Repairable Threshold Secret Sharing Schemes

Xuan Guang Member, IEEE, Jiyong Lu Student Member, IEEE, and Fang-Wei Fu

Abstract

In this paper, we propose a class of new threshold secret sharing schemes with repairing function between shares. Specifically, each share, when it is broken or lost, can be repaired by some others without the help of the dealer. Further, a construction of such repairable threshold secret sharing schemes is designed by applying linearized polynomials and regenerating codes in distributed storage systems. In addition, a new repairing rate is introduced to characterize the performance and efficiency of the repairing function, and a tight upper bound is derived, which implies the optimality of repair. Under this optimality, we further discuss the optimality of traditional information rate which describes the efficiency of secret sharing schemes in the aspect of storage. Finally, we find that, by applying the minimum bandwidth regenerating codes in distributed storage systems to our construction, our proposed schemes can achieve such optimality of repairing and information rates.

Index Terms

threshold secret sharing schemes, repairable threshold schemes, the repairing rate, the information rate, optimality.

I. INTRODUCTION

In order to keep a secret (usually a cryptographic key) highly reliable and secure, Blakley [1] and Shamir [2] presented threshold secret sharing schemes, respectively. In Shamir’s \((k, n)\) threshold scheme, a dealer shares a secret \(D\) to \(n\) participants \(P_1, P_2, \ldots, P_n\). He first generates \(n\) shares of the secret \(D\),
denoted by $S_1, S_2, \cdots, S_n$, and then distributes $S_i$ to $P_i$ for $1 \leq i \leq n$ such that $k$ or more participants can recover the secret $D$ together (called recovery of the secret $D$) and $k - 1$ or less participants can obtain no information about the secret $D$ (called perfectly secure). It is easy to see that this $(k, n)$ threshold scheme is highly reliable and secure for the secret $D$, since it can resist no more than $n - k$ erasure errors and $k - 1$ leakages of shares. Lai and Ding [3] proposed several generalizations of Shamir’s threshold scheme. McEliece and Sarwate [4] discussed the close relationship between Shamir’s $(k, n)$ threshold scheme and $[n, k]$ Reed-Solomon codes [5], which indicated that one has to connect to at least $k + h$ shares for recovering the secret $D$ provided that $h$ erasures appear in the threshold scheme. For threshold secret sharing schemes, sometimes the share of a participant fails such as destroyed or lost, how to recover the failed share in order to keep the stability of the system. One natural approach is to request the dealer to regenerate the share and redistribute it to the corresponding participant. But it is not difficult to see that this way has some shortcomings. It has to seek the help of the dealer, and the dealer must maintain the original secret and the regenerating and redistributing functions for the share to the corresponding participant. Moreover, in practical applications, it possibly costs a lot to request the service of the dealer. Hence, we hope that the system can realize the self-repairing function without the help of the dealer, which will avoid the above mentioned shortcomings. In this paper, we propose repairable threshold secret sharing schemes, where the failed share of any participant can be just repaired by some others, meanwhile the recovery and perfectly secure properties of the system are still kept.

Motivated by the above goal, the recent research on distributed storage systems [6] may become a feasible approach to solve our problem. An $(n, k, d)$ regenerating code in distributed storage systems is used to distribute original data $M$, regarded as a row vector, to $n$ nodes such that any $k$ nodes can recover the original data $M$ and each failed node can be regenerated by the aid of any other $d$ nodes. However, different from the goals in distributed storage systems, secret sharing systems have their own requirements, such as perfectly secure property and threshold constraint. Thus, a natural and simple concatenation of the existing secret sharing schemes and regenerating codes may not satisfy the above mentioned fundamental requirements as to be discussed in Example 1 below. Further, let alone the repairable secret sharing schemes of good performance. This is the difficulty we face.

In this paper, we first present our research problem and the idea of its solution. After that, a construction of repairable threshold secret sharing schemes is proposed. Furthermore, we introduce a new rate, say repairing rate, to characterize the performance of repairing function of repairable schemes and present its tight upper bound. Combining with the fundamental information rate from classical secret sharing theory, we give the optimal information rate when optimal repairing rate is achieved, and further show
that our proposed schemes can achieve such optimality.

II. REPAIRABLE THRESHOLD SECRET SHARING SCHEMES

In this section, we will discuss threshold secret sharing schemes with repairing function in detail. Throughout this paper, we always consider \((k, n)\)-threshold secret sharing schemes. Our initial and natural idea is combining Shamir’s \((k, n)\)-threshold secret sharing scheme and an \((n, k, d)\) regenerating code directly. To be specific, first apply Shamir’s \((k, n)\)-threshold secret sharing scheme to obtain some statistically independent evaluations which further are regarded as the original data in a distributed storage scheme, and finally apply an \((n, k, d)\) regenerating code to implement the recovery of the secret by the cooperation of \(k\) or more shares and the repair of a failed share by the cooperation of any other \(d \geq k\) participants. However, notice that in this case the shares corresponding to different participants are no longer statistically independent because of the repairing requirement. This implies that the necessary perfectly secure property may be not satisfied as what the following example illustrates.

**Example 1:** A secret \(D\) needs to be shared among 4 participants \(P_i,\ 1 \leq i \leq 4\), and it requires that any at least 2 participants can recover the secret \(D\) and any 3 participants can repair a failed share. That is, the parameters are \(n = 4, k = 2, d = 3\). We give a scheme as follows.

**Step 1:** select 3 elements \(a_1, a_2, a_3\) in the finite field \(F_{11}\) independently and uniformly at random. Then define a polynomial \(f(x) = D + \sum_{j=1}^{3} a_j \cdot x^j \in F_{11}[x]\).

**Step 2:** compute \(y_i = f(x_i)\) where \(x_i = i\) for \(1 \leq i \leq 4\) \(\in F_{11}\).

**Step 3:** use a \((4, 2, 3)\) regenerating code with generator matrix

\[
G = [G_1, G_2, G_3, G_4] = \begin{bmatrix}
1 & 0 & 0 & 0 & 5 & 1 & 1 \\
0 & 1 & 0 & 0 & 2 & 1 & 9 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 2 & 4 \\
0 & 0 & 0 & 1 & 1 & 3 & 0 & 4
\end{bmatrix},
\]

where each \(G_i\) is a \(4 \times 2\) submatrix. This can generate 4 shares \(S_i\) to participant \(P_i\) by computing \(S_i = [y_1, y_2, y_3, y_4] \cdot G_i\) for \(1 \leq i \leq 4\). We obtain \(S_1 = (y_1, y_2),\ S_2 = (y_3, y_4),\ S_3 = (2y_2 + y_3 + y_4, 5y_1 + y_2 + y_3 + 3y_4)\) and \(S_4 = (y_1 + 9y_2 + 2y_3, y_1 + 4y_3 + 4y_4)\).

It is not difficult to verify that the recovery of the secret \(D\) and the repair of each share is satisfied. However, this scheme is no longer perfectly secure for the secret \(D\). For example \(P_3\), the share \(S_3\) of

\[\text{Notice that } d > k \text{ is necessary to guarantee that arbitrary } d \text{ shares can repair a failed one and the secret } D \text{ is still perfectly secure during the repair process. Actually, each of } d \text{ shares provides only a part of data for the repair such that the share can be repaired and the secret } D \text{ cannot be recovered.}\]
Theorem 1: \[ P_3 \text{ is } (2y_2 + y_3 + y_4, 5y_1 + y_2 + y_3 + 3y_4), \text{ further substituted by } y_i = D + \sum_{j=1}^{3} a_j \cdot i^j \text{ for } 1 \leq i \leq 4. \]

We have \(2y_2 + y_3 + y_4 = 4D + 8a_3 \) and \(5y_1 + y_2 + y_3 + 3y_4 = 10D + a_3.\) Thus, \(P_3\) itself can solve the secret \(D,\) which conflicts to the perfectly secure requirement.

Next, we will present our feasible \((n, k, d)\) repairable threshold secret sharing scheme. First, we restate the proposed problem and interpret some parameters. Let the base field be \(\mathbb{F}_{p^m}, p \text{ a prime and } m \text{ a positive integer.}\) A secret \(D \in \mathbb{F}_{p^m}\) will be shared to \(n\) participants \(P_1, P_2, \ldots, P_n.\) Each participant \(P_i\) keeps a share \(S_i\) of the secret \(D,\) which is an \(\alpha\)-dimensional vector over \(\mathbb{F}_{p^m}.\) Any \(k\) participants can use their shares together to recover the secret \(D.\) Once one share fails, any other \(d\) participants, each of which provides \(\beta < |M|/d\) symbols, can repair the failed share. Now we can give our threshold scheme.

**Step 1:** let \(t = \sum_{i=0}^{k-1} \min\{(d - i)\beta, \alpha\}.\) Select randomly \((t - 1)\) elements \(a_i, 1 \leq i \leq t - 1,\) in \(\mathbb{F}_{p^m}\) independently and uniformly, where \(m \geq t.\) Then define a linearized polynomial \(f(x) = Dx + \sum_{i=1}^{t-1} a_i x^{p^i} \in \mathbb{F}_{p^m}[x].\)

**Step 2:** select \(t\) elements \(x_i, 1 \leq i \leq t,\) in \(\mathbb{F}_{p^m}\) such that they are linearly independent over the prime field \(\mathbb{F}_p.\) Calculate \(f(x_i)\) for \(1 \leq i \leq t\) as \(t\) evaluations \(y_i = f(x_i), 1 \leq i \leq t.\)

**Step 3:** let \(C\) be an \((n, k, d)\) regenerating code with \(\mathbb{F}_{p^m}\)-valued generator matrix \(G = [G_1, G_2, \ldots, G_n],\) where each \(G_i\) is a \(t \times \alpha\) submatrix for \(1 \leq i \leq n.\) Each share \(S_i\) is generated by \(S_i = [y_1, y_2, \ldots, y_t] \cdot G_i,\) an \(\alpha\)-dimensional \(\mathbb{F}_{p^m}\)-valued vector, and then distributed to \(P_i\) for \(1 \leq i \leq n.\) Notice that this regenerating code \(C\) must satisfy that any other \(d\) shares can repair a failed share by providing \(\beta\) symbols for each one.

**A. Function Analysis**

In the following, we analyze the functions of recovery of the secret \(D\) and the repair of a failed share. Before discussion further, we need the following lemma.

**Lemma 1:** \([7] \text{ Lemma } 3.51\) Let \(x_1, x_2, \ldots, x_n \in \mathbb{F}_{p^m} (m \geq n),\) then

\[
\det\begin{bmatrix}
x_1 & x_1^p & x_1^{p^2} & \cdots & x_1^{p^{n-1}} \\
x_2 & x_2^p & x_2^{p^2} & \cdots & x_2^{p^{n-1}} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
x_n & x_n^p & x_n^{p^2} & \cdots & x_n^{p^{n-1}}
\end{bmatrix} \neq 0
\]

if and only if \(x_1, x_2, \ldots, x_n\) are linearly independent over \(\mathbb{F}_p.\)

\(^2\)The goal of this restriction is to ensure that the secret \(D\) is not recovered during the repair process.
Theorem 2: For our proposed secret sharing scheme, any $k$ participants can recover the secret $D$, and any $d$ participants can use their shares together, each of which provides $\beta$ symbols, to repair a failed share.

Proof: Since $C$ is an $(n, k, d)$ regenerating code, any $k$ participants can recover $t$ evaluations $y_1, y_2, \cdots, y_t$, which further deduces the secret $D$ by solving the following system of linear equations:

$$Dx_j + \sum_{i=1}^{t-1} a_i x_j^i = y_j, \quad 1 \leq j \leq t.$$ 

Particularly, since $x_1, x_2, \cdots, x_t$ are linearly independent over the prime field $\mathbb{F}_p$, together with Lemma 1, the above system has unique solution, that is, $D$ is recovered. Moreover, the repairing function is evident as the repairing property of the $(n, k, d)$ regenerating code $C$. We accomplish the proof.

B. Security Analysis

Next, we will show that our proposed scheme is still perfectly secure, that is, any $k-1$ or less participants obtain no information about the secret $D$. First, we need the following dimension lemma on regenerating codes. Similarly, consider an $(n, k, d)$ regenerating code, where it is required that each node, regarded as a participant, can store $\alpha$ symbols, and any $d$ ($> k$) nodes can repair a failed node by providing $\beta$ symbols for each one. Thus, for this $(n, k, d)$ regenerating code, the size of original data $M$ is

$$t = \sum_{i=0}^{k-1} \min \{ \alpha, (d-i)\beta \}.$$ 

Let the generator matrix be $G = [G_1, G_2, \cdots, G_n]$ with $G_i$ being a $t \times \alpha$ submatrix for $1 \leq i \leq n$, and then each node stores $\alpha$ linear combinations of original data $M$ by $M \cdot G_i$, $1 \leq i \leq n$. Let $W_i$ denote the vector space spanned by $\alpha$ column vectors of $G_i$, $1 \leq i \leq n$, and clearly $\dim(W_i) \leq \alpha$.

Lemma 3: For any $(n, k, d)$ regenerating code, the dimension of the vector space spanned by the corresponding column vectors of any $k-1$ nodes is strictly smaller than $t$.

Proof: Consider any $k-1$ nodes, without loss of generality, assume that they are the first $k-1$ nodes $P_1, P_2, \cdots, P_{k-1}$, and the corresponding spaces are $W_1, W_2, \cdots, W_{k-1}$ of dimensions $\Omega_1, \Omega_2, \cdots, \Omega_{k-1}$, respectively. By using the dimension theorem recursively, one has

$$\dim \left( \sum_{i=1}^{k-1} W_i \right) = \sum_{i=1}^{k-1} \dim(W_i) - \sum_{j=1}^{k-2} \dim \left( W_j \cap \sum_{i=j+1}^{k-1} W_i \right).$$  \(1\)

Further, notice that for any $j, 1 \leq j \leq k-2$, the nodes $P_{j+1}, P_{j+2}, \cdots, P_{k-1}$ and the other $d-(k-1-j)$ nodes except $P_j$ can repair the node $P_j$ together when it fails, and the other $d-(k-1-j)$ nodes provide $(d-(k-1-j))\beta$ linearly independent vectors at most. Hence all remaining dimensions of $P_j$ are from
the nodes \( P_{j+1}, P_{j+2}, \cdots, P_{k-1} \), i.e.,
\[
\dim \left( W_j \cap \sum_{i=j+1}^{k-1} W_i \right) \geq \max \{ 0, \Omega_j - (d - (k - 1 - j)) \beta \}
\]

\[= (\Omega_j - (d - (k - 1 - j)) \beta)^+.\]

Combining with the equality (1), we further have
\[
\dim \left( \sum_{i=1}^{k-1} W_i \right) \leq \sum_{i=1}^{k-1} \Omega_i - \sum_{j=1}^{k-2} (\Omega_j - (d - (k - 1 - j)) \beta)^+
\]
\[
\leq \min \{ \alpha, d\beta \} + \sum_{j=1}^{k-2} \min \{ \alpha, (d - (k - 1 - j)) \beta \}
\]
\[
= \sum_{j=1}^{k-1} \min \{ \alpha, (d - (k - 1 - j)) \beta \}
\]
\[
= \sum_{i=0}^{k-2} \min \{ \alpha, (d - i) \beta \}
\]
\[
< \sum_{i=0}^{k-1} \min \{ \alpha, (d - i) \beta \} = t,
\]
where from \( \min \{ \alpha, (d - (k - 1)) \beta \} > 0 \), the last inequality follows. This completes the proof.

**Theorem 4:** The above repairable threshold secret sharing scheme satisfies the perfectly secure property.

**Proof:** For the perfectly secure property, we indicate that any \( k - 1 \) or less participants can obtain no information on the secret \( D \). By Lemma 3, we know that any \( k - 1 \) or less participants together keep a subspace of dimension less than \( t \), say an \( r \)-dimensional subspace. Thus, it suffices to prove that even if any \( r \) linear combinations \( z_1, z_2, \cdots, z_r \) of \( y_1, y_2, \cdots, y_t \) with \( y_i = f(x_i), 1 \leq i \leq t \), are known completely, the secret \( D \) could be arbitrary element in \( \mathbb{F}_{p^m} \) with equal probability.

Let \( [z_1, z_2, \cdots, z_r] = [y_1, y_2, \cdots, y_t] \cdot \hat{G} \), where \( \hat{G} = [g_{i,j}]_{1 \leq i \leq t, 1 \leq j \leq r} \) is a \( t \times r \) submatrix of \( G \) over the prime field \( \mathbb{F}_p \), and without loss of generality, let \( \hat{G} \) be full column rank. Since \( [y_1, y_2, \cdots, y_t] = [D, a_1, \cdots, a_{t-1}] \cdot X \), where \( X = [x_j^p]_{0 \leq i \leq t-1, 1 \leq j \leq t} \) is a \( t \times t \) matrix over \( \mathbb{F}_{p^m} \), we deduce
\[
[z_1, z_2, \cdots, z_r] = [D, a_1, \cdots, a_{t-1}] \cdot \hat{X} G
\]
\[
=[D, a_1, \cdots, a_{t-1}]
\begin{bmatrix}
  x_1 & x_2 & \cdots & x_t \\
  x_1^2 & x_2^2 & \cdots & x_t^2 \\
  \vdots & \vdots & \ddots & \vdots \\
  x_1^{t-1} & x_2^{t-1} & \cdots & x_t^{t-1}
\end{bmatrix}
\begin{bmatrix}
  g_{1,1} & g_{1,2} & \cdots & g_{1,r} \\
  g_{2,1} & g_{2,2} & \cdots & g_{2,r} \\
  \vdots & \vdots & \ddots & \vdots \\
  g_{t,1} & g_{t,2} & \cdots & g_{t,r}
\end{bmatrix}
\]
\[
=[D, a_1, \cdots, a_{t-1}]
\begin{bmatrix}
  \sum_{i=1}^t g_{i,1} x_i & \sum_{i=1}^t g_{i,2} x_i & \cdots & \sum_{i=1}^t g_{i,r} x_i \\
  \sum_{i=1}^t g_{i,1} x_i^p & \sum_{i=1}^t g_{i,2} x_i^p & \cdots & \sum_{i=1}^t g_{i,r} x_i^p \\
  \vdots & \vdots & \ddots & \vdots \\
  \sum_{i=1}^t g_{i,1} x_i^{t-1} & \sum_{i=1}^t g_{i,2} x_i^{t-1} & \cdots & \sum_{i=1}^t g_{i,r} x_i^{t-1}
\end{bmatrix}
\begin{bmatrix}
  \sum_{i=1}^t g_{i,1} x_i & \sum_{i=1}^t g_{i,1} x_i^p & \cdots & \sum_{i=1}^t g_{i,1} x_i^{t-1} \\
  \sum_{i=1}^t g_{i,2} x_i & \sum_{i=1}^t g_{i,2} x_i^p & \cdots & \sum_{i=1}^t g_{i,2} x_i^{t-1} \\
  \vdots & \vdots & \ddots & \vdots \\
  \sum_{i=1}^t g_{i,r} x_i & \sum_{i=1}^t g_{i,r} x_i^p & \cdots & \sum_{i=1}^t g_{i,r} x_i^{t-1}
\end{bmatrix}
\]

Since \(\hat{G}\) is full column rank, and \(x_i, 1 \leq i \leq t\), are linearly independent over \(\mathbb{F}_p\), \(\sum_{i=1}^t g_{i,j} x_i, 1 \leq j \leq r\), are also linearly independent over \(\mathbb{F}_p\). Together with Lemma 1, it is implied that \(X \hat{G}\) is also full column rank. Therefore, it is shown that for every element \(D\) in \(\mathbb{F}_{p^m}\), the number of solutions of the above system of linear equations is equal, which implies that the secret \(D\) is equal probability even though \(z_1, z_2, \cdots, z_r\) are known completely. We accomplish the proof.

\[\blacksquare\]

III. Performance Analysis of The Proposed Schemes

In this section, we focus on the efficiency of our proposed schemes. Specially, since repairable threshold secret sharing schemes contain a new function of repair, we define a repairing rate below to characterize the efficiency of repair, which is also important in the aspect of security. First, we introduce some necessary notation. We still consider an \((n, k, d)\) repairable threshold secret sharing scheme. When one share fails, say \(S_i\), any other \(d\) participants can repair it. We use \(T\) to denote the index set of the \(d\) participants, say a repairing set, and further for each \(j \in T\), let \(R^i_{j, T}\) represent the symbols provided by \(P_j\) to repair \(S_i\). Now, we define the repairing rate.

\textit{Definition 1:} For a repairable threshold secret sharing scheme, the repairing rate for participant \(P_i\) is defined as the ratio \(\rho_{\text{rep}}^{(i)} = \min\{\frac{\log_2|S|}{\log_2|T|} \mid T \subseteq [n] \setminus \{i\}, |T| = d\}\), where \(|n| = \{1, 2, \cdots, n\}\), and \(S_i\) and \(R^i_{j, T}\) are the sets of all possible values taken by \(S_i\) and \(R^i_{j, T}\), respectively. Further, the repairing rate of this scheme is defined as \(\rho_{\text{rep}} = \min_{1 \leq i \leq n} \rho_{\text{rep}}^{(i)}\).

Actually, \(\rho_{\text{rep}}^{(i)}\) is the minimum of the ratios of the number of bits in share to the total number of bits provided by all participants in \(T\) to repair \(S_i\) amongst all sets \(T \subseteq [n] \setminus \{i\}\) of size \(d\). This naturally
characterizes the repairing efficiency of $P_i$, and also to some extent describes the security of repair, since $P_i$ possibly obtains more information on the secret and the shares of others than the necessary just for repair during the repairing process. And the smaller the $\rho_{\text{rep}}^{(i)}$ is, the more information $P_i$ can obtain. For our proposed repairable threshold secret sharing schemes, all shares $S_i$, $1 \leq i \leq n$, are $\alpha$-dimensional vectors and all $R_{j,T}^i$, $j \in T$, are $\beta$-dimensional vectors over $\mathbb{F}_{p^m}$, so $|S_i| = p^{m\alpha}$, $|R_{j,T}^i| = p^{m\beta}$. Thus, the repairing rate of our schemes is $\alpha/d\beta$. Notice that higher repairing rate is preferable, and evidently $\alpha \leq d\beta$ for successful repair. Hence, the repairing rate $\rho_{\text{rep}}$ of the schemes is upper bounded by 1, i.e., $\rho_{\text{rep}} \leq 1$. We say it optimal repairing rate if this upper bound is achieved. Actually, besides achieving the most efficiency of repair, a repairable threshold secret sharing scheme with optimal repairing rate is more secure. Specifically, if $\rho_{\text{rep}} < 1$, that is, $\alpha < d\beta$, then except the necessary information quantity for repairing the failed share, those $d$ participants provide more information to that participant of failed share. In other words, the participant of failed share obtains extra information of other shares except the necessary information for repairing its share. Not difficult to see that this case is not secure enough, since a malicious participant can always claim it fails in order to obtain more information, and then after several repairing processes, he even possibly obtains enough information to recover the secret $D$. Thus, we should require schemes always achieving optimal repairing rate, i.e., $\rho_{\text{rep}} = 1$. Furthermore, in secret sharing theory, the information rate, as a traditional index to characterize the efficiency of the schemes, is defined below.

**Definition 2:** For a secret sharing scheme, the information rate for participant $P_i$ is the ratio $\rho_{\text{inf}}^{(i)} = \frac{\log_2|D|}{\log_2|S_i|}$, where $D$ and $S_i$ are the sets of all possible values that $D$ and $S_i$ can take, respectively. Further, the information rate of this scheme is defined as $\rho_{\text{inf}} = \min_{1 \leq i \leq n} \rho_{\text{inf}}^{(i)}$.

It is not difficult to see that this rate characterizes the storage efficiency of the system. Therefore, we also concern the optimal information rate of repairable threshold secret sharing schemes under optimal repairing rate.

**Theorem 5:** For an $(n, k, d)$ repairable threshold secret sharing scheme of optimal repairing rate, i.e., $\rho_{\text{rep}} = 1$, the information rate $\rho_{\text{inf}}$ is upper bounded by $\frac{k(2d-k+1)}{2d}$. 

**Proof:** Reviewing our proposed threshold schemes, let $D$ and $a_1, a_2, \cdots, a_{t-1}$ be $t$ random variables, which are independently and uniformly over $\mathbb{F}_{p^m}$. Each share is an $\alpha$-dimensional vector over $\mathbb{F}_{p^m}$ and the data provided by a participant for repair is regarded as a $\beta$-dimensional vector over $\mathbb{F}_{p^m}$. We use $H(\cdot)$ to denote the entropy function.
Consider any \( k \) participants, without loss of generality, assume that they are \( P_1, P_2, \cdots, P_k \) with shares \( S_1, S_2, \cdots, S_k \), respectively. Then, we have

\[
tH(D) = H(D, a_1, \cdots, a_{t-1}) = H(S_l, 1 \leq l \leq k)
\]

\[
\leq H(R_{j,T}^1, j \in T \setminus \{2, \cdots, k\}, R_{i,T}^1, S_i, 2 \leq l \leq k) \tag{2}
\]

\[
= H(R_{j,T}^1, j \in T \setminus \{2, \cdots, k\}, S_i, 2 \leq l \leq k) \tag{3}
\]

\[
\leq H(R_{j,T}^1, j \in T \setminus \{2, \cdots, k\}) + H(S_i, 2 \leq l \leq k)
\]

\[
\leq (d - (k - 1))\beta \log_2 p^m + H(S_i, 2 \leq l \leq k) \tag{4}
\]

\[
= (d - k + 1)\beta H(D) + H(S_i, 2 \leq l \leq k),
\]

where \( T \) in (2) is a repairing set of \( S_1 \), containing the indexes of \( P_2, P_3, \cdots, P_k \) and other \( d - (k - 1) \) participants except \( P_1 \), and the equality (2) follows since \( R_{j,T}^1, j \in T \), can repair \( S_1 \). The equality (3) follows from \( H(R_{i,T}^1|S_i) = 0 \) for \( 2 \leq l \leq k \). The equality (4) follows because each of \( R_{j,T}^1, j \in T \setminus \{2, \cdots, k\} \), is regarded as a \( \beta \)-dimensional random vector taking values in \( \mathbb{F}_p^\beta \).

Applying the same analysis method on \( H(S_i, 2 \leq l \leq k) \), we further obtain

\[
H(S_i, 2 \leq l \leq k) \leq (d - k + 2)\beta H(D) + H(S_i, 3 \leq l \leq k).
\]

So far and so forth, we finally obtain

\[
tH(D) \leq \sum_{i=0}^{k-1} (d - i)\beta H(D) = \frac{k(2d - k + 1)}{2} \beta H(D).
\]

Thus, we obtain \( \beta \geq \frac{2t}{k(2d - k + 1)} \), further indicating \( \rho_{\inf} = \frac{\log |D|}{\log |S_i|} = \frac{1}{\alpha} = \frac{1}{d\beta} \leq \frac{k(2d - k + 1)}{2d} \). We accomplish the proof.

Particularly, for some applications, if it is not necessary to give the parameter \( t \) in advance, then we can set \( \beta = 1 \) as \( \beta \geq 1 \). In this case, \( \alpha = d\beta = d \), showing \( |S_i| = p^{md} \). Together with \( |D| = p^m \), the information rate \( \rho_{\inf} \) is upper bounded by \( \frac{1}{d} \), which only depends on the size of a repairing set. In fact, this upper bound is also tight. Moreover, it is necessary to indicate that this rate \( \frac{1}{d} \) degrades to 1 when the repairing function isn’t considered, which is the optimal information rate for classical threshold secret sharing schemes (see Fig. 2). If the participant of failed share obtaining some extra information during the repair process is allowed, i.e., \( d\beta > \alpha \), then the repairing rate \( \rho_{\text{rep}} \) will become smaller while the information rate \( \rho_{\inf} \) will become higher. This implies that there is a tradeoff between the repairing rate \( \rho_{\text{rep}} \) and the information rate \( \rho_{\inf} \). At last, we observe that if our proposed schemes use the minimum
bandwidth regenerating (MBR) codes [6] to generate shares, this optimal information rate under the optimal repairing rate can be achieved. We take the following example to show it.

**Example 2:** A secret \( D \in \mathbb{F}_{2^5} \) is shared among 4 participants \( P_i, 1 \leq i \leq 4 \). It is required that any at least 2 participants can recover the secret \( D \) and any failed share can be repaired by the other 3 participants. First we select 4 elements \( a_i, 1 \leq i \leq 4 \), in \( \mathbb{F}_{2^5} \) and define a linearized polynomial \( f(x) = Dx + \sum_{i=1}^{4} a_i x^{2^i} \in \mathbb{F}_{2^5}[x] \). Then we select 5 elements \( x_1, x_2, \cdots, x_5 \in \mathbb{F}_{2^5} \), which are linearly independent over the prime field \( \mathbb{F}_2 \), and then evaluate \( y_i = f(x_i), 1 \leq i \leq 5 \). Furthermore, we use a (4,2,3) MBR code to generate 4 shares \( S_1 = [y_1, y_2, y_3], S_2 = [y_1, y_4, y_5], S_3 = [y_2, y_4, \sum_{i=1}^{5} y_i] \) and \( S_4 = [y_3, y_5, \sum_{i=1}^{5} y_i] \). It is easy to verify that the secret \( D \) can be recovered by any 2 participants and the perfectly secure property is satisfied, and further, the repairing function is also qualified. In addition, it is evident that this scheme achieves the optimal information rate under the optimal repairing rate, that is, \( \rho_{rep} = \frac{\alpha}{d \beta} = 1 \) and \( \rho_{inf} = \frac{k(2d-k+1)}{2dt} = \frac{1}{3} \), where \( k = 2, d = 3, t = 5, \alpha = 3, \beta = 1 \).

**IV. Conclusion**

In this paper, we consider the repair problem of threshold secret sharing schemes without the help of the dealer. We present a construction of repairable threshold secret sharing schemes, which can accomplish repairing function of failed shares and still guarantee the perfectly secure property of the secret. Finally, we analyze the performance of repairable threshold schemes by discussing the introduced repairing rate and traditional information rate.

**References**

[1] G. R. Blakley, “Safeguarding Cryptographic Keys,” *in Proc. APIPS 1979 National Computer Conference*, vol. 48, pp. 313-317, Arlington, Jun. 1979.

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

[3] C.-P. Lai, and C. Ding, “Several Generalizations of Shamir’s Secret Sharing Scheme” *Int. J. Found. Inf. Comput. Sci.*, vol. 15, no. 2, pp. 445-458, 2004.

[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, Sep. 1981.

[5] F. J. MacWilliams, and N. J. A. Sloane, “The Theory of Error-Correcting Codes,” North-Holland Publishing Company, New York, USA, 1981.

[6] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, “Network Coding for Distributed Storage Systems,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4539-4551, Sep. 2010.

[7] R. Lidl, H. Niederreiter, and P. M. Cohn, “Finite Fields,” Cambridge University Press, Cambridge, UK, 1997.

[8] D. R. Stinson, “cryptography theory and practice (third edition),” Taylor & Francis Group, New York, USA, 2006.