Staircase Codes for Secret Sharing with Optimal Communication and Read Overheads

Rawad Bitar, *Student Member, IEEE* and Salim El Rouayheb, *Member, IEEE*

Abstract—We study the communication efficient secret sharing (CESS) problem. A classical threshold secret sharing scheme 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, $z < t < n$, colluding parties cannot obtain any information about the secret. A CESS scheme satisfies the previous properties of threshold secret sharing. Moreover, it allows to reconstruct the secret from any set of $d \geq t$, parties by reading and communicating the minimum amount of information. In this paper, we introduce three explicit constructions of CESS codes called *Staircase codes*. The first construction achieves optimal communication and read costs for a given d. The second construction achieves optimal costs universally for all possible values of d between t and n. The third construction, which is the most general, achieves optimal costs universally for all values of d in any given set $\Delta \subseteq \{t, \dots, n\}$. The introduced Staircase codes can store a secret of maximal size, i.e., equal to $t - z$ shares, and they are all designed over a small finite field $GF(q)$, for any prime power $q > n$. However, Staircase codes may require to divide the secret and the shares into many symbols. We also describe how Staircase codes can be used to construct threshold changeable secret sharing with minimum storage cost, i.e., minimum share size.

I. INTRODUCTION

Consider the threshold secret sharing (SS) problem [2], [3] in which a dealer encodes a secret using random keys into n shares and distributes them to n parties. The threshold SS allows a legitimate user contacting any set of at least t, $t < n$, parties to reconstruct the secret by downloading their shares. In addition, the scheme ensures that any set of at most z, $z < t < n$, colluding parties cannot obtain any information, in an information theoretic sense, about the secret. The following example illustrates the construction of a threshold SS on $n = 4$ shares.

Example 1 (Threshold SS). *Let $n = 4, t = 2$ and $z = 1$ and let s be a secret uniformly distributed over $GF(5)$. Then, the following 4 shares $(s+r, s+2r, s+3r, s+4r)$ form a threshold SS scheme, with r being a random symbol, called key, chosen uniformly at random from $GF(5)$ and independently of s. A user can decode the secret by contacting any $t = 2$ parties, downloading their shares and decoding s and r. Secrecy is ensured, 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., [2]–[8]. The literature on secret sharing predominantly studies non-threshold secret sharing schemes, with so-called general access structures, e.g., [9]–[11]. We refer the interested reader to the following survey works [12]–[14] 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 achieves minimum communication and read overheads when the user

Party 1	Party 2	Party 3	Party 4
$s_1 + s_2 + r_1$	$s_1 + 2s_2 + 4r_1$	$s_1 + 3s_2 + 4r_1$	$s_1 + 4s_2 + r_1$
$r_1 + r_2$	$r_1 + 2r_2$	$r_1 + 3r_2$	$r_1 + 4r_2$

TABLE I: An example of a CESS code based on the Staircase code construction over $GF(5)$ for $n = 4$ parties, threshold $t = 2$, $z = 1$ colluding parties and any $d = 3$ parties can efficiently reconstruct the secret. A user contacting any $t = 2$ parties downloads all their shares, i.e., 4 symbols in total, in order to decode the secret. The resulting overheads are CO = RO = 2 symbols. However, a user contacting any $d = 3$ parties decodes the secret by downloading the first symbol (in blue) of each share, i.e., 3 symbols in total. Hence, CO = RO = 1 symbol. For instance, a user contacting parties $1, 2$ and 3 downloads $s_1 + s_2 + r_1$, $s_1 + 2s_2 + 4r_1$, and $s_1 + 3s_2 + 4r_1$ and can decode the secret and r_1. Notice that a user contacting $d = 3$ parties can only decode r_1, whereas a user contacting $t = 2$ parties has to decode r_1 and r_2.

contacts d parties for any $t \leq d \leq n$. The communication overhead (CO) is defined as the extra amount of information (beyond the secret size) downloaded by a user contacting d parties in order to decode the secret. The read overhead RO is defined similarly. Next, we give an example of a CESS code that minimizes CO and RO. The CESS code in this example belongs to the family of Staircase codes which we introduce in Section III-A.

Example 2. *Consider again the SS problem of Example 1 with $n = 4$, $t = 2$, $z = 1$. We assume now that the secret $\mathbf{s}$ is formed of 2 symbols s_1, s_2 uniformly distributed over $GF(5)$ and we use two keys r_1, r_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[1] code shown in Table I.*

$$C = VM = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 4 \\ 1 & 4 & 1 \end{bmatrix} \underbrace{\begin{bmatrix} s_1 & r_1 \\ s_2 & r_2 \\ r_1 & 0 \end{bmatrix}}_{M}. \quad (1)$$

The CESS scheme enjoys the following properties. First, a user decodes the secret either by

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

contacting any $t = 2$ parties and downloading all their shares, i.e., 4 symbols, or by contacting any $d = 3$ parties and downloading the first symbol (in blue) of each share, i.e., 3 symbols in total. 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 only the key r_1, whereas when $d = t = 2$, the user has to decode the secret and both of the keys. This code actually 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). Second, secrecy is achieved because the secret s_1, s_2 is padded by random keys r_1, r_2 and each $z = 1$ party cannot obtain any information about s_1 and s_2.

Related work: The CESS problem was introduced by Wang and Wong in [15] where they focused on perfect CESS, i.e., the case in which $z = t - 1 < n - 1$. The authors showed that there exists a tradeoff between the number of contacted parties d and the amount of information downloaded by a user in order to decode the secret. They derived a lower bound on CO and constructed codes for the special case of $z = t - 1$ using polynomial evaluation over $GF(q)$, where $q > n + v$, that achieve minimum CO and RO universally for all $t \leq d \leq t + v - 1$, for some positive integer v. Zhang et al. [16] constructed CESS codes for the special case of $z = t - 1$ over $GF(q)$, where $q > n$, that achieve minimum CO and RO for any given $t \leq d \leq n$. Recently, Huang et al. [17] studied the CESS problem for all values of

z, i.e., $z < t < n$, and generalized the lower bound on CO. The authors constructed explicit CESS codes for any z 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 $t \leq d \leq n$ using random linear code constructions[2]. In our setting, we assume that the dealer has direct access to all the parties. In the case where the dealer can access the parties through a network, Shah et al. [21] studied the problem of minimizing the communication cost of securely delivering the shares to the parties.

Contributions: In this paper, we introduce three new classes of explicit constructions of linear CESS codes that achieve minimum CO and RO. More specifically, we make the following contributions:

1) We describe the *Staircase code* construction that achieves minimum CO and RO for any given $t \leq d \leq n$. This construction generalizes the construction in Example 2.

2) We describe the *Universal Staircase code* construction that achieves minimum CO and RO simultaneously for all values of $t \leq d \leq n$.

3) We generalize the previous two constructions into the Δ-*Universal Staircase code* construction, which achieves minimum CO and RO simultaneously for all possible values of $d \in \Delta$, for any given set $\Delta \subseteq \{t, \ldots, n\}$.

Moreover, we construct a class of secret sharing codes, called threshold changeable secret sharing (TCSS) codes [22], based on the introduced Staircase codes. In all the previous constructions, the threshold t satisfies $t < n$ and the parameter z that represents the number of colluding parties can take any value between 0 and $t - 1$.

The Staircase codes and the resulting TCSS codes can store a secret of maximal size, i.e., equal to $t - z$ shares, and require a small finite field $GF(q)$ of size $q > n$, which is the same requirement for Reed Solomon based SS codes [4]. However,

unlike SS codes, these codes require to divide the secret and the shares into α symbols (α defined later).

Organization: The paper is organized as follows. In Section II, we formulate the CESS problem, introduce the necessary notations and summarize our results. We describe the Staircase code and Universal Staircase code constructions in Section III. In Section IV, we prove that the Staircase codes achieve secrecy and minimum CO and RO. In Section V, we prove that the Universal Staircase codes achieve secrecy and minimum CO and RO. We describe the most general Δ-Universal Staircase code construction in Section VI. In Section VII we show how to use the Staircase codes to construct threshold changeable secret sharing. We conclude in Section VIII.

II. PROBLEM FORMULATION AND MAIN RESULTS

We consider the CESS problem and follow the majority of the notations in [17]. 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 encodes the secret, using random keys, into n shares $w_1, \ldots, w_n$, of unit size each, and distributes them to n distinct parties. Let W_i denote the random variable representing the share of party i, let S denote the random variable representing the secret $\mathbf{s}$, let $[n] = \{1, \ldots, n\}$, and for any subset $B \subseteq [n]$ denote by W_B the set of random variables representing the shares indexed by B, i.e., $W_B = \{W_i; i \in B\}$. Then, a CESS code must satisfy the following properties:

1) *Perfect secrecy:* Any subset of z or less parties should not be able to get any information about the secret. The perfect secrecy condition can be expressed as

$$H(\mathrm{S} \mid \mathrm{W}_Z) = H(\mathrm{S}), \ \forall Z \subset [n] \ \text{s.t.} \ |Z| = z. \tag{2}$$

2) *MDS:* A user downloading t shares is able to recover the secret, i.e.,

$$H(\mathrm{S} \mid \mathrm{W}_A) = 0, \ \forall A \subseteq [n] \ \text{s.t.} \ |A| = t, \tag{3}$$

---

[2]After the appearance of the original version of this work on Arxiv [18], an equivalent CESS code construction for all parameters was given concurrently in [19] and [20].

and the secret is of maximal size $k = t - z$ units as implied by (2) and (3) (see [17, Proposition 1]).

3) *Minimum* CO *and* RO: a user contacting d parties, $t \leq d \leq n$, is able to decode the secret by reading and downloading exactly $k + CO(d)$ units of information in total from all the contacted shares, where

$$\text{CO}(d) = \frac{kz}{d - z}. \tag{4}$$

Equation (4) represents the achievable information theoretic lower bound [15, Theorem 3.1], [17, Theorem 1] on the communication overhead, CO(d), needed to satisfy the constraints in (2) and (3), when the user contacts d parties[3]. Since the amount of information read cannot be less than the downloaded amount, the following lower bound on RO holds,

$$\text{RO}(d) \geq \text{CO}(d). \tag{5}$$

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 2 is an $(4, 1, 1, 3)$ CESS code. We define a universal (n, k, z) CESS code that achieves minimum CO(d) and RO(d) simultaneously for all possible values of d. Note that the MDS constraint can be omitted since it is subsumed by the minimum CO and RO constraint since it corresponds to the case of $d = t$ and CO$(t) = z$. However, we will make this distinction for clarity of exposition. In the sequel whenever referring to t, $t < n$ should be understood and whenever referring to z, $z < t < n$ should be understood. Also, whenever referring to d, $k + z \leq d \leq n$ should be understood unless otherwise stated.

Given the model described above, we are ready to state our main results. We introduce the first class of Staircase codes that satisfy minimum CO and RO for any given d.

Theorem 1. *The (n, k, z, d) Staircase CESS code defined in Section III-A over $GF(q)$, $q > n$, satisfies the required MDS and perfect secrecy*

constraints given in (2) *and* (3) *for any given* $z < t < n$, *and achieves optimal communication and read overheads* CO(d) *and* RO(d) *given in* (4) *and* (5) *for any given* $k + z \leq d \leq n$.

Our next result introduces the Universal Staircase codes which achieve optimal overheads simultaneously for all possible values of d.

Theorem 2. *The (n, k, z) Universal Staircase CESS code defined in Section III-B over $GF(q)$, $q > n$, satisfies the required MDS and perfect secrecy constraints given in* (2) *and* (3) *for any given* $z < t < n$, *and achieves optimal communication and read overheads* CO(d) *and* RO(d) *given in* (4) *and* (5) *simultaneously for all* $k + z \leq d \leq n$.

Theorem 3 generalizes the first two constructions.

Theorem 3. *Let* $\Delta \subseteq \{k + z, \ldots, n\}$. *The (n, k, z, Δ) Δ-universal Staircase codes defined in Section VI over $GF(q)$, $q > n$, satisfies the required MDS and perfect secrecy constraints given in* (2) *and* (3) *for any given* $z < t < n$, *and achieves optimal communication overhead* CO(d) *and read overhead* RO(d) *given in* (4) *and* (5) *simultaneously for all* $d \in \Delta$.

All Staircase codes constructions require dividing the shares into α symbols (therefore dividing the secret into $k\alpha$ symbols) as defined in Sections III and VI. No lower bounds on α are currently known for a given field size q.

We note that codes achieving minimum CO and RO for all possible values of d were presented in [19] and [20] concurrently with the original version of this work [18]. As explained in [20], the Staircase code constructions and the construction in [20] are equivalent. The equivalence between the two constructions is similar to the equivalence between the construction of threshold SS codes based on linear block codes and the one based on polynomial evaluations[4]. Staircase codes presented here is a linear block code construction based on Vandermonde matrices, whereas the construction presented in [20] is based on polynomial evaluations.

---

[3]Note that a user contacting d parties and achieving (4) for a threshold secret sharing with threshold t downloads the same amount of information as a user contacting d parties in a threshold secret sharing with threshold d.

[4]This is also similar to constructing Reed Solomon codes either based on polynomial evaluations, or based on linear block codes with a Vandermonde generator matrix.

III. STAIRCASE CODE CONSTRUCTIONS

A. Staircase code construction for given d

We describe the (n, k, z, d) Staircase code construction that achieves optimal communication and read overheads $\mathtt{CO}(d)$ and $\mathtt{RO}(d)$ for any given $k + z \leq d \leq n$. In this construction, we take $\alpha = d - z$. Hence, the secret $\mathbf{s}$ of size k units is formed of $k(d - z)$ symbols $s_1, \dots, s_{k\alpha}$, 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 $\mathcal{R}_1$ and $\mathcal{R}_2$ 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 $\begin{bmatrix} \mathcal{S} \\ \mathcal{R}_1 \end{bmatrix}$[5] 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 construction is to arrange the secret and the keys in a $d \times \alpha$ matrix M defined in Table II. The inspiration behind this construction is the class of Product Matrix codes that minimizes the repair bandwidth in distributed storage systems[6] [24].
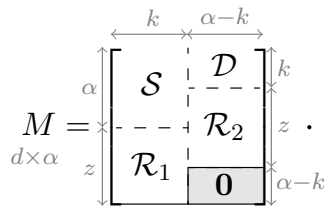

TABLE II: The structure of the matrix M that contains the secret and keys in the Staircase code construction for given d.

Encoding: Let V be an $n \times d$ Vandermonde[7] matrix defined over $GF(q)$. The matrix M, defined in Table II, is multiplied by V to obtain the matrix

[5]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 $\mathcal{R}_1$.

[6]After the appearance of the original version of this work on Arxiv [18], a connection between the family of regenerating codes and CESS codes was explored in more details in [23].

[7]We require all square sub-matrices formed by consecutive columns of V to be invertible. Vandermonde and Cauchy matrices satisfy this property.

$C = VM$. The n rows of C form the n different shares.

Decoding: A user contacting $t = k + z$ parties downloads all the shares of the contacted parties. A user contacting d parties, indexed by $I \subseteq [n]$, downloads the first k symbols from each contacted party corresponding to $v_i \begin{bmatrix} \mathcal{S} & \mathcal{R}_1 \end{bmatrix}^T, i \in I$, where v_i denotes the ith row of the Vandermonde matrix V (the superscript T denotes the transpose of a matrix). The decoding procedure given in the proof of Theorem 1 guarantees that the user will be able to decode the secret in both cases.

Example 2 (Continued). *We give the details of the construction of the $(n, k, z, d) = (4, 1, 1, 3)$ CESS code of Example 2. We take $\alpha = d - z = 2$, thus the secret $\mathbf{s}$ is formed of $k\alpha = 2$ symbols s_1, s_2 uniformly distributed over $GF(q)$, $q = 5 > n = 4$. The construction uses $z\alpha = 2$ iid random keys r_1, r_2 drawn uniformly at random over $GF(5)$ and independently of the secret. The keys are partitioned into two matrices $\mathcal{R}_1$ and $\mathcal{R}_2$ 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 $\mathcal{R}_1$. Hence, we have, $\mathcal{R}_1 = \mathcal{D} = r_1$, $\mathcal{R}_2 = r_2$, and $\mathcal{S} = \begin{bmatrix} s_1 \\ s_2 \end{bmatrix}$. The secret and the keys are arranged in a $d \times \alpha = 3 \times 2$ matrix M. Let V be an $n \times d = 4 \times 3$ Vandermonde matrix. M and V are given again in (6).*

$$M = \begin{bmatrix} s_1 & r_1 \\ s_2 & r_2 \\ r_1 & 0 \end{bmatrix} \text{ and } V = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 4 \\ 1 & 4 & 1 \end{bmatrix}. \quad (6)$$

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 $\mathtt{CO}$ and $\mathtt{RO}$ for $d = 3$: *We check that a user contacting $d = 3$ parties can reconstruct the secret with minimum $\mathtt{CO}$ and $\mathtt{RO}$. 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,*

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 4 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ r_1 \end{bmatrix}. \quad (7)$$

The matrix on the left is a 3×3 square Vandermonde matrix, hence invertible. Therefore, the user can decode the secret (and r_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*

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} s_1 & r_1 \\ s_2 & r_2 \\ r_1 & 0 \end{bmatrix}. \qquad (8)$$

The system in (8) is equivalent to the two following systems $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \\ r_1 \end{bmatrix}$ *and* $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} r_1 \\ r_2 \end{bmatrix}$.
The decoder uses the latter system to decode r_1 and r_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 r_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.*

B. Universal Staircase code construction

We describe the (n, k, z) Universal Staircase code construction that achieves optimal communication and read overheads $\mathrm{CO}(d)$ and $\mathrm{RO}(d)$ simultaneously for all possible values of $k + z \leq d \leq n$. 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 $s_1, \ldots, s_{k\alpha}$, uniformly distributed
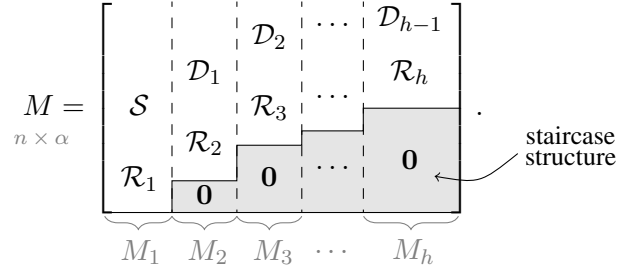

TABLE III: The structure of the matrix M that contains the secret and keys in the universal Staircase code construction.

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 $\mathcal{R}_i, i = 1, \ldots, h$, of respective dimensions $z \times k\alpha/\alpha_i\alpha_{i-1}$ (take $\alpha_0 = 1$). The matrices $\mathcal{R}_1, \ldots, \mathcal{R}_i$ consist 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,

$$M_1 = n \left[\begin{matrix} \mathcal{S} \\ \mathcal{R}_1 \end{matrix} \right] \begin{matrix} \alpha_1 \\ z \end{matrix}, \quad M_2 = n \left[\begin{matrix} \mathcal{D}_1 \\ \mathcal{R}_2 \\ \mathbf{0} \end{matrix} \right] \begin{matrix} \alpha_2 \\ z \\ 1 \end{matrix}, \ldots,$$

$$M_j = n \left[\begin{matrix} \mathcal{D}_{j-1} \\ \mathcal{R}_j \\ \mathbf{0} \end{matrix} \right] \begin{matrix} \alpha_j \\ z \\ n-d_j \end{matrix}, \ldots, \quad M_h = n \left[\begin{matrix} \mathcal{D}_{h-1} \\ \mathcal{R}_h \\ \mathbf{0} \end{matrix} \right] \begin{matrix} k \\ z \\ h-1 \end{matrix}.$$

$$\tag{9}$$

Each matrix $\mathcal{D}_j$ is formed of the $(n - j + 1)^{th}$ row of $\begin{bmatrix} M_1 & M_2 \ldots M_j \end{bmatrix}$ 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 $M = \begin{bmatrix} M_1 \ldots M_h \end{bmatrix}$ defined in Table III.

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 d.

Encoding: The encoding is similar to the Staircase code construction. Let V be an $n \times n$

Vandermonde matrix defined over $GF(q)$. The matrix M, defined in Table III, is multiplied by V to obtain the matrix $C = VM$. The n rows of C form the n different shares.

Decoding: To reconstruct the secret, a user contacting d_j parties indexed by $I \subseteq [n]$ downloads the first $k\alpha/\alpha_j$ symbols from each contacted party corresponding to $v_i \begin{bmatrix} M_1 \ldots M_j \end{bmatrix}$, for all $i \in I$. The decoding procedure given in the proof of Theorem 2 guarantees that the user will be able to decode the secret.

We postpone the example of a Universal Staircase code to Section V-A to have it next to the proof of Theorem 2.

IV. STAIRCASE CODE FOR GIVEN d

Proof of Theorem 1. Consider the (n, k, z, d) Staircase code defined in Section III-A. We prove Theorem 1 by establishing the following properties of the code:

1) Minimum CO(d) *and* RO(d)*:* We prove that a user contacting d parties can reconstruct the secret while incurring minimum CO and RO. A user contacting 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 $V_I \begin{bmatrix} \mathcal{S} & \mathcal{R}_1 \end{bmatrix}^T$, 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 $\mathcal{R}_1$) by inverting V_I. The code is optimal on communication and read overheads CO(d) and 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 CO(d) and RO(d) given in (4) and (5).

2) MDS: We prove that a user contacting $t = k + z$ 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,

$$V_I \begin{bmatrix} \mathcal{S} & \mathcal{D} \\ \mathcal{R}_1 & \mathcal{R}_2 \\ & \mathbf{0} \end{bmatrix}.$$

First, we show that the user can decode the entries of $\mathcal{D}$ and $\mathcal{R}_2$. The decoder considers the system,

$$V_I \begin{bmatrix} \mathcal{D} & \mathcal{R}_2 & \mathbf{0} \end{bmatrix}^T = V_I' \begin{bmatrix} \mathcal{D} & \mathcal{R}_2 \end{bmatrix}^T. \quad (10)$$

Recall that the dimensions of the all zero matrix in (10) 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 $\mathcal{R}_2$ because V_I' is invertible. Second, we prove that the user can always decode the entries of $\mathcal{S}$ and $\mathcal{R}_1$ and hence reconstruct the secret. Recall that $\mathcal{D}$ is the transpose of the last $\alpha - k$ rows of $M_1 \triangleq \begin{bmatrix} \mathcal{S} & \mathcal{R}_1 \end{bmatrix}^T$. By subtracting the previously decoded entries of $\mathcal{D}$ from $V_I \begin{bmatrix} \mathcal{S} & \mathcal{R}_1 \end{bmatrix}^T$, 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 indexed by z, denoted by $\mathcal{W}_Z = \{w_i, i \in Z\}$, does not reveal any information about the secret as given in equation (2), i.e., $H(\mathrm{S} \mid \mathrm{W}_Z) = H(\mathrm{S})$. Let R denote the random variable representing all the random keys, then it suffices to prove that $H(\mathrm{R} \mid \mathrm{W}_Z, \mathrm{S}) = 0$ as detailed in the Appendix. Therefore, we need to show that given the secret s as side information, any collection of z shares can decode all the random keys. A collection of $\mathcal{W}_Z$ shares can be written as

$$V_Z \begin{bmatrix} \mathcal{S} & \mathcal{D} \\ \mathcal{R}_1 & \mathcal{R}_2 \\ & \mathbf{0} \end{bmatrix}, \quad (11)$$

where V_Z is a $z \times d$ matrix corresponding to the rows of V_Z indexed by Z. The linear system in (11) can be divided into two systems as

follows,

$$V_Z \begin{bmatrix} \mathcal{S} & \mathcal{R}_1 \end{bmatrix}^T, \tag{12}$$

$$V_Z \begin{bmatrix} \mathcal{D} & \mathcal{R}_2 & \mathbf{0} \end{bmatrix}^T. \tag{13}$$

Given the secret as side information, it can be subtracted from (12), which becomes

$$V_Z \begin{bmatrix} \mathbf{0} & \mathcal{R}_1 \end{bmatrix}^T = V_Z'' \mathcal{R}_1,$$

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

V. UNIVERSAL STAIRCASE CODES

A. Example

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 III-B. 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 uniformly distributed 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,

$$\mathcal{S} = \begin{bmatrix} s_1 & s_4 \\ s_2 & s_5 \\ s_3 & s_6 \end{bmatrix}, \quad \mathcal{R}_1 = \begin{bmatrix} r_1 & r_2 \end{bmatrix},$$

$$\mathcal{R}_2 = \begin{bmatrix} r_3 \end{bmatrix} \quad \text{and} \quad \mathcal{R}_3 = \begin{bmatrix} r_4 & r_5 & r_6 \end{bmatrix}.$$

To build the matrix M which will be used for encoding the secret, we start with

$$M_1 = \begin{bmatrix} \mathcal{S} \\ \mathcal{R}_1 \end{bmatrix} = \begin{bmatrix} s_1 & s_4 \\ s_2 & s_5 \\ s_3 & s_6 \\ r_1 & r_2 \end{bmatrix}.$$

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 nth row of M_1, i.e., $\mathcal{D}_1 = \begin{bmatrix} r_1 & r_2 \end{bmatrix}^T$. Therefore, $M_2 = \begin{bmatrix} \mathcal{D}_1 & \mathcal{R}_2 & \mathbf{0} \end{bmatrix}^T = \begin{bmatrix} r_1 & r_2 & r_3 & 0 \end{bmatrix}^T$. Similarly, we have $\mathcal{D}_2 = \begin{bmatrix} s_3 & s_6 & r_3 \end{bmatrix}$ and

$$M_3 = \begin{bmatrix} s_3 & s_6 & r_3 \\ r_4 & r_5 & r_6 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

We obtain M by concatenating M_1, M_2 and M_3,

$$M = \begin{bmatrix} s_1 & s_4 & r_1 & s_3 & s_6 & r_3 \\ s_2 & s_5 & r_2 & r_4 & r_5 & r_6 \\ s_3 & s_6 & r_3 & 0 & 0 & 0 \\ r_1 & r_2 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{14}$$

$$\underbrace{}_{M_1} \underbrace{}_{M_2} \underbrace{}_{M_3}$$

Here, V is the $n \times n = 4 \times 4$ Vandermonde matrix over $GF(5)$ given in (15). The shares are given by the rows of the matrix $C = VM$ and shown in Table IV.

$$V = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 3 & 4 & 2 \\ 1 & 4 & 1 & 4 \end{bmatrix}. \tag{15}$$

The constructed Universal Staircase code satisfies the following properties:

1) MDS: We check that a user contacting $d_3 = k + z = 2$ parties can decode the secret. Suppose that the user contacts parties 1 and 2. The data downloaded by the user is $V_{\{1,2\}} M$ and is given by,

$$\underbrace{\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \end{bmatrix}}_{V_{\{1,2\}}} \underbrace{\begin{bmatrix} s_1 & s_4 & r_1 & s_3 & s_6 & r_3 \\ s_2 & s_5 & r_2 & r_4 & r_5 & r_6 \\ s_3 & s_6 & r_3 & 0 & 0 & 0 \\ r_1 & r_2 & 0 & 0 & 0 & 0 \end{bmatrix}}_{M_1 \quad M_2 \quad M_3}.$$

$$\tag{16}$$

We will show that the user can decode the secret by successively solving the linear systems

Party 1	Party 2	Party 3	Party 4
$s_1 + s_2 + s_3 + r_1$	$s_1 + 2s_2 + 4s_3 + 3r_1$	$s_1 + 3s_2 + 4s_3 + 2r_1$	$s_1 + 4s_2 + s_3 + 4r_1$
$s_4 + s_5 + s_6 + r_2$	$s_4 + 2s_5 + 4s_6 + 3r_2$	$s_4 + 3s_5 + 4s_6 + 2r_2$	$s_4 + 4s_5 + s_6 + 4r_2$
$r_1 + r_2 + r_3$	$r_1 + 2r_2 + 4r_3$	$r_1 + 3r_2 + 4r_3$	$r_1 + 4r_2 + r_3$
$s_3 + r_4$	$s_3 + 2r_4$	$s_3 + 3r_4$	$s_3 + 4r_4$
$s_6 + r_5$	$s_6 + 2r_5$	$s_6 + 3r_5$	$s_6 + 4r_5$
$r_3 + r_6$	$r_3 + 2r_6$	$r_3 + 3r_6$	$r_3 + 4r_6$

TABLE IV: An example of a universal Staircase code for $(n, k, z) = (4, 1, 1)$ over $GF(5)$.

$V_{\{1,2\}} M_3$, $V_{\{1,2\}} M_2$ and $V_{\{1,2\}} M_1$. The decoder starts by considering $V_{\{1,2\}} M_3$ which gives,

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} s_3 & s_6 & r_3 \\ r_4 & r_5 & r_6 \end{bmatrix}. \qquad (17)$$

The matrix on the left is invertible, and the user can decode the secret symbols and keys in (17). Then, the decoder considers the system $V_{\{1,2\}} M_2$ after subtracting from it the value of r_3 decoded in the previous step. The obtained system is again invertible and the decoder can decode r_1 and r_2. The decoder then considers $V_{\{1,2\}} M_1$, after canceling out r_1, r_2, s_3, s_6 decoded so far, to obtain the following system,

$$\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} s_1 & s_4 \\ s_2 & s_5 \end{bmatrix}.$$

The matrix on the left is again invertible and the decoder can reconstruct the secret. This remains true irrespective of which 2 parties are contacted.

2) Minimum CO *and* RO *for* $d_2 = 3$ *and* $d_1 = 4$: We check that a user contacting d parties, $d = 3, 4$, can decode the secret while achieving the minimum communication and read overheads given in (4) and (5). 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 $V_I [M_1 \; M_2]$ (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 by implementing a decoding procedure similar to the one above. The resulting CO and RO are equal to $3/2 - k = 1/2$ units achieving the optimal CO(d_2) and 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 CO(d_1) and RO(d_1) given in (4) and (5).

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.

B. Proof of Theorem 2

Consider the (n, k, z) Universal Staircase code construction defined in Section III-B. We prove Theorem 2 by establishing the following properties.

1) Encoding is well defined: We prove that the $(n - j + 1)^{th}$ row of $[M_1 \dots M_j]$ has the same number of entries as $\mathcal{D}_j, j = 1, \dots, h - 1$. Therefore, we can always construct the matrix $\mathcal{D}_j$. In fact, the number of entries of one row of $[M_1 \dots M_j]$ is equal to the sum of the number of columns of the M_i's, $i = 1, \dots, j$. Notice that $\alpha_{i-1} = \alpha_i + 1$, then we can write,

$$\frac{k\alpha}{\alpha_i \alpha_{i-1}} = k\alpha \left(\frac{1}{\alpha_i} - \frac{1}{\alpha_{i-1}} \right).$$

Hence, the number of columns of $[M_1 \dots M_j]$ is given by,

$$\frac{k\alpha}{\alpha_1} + k\alpha \left(\frac{1}{\alpha_2} - \frac{1}{\alpha_1} \right) + \cdots + k\alpha \left(\frac{1}{\alpha_j} - \frac{1}{\alpha_{j-1}} \right) = \frac{k\alpha}{\alpha_j}, \qquad (18)$$

which is equal to the number of entries of $\mathcal{D}_j$.

2) MDS and minimum CO(d) *and* RO(d) *for all* $k + z \leq d \leq n$: We prove that for all $k + z \leq$

$d \leq n$, a user contacting d parties can decode the secret while achieving the minimum communication and read overheads given in (4) and (5). Notice that the MDS property follows directly from the fact that a user contacting $d_h = k + z$ parties can reconstruct the secret by reading and downloading all the contacted shares.

A user contacting d_j, $j = 1, \ldots, h$, parties downloads the first $k\alpha/\alpha_j$ symbols of each party. Let $I \subseteq [n]$, $|I| = d_j$, be the set of indices of the contacted parties and let V_I be the matrix formed of the rows of V indexed by I. The total downloaded data is given by $V_I \begin{bmatrix} M_1 \ldots M_j \end{bmatrix}$ and can be divided into j linear systems given as follows,

$$V_I M_1 = V_I \begin{bmatrix} \mathcal{S} & \mathcal{R}_1 \end{bmatrix}^T \qquad (19)$$

$$V_I M_2 = V_I \begin{bmatrix} \mathcal{D}_1 & \mathcal{R}_2 & \mathbf{0} \end{bmatrix}^T \qquad (20)$$

$$\vdots$$

$$V_I M_{j-1} = V_I \begin{bmatrix} \mathcal{D}_{j-2} & \mathcal{R}_{j-1} & \mathbf{0} \end{bmatrix}^T \qquad (21)$$

$$V_I M_j = V_I \begin{bmatrix} \mathcal{D}_{j-1} & \mathcal{R}_j & \mathbf{0} \end{bmatrix}^T. \qquad (22)$$

We prove by induction that the user can always reconstruct the secret by iteratively decoding M_i, $i = j, \ldots, 1$, in each linear system $V_I M_i$. To that end, we verify the induction hypothesis for $i = j$. Given the system in (22), we show that the user can always decode M_j. The zero block matrix in (22) is of dimensions $(n - d_j) \times (k\alpha/\alpha_j\alpha_{j-1})$. Therefore, (22) can be rewritten as $V_I' \begin{bmatrix} \mathcal{D}_{j-1} & \mathcal{R}_j \end{bmatrix}^T$, where V_I' is the square Vandermonde matrix of dimensions $d_j \times d_j$ formed by the first d_j columns of V_I. Hence, the user can always decode the entries of M_j by inverting V_I'.

Next, suppose that the user can decode all the M_i's, $i = j, \ldots, l+1$, we prove that the user can always decode M_l. The lth system is given by $V_I M_l$. By construction M_l contains d_l non-zero rows, because the $\mathbf{0}$ block matrix is of dimensions $(n - d_l) \times (k\alpha/\alpha_l\alpha_{l-1})$. In addition, the entries of the last $l - 1$ non-zero rows of M_j are present in $\mathcal{D}_f$ for $f = j-1, \ldots, l-1$, which were previously decoded. It can be checked that $d_j = d_l - (l-1)$ for all $l < j$. Therefore, after subtracting the last $l - 1$ rows of M_l, the system becomes $V_I' M_l'$, where V_I' is again the $d_j \times d_j$ square Vandermonde matrix defined above and M_l' is the matrix formed

of the first $d_j = d_l - (l - 1)$ rows of M_l. Henceforth, the user can always decode M_l' by inverting V_I'. Finally, the user can decode all the entires of M_l that consist of the entries of M_l' and the entries of the last $l - 1$ rows of M_l, which were previously decoded.

Next, we show that minimum CO and RO are achieved. The number of symbols read and downloaded by a user contacting d_j parties is equal to $d_j(k\alpha/\alpha_j)$ symbols which corresponds to $d_j k/\alpha_j$ units. Then, the communication and read overheads are given by $d_j k/\alpha_j - k = kz/\alpha_j = kz/(d_j - z)$, which matches the optimal CO(d_j) and RO(d_j) for all $d_j = k + z, \ldots, n$, given in (4) and (5).

3) Perfect secrecy: Similarly to the proof of perfect secrecy in Theorem 1, we need to show that $H(\mathrm{R} \mid \mathrm{W}_Z, \mathrm{S}) = 0$ for all $Z \subset [n]$, $|Z| = z$ (see Appendix). This is equivalent to showing 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 $\mathcal{W}_Z$ of z shares can be written as $V_Z \begin{bmatrix} M_1 \ldots M_h \end{bmatrix}$, which can be divided into $h = n - k - z + 1$ linear systems as follows,

$$V_Z M_1 = V_Z \begin{bmatrix} \mathcal{S} & \mathcal{R}_1 \end{bmatrix}^T \qquad (23)$$

$$V_Z M_2 = V_Z \begin{bmatrix} \mathcal{D}_1 & \mathcal{R}_2 & \mathbf{0} \end{bmatrix}^T \qquad (24)$$

$$\vdots$$

$$V_Z M_h = V_Z \begin{bmatrix} \mathcal{D}_{h-1} & \mathcal{R}_h & \mathbf{0} \end{bmatrix}^T. \qquad (25)$$

We will prove by induction that given the secret $\mathbf{s}$ as side information, any collection $\mathcal{W}_Z$ of z shares can always iteratively decode $\mathcal{R}_i$, $i = 1, \ldots, h$, in each linear system $V_Z M_i$. To that end, we verify the induction hypothesis for $i = 1$ by showing that a collection of $\mathcal{W}_Z$ shares can always decode $\mathcal{R}_1$ in (23). Recall that the dimensions of $\mathcal{R}_1$ are $z \times k\alpha/\alpha_1$. Given the secret $\mathbf{s}$, (23) becomes,

$$V_Z \begin{bmatrix} \mathbf{0} & \mathcal{R}_1 \end{bmatrix}^T = V_Z'' \mathcal{R}_1,$$

where V_Z'' is a $z \times z$ square Vandermonde matrix formed by the last z columns of V_Z. Therefore, $\mathcal{R}_1$ can be decoded by inverting V_Z''.

Next, we suppose that any collection of $\mathcal{W}_Z$ shares can decode all the $\mathcal{R}_i$'s for $i = 1, \ldots, l-1$,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TIT.2017.2723019, IEEE Transactions on Information Theory

11

and show that any collection of $\mathcal{W}_Z$ can decode $\mathcal{R}_l$. The lth system is given by $V_I M_l = V_I \begin{bmatrix} \mathcal{D}_{l-1} & \mathcal{R}_l & \mathbf{0} \end{bmatrix}^T$. By construction, $\mathcal{D}_{l-1}$ consists of the entries of the last row of M_{l-1} which were previously decoded. Given the previously decoded information, any collection of $\mathcal{W}_Z$ shares can cancel out the entries of $\mathcal{D}_{l-1}$ to obtain $V_Z^* \mathcal{R}_l$. Since the dimensions of $\mathcal{R}_l$ are $z \times k\alpha/\alpha_l \alpha_{l-1}$, the matrix V_Z^* is a $z \times z$ square Vandermonde matrix formed by the $(\alpha_l + 1)^{th}$ to $(\alpha_l + z)^{th}$ rows of V_Z. Thus, $\mathcal{R}_l$ can be always decoded because V_Z^* is invertible. Therefore, all the keys can always be decoded. Hence, $H(\mathrm{R} \mid \mathrm{W}_Z, \mathrm{S}) = 0$. This concludes the proof of Theorem 2.

VI. Δ-Universal Staircase codes

We explain how to modify the Universal Staircase codes to construct Staircase codes that achieve minimum CO and RO only for a desired subset Δ of all possible d's, i.e., $\Delta \subseteq \{k + z, \ldots, n\}$. We refer to these codes as (n, k, z, Δ) Δ-universal Staircase codes. The advantage of these codes over universal codes is that they may require smaller number of symbols per share α.

Encoding: Let $\Delta' \triangleq \Delta \setminus \{k + z\}$ and order the d's in Δ' in decreasing order. We write $\Delta' = \{d_{i_1}, \ldots, d_{i_{|\Delta'|}}\} \subseteq \{d_1, \ldots, d_{h-1}\}$, where $d_{i_1} > d_{i_2} > \cdots > d_{i_{|\Delta'|}}$. Let $\alpha_{i_j} = d_{i_j} - z$ for all $d_{i_j} \in \Delta'$ and let $\alpha = LCM(\alpha_1, \ldots, \alpha_{|\Delta'|})$. Define $d_{i_{|\Delta'|+1}} \triangleq k + z$ and $\alpha_{i_{|\Delta'|+1}} \triangleq k$. The secret symbols are arranged in a matrix $\mathcal{S}$ of dimensions $\alpha_{d_{i_1}} \times k\alpha/\alpha_{d_{i_1}}$ and the random keys are partitioned into the matrices $\mathcal{R}_{i_1}, \ldots, \mathcal{R}_{i_{|\Delta'|+1}}$, of dimensions $z \times k\alpha/\alpha_{i_1}$ for $\mathcal{R}_{i_1}$ and $z \times k\alpha(\alpha_{i_j} - \alpha_{i_{j-1}})/(\alpha_{i_j}\alpha_{i_{j-1}})$ for all other $\mathcal{R}_{i_j}$, $j = 2, \ldots, |\Delta'|+1$. Construct M_{i_1} as the $d_{i_1} \times k\alpha/\alpha_{i_1}$ matrix structured as M_1 in (9). And, for each d_{i_j}, $j = 2, \ldots, |\Delta'| + 1$, construct M_{i_j} as the $d_{i_1} \times k\alpha(\alpha_{i_j} - \alpha_{i_{j-1}})/(\alpha_{i_j}\alpha_{i_{j-1}})$ structured as M_{i_j} in (9). The matrix $\mathcal{D}_{i_j}$, $j = 1, \ldots, |\Delta'|$, is the matrix of dimensions $\alpha_{i_{j+1}} \times k\alpha(\alpha_{i_{j+1}} - \alpha_{i_j})/(\alpha_{i_{j+1}}\alpha_{i_j})$ containing the last $d_{i_j} - d_{i_{j+1}}$ rows of $\begin{bmatrix} M_{i_1} \ldots M_{i_j} \end{bmatrix}$, from row d_{i_j} to row $d_{i_{j+1}} + 1$. Then, concatenate the constructed matrices, $M_{i_1}, \ldots, M_{i_{|\Delta'|+1}}$, to obtain the matrix M of dimensions $d_{i_1} \times \alpha$. The matrix M is multiplied by a Vandermonde matrix of dimensions $n \times d_{i_1}$ to obtain the shares.

Decoding: To reconstruct the secret, a user contacting d_{i_j} parties, indexed by $I \subseteq [n]$, downloads the first $k\alpha/\alpha_{i_j}$ symbols from each contacted party corresponding to $v_i \begin{bmatrix} M_{i_1} \ldots M_{i_j} \end{bmatrix}$, for all $i \in I$. The decoding procedure follows the same steps of the decoding procedure presented in the proof of Theorem 2 and the user will be able to decode the secret.

We omit the proof of Theorem 3 since it follows the same steps of the proof of Theorem 2.

VII. Threshold changeable secret sharing

An $(n, k, z; t')$ threshold changeable secret sharing (TCSS) code, defined in [22], is an (n, k, z) secret sharing scheme (satisfying (2) and (3)), where the threshold $t = k + z$ can be increased to $t' > t$ in a decentralized way without the intervention of the dealer. After the threshold increase, the security parameter z remains the same and k is increased to $k' = t' - z$. The parties are allowed to communicate as long as the security constraint is not violated. The efficiency of a TCSS is measured by the new share size for the new threshold t', which we refer to as the storage cost (SC) of the scheme[8]. Different variants of threshold changeable secret sharing schemes have been studied in the literature, see e.g., [25]–[27]. A connection between TCSS and CESS is shown in [15]. Code constructions are provided in [15], [16], [22] for the case when $z = t - 1$ and the threshold t' is given a priori.

In this section, we show how to construct an $(n, k, z; t')$ TCSS code for a given $t' > t$ using an $(n, k, z, d = t')$ Staircase code. However, different values of t' for the same (n, k, z) may require different Staircase codes. We show that this can be avoided by constructing what we call an $(n, k, z; [t + 1 : n])$ Universal TCSS code using an (n, k, z) Universal Staircase code. Both constructions involve the parties deleting parts of their shares and do not require communication

---

[8]Any secret sharing scheme is trivially threshold changeable, because a user contacting $t' > t$ parties can decode the secret by downloading any t shares. However, it does not achieve minimum storage cost for the new threshold.

	Party 1	Party 2	Party 3	Party 4
New share for $t'=3$	$s_1+s_2+s_3+r_1$	$s_1+2s_2+4s_3+3r_1$	$s_1+3s_2+4s_3+2r_1$	$s_1+4s_2+s_3+4r_1$
	$s_4+s_5+s_6+r_2$	$s_4+2s_5+4s_6+3r_2$	$s_4+3s_5+4s_6+2r_2$	$s_4+4s_5+s_6+4r_2$
	$r_1+r_2+r_3$	$r_1+2r_2+4r_3$	$r_1+3r_2+4r_3$	$r_1+4r_2+r_3$
Deleted for $t'=3$	s_3+r_4	s_3+2r_4	s_3+3r_4	s_3+4r_4
	s_6+r_5	s_6+2r_5	s_6+3r_5	s_6+4r_5
	r_3+r_6	r_3+2r_6	r_3+3r_6	r_3+4r_6

TABLE V: A $(4,1,1;[3:4])$ Universal TCSS code obtained from an $(4,1,1)$ Universal Staircase code over $GF(5)$. The original code has threshold $t=k+z=2$ and can be changed to either $t'=3$ or 4. The threshold change from $t=2$ to $t'=3$ is depicted. Each party deletes the last 3 symbols of its share. Similarly, the threshold can be changed to $t'=4$ by keeping the first two symbols of each share. In both cases, the obtained code achieves minimum storage cost (SC) (share size) given by (26).

among the parties. Moreover, this construction achieves the optimal storage cost (SC)

$$\text{SC} = \frac{k}{t'-z}, \qquad (26)$$

which is the minimum share size required if the dealer were present. The next example shows how to construct an $(n,k,z;[t+1:n])$ Universal TCSS code with optimal SC from an (n,k,z) Universal Staircase code by deleting parts of each share.

Example 3. *Consider the problem of constructing an $(n,k,z;[t+1:n]) = (4,1,1;[3:4])$ Universal TCSS code for all possible t', i.e., $t'=3$ and 4. To this end, we use an $(n,k,z) = (4,1,1)$ Universal Staircase code constructed in Section V-A. The shares given to each party are depicted in Table V.*

In our construction, to change the threshold from $t=k+z$ to any $t+1 \leq t' \leq n$, each party deletes the last $\frac{t'-z-k}{t'-z}\alpha$ symbols of its share. Recall that in CESS, each share is of unit size and consists of α symbols (α symbols = 1 unit). In this example, to change the threshold from $t=2$ to $t'=3$, each party deletes the last 3 symbols (in shaded blue) of its share. The obtained code achieves the minimum Storage Cost (SC) given in (26), because each new share is of size 3 symbols equal to $1/2$ unit. One can verify that a user contacting any $t'=3$ parties and downloading their new shares can decode the secret.

Similarly, the same code can be used to change the threshold from $t=2$ to $t'=4$. Each party deletes the last 4 symbols (in red and shaded blue) of its original share (or deletes the last symbol, in red, if the threshold was already changed to 3). Each new share consists of 2 symbols equal to $1/3$ unit. Hence, the obtained code achieves minimum Storage Cost (SC) given in (26). One can verify that a user downloading all the shares can decode the secret. In both cases, secrecy is inherited from the Staircase code, because the parties do not exchange any information when changing the threshold.

Corollary 1. *An $(n,k,z;t')$ TCSS code, respectively an $(n,k,z;[t+1:n])$ Universal TCSS code, can be constructed using an (n,k,z,d) Staircase code defined in Section III-A, respectively an (n,k,z) Universal Staircase code defined in Section III-B. To change the threshold from $t=k+z$ to t', each party deletes the last $\frac{t'-k-z}{t'-z}\alpha$ symbols of its share. Both constructions achieve optimal storage cost (SC) given in (26).*

Proof. We prove that an $(n,k,z;[t+1:n])$ Universal TCSS code can be constructed using an (n,k,z) Universal Staircase code and omit the proof for $(n,k,z;t')$ TCSS code, since it follows the same steps.

Starting with an (n,k,z) Universal Staircase code, the threshold is $t=k+z$. Assume that the threshold is to be changed to t' for any $t+1 \leq t' \leq n$. Each party deletes the last

$\frac{t'-z-k}{t'-z}\alpha$ symbols of its share (original share size is α symbols).

We establish the following properties.

1) *Minimum Storage Cost (SC):* By construction, the new share size is $\alpha - (t'-z-k)\alpha/(t'-z) = k\alpha/(t'-z)$ symbols. Recall that each α symbols are equal to 1 unit, hence each share is of size $k/(t'-z)$ units and (26) is achieved.

2) *Perfect secrecy:* Since the parties do not exchange any information when changing the threshold, perfect secrecy follows from the properties of the original Universal Staircase code.

3) *MDS:* By construction, after changing the threshold to t', each party keeps exactly the symbols that are sent to a user contacting any t' parties in the original CESS code. Therefore, the user can decode the secret by downloading any t' shares. Moreover, the secret is of maximal $k = t'-z$ shares. In fact, from (26) we know that the new share size α' is given by $\alpha' = k\alpha/(t'-z)$. Hence, the secret of size $k\alpha$ symbols is of size $(t'-z)\alpha'$ symbols equal to $t'-z$ shares and is of maximal size.

$\square$

Remark 1. *Note that the Universal TCSS code obtained from our construction also minimizes the communication and read overheads (CO and RO) in addition to minimizing the storage cost (SC). In other words, the new n shares stored after the threshold update, allow a user contacting d parties, for all $k+z \le d \le n$, to decode the secret while achieving the minimum communication and read overheads given in (4) and (5).*

For instance, in Example 3 for the new threshold $t' = 3$, a user contacting any $d = 4$ parties and downloading the first two symbols (in black) of each new share can decode the secret. The incurred CO (and RO) is equal to 2 symbols equal to $1/3$ unit and is minimum, i.e., achieves (4) and (5).

VIII. CONCLUSION

We considered the communication efficient secret sharing (CESS) problem. The goal is to minimize the read and download 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 three explicit constructions of Staircase codes. The first construction achieves minimum overhead for any given number of parties d contacted by the user. The second is a universal construction that achieves minimum overheads simultaneously for all possible values of d. The third construction achieves optimal costs universally for all values of d in a given set $\Delta \subseteq \{t, \ldots, n\}$. All Staircase code constructions can store a secret of maximal size and require a small finite field $GF(q)$ of size $q > n$. However, these code constructions require dividing the shares into α symbols. Finally, we described how Staircase codes can be used to construct threshold changeable secret sharing (TCSS) codes.

In conclusion, we point out some problems that remain open. The model we considered here and the proposed Staircase codes can provide security against parties corrupted by a passive Eavesdropper. However, the problem of constructing communication and read efficient codes that provide security against an active (malicious) adversary remains open. Moreover, constructing threshold changeable secret sharing codes where the security level can be increased by increasing the number of possibly colluding parties remains open in general (only special cases were solved in [26]).

APPENDIX

Let W_i denote the random variable representing share w_i, and for any subset $B \subseteq \{1, \ldots, n\}$ denote by W_B the set of shares indexed by B, i.e., $\mathcal{W}_B = \{W_i; i \in B\}$. We prove that, for all $Z \subset \{1, \ldots, n\}$, $|Z| = z$, the perfect secrecy constraint $H(S \mid W_Z) = H(S)$, given in (2), is equivalent to $H(R \mid W_Z, S) = 0$. The proof is standard [28], [29] but we reproduce it here for completeness. In what follows, the logarithms in the entropy function are taken base q. We can

write,

$$
\begin{aligned}
H(\mathrm{S} \mid \mathrm{W}_Z) &= H(\mathrm{S}) - H(\mathrm{W}_Z) + H(\mathrm{W}_Z \mid \mathrm{S}) \\
&= H(\mathrm{S}) - H(\mathrm{W}_Z) + H(\mathrm{W}_Z \mid \mathrm{S}) \\
&\quad - H(\mathrm{W}_Z \mid \mathrm{S}, \mathrm{R}) \qquad (27) \\
&= H(\mathrm{S}) - H(\mathrm{W}_Z) + I(\mathrm{W}_Z; \mathrm{R} \mid \mathrm{S}) \\
&= H(\mathrm{S}) - H(\mathrm{W}_Z) + H(\mathrm{R} \mid \mathrm{S}) \\
&\quad - H(\mathrm{R} \mid \mathrm{W}_Z, \mathrm{S}) \qquad (28) \\
&= H(\mathrm{S}) - H(\mathrm{W}_Z) + H(\mathrm{R} \mid \mathrm{S}) \\
&\qquad\qquad\qquad\qquad\qquad\qquad (29) \\
&= H(\mathrm{S}) - H(\mathrm{W}_Z) + H(\mathrm{R}) \\
&= H(\mathrm{S}) - z\alpha + z\alpha \qquad (30) \\
&= H(\mathrm{S}). \qquad (31)
\end{aligned}
$$

Equation (27) follows from the fact that given the secret $\mathbf{s}$ and the keys $\mathcal{R}$ any share can be decoded, equation (29) follows because $H(\mathrm{R} \mid \mathrm{S}, \mathrm{W}_Z) = 0$ and equation (30) follows because the Staircase code constructions use $z\alpha$ independent random keys.

REFERENCES

[1] R. Bitar and S. E. Rouayheb, "Staircase codes for secret sharing with optimal communication and read overheads," in *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 1396–1400, July 2016.

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

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions," in *Proceedings on Advances in Cryptology*, pp. 27–35, Springer-Verlag New York, Inc., 1990.

[10] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)*, vol. 72, no. 9, pp. 56–64, 1989.

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

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

[13] A. Beimel, "Secret-sharing schemes: a survey," in *Coding and Cryptology*, pp. 11–46, Springer, 2011.

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

[15] 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.

[16] 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.

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

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

[19] W. Huang, M. Langberg, J. Kliewer, and J. Bruck, "Communication efficient secret sharing," *arXiv preprint arXiv:1505.07515v2*, April 2016.

[20] W. Huang, M. Langberg, J. Kliewer, and J. Bruck, "Communication efficient secret sharing," *IEEE Transactions on Information Theory*, vol. 62, pp. 7195–7206, Dec 2016.

[21] N. B. Shah, K. V. Rashmi, and K. Ramchandran, "Distributed secret dissemination across a network," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, pp. 1206–1216, Oct 2015.

[22] K. M. Martin, J. Pieprzyk, R. Safavi-Naini, and H. Wang, "Changing thresholds in the absence of secure channels," in *Information Security and Privacy*, pp. 177–191, Springer, 1999.

[23] A. S. Rawat, O. O. Koyluoglu, and S. Vishwanath, "Centralized repair of multiple node failures with applications to communication efficient secret sharing," *arXiv preprint arXiv:1603.04822*, 2016.

[24] 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.

[25] F. Wang, Y.-s. Zhou, and D.-f. Li, "Dynamic threshold changeable multi-policy secret sharing scheme," *Security and Communication Networks*, vol. 8, no. 18, pp. 3653–3658, 2015.

[26] M. Nojoumian and D. R. Stinson, "On dealer-free dynamic threshold schemes.," *Adv. in Math. of Comm.*, vol. 7, no. 1, pp. 39–56, 2013.

[27] R. Shi and H. Zhong, "A secret sharing scheme with the changeable threshold value," in *Information Engineering and Electronic Commerce, 2009. IEEC'09. International Symposium on*, pp. 233–236, IEEE, 2009.

[28] N. B. Shah, K. V. Rashmi, and P. V. Kumar, "Information-theoretically secure regenerating codes for distributed storage," in *Proc. IEEE Global Communications Conference*, 2011.

[29] S. E. Rouayheb, E. Soljanin, and A. Sprintson, "Secure network coding for wiretap networks of type II," *IEEE Transactions on Information Theory*, vol. 58, pp. 1361–1371, March 2012.

Rawad Bitar (S'10) is currently a Ph.D. student in the ECE department at the Illinois Institute of Technology, Chicago. He received the Diploma degree in computer and communication engineering from the Lebanese University, Faculty of Engineering, Roumieh, Lebanon in 2013 and the M.S. degree from the Lebanese University, Doctoral school, Tripoli, Lebanon in 2014. His research interests are in the broad area of information theory and coding theory with a focus on coding for distributed storage and information theoretic security.

Salim El Rouayheb (S?07-M?09) is currently an assistant professor in the ECE department at the Illinois Institute of Technology, Chicago. He is the recipient of the NSF career award. He received the Diploma degree in electrical engineering from the Lebanese University, Faculty of Engineering, Roumieh, Lebanon, in 2002, and the M.S. degree from the American University of Beirut, Lebanon, in 2004. He received the Ph.D. degree in electrical engineering from Texas A&M University, College Station, in 2009. He was a postdoctoral research fellow at UC Berkeley (2010-2011) and a research scholar at Princeton University (2012-2013). His research interests are in the broad area of information theory and coding theory with a focus on network coding, coding for distributed storage and information theoretic security.