BAREKENG: Journal of Mathematics and Its Applications
September 2025 Volume 19 Issue 3 Page 1989-2002
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol19iss3pp1989-2002

SECURING INFORMATION CONFIDENTIALITY: A MATHEMATICAL APPROACH TO DETECTING CHEATING IN ASMUTH-BLOOM SECRET SHARING

Azhar Janjang Darmawan[1*], Sugi Guritman[2], Jaharuddin[3]

[1,2,3]*Department of Mathematics, Faculty of Mathematics and Natural Sciences, IPB University*
Jln. Meranti, IPB Dramaga Campus, Bogor, 16680, Indonesia

*Corresponding author's e-mail: *azhardarmawan.apps.ipb.ac.id*

Article History:

Received: 21st January 2025
Revised: 20th March 2025
Accepted: 8th April 2025
Published: 1st July 2025

Keywords:

Asmuth-Bloom;
Chinese Remainder Theorem;
Cryptography;
Mathematical algorithms;
Secret Sharing Scheme.

ABSTRACT

The Secret Sharing Scheme (SSS) based on the Chinese Remainder Theorem (CRT) is a crucial method for safeguarding confidential information. However, this scheme is vulnerable to collaborative cheating involving multiple participants. This study aims to modify the Asmuth-Bloom scheme by introducing two detection mechanisms: Threshold Range Detection and Detection Parameter Verification, to identify and prevent collaborative fraudulent activities. The research design is based on mathematical algorithms and tests the effectiveness of detection against predetermined cheating scenarios using structured parameters. The results indicate that the proposed modifications can accurately detect the manipulation of secret fragments, even in cases involving participant collusion. This robustness is achieved through the mathematical structure of the CRT, which enables the detection of inconsistencies during the secret reconstruction process. In addition to maintaining the efficiency of the original Asmuth-Bloom scheme, these modifications enhance the reliability of the scheme in protecting sensitive data. The study concludes that the implementation of dual detection mechanisms significantly strengthens the security of the SSS, particularly in applications prone to dishonest participant collaboration. Future research is recommended to explore computational efficiency and the implementation of this scheme in real-world environments, such as financial systems and blockchain technology.

How to cite this article:

A. J. Darmawan, S. Guritman and Jaharuddin., "SECURING INFORMATION CONFIDENTIALITY: A MATHEMATICAL APPROACH TO DETECTING CHEATING IN ASMUTH-BLOOM SECRET SHARING," *BAREKENG: J. Math. & App.*, vol. 19, no.. 3, pp. 1989-2002, September, 2025.

Journal homepage: *https://ojs3.unpatti.ac.id/index.php/barekeng/*
Journal e-mail: *barekeng.math@yahoo.com; barekeng.journal@mail.unpatti.ac.id*

Research Article · Open Access

1. INTRODUCTION

Mathematics plays a crucial role in supporting information security [1], [2], one of which is through the Secret Sharing Scheme (SSS) [3]–[5]. SSS is a method that divides confidential information into smaller parts (shares), which are then distributed among a number of participants [6], [7]. Through this approach, only a specific group of participants that meet the criteria in the access structure can reconstruct the secret, while others gain no information about it [8], [9]. One of the most popular variants of SSS is the threshold access structure, where a secret can be reconstructed if at least k out of n shares are combined [10], [11]. The mathematical approaches in SSS can be categorized into three main types: polynomial-based, hyperplane geometry-based, and Chinese Remainder Theorem (CRT)-based methods [12]–[14]. Among these approaches, this study focuses on CRT-based SSS, particularly the Asmuth-Bloom scheme. This scheme is renowned for its efficiency in dividing and reconstructing secrets using modulus numbers. Such an approach allows for more efficient and secure management of confidential data, making it attractive for various information security applications. Previous studies have examined the implementation of CRT-based SSS, including simulations and analyses of potential cheating in schemes such as the Mignotte (k, n) and Asmuth-Bloom (k, n) models. Researchers have shown that participants attempting to manipulate shares randomly often fail, as the reconstruction process still results in the correct secret [9], [15]. However, most of these studies focus on single-cheater scenarios, where only one participant attempts to manipulate the system. The identified gap lies in the lack of in-depth research on collaborative cheating scenarios, where multiple participants work together to deceive the system. Such collaboration among malicious participants is significantly more dangerous, as it increases the likelihood of successfully manipulating the secret and undermining the system's integrity. Moreover, effective fraud detection methods for these collaborative scenarios have not been systematically explored. Research on collaborative cheating involving multiple participants remains limited, despite its higher complexity and the substantial threats it poses.

The main gap lies in the lack of in-depth analysis of collaborative cheating and its impact on system integrity. In collaborative scenarios, multiple dishonest participants can work together to deceive others, thereby increasing the threat to system reliability [16], [17]. Moreover, effective cheating detection methods for such collaborative scenarios have yet to be extensively explored. This study shares some similarities with previous research but also offers significant distinctions. Like Chattopadhyay et al., this research discusses SSS methods to protect information confidentiality and address potential single-point-of-failure issues [13]. However, this study is more specific to the issue of cheating in CRT-based schemes. Compared to Ghamdi et al., this research not only addresses security improvements in secret sharing processes but also introduces a novel approach to detecting collaborative cheating [18]. In contrast to Hakeem & Kim, which focuses on key management in communication systems, this study modifies the (k, n)-Asmuth-Bloom scheme to detect cheating [19].

This research aims to broaden the understanding of cheating processes in CRT-based SSS, particularly in collaborative cheating scenarios. Additionally, it proposes modifications to the Asmuth-Bloom scheme to effectively detect cheating even when committed by multiple participants. By understanding the complexities of collaborative cheating and developing relevant detection methods, this study aims to enhance the reliability of SSS in information security applications. The main modification in the Asmuth-Bloom scheme lies in the structure of the initial value that is shared, known as the pre-share. In the original version of this scheme, the pre-share is formed by summing the secret with the product of a positive integer and an initial modulus value, denoted as m_0, which precedes the first element in the Asmuth-Bloom sequence (m_1). The value of m_0 is chosen such that it satisfies certain conditions related to the product of the moduli sequence used. In this context, the secret lies within a specific value space that is bounded by the ratio of the product of several moduli to the product of other selected moduli. In the modified scheme, the pre-share is restructured into a combination of the value A (representing the hidden secret), a positive integer gamma, a distinguishing parameter D, the initial modulus value m_0, and an additional random value r. All of these parameters are explained in detail in Section 3.1. This modification aims to enable the implementation of a cheating detection mechanism during the secret reconstruction process. One of the core mechanisms is the computation of a specific value, referred to as R, which is derived by manipulating the pre-shares received by the participants. This R value is used to identify inconsistencies or potential cheating that may arise from dishonest collaboration among participants. Additionally, this study introduces two supplementary mechanisms for fraud detection, namely Threshold Range Detection and Detection Parameter Verification. These mechanisms are designed to enhance the effectiveness of the scheme in identifying malicious behavior, including collusion. The modifications are applied starting from the pre-sharing phase, where the scheme is

constructed using a linear structure with additional verification parameters to ensure the integrity of the reconstructed secret.

During the reconstruction phase, the Threshold Range Detection method is used to verify whether the reconstruction result falls within a predetermined range, while Detection Parameter Verification evaluates parameter values against reference values established during the initial scheme design phase. Through this approach, any manipulation of secret shares by dishonest participants will result in mathematical inconsistencies that are detectable during the reconstruction phase. By addressing the complexities of collaborative cheating and developing effective detection mechanisms, this research aims to improve the reliability of the Asmuth-Bloom-based SSS in information security applications, especially in environments prone to manipulation by multiple actors. The uniqueness of this research lies in the development and expansion of the concept of cheating in CRT-based SSS, specifically involving more than one cheater. It also offers an innovative solution in the form of modifications to the (k, n)-Asmuth-Bloom scheme to detect and prevent collaborative cheating. The expected outcomes include the development of a robust cheating detection system against threats from collaborative dishonest participants, as well as enhanced data security protection in various fields such as banking, cryptography, and digital security applications. Thus, this research contributes both theoretically and practically to the literature on CRT-based SSS.

2. RESEARCH METHODS

This study employed an operational research design based on mathematical algorithms, focusing on the development and testing of a modified (k, n)-Asmuth-Bloom Secret Sharing Scheme (SSS) algorithm for cheating detection.

2.1 Asmuth-Bloom SSS

An (k, n)-Asmuth-Bloom Scheme uses a special sequence of integers, which in this paper will referred to as the (k, n)-Asmuth-Bloom's sequence. An (k, n)-Asmuth-Bloom's sequence m_j, $j \in \{0,1,\cdots,n\}$, with $n \leq 2; 2 \leq k \leq n$; and $m_0 < m_1 < m_2 < \cdots < m_k$, is a pairwise coprime integer which satisfies $m_0 \cdot \beta < \alpha$, with $\beta = \prod_{i=0}^{k-2} m_{n-i}$ and $\alpha = \prod_{i=1}^{k} m_i$.

Construction Phase

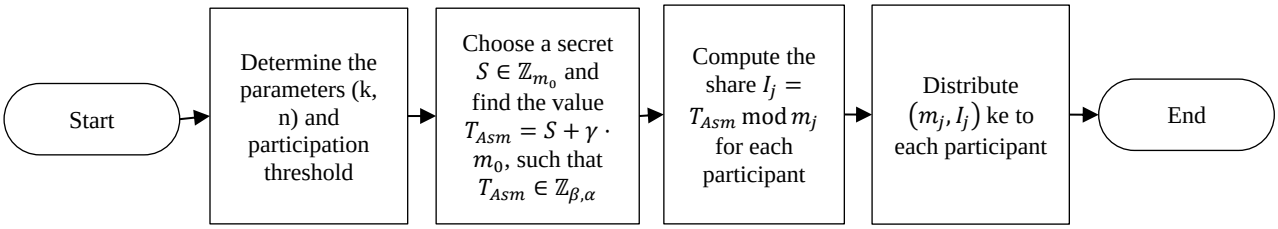

Figure 1. Construction Phase

The dealer performs the following operations:

Step 1. Generate an (k, n)-Asmuth-Bloom's sequence according to the number of participants n and the threshold k.

Step 2. Choose a secret $S \in \mathbb{Z}_{m_0}$; $\gamma \in \mathbb{Z}$ such that $T_{Asm} \in \mathbb{Z}_{\beta,\alpha}$, with $T_{Asm} = S + \gamma \cdot m_0$. In this paper:

a. the symbol T will referred to as *pre-share*

b. $\mathbb{Z}_{\beta,\alpha}$ is called threshold range, $T_{Asm} \in \mathbb{Z}_{\beta,\alpha}$ means $\beta < T_{Asm} < \alpha$

Step 3. Generating share I_j as $I_j = T_{Asm} \bmod m_j$

Step 4. Distribute pairs (m_j, I_j) to each j^{th}-participant

Reconstruction Phase

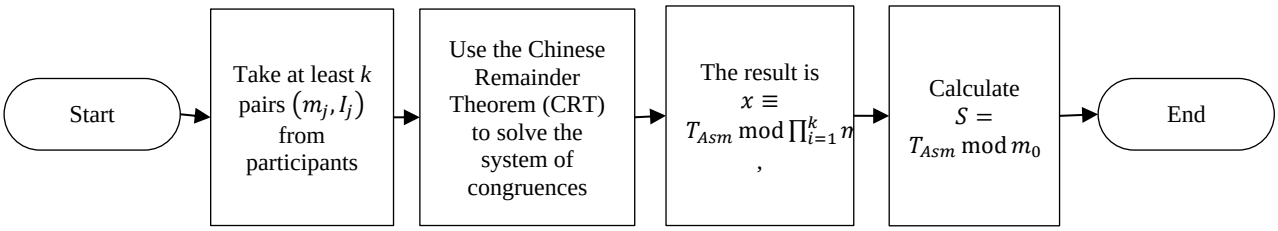

Figure 2. Reconstruction Phase

Suppose a group of k participants collect their pairs (m_j, I_j) to the combiner in order to recover/reconstruct the secret S. The combiner, then, performs the following operations:

Step 1. Computing the solution of the following system of congruences:

$$x \equiv I_{j_1} \bmod m_{j_1}$$
$$x \equiv I_{j_2} \bmod m_{j_2}$$
$$\vdots$$
$$x \equiv I_{j_k} \bmod m_{j_k}$$

using CRT, which gives the result x as $x \equiv T_{Asm} \bmod \prod_{i=1}^{k} m_{j_i}$,

Step 2. Obtaining the secret S as $S = T_{Asm} \bmod m_0$.

2.2 Cheating on CRT-Based (k, n)-Threshold Secret Sharing

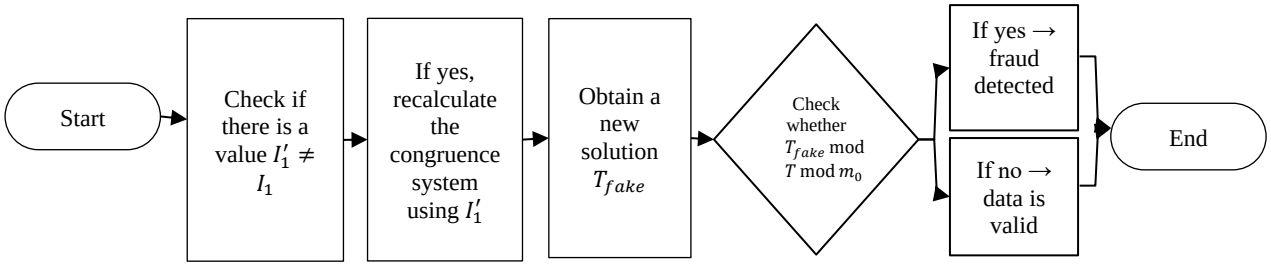

Figure 3. Cheating Detection Flow in Modified CRT-Based SSS

Suppose a group of k participants collect their pairs (m_j, I_j) in order to recover the secret S. If $I_j = T \bmod m_j$, with $T \in \mathbb{Z}_{\beta,\alpha}$ then, by using CRT a unique solution $x \in \mathbb{Z}_{m_1 \times \cdots \times m_k}$ can be obtained as a result of solving the system of congruences $x \equiv I_j \bmod m_j$ as $x \equiv T \bmod(\prod_{j=1}^{k} m_j)$. Pre-share T has the form $T = w\lambda + q$ with $w \in \mathbb{Z}_{m_1}$; $\lambda = \prod_{j=2}^{k} m_j$; and $q \in \mathbb{Z}_{m_2 \times \cdots \times m_k}$; with q is an unique solution of the system of congruences $x \equiv T \bmod(\prod_{j=2}^{k} m_j)$. Suppose $T' \bmod(\prod_{j=1}^{k} m_j)$, such that $T' \in \mathbb{Z}_{\beta,\alpha}$ and $T' \neq T$, are solutions to the system of congruences:

$$\begin{aligned} x &\equiv I_1' \bmod m_1 \\ x &\equiv I_2 \bmod m_2 \\ &\vdots \\ x &\equiv I_k \bmod m_k \end{aligned} \tag{1}$$

with $I_1' \neq I_1$. Similar to pre-share T, pre-share T' has the form $T' = w'\lambda + q$ such $w' \neq w$. Since $I_1' = T' \bmod m_1$, then $I_1' = (w'\lambda + q) \bmod m_1$. If we defined $w' = w + \delta$, $\delta \in \mathbb{Z}$ then we get $I_1' = [(w + \delta)\lambda + q] \bmod m_1 = (w\lambda + q + \delta\lambda) \bmod m_1 = (I_1 + \delta\lambda) \bmod m_1$.

It can be seen that in scenario of cheating on CRT-based SSS with one cheater, if we take for example participant-1 as a cheater, his share I_1 must be changed to I_1' with $I_1' = (I_1 + \delta\lambda) \bmod m_1$ so that a unique solution T' is obtained from reconstruction phase that deceives other honest participants.

The above scenario can be expanded to cheating scenario of c cheaters, with $c \geq 1$, to deceives $n - c$ honest participants. We defined:

1. $\Im_{\mathrm{D}} = \{I_{d_j}\},\ 1 \le j \le c$; with I_{d_j} as the share owned by the j-th cheaters.
2. $\mathcal{M}_{\mathrm{D}} = \{m_{d_j}\},\ 1 \le j \le c$; with m_{d_j} as the m owned by the j-th cheaters.
3. $\Im_{\mathrm{H}} = \{I_{h_j}\},\ 1 \le j \le k-c$; with I_{h_j} as the share owned by the j-th honest participants.
4. $\mathcal{M}_{\mathrm{H}} = \{m_{h_j}\},\ 1 \le j \le k-c$; with m_{h_j} as the m owned by the j-th honest participants.

Suppose a group of k participants collect their pairs (m_j, I_j) in order to recover the secret S, that c participants among them are cheaters, but the cheaters have not changet their shares I_{d_j}. The system of congruences constructed using the collected pairs (m_j, I_j) gives:

$$\begin{aligned} x &\equiv I_{d_1} \bmod m_{d_1} \\ &\vdots \\ x &\equiv I_{d_c} \bmod m_{d_c} \\ x &\equiv I_{h_1} \bmod m_{h_1} \\ &\vdots \\ x &\equiv I_{h_{k-c}} \bmod m_{h_{k-c}} \end{aligned} \tag{2}$$

with unique solutions $x \equiv T \bmod \left(\prod_{j=1}^{c} m_{d_j} \times \prod_{j=1}^{k-c} m_{h_j}\right)$ Pre-share T can be written in the form $T = w_D M_H + q$ with $w_D \in \mathbb{Z}_{m_{d_1} \times \cdots \times m_{d_c}}$; $M_H = \prod_{j=1}^{k-c} m_{h_j}$; and $q \in \mathbb{Z}_{M_H}$; with q is the unique solution of the system of congruences $x \equiv T \bmod m_{h_j}$. If the cheaters replace the shares $I_{d_1}, \cdots, I_{d_c}$ to $I'_{d_1}, \cdots, I'_{d_c}$such that $I_{d_j} \neq I'_{d_j},\ 1 \le j \le c$, then a system of congruences can be constructed as

$$\begin{aligned} x &\equiv I'_{d_1} \bmod m_{d_1} \\ &\vdots \\ x &\equiv I'_{d_c} \bmod m_{d_c} \\ x &\equiv I_{h_1} \bmod m_{h_1} \\ &\vdots \\ x &\equiv I_{h_{k-c}} \bmod m_{h_{k-c}} \text{ with a unique solution} \end{aligned} \tag{3}$$

$x \equiv T_{fake} \bmod \left(\prod_{j=1}^{c} m_{d_j} \times \prod_{j=1}^{k-c} m_{h_j}\right)$. T_{fake} can be written in the form $T_{fake} = w'_D M_H + q$ with $w'_D \in \mathbb{Z}_{m_{d_1} \times \cdots \times m_{d_c}}$; $w'_D \neq w_D$; $M_H = \prod_{j=1}^{k-c} m_{h_j}$; and $q \in \mathbb{Z}_{M_H}$. Since $I'_{d_j} = T_{fake} \bmod m_{d_j}$, then $I'_{d_j} = (w'_D M_H + q) \bmod m_j$. If we defined $w'_D = w_D + \delta$, $\delta \in \mathbb{Z}$ then we obtained

$$I'_{d_j} = [(w_D + \delta)M_H + q] \bmod m_{c_i} = (w_D M_H + q + \delta M_H) \bmod m_{d_j} = \left(I_{d_j} + \delta M_H\right) \bmod m_{d_j}.$$

Cheating is successful if the altered shares I'_{d_j} created by the cheaters lead the honest participants to reconstruct the false secret S_{fake} during the reconstruction phase. In the Asmuth-Bloom's SSS, cheating is successful if the reconstruction phase gives: (1) $T_{fake} \in \mathbb{Z}_{\beta,\alpha}$ and; (2) $S_{fake} \neq S$. Since in Asmuth-Bloom's SSS we defined $S = T \bmod m_0$, point (2) can be written as $T_{fake} \bmod m_0 \neq T \bmod m_0$. This could be satisified by choosing δ at $I'_{d_j} = \left(I_{d_j} + \delta M_H\right) \bmod m_{d_j}$ such that $T_{fake} \neq T + y m_0$, with $y \in \mathbb{Z}$.

2.3 Asmuth-Bloom Sequence Generator

We define:

1. d_1 as lower limit; d_2 as an upper limit; n as the sum of the numbers in a number sequence; n_{m_0} as the quantitiy of numbers m_0; and k as threshold; with all all of them are integers that satisfy $d_1 < d_2$ and $2 \le k \le n$
2. m_{init} as the largest number in a sequence of numbers as $m_{init} = d_2 - 1$.

3. L_{seq} as a set of sequences of pair-wise coprime integers
4. L_{pf} as a set of the prime factorization of L_{seq}
5. L_{m_0} as a set of possible values of m_0
6. m^* as a temporary integer before being inserted into L_{seq}.
7. m_0^* as a temporary integer before being inserted into L_{m_0}.
8. F_m^* as a temporary set of prime factors of m^*
9. $F_{m_0}^*$ as a temporary set of prime factors of m_0^*
10. r_1 and r_2 as a counter variable

Algorithm 1 Choose $d_1 d_1$, d_2, n and n_{m_0} that satisfies the above definition. The algorithm proceed as follows:

1. Set $m^* = m_{init}$.
2. Set $r_1 = 0$.
3. For $d_2 < m^*$, the loop is performed as follows:
   a. If $F_m^* \cap L_{pf} = \emptyset$, then $L_{pf} = L_{pf} \cup F_m^*$; $L_{seq} = L_{seq} \cup m^*$; and $r_1 = r_1 + 1$. If $F_m^* \cap L_{pf} \neq \emptyset$, proceed to the next step
   b. $m^* = m^* - 1$
   c. If $r_1 \not< n$, stop looping.
4. Check the truth of the statement $\beta < \alpha$:
   a. If $\beta < \alpha$, proceed to step e.
   b. If $\beta \not< \alpha$, repeat from step a with $d_2 = d_2 - 1$
5. Set $m_0^* = (\alpha/\beta) - 1$; with α and β obtained from data L_{seq} and k
6. Set $r_2 = 0$.
7. For $r_2 < n_{m_0}$, the loop is performed as follows:
   a. If $F_{m_0}^* \cap L_{pf} = \emptyset$, then $L_{m_0} = L_{m_0} \cup m_0^*$; and $r_2 = r_2 + 1$. If $F_{m_0}^* \cap L_{pf} \neq \emptyset$, proceed to the next step
   b. $m_0^* = m_0^* - 1$
   c. If $r_2 \not< n_{m_0}$, stop looping.
8. If $L_{m_0} = \emptyset$, repeat from step a with $d_2 = d_2 - 1$
9. If $L_{m_o} \neq \emptyset$, proceed to step j
10. L_{seq} is obtained as the set of Asmuth-Bloom sequences (k, n); L_{pf} as the set of prime factors; and m_0 is picked randomly from L_{m_0}.

3. RESULTS AND DISCUSSION

To support the claim of enhanced security against collaborative cheating, an initial test was conducted by comparing the secret reconstruction process between the original Asmuth-Bloom scheme and the modified scheme. Preliminary results show that in the original scheme, value manipulation by two participants can still produce a false secret without being detected. In contrast, the modified scheme successfully detects such alterations through a parameter verification method. This indicates an improvement in the effectiveness of fraud detection from the early stages of reconstruction.

3.1 The Proposed Scheme

Here, we present a proposed scheme as a form of modification of Asmuth-Bloom SSS in which contains cheating detection method.

Construction Phase

An (k, n)-Asmuth-Bloom's sequence is used by dealers in calculating pre-share T as:

$$T = A + \gamma \cdot D \cdot m_0 + r$$

such $T \in \mathbb{Z}_{\beta,\alpha}$ and $T \bmod m_0 \neq 0$. Such conditions are fulfilled by choosing A, γ, D, and r satisfy the following:

$A \in \{\beta + 1, \cdots, \alpha - 2(1 + m_0 + m_1)\}$;

$\gamma \in \left\{\frac{1 + m_1}{m_0} + 1, \cdots, \frac{\alpha - A}{2m_0} - 1\right\}$;

$r \in \{\gamma m_0 - m_1 + 1, \cdots, \gamma m_0 - 1\}$;

$D \in \left\{1, \cdots, \frac{\alpha - A + m_1}{\gamma m_0} - 2\right\}$.

After pre-share T is obtained, the dealer then constructs the shares I_j for each j-th participant, $1 \leq j \leq n$, using the formula:

$$I_j = T \bmod m_j$$

The constructed shares I_j are distributed to each j-th participant in the form of pairs (m_j, I_j). The proposed pre-share differs from the pre-share defined in the original Asmuth-Bloom scheme, which is in the form of $= S + \gamma \cdot m_0$. The advantage of the proposed pre-share is that it can be used to detect fraud/cheating in the fraud detection method implemented during the Reconstruction Phase.

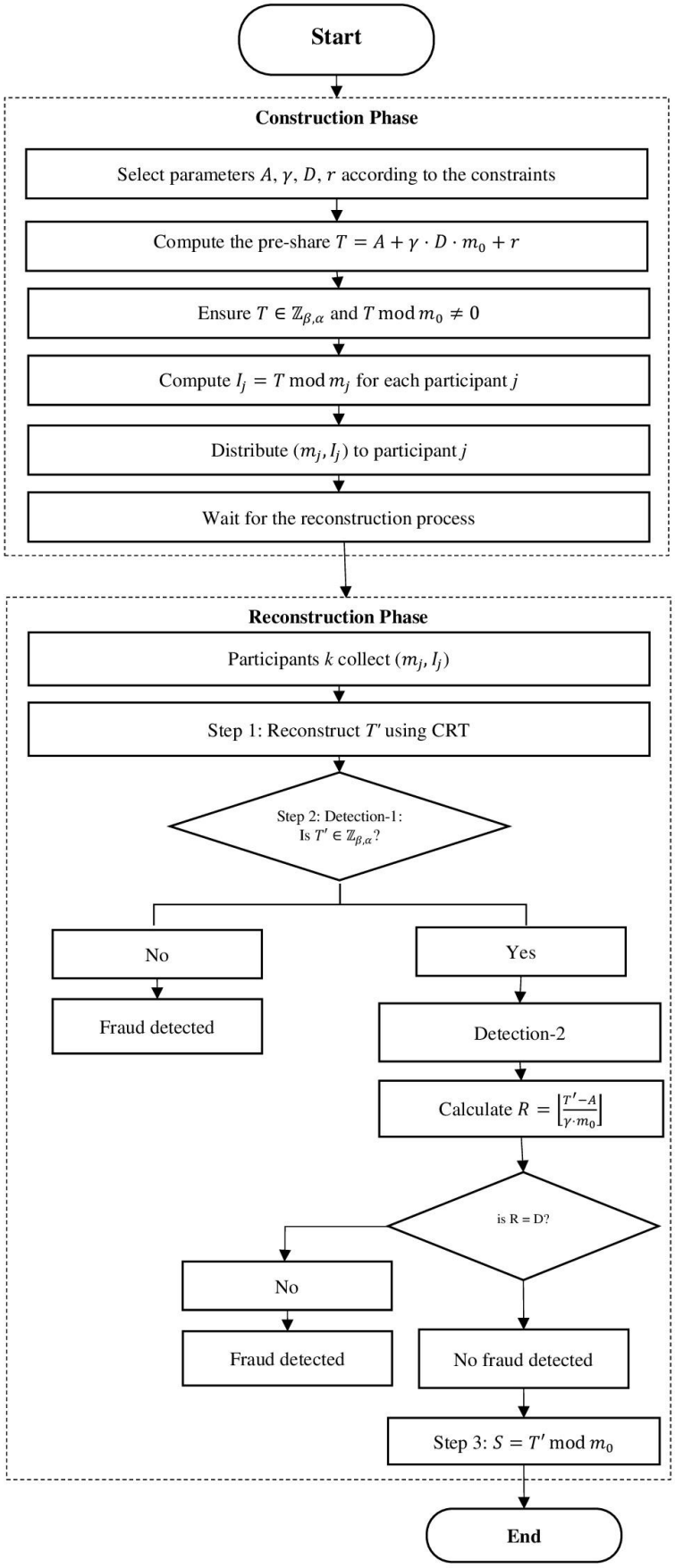

Figure 4. The Proposed Scheme

Reconstruction Phase

Suppose a group of k participants collect their pairs (m_j, I_j) to the combiner in order to recover/reconstruct the secret S. The combiner, then, performs the following operations:

Step 1. Computing the solution of the following system of congruence:

$$x \equiv I_{j_1} \bmod m_{j_1}$$
$$x \equiv I_{j_2} \bmod m_{j_2}$$
$$\vdots$$
$$x \equiv I_{j_k} \bmod m_{j_k}$$

using CRT, which gives the result x as $x \equiv T' \bmod \prod_{i=1}^{k} m_{j_i}$,

Step 2. Run cheating detection method as follows:

1. Detection-1 (Threshold Range Detection $\mathbb{Z}_{\beta,\alpha}$)
   a. Check whether the statement $T' \in \mathbb{Z}_{\beta,\alpha}$ is true.
   b. If it's not, then the cheating within the scheme is detected.
   c. If it's true, then there are two possibilities:
      i. no cheating occurs
      ii. cheatings occurred, but was not detected by Detection-1

   Therefore, the verification is continued to Detection-2.
2. Detection-2 (Detection Parameter Detection D)
   a. Check whether the statement $R = D$ is true, with $R = \left\lfloor \frac{T'-A}{\gamma \cdot m_0} \right\rfloor$.
   b. If $R \neq D$, then cheating is detected.
   c. If $R = D$, then there is no cheating occurs within the scheme.

Step 3. If there's no cheating, then the secret S is obtained as $S = T' \bmod m_0$.

3.2. Results

Experimental result of the study is presented as a numerical simulation of an Asmuth-Bloom's SSS being attacked by c cheaters simulated using Python programming. The simulation is executed with data input as $d_1 = 2^{15} = 32768$; $d_2 = 2^{16} = 65536$; $n = 20$; $k = 7$; $n_{m_0} = 10$.

Construction Phase

Given the data input, the dealer uses Algorithm 1 to generate an Asmuth-Bloom's sequence that gives:

1. L_{m_0} ={64913, 64919, 64921, 64927, 64937, 64943, 64949, 64951, 64963, 64969}. Then m_0 randomly chosen from L_{m_0} and assigned m_0 as $m_0 = 64913$.
2. L_{seq} ={65431, 65437, 65447, 65449, 65453, 65459, 65473, 65477, 65479, 65483, 65489, 65491, 65497, 65509, 65519, 65521, 65531, 655 33, 65534, 65535}
3. L_{pf} ={2, 3, 5, 7, 11, 13, 17, 19, 29, 31, 37, 41, 43, 59, 61, 67, 71, 79, 109, 151, 233, 257, 281, 601, 829, 977, 1109, 1523, 1597, 3449, 5953, 65437, 65447, 65449, 65479, 65497, 65519, 65521}
4. $\alpha = 514470955834865968431267159528421 1$
5. $\beta = 791761906563351192655498521 30$

Then, the dealer can choose A, γ, D and r as follows:

1. A =791761906563351192655498521 31

2. γ =39627119237733607
3. r =2572315191079001598475
4. D =285714285714

Given the data A, γ, D and r, pre-share T can be computed and gives T as $T = A + \gamma \cdot D \cdot m_0 + r$ =735026373643637026310321979555980; and the secret S as $S = T \bmod m_0 = 49702$.

The dealer then computes the share I_j for each j-th participant as $I_j = T \bmod m_j$. This gives a set of pairs (m_j, I_j) for each j-th participant as: L_{pair} ={(65431, 16455), (65437, 21684), (65447, 59316), (65449, 13238), (65453, 48209), (65459, 60987), (65473, 13291), (65477, 62855), (65479, 14465), (65483, 49006), (65489, 50455), (65491, 12286), (65497, 452), (65509, 40853), (65519, 13759), (65521, 16236), (65531, 27933), (65533, 43783), (65534, 8400), (65535, 43760)}.

Reconstruction Phase

Suppose a group of k participants collect their pairs (m_j, I_j) to the combiner in order to recover/reconstruct the secret S that the collected pairs is a set L_{pool} as L_{pool} ={ (65447, 59316), (65473, 13291), (65483, 49006), (65489, 50455), (65509, 40853), (65521, 16236), (65533, 43783)}. The combiner then compute the solution using CRT of the system of congruence composed by the collected pairs (m_j, I_j) as follows:

$$\begin{aligned} x &\equiv 59316 \bmod 65447 \\ x &\equiv 13291 \bmod 65473 \\ x &\equiv 49006 \bmod 65483 \\ x &\equiv 50455 \bmod 65489 \\ x &\equiv 40853 \bmod 65509 \\ x &\equiv 16236 \bmod 65521 \\ x &\equiv 43783 \bmod 65533 \end{aligned}$$

that gives the solution as T' =735026373643637026310321979555980. Next, the combiner compute the secret S' as $S' = T' \bmod m_0$ =49702.

Scenario of Cheating

Suppose that among k participants in L_{pool} there is a group of cheaters who owned pairs $(p_{d_1}, I_{d_1}), \cdots, (p_{d_c}, I_{d_c})$ as L_C ={(65447, 59316), (65489, 50455), (65509, 40853))}. Each of the cheaters can change their share $I_{d_j}$to I'_{d_j} as $I'_{d_j} = \left(I_{d_j} + \delta M_H\right) \bmod m_{d_j}$.

Given L_{pool} and L_C, M_H can be computed as $M_H = \prod_{j=1}^{k-c} m_{h_j} = \prod_{j=1}^{4} m_{h_j}$ = 65473×65483×65521×65533 = 18409049924610575087. By choosing δ =1458, the share $I'_{d_j}$for each cheater in the form of a pair (m, I) as L'_C = {(65447, 44212), (65489, 39668), (65509, 29782)}.

When cheaters execute the attack, the collection of pair L_{pool} changed to L'_{pool} as L'_{pool} ={(65447, 44212), (65473, 13291), (65483, 49006), (65489, 39668), (65509, 29782), (65521, 16236), (65533, 43783)}. A system of congruences composed by pair (m_j, I_j) from L'_{pool} gives:

$$\begin{aligned} x &\equiv 44212 \bmod 65447 \\ x &\equiv 13291 \bmod 65473 \\ x &\equiv 49006 \bmod 65483 \\ x &\equiv 39668 \bmod 65489 \\ x &\equiv 29782 \bmod 65509 \\ x &\equiv 16236 \bmod 65521 \\ x &\equiv 43783 \bmod 65533 \end{aligned}$$

which gives solution T'' =735026373670348557750931924007217.

With the obtained pre-share T'', the combiner can run cheating detection method as follows:

1. Detection-1 (Threshold Range Detection $\mathbb{Z}_{\beta,\alpha}$)

a. Check whether the statement $T'' \in \mathbb{Z}_{\beta,\alpha}$ is true

b. Check whether the statement $T'' \in \mathbb{Z}_{\beta,\alpha}$ $(\beta < T'' < \alpha)$ is true, given:

i. $\alpha = 514470955834865968431267159528 4211$

ii. $\beta = 791761906563351192655498521 30$

c. It can be seen that the statement $T'' \in \mathbb{Z}_{\beta,\alpha}$ is true, so the process continues to Detection-2.

2. Detection-2 (Detection Parameters Detection D)

a. Check whether the statement $R = D$ is true, with $R = \left\lfloor \frac{T''-A}{\gamma \cdot m_0} \right\rfloor$, given:

i. $A = 791761906563351192655498521 31$

ii. $\gamma = 39627119237733607$

iii. $m_0 = 64913$

iv. $D = 285714285714$

b. Therefore $R = \left\lfloor \frac{T''-A}{\gamma \cdot m_0} \right\rfloor$ =285714285725 $\neq D$ =285714285714, it can be concluded that cheating has occurred.

3.3 Discussion

It can be seen in simulation, that the act of cheating is prevented by the cheating detection method conducted by the combiner. Without such a method, honest participant can be fooled by retrieving the false secret $S'' = T'' \bmod m_0 = 10281$.In the proposed scheme, since $T = A + \gamma D m_0 + r \in \mathbb{Z}_{\beta,\alpha}$ then, as with the original Asmuth-Bloom's SSS, the secret S, with $S = T \bmod m_0$, is guaranteed to be: (1) obtainable from a secret reconstruction with data (m, I) from at least k participants; (2) not obtainable from a secret reconstruction with data (m, I) from fewer than k participants. However, compared to the original Asmuth-Bloom scheme, the proposed scheme demonstrates improvements in terms of security metrics, particularly in cheating detectability. This scheme significantly enhances the ability to detect manipulations of secret fragments, even when carried out collaboratively by multiple participants. Detection is performed through two stages: Threshold Range Detection and Detection Parameter Verification, which mathematically ensure that any deviation in the secret reconstruction result due to data manipulation can be identified. Consequently, the improved metrics include robustness against collusion, accuracy of fraud detection, and reliability of reconstruction, making the scheme more secure and dependable for real-world applications prone to participant collusion

Suppose there are $k-1$ participants gathers and perform secret reconstruction with their own pairs (m, I). Then, with CRT, a unique solution can be obtained in the form of $x'' = T'' \bmod (\prod_{j=1}^{k-1} m_{i_j})$. It is known that for k participants, secret reconstruction gives a unique solution in the form of $x = T \bmod (\prod_{j=1}^{k} m_{i_j})$ which follows the relation $x = \varepsilon \cdot \prod_{j=1}^{k-1} m_{i_j} + x''$. With the right value of ϵ, $\epsilon \in \mathbb{N}$, $k-1$ participants can obtain T. The value of ε is not fixed (non-unique) for each reconstruction involving $k-1$ participants, resulting in potentially different values of x. Therefore, information about T cannot be determined from the reconstruction with only $k-1$ participants. This reinforces the threshold property of the Asmuth-Bloom scheme, in which the secret can only be validly reconstructed if at least k participants are involved. However, it has been shown by Harn & Fuyou that the possibility of the value ϵ is greater than the possibility of the value S, so there is no information about S that can be obtained when $k-1$ participants perform secret reconstruction **[20]**.

An act of cheating in an Asmuth-Bloom's SSS will be successful if the cheaters knows the values m_0 and T. The pre-share value T can be obtained by knowing all the value of shares owned by each participant in a secret reconstrution session. It is impossible for cheaters to obtain m_0 in an Asmuth-Bloom's SSS other than using a random guess attack between the values 0 and $\frac{\alpha}{\beta}$.

If somehow the cheaters manages to obtain the values T and m_0, in the original Asmuth-Bloom's SSS, then the cheating can be carried out successfully as demonstrated by Pasailă et al. in their study. This does

not apply to the proposed scheme [21]. In the proposed scheme, since pre-share T has the form $T = A + \gamma D m_0 + r$ and since there exist a cheating detection method with Detection-2 in the form of $R = \left\lfloor \frac{T'-A}{\gamma \cdot m_0} \right\rfloor$, we can see that,

$$R = \left\lfloor \frac{T' - A}{\gamma \cdot m_0} \right\rfloor = \left\lfloor \frac{(T + y \cdot M_H) - A}{\gamma \cdot m_0} \right\rfloor = \left\lfloor D + \frac{r + y \cdot M_H}{\gamma \cdot m_0} \right\rfloor.$$

Since $r \in \{\gamma m_0 - m_1 + 1, \cdots \gamma m_0 - 1\}$; $y_{min} = 1$; and $M_{H_{min}} = m_1$, we obtain:

$$\frac{r + y \cdot M_H}{\gamma \cdot m_0} > 1 ;$$

so that

$$R \neq D$$

It is shown that with the parameters set in the proposed SSS the cheating detection method is guaranteed to detect cheating within scheme.

This study found that the modifications to the (*k*, *n*)-Threshold Secret Sharing Scheme (SSS) based on the Chinese Remainder Theorem (CRT) successfully detected cheating attempts, including collaborative cheating carried out by multiple participants. By integrating Threshold Range Detection and Detection Parameter Verification steps, the method demonstrated high accuracy in identifying cheating scenarios. Theoretically, these findings are supported by the fundamental principles of CRT, which enable the decomposition of secrets into unique interrelated fragments. Any alteration or manipulation of a single fragment can be detected through inconsistencies in the reconstructed secret. This aligns with modern cryptographic information security theories, which assert that the success of a secret sharing scheme relies on its resilience to manipulation by participants [21], [23]. Simulation experiments using numerical data showed that the system effectively prevents secret manipulation and the disclosure of false secrets, ensuring the scheme's reliability in safeguarding information confidentiality, even under the threat of participant collusion. The success of cheating detection in this study was influenced by careful parameter selection during the construction phase and the implementation of an effective algorithm for generating coprime numbers. Additionally, the use of precise Python simulations provided empirical validation for the proposed scheme. A deep understanding of the mathematical structure of the Chinese Remainder Theorem (CRT) was also a crucial factor in ensuring accurate cheating detection.

The primary advantage of this study is its development of an innovative and comprehensive cheating detection method, which includes scenarios involving collaboration among cheaters. The study also retained the efficiency of the original scheme while enhancing its security. However, the limitation lies in the added complexity of implementation, such as the need for additional parameter calculations, which may increase execution time in scenarios with a large number of participants. The findings of this study align with Chattopadhyay et al., which also discussed SSS methods for addressing single points of failure in systems [13]. However, this study differs by focusing on collaborative cheating detection, a topic not extensively covered in Chattopadhyay's research. The strength of the proposed method lies in the integration of two detection stages—Threshold Range Detection and Detection Parameter Verification—which enables the identification of manipulation even when carried out by multiple participants. This approach enhances the accuracy of fraud detection compared to conventional methods that rely solely on verifying the reconstructed secret values. Compared to Ghamdi et al., the approach in this study is broader, as it not only improves security during the secret sharing process but also incorporates a collaborative fraud detection mechanism, which has not been widely implemented in CRT-based schemes [18]. Furthermore, simulation results indicate that the modified algorithm maintains computational efficiency equivalent to the original Asmuth-Bloom scheme, while offering significant added verification capabilities. In contrast, Hakeem & Kim, focused on key management and authentication aspects in communication systems, whereas this study emphasizes modifying the mathematical structure of the Asmuth-Bloom scheme to prevent and detect fraud based on modulus value manipulation during secret reconstruction [19]. Therefore, the proposed method makes a tangible contribution to enhancing cryptographic security in scenarios involving participant collusion. This study provides a theoretical contribution by developing a robust cheating detection method resilient to collaboration among dishonest participants, thereby expanding the literature on CRT-based security schemes. Practically, the findings can be implemented in various fields, such as banking, cryptography, and other digital security applications, to enhance the protection of sensitive data. By integrating this cheating detection

method, SSS-based applications can improve their reliability and security in increasingly complex real-world scenarios.

4. CONCLUSIONS

This study concludes that cheating in Secret Sharing Schemes (SSS) based on the Chinese Remainder Theorem (CRT), particularly in cases involving collaboration among multiple malicious parties, is conducted by manipulating secret shares to reconstruct a false secret. The proposed modification to the Asmuth-Bloom SSS is capable of detecting and preventing collaborative cheating through two mechanisms: Threshold Range Detection and Detection Parameter Verification. The effectiveness of the scheme was validated through numerical simulations using Python and theoretical analysis of the CRT structure. Two key metrics were used: (a) the consistency of the pre-share reconstruction results with the initial parameters, and (b) parameter verification to identify any manipulation. In scenarios without cheating, the reconstruction results fall within the valid range and yield an integer when divided by the parameter m_0. In contrast, manipulations lead to deviations in the results, which are detected by the dual mechanisms. Simulations demonstrated that even if a manipulated reconstruction falls within the valid range (passing the first detection mechanism), parameter inconsistencies will be identified by the second mechanism. This highlights the system's resilience against collaborative manipulation, reinforced by the theoretical foundation of CRT, which guarantees the uniqueness of solutions in a system of congruences—making even minor alterations detectable. This mechanism enhances the reliability of CRT-based SSS in securing sensitive information without sacrificing efficiency. Future research may focus on optimizing computational efficiency and implementing this scheme in real-world systems such as financial transactions, distributed databases, or blockchain technology. Further analysis of alternative mathematical approaches in SSS could also expand contributions to cryptographic security.

ACKNOWLEDGMENT

Gratitude is extended to the Department of Mathematics, Faculty of Mathematics and Natural Sciences, IPB University, Indonesia, for the invaluable support and facilities provided during this research. Appreciation is also directed to the faculty members for their guidance and encouragement, which greatly contributed to the success of this study.

REFERENCES

[1] F. Tita, A. Setiawan, and B. Susanto, "CONSTRUCTION OF SUBSTITUTION BOX (S-BOX) BASED ON IRREDUCIBLE POLYNOMIALS ON GF(2^8)," *BAREKENG: Jurnal Ilmu Matematika dan Terapan*, vol. 18, no. 1, pp. 0517–0528, 2024, doi: https://doi.org/10.30598/barekengvol18iss1pp0517-0528.

[2] B. P. Tomasouw, G. E. Mado, and E. R. Persulessy, "MATRIKS SCORE DAN APLIKASINYA DALAM PENGAMANAN PESAN RAHASIA," *Barekeng: Jurnal Ilmu Matematika Dan Terapan*, vol. 12, no. 2, pp. 107–116, 2018, doi: https://doi.org/10.30598/vol12iss2pp107-116ar623.

[3] L. Harn, Z. Xia, C. Hsu, and Y. Liu, "SECRET SHARING WITH SECURE SECRET RECONSTRUCTION," *Information Sciences*, vol. 519, no. 1, pp. 1–8, 2020, doi: https://doi.org/10.1016/j.ins.2020.01.038.

[4] B. Parihar, M. Deshmukh, and A. S. Rawat, "EFFICIENT SINGLE SECRET IMAGE SHARING IN RESOURCE-CONSTRAINED ENVIRONMENT USING COUNTING-BASED SECRET SHARING OVER CLOUD," *Procedia Computer Science*, vol. 230, no. 1, pp. 158–167, 2023, doi: https://doi.org/10.1016/j.procs.2023.12.071.

[5] O. Ersoy, T. B. Pedersen, and E. Anarim, "HOMOMORPHIC EXTENSIONS OF CRT-BASED SECRET SHARING," *Discrete Applied Mathematics*, vol. 285, no. 1, pp. 317–329, 2020, doi: https://doi.org/10.1016/j.dam.2020.06.006.

[6] A. Alahmadi, A. Altassan, A. K. Al, S. Çalkavur, H. Shoaib, and P. Solé, "A MULTISECRET-SHARING SCHEME BASED ON LCD CODES," *Mathematics*, vol. 8, no. 2, pp. 1–10, 2020, doi: https://doi.org/10.3390/math8020272.

[7] Y. Sun, Y. Lu, J. Chen, W. Zhang, and X. Yan, "MEANINGFUL SECRET IMAGE SHARING SCHEME WITH HIGH VISUAL QUALITY BASED ON NATURAL STEGANOGRAPHY," *Mathematics*, vol. 8, no. 9, pp. 1–17, 2020, doi: 1 https://doi.org/10.3390/math8091452.

[8] S. Ali, J. Wang, and V. C. Ming Leung, "DEFENSIVE STRATEGIES AGAINST PCC ATTACKS BASED ON IDEAL (T,N)-SECRET SHARING SCHEME," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 9, p. 101784, 2023, doi: https://doi.org/10.1016/j.jksuci.2023.101784.

[9] S. Chhabra and A. K. Singh, "SECURITY ENHANCEMENT IN CLOUD ENVIRONMENT USING SECURE SECRET KEY SHARING," *Journal of Communications Software and Systems*, vol. 16, no. 3, pp. 296–307, 2020, doi: https://doi.org/10.24138/jcomss.v16i3.964.

[10] K. Shima and H. Doi, "HIERARCHICAL SECRET-SHARING SCHEME BASED ON XOR OPERATIONS," *Journal of Information Processing*, vol. 32, no. 1, pp. 719–730, 2024, doi: https://doi.org/10.2197/ipsjjip.32.719.

[11] R. Eriguchi and N. Kunihiro, "STRONG SECURITY OF LINEAR RAMP SECRET SHARING SCHEMES WITH GENERAL ACCESS STRUCTURES," *Information Processing Letters*, vol. 164, no. 1, pp. 1–9, 2020, doi: https://doi.org/10.1016/j.ipl.2020.106018.

[12] O. B. Chanu and A. Neelima, "A SURVEY PAPER ON SECRET IMAGE SHARING SCHEMES," *International Journal of Multimedia Information Retrieval*, vol. 8, no. 4, pp. 195–215, 2019, doi: https://doi.org/10.1007/s13735-018-0161-3.

[13] A. K. Chattopadhyay, S. Saha, A. Nag, and S. Nandi, "SECRET SHARING: A COMPREHENSIVE SURVEY, TAXONOMY AND APPLICATIONS," *Computer Science Review*, vol. 51, no. 1, pp. 1–22, 2024, doi: https://doi.org/10.1016/j.cosrev.2023.100608.

[14] A. Voudouris, A. Tressos, A. Zarras, and C. Xenakis, "GAME ON: A PERFORMANCE COMPARISON OF INTERPOLATION TECHNIQUES APPLIED TO SHAMIR'S SECRET SHARING," *The Computer Journal*, vol. 1, no. 1, pp. 1–12, 2024, [Online]. Available: https://watermark.silverchair.com/bxae109.pdf

[15] V. S. Lakshmi, S. Deepthi, and P. P. Deepthi, "COLLUSION RESISTANT SECRET SHARING SCHEME FOR SECURE DATA STORAGE AND PROCESSING OVER CLOUD," *Journal of Information Security and Applications*, vol. 60, no. 1, pp. 1–16, 2021, doi: https://doi.org/10.1016/j.jisa.2021.102869.

[16] S. Zhao, Z. Zeng, J. Peng, and F. Yu, "ACHIEVING A SECURE AND TRACEABLE HIGH-DEFINITION MULTIMEDIA DATA TRADING SCHEME BASED ON BLOCKCHAIN," *Mathematics*, vol. 11, no. 10, pp. 1–16, 2023, doi: https://doi.org/10.3390/math11102224.

[17] S. A. Bhat, N. F. Huang, I. B. Sofi, and M. Sultan, "AGRICULTURE-FOOD SUPPLY CHAIN MANAGEMENT BASED ON BLOCKCHAIN AND IOT: A NARRATIVE ON ENTERPRISE BLOCKCHAIN INTEROPERABILITY," *Agriculture (Switzerland)*, vol. 12, no. 1, pp. 1–25, 2022, doi: https://doi.org/10.3390/agriculture12010040.

[18] M. Al Ghamdi, M. Al Ghamdi, and A. Gutub, "SECURITY ENHANCEMENT OF SHARES GENERATION PROCESS FOR MULTIMEDIA COUNTING-BASED SECRET-SHARING TECHNIQUE," *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 16283–16310, 2019, doi: https://doi.org/10.1007/s11042-018-6977-2.

[19] S. A. A. Hakeem and H. Kim, "CENTRALIZED THRESHOLD KEY GENERATION PROTOCOL BASED ON SHAMIR SECRET SHARING AND HMAC AUTHENTICATION," *Sensors*, vol. 22, no. 1, pp. 1–25, 2022, doi: https://doi.org/10.3390/s22010331.

[20] L. Harn and M. Fuyou, "MULTILEVEL THRESHOLD SECRET SHARING BASED ON THE CHINESE REMAINDER THEOREM," *Information Processing Letters*, vol. 114, no. 9, pp. 504–509, 2014, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0020019014000659

[21] D. Pasailă, V. Alexa, and S. Iftene, "CHEATING DETECTION AND CHEATER IDENTIFICATION IN SECRET SHARING SCHEMES," *International Journal of Computing*, vol. 9, no. 2, pp. 107–117, 2010, doi: https://doi.org/10.47839/ijc.9.2.702.

[22] S. Saha, A. K. Chattopadhyay, A. K. Barman, A. Nag, and S. Nandi, "SECRET IMAGE SHARING SCHEMES: A COMPREHENSIVE SURVEY," *IEEE Access*, vol. 11, no. 1, pp. 98333–98361, 2023, doi: https://doi.org/10.1109/ACCESS.2023.33040555.

[23] O. S. Althobaiti and M. Dohler, "QUANTUM-RESISTANT CRYPTOGRAPHY FOR THE INTERNET OF THINGS BASED ON LOCATION-BASED LATTICES," *IEEE Access*, vol. 9, no. 1, pp. 133185–133203, 2021, doi: https://doi.org/10.1109/ACCESS.2021.3115087.