Staircase Codes for Secret Sharing with Optimal Communication and Read Overheads

Rawad Bitar, Salim El Rouayheb
ECE Department, IIT, Chicago
rbitar@hawk.iit.edu, salim@iit.edu

***Abstract*—We study the communication efficient secret sharing (CESS) problem. A classical threshold secret sharing scheme randomly encodes a secret into n shares given to n parties, such that any set of at least t, $t < n$, parties can reconstruct the secret, and any set of at most z, $z < t$, colluding parties cannot obtain any information about the secret. A CESS scheme satisfies the previous properties of threshold secret sharing. In addition, it has minimum communication and read costs when the user contacts d, $d \geq t$, shares. The intuition behind the possible savings on these costs is that the user is only interested in decoding the secret and does not have to decode the random keys involved in the encoding process. In this paper, we introduce two explicit constructions of CESS codes called *Staircase Codes*. The first construction achieves optimal communication and read costs for a fixed d, $d \geq t$. The second construction achieves optimal costs universally for all possible values of $d, t \leq d \leq n$. Both constructions can be designed over a field $GF(q)$, for any prime power $q > n$.**

I. Introduction

Consider the threshold secret sharing (SS) problem [1], [2] in which a dealer randomly encodes a secret into n shares and distribute them to n parties, such that any set of at least t, $t < n$, parties can reconstruct the secret, and any set of at most z, $z < t$, parties cannot obtain any information about the secret. For instance, let $n = 4, t = 2$ and $z = 1$ and let s be a secret uniformly distributed over $GF(5)$. Then, the following 4 shares $(s+k_1, s+2k_1, s+3k_1, s+4k_1)$ form an SS scheme, with k_1 being a random symbol, called key, chosen uniformly at random from $GF(5)$ and independently of s. A legitimate user can decode the secret by contacting any $t = 2$ parties, downloading their t shares and inverting the linear system. Secrecy is ensured, in an information theoretic sense, because the secret is padded with the key in each share.

Threshold secret sharing code constructions have been extensively studied in the literature, e.g., [1], [3]–[7]. The literature on secret sharing predominantly studies non-threshold secret sharing schemes, with so-called general access structures, e.g., [8]–[10] and references within. In this paper, we focus on the problem of communication (and read) efficient secret sharing (CESS). A CESS scheme satisfies the properties of threshold secret sharing described in the previous paragraph. In addition, it has minimum communication and read overheads when the user contacts d, $d \geq t$, shares. The communication overhead (CO) (respectively read overhead, RO) is defined as the extra amount of information (beyond the secret size) that needs to be downloaded (respectively read) for a legitimate user contacting d parties to be able to decode the secret.

Party 1	Party 2	Party 3	Party 4
$s_1 + s_2 + k_1$	$s_1 + 2s_2 + 4k_1$	$s_1 + 3s_2 + 4k_1$	$s_1 + 4s_2 + k_1$
$k_1 + k_2$	$k_1 + 2k_2$	$k_1 + 3k_2$	$k_1 + 4k_2$

TABLE I
THE STAIRCASE SECRET SHARING CODE FOR $n = 4, t = 2, z = 1$ AND $d = 3$ OVER $GF(5)$.

The CESS problem was introduced by Wang and Wong in [11]. They focused on perfect CESS, where $z = t - 1$, and showed that when $d > t$, the user can download an amount of information that is less than t shares and still decode the secret. Huang et al. [12] studied the CESS problem for all $z < t$. Before going into more details, we illustrate in Example 1 how communication and read costs can be reduced. The CESS code in this example belongs to the new family of Staircase codes which we introduce in Section III.

Example 1: Consider again the SS problem with $n = 4$, $t = 2$, $z = 1$. We assume now that the secret $\mathbf{s}$ is formed of 2 symbols s_1, s_2 over $GF(5)$ and use two keys k_1, k_2 drawn independently and uniformly at random from $GF(5)$. To construct the Staircase code, the secret symbols and keys are arranged in a matrix M as shown in (1). The matrix M is multiplied by a 4×3 Vandermonde matrix V to obtain the matrix $C = VM$. The 4 rows of C form the 4 different shares and give the Staircase code in Table I.

$$C = VM = \underbrace{\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 4 \\ 1 & 4 & 1 \end{bmatrix}}_{V} \underbrace{\begin{bmatrix} s_1 & k_1 \\ s_2 & k_2 \\ k_1 & 0 \end{bmatrix}}_{M}. \tag{1}$$

The nomenclature of Staircase codes comes from the position of the zero block matrices in the general structure of the matrix M (see Table III).

A legitimate user contacting any $t = 2$ parties can decode the secret by downloading the two contacted shares, i.e., 4 symbols. However, a user contacting $d = 3$ parties can decode the secret by downloading only 3 symbols, namely the first symbol (in blue) of each contacted share. The key idea here is that the user is only interested in decoding the secret and not necessarily the keys. When $d = 3$, the user decodes the secret and key k_1, whereas when $d = t = 2$, the user has to decode the secret and both of the keys. This code actually

978-1-5090-1806-2/16/$31.00 ©2016 IEEE

achieves the minimum CO and RO equal to 1 symbol for $d = 3$ (and 2 symbols for $d = t = 2$) given later in (4) and (5). Secrecy is achieved because each $z = 1$ party cannot obtain any information about s_1 and s_2.

Related work: Wang and Wong derived in [11] a lower bound on CO for perfect CESS, where $z = t - 1$. They constructed codes, using polynomial evaluation over $GF(q)$, where $q > n+v$ and $v = LCM\{t+1, \ldots, n\}$[1], which achieve minimum CO and RO universally for all $d,\ t \leq d \leq n$. Zhang et al. [13] constructed CESS codes for the same parameters over $GF(q)$, where $q > n$. Recently, Huang et al. [12] generalized the lower bound on CO for any $z,\ z < t$. They constructed explicit CESS codes for any $z,\ z < t$, achieving the minimum CO and RO for $d = n$ over $GF(q),\ q > n(n-z)$. Moreover, they proved the achievability of the lower bound on CO and RO universally for all possible values of $d, t \leq d \leq n$ using random linear code constructions.

Contribution: In this paper, we introduce a new class of deterministic linear CESS codes, called *Staircase Codes*, which generalizes the construction in Example 1. We describe two explicit constructions of Staircase codes. The first construction achieves minimum CO and RO for any given d. The second is a universal construction that achieves minimum CO and RO simultaneously for all possible values of $d,\ t \leq d \leq n$. Staircase codes require a small finite field $GF(q)$ of size $q > n$, which is the same requirement for Reed Solomon based SS codes[2] [3].

Organization: The paper is organized as follows. In section II, we formulate the problem and introduce the notation. In section III, we describe the Staircase code construction for fixed d. Moreover, we give an example and prove that this construction achieves minimum CO and RO (Theorem 1). In section IV, we give the construction for universal Staircase codes (Theorem 2). We conclude in section V.

II. System Model

We consider the CESS problem and follow the majority of the notations in [12]. A secret $\mathbf{s}$ of size k units is formed of $k\alpha$ symbols (1 unit = α symbols). The secret symbols are drawn independently and uniformly at random from a finite alphabet, typically a finite field. A CESS code is a scheme that randomly encodes the secret into n shares $w_1, \ldots, w_n$ of unit size each, and distribute them to n distinct parties. A CESS code must satisfy the following properties:

1) *Perfect secrecy:* Any subset of z or less parties should not be able to obtain any information about the secret. Let $[n] = \{1, \ldots, n\}$, and for any subset $B \subseteq [n]$ denote by $\mathcal{W}_B$ the set of shares indexed by B, i.e., $\mathcal{W}_B = \{w_i; i \in B\}$. Then, the perfect secrecy condition can be expressed as
$$H(\mathbf{s} \mid \mathcal{W}_Z) = H(\mathbf{s}), \forall Z \subset [n] \text{ s.t. } |Z| = z. \quad (2)$$
2) *MDS:* A user downloading any t shares is able to recover the secret, i.e.,
$$H(\mathbf{s} \mid \mathcal{W}_A) = 0, \forall A \subseteq [n] \text{ s.t. } |A| = t. \quad (3)$$
Equations (2) and (3) imply that the secret can be of at most $t - z$ units (see [12, Proposition 1]). We will take the secret to be of maximum size, i.e., $k = t - z$ units.
3) *Minimum* CO *and* RO*:* a user contacting any d parties, $t \leq d \leq n$, is able to decode the secret by reading and downloading exactly $k + \mathrm{CO}(d)$ units of information in total from all the contacted shares, where
$$\mathrm{CO}(d) = \frac{kz}{d-z}. \quad (4)$$

Here, $H(.)$ denotes the entropy function. Equation (4) represents the achievable information theoretic lower bound [12, Theorem 1] on the communication overhead, $\mathrm{CO}(d)$, needed to satisfy the constraints in (2) and (3), when the user contacts d shares. Since the amount of information read cannot be less than the downloaded amount, the following lower bound on RO holds,
$$\mathrm{RO}(d) \geq \mathrm{CO}(d). \quad (5)$$

We will refer to a CESS code described above as an (n, k, z, d) CESS code, where the threshold is $t = k+z$. For instance, the code in Example 1 is an $(4, 1, 1, 3)$ CESS code. We will also be interested in universal (n, k, z) CESS code that achieves minimum $\mathrm{CO}(d)$ and $\mathrm{RO}(d)$ simultaneously for all possible values of d. Note that the MDS constraint is subsumed by the minimum CO and RO constraint since it corresponds to the case of $d = t$ and $\mathrm{CO}(t) = z$. However, we will make this distinction for clarity of exposition.

III. Staircase code construction for fixed d

A. Code construction

Theorem 1: The (n, k, z, d) Staircase CESS code construction defined below over $GF(q)$, $q > n$, satisfies the required MDS and perfect secrecy constraints given in (2) and (3), and achieves optimal communication and read overheads $\mathrm{CO}(d)$ and $\mathrm{RO}(d)$ given in (4) and (5) for any given $d,\ d \in \{k + z, \ldots, n\}$.

We describe the (n, k, z, d) Staircase code construction that achieves optimal communication and read overheads $\mathrm{CO}(d)$ and $\mathrm{RO}(d)$ for any given d, $k+z \leq d \leq n$. In this construction, we take $\alpha = d - z$. Hence, the secret $\mathbf{s}$ of size k units is formed of $k(d-z)$ symbols $s_1, \ldots, s_{k\alpha}$, where $s_i \in GF(q)$ and $q > n$. The symbols s_i are arranged in an $\alpha \times k$ matrix $\mathcal{S}$. The construction uses $z\alpha$ iid random keys drawn uniformly at random from $GF(q)$ and independently of the secret. The keys are partitioned into two matrices $\mathcal{K}_1$ and $\mathcal{K}_2$ of dimensions $z \times k$ and $z \times (\alpha - k)$, respectively. Let $\mathcal{D}$ be the transpose of the last $(\alpha - k)$ rows of the matrix $\begin{bmatrix} \mathcal{S} \\ \mathcal{K}_1 \end{bmatrix}$[3] and let $\mathbf{0}$ be the all zero square matrix of dimensions $(\alpha - k) \times (\alpha - k)$. Note that $\alpha - k \geq 0$ since $d \geq z + k$. The key ingredient of the

[1] Least common multiple.

[2] However, the proposed constructions require to divide the secret into a certain number of symbols α, which may not be necessary for SS codes.

[3] If $\alpha - k \leq z$, i.e., $d \leq 2z + k$, then $\mathcal{D}$ consists of the transpose of the last $\alpha - k$ rows of $\mathcal{K}_1$.

construction is to arrange the secret and the keys in the $d \times \alpha$ matrix M defined in Table II. The inspiration here is from the class of Product Matrix codes that minimizes the repair bandwidth in distributed storage systems [14].

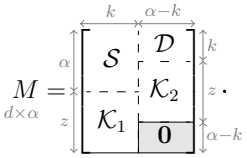

TABLE II
THE STRUCTURE OF THE MATRIX M THAT CONTAINS THE SECRET AND KEYS IN THE STAIRCASE CODE CONSTRUCTION FOR FIXED d.

Encoding: Let V be an $n \times d$ Vandermonde matrix over $GF(q)$. The matrix M is multiplied by V to obtain the matrix $C = VM$. The n rows of C form the n different shares, i.e., $w_i = v_i M, i = 1, \ldots, n$, where v_i is the i^{th} row of V.
Decoding: A user contacting any $t = k + z$ parties downloads all the contacted shares. A user contacting d parties, indexed by $I \subseteq [n]$, downloads the first k symbols from each contacted party corresponding to $v_i \begin{bmatrix} \mathcal{S} & \mathcal{K}_1 \end{bmatrix}^t, i \in I$ (the superscript t denotes the transpose of a matrix). Theorem 1 guaranties that the user will be able to decode the secret in both cases.

B. Example

We give the details of the construction of the $(n, k, z, d) = (4, 1, 1, 3)$ CESS code of Example 1. We take $\alpha = d - z = 2$, thus the secret $\mathbf{s}$ is formed of $k\alpha = 2$ symbols s_1, s_2 over $GF(q)$, $q = 5 > n = 4$. The construction uses $z\alpha = 2$ iid random keys $k_1,\ k_2$ drawn uniformly at random over $GF(5)$ and independently of the secret. The keys are partitioned into two matrices $\mathcal{K}_1$ and $\mathcal{K}_2$ of dimensions $z \times k = 1 \times 1$ and $z \times (\alpha - k) = 1 \times 1$, respectively. The matrix $\mathcal{D}$ is the transpose of the last $\alpha - k = 1$ row of $\mathcal{K}_1$. Hence, we have, $\mathcal{K}_1 = \mathcal{D} = k_1, \mathcal{K}_2 = k_2$, and $\mathcal{S} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$. The secret and the keys are arranged in an $d \times \alpha = 4 \times 2$ matrix M. Let V be an $n \times d = 4 \times 3$ Vandermonde matrix. M and V are given again in (6).

$$M = \begin{bmatrix} s_1 & k_1 \\ s_2 & k_2 \\ k_1 & 0 \end{bmatrix} \text{ and } V = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 4 \\ 1 & 4 & 1 \end{bmatrix}. \tag{6}$$

The shares are the rows of the matrix $C = VM$ as given in Table I. We want to check that this code satisfies the following properties.
1) Minimum CO *and* RO *for* $d = 3$*:* We check that a user contacting $d = 3$ parties can reconstruct the secret with minimum CO and RO. For instance, if a user contacts the first 3 parties and downloads the first symbol of each contacted share, then the downloaded data is given by, $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 4 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ k_1 \end{bmatrix}$. The matrix on the left is a 3×3 square Vandermonde matrix, hence invertible. Therefore, the user can decode the secret (and k_1). This remains true irrespective of which 3 parties are contacted. The user reads and downloads 3 symbols of size $3/\alpha = 3/2$ units resulting in minimum overheads, $\mathrm{CO}(3) = \mathrm{RO}(3) = 3/2 - k = 1/2$, as given in (4) and (5).

2) MDS: We check that a user contacting $t = k + z = 2$ parties can reconstruct the secret. Suppose the user contacts parties 1 and 2 and downloads all their shares given by $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} s_1 & k_1 \\ s_2 & k_2 \\ k_1 & 0 \end{bmatrix}$. This system is equivalent to the two following systems $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ k_1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \end{bmatrix}$. The decoder uses the latter system to decode k_1 and k_2. This is possible because the matrix on the left is a square Vandermonde matrix, hence invertible. Then, the decoder subtracts the obtained value of k_1 from the former system to obtain again the following invertible system $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$. The decoder then decodes s_1 and s_2. Again, this procedure is possible for any 2 contacted parties .
3) Perfect secrecy: At a high level, perfect secrecy is achieved here because each symbol in a share is "padded" with at least one distinct key statistically independent of the secret, making the shares of any party independent of the secret.

C. Proof of Theorem 1

Consider the (n, k, z, d) Staircase code defined above. We prove Theorem 1 by establishing the following properties:
1) Minimum $\mathrm{CO}(d)$ *and* $\mathrm{RO}(d)$*:* We prove that a user contacting any d parties can reconstruct the secret while incurring minimum CO and RO. A user contacting any d parties downloads the first k symbols of each party. Let $I \subset [n],\ |I| = d$, be the set of indices of the contacted parties, then the downloaded data is given by $V_I \begin{bmatrix} \mathcal{S} & \mathcal{K}_1 \end{bmatrix}^t$, where V_I is a $d \times d$ square Vandermonde matrix formed of the rows of V indexed by I, hence invertible. The user can always decode the secret (and the keys in $\mathcal{K}_1$) by inverting V_I. The code is optimal on communication and read overheads $\mathrm{CO}(d)$ and $\mathrm{RO}(d)$, because the user only reads and downloads kd symbols of size $kd/\alpha = kd/(d - z)$ units resulting in an overhead of $kd/\alpha - k = kz/\alpha = kz/(d - z)$ achieving the optimal $\mathrm{CO}(d)$ and $\mathrm{RO}(d)$ given in (4) and (5).

2) MDS property: We prove that a user contacting any $t = k + z$ parties and downloading all their shares can reconstruct the secret. Let $I \subset [n], |I| = t$, be the set of indices of the contacted parties. The information downloaded by the user is $V_I M$ and is given by $V_I \begin{bmatrix} \mathcal{S} & \mathcal{D} \\ \mathcal{K}_1 & \mathcal{K}_2 \\ & \mathbf{0} \end{bmatrix}$. First, we show that the user can decode the entries of $\mathcal{D}$ and $\mathcal{K}_2$. The decoder considers the system $V_I \begin{bmatrix} \mathcal{D} & \mathcal{K}_2 & \mathbf{0} \end{bmatrix}^t = V_I' \begin{bmatrix} \mathcal{D} & \mathcal{K}_2 \end{bmatrix}^t$. Recall that the dimensions of the all zero sub-matrix in $\begin{bmatrix} \mathcal{D} & \mathcal{K}_2 & \mathbf{0} \end{bmatrix}^t$ are $(\alpha - k) \times (\alpha - k)$. Then, V_I' is a $(k + z) \times (k + z)$ square Vandermonde matrix formed by the first $(k + z)$ columns of V_I. Therefore, the user can always decode the entries of $\mathcal{D}$ and $\mathcal{K}_2$ because V_I' is invertible. Second, we prove that the user can always decode the entries of $\mathcal{S}$ and hence reconstruct the

secret. Recall that $\mathcal{D}$ is the transpose of the last $\alpha - k$ rows of $M_1 \triangleq \begin{bmatrix}\mathcal{S} & \mathcal{K}_1\end{bmatrix}^t$. By subtracting the previously decoded entries of $\mathcal{D}$ from $V_I \begin{bmatrix}\mathcal{S} & \mathcal{K}_1\end{bmatrix}^t$, the user obtains $V_I' M_1'$, where V_I' is defined above and M_1' is a $(k+z) \times k$ matrix formed by the first $k+z$ rows of M_1. Therefore, the user can always decode the entries of M_1' because V_I' is invertible. If $k + z \geq \alpha$, then $\mathcal{S}$ is directly obtained since it is contained in M_1'. Otherwise, M_1' consists of the first $k+z$ rows of $\mathcal{S}$. The remaining rows of $\mathcal{S}$ are contained in $\mathcal{D}$ and were previously decoded. In both cases, the user can decode all the secret symbols $s_1, \ldots, s_{k\alpha}$.

3) Perfect secrecy: We prove that for any subset $Z \subset [n]$, $|Z| = z$, the collection of shares $\mathcal{W}_Z$ indexed by Z does not reveal any information about the secret as given in equation (2), i.e., $H(\mathbf{s} \mid \mathcal{W}_z) = H(\mathbf{s})$. To that end, it suffices to prove that $H(\mathcal{K}_1, \mathcal{K}_2 \mid \mathcal{W}_Z, \mathbf{s}) = 0$ [15]. Therefore, we need to show that given the secret $\mathbf{s}$ as side information, any collection $\mathcal{W}_Z$ of z shares can decode all the random keys. A collection of $\mathcal{W}_Z$ shares can be written as $V_Z \begin{bmatrix}\mathcal{S} & \mathcal{D} \\ \mathcal{K}_1 & \mathcal{K}_2 \\ & \mathbf{0}\end{bmatrix}$, where V_Z is a $z \times d$ matrix corresponding to the rows of V indexed by Z. This linear system can be divided into two systems as follows,

$$V_Z \begin{bmatrix}\mathcal{S} & \mathcal{K}_1\end{bmatrix}^t, \tag{7}$$

$$V_Z \begin{bmatrix}\mathcal{D} & \mathcal{K}_2 & \mathbf{0}\end{bmatrix}^t. \tag{8}$$

Given the secret as side information, it can be subtracted from (7), which becomes $V_Z \begin{bmatrix}\mathbf{0} & \mathcal{K}_1\end{bmatrix}^t = V_Z'' \mathcal{K}_1$, where V_Z'' is a $z \times z$ square Vandermonde matrix consisting of the last z columns of V_Z. The entries of $\mathcal{K}_1$ can always be decoded because V_Z'' is invertible. Now that $\mathcal{K}_1$ is decoded and we have $\mathcal{S}$ as side information, we can obtain $\mathcal{D}$ as the last $\alpha - k$ rows of $\begin{bmatrix}\mathcal{S} & \mathcal{K}_1\end{bmatrix}^t$. Then, the entries of $\mathcal{D}$ are subtracted from the second system to obtain $V_Z^* \mathcal{K}_2$, where V_Z^* is a $z \times z$ square Vandermonde matrix consisting of the $(k+1)^{th}$ to the $(k+z)^{th}$ columns of V_Z. Hence, the entries of $\mathcal{K}_2$ can always be decoded because V_Z^* is invertible. Therefore, $H(\mathcal{K}_1, \mathcal{K}_2 \mid \mathcal{W}_Z, \mathbf{s}) = 0$, $\forall\ Z,\ Z \subset [n],\ |Z| = z$ and perfect secrecy is achieved.

IV. Universal Staircase code construction

A. Universal Code construction

Theorem 2: The (n, k, z) Staircase CESS code construction defined below over $GF(q)$, $q > n$, satisfies the required MDS and perfect secrecy constraints given in (2) and (3), and achieves optimal communication and read overheads $\mathrm{CO}(d)$ and $\mathrm{RO}(d)$ given in (4) and (5) simultaneously for all d, $k + z \leq d \leq n$.

The proof of Theorem 2 is omitted and can be found in [15].

We describe the (n, k, z) Staircase code construction mentioned in Theorem 2, which achieves optimal communication and read overheads $\mathrm{CO}(d)$ and $\mathrm{RO}(d)$ simultaneously for all possible values of d, i.e., $k + z \leq d \leq n$. Let $d_1 = n, d_2 = n-1, \ldots, d_h = k+z$, with $h = n - k - z + 1$, and $\alpha_i = d_i - z,\ i = 1, \ldots, h$. Choose $\alpha = LCM(\alpha_1, \alpha_2, \ldots, \alpha_{h-1})$, that is the least common multiple of all the α_i's except for the last $\alpha_h = k$. The secret $\mathbf{s}$ consists of $k\alpha$ symbols $s_1, \ldots, s_{k\alpha}$ over $GF(q),\ q > n$, arranged in an $\alpha_1 \times k\alpha/\alpha_1$ matrix $\mathcal{S}$. The construction uses $z\alpha$ iid random keys, drawn uniformly at random from $GF(q)$ and independently of the secret. The keys are partitioned into h matrices $\mathcal{K}_i, i = 1, \ldots, h$, of respective dimensions $z \times k\alpha/\alpha_i\alpha_{i-1}$ (take $\alpha_0 = 1$). The matrix $\begin{bmatrix}\mathcal{K}_1 & \cdots & \mathcal{K}_i\end{bmatrix}$ consists of the overhead of keys decoded by a user contacting d_i parties. We form h matrices M_i, $i = 1, \ldots, h$, as follows,

$$M_1 = \underset{k\alpha/\alpha_1}{\overset{n}{\left[\begin{matrix}\mathcal{S} \\ \mathcal{K}_1\end{matrix}\right]}} \begin{matrix}\alpha_1 \\ z\end{matrix} \text{ and } M_i = \underset{k\alpha/\alpha_{i-1}\alpha_i}{\overset{n}{\left[\begin{matrix}\mathcal{D}_{i-1} \\ \mathcal{K}_i \\ \mathbf{0}\end{matrix}\right]}} \begin{matrix}\alpha_i \\ z \\ n-d_i\end{matrix} \quad i \neq 1, \tag{9}$$

where, $\mathcal{D}_j$ is formed of the $(n-j+1)^{th}$ row of $\begin{bmatrix}M_1 & M_2 & \cdots & M_j\end{bmatrix}$ wrapped around to make a matrix of dimensions $\alpha_{j+1} \times k\alpha/\alpha_j\alpha_{j+1}$ for $j = 1, \ldots, h-1$. The $\mathbf{0}$'s are the all zero matrices used to complete the M_i's to n rows. The secret and the keys are arranged in the matrix $M = \begin{bmatrix}M_1 & \cdots & M_t\end{bmatrix}$ defined in Table III.

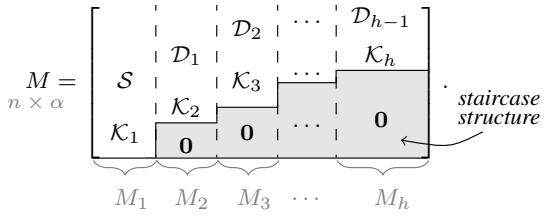

TABLE III
THE STRUCTURE OF THE MATRIX M THAT CONTAINS THE SECRET AND KEYS IN THE UNIVERSAL STAIRCASE CODE CONSTRUCTION.

The matrix M is characterized by a special structure resulting from carefully choosing the entries of the $\mathcal{D}_j$'s and placing the all zero sub-blocks in a staircase shape, giving these codes their name. This staircase shape allows to achieve optimal communication and read overheads CO and RO for all possible d.

Encoding: The encoding is similar to the first Staircase code construction. The matrix M is multiplied by an $n \times n$ Vandermonde matrix over $GF(q)$ to obtain the matrix $C = VM$. The n rows of C form the n different shares.

Decoding: To reconstruct the secret, a user contacting any d_j parties indexed by $I \subseteq [n]$ downloads the first $k\alpha/\alpha_j$ symbols from each contacted party corresponding to $v_i \begin{bmatrix}M_1 & \cdots & M_j\end{bmatrix}$, for all $i \in I$.

B. Example of Universal Staircase code

We describe here the construction of an $(n, k, z) = (4, 1, 1)$ universal Staircase code over $GF(q),\ q = 5 > n = 4$, by following the construction in Section IV. This example is explained in more details in [15]. We have $d_1 = 4,\ d_2 = 3,\ d_3 = 2$ and $\alpha_1 = 3,\ \alpha_2 = 2,\ \alpha_3 = 1$ and $\alpha = LCM(\alpha_1, \alpha_2) = LCM(3, 2) = 6$. The secret $\mathbf{s}$ is formed of $k\alpha = 6$ symbols over $GF(5)$. The construction uses $z\alpha = 6$ iid random keys drawn uniformly at random from $GF(5)$ and independently of the secret. The secret symbols

and the random keys are arranged in the following matrices, $\mathcal{S} = \begin{bmatrix} s_1 & s_4 \\ s_2 & s_5 \\ s_3 & s_6 \end{bmatrix}$, $\mathcal{K}_1 = \begin{bmatrix} k_1 & k_2 \end{bmatrix}$, $\mathcal{K}_2 = \begin{bmatrix} k_3 \end{bmatrix}$, and $\mathcal{K}_3 = \begin{bmatrix} k_4 & k_5 & k_6 \end{bmatrix}$. To build the matrix M which will be used for encoding the secret, we start with $M_1 = \begin{bmatrix} s_1 & s_2 & s_3 & k_1 \\ s_4 & s_5 & s_6 & k_2 \end{bmatrix}^t$. Then, $\mathcal{D}_1$ is the $\alpha_2 \times k\alpha/\alpha_1\alpha_2 = 2\times 1$ matrix that contains the symbols of the n^{th} row of M_1, i.e., $\mathcal{D}_1 = \begin{bmatrix} k_1 & k_2 \end{bmatrix}^t$. Therefore, $M_2 = \begin{bmatrix} \mathcal{D}_1 & \mathcal{K}_2 & \mathbf{0} \end{bmatrix}^t = \begin{bmatrix} k_1 & k_2 & k_3 & 0 \end{bmatrix}^t$. Similarly, we have $\mathcal{D}_2 = \begin{bmatrix} s_3 & s_6 & k_3 \end{bmatrix}$ and $M_3 = \begin{bmatrix} s_3 & s_6 & k_3 \\ k_4 & k_5 & k_6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$. We obtain M by concatenating M_1, M_2 and M_3,

$$M = \underbrace{\left[\begin{array}{cccccc} s_1 & s_4 & k_1 & s_3 & s_6 & k_3 \\ s_2 & s_5 & k_2 & k_4 & k_5 & k_6 \\ s_3 & s_6 & k_3 & 0 & 0 & 0 \\ k_1 & k_2 & 0 & 0 & 0 & 0 \end{array}\right]}_{M_1 \quad M_2 \quad M_3}. \tag{10}$$

Here, V is the $n\times n = 4\times 4$ Vandermonde matrix over $GF(5)$ given in (11). The shares are given by the rows of the matrix $C = VM$ and shown in Table IV.

$$V = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 3 & 4 & 2 \\ 1 & 4 & 1 & 4 \end{bmatrix}. \tag{11}$$

Party 1	Party 2
$s_1 + s_2 + s_3 + k_1$	$s_1 + 2s_2 + 4s_3 + 3k_1$
$s_4 + s_5 + s_6 + k_2$	$s_4 + 2s_5 + 4s_6 + 3k_2$
$k_1 + k_2 + k_3$	$k_1 + 2k_2 + 4k_3$
$s_3 + k_4$	$s_3 + 2k_4$
$s_6 + k_5$	$s_6 + 2k_5$
$k_3 + k_6$	$k_3 + 2k_6$

Party 3	Party 4
$s_1 + 3s_2 + 4s_3 + 2k_1$	$s_1 + 4s_2 + s_3 + 4k_1$
$s_4 + 3s_5 + 4s_6 + 2k_2$	$s_4 + 4s_5 + s_6 + 4k_2$
$k_1 + 3k_2 + 4k_3$	$k_1 + 4k_2 + k_3$
$s_3 + 3k_4$	$s_3 + 4k_4$
$s_6 + 3k_5$	$s_6 + 4k_5$
$k_3 + 3k_6$	$k_3 + 4k_6$

TABLE IV
AN EXAMPLE OF A UNIVERSAL STAIRCASE CODE FOR $(n, k, z) = (4, 1, 1)$ OVER $GF(5)$.

The decoding rules for each d follow the general rules described in the previous section. We check that this code achieves minimum CO and RO simultaneously for $d_2 = 3$ and $d_1 = 4$. Suppose a user contacts $d_2 = 3$ parties indexed by $I \subset [n]$. The user reads and downloads the first $k\alpha/\alpha_2 = 3$ symbols of each contacted share corresponding to $V_I \begin{bmatrix} M_1 & M_2 \end{bmatrix}$ (in black and red), where V_I is the matrix formed by the rows of V indexed by I. The user will be able to reconstruct the secret. The resulting CO and RO are equal to $3/2 - k = 1/2$ units achieving the optimal $\mathrm{CO}(d_2)$ and $\mathrm{RO}(d_2)$ given in (4) and (5). In the case when a user contacts $d_1 = 4$ parties, the user reads and downloads the first $k\alpha/\alpha_1 = 2$ symbols of each contacted share corresponding to $V_I M_1$ (in black). The user can always decode the secret because V_I here is a 4×4 square Vandermonde matrix, hence invertible. The resulting CO and RO are equal to $1/3$ achieving the optimal $\mathrm{CO}(d_1)$ and $\mathrm{RO}(d_1)$ given in (4) and (5).

V. CONCLUSION

We considered the communication efficient secret sharing (CESS) problem. The goal is to minimize the communication and read overheads for a user interested in decoding the secret. To that end, we introduced a new class of deterministic linear CESS codes, called *Staircase Codes*. We described two explicit constructions of Staircase codes. The first construction achieves minimum overheads for any given number d of parties contacted by the user. The second is a universal construction that achieves minimum overheads simultaneously for all possible values of d. The introduced codes require a small finite field $GF(q)$ of size $q > n$, which is the same requirement for Reed Solomon based SS codes.

REFERENCES

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proceedings of the National Computer Conference*, vol. 48, pp. 313–317, 1979.

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

[4] H.-Y. Chien, J. Jinn-Ke, and Y.-M. Tseng, "A practical (t, n) multi-secret sharing scheme," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 83, no. 12, pp. 2762–2765, 2000.

[5] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Transactions on Information Theory*, vol. 29, no. 1, pp. 35–41, 1983.

[6] C.-P. Lai and C. Ding, "Several generalizations of Shamir's secret sharing scheme," *International Journal of Foundations of Computer Science*, vol. 15, no. 02, pp. 445–458, 2004.

[7] C.-C. Yang, T.-Y. Chang, and M.-S. Hwang, "A (t,n) multi-secret sharing scheme," *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483–490, 2004.

[8] C. Padró, "Lecture notes in secret sharing," *IACR Cryptology ePrint Archive*, vol. 2012, p. 674, 2012.

[9] E. F. Brickell, "Some ideal secret sharing schemes," in *Advances in Cryptology–EUROCRYPT'89*, pp. 468–475, 1990.

[10] R. Cramer, I. B. Damgård, and J. B. Nielsen, *Secure Multiparty Computation and Secret Sharing*. Cambridge, England: Cambridge University Press, 2015.

[11] H. Wang and D. S. Wong, "On secret reconstruction in secret sharing schemes," *IEEE Transactions on Information Theory*, vol. 54, pp. 473–480, Jan 2008.

[12] W. Huang, M. Langberg, J. Kliewer, and J. Bruck, "Communication efficient secret sharing," *arXiv preprint arXiv:1505.07515*, 2015.

[13] Z. Zhang, Y. M. Chee, S. Ling, M. Liu, and H. Wang, "Threshold changeable secret sharing schemes revisited," *Theoretical Computer Science*, vol. 418, pp. 106–115, 2012.

[14] K. V. Rashmi, N. B. Shah, and P. V. Kumar, "Optimal exact-regenerating codes for distributed storage at the MSR and MBR points via a product-matrix construction," *IEEE Transactions on Information Theory*, vol. 57, no. 8, pp. 5227–5239, 2011.

[15] R. Bitar and S. El Rouayheb, "Staircase codes for secret sharing with optimal communication and read overheads," *arXiv preprint arXiv:1512.02990*, 2015.