Multi-level Access and Information Leakage in Scalable Cloud Storage

Siyi Yang[1], *Student Member, IEEE*, Clayton Schoeny[1], *Student Member, IEEE*,
Laura Conde-Canencia[2], and Lara Dolecek[1], *Senior Member, IEEE*
[1] Department of Electrical and Computer Engineering, University of California, Los Angeles, Los Angeles, CA 90095 USA
[2] Lab-STICC, CNRS UMR 6285, Université de Bretagne Sud, Lorient, France

***Abstract*—Codes providing multi-level access have received substantial research attention because of their capabilities to combat server failures in cloud storage. We provide a general construction that is both sufficient and necessary for reaching the well-known singleton bound for multi-level accessible codes. We present a general decoding protocol as well. Based on this result, we derive the lower bound on information leakage, which is viewed as the amount of information conveyed from unintended local clouds to the central cloud about their own local messages. We introduce a code construction based on Cauchy Reed-Solomon (CRS) codes, and prove that this construction achieves the lower bound on the information leakage.**

I. Introduction

Codes offering multi-level access have been intensely studied for their capabilities to reduce the average reading cost in various erasure-resilient data storage applications including Flash storage, RAID, cache, and future SSD-based cloud storage architectures, etc [1]. In the conventional setting, the occurrence of an additional error, beyond the error correction capability of a code, results in decoding failure. *Multi-level accessible codes* provide protection against these unexpected errors, where consecutive p messages are jointly written into p sub-blocks. Multi-level access property provides unexpected extra protection against additional errors without affect average reading cost in the normal case, which is beneficial for speeding up reading process in memory.

Various codes offering multi-level decoding have been proposed in recent literature. The family of Reed-Solomon (RS) codes has been a major prototype for constructions of double-level codes with efficient rates [2]. Pyramid Codes [3] and ladder codes [4] offer reduced read reconstruction cost in large-scale storage systems, where extra global parity check nodes are added at each layer while scaling hierarchical networks. The integrated-interleaving (I-I) codes [5] are the first constructions that offer double-level error-correction and achieve the singleton bound. However, these codes are not *multi-level accessible* when they are *multi-level decodable*, in other words, there is no clear mapping between the local information symbols and the corresponding sub-block in a codeword in the I-I codes. Multi-block interleaved codes presented in [6] are the first known codes that enable multi-level access in literature. In this paper, we focus on more general constructions of multi-level accessible codes and their decoding protocols.

II. Model and Notation

We say $\mathcal{C}$ is an $(\mathbf{n}, \mathbf{k}, \mathbf{d})_{\mathbf{q}}$**-code** if $\mathcal{C} \subset GF(q)^n$, $\dim(\mathcal{C}) = k$, and $\min_{\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}, \mathbf{c}_1 \neq \mathbf{c}_2} d_H(\mathbf{c}_1, \mathbf{c}_2) = d$, where d_H refers to the Hamming distance. In a multi-level accessible code $\mathcal{C}$, consecutive p messages, $\mathbf{m}_1, \mathbf{m}_2, \cdots, \mathbf{m}_p$, are jointly mapped into consecutive p codewords, $\mathbf{c}_1, \mathbf{c}_2, \cdots, \mathbf{c}_p$, where $\mathbf{m}_i \in GF(q)^k$, $\mathbf{c}_i \in GF(q)^n$, for all $1 \leq i \leq p$. If there exist (n, k, d_1)-codes $\{\mathcal{C}_i\}_{i=1}^p$, such that $\mathbf{c}_i \in \mathcal{C}_i$ for all $1 \leq i \leq p$, and $\mathcal{C}$ is an (pn, pk, d_2)-code, then we call $\mathcal{C}$ a $(\mathbf{p}, \mathbf{n}, \mathbf{k}, \mathbf{d_1}, \mathbf{d_2})_{\mathbf{q}}$**-code**. Suppose that servers connected to local cloud i store the codeword $\mathbf{c}_i$, $i \in [p]$, then each $(\mathbf{p}, \mathbf{n}, \mathbf{k}, \mathbf{d_1}, \mathbf{d_2})_{\mathbf{q}}$-code, $d_2 \leq 2d_1$, provides multi-level access in the cloud configuration.

Lemma 1. (cf. [7]) *Consider a $(p, n, k, d_1, d_2)_q$-code, and let $r = n - k$. For $\delta \in \mathbb{N}$, $\delta < r$, if $d_2 \leq n + 1$, $d_1 = r - \delta + 1$, then $d_2 \leq r + (p-1)\delta + 1$.*

III. Codes for Multi-Level Access

Note that a generator matrix $\mathbf{G}$ of any $(p, n, k, r - \delta + 1, \min\{r + (p-1)\delta + 1, 2(r - \delta + 1)\})_q$-code has a natural block structure as follows:

$$\mathbf{G} = \left[\begin{array}{c|c|c|c} \mathbf{A}_{1,1} & \mathbf{A}_{1,2} & \cdots & \mathbf{A}_{1,p} \\ \hline \mathbf{A}_{2,1} & \mathbf{A}_{2,2} & \cdots & \mathbf{A}_{2,p} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \mathbf{A}_{p,1} & \mathbf{A}_{p,2} & \cdots & \mathbf{A}_{p,p} \end{array}\right], \tag{1}$$

where $\mathbf{A}_{i,j} \in GF(q)^{k \times n}$, $\forall i, j \in [p]$.

Theorem 1. *The generator matrix $\mathbf{G}$ in (1) must satisfy the following constraints:*

1) *(Local accessibility) $rank\,(\mathbf{A}_{j,j}) = k$, for all $i \in [p]$.*
2) *(Multi-level distance) $\mathbf{A}_{i,j} = \mathbf{B}_{i,j}\mathbf{U}_j$ for some $\mathbf{B}_{i,j}$ and $\mathbf{U}_j$ such that $dim\,(\mathbf{B}_{i,j}) = dim\,(\mathbf{U}_j) = \delta$, $\mathcal{R}(\mathbf{U}_j^T) \cap \mathcal{R}(\mathbf{A}_{j,j}^T) = \{\mathbf{0}_n\}$, for all $i, j \in [p]$, $i \neq j$.*
3) *(Local parity matrix) Let $\mathbf{H}_{\mathrm{C},j} \in GF(q)^{n \times (r-\delta)}$ be a full column rank matrix such that $\mathbf{A}_j\mathbf{H}_{\mathrm{C},j} = \mathbf{U}_j\mathbf{H}_{\mathrm{C},j} = \mathbf{0}_r$. Then, $\mathbf{H}_{\mathrm{C},j}$ is a parity check matrix of an $(n, n - r + \delta, r - \delta + 1)_q$-code, for all $j \in [p]$.*
4) *(Global parity matrix) Let $\mathbf{H}_j \in GF(q)^{n \times r}$ be a full column rank matrix such that $\mathbf{A}_{j,j}\mathbf{H}_j = \mathbf{0}_r$. Then, $\mathbf{H}_j^{\mathrm{G}}$, which is described below, is a parity check matrix of an $(n, n - r - (p-1)\delta, r + (p-1)\delta + 1)_q$-code, for some*

permutation matrix $\mathbf{Q}_j$ *and nonsingular matrix* $\mathbf{L}_j$*, for all* $j \in [p]$*,*

$$\mathbf{H}_j^{\mathrm{G}} = \left[\begin{array}{c|c} \mathbf{Q}_j\mathbf{H}_j & \begin{array}{c} \overbrace{\begin{array}{c|c|c} \mathbf{L}_j\mathbf{B}_{j,1} & \cdots & \mathbf{L}_j\mathbf{B}_{j,p} \end{array}}^{\text{not including } \mathbf{L}_j\mathbf{B}_{j,j}} \\ \hline \mathbf{0}_{r\times(p-1)\delta} \end{array} \end{array}\right]. \quad (2)$$

Construction 1. *(Converse of Theorem 1) Let* $\mathbf{H}_j^{\mathrm{C}} \in GF(q)^{n\times(r-\delta)}$*,* $\mathbf{H}_j^{\mathrm{R}} \in GF(q)^{n\times\delta}$*,* $\mathbf{H}_{i,j} \in GF(q)^{k\times r}$*,* $i, j \in [q]$*,* $i \neq j$*. Suppose that for any* $j \in [p]$*,* $\mathbf{H}_j^{\mathrm{C}}$ *and* $\mathbf{H}_j^{\mathrm{G}}$ *in the following equation can be parity check matrices for an* $(n, n-r+\delta, r-\delta+1)_q$ *code and an* $(n, n-r-(q-1)\delta, r+(q-1)\delta+1)_q$ *code, respectively.*

$$\mathbf{H}_j^{\mathrm{G}} = \left[\begin{array}{c|c|c} \underbrace{\mathbf{H}_j^{\mathrm{C}}}_{n\times(r-\delta)} & \underbrace{\mathbf{H}_j^{\mathrm{R}}}_{n\times\delta} & \begin{array}{c} \overbrace{\begin{array}{c|c|c} \mathbf{H}_{j,1} & \cdots & \mathbf{H}_{j,p} \end{array}}^{\mathbf{H}_{j,i}:\ k\times\delta,\ i\in[p]\setminus\{j\}} \\ \hline \mathbf{0}_{r\times(p-1)\delta} \end{array} \end{array}\right]. \quad (3)$$

Let $\mathbf{Q}_j \in GF(q)^{n\times n}$ *and* $\mathbf{L}_j \in GF(q)^{k\times k}$ *be permutation matrices and invertible matrices, respectively,* $\forall j \in [p]$*. Let* $\tilde{\mathbf{A}}_{j,j} \in GF(q)^{k\times n}$ *be full row rank matrices such that* $\tilde{\mathbf{A}}_{j,j}\left[\mathbf{H}_j^{\mathrm{C}}, \mathbf{H}_j^{\mathrm{R}}\right] = \mathbf{0}_{k\times r}$*,* $\forall j \in [p]$*. Let* $\tilde{\mathbf{U}}_j \in GF(q)^{\delta\times n}$ *be full row rank matrices such that* $\tilde{\mathbf{U}}_j\mathbf{H}_j^{\mathrm{C}} = \mathbf{0}_{\delta\times(r-\delta)}$*,* $\mathcal{R}(\tilde{\mathbf{U}}_j^T) \cap \mathcal{R}(\mathbf{A}_j^T) = \{\mathbf{0}_n\}$*.*

Let $\mathbf{A}_{j,j} = \tilde{\mathbf{A}}_{j,j}\mathbf{Q}_j$*,* $\mathbf{A}_{i,j} = \mathbf{L}_i^{-1}\mathbf{H}_{i,j}\tilde{\mathbf{U}}_j\mathbf{Q}_j$*, for* $i, j \in [p]$*,* $i \neq j$*. Then* $\mathbf{G}$ *in (1) is a generator matrix of a* $(p, n, k, r-\delta+1, r+(p-1)\delta+1)_q$*-code.*

Construction 2. *(CRS-based code) Let* $\mathbf{Q}_j = \mathbf{I}_n$*,* $\mathbf{L}_j = \mathbf{I}_k$*,* $j \in [p]$*. Let* a_i*,* b_j*,* $i \in [k+\delta]$*,* $j \in [r+(p-1)\delta]$ *be distinct elements of* $GF(q)$*, where* $q > n + p\delta$*. Consider the Cauchy matrix* $\mathbf{T} \in GF(q)^{(k+\delta)\times(r+(p-1)\delta)}$ *such that* $(\mathbf{T})_{i,j} = 1/(a_i - b_j)$*,* $i \in [k+\delta]$*,* $j \in [r+(p-1)\delta]$*. For each* $j \in [p]$*, we obtain* $\mathbf{P}_j$*,* $\mathbf{R}_j$*,* $\mathbf{H}_{j,i}$*,* $i, j \in [p]$*,* $i \neq j$*, according to the following partition of* $\mathbf{T}$*,*

$$\mathbf{T} = \left[\begin{array}{c|c} \overbrace{\mathbf{P}_j}^{k\times r} & \begin{array}{c} \overbrace{\begin{array}{c|c|c} \mathbf{H}_{j,1} & \cdots & \mathbf{H}_{j,p} \end{array}}^{\mathbf{H}_{j,i}:\ k\times\delta,\ i\in[p]\setminus\{j\}} \\ \hline \mathbf{0}_{\delta\times(p-1)\delta} \end{array} \\ \hline \mathbf{R}_j & \end{array}\right]. \quad (4)$$

Let $\mathbf{A}_{j,j} = [\mathbf{I}_k, \mathbf{P}_j]$*, and* $\mathbf{U}_j = [\mathbf{0}_{\delta\times k}, \mathbf{R}_j]$*. Then, according to Construction 1,* $\mathbf{B}_{i,j} = \mathbf{H}_{i,j}$*,* $\mathbf{A}_{i,j} = \mathbf{B}_{i,j}\mathbf{U}_j$*,* $i, j \in [p]$*,* $i \neq j$*. Then* $\mathbf{G}$ *in (1) is a generator matrix of a* $(p, n, k, r-\delta+1, r+(p-1)\delta+1)_q$*-code.*

IV. Global Decoding and Data-Privacy

Protocol 1 presents the global decoding protocol for local message $\mathbf{m}_i$, $i \in [p]$. Without loss of generality, suppose the target cloud is cloud 1. Suppose $\mathbf{m}_j = (m_{j,1}, m_{j,2}, \cdots, m_{j,k})$. Define the **information leakage** from neighboring servers $i \in J$, $J \subset [k]$, of local cloud j to local cloud 1 as $I_{j\to1}^{\mathrm{C}}(J) \triangleq I(\mathbf{x}_{j,1}; \{m_{j,i}\}_{i\in J})$. Then, for all $\epsilon \in [k]$ such that $|J| = k-\epsilon$, we have,

$$\min I_{j\to1}^{\mathrm{C}}(J) = \begin{cases} (p-1)\delta - \epsilon, & 0 \leq \epsilon < (p-1)\delta, \\ 0, & \epsilon \geq (p-1)\delta. \end{cases} \quad (5)$$

When the lower bound 0 on the information leakage is attained for all $J \subset [k]$ such that $|J^c| > (p-1)\delta$, as in CRS-based codes presented in Construction 2, every group of $k-(p-1)\delta$ information symbols of the message stored in cloud i appear to be uniformly distributed over $GF(q)^{k-(p-1)\delta}$ at the central cloud. In contrast, when the information leakage is strictly positive, as in RS-based codes presented in [6], the central cloud can obtain nontrivial information about the message symbols in this group.

Protocol 1 Global Decoding of Local Message $\mathbf{m}_i$

Encoding Parameters:
$\mathbf{D}_{j\to i}$, $\mathbf{E}_{j\to i}$, $\mathbf{F}_{j\to i}$, $j \in [p] \setminus \{i\}$;

1: **for** $j \in [p] \setminus \{i\}$ **do**
2: Local cloud j inquires data $\mathbf{c}_j$ from its neighboring servers;
3: Local cloud j decodes $\mathbf{m}_j$ and $\mathbf{y}_j = \sum_{l\neq j} \mathbf{m}_l\mathbf{B}_{l,j}$;
4: Local cloud j sends $\mathbf{x}_{j\to i} = \mathbf{m}_j\mathbf{D}_{j\to i} + \mathbf{y}_j\mathbf{E}_{j\to i}$ to the central cloud;
5: **end for**
6: The central cloud sends $\mathbf{z}_{\mathrm{C}\to i} = \sum_{j\neq i} \mathbf{x}_{j\to i}\mathbf{F}_{j\to i} = [\mathbf{y}_i, \mathbf{m}_i\mathbf{B}_{i,1}, \cdots, \mathbf{m}_i\mathbf{B}_{i,p}]$ to local cloud i;
7: Local cloud i inquires data $\mathbf{c}_i$ from its neighboring servers;
8: Local cloud i decodes $\mathbf{m}_i$ from $\mathbf{c}_i$ and $\mathbf{z}_i$;

V. Conclusion and Future Work

Multi-level accessible codes can be well suited for future SSD-based cloud storage architectures. In this paper, we presented a general construction of these codes and showed that this construction is necessary for any singleton-bound achieving multi-level accessible code. We believe this will be useful for designing other codes in this domain. We studied the decoding protocols and derived bounds on the information leakage of local messages to the central cloud. We proved that the proposed CRS-based construction achieves those bounds.

Acknowledgment

This work has received funding from DYF, NSF under the grant CCF-BSF 1718389, and from the People Programme (Marie Curie Actions) of the European Union's Seventh Framework Programme (FP7/2007-2013) under REA grant agreement n. PCOFUND-GA-2013-609102.

References

[1] M. Blaum and S. R. Hetzler, "Extended product and integrated interleaved codes," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 1497–1513, 2018.

[2] Y. Wu, "Generalized integrated interleaved codes," *IEEE Transactions on Information Theory*, vol. 63, no. 2, pp. 1102–1119, 2017.

[3] C. Huang, M. Chen, and J. Li, "Pyramid codes: Flexible schemes to trade space for access efficiency in reliable data storage systems," *ACM Transactions on Storage (TOS)*, vol. 9, no. 1, pp. 3:1–3:28, 2013.

[4] P. Huang, E. Yaakobi, and P. H. Siegel, "Ladder codes: A class of error-correcting codes with multi-level shared redundancy," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7.

[5] M. Hassner, K. Abdel-Ghaffar, A. Patel, R. Koetter, and B. Trager, "Integrated interleaving-a novel ECC architecture," *IEEE Transactions on Magnetics*, vol. 37, no. 2, pp. 773–775, 2001.

[6] Y. Cassuto, E. Hemo, S. Puchinger, and M. Bossert, "Multi-block interleaved codes for local and global read access," in *Proc. IEEE Int. Symp. Inf. Theory*, 2017, pp. 1758–1762.

[7] J. Han and L. A. Lastras-Montano, "Reliable memories with subline accesses," in *Proc. IEEE Int. Symp. Inf. Theory*, June 2007, pp. 2531–2535.