l}^{(M)}} \right)_{d \in \mathcal{D}, l \in \mathcal{L}}, \left(2^{r_l^{(S)}} \right)_{l \in \mathcal{L}} \right)$ private file storage strategy that $(\mathbf{t}, \mathbf{z})$-achieves $\left(r_d^{(F)} \right)_{d \in \mathcal{D}}$. Assume that (6) holds. Fix $d \in \mathcal{D}$, $l \in \mathcal{L}$. By exploiting the leakage symmetry condition (6), we derive a first lower bound on the public communication to a specific server in the following lemma.

Lemma 5: For $i \in [z_d, t_d - 1]$, define $\mathcal{V}_i \triangleq \begin{cases} [1, i] & \text{if } l > i \\ [1, i + 1] \backslash \{l\} & \text{if } l \leq i \end{cases}$ and $\mathcal{V}_{t_d} \triangleq \mathcal{V}_{t_d - 1} \cup \{l\}$. For $i \in \mathcal{L}$, and $\mathcal{S} \subseteq \mathcal{L}$ such that $|\mathcal{S}| = i$, define $\alpha_i \triangleq I(F_d; M_{d,\mathcal{S}}, K_{d,\mathcal{S}})$ and $\alpha_{L+1} \triangleq \alpha_L$. Note that α_i only depends on i and not on the specific elements of $\mathcal{S}$ by (6). Note also that $\alpha_{z_d} = 0$ by (5) and $\alpha_{t_d} = H(F_d)$ by (4). Then, we have

$$H(M_{d,l}) \geq \sum_{i = z_d}^{t_d - 1} [2\alpha_{i+1} - \alpha_i - \alpha_{i+2}]^+. \tag{14}$$

Proof: We have

$$H(M_{d,l}) + H(K_{d,l})$$

$$\overset{(a)}{\geq} H(M_{d,l}) + H(K_{d,l}|M_{d,l})$$

$$= H(M_{d,l}, K_{d,l})$$

$$\overset{(b)}{\geq} H(M_{d,l}, K_{d,l}|M_{d,v_{z_d}}, K_{d,v_{z_d}})$$

$$\overset{(c)}{=} H(M_{d,l}, K_{d,l}|M_{d,v_{z_d}}, K_{d,v_{z_d}})$$
$$\quad - H(M_{d,l}, K_{d,l}|M_{d,v_{t_d}}, K_{d,v_{t_d}})$$

$$= \sum_{i=z_d}^{t_d-1} [H(M_{d,l}, K_{d,l}|M_{d,v_i}, K_{d,v_i})$$
$$\quad - H(M_{d,l}, K_{d,l}|M_{d,v_{i+1}}, K_{d,v_{i+1}})] \qquad (15)$$

$$\overset{(d)}{=} \sum_{i=z_d}^{t_d-1} [H(M_{d,l}, K_{d,l}, F_d|M_{d,v_i}, K_{d,v_i})$$
$$\quad - H(F_d|M_{d,v_i \cup \{l\}}, K_{d,v_i \cup \{l\}})$$
$$\quad - H(M_{d,l}, K_{d,l}, F_d|M_{d,v_{i+1}}, K_{d,v_{i+1}})$$
$$\quad + H(F_d|M_{d,v_{i+1} \cup \{l\}}, K_{d,v_{i+1} \cup \{l\}})]$$

$$\overset{(e)}{=} \sum_{i=z_d}^{t_d-1} [H(F_d|M_{d,v_i}, K_{d,v_i})$$
$$\quad + H(M_{d,l}, K_{d,l}|F_d, M_{d,v_i}, K_{d,v_i})$$
$$\quad - H(F_d|M_{d,v_i \cup \{l\}}, K_{d,v_i \cup \{l\}})$$
$$\quad - H(F_d|M_{d,v_{i+1}}, K_{d,v_{i+1}})$$
$$\quad - H(M_{d,l}, K_{d,l}|F_d, M_{d,v_{i+1}}, K_{d,v_{i+1}})$$
$$\quad + H(F_d|M_{d,v_{i+1} \cup \{l\}}, K_{d,v_{i+1} \cup \{l\}})]$$

$$= \sum_{i=z_d}^{t_d-1} [-I(F_d; M_{d,v_i}, K_{d,v_i})$$
$$\quad + H(M_{d,l}, K_{d,l}|F_d, M_{d,v_i}, K_{d,v_i})$$
$$\quad + I(F_d; M_{d,v_i \cup \{l\}}, K_{d,v_i \cup \{l\}})$$
$$\quad + I(F_d; M_{d,v_{i+1}}, K_{d,v_{i+1}})$$
$$\quad - H(M_{d,l}, K_{d,l}|F_d, M_{d,v_{i+1}}, K_{d,v_{i+1}})$$
$$\quad - I(F_d; M_{d,v_{i+1} \cup \{l\}}, K_{d,v_{i+1} \cup \{l\}})]$$

$$\overset{(f)}{=} \sum_{i=z_d}^{t_d-1} [2\alpha_{i+1} - \alpha_i - \alpha_{i+2}$$
$$\quad + H(M_{d,l}, K_{d,l}|F_d, M_{d,v_i}, K_{d,v_i})$$
$$\quad - H(M_{d,l}, K_{d,l}|F_d, M_{d,v_{i+1}}, K_{d,v_{i+1}})]$$

$$\overset{(g)}{\geq} [2\alpha_{t_d} - \alpha_{t_d-1} - \alpha_{t_d+1}$$
$$\quad + H(M_{d,l}, K_{d,l}|F_d, M_{d,v_{t_d-1}}, K_{d,v_{t_d-1}})]$$
$$\quad + \sum_{i=z_d}^{t_d-2} [2\alpha_{i+1} - \alpha_i - \alpha_{i+2}]$$

$$\overset{(h)}{\geq} [2\alpha_{t_d} - \alpha_{t_d-1} - \alpha_{t_d+1}$$
$$\quad + H(M_{d,l}, K_{d,l}|F_d, M_{d,v_{t_d-1}}, K_{d,v_{t_d-1}})]^+$$
$$\quad + \sum_{i=z_d}^{t_d-2} [2\alpha_{i+1} - \alpha_i - \alpha_{i+2}]^+$$

$$\overset{(i)}{=} [\alpha_{t_d} - \alpha_{t_d-1} + H(M_{d,l}, K_{d,l}|F_d, M_{d,v_{t_d-1}}, K_{d,v_{t_d-1}})]^+$$
$$\quad + \sum_{i=z_d}^{t_d-2} [2\alpha_{i+1} - \alpha_i - \alpha_{i+2}]^+$$

$$\overset{(j)}{=} [\alpha_{t_d} - \alpha_{t_d-1} + H(M_{d,l}, K_{d,l}|F_d, M_{d,v_{t_d-1}}, K_{d,v_{t_d-1}})]$$
$$\quad + \sum_{i=z_d}^{t_d-2} [2\alpha_{i+1} - \alpha_i - \alpha_{i+2}]^+$$

$$\overset{(k)}{=} H(M_{d,l}, K_{d,l}|F_d, M_{d,v_{t_d-1}}, K_{d,v_{t_d-1}})$$
$$\quad + \sum_{i=z_d}^{t_d-1} [2\alpha_{i+1} - \alpha_i - \alpha_{i+2}]^+$$

$$\overset{(l)}{\geq} H(K_{d,l}|F_d, M_{d,v_{t_d-1}}, K_{d,v_{t_d-1}})$$

$$\overset{(m)}{\geq} H(K_{d,l}|F_d, R_d, K_{d,v_{t_d-1}}) + \sum_{i=z_d}^{t_d-1} [2\alpha_{i+1} - \alpha_i - \alpha_{i+2}]^+$$

$$\overset{(n)}{=} H(K_{d,l}) + \sum_{i=z_d}^{t_d-1} [2\alpha_{i+1} - \alpha_i - \alpha_{i+2}]^+,$$

where (a) and (b) hold because conditioning reduces entropy, (c) holds because $l \in \mathcal{V}_{t_d}$, (d) and (e) hold by the chain rule, (f) holds by the definition of α_i, (g) holds because for any $i \in [z_d, t_d - 2]$, $H(M_{d,l}, K_{d,l}|F_d, M_{d,v_i}, K_{d,v_i}) \geq H(M_{d,l}, K_{d,l}|F_d, M_{d,v_{i+1}}, K_{d,v_{i+1}})$ since conditioning reduces entropy and $\mathcal{V}_i \subset \mathcal{V}_{i+1}$, and because $H(M_{d,l}, K_{d,l}|F_d, M_{d,v_{t_d}}, K_{d,v_{t_d}}) = 0$ since $l \in \mathcal{V}_{t_d}$, (h) holds because in (15), we observe that $H(M_{d,l}, K_{d,l}|M_{d,v_i}, K_{d,v_i}) - H(M_{d,l}, K_{d,l}|M_{d,v_{i+1}}, K_{d,v_{i+1}}) \geq 0$ since conditioning reduces entropy and $\mathcal{V}_i \subset \mathcal{V}_{i+1}$, (i) holds because $\alpha_{t_d+1} = \alpha_{t_d} = H(F_d)$ by (4), (j) holds because $\alpha_{t_d} \geq \alpha_{t_d-1}$ by the definition of α_{t_d} and α_{t_d-1}, (k) holds because $\alpha_{t_d} - \alpha_{t_d-1} = [2\alpha_{t_d} - \alpha_{t_d-1} - \alpha_{t_d+1}]^+$, (l) holds by the chain rule and non-negativity of the entropy, (m) holds because $M_{d,v_{t_d-1}}$ is a function of $(F_d, R_d, K_{d,v_{t_d-1}})$, (n) holds by independence between $K_{d,l}$ and $(F_d, R_d, K_{d,v_{t_d-1}})$ since $\{l\} \cap \mathcal{V}_{t_d-1} = \emptyset$. ∎

Next, we remark that the lower bound of Lemma 5 is lower bounded by

$$\min_{f \in \mathcal{F}} \sum_{i=1}^{t_d - z_d} [2 f(i+1) - f(i) - f(i+2)]^+,$$

where the minimum is taken over the set $\mathcal{F}$ of all the functions $f : [1, t_d - z_d + 2] \to [0, H(F_d)]$ that are non-decreasing (because, by construction, $(\alpha_i)_{i \in [1, L+1]}$ is a non-decreasing sequence) and such that $f(1) = \alpha_{z_d} = 0$, $f(t_d - z_d + 2) = f(t_d - z_d + 1) = \alpha_{t_d} = H(F_d)$. In the following lemma, we determine a lower bound for this optimization problem.

Lemma 6: For any $f \in \mathcal{F}$, we have

$$\sum_{i=1}^{t_d - z_d} [2 f(i+1) - f(i) - f(i+2)]^+ \geq \frac{H(F_d)}{t_d - z_d}. \qquad (16)$$

Proof: Let $f \in \mathcal{F}$ and let f^+ be the concave envelope of f over $[1, t_d - z_d + 2]$, i.e., for $i \in [1, t_d - z_d + 2]$, $f^+(i) \triangleq \min\{g(i) : g \geq f, g \text{ is concave}\}$. Note that $f^+(1) = f(1)$ and $f^+(t_d - z_d + 2) = f(t_d - z_d + 2)$. Then, for any $i \in [1, t_d - z_d]$ such that $f(i+1) = f^+(i+1)$, we have

$$[2f(i+1) - f(i) - f(i+2)]^+$$
$$\geq 2f(i+1) - f(i) - f(i+2)$$
$$\overset{(a)}{\geq} 2f(i+1) - f^+(i) - f^+(i+2)$$
$$\overset{(b)}{=} 2f^+(i+1) - f^+(i) - f^+(i+2), \qquad (17)$$

where (a) holds because $f^+ \geq f$, (b) holds because $f(i+1) = f^+(i+1)$. Moreover, for any $i \in [1, t_d - z_d]$ such that $f(i+1) \neq f^+(i+1)$, we have

$$[2f(i+1) - f(i) - f(i+2)]^+$$
$$\geq 0$$
$$= 2f^+(i+1) - f^+(i) - f^+(i+2), \qquad (18)$$

where the last equality holds because f^+ is linear between i and $i+2$, i.e., $f^+(i+1) - f^+(i) = f^+(i+2) - f^+(i+1)$. Indeed, by contradiction, assume that f^+ is not linear between i and $i+2$, then, since f^+ is concave, we must have

$$f^+(i+1) > \frac{f^+(i+2) + f^+(i)}{2}. \tag{19}$$

Next, we have a contradiction by constructing h_i, a concave function such that $f \leq h_i < f^+$, as follows:

$$h_i : j \mapsto \begin{cases} f^+(j) & \text{if } j \neq i+1 \\ \max\left(\frac{f^+(i+2) + f^+(i)}{2}, f(i+1)\right) & \text{if } j = i+1 \end{cases}.$$

We have $f \leq h_i$ (since $f \leq f^+$), and $h_i < f^+$ by (19) and because $f^+(i+1) > f(i+1)$ (since $f^+ \geq f$ and $f^+(i+1) \neq f(i+1)$). Then, to show concavity of h_i, it is sufficient to show that h_i^Δ is non-increasing where h_i^Δ is defined as

$$h_i^\Delta : [1, t_d - z_d + 1] \to \mathbb{R}$$
$$j \mapsto h_i(j+1) - h_i(j).$$

For $j \in [1, i-2] \cup [i+2, t_d - z_d + 1]$, we have

$$h_i^\Delta(j+1) \leq h_i^\Delta(j) \tag{20}$$

by definition of h_i^Δ and concavity of f^+. Then, we have

$$h_i^\Delta(i) \overset{(a)}{=} h_i(i+1) - h_i(i)$$
$$\overset{(b)}{=} h_i(i+1) - f^+(i)$$
$$\overset{(c)}{\leq} f^+(i+1) - f^+(i)$$
$$\overset{(d)}{\leq} f^+(i) - f^+(i-1)$$
$$\overset{(e)}{=} h_i(i) - h_i(i-1)$$
$$\overset{(f)}{=} h_i^\Delta(i-1),$$

where (a) and (f) hold by definition of h_i^Δ, (b) and (e) hold by definition of h_i, (c) holds because $h_i < f^+$, (d) holds by concavity of f^+. Then, we have

$$h_i^\Delta(i+1) \overset{(a)}{=} h_i(i+2) - h_i(i+1)$$
$$\overset{(b)}{=} f^+(i+2) - h_i(i+1)$$
$$\overset{(c)}{\leq} h_i(i+1) - f^+(i)$$
$$\overset{(d)}{=} h_i(i+1) - h_i(i)$$
$$\overset{(e)}{=} h_i^\Delta(i), \tag{21}$$

where (a) and (e) hold by definition of h_i^Δ, (b) and (d) hold by definition of h_i, (c) holds because $\frac{f^+(i+2) + f^+(i)}{2} \leq h_i(i+1)$.

Then, we also have

$$h_i^\Delta(i+2) \overset{(a)}{=} h_i(i+3) - h_i(i+2)$$
$$\overset{(b)}{=} f^+(i+3) - f^+(i+2)$$
$$\overset{(c)}{\leq} f^+(i+2) - f^+(i+1)$$
$$\overset{(d)}{\leq} f^+(i+2) - h_i(i+1)$$
$$\overset{(e)}{=} h_i(i+2) - h_i(i+1)$$
$$\overset{(f)}{=} h_i^\Delta(i+1), \tag{22}$$

where (a) and (f) hold by definition of h_i^Δ, (b) and (e) hold by definition of h_i, (c) holds by concavity of f^+, (d) holds because $h_i < f^+$. Hence, by (20), (21), and (22), h_i^Δ is non-increasing and we have thus proved (18) by contradiction.

Next, we have

$$\sum_{i=1}^{t_d - z_d} [2 f(i+1) - f(i) - f(i+2)]^+$$
$$\overset{(a)}{\geq} \sum_{i=1}^{t_d - z_d} [2 f^+(i+1) - f^+(i) - f^+(i+2)]$$
$$= \sum_{i=1}^{t_d - z_d} [(f^+(i+1) - f^+(i)) - (f^+(i+2) - f^+(i+1))]$$
$$= f^+(2) - f^+(1) + f^+(t_d - z_d + 2) - f^+(t_d - z_d + 1)$$
$$\overset{(b)}{=} f^+(2)$$
$$\overset{(c)}{\geq} \frac{H(F_d)}{t_d - z_d},$$

where (a) holds by (17) and (18), (b) holds because $f^+(t_d - z_d + 2) = f^+(t_d - z_d + 1) = f(t_d - z_d + 1) = H(F_d)$ and $f^+(1) = 0$, (c) holds because $f^+(2) = f^+(2) - f^+(1) \geq (f^+(t_d - z_d + 1) - f^+(1))/(t_d - z_d)$ by concavity of f^+ and where we have used that $f^+(t_d - z_d + 1) = H(F_d)$ and $f^+(1) = f(1) = 0$. ∎

Next, by combining Lemmas 5 and 6, we have

$$r_{d,l}^{(M)} \geq H(M_{d,l})$$
$$\overset{(a)}{\geq} H(F_d)\frac{1}{t_d - z_d}$$
$$\overset{(b)}{=} r_d^{(F)}\frac{1}{t_d - z_d}, \tag{23}$$

where (a) holds by (14) and (16), which is valid for any $f \in \mathcal{F}$, (b) holds by uniformity of F_d.

Finally, since (23) is valid for any private file storage strategy, (23) is also valid for a file storage strategy that $(\mathbf{t}, \mathbf{z})$-achieves $\left(\bar{r}_d^{(F)}\right)_{d \in \mathcal{D}}$, where $\left(\bar{r}_d^{(F)}\right)_{d \in \mathcal{D}} \in \mathcal{C}_F(\mathbf{t}, \mathbf{z})$ is such that $\bar{r}_d^{(F)} = r_{d,\star}^{(F)}(\mathbf{t}, \mathbf{z})$ and $\bar{r}_{d,l}^{(M)} = r_{d,l,\star}^{(M)}(\mathbf{t}, \mathbf{z})$.

<div style="column: left">

APPENDIX E
PROOF OF EQUATION (11)

Consider an arbitrary $\left(\left(2^{r_d^{(F)}}\right)_{d\in\mathcal{D}}, \left(2^{r_d^{(R)}}\right)_{d\in\mathcal{D}}, \left(2^{r_{d,l}^{(M)}}\right)_{d\in\mathcal{D},l\in\mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l\in\mathcal{L}}\right)$ private file storage strategy that $(\mathbf{t},\mathbf{z})$-achieves $\left(r_d^{(F)}\right)_{d\in\mathcal{D}}$. Fix $d\in\mathcal{D}$. Let $\mathcal{V}\subseteq\mathcal{L}$ such that $v\triangleq|\mathcal{V}|<z_d$. For $\mathcal{T}\subseteq\mathcal{L}\backslash\mathcal{V}$ and $\mathcal{S}\subseteq\mathcal{L}\backslash(\mathcal{T}\cup\mathcal{V})$ such that $|\mathcal{T}|=z_d-v$ and $|\mathcal{S}|=t_d-z_d$. Using Definition 4 and the reliability and security constraints (4) and (5) from Definition 5, we first derive the following lemma.

Lemma 7: We have

$$\sum_{l\in\mathcal{S}}H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})\geq H(F_d)+\sum_{l\in\mathcal{S}}H(K_{d,l}).$$
(24)

Proof: We have

$\sum_{l\in\mathcal{S}}H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})$

$\overset{(a)}{\geq} H(M_{d,\mathcal{S}},K_{d,\mathcal{S}}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})$

$\overset{(b)}{\geq} H(M_{d,\mathcal{S}},K_{d,\mathcal{S}}|M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})$

$= I(M_{d,\mathcal{S}},K_{d,\mathcal{S}};F_d|M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})$
$\quad + H(M_{d,\mathcal{S}},K_{d,\mathcal{S}}|F_d,M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})$

$= H(F_d|M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})$
$\quad - H(F_d|M_{d,\mathcal{V}\cup\mathcal{T}\cup\mathcal{S}},K_{d,\mathcal{V}\cup\mathcal{T}\cup\mathcal{S}})$
$\quad + H(M_{d,\mathcal{S}},K_{d,\mathcal{S}}|F_d,M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})$

$\overset{(c)}{\geq} H(F_d|M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})-H(F_d|S_{\mathcal{V}\cup\mathcal{T}\cup\mathcal{S},d})$
$\quad + H(M_{d,\mathcal{S}},K_{d,\mathcal{S}}|F_d,M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})$

$\overset{(d)}{\geq} H(F_d|M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})-H(F_d|\widehat{F}_d(\mathcal{V}\cup\mathcal{T}\cup\mathcal{S}))$
$\quad + H(M_{d,\mathcal{S}},K_{d,\mathcal{S}}|F_d,M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})$

$\overset{(e)}{=} H(F_d)+H(M_{d,\mathcal{S}},K_{d,\mathcal{S}}|F_d,M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})$

$\overset{(f)}{\geq} H(F_d)+H(M_{d,\mathcal{S}},K_{d,\mathcal{S}}|F_d,R_d,K_{d,\mathcal{V}\cup\mathcal{T}})$

$\overset{(g)}{\geq} H(F_d)+H(K_{d,\mathcal{S}}|F_d,R_d,K_{d,\mathcal{V}\cup\mathcal{T}})$

$\overset{(h)}{=} H(F_d)+H(K_{d,\mathcal{S}})$

$\overset{(i)}{=} H(F_d)+\sum_{l\in\mathcal{S}}H(K_{d,l}),$

where (a) holds by the chain rule and because conditioning reduces entropy, (b) holds because conditioning reduces entropy, (c) holds because $S_{\mathcal{V}\cup\mathcal{T}\cup\mathcal{S},d}$ is a function of $(M_{d,\mathcal{V}\cup\mathcal{T}},K_{d,\mathcal{V}\cup\mathcal{T}})$, (d) holds because $\widehat{F}_d(\mathcal{V}\cup\mathcal{T}\cup\mathcal{S})$ is a function of $S_{\mathcal{V}\cup\mathcal{T}\cup\mathcal{S},d}$, (e) holds by (4) because $|\mathcal{V}\cup\mathcal{T}\cup\mathcal{S}|=t_d$ and by (5) because $|\mathcal{V}\cup\mathcal{T}|=z_d$, (f) holds because $M_{d,\mathcal{V}\cup\mathcal{T}}$ is a function of $(F_d,R_d,K_{d,\mathcal{V}\cup\mathcal{T}})$, (g) holds by the chain rule and non-negativity of entropy, (h) holds by independence

</div>

<div style="column: right">

between $K_{d,\mathcal{S}}$ and $(F_d,R_d,K_{d,\mathcal{V}\cup\mathcal{T}})$ because $\mathcal{S}\cap(\mathcal{V}\cup\mathcal{T})=\emptyset$, (i) holds by independence of the keys $(K_{d,l})_{l\in\mathcal{S}}$. ∎

Next, by summing both side of the equation of Lemma 7 over of all possible sets $\mathcal{T}\subseteq\mathcal{L}\backslash\mathcal{V}$ and $\mathcal{S}\subseteq\mathcal{L}\backslash(\mathcal{T}\cup\mathcal{V})$ such that $|\mathcal{T}|=z_d-v$ and $|\mathcal{S}|=t_d-z_d$, we obtain the following lemma.

Lemma 8: Consider

$$l^\star(\mathcal{V})\in\arg\max_{l\in\mathcal{L}\backslash\mathcal{V}}\left[H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l})\right].$$

We have

$\frac{1}{t_d-z_d}H(F_d)$
$\leq H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d,M_{d,\mathcal{V}},K_{d,\mathcal{V}})$
$\quad - H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d,M_{d,\mathcal{V}\cup\{l^\star(\mathcal{V})\}},K_{d,\mathcal{V}\cup\{l^\star(\mathcal{V})\}})-n_d.$
(25)

Proof: We have

$\frac{1}{t_d-z_d}H(F_d)$

$\overset{(a)}{=}\Omega_d\sum_{\substack{\mathcal{T}\subseteq\mathcal{L}\backslash\mathcal{V}\\|\mathcal{T}|=z_d-v}}\sum_{\substack{\mathcal{S}\subseteq\mathcal{L}\backslash(\mathcal{T}\cup\mathcal{V})\\|\mathcal{S}|=t_d-z_d}}H(F_d)$

$\overset{(b)}{\leq}\Omega_d\sum_{\substack{\mathcal{T}\subseteq\mathcal{L}\backslash\mathcal{V}\\|\mathcal{T}|=z_d-v}}\sum_{\substack{\mathcal{S}\subseteq\mathcal{L}\backslash(\mathcal{T}\cup\mathcal{V})\\|\mathcal{S}|=t_d-z_d}}$
$\quad\sum_{l\in\mathcal{S}}[H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l})]$

$\overset{(c)}{=}\Omega_d\sum_{\substack{\mathcal{T}\subseteq\mathcal{L}\backslash\mathcal{V}\\|\mathcal{T}|=z_d-v}}\binom{L-z_d-1}{t_d-z_d-1}$
$\quad\times\sum_{l\in\mathcal{L}\backslash(\mathcal{T}\cup\mathcal{V})}[H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l})]$

$\overset{(d)}{=}\Omega_d\binom{L-z_d-1}{t_d-z_d-1}$
$\quad\times\sum_{\substack{\mathcal{T}\subseteq\mathcal{L}\backslash\mathcal{V}\\|\mathcal{T}|=L-z_d}}\sum_{l\in\mathcal{T}}[H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l})]$

$\overset{(e)}{=}\Omega_d\binom{L-z_d-1}{t_d-z_d-1}\binom{L-v-1}{L-z_d-1}$
$\quad\times\sum_{l\in\mathcal{L}\backslash\mathcal{V}}[H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l})]$

$=\frac{1}{L-v}\sum_{l\in\mathcal{L}\backslash\mathcal{V}}[H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l})]$

$\overset{(f)}{\leq}[H(M_{d,l^\star(\mathcal{V})},K_{d,l^\star(\mathcal{V})}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l^\star(\mathcal{V})})]$

$= H(M_{d,l^\star(\mathcal{V})},K_{d,l^\star(\mathcal{V})}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-n_d$

$\overset{(g)}{=} H(M_{d,l^\star(\mathcal{V})},K_{d,l^\star(\mathcal{V})}|F_d,M_{d,\mathcal{V}},K_{d,\mathcal{V}})-n_d$

$\overset{(h)}{=} H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d,M_{d,\mathcal{V}},K_{d,\mathcal{V}})$
$\quad - H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d,M_{d,\mathcal{V}\cup\{l^\star(\mathcal{V})\}},K_{d,\mathcal{V}\cup\{l^\star(\mathcal{V})\}})-n_d,$

where (a) holds with $\Omega_d\triangleq\frac{1}{t_d-z_d}\binom{L-v}{z_d-v}^{-1}\binom{L-z_d}{t_d-z_d}^{-1}$, (b) holds by (24), (c) holds because for any $l\in\mathcal{L}\backslash(\mathcal{T}\cup\mathcal{V})$, the term $[H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l})]$

</div>

appears exactly $\binom{L-z_d-1}{t_d-z_d-1}$ times in the term $\sum_{\substack{S\subseteq\mathcal{L}\setminus(\mathcal{T}\cup\mathcal{V})\\|S|=t_d-z_d}}\sum_{l\in S}[H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l})]$ (note that a similar argument is made in [34, Lemma 3.2]), (d) holds by a change of variables in the sums, (e) holds because for any $l\in\mathcal{L}\setminus\mathcal{V}$, $[H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l})]$ appears exactly $\binom{L-v-1}{L-z_d-1}$ times in the term $\sum_{\mathcal{T}\subseteq\mathcal{L}\setminus\mathcal{V}|\mathcal{T}|=L-z}\sum_{l\in\mathcal{T}}[H(M_{d,l},K_{d,l}|M_{d,\mathcal{V}},K_{d,\mathcal{V}})-H(K_{d,l})]$, (f) holds by the definition of $l^\star(\mathcal{V})$, (g) holds because $I(F_d;M_{d,\mathcal{V}\cup\{l^\star(\mathcal{V})\}},K_{d,\mathcal{V}\cup\{l^\star(\mathcal{V})\}})=0$ by (2) and since $|\mathcal{V}\cup\{l^\star(\mathcal{V})\}|\leq z_d$, (h) holds by the chain rule. ∎

Next, we apply multiple times Lemma 8 to obtain the following lemma.

Lemma 9: Define $\mathcal{V}_0\triangleq\emptyset$ and for $i\in[1,z_d]$, $\mathcal{V}_i\triangleq\mathcal{V}_{i-1}\cup\{l^\star(\mathcal{V}_{i-1})\}$. We have

$$\frac{z_d}{t_d-z_d}H(F_d)\leq H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d)$$
$$-H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d,M_{d,\mathcal{V}_{z_d}},K_{d,\mathcal{V}_{z_d}})-n_dz_d.$$

Proof: We have

$$\frac{z_d}{t_d-z_d}H(F_d)$$
$$=\sum_{i=0}^{z_d-1}\frac{1}{t_d-z_d}H(F_d)$$
$$\leq\sum_{i=0}^{z_d-1}[H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d,M_{d,\mathcal{V}_i},K_{d,\mathcal{V}_i})$$
$$-H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d,M_{d,\mathcal{V}_{i+1}},K_{d,\mathcal{V}_{i+1}})-n_d]$$
$$=H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d)$$
$$-H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d,M_{d,\mathcal{V}_{z_d}},K_{d,\mathcal{V}_{z_d}})-n_dz_d,$$

where the inequality holds by applying z_d times Equation (25) and the definition of $\mathcal{V}_i$, $i\in[\![0,z_d]\!]$. ∎

Finally, we simplify the upper bound of Lemma 9 as follows. We have

$$\frac{z_d}{t_d-z_d}r_d^{(F)}$$
$$\overset{(a)}{=}\frac{z_d}{t_d-z_d}H(F_d)$$
$$\overset{(b)}{\leq}H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d)$$
$$-H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d,M_{d,\mathcal{V}_{z_d}},K_{d,\mathcal{V}_{z_d}})-n_dz_d$$
$$\overset{(c)}{\leq}H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d)$$
$$-H(K_{d,\mathcal{L}}|F_d,M_{d,\mathcal{V}_{z_d}},K_{d,\mathcal{V}_{z_d}})-n_dz_d$$
$$\overset{(d)}{\leq}H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d)-H(K_{d,\mathcal{L}}|F_d,R_d,K_{d,\mathcal{V}_{z_d}})-n_dz_d$$
$$=H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d)-H(K_{d,\mathcal{V}_{z_d}^c}|F_d,R_d)-n_dz_d$$
$$\overset{(e)}{=}H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d)-H(K_{d,\mathcal{V}_{z_d}^c})-n_dz_d$$
$$\overset{(f)}{=}H(M_{d,\mathcal{L}},K_{d,\mathcal{L}}|F_d)-n_dL$$
$$\overset{(g)}{\leq}H(R_d,F_d,K_{d,\mathcal{L}}|F_d)-n_dL$$
$$=H(R_d,K_{d,\mathcal{L}}|F_d)-n_dL$$
$$\overset{(h)}{=}H(R_d)+H(K_{d,\mathcal{L}})-n_dL$$
$$\overset{(i)}{=}H(R_d)$$
$$\overset{(j)}{=}r_d^{(R)},\tag{26}$$

where (a) holds by uniformity of F_d, (b) holds by Lemma 9, (c) holds by the chain rule and non-negativity of entropy, (d) holds because $M_{d,\mathcal{V}_{z_d}}$ is a function of $(F_d,R_d,K_{d,\mathcal{V}_{z_d}})$, (e) holds by independence between $K_{d,\mathcal{V}_{z_d}^c}$ and (F_d,R_d), (f) holds by the uniformity of the keys $(K_{d,l})_{l\in\mathcal{V}_{z_d}^c}$, (g) holds because $M_{d,\mathcal{L}},K_{d,\mathcal{L}}$ is a function of $(R_d,F_d,K_{d,\mathcal{L}})$, (h) holds by mutual independence between R_d, F_d, and $K_{d,\mathcal{L}}$, (i) holds by the uniformity of the keys $(K_{d,l})_{l\in\mathcal{L}}$, (j) holds by uniformity of R_d.

Since (26) is valid for any private file storage strategy, (26) is also valid for a

$$\left(\left(2^{\tilde{r}_d^{(F)}}\right)_{d\in\mathcal{D}},\left(2^{\tilde{r}_d^{(R)}}\right)_{d\in\mathcal{D}},\left(2^{\tilde{r}_{d,l}^{(M)}}\right)_{d\in\mathcal{D},l\in\mathcal{L}},\left(2^{\tilde{r}_l^{(S)}}\right)_{l\in\mathcal{L}}\right)$$

file storage strategy that $(\mathbf{t},\mathbf{z})$-achieves $\left(\tilde{r}_d^{(F)}\right)_{d\in\mathcal{D}}$, where $\left(\tilde{r}_d^{(F)}\right)_{d\in\mathcal{D}}\in\mathcal{C}_F(\mathbf{t},\mathbf{z})$ is such that $\tilde{r}_d^{(F)}=r_{d,\star}^{(F)}(\mathbf{t},\mathbf{z})$ and $\tilde{r}_d^{(R)}=r_{d,\star}^{(R)}(\mathbf{t},\mathbf{z})$.

APPENDIX F
PROOF OF THEOREM 9

We first review the notion of ramp secret sharing [21], [22] in Section F-A. We then present our achievability scheme and its analysis in Section F-B.

A. Review of Ramp Secret Sharing

Definition 7 ([21], [22]): Let $t\in[1,L]$ and $z\in[1,t-1]$. A (t,z,L)-ramp secret sharing scheme consists of

- A secret S uniformly distributed over $\{0,1\}^{n_s}$;
- A stochastic encoder $e:\{0,1\}^{n_s}\times\{0,1\}^{n_r}\to\{0,1\}^{n_{sh}L}$, $(S,R)\mapsto(H_l)_{l\in\mathcal{L}}$, which takes as input the secret S and a randomization sequence R uniformly distributed over $\{0,1\}^{n_r}$ and independent of S, and outputs L shares $(H_l)_{l\in\mathcal{L}}$ of length n_{sh}. For any $S\subseteq\mathcal{L}$, we define $H_S\triangleq(H_l)_{l\in\mathcal{S}}$;

and satisfies the two conditions

$$\max_{\mathcal{T}\subseteq\mathcal{L}:|\mathcal{T}|=t}H(S|H_\mathcal{T})=0,\quad\text{(Recoverability)}\tag{27}$$

$$\max_{\mathcal{U}\subseteq\mathcal{L}:|\mathcal{U}|\leq z}I(S;H_\mathcal{U})=0.\quad\text{(Security)}\tag{28}$$

Theorem 11 ([21], [22]): Let $t\in[1,L]$ and $z\in[1,t-1]$. For a fixed secret length n_s, there exists a (t,z,L)-ramp secret sharing scheme such that the length of a share n_{sh} and the length of the randomization sequence n_r satisfy

$$n_{sh}=\frac{n_s}{t-z},\quad n_r=\frac{n_sz}{t-z}.$$

B. Achievability Scheme for Theorem 9

Coding scheme: Fix $d\in\mathcal{D}$ and consider a file F_d such that $r_d^{(F)}=|F_d|=n_d(t_d-z_d)$. Then, User d forms $(H_{l,d})_{l\in\mathcal{L}}$ with a (t_d,z_d,L)-ramp secret sharing scheme taken from Theorem 11 applied to F_d. By Theorem 11, for $l\in\mathcal{L}$, the length of a share is $|H_{l,d}|=\frac{|F_d|}{t_d-z_d}=n_d$, and the length of the randomization sequence is $n_r=\frac{|F_d|z_d}{t_d-z_d}=n_dz_d$. Hence, since $|K_{d,l}|=n_d$, $l\in\mathcal{L}$, User d can form $M_{d,l}\triangleq H_{l,d}\oplus K_{d,l}$ and publicly send it to Server l, where $\oplus$ denotes bitwise

modulo-two addition. Upon receiving $M_{d,l}$, Server l stores $S_{l,d} \triangleq K_{d,l} \oplus M_{d,l} = H_{l,d}$.

Resources needed: For $d \in \mathcal{D}$, $l \in \mathcal{L}$, the length of the randomization sequence at User d is $r_d^{(R)} = n_r = n_d z_d$, the length of the public communication from User d to Server l is $r_{d,l}^{(M)} = |M_{d,l}| = n_d$, and the storage needed at Server l is $r_l^{(S)} = \sum_{d \in \mathcal{D}} |M_{d,l}| = \sum_{d \in \mathcal{D}} n_d$.

Analysis of recoverability: For $d \in \mathcal{D}$, consider an arbitrary subset $\mathcal{A} \subseteq \mathcal{L}$ of t_d servers that pool their information, they then have access to $(S_{l,d})_{l \in \mathcal{A}} = (H_{l,d})_{l \in \mathcal{A}}$ such that by Theorem 11, $H(F_d|(H_{l,d})_{l \in \mathcal{A}}) = 0$ since $|\mathcal{A}| = t_d$.

Analysis of security: For $d \in \mathcal{D}$, consider an arbitrary subset $\mathcal{U} \subseteq \mathcal{L}$ of z_d colluding servers. Then, we have

$$I(F_{\mathcal{Z}_d}; M_{\mathcal{D}}, K_{\mathcal{D},\mathcal{U}})$$

$$\overset{(a)}{=} I(F_{\mathcal{Z}_d}; M_{\mathcal{Z}_d}, K_{\mathcal{Z}_d,\mathcal{U}})$$
$$+ I(F_{\mathcal{Z}_d}; M_{\mathcal{Z}_d^c}, K_{\mathcal{Z}_d^c,\mathcal{U}}|M_{\mathcal{Z}_d}, K_{\mathcal{Z}_d,\mathcal{U}})$$

$$\overset{(b)}{=} I(F_{\mathcal{Z}_d}; M_{\mathcal{Z}_d}, K_{\mathcal{Z}_d,\mathcal{U}})$$

$$\overset{(c)}{=} I(F_{\mathcal{Z}_d \setminus \{d\}}; M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}})$$
$$+ I(F_{\mathcal{Z}_d \setminus \{d\}}; M_d, K_{d,\mathcal{U}}|M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}})$$
$$+ I(F_d; M_{\mathcal{Z}_d}, K_{\mathcal{Z}_d,\mathcal{U}}|F_{\mathcal{Z}_d \setminus \{d\}})$$

$$\overset{(d)}{=} I(F_{\mathcal{Z}_d \setminus \{d\}}; M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}})$$
$$+ I(F_d; M_{\mathcal{Z}_d}, K_{\mathcal{Z}_d,\mathcal{U}}|F_{\mathcal{Z}_d \setminus \{d\}})$$
$$\leq I(F_{\mathcal{Z}_d \setminus \{d\}}; M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}})$$
$$+ I(F_d; M_{\mathcal{Z}_d}, K_{\mathcal{Z}_d,\mathcal{U}}, F_{\mathcal{Z}_d \setminus \{d\}})$$
$$= I(F_{\mathcal{Z}_d \setminus \{d\}}; M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}}) + I(F_d; M_d, K_{d,\mathcal{U}})$$
$$+ I(F_d; M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}}, F_{\mathcal{Z}_d \setminus \{d\}}|M_d, K_{d,\mathcal{U}})$$

$$\overset{(e)}{=} I(F_{\mathcal{Z}_d \setminus \{d\}}; M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}}) + I(F_d; M_d, K_{d,\mathcal{U}})$$

$$\overset{(f)}{\leq} \sum_{i \in \mathcal{Z}_d} I(F_i; M_i, K_{i,\mathcal{U}})$$

$$\overset{(g)}{=} \sum_{i \in \mathcal{Z}_d} I(F_i; H_{\mathcal{U},i}, M_{i,\mathcal{U}^c}, K_{i,\mathcal{U}})$$

$$= \sum_{i \in \mathcal{Z}_d} [I(F_i; H_{\mathcal{U},i}) + I(F_i; M_{i,\mathcal{U}^c}, K_{i,\mathcal{U}}|H_{\mathcal{U},i})]$$

$$\overset{(h)}{=} \sum_{i \in \mathcal{Z}_d} I(F_i; M_{i,\mathcal{U}^c}, K_{i,\mathcal{U}}|H_{\mathcal{U},i})$$

$$= \sum_{i \in \mathcal{Z}_d} [I(F_i; K_{i,\mathcal{U}}|H_{\mathcal{U},i}) + I(F_i; M_{i,\mathcal{U}^c}|H_{\mathcal{U},i}, K_{i,\mathcal{U}})]$$

$$\overset{(j)}{=} \sum_{i \in \mathcal{Z}_d} I(F_i; M_{i,\mathcal{U}^c}|H_{\mathcal{U},i}, K_{i,\mathcal{U}})$$

$$\leq \sum_{i \in \mathcal{Z}_d} I(F_i, H_{\mathcal{U}^c,i}; M_{i,\mathcal{U}^c}|H_{\mathcal{U},i}, K_{i,\mathcal{U}})$$

$$= \sum_{i \in \mathcal{Z}_d} [H(M_{i,\mathcal{U}^c}|H_{\mathcal{U},i}, K_{i,\mathcal{U}})$$
$$- H(M_{i,\mathcal{U}^c}|F_i, H_{\mathcal{U}^c,i}, H_{\mathcal{U},i}, K_{i,\mathcal{U}})]$$
$$\leq \sum_{i \in \mathcal{Z}_d} [|M_{i,\mathcal{U}^c}| - H(M_{i,\mathcal{U}^c}|F_i, H_{\mathcal{U}^c,i}, H_{\mathcal{U},i}, K_{i,\mathcal{U}})]$$

$$\overset{(k)}{=} \sum_{i \in \mathcal{Z}_d} [|M_{i,\mathcal{U}^c}| - H(K_{i,\mathcal{U}^c}|F_i, H_{\mathcal{U}^c,i}, H_{\mathcal{U},i}, K_{i,\mathcal{U}})]$$

$$\overset{(l)}{=} \sum_{i \in \mathcal{Z}_d} [|M_{i,\mathcal{U}^c}| - H(K_{i,\mathcal{U}^c})]$$

$$\overset{(m)}{=} 0,$$

where (a) holds by the chain rule and $\mathcal{Z}_d^c$ denotes the complement of $\mathcal{Z}_d$ in $\mathcal{D}$, (b) holds because $I(F_{\mathcal{Z}_d}; M_{\mathcal{Z}_d^c}, K_{\mathcal{Z}_d^c,\mathcal{U}}|M_{\mathcal{Z}_d}, K_{\mathcal{Z}_d,\mathcal{U}}) \leq I(F_{\mathcal{Z}_d}, M_{\mathcal{Z}_d}, K_{\mathcal{Z}_d,\mathcal{U}}; M_{\mathcal{Z}_d^c}, K_{\mathcal{Z}_d^c,\mathcal{U}}) = 0$, (c) holds by the chain rule applied twice, (d) holds because $I(F_{\mathcal{Z}_d \setminus \{d\}}; M_d, K_{d,\mathcal{U}}|M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}}) \leq I(F_{\mathcal{Z}_d \setminus \{d\}}, M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}}; M_d, K_{d,\mathcal{U}}) = 0$, (e) holds because $I(F_d; M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}}, F_{\mathcal{Z}_d \setminus \{d\}}|M_d, K_{d,\mathcal{U}}) \leq I(F_d, M_d, K_{d,\mathcal{U}}; M_{\mathcal{Z}_d \setminus \{d\}}, K_{\mathcal{Z}_d \setminus \{d\},\mathcal{U}}, F_{\mathcal{Z}_d \setminus \{d\}}) = 0$, (f) holds by iterating the steps between (b) and (e), (g) holds because $M_i = (M_{i,\mathcal{U}^c}, M_{i,\mathcal{U}}) = (M_{i,\mathcal{U}^c}, (H_{i,i} \oplus K_{i,l})_{l \in \mathcal{U}})$, (h) holds because $I(F_i; H_{\mathcal{U},i}) = 0$ by Theorem 11 and since $|\mathcal{U}| = z_d \leq z_i$ for any $i \in \mathcal{Z}_d$, (j) holds because $I(F_i; K_{i,\mathcal{U}}|H_{\mathcal{U},i}) \leq I(F_i, H_{\mathcal{U},i}; K_{i,\mathcal{U}}) = 0$, (k) holds because $M_{i,\mathcal{U}^c} = (H_{i,i} \oplus K_{i,l})_{l \in \mathcal{U}^c}$, (l) holds by independence between $K_{i,\mathcal{U}^c}$ and $(F_i, H_{\mathcal{U}^c,i}, H_{\mathcal{U},i}, K_{i,\mathcal{U}})$, (m) holds because by uniformity of $K_{i,\mathcal{U}^c}$, $H(K_{i,\mathcal{U}^c}) = |K_{i,\mathcal{U}^c}| = |\mathcal{U}^c|n_i = |M_{i,\mathcal{U}^c}|$ for any $i \in \mathcal{Z}_d$.

APPENDIX G
PROOF OF THEOREM 10

The achievability scheme presented in the proof of Theorem 9 provides a

$$\left(\left(2^{r_d^{(F)}}\right)_{d \in \mathcal{D}}, \left(2^{r_d^{(R)}}\right)_{d \in \mathcal{D}}, \left(2^{r_{d,l}^{(M)}}\right)_{d \in \mathcal{D}, l \in \mathcal{L}}, \left(2^{r_l^{(S)}}\right)_{l \in \mathcal{L}} \right)$$

private file storage strategy that $(\mathbf{t}, \mathbf{z})$-achieves $\left(r_d^{(F)} \right)_{d \in \mathcal{D}}$ such that for any $d \in \mathcal{D}$

$$r_d^{(F)} = n_d(t_d - z_d), \tag{29}$$

$$r_d^{(R)} = n_d z_d, \tag{30}$$

$$r_{d,l}^{(M)} = n_d, \forall l \in \mathcal{L}, \tag{31}$$

$$\sum_{l \in \mathcal{L}} r_{d,l}^{(M)} = L n_d, \tag{32}$$

$$r_l^{(S)} = \sum_{d \in \mathcal{D}} n_d, \forall l \in \mathcal{L}. \tag{33}$$

Next, by (29) and (7), we have $r_{d,\star}^{(F)}(\mathbf{t}, \mathbf{z}) = n_d(t_d - z_d)$, $\forall d \in \mathcal{D}$. By (30) and (11), we have $r_{d,\star}^{(R)}(\mathbf{t}, \mathbf{z}) = n_d z_d = \frac{z_d}{t_d - z_d} r_{d,\star}^{(F)}(\mathbf{t}, \mathbf{z}), \forall d \in \mathcal{D}$. By (32) and (9), we have $r_{d,\Sigma,\star}^{(M)}(\mathbf{t}, \mathbf{z}) = L n_d = \frac{L}{t_d - z_d} r_{d,\star}^{(F)}(\mathbf{t}, \mathbf{z}), \forall d \in \mathcal{D}$. By (33) and (8), we have $r_{d,l,\star}^{(S)}(\mathbf{t}, \mathbf{z}) = \sum_{d \in \mathcal{D}} n_d, \forall d \in \mathcal{D}, \forall l \in \mathcal{L}$. Assume that (6) holds, by (31) and (10), we have $r_{d,l,\star}^{(M)}(\mathbf{t}, \mathbf{z}) = n_d = \frac{1}{t_d - z_d} r_{d,\star}^{(F)}(\mathbf{t}, \mathbf{z}), \forall d \in \mathcal{D}, \forall l \in \mathcal{L}$.

REFERENCES

[1] R. A. Chou, "Quantifying the cost of privately storing data in distributed storage systems," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2022, pp. 3287–3292.

[2] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[3] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. Int. Workshop Manag. Requirements Knowl. (MARK)*, Jun. 1979, pp. 313–317.

[4] A. S. Rawat, O. O. Koyluoglu, and S. Vishwanath, "Centralized repair of multiple node failures with applications to communication efficient secret sharing," *IEEE Trans. Inf. Theory*, vol. 64, no. 12, pp. 7529–7550, Dec. 2018.

[5] A. Agarwal and A. Mazumdar, "Security in locally repairable storage," *IEEE Trans. Inf. Theory*, vol. 62, no. 11, pp. 6204–6217, Nov. 2016.

[6] M. Soleymani and H. Mahdavifar, "Distributed multi-user secret sharing," *IEEE Trans. Inf. Theory*, vol. 67, no. 1, pp. 164–178, Jan. 2021.

[7] W. Huang, M. Langberg, J. Kliewer, and J. Bruck, "Communication efficient secret sharing," *IEEE Trans. Inf. Theory*, vol. 62, no. 12, pp. 7195–7206, Dec. 2016.

[8] R. Bitar and S. E. Rouayheb, "Staircase codes for secret sharing with optimal communication and read overheads," *IEEE Trans. Inf. Theory*, vol. 64, no. 2, pp. 933–943, Feb. 2018.

[9] N. B. Shah, K. V. Rashmi, and K. Ramchandran, "Distributed secret dissemination across a network," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1206–1216, Oct. 2015.

[10] W. Huang and J. Bruck, "Secure RAID schemes for distributed storage," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2016, pp. 1401–1405.

[11] W. Huang and J. Bruck, "Secret sharing with optimal decoding and repair bandwidth," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 1813–1817.

[12] R. A. Chou and J. Kliewer, "Secure distributed storage: Rate-privacy trade-off and XOR-based coding scheme," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2020, pp. 605–610.

[13] A. Bessani, M. Correia, B. Quaresma, F. André, and P. Sousa, "DepSky: Dependable and secure storage in a cloud-of-clouds," *ACM Trans. Storage*, vol. 9, no. 4, pp. 1–33, 2013.

[14] R. Shor, G. Yadgar, W. Huang, E. Yaakobi, and J. Bruck, "How to best share a big secret," in *Proc. 11th ACM Int. Syst. Storage Conf.*, 2018, pp. 76–88.

[15] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Inf. Syst.*, vol. 48, pp. 132–150, Mar. 2015.

[16] W. Huang and J. Bruck, "Secure RAID schemes from EVENODD and STAR codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2017, pp. 609–613.

[17] E. Karnin, J. Greene, and M. Hellman, "On secret sharing systems," *IEEE Trans. Inf. Theory*, vol. IT-29, no. 1, pp. 35–41, Jan. 1983.

[18] R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed–Solomon codes," *Commun. ACM*, vol. 24, no. 9, pp. 583–584, 1981.

[19] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Proc. Conf. Theory Appl. Cryptogr.* Berlin, Germany: Springer, 1988, pp. 27–35.

[20] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Electron. Commun. Jpn.*, vol. 72, no. 9, pp. 56–64, 2010.

[21] H. Yamamoto, "Secret sharing system using (k, L, N) threshold scheme," *Electron. Commun. Jpn., I, Commun.*, vol. 69, no. 9, pp. 46–54, 1986.

[22] G. R. Blakley and C. Meadows, "Security of ramp schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1984, pp. 242–268.

[23] C. Blundo, A. De Santis, and U. Vaccaro, "Randomness in distribution protocols," *Inf. Comput.*, vol. 131, no. 2, pp. 111–139, Dec. 1996.

[24] C. Blundo, A. D. Santis, and U. Vaccaro, "Efficient sharing of many secrets," in *Proc. Annu. Symp. Theor. Aspects Comput. Sci.* Berlin, Germany: Springer, 1993, pp. 692–703.

[25] M. Yoshida, T. Fujiwara, and M. P. Fossorier, "Optimal uniform secret sharing," *IEEE Trans. Inf. Theory*, vol. 65, no. 1, pp. 436–443, 2018.

[26] S. Zou, Y. Liang, L. Lai, and S. Shamai (Shitz), "An information theoretic approach to secret sharing," *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3121–3136, Apr. 2015.

[27] R. A. Chou, "Unified framework for polynomial-time wiretap channel codes," 2020, *arXiv:2002.01924*.

[28] R. A. Chou, "Explicit codes for the wiretap channel with uncertainty on the eavesdropper's channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 476–480.

[29] V. Rana, R. A. Chou, and H. M. Kwon, "Information-theoretic secret sharing from correlated Gaussian random variables and public communication," *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 549–559, Jan. 2022.

[30] R. A. Chou, "Distributed secret sharing over a public channel from correlated random variables," 2021, *arXiv:2110.10307*.

[31] R. A. Chou, "Secret sharing over a public channel from correlated random variables," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 991–995.

[32] I. Csiszar and P. Narayan, "Capacity of a shared secret key," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2593–2596.

[33] R. Sultana and R. A. Chou, "Low-complexity secret sharing schemes using correlated random variables and rate-limited public communication," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 970–975.

[34] A. D. Santis and B. Masucci, "Multiple ramp schemes," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1720–1728, Jul. 1999.

Rémi A. Chou received the engineering degree from Supélec, Gif-sur-Yvette, France, in 2011, and the Ph.D. degree in electrical engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2015. From 2015 to 2017, he was a Post-Doctoral Scholar at The Pennsylvania State University, University Park, PA, USA. He is currently an Assistant Professor with the Electrical Engineering and Computer Science Department, Wichita State University, Wichita, KS, USA.