Improving the Cheater Identification Capability of Threshold Secret Sharing Schemes

Tanmoy Mandal
MFSDSAI
IIT Guwahati
Assam, India
m.tanmoy@iitg.ac.in

Srinivasan Krishnaswamy
Department of EEE
IIT Guwahati
Assam, India
srinikris@iitg.ac.in

Ratnajit Bhattacharjee
MFSDSAI, IIT Guwahati
Department of EEE, IIT Guwahati
Assam, India
ratnajit@iitg.ac.in

***Abstract*—Secret sharing is an important cryptographic primitive by which any confidential information or secret is shared among a group of participants. Only authorized subsets of participants can recover the secret correctly, while unauthorized subsets of participants eventually get no information about the secret. Vulnerabilities arise in a secret sharing scheme due to a single or multiple dishonest participants. A single or multiple participants can collude to cheat by modifying their shares during the reconstruction of the secret. This enables them to recover the secret correctly for themselves by misleading the honest participants. The proposed scheme aims to detect such dishonest activity of the cheating participants and identify them. The detection mechanism utilizes the property of divided difference and identifies cheaters by checking the consistency of the inherent algebraic constraints across multiple subsets of shares arising from the divided difference structure. Further, the scheme does not rely on any cryptographic assumption and achieves an improved bound on the maximum number of identifiable cheaters while maintaining the share size equal to that of the secret. In addition, a lower bound on the minimum number of participants required for successful undetectable cooperative cheating is established.**

***Index Terms*—Secret Sharing, Cheating Detection, Cheater Identification**

I. Introduction

Secret sharing is a method by which an authorized party, called the dealer, generates multiple shares from the secret and distributes them among participants. Only authorized subsets of participants can recover the secret correctly by combining their shares. Introduced by Shamir [1] and Blackley [2] separately, it plays a crucial role in protecting any sensitive information from being lost, damaged, or stolen. Secrets in these schemes can be recovered only if the cardinality of sets of participants satisfies a minimum predetermined threshold. Such a scheme is called a threshold scheme. However, the knowledge gained from the sets of shares having cardinality less than the threshold reveals no information about the secret. A scheme with the above property is called a perfect scheme. The proposed scheme is one such perfect threshold secret sharing scheme.

However, a secret sharing scheme becomes vulnerable when a dishonest dealer or participant deceives in the sharing or reconstruction phase. A dishonest dealer can distribute a forged share to a single or multiple participants, preventing the original secret from ever being retrieved. Further, a single participant or a group of participants may collude to deceive the reconstruction phase by distorting their shares. While the cheating participants can recover the secret correctly, the honest participants are deprived of the correct one. Such an attack, known as the Tompa-Woll attack, has been introduced in [3] which poses a threat to Shamir's scheme. To mitigate this issue, several schemes have been proposed in [4]–[13]. This paper presents a perfect threshold secret sharing scheme that utilizes the concept of divided difference to detect cheating and identify cheaters. The novelty of the scheme lies in the fact that it can identify multiple cheaters by checking the verification condition across several sliding windows (subsets of participants). Further, unlike the existing cheater identification schemes, the share size in the proposed scheme remains equal to the size of the secret. Analysis shows that for scenarios with a large number of participants and a lower threshold, the proposed scheme performs better than the existing ones. Moreover, the proposed scheme does not leverage any cryptographic primitives like commitments or hash functions or digital signatures to detect and identify cheaters.

A. Related Work

Harn [4] and Lin et al. [5] propose schemes that can detect and identify cheaters using redundant shares. A scheme using a one-way hash function with the aid of arithmetic coding is presented in [9]. Using the symmetric property of bivariate polynomials and the linearity property of interpolating polynomials, a threshold scheme is described in [7] which uses two algorithms. While the first algorithm identifies cheaters using m ($\geq k$) shares used to recover the secret, the second one deals with the redundant shares not involved in the secret reconstruction. Here, k denotes the threshold of the scheme. Based on the digital signature algorithm, a scheme is proposed in [6]. The security of the scheme relies on the robustness of the chosen signature algorithm. Further, based on the quadratic residues, a cheater identification scheme is presented in [14]. Cheaters in this scheme are identified by using a digital signature algorithm that verifies the integrity and authenticity of a public value computed by the Share Distribution Center (SDC). The proposed scheme, on the other hand, detects and

identifies cheaters by checking the consistency of a system of algebraic constraints across multiple subsets of shares.

B. Motivation and Contribution

As stated above, a secret sharing scheme is susceptible to single or multiple cheating participants. This issue was first systematically studied by Tompa and Woll [3], who demonstrated that even a single participant can take advantage of modifying the share. However, they have not analyzed any mechanism to identify the cheaters. The schemes proposed in [12] and [15] can identify any number of cheaters less than the threshold. But the sizes of the shares in these schemes are significantly larger than the secret. Based on polynomial evaluations and algebraic geometry codes, a scheme is proposed in [16]. However, they have not rigorously analyzed the threat models for the scheme. Recently, a code-based threshold scheme has been presented in [17] which uses the duality property of a linear MDS code as its inherent verification. Although the verification condition can detect any inconsistency of a share made by the participant, the cheater identification mechanism relies on assumptions such as non-collusion, non-cancellation of error contributions, and the availability of sufficiently many appropriate dual codewords. Under these assumptions, the iterative identification procedure may potentially identify up to $n-k$ cheaters. However, no such formal bound has been established on the maximum number of identifiable cheaters. Such a model is very restrictive in practice due to its several assumptions. In contrast, the proposed scheme can detect cheating by up to k (threshold) colluding participants. Further, the larger share size in [17] reduces the space efficiency, which the proposed scheme overcomes by maintaining the share size equal to that of the secret. Although the scheme presented in [18] enhances the space efficiency by reducing the share size, it can identify only a small number of cheaters. Schemes presented in [7] [11] [12] [15] [19] [20] neither achieve a better space efficiency in terms of the share size, nor significantly improves the upper bound (except scheme 2 in [20]) for the maximum number of cheaters to be identified. Although the scheme 2 of [20] improves this bound somewhat better, it again suffers due to its space inefficiency. Further, this upper bound for all these schemes is a function of the threshold only. This makes the schemes inefficient for scenarios with large number of participants and a small threshold. This motivates designing scheme having capability of identifying significantly more number of cheaters while keeping the share size minimal for an information-theoretic security.

Unlike Shamir's [1] scheme, where the secret is an evaluation of the polynomial at a fixed point, the proposed scheme encodes the secret as a higher-order invariant (divided difference [21]) of the underlying polynomial. This allows reconstruction via a direct linear functional rather than recovering the entire polynomial implicitly (or explicitly) as in Shamir's scheme. Further, the proposed divided difference–based scheme inherently provides algebraic consistency checks across several subsets of shares without relying on any cryptographic tools or assumptions. Moreover, since the share size is equal to the size of the secret, the scheme achieves the same level of information-theoretic secrecy as in Shamir's scheme.

C. Paper Organization

The rest of the paper is organized as follows:
Section II provides the necessary background and foundational knowledge required to understand the proposed work. It formally defines the concept of secret sharing and divided difference. The proposed scheme along with its design principle, cheating detection and cheater identification mechanisms are described in Section III. Finally, the paper is concluded in Section IV.

II. Preliminaries

A. Secret Sharing Scheme

Consider a secret sharing scheme with a secret $s \in \mathcal{K}$(secret space). The dealer generates n shares $s_1, s_2, \ldots, s_n \in \mathcal{S}$ (share space) from the secret s using some randomized algorithm. The shares are then distributed among a set of n participants $\mathcal{P} = \{P_1, P_2, \ldots, P_n\}$ securely over a private channel. Only authorized subsets of participants can recover the secret s by combining their shares and evaluating a secret recovery function. The collection of all authorized subsets of participants who are allowed to recover the secret correctly is called the access structure of the scheme and is denoted by Γ. The access structure is monotone increasing. However, any unauthorized subsets of participants cannot extract any meaningful information about the secret from their sets of shares. The collection of all such unauthorized subsets of participants is called the forbidden structure and is denoted by Δ. Thus, a secret sharing scheme consists of two phases: (1) Shares generation and distribution and (2) Secret reconstruction. An information theoretically secure secret sharing scheme must satisfy the following two properties:

1) **Correctness:** If the shares corresponding to the participants in an element of the access structure are not tampered with, the reconstruction function correctly outputs the secret. Let S and U_A denote the random variables corresponding to the secret s and the set of honest shares. Then $H(S|U_A) = 0, \forall A \in \Gamma$, where $H(X \mid Y)$ denotes the conditional entropy of the random variable X given Y.
2) **Perfectness:** The perfectness property states that the mutual information between the secret and the set of shares of an element of the forbidden structure must be equal to zero. Let V_B denote the random variable corresponding to the set of shares of elements of Δ, then $H(S|V_B) = H(S), \forall B \in \Delta$.

B. Divided Difference

Let $f \in \mathbb{F}_q[x]$ with $\deg(f) \leq k-1$, and let $x_1, x_2, \ldots, x_n$ be n distinct evaluation points, i.e., $x_i \neq x_j$ for $i \neq j$, where $i, j \in \{1, 2, \ldots, n\}$. The first-order divided difference of f for two distinct arguments x_i and x_j is defined as

$f[x_i, x_j] := \frac{f(x_j)-f(x_i)}{x_j-x_i}$. Higher-order divided differences are defined recursively. Let $I = \{i_1, i_2, \ldots, i_r\} \subseteq \{1, 2, \ldots, n\}$ with distinct elements. The $(r-1)^{th}$ order divided difference is defined as $f[x_{i_1}, x_{i_2}, \ldots, x_{i_r}] := \frac{f[x_{i_2}, \ldots, x_{i_r}] - f[x_{i_1}, \ldots, x_{i_{r-1}}]}{x_{i_r} - x_{i_1}}$. Equivalently, it can also be expressed as

$$f[x_{i_1}, x_{i_2}, \ldots, x_{i_r}] = \sum_{j=1}^{r} \frac{f(x_{i_j})}{\prod_{\substack{m=1 \\ m \neq j}}^{r} (x_{i_j} - x_{i_m})}.$$

Lemma 1. *Let $f(x) = \sum_{i=0}^{k-1} a_i x^i$ be a polynomial over $\mathbb{F}_q$ with $\deg(f) \leq k-1$. Then the following hold.*

1) *For any k distinct points $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$, $f[x_{i_1}, x_{i_2}, \ldots, x_{i_k}] = a_{k-1}$.*
2) *For any $r \geq k+1$ and any r distinct points $x_{i_1}, x_{i_2}, \ldots, x_{i_r}$, $f[x_{i_1}, x_{i_2}, \ldots, x_{i_r}] = 0$. In a compact form, $f[x_{i_1}, x_{i_2}, \ldots, x_{i_r}] = \begin{cases} a_{k-1}, & \text{if } r = k, \\ 0, & \text{if } r \geq k+1. \end{cases}$*

Proof. The result is a direct consequence of Theorem 2.1.3.10 of [21]. See [21] for detailed proof. □

III. Proposed Secret Sharing Scheme

Let $s \in \mathbb{F}_q$ be the secret to be shared among a set of n participants $\mathcal{P} = \{P_{x_1}, P_{x_2}, \ldots, P_{x_n}\}$. The proposed scheme is a (k, n)-threshold scheme. The participants in $\mathcal{P}$ are indexed by $[n] := \{1, 2, \ldots, n\}$. The dealer communicates with the participants through a secure and noise-free channel.

A. Generation and Distribution of Shares

1) Set $s = a_{k-1}$.
2) Randomly sample $a_0, a_1, \ldots, a_{k-2} \xleftarrow{\$} \mathbb{F}_q$.
3) Construct the polynomial $f(x) = \sum_{i=0}^{k-1} a_i x^i = a_0 + a_1 x + \cdots + a_{k-2} x^{k-2} + s x^{k-1}$.
4) Compute the shares $s_i = f(x_i)$ for $i = 1, 2, \ldots, n$.
5) For each $i \in \{1, 2, \ldots, n\}$, distribute s_i securely to the participant P_{x_i}.

B. Reconstruction of the Secret

Let $I = \{i_1, i_2, \ldots, i_k\} \subseteq [n]$ with $|I| = k$, where $1 \leq i_1 < i_2 < \cdots < i_k \leq n$. Let $\mathcal{P}_I = \{P_{x_{i_1}}, P_{x_{i_2}}, \ldots, P_{x_{i_k}}\}$ be the corresponding set of participants. The secret can be reconstructed as follows.

1) Collect the shares $f(x_{i_1}), f(x_{i_2}), \ldots, f(x_{i_k})$.
2) Compute the $(k-1)^{th}$ order divided difference $f[x_{i_1}, x_{i_2}, \ldots, x_{i_k}]$.
3) Output the secret $s = f[x_{i_1}, x_{i_2}, \ldots, x_{i_k}]$.

Since $\deg(f) \leq k-1$, the $(k-1)^{th}$ order divided difference of f over any k distinct arguments equals the leading coefficient of the polynomial f. Hence, $f[x_{i_1}, x_{i_2}, \ldots, x_{i_k}] = a_{k-1} = s$.

C. Cheating Detection

Let $I = \{i_1, i_2, \ldots, i_{k+1}\} \subseteq [n]$ be any subset of size $k+1$. For each such subset I, compute the k^{th} order divided difference $D_I := f[x_{i_1}, x_{i_2}, \ldots, x_{i_{k+1}}]$, where $f(x_{i_j}) := s_{i_j}$ for $1 \leq j \leq k+1$. On expanding, the above formula can be written as $D_I = \sum_{j \in I} \alpha_j^{(I)} s_j$, where $\alpha_j^{(I)} = \left(\prod_{\substack{m \in I \\ m \neq j}} (x_j - x_m) \right)^{-1} \in \mathbb{F}_q$. Since $\deg(f) \leq k-1$, the k-th order divided difference satisfies $D_I = f[x_{i_1}, x_{i_2}, \ldots, x_{i_{k+1}}] = 0$, for all subsets I when the shares are honest. Consider a structured family of subsets (e.g., sliding windows) $I_\ell = \{\ell, \ell+1, \ldots, \ell+k\}, \ell = 1, 2, \ldots, n-k$. For each window I_ℓ, compute $D_{I_\ell} = \sum_{j \in I_\ell} \alpha_j^{(I_\ell)} s_j$. If all shares are valid, then $D_{I_\ell} = 0, \forall \ell$. However, if the shares are modified, then there exists at least one window I_ℓ for which $D_{I_\ell} \neq 0$. Thus, the cheating is detected. Therefore,

- If $D_{I_\ell} = 0 \quad \forall \ell$, accept the shares.
- If there exists an ℓ for which $D_{I_\ell} \neq 0$, output "**Cheating detected**".

D. Cheater Identification

The cheater identification algorithm leverages the result in Lemma 1 that the k^{th} order divided difference of a polynomial of degree $(k-1)$ is zero when evaluated over any $k+1$ correct evaluations of the polynomial. Let c denote the number of cheaters. The identification algorithm assumes the existence of at least one clean verification window of size $k+1$. Let $C \subseteq [n]$ denote the set of cheating participants, and define $\mathcal{W} := \{I \subseteq [n] : |I| = k+1\}$ be the set of all windows of size $k+1$. For each $I = \{i_1, i_2, \ldots, i_{k+1}\} \in \mathcal{W}$, compute $D_I := \sum_{j \in I} \alpha_j^{(I)} s_j$. The steps for cheater identification are as follows.

1) Find a subset $I_r \in \mathcal{W}$ such that $D_{I_r} = 0$. Clearly $I_r \subseteq [n] \setminus C$.
2) For each participant $j \in [n] \setminus I_r$, perform
   a) For each $i \in I_r$, define $I_{i \to j} := (I_r \setminus \{i\}) \cup \{j\}$.
   b) Compute $D_{I_{i \to j}} := \sum_{\ell \in I_{i \to j}} \alpha_\ell^{(I_{i \to j})} s_\ell$.
3) For each $j \notin I_r$,
   a) If there exists $i \in I_r$ such that $D_{I_{i \to j}} \neq 0$, declare j as a cheater.
   b) Otherwise, if $D_{I_{i \to j}} = 0$ for all $i \in I_r$, declare j as honest.
4) Output the identified set of cheaters as

$$\hat{C} = \left\{ j \in [n] \setminus I_r \;\middle|\; \exists\, i \in I_r \text{ such that } D_{I_{i \to j}} \neq 0 \right\}.$$

Thus, under the condition $c \leq n-k-1$, the above algorithm uniquely and deterministically identifies all cheating participants.

Observe that a group of cheating participants can collaboratively modify their shares so that the consistency condition $\sum_{j \in I} \alpha_j^{(I)} s_j = 0$ is satisfied locally for a particular window I of size $k+1$. However, the proposed verification mechanism is inherently global, as it requires checking consistency across all windows $I_r \subseteq [n]$ of size $k+1$. Thus, to remain undetected, cheaters must simultaneously satisfy a system of such constraints corresponding to all verification windows. The following theorem establishes the minimum number of shares that must be corrupted to enable successful undetectable cooperative cheating.

Theorem 1. *Let $C := \{j_1, j_2, \ldots, j_c\} \subseteq [n]$ and $\mathcal{P}_C := \{P_{x_{j_1}}, P_{x_{j_2}}, \ldots, P_{x_{j_c}}\}$ be the set of cheating participants. Let*

their modified shares be $s'_i = s_i + \delta_i$ for $i \in C$, where $\delta_i \in \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$. Assume that the verification condition $\sum_{j\in I} \alpha_j^{(I)} s'_j = 0$ is checked for all subsets $I \subseteq [n]$ with $|I| = k+1$.

I. *Let $n \geq 2k$. If $c \leq k$, the system of equations*

$$\sum_{j\in I\cap C} \alpha_j^{(I)}\delta_j = 0, \forall I \subseteq [n],\ |I| = k+1$$

implies $\delta_j = 0$ for all $j \in C$. Hence, any nonzero modification is necessarily detected.

II. *If $c \geq k+1$, there exists a nonzero vector $(\delta_j)_{j\in C} \neq 0$ such that*

$$\sum_{j\in I\cap C} \alpha_j^{(I)}\delta_j = 0, \forall I \subseteq [n],\ |I| = k+1,$$

and thus cheating remains undetected.

Equivalently, the minimum number of participants required for successful undetectable cooperative cheating is $k+1$, provided that verification is performed over all subsets of size $k+1$.

Proof. **Part I:** For every window $I \subseteq [n]$ with $|I| = k+1$, the verification condition is $\sum_{j\in I} \alpha_j^{(I)} s'_j = 0$. Now,

$$\begin{aligned}\sum_{j\in I} \alpha_j^{(I)} s'_j &= \sum_{j\in I\cap C} \alpha_j^{(I)}(s_j + \delta_j) + \sum_{j\in I\setminus C} \alpha_j^{(I)} s_j \\ &= \sum_{j\in I} \alpha_j^{(I)} s_j + \sum_{j\in I\cap C} \alpha_j^{(I)}\delta_j\end{aligned}$$

Since $\sum_{j\in I} \alpha_j^{(I)} s_j = 0$ for every window I, it follows that

$$\sum_{j\in I\cap C} \alpha_j^{(I)}\delta_j = \sum_{j\in I} \alpha_j^{(I)} s'_j = 0. \tag{1}$$

We now show that if $c \leq k$, the only solution to (1) is the trivial solution $\delta_j = 0$ for all $j \in C$. Fix any $i \in C$. Since $c \leq k$, we have $|C \setminus \{i\}| \leq k-1$. Further, $c \leq k$ and $n \geq 2k$ implies that $n - c \geq k$. Therefore, there exists at least a set $T \subseteq [n] \setminus C$ such that $|T| = k$. Construct a window $I_i \subseteq [n]$ as $I_i := \{i\} \cup T$, where $T \subseteq [n] \setminus (C \setminus \{i\})$ and $|T| = k$. Then $|I_i| = k+1$, $i \in I_i$, and $I_i \cap C = \{i\}$. Substituting $I = I_i$ into (1), we obtain $\sum_{j\in I_i\cap C} \alpha_j^{(I_i)}\delta_j = \alpha_i^{(I_i)}\delta_i = 0$.

Since $\alpha_i^{(I_i)} \in \mathbb{F}_q^*$, it follows that $\delta_i = 0$. As $i \in C$ is arbitrary, it follows that $\delta_j = 0, \forall j \in C$. Hence, the only solution to (1) is the trivial solution. Therefore, any nonzero modification of shares by at most k colluding participants is necessarily detected.

Part II: We now show that if $c \geq k+1$, then there exists a nontrivial solution to (1).

Let $C_0 \subseteq C$ be any subset such that $|C_0| = k+1$. Choose a polynomial $g(x) \in \mathbb{F}_q[x]$ satisfying $\deg(g) \leq k-1$ and $g \not\equiv 0$. Define the vector $\delta = (\delta_j)_{j\in C} \in \mathbb{F}_q^c$ by

$$\delta_j = \begin{cases} g(x_j), & \text{for } j \in C_0, \\ 0, & \text{for } j \in C \setminus C_0. \end{cases}$$

Since a nonzero polynomial of degree $k-1$ has at most $k-1$ roots, and $|C_0| = k+1$, it follows that there exists at least one $j \in C_0$ such that $g(x_j) \neq 0$. Hence, $\delta \neq 0$. Take any window $I \subseteq [n]$ with $|I| = k+1$.

Now, $C = C_0 \cup (C \setminus C_0)$, and $C_0 \cap (C \setminus C_0) = \emptyset$. Then, for any subset $I \subseteq [n]$, we get $I \cap C = (I \cap C_0) \cup \big(I \cap (C \setminus C_0)\big)$. Therefore, $\sum_{j\in I\cap C} \alpha_j^{(I)}\delta_j = \sum_{j\in I\cap C_0} \alpha_j^{(I)}\delta_j + \sum_{j\in I\cap(C\setminus C_0)} \alpha_j^{(I)}\delta_j$. Applying the definition of δ_j,

$$\begin{aligned}\sum_{j\in I\cap C} \alpha_j^{(I)}\delta_j &= \sum_{j\in I\cap C_0} \alpha_j^{(I)} g(x_j) + \sum_{j\in I\cap(C\setminus C_0)} \alpha_j^{(I)} \cdot 0 \\ &= \sum_{j\in I\cap C_0} \alpha_j^{(I)} g(x_j). \end{aligned} \tag{2}$$

Now, $I = (I\cap C_0)\cup(I\setminus C_0)$ and $(I\cap C_0)\cap(I\setminus C_0) = \emptyset$. Since $g(x)$ has degree $\leq k-1$, using Lemma 1, $\sum_{j\in I} \alpha_j^{(I)} g(x_j) = 0$

$$\implies \sum_{j\in I\cap C_0} \alpha_j^{(I)} g(x_j) + \sum_{j\in I\setminus C_0} \alpha_j^{(I)} g(x_j) = 0.$$

If the window is fully contained with the cheaters, then $I = C_0 \implies I \setminus C_0 = \emptyset$. Therefore, $\sum_{j\in I\setminus C_0} \alpha_j^{(I)} g(x_j) = 0$. Hence

$$\sum_{j\in I\cap C_0} \alpha_j^{(I)} g(x_j) = 0. \tag{3}$$

Using (3) in (2), we obtain $\sum_{j\in I\cap C} \alpha_j^{(I)}\delta_j = 0, \forall I$. Thus, we have constructed a nonzero vector δ that satisfies the verification condition. This makes the cheating undetectable. Therefore, the minimum number of shares required to be corrupted for undetectable cooperative cheating is $k+1$. □

E. Computational Complexity

TABLE I
COMPUTATIONAL COMPLEXITY OF THE PROPOSED SCHEME

Procedure	Complexity
Share Generation	$O(nk)$
Reconstruction	$O(k^2)$
Verification	$O\Big(\binom{n}{k+1}(k+1)\Big)$
Practical Verification	$O((n-k)(k+1))$

Table I summarizes the computational complexity of the major operations in the proposed scheme. While the theoretical analysis considers all possible subsets of size $k+1$, sliding windows can be considered for practical implementations to reduce the verification complexity to $O((n-k)(k+1))$.

F. A Comparative Analysis

Table II provides a comparative analysis of the proposed scheme with the existing ones. In scheme [7], m denotes the number of shares used for secret reconstruction, while u that of the detection shares. Here, p denotes the probability of successful cheating, t denotes the maximum number of cheaters to be identified, and $|s|$ denotes the size of the secret. In many of these constructions, p is chosen as a function of the secret size. The share size, being dependent on p, exceeds the size of the secret, even for a negligible probability of successful cheating. Further, in most schemes (except [7], and

TABLE II
COMPARISON OF VARIOUS CHEATER DETECTION SCHEMES

Schemes	Size of the Share	Maximum Identifiable Cheaters
Shamir [1]	$\|s\|$	Cannot detect cheating
Sergio [15]	$\frac{2\|s\|}{p}$, where $p = \frac{2}{\|s\|}$	$t \leq k-1$
Yanxiang [12]	$\frac{\|s\|}{p}$, where $p = \frac{1}{\|s\|}$	$t \leq k-1$
Liu [13]	$\frac{2^{k-1}\|s\|}{p}$, $p = \frac{2^{k-1}}{\|s\|}$	$t \leq \lfloor \frac{k-2}{2} \rfloor$
Zheng [18]	$\frac{2\|s\|}{k+\omega}$	$t \leq \left\lfloor \frac{k-2}{2} \right\rfloor = \omega$
S. Obana [19] (Algorithm 1)	$\frac{\|s\|}{p}$, where $p = \frac{1}{\|s\|}$	$t \leq \left\lfloor \frac{k-1}{3} \right\rfloor$
S. Obana [19] (Algorithm 2)	$\frac{n(t+1)2^{3t-1}\|s\|}{p}$, $p = \frac{(t+1)2^{3t-1}}{\|s\|}$	$t \leq \left\lfloor \frac{k-2}{2} \right\rfloor$
Liu [7] (Algorithm 1)	$\frac{\|s\|}{p^{k-1}}$, where $p = \frac{1}{\|s\|}$	$t < \frac{m-k+u+1}{2}$
Liu [7] (Algorithm 2)		$t < \frac{n-k+1}{2}$
Adhikari [20] (Scheme 1)	$\frac{\|s\|}{p^3}$, where $p = \frac{1}{\|s\|}$	$t \leq \frac{k-1}{3}$
Adhikari [20] (Scheme 2)	$\frac{\lceil s \rceil}{p^{k+1}}$, $p = \frac{1}{\|s\|}$	$t \leq n-1$
Adhikari [20] (Scheme 3)	$\frac{\|s\|}{p^k}$, where $p = \frac{1}{\|s\|}$	$t \leq \frac{k-1}{3}$
Adhikari [20] (Scheme 4)	$\frac{(n-t)^{n+2t}\|s\|}{p^{n+2t}}$, where $p = \frac{1}{\|s\|}$	$t \leq \frac{k-1}{2}$
Proposed scheme	$\|s\|$	$t \leq n-k-1$

Scheme 2 of [20]), the maximum number of cheaters that can be detected is upper bounded by a function of the threshold k alone, which is not the case for the proposed one. Although this bound for the maximum number of identifiable cheaters is improved in schemes [7] and [20] (scheme 2), the share size in these schemes exceeds the size of the secret. However, this storage inefficiency is partially relaxed in [18]. But again, the number of detectable cheaters remains comparatively small. Observe that all these limitations are overcome in the proposed scheme. While maintaining the share size equal to the secret, it yields a larger bound on the maximum number of cheaters that can be identified. This makes the proposed scheme space-efficient and a good candidate for scenarios with a large number of participants and a relatively small threshold.

IV. CONCLUSION

This paper presents a perfect threshold secret sharing scheme with mechanisms of cheating detection and cheater identification based on the concept of divided difference. The proposed scheme achieves an improved bound on the maximum number of identifiable cheaters without increasing the share size beyond the secret. Moreover, the detection and identification mechanisms do not rely on any cryptographic assumptions. Additionally, a lower bound for the minimum number of shares to be corrupted to make cheating undetectable has been calculated. Estimating the probability of successful cooperative cheating can be taken in future. Further, designing information-theoretic schemes capable of identifying cheating participants without introducing any redundant share remains an interesting direction for future work.

REFERENCES

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

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Managing Requirements Knowledge, International Workshop on*. IEEE Computer Society, 1979, pp. 313–313.

[3] M. Tompa and H. Woll, "How to share a secret with cheaters," *journal of Cryptology*, vol. 1, no. 3, pp. 133–138, 1989.

[4] L. Harn, "Generalised cheater detection and identification," *IET Information Security*, vol. 8, no. 3, pp. 171–178, 2014.

[5] L. Harn and C. Lin, "Detection and identification of cheaters in (t, n) secret sharing scheme," *Designs, Codes and Cryptography*, vol. 52, pp. 15–24, 2009.

[6] R.-J. Hwang, W.-B. Lee, and C.-C. Chang, "A concept of designing cheater identification methods for secret sharing," *Journal of systems and software*, vol. 46, no. 1, pp. 7–11, 1999.

[7] Y. Liu, C. Yang, Y. Wang, L. Zhu, and W. Ji, "Cheating identifiable secret sharing scheme using symmetric bivariate polynomial," *Information Sciences*, vol. 453, pp. 21–29, 2018.

[8] Z. Wang, Y. Liu, W. Yan, W. Wei, J. Li, D. Zhang, and O. Alfandi, "Cheating detection and cheater identification in (t, n) secret sharing scheme," 2014.

[9] T.-C. Wu and T.-S. Wu, "Cheating detection and cheater identification in secret sharing schemes," *IEE Proceedings-Computers and Digital Techniques*, vol. 142, no. 5, pp. 367–369, 1995.

[10] J. Zhao, J. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," *Computer Standards & Interfaces*, vol. 29, no. 1, pp. 138–141, 2007.

[11] K. Kurosawa, S. Obana, and W. Ogata, "t-cheater identifiable (k, n) threshold secret sharing schemes," in *Annual International Cryptology Conference*. Springer, 1995, pp. 410–423.

[12] Y. Liu, "Linear (k, n) secret sharing scheme with cheating detection," *Security and Communication Networks*, vol. 9, no. 13, pp. 2115–2121, 2016.

[13] Y.-X. Liu, "Efficient t-cheater identifiable (k, n) secret-sharing scheme for $t \leq \left\lfloor \frac{k-2}{2} \right\rfloor$," *IET information security*, vol. 8, no. 1, pp. 37–41, 2014.

[14] K.-J. Tan, H.-W. Zhu, and S.-J. Gu, "Cheater identification in (t, n) threshold scheme," *Computer Communications*, vol. 22, no. 8, pp. 762–765, 1999.

[15] C. Sergio, P. Carles, and S. Germán, "Secret sharing schemes with detection of cheaters for a general access structure [j]," *Designs, Codes and Cryptography*, vol. 25, no. 2, pp. 175–188, 2002.

[16] C. Xing and C. Yuan, "Evolving secret sharing schemes based on polynomial evaluations and algebraic geometry codes," *IEEE Transactions on Information Theory*, vol. 70, no. 5, pp. 3718–3728, 2024.

[17] T. Mandal, S. Krishnaswamy, and R. Bhattacharjee, "A code-based threshold secret sharing scheme with cheating detection and cheater identification mechanisms," in *2026 National Conference on Communications (NCC)*. IEEE, 2026, pp. 162–167.

[18] Z. Ma, Y. Ma, X. Huang, M. Zhang, and Y. Liu, "Applying cheating identifiable secret sharing scheme in multimedia security," *EURASIP Journal on Image and Video Processing*, vol. 2020, no. 1, p. 42, 2020.

[19] S. Obana, "Almost optimum t-cheater identifiable secret sharing schemes," in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2011, pp. 284–302.

[20] A. Adhikari, K. Morozov, S. Obana, P. S. Roy, K. Sakurai, and R. Xu, "Efficient threshold secret sharing schemes secure against rushing cheaters," in *International conference on information theoretic security*. Springer, 2016, pp. 3–23.

[21] J. Stoer, R. Bulirsch, R. Bartels, W. Gautschi, and C. Witzgall, *Introduction to numerical analysis*. Springer, 1980, vol. 1993.