BAREKENG: Journal of Mathematics and Its Applications
December 2025 Volume 19 Issue 4 Page 2981–2992
P-ISSN: 1978-7227 E-ISSN: 2615-3017
https://doi.org/10.30598/barekengvol19iss4pp2981-2992

NEW SCHEME OF MIGNOTTE (t, n) COLLABORATIVE SECRET SHARING ON CLOUD STORAGE

Dhea Ekaputri[1*], **Sugi Guritman**[2], **Jaharuddin**[3]

[1,2,3]*Departement of Mathematics, School of Data Science, Mathematics, and Informatics, IPB University*
Jln. Dramaga, Kampus IPB Dramaga, Bogor, 16680, Indonesia

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

Article History:
Received: 29th March 2025
Revised: 21st April 2025
Accepted: 20th May 2025
Available online: 1st September 2025

Keywords:
Cheating detection;
Cloud storage;
Collaborative secret sharing;
Mignotte.

ABSTRACT

Cloud storage is an internet-based data storage service that allows users to collaborate to store, manage, and access data remotely. However, this collaborative characteristic creates challenges in security and privacy. One potential solution to these issues is implementing a collaborative secret sharing scheme. This research proposes a modified Mignotte (t, n) collaborative secret sharing scheme by introducing a detector parameter (r) to detect cheating. Additionally, the scheme is designed so that participants with multiple privileges only need to store a single share. The main contribution of this research is the integration of a cheating detection mechanism into the Mignotte (t, n) collaborative secret sharing scheme while maintaining storage efficiency. Experimental results show that the scheme produces correct outputs across various test cases. The proposed modification enhances the security of the secret sharing scheme for cloud storage applications by protecting against cheating and unauthorized access. However, the current scheme is limited to detection without identifying the cheater. Future research can focus on developing mechanisms for further identifying cheaters to enhance overall security.

How to cite this article:

D. Ekaputri, S. Guritman and Jaharuddin., "NEW SCHEME OF MIGNOTTE (t,n) COLLABORATIVE SECRET SHARING ON CLOUD STORAGE," *BAREKENG: J. Math. & App.,* vol. 19, iss. 4, pp. 2981-2992, December, 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

Cloud computing is a model that stores information permanently on cloud servers connected to the internet and temporarily on user computers [1]. One of the core facilities in cloud computing is cloud storage, which has a very large data storage capacity [2]. In the era of big data, cloud storage has a huge capacity due to the increasingly large data storage needs. Cloud storage provides many advantages, including the fact that stored data can be accessed from anywhere and anytime as long as an internet connection is available. However, data stored in cloud storage can be leaked and misused [3]. Thus, cloud storage requires high security to maintain the data stored in it.

Current cloud storage security methods are no longer adequate because, in the era of big data, cloud storage is vulnerable to unauthorized access and data theft [4]. To prevent data leakage, cloud storage users must be able to control access to data collaboratively [5]. Every user with a common interest can collaborate to secure the data stored in cloud storage. Cryptography is the main tool that can be used to maintain data security, such as ensuring confidentiality [6]. One of the cryptographic methods that can be used is the collaborative secret sharing scheme. In this scheme, the key management of a group is done jointly, and entities that do not trust each other can work together safely [7].

A secret sharing scheme is a security protocol that involves many participants in the formation of the secret key [8]. The secret sharing scheme (t,n), where t is the threshold and n is the number of participants, is a method that shares a secret to n participants, and the participants must work together to access it [9]. The secret sharing scheme (t,n) is a method where a secret is broken into n parts called shares so that the secret can only be reconstructed if there are at least t shares, while fewer than t shares do not provide any information about the secret [10]. In the secret sharing scheme (t,n), there is the term access structure. The access structure consists of all subsets that satisfy the conditions of P, i.e., Γ and subsets that do not satisfy the conditions of P, i.e., F [11], [12]. That is, if a group can recover the secret, then groups with more members than that group can also recover it [13].

Secret sharing schemes were first introduced by Shamir and Blakley separately in 1979 to protect their keys [14], [15], [16]. Shamir's (t,n) secret sharing scheme is based on the Lagrange polynomial interpolation method, while the scheme developed by Blakley is based on a geometric concept that utilizes the intersection of hyperplanes [17]. Another (t,n) secret sharing scheme is the one based on the Chinese Remainder Theorem (CRT) proposed separately by Mignotte [18] and Asmuth-Bloom [19]. The purpose of secret sharing schemes is to improve the security of data by ensuring that data can only be reconstructed if several legitimate participants combine their shares [20]. In secret sharing schemes, participants can cheat. Secret sharing schemes that include a cheating detection mechanism allow honest participants to detect cheating during the secret reconstruction process [21].

In line with these developments, the secret sharing (SS) scheme is relevant for securing data in cloud storage. However, since cloud storage is inherently collaborative, an adaptation of the scheme, known as collaborative secret sharing (CSS), is required. The CSS scheme in [9] is based on the Chinese Remainder Theorem (CRT), specifically the Asmuth-Bloom scheme. In this research, the scheme employed is the Mignotte scheme, which is also based on CRT. Furthermore, according to [21], a secret sharing scheme can be enhanced with a cheating detection mechanism to improve its security and reliability. Since the scheme referenced in [21] is not based on CRT, the cheating detection mechanism must be adapted to suit the characteristics of the Mignotte scheme. In this research, detection is performed using a detector parameter (r). Once successfully adapted, the detection mechanism is integrated into the Mignotte CSS scheme, resulting in a scheme that not only ensures security but is also capable of detecting cheating.

The collaborative secret sharing (CSS) scheme secures data stored in cloud storage using a key represented by a numerical value. This numerical value is then protected through the CSS scheme. Cloud storage users may be involved in multiple management groups. In the CSS scheme, users who are members of multiple management groups, referred to as multi-privileged participants, are required to store only a single share. A CSS scheme - $((t_1,n_1);\ (t_2,n_2))$, with the set of multi-privileged participants denoted by U, constitutes a collaborative scheme. It is assumed that the scheme (t_1,n_1) is reconstructed first and then the multi-privileged shares are passed to the dealer in scheme (t_2,n_2). The schemes (t_1,n_1) and (t_2,n_2) are independent. Accordingly, the main contribution of this research is the development of a Mignotte-based CSS scheme that supports storage efficiency by reducing the number of shares held by multi-privileged participants and incorporates a cheating detection mechanism to enhance its overall security and reliability.

2. RESEARCH METHODS

2.1 Chinese Remainder Theorem (CRT)

Suppose $k \geq 2, b_1, b_2, \ldots, b_k \in \mathbb{Z}$, and $m_1, m_2, \ldots, m_k$ are positive integers greater than or equal to 2 with $gcd(m_i, m_j) = 1$ for $1 \leq i, j \leq k$, then the system of congruent equations

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k}, \end{cases} \tag{1}$$

has a unique solution modulo M, with $M = m_1 m_2 \cdots m_k$, i.e.,

$$x = \left(\sum_{i=1}^{n} a_i t_i M_i \right) (\bmod M), \tag{2}$$

with $M_i = \frac{M}{m_i}$, $M_i M_i^{-1} \equiv 1 \pmod{m_i}$ for $i = 1, 2, \ldots, n$ [22].

The inverse of M_i can be found using the extended Euclidean [23]. Suppose positive integers a and b with $a > b$, it is known that $gcd(a, b) = s_n a + t_n b$ for $n = 0,1,2, \ldots$ where s_n and t_n are the nth terms defined recursively by

$$s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1$$

$$s_j = s_{j-2} - q_{j-1}.s_{j-1}, t_j = t_{j-2} - q_{j-1}.t_{j-1}, j \geq 2.$$

To ensure M_i has an inverse, the Greatest Common Divisor (GCD) of M_i and p_i must be 1. The GCD of two numbers can be found using Euclidean [24]. Suppose a and b are two integers, to find $gcd\ (a, b)$ with $a \geq b > 0$, then the following steps can be applied.

$$\begin{aligned} a &= q_1 b + r_1 && 0 < r_1 < b \\ b &= q_2 r_1 + r_2 && 0 < r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 && 0 < r_3 < r_2 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0, \end{aligned}$$

with q_i the quotient and r_i the remainder for $i = 1,2, \ldots, n$. The last non-zero remainder, r_n, is $gcd(a, b)$.

2.2 Mignotte (k, n) Secret Sharing Scheme

The Mignotte (k, n) secret sharing scheme uses a sequence of positive integers called the Mignotte sequence [18]. The Mignotte sequence (k, n) with $n \geq 2, 2 \leq k \leq n$, $n \in \mathbb{Z}$, is defined as a sequence of coprime pairs or relative primes of positive integers $p_1 < p_2 < \cdots < p_n$ such that

$$\prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^{k} p_i.$$

Suppose given a Mignotte sequence (k, n), then the Mignotte secret sharing scheme is as follows:

1. The secret S is chosen as a random integer with $\alpha < S < \beta$, with $\alpha = \prod_{i=0}^{k-2} p_{n-i}$ and $\beta = \prod_{i=1}^{k} p_i$.
2. Shares i for each $1 \leq i \leq n$ are counted as $I_i \equiv S \pmod{p_i}$.

   If k shares are collected, then the secret S can be reconstructed using CRT.

2.3 Collaborative Secret Sharing Scheme

Suppose the secret sharing scheme (t_1, n_1) with the set of participants $P_1 = \{P_1^1, \dots, P_{n_1}^1\}$ is used to share the secret s_1. Then, the secret sharing scheme (t_2, n_2) with the set of participants $P_2 = \{P_1^2, \dots, P_{n_2}^2\}$ is used to share the secret s_2. A collaborative secret sharing scheme $((t_1, n_1);(t_2, n_2))$ with multi-privilege participant U, $U = P_1 \cap P_2 = \{P_1^{2,1}, \dots, P_u^{2,1}\}$ and $|U| = u$, if the following two conditions are met [9].

1. For each $A \subseteq P_1$ and $|A| \geq t_1, H(s_1|S_A) = 0$; for each $A \subseteq P_2$ and $|A| \geq t_2, H(s_2|S_A) = 0$, where $H(s_1|S_A)$ and $H(s_2|S_A)$ are conditional entropies.
2. For each $A \subseteq P_1 \cup P_2$ and $|A \cap P_1| < t_1$, $H(s_1|S_A) = H(s_1) > 0$; for each $A \subseteq P_1 \cup P_2$ and $|A \cap P_2| < t_2$, $H(s_2|S_A) = H(s_2) > 0$, where $H(s_1|S_A)$ and $H(s_2|S_A)$ are conditional entropies.

One collaborative secret sharing scheme is a CRT-based scheme, namely the Mignotte (t, n) collaborative secret sharing scheme. The Mignotte (t, n) collaborative secret sharing scheme consists of two stages, namely the distribution phase and reconstruction phase. In the distribution phase, the dealer determines the Mignotte sequence. The Mignotte sequence is determined based on the distance between the values $\alpha = \prod_{i=0}^{k-2} p_{n-i}$ and $\beta = \prod_{i=1}^{k} p_i$ which are very far apart, which are primes in the interval $(p_t^{\frac{k^2-1}{k^2}}, p_t]$ such that $\frac{(\beta-\alpha)}{\alpha} \geq p_t^{\frac{k-1}{k}} - 1$ [25]. To ensure that the number of prime numbers contained in the interval is sufficient to build the desired scheme, calculations can be made using the Prime Number Theorem [26]. The secret chosen is between α and β, i.e., $\alpha < s < \beta$.

3. RESULTS AND DISCUSSION

Mignotte scheme [18] is modified to detect possible cheating by adding a detector parameter (r).

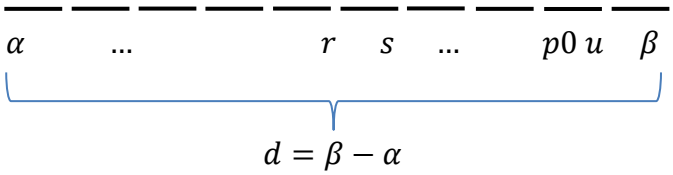

Figure 1. Detector Parameter Selection (r)

Figure 1 illustrates the concept of selecting the detector parameter (r) used to enable cheating detection. The detector parameter algorithm is defined as follows:

1. Compute $\alpha = \prod_{i=0}^{t-1} p_{n-i+1}$ and $\beta = \prod_{i=1}^{t} p_i$, with the condition that $\alpha < \beta$.
2. Compute $d = \beta - \alpha$.
3. Compute $u = \lfloor \sqrt{d} \rfloor$.
4. Determine $p0$, where $p0$ is the largest prime number less than u.
5. Randomly select the detector parameter (r) and the secret (s) from the interval $[0, \dots, p0 - 1]$.
6. Compute the value of S as $S = (\beta + (r \times p0) + s)$.

The detector parameter (r) in the Mignotte scheme is randomly selected within a specific range determined based on the value of $p0$. The value S is then constructed by embedding the detector parameter (r) and the secret (s) into a mathematical structure that enables the system to verify its authenticity and consistency. If the resulting value of S does not match the expected outcome, it leads to a different value of r, thereby indicating the presence of cheating.

Each dealer determines the secret differently from Mignotte [18] and distributes shares to each participant. Subsequently, during the secret reconstruction phase, the collected shares form a system of congruence equations. The secret is recovered by solving this system using the Chinese Remainder Theorem (CRT). Once the scheme is constructed, it can be implemented to improve cloud storage security.

3.1 Modified Mignotte (t, n) Collaborative Secret Sharing Scheme

1. Distribution Phase

   The steps for the distribution phase in the CSS Scheme - $((t_1, n_1); (t_1, n_1); \ldots; (t_l, n_l))$ with multi-privileged participant U, where $2 \leq t_i \leq n_i$, are as follows:

   a. Dealer 1 generates a Mignotte sequence $p_{1,1} < p_{2,1} < \cdots < p_{n_{1,1}}$ such that $\alpha_1 = \prod_{i=1}^{t_1-1} p_{n_1-i+1,1} < \prod_{i=1}^{t_1} p_{i,1} = \beta_1$. Security is ensured if the prime numbers are chosen such that the value of $\frac{\beta-\alpha}{\alpha}$ is significantly large, where the selected primes fall within the interval $(p_k^{\frac{t^2-1}{t^2}}, p_k]$, p_k is an integer [25]. The coprime sequence is necessary to ensure that **Equation (1)** and **Equation (2)** can be used during secret reconstruction and a unique solution is obtained.

   b. Dealer 1 calculates $d_1 = \beta_1 - \alpha_1, u_1 = \lfloor \sqrt{d_1} \rfloor$, $p0_1$ as the prime number preceding u_1, and selects a detector parameter (r_1) and determines the secret (s_1) as a random number in the $[0, \ldots, p0_1 - 1]$.

   c. Dealer 1 determines $S_1 = \alpha_1 + (r_1 \times p0_1) + s_1$. The shares for participants in P_1 are given by $S_{i,1} \equiv S_1 \pmod{p_{i,1}}$. Dealer 1 distributes the shares $I_i = (S_{i,1}, p_{i,1})$ to n_1 participants in P_1 and determines $u_{i,1}$ multi-privileged shares, denoted as $\{S_1^{i,1}, S_2^{i,1}, \ldots, S_{u_{i,1}}^{i,1}\}$. The index in $S_1^{i,j}$ indicates that the share originates from dealer j and is assigned to dealer i as the first participant. Then, dealer 1 forwards these multi-privileged shares to dealer i for $i \in \{2,3,4, \ldots, l\}$.

   d. Dealer i receives multiple privilege shares $\{S_1^{i,j}, S_2^{i,j}, \ldots, S_{u_{i,j}}^{i,j}\}$ from dealer j, where $j \in \{1,1, \ldots, i-1\}$ and $i \in \{3,4, \ldots, l\}$, with the condition that $u_{i,1} + u_{i,2} + \cdots + u_{i,j} < t_i$. Here, $u_{i,j}$ denotes the number of multi privileged participants associated with dealer i from dealer j, for each $j = 1,2, \ldots, i-1$. By receiving these multi-privileged shares, the multi-privileged participants within the set P_i are not required to obtain new shares. Therefore, each multi-privileged participant only needs to hold a single share. Dealer i generates a Mignotte sequence, satisfying the ordering $p_{1,i} < p_{2,i} < \cdots < p_{u_{i,1}+u_{i,2}+\cdots+u_{i,j},i} < \cdots < p_{n_{2,i}}$, such that $\prod_{j=1}^{t_i-1} p_{n_i-j+1,2} < \prod_{i=1}^{t_i} p_{j,2}$.

   e. Dealer i selects $S_{u_{i,1}+u_{i,2}+\cdots+u_{i,j}+1,i}, S_{u_{i,1}+u_{i,2}+\cdots+u_{i,j}+2,i}, \ldots, S_{t_i,i}$, subject to the condition that $S_{u_{i,1}+u_{i,2}+\cdots+u_{i,j}+k,i} \in \mathbb{Z}_{p_{u_{i,1}+u_{i,2}+\cdots+u_{i,j}+k,i}}$, for each $k = 1, \ldots, t_i - (u_{i,1} + u_{i,2} + \cdots + u_{i,j})$. $S_{i,j}$ is the share for the i-th participant in P_j. Then, S_i is determined by solving the following system of congruent equations using the Chinese Remainder Theorem (CRT).

$$\begin{cases} \left.\begin{array}{c} S_i \equiv S_1^{i,1}(S_{1,i}) \bmod p_{1,i}, \\ \vdots \\ S_i \equiv S_{u_{i,1}}^{i,1}(S_{u_{i,1},i}) \bmod p_{u_{i,1},i}, \end{array}\right\} U_{i,1}, \\ \left.\begin{array}{c} S_i \equiv S_1^{i,2}(S_{u_{i,1}+1,i}) \bmod p_{u_{i,1}+1,i}, \\ \vdots \\ S_i \equiv S_{u_{i,2}}^{i,2}(S_{u_{i,1}+u_{i,2},i}) \bmod p_{u_{i,1}+u_{i,2},i}, \end{array}\right\} U_{i,2}, \\ \left.\begin{array}{c} S_i \equiv S_1^{i,j}\left(S_{u_{i,1}+u_{i,2}+\cdots+u_{i,j-1}+1,i}\right) \bmod p_{S_{u_{i,1}+u_{i,2}+\cdots+u_{i,j-1}+1,i}}, \\ \vdots \\ S_i \equiv S_{u_{i,j}}^{i,j}\left(S_{u_{i,1}+u_{i,2}+\cdots+u_{i,j},i}\right) \bmod p_{u_{i,1}+u_{i,2}+\cdots+u_{i,j},i}, \\ \vdots \\ S_i \equiv S_{t_i,i} \bmod p_{t_i,i}. \end{array}\right\} \begin{array}{c} U_{i,j}, \\ 3 \leq j \end{array} \end{cases}$$

   $U_{i,j}$ is a multi-privileged participant of scheme j for scheme i. The multi-privileged participants of each scheme are ordered in ascending order based on index j and the order of participants within the set $U_{i,j}$.

f. Dealer i calculates $\alpha_i = \prod_{i=1}^{t_1-1} p_{n_1-i+1,1}$ and $\beta_i = \prod_{i=1}^{t_1} p_{i,1}$. Then the dealer computes $d_i = \beta_i - \alpha_i, u_i = \lfloor\sqrt{d_i}\rfloor$ and $p0_i$. Next, dealer i determines the detector parameter (r_i) and the secret (s_i) as elements of the set $[0, \dots, p0_i - 1]$ such that $S_i = \alpha_i + (r_i \times p0_i) + s_i$. The value of r_i is obtained by computing $r_i = \left\lfloor\frac{S_i-\alpha_i}{p0_i}\right\rfloor$, ensuring that r_i always belongs to the set $[0, \dots, p0_i - 1]$. Once r_i is determined, the value of s_i can be computed as $s_i = S_i - \alpha_i - (r_i \times p0_i)$.

g. Dealer i determines the shares for other participants in P_i as follows:

$$S_{k,i} \equiv s_i \bmod p_{k,i},$$

for $k = t_i + 1, t_i + 2, \dots, n_i$. Dealer i distributes the shares $I_k = (S_{k,i}, p_{k,i})$ to n_i participants in P_i for $k = 1, 2, \dots, n_i$ and multi-privileged shares, totaling $u_{j,i}$, denoted as $\{S_1^{j,i}, S_2^{j,i}, \dots, S_{u_{j,i}}^{j,i}\}$, are distributed to dealer j for $j = i + 1, i + 2, \dots, l$.

2. Reconstruction Phase

a. Suppose at least $k_i \geq t_i$ shares are collected from the participants in P_i. The collected shares form a system of congruent equations whose solution can be determined using the Chinese Remainder Theorem (CRT). Let the solution obtained from solving this system of congruent equations be denoted as S_i'.

b. The value R_i is then computed as $R_i = \left\lfloor\frac{S_i'-\alpha_i}{p0_i}\right\rfloor$. This value R_i is used to determine whether cheating has occurred.

c. If $R_i = r_i$, then no cheating has occurred, and the secret can be reconstructed as $s_i = S_i' - \alpha_i - (r_i \times p0_i)$. Conversely, if $R_i \neq r_i$, then cheating has been detected.

Remark 1. In step 6 of the distribution phase, the value r_i is guaranteed to be an element of the set $[0, \dots, p0_i - 1]$. Given that $\left\lfloor\frac{S_i-\alpha_i}{p0_i}\right\rfloor = r_i$, based on the definition of the floor function, this equation can be rewritten as the inequality $r_i \leq \frac{S_i-\alpha_i}{p0_i} < r_i + 1$. Suppose $r_i \geq p0_i$, then obtain $p0_i \leq \frac{S_i-\alpha_i}{p0_i} < p0_i + 1$. From the left-hand side of the inequality, we obtained $p0_i \leq \frac{S_i-\alpha_i}{p0_i}$. Multiplying both sides by $p0_i$, gives ${p0_i}^2 \leq S_i - \alpha_i$. Thus, if $r_i \geq p0_i$, then $S_i - \alpha_i \geq {p0_i}^2$. However, this result contradicts the prior selection of $p0_i$. The value $p0_i$ is chosen as the largest prime number before $\lfloor\sqrt{d_i}\rfloor$, where $d_i = \beta_i - \alpha_i$. This means that $p0_i < \lfloor\sqrt{d_i}\rfloor$, but its value is nearly equal. It can be assumed that ${p0_i}^2 \approx d$. In the Mignotte scheme $\alpha_i < S_i < \beta_i$, which implies $S_i - \alpha_i < \beta_i - \alpha_i = d_i \approx {p0_i}^2$. Therefore, $S_i - \alpha_i < {p0_i}^2$. Since our assumption leads to a contradiction, it must be false. Consequently, we conclude that $0 \leq r_i < p0_i$, where r_i is an element of the set $[0, \dots, p0_i - 1]$.

Remark 2. In step 6 of the distribution phase, the value s_i is automatically a member of the set $[0, \dots, p0_i - 1]$. Given that $\left\lfloor\frac{S_i-\alpha_i}{p0_i}\right\rfloor = r_i$, by the definition of the floor function, this equation can be rewritten as the inequality $r_i \leq \frac{S_i-\alpha_i}{p0_i} < r_i + 1$. Multiplying both sides by $p0_i$ gives $r_i \times p0_i \leq S_i - \alpha_i < (r_i + 1) \times p0_i$. From this, we obtained:

$$S_i - \alpha_i < (r_i + 1) \times p0_i$$
$$S_i - \alpha_i < (r_i \times p0_i) + p0_i$$
$$0 \leq S_i - \alpha_i - (r_i \times p0_i) < p0_i.$$

Since it is known that $s_i = S_i - \alpha_i - (r_i \times p0_i)$, so that $0 \leq s_i < p0_i$. Thus, this can conclude that $0 \leq s_i < p0_i$, with s_i belonging to the set $[0, \dots, p0_i - 1]$.

Remark 3. In step 2 of the reconstruction phase, the value R_i can be used to determine whether cheating has occurred. From the equation $S_i = \alpha_i + (r_i \times p0_i) + s_i$, we obtained $r_i = \frac{S_i-\alpha_i-s_i}{p0_i}$. This formula indicates that the difference $S_i - \alpha_i - s_i$ must be a multiple of $p0_i$, as the result of the division must be an integer. Mathematically, this can be expressed as:

$$(S_i - \alpha_i - s_i) \bmod p0_i \equiv 0.$$

Assuming that $s_i < p0_i$, it follows that $\frac{s_i}{p0_i} < 1$. The floor operation applied to the expression $\frac{S_i-\alpha_i-s_i+s_i}{p0_i}$ will yield the same result as r_i. Therefore, the computation of the value

$$r_i = \frac{S_i - \alpha_i - s_i}{p0_i} = \left\lfloor \frac{S_i - \alpha_i - s_i + s_i}{p0_i} \right\rfloor = \left\lfloor \frac{S_i - \alpha_i}{p0_i} \right\rfloor.$$

The calculation of the value $R_i = \left\lfloor \frac{s_i' - \alpha_i}{p0_i} \right\rfloor$ performed during the reconstruction process will yield a result identical to r_i if no data manipulation has occurred. Any discrepancy between R_i and r_i can be used as an indicator of cheating.

3.2 Simple Case Study Implementation: Cloud Storage

A user uploads data to cloud storage. First, the data is encrypted using a primary encryption key (s). The primary key is then divided into n shares using the Mignotte (t, n) scheme. These shares are distributed among various authorized authorities. The cloud storage only stores the encrypted data and never has access to the primary encryption key. When the user wants to access the stored data, they must request the reconstruction of the encryption key by collecting at least t shares from the relevant authorities. If the required number of shares is obtained, the encryption key can be reconstructed, allowing the data to be decrypted. However, if the number of shares is insufficient, access to the data is denied.

Mignotte's (t, n) collaborative secret sharing scheme can be implemented in real life to maintain the confidentiality of data or information stored in cloud storage. Suppose there is a technology company that handles sensitive documents, including financial data, business strategies, and customer information. These documents will be stored in encrypted form in cloud storage and secured using the Mignotte scheme (t, n). There are three main keys with different access: key A provides access to financial documents, key B provides access to business strategies, and key C provides access to customer information. Key A is secured using the Mignotte scheme (3,7), key B using the Mignotte scheme (4,7), and key C using the Mignotte scheme (5,8). Additionally, there are multi-privileged participants, who are individuals who hold high-ranking positions within the company. The structure of participants and their respective access rights are shown in **Table 1** below:

Table 1. Participant Structure and Access Right

Participant	Participant Key A	Participant Key B	Participant Key C
CEO	✓	✓	✓
CFO	✓		
CTO		✓	
CIO		✓	✓
COO	✓		
Finance Manager	✓		
Marketing Manager	✓	✓	
AI Researcher			✓
IT Team		✓	
Sales Engineer		✓	
Digital Marketing Specialist		✓	✓
Finance Analyst	✓		
Operations Manager	✓		
Data Analyst			✓
Customer Success Manager			✓
Sales Representative			✓
Database Administrator			✓

In **Table 1**, the checkmark (✓) indicates that the participant is included in the scheme corresponding to the column where the mark is placed. In this scheme, three keys need to be secured. Therefore, the share construction process will be carried out in three stages. The steps for the given illustration are as follows.

Step 1: Shares distribution for the (3,7) scheme.

Key Management System (KMS) 1 generates the Mignotte sequence $p_{1,1} = 359,\ p_{2,1} = 367, p_{3,1} = 373, p_{4,1} = 379, p_{5,1} = 383, p_{6,1} = 389, p_{7,1} = 397$. From this sequence, the values $\alpha_1 = 154433$ and $\beta_1 = 49143869$ are obtained. Through further calculations, the following values are derived: $d_1 = 48989436, u_1 = 6999, p0_1 = 6997$. Given a detector parameter $r_1 = 5798$ and a secret $s_1 = 4275$, the computed value of S_1 is 40727314. Next, the shares to be distributed to participants in P_1 are calculated as follows.

$$S_{1,1} = 40727314 (\text{mod } 359) \equiv 200 (\text{mod } 359)$$
$$S_{2,1} = 40727314 (\text{mod } 367) \equiv 223 (\text{mod } 367)$$
$$S_{3,1} = 40727314 (\text{mod } 373) \equiv 190 (\text{mod } 373)$$
$$S_{4,1} = 40727314 (\text{mod } 379) \equiv 353 (\text{mod } 379)$$
$$S_{5,1} = 40727314 (\text{mod } 383) \equiv 243 (\text{mod } 383)$$
$$S_{6,1} = 40727314 (\text{mod } 389) \equiv 181 (\text{mod } 389)$$
$$S_{7,1} = 40727314 (\text{mod } 397) \equiv 275 (\text{mod } 397).$$

The shares distributed to the participants in P_1 are $I_{1,1} = (200, 359), I_{2,1} = (223, 367), I_{3,1} = (190,373), I_{4,1} = (353,379), I_{5,1} = (243,383), I_{6,1} = (181,389), I_{7,1} = (275,397)$. Additionally, multi-privileged shares are given to KMS 2, namely $S_1^{2,1} = 200, S_2^{2,1} = 243$ and KMS 3, namely $S_1^{3,1} = 200$.

Step 2: Shares distribution for the (4,7) scheme.

KMS 2 generates the Mignotte sequence $p_{1,2} = 419,\ p_{2,2} = 421, p_{3,2} = 431, p_{4,2} = 433, p_{5,2} = 439, p_{6,2} = 443, p_{7,2} = 449$. Next, KMS 2 determines the shares for participants 3 and 4, namely $S_{3,2} = 267$ and $S_{4,2} = 335$. Then, KMS 2 computes S_2 by solving the system of congruent equations that has been formed. The calculations proceed as follows:

$$M = 32920110577,$$
$$M_1 = 78568283, M_2 = 78195037, M_3 = 76380767, M_4 = 76027969,$$
$$M_1^{-1} = 106, M_2^{-1} = 107, M_3^{-1} = 88, M_4^{-1} = 125.$$

As a result, KMS 2 obtains $S_2 = 19121378193$. The next calculation process, obtained $\alpha_2 = 87320173$ and $\beta_2 = 32920110577,\ d_2 = 32832790404, u_2 = 181198, p0_2 = 181193, r_2 = 105048, s_2 = 95756$. Finally, the shares to be distributed to the remaining participants in P_2 are computed as follows.

$$S_{5,2} = 19121378193 (\text{mod } 439) \equiv 63 (\text{mod } 439)$$
$$S_{6,2} = 19121378193 (\text{mod } 443) \equiv 410 (\text{mod } 443)$$
$$S_{7,2} = 19121378193 (\text{mod } 449) \equiv 181 (\text{mod } 449).$$

The shares distributed to the participants in P_2 are $I_{1,2} = (200, 419), I_{2,2} = (243, 421), I_{3,2} = (267,431), I_{4,2} = (335,433), I_{5,2} = (63,439), I_{6,2} = (410,443), I_{7,2} = (181,449)$. Additionally, multi-privileged shares are given to KMS 3, namely $S_1^{3,2} = 267$ and $S_2^{3,2} = 181$.

Step 3: Shares distribution for the (5,8) scheme.

KMS 3 generates the Mignotte sequence $p_{1,3} = 457,\ p_{2,3} = 461, p_{3,3} = 463, p_{4,3} = 467, p_{5,3} = 479, p_{6,3} = 487, p_{7,3} = 491, p_{8,3} = 499$. Next, KMS 3 determines the shares for participants 4 and 5, namely $S_{4,3} = 400$ and $S_{5,3} = 381$. Then, KMS 3 computes S_3 by solving the system of congruent equations that has been formed. The calculations proceed as follows:

$$M = 21819787184543,$$
$$M_1 = 47745704999, M_2 = 47331425563, M_3 = 47126970161,$$
$$M_4 = 46723313029, M_5 = 45552791617,$$
$$M_1^{-1} = 56, M_2^{-1} = 310\ , M_3^{-1} = 126, M_4^{-1} = 461, M_5^{-1} = 453.$$

As a result, KMS 3 obtains $S_3 = 10678075411213$. The next calculation process, obtained $\alpha_3 = 57153984457,\ \beta_3 = 21819787184543, d_3 = 21762633200086, u_3 = 4665043, p0_3 = 4665019, r_3 =$

2276715, and $s_3 = 2694171$. Finally, the shares to be distributed to the remaining participants in P_3 are computed as follows.

$$S_{6,3} = 10678075411213 \pmod{487} \equiv 114 \pmod{487}$$
$$S_{7,3} = 10678075411213 \pmod{491} \equiv 71 \pmod{491}$$
$$S_{8,3} = 10678075411213 \pmod{499} \equiv 432 \pmod{499}.$$

The shares distributed to the participants in P_3 are $I_{1,3} = (200,457), I_{2,3} = (267,461), I_{3,3} = (181,463), I_{4,3} = (400,467), I_{5,3} = (381,479), I_{6,3} = (114,487), I_{7,3} = (71,491), I_{8,3} = (432,499)$.

Step 4: Secret reconstruction

Suppose a CEO wishes to access data related to the company's business strategy. To decrypt the data, at least four shares from participant 2 must be collected. Assume that five shares are gathered that are $I_{1,2} = (200,419), I_{2,2} = (243,421), I_{3,2} = (267,431), I_{4,2} = (335,433), I_{5,2} = (63,439)$. The key is reconstructed using CRT, resulting in $S_2' = 19121378193$. Given that $\alpha_2 = 87320173, r_2 = 105048$, and $p0_2 = 181193$, the value of R_2 is calculated as $R_2 = \left\lfloor \frac{S_2' - \alpha_2}{p0_2} \right\rfloor = \left\lfloor \frac{19121378193 - 87320173}{181193} \right\rfloor = 105048$. Since $R_2 = 105048 = r_2$, no cheating is detected. Secret key $s_2 = S_2' - \alpha_2 - (r_2 \times p0_2) = 19121378193 - 87320173 - (105048 \times 181193) = 95756$. Thus, the CEO is able to access the business strategy data. However, if only three shares from participant 2 are collected, namely $I_{1,2} = (200,419), I_{2,2} = (243,421), I_{3,2} = (267,431)$. When secret reconstruction, the actual key cannot be recovered because the number of accumulated shares is less than the threshold.

In another case, suppose a COO needs access to financial data. To decrypt the data, at least three shares from participant 1 must be collected. Assume that four shares are obtained $I_{1,1} = (200,359), I_{2,1} = (250,367), I_{3,1} = (190,373), I_{4,1} = (353,379)$. The key is reconstructed using the CRT, resulting in $S_1' = 13134421588$. Given that $\alpha_1 = 154433, r_1 = 5798$, and $p0_1 = 6997$, the value of R_1 is calculated as $R_1 = \left\lfloor \frac{S_1' - \alpha_1}{p0_1} \right\rfloor = \left\lfloor \frac{13134421588 - 154433}{6997} \right\rfloor = 1877128$. It is obtained that $R_1 \neq r_1$, so cheating is detected. As a result, the original key cannot be recovered and COO is unable to access the financial data.

3.3 Security and Correctness

In this session, the security and correctness of the Mignotte (t, n) collaborative secret sharing scheme will be analyzed. According to [25], the security of the Mignotte scheme (t, n) is high if the generated Mignotte sequence ensures that the value of $\frac{\beta - \alpha}{\alpha}$ alpha is significantly large. This can be achieved by selecting prime numbers within the interval $(p_k^{\frac{t^2-1}{t^2}}, p_k]$ such that $\frac{(\beta-\alpha)}{\alpha} \geq p_k^{\frac{t-1}{t}} - 1$. The following explanation discusses the impact of selecting prime numbers within the interval $(p_k^{\frac{t^2-1}{t^2}}, p_k]$, which results in the condition $\frac{(\beta-\alpha)}{\alpha} \geq p_k^{\frac{t-1}{t}} - 1$. Suppose,

$$\beta = \prod_{i=1}^{t} p_i = p_1 p_2 \dots p_t$$
$$\alpha = \prod_{i=0}^{t-2} p_{n-i} = p_n p_{n-1} \dots p_{n-t+2}.$$

Since $p_k^{\frac{t^2-1}{t^2}} \leq p_k$, it follows that

$$\beta = p_1 p_2 \dots p_t \geq p_k^{\left(\frac{t^2-1}{t^2}\right)t} = p_k^{\frac{t^2-1}{t}}.$$

Since p_k is the upper bound of the interval containing prime numbers, that $p_k^{t-1} \geq p_n p_{n-1} \dots p_{n-t+2} = \alpha$. Thus, $\frac{\beta-\alpha}{\alpha} \geq \frac{p_k^{\frac{t^2-1}{t}} - p_k^{t-1}}{p_k^{t-1}} = p_k^{\frac{t-1}{t}} - 1$.

Based on this result, security is enhanced when the difference between α and β is significantly large. In other words, the level of security is highly dependent on the choice of prime numbers.

Three possible attacks can be launched against multi-privileged participants: an independent attack by a multi-privileged participant, a collaborative attack within a subgroup Γ_i, and a collaborative attack with another group P_i [9]. The security of the scheme against these three types of attacks is ensured for the following reasons.

1. A multi-privileged participant cannot reconstruct the secret independently because $|U \cap P_i)| < t_i$. Although they are involved in multiple schemes, they are still unable to reconstruct the secret from any of them.
2. Collaboration between a multi-privileged participant and participants in Γ_i cannot reconstruct the correct secret s_i if their combined number is less than the threshold t_i.
3. Collaboration between a multi-privileged participant and participants in P_i cannot reconstruct the secret s_j for $j \neq i$. Regardless of whether their combined number meets or does not meet t_j, the secret cannot be recovered because $|((U \cup P_i) \cap P_j)| \leq t_j - 1$. The number of shares related to the secret s_j never reaches the threshold. In other words, although the number of participants may be sufficient, the information they possess is not. As a result, the secret remains secure from unauthorized access.

Theorem 1. *Let U be the set of multi privileged participants, P_i the set of participants in the i-th scheme, and t_i the threshold of the i-th scheme. The Mignotte (t,n) collaborative secret sharing scheme is considered secure against cheating if the following conditions are satisfied:*

$$\left|\left(\bigcup_{j=1,j\neq i}^{l} P_j\right) \bigcap P_i\right| < t_i.$$

Proof. In the Mignotte (t, n) collaborative secret sharing scheme, multi-privileged participants may contribute to more than one individual scheme. To ensure security and prevent cheating, the number of participants in scheme i who also appear in other schemes must be fewer than the threshold t_i. If the condition $\left|(\bigcup_{j=1,j\neq i}^{l} P_j) \cap P_i\right| \geq t_i$ is satisfied, the participants from outside P_i who are also members of P_i can collaborate to collect at least t_i shares. These participants would be able to reconstruct the secret of scheme i without involving all the legitimate participants of that scheme. Conversely, if the number of participants in the intersection of scheme i and the other schemes is less than t_i, they would not be able to gather enough shares to reconstruct the secret of scheme i. Therefore, the Mignotte (t,n) collaborative secret sharing scheme is secure against cheating if:

$$\left|\left(\bigcup_{j=1,j\neq i}^{l} P_j\right) \bigcap P_i\right| < t_i. \blacksquare$$

For example, in the illustration provided in section 2, the multi-privileged participants in scheme 3 cannot recover the secret of that scheme. This is because the number of multi-privileged participants in scheme 3 is less than the predefined threshold. If the number of shares in the secret reconstruction process is below the threshold, the original secret cannot be recovered. In the illustration from section 2, in the secret reconstruction step, the CEO is unable to access the company's business strategy data. This is because only three shares are collected, while the threshold for that scheme is four. As a result, the original secret key cannot be recovered, and the CEO cannot access the business strategy data. However, when the threshold of any individual scheme is met, the secret can be reconstructed by solving the system of congruences using the CRT. The correctness of this process has been demonstrated through the illustration provided in Section 2. The illustration shows that the scheme possesses a high level of security and satisfies the property of correctness, as it can produce outputs consistent with the given inputs.

4. CONCLUSION

The Mignotte secret sharing scheme in [18] can be modified by adding a detector parameter (r). This addition enhances the scheme by incorporating a cheating detection mechanism. With the inclusion of the detector parameter, the secret is determined using the formula $S_1 = \alpha_1 + (r_1 \times p0_1) + s_1$ and cheating detection is performed by computing $R_i = \left\lfloor \frac{S_i' - \alpha_i}{p0_i} \right\rfloor$. This scheme can be applied to the Mignotte (t, n) collaborative secret sharing scheme, allowing multi privileged participants to store only a single share. The method is suitable for securing data in cloud storage, as the key can only be accessed by authorized parties. The key is represented as a numerical value and secured using the Mignotte (t, n) collaborative secret sharing scheme. The addition of the cheating detection mechanism and the selection of a Mignotte sequence that satisfies the condition $\frac{(\beta-\alpha)}{\alpha} \geq p_k^{\frac{t-1}{t}} - 1$ make this scheme more secure. The scheme also satisfies **Theorem 1**, ensuring the secret remains protected from cheating attempts and unauthorized access. The correctness of the proposed scheme is demonstrated through a series of test cases, all of which produced the expected results. Nevertheless, this study is limited to detecting the presence of cheating without the ability to identify the cheater. Future work may focus on developing an identification mechanism to improve the scheme's security further.

AUTHOR CONTRIBUTIONS

Dhea Ekaputri: Conceptualization, Formal Analysis, Funding Acquisition, Investigation, Methodology, Project Administration, Resources, Software, Visualization, Writing - Original Draft, Writing - Review and Editing. Sugi Guritman: Conceptualization, Formal Analysis, Methodology, Project Administration, Supervision, Validation, Writing - Review and Editing. Jaharuddin: Project Administration, Supervision, Validation, Visualization, Writing - Original Draft, Writing - Review and Editing. All authors discussed the results and contributed to the final manuscript.

FUNDING STATEMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the reviewers for their valuable comments, constructive suggestions, and critical insights that have significantly improved the quality of this article. The authors also extend their appreciation to the editorial team for their professional handling and support throughout the review process.

CONFLICT OF INTEREST

The authors declare that no conflicts of interest exist in this study.

REFERENCES

[1] Y. E. Rachmad, R. Dewantara, R. S. Junaidi, M. Firdaus, S. S. W., S. and E. , MASTERING CLOUD COMPUTING (FOUNDATIONS AND APPLICATIONS PROGRAMMING), Jambi: Sonpedia Publishing Indonesia, 2023.

[2] I. Odun-Ayo, O. Ajayi, B. Akanle and R. Ahuja, "AN OVERVIEW OF DATA STORAGE IN CLOUD COMPUTING," in *IEEE*, New York (NY), 2017, doi: https://doi.org/10.1109/ICNGCIS.2017.9.

[3] N. Vurukonda and B. T. Rao, "A STUDY ON DATA STORAGE SECURITY ISSUES IN CLOUD COMPUTING," in *Elsevier*, Belanda, 2016, doi: ttps://doi.org/10.1016/j.procs.2016.07.335

[4] P. Yang, N. Xiong and J. Ren, "DATA SECURITY AND PRIVACY PROTECTION FOR CLOUD STORAGE: A SURVEY," *IEEE Access,* vol. 8, pp. 131723-131740, 2020, doi: https://doi.org/10.1109/ACCESS.2020.3009876.

[5] Y.-H. Chen and P.-C. Huang, "COLLABORATIVE ACCESS CONTROL OF CLOUD STORAGE SYSTEMS," in *IEEE*, New York (NY), 2018, doi: https://doi.org/10.1109/ICASI.2018.8394460

[6] L. Yuan, M. Li, C. Guo, K.-K. R. Choo and Y. Ren, "NOVEL THRESHOLD CHANGEABLE SECRET SHARING SCHEMES BASED ON POLYNOMIAL INTERPOLATION," *PLOS ONE,* vol. 11, no. 10, pp. 1-19, 2016, doi: https://doi.org/10.1371/journal.pone.0165512

[7] X. Jia, D. Wang, D. Nie, X. Luo and J. Z. Sun, "A NEW THRESHOLD CHANGEABLE SECRET SHARING SCHEME BASED ON THE CHINESE REMAINDER THEOREM," *Information Sciences,* vol. 473, pp. 13-30, 2019, doi: https://doi.org/10.1016/j.ins.2018.09.024.

[8] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone, HanDBOOK OF APPLIED CRYPTOGRAPHY, Florida: CRC Press, 1996.

[9] X. Jia, Y. Song, D. Wang, D. Nie and J. Wu, "A COLLABORATIVE SECRET SHARING SCHEME BASED ON THE CHINESE REMAINDER THEOREM," *Mathematical Biosciences and Engineering,* vol. 16, no. 3, pp. 1280-1299, 2019, doi: https://doi.org/10.3934/mbe.2019062

[10] 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, doi: https://doi.org/10.1016/j.ins.2018.04.043.

[11] M. Gharahi and S. Khazaei, "OPTIMAL LINEAR SECRET SHARING SCHEMES FOR GRAPH ACCESS STRUCTURES ON SIX PARTICIPANTS," *Theoretical Computer Science,* vol. 771, pp. 1-8, 2019, doi: https://doi.org/10.1016/j.tcs.2018.11.007

[12] X. Jia, Y. Guo, X. Luo, D. Wang and C. Zhang, "A PERFECT SECRET SHARING SCHEME FOR GENERAL ACCESS STRUCTURES," *Information Sciences,* vol. 595, pp. 54-69, 2022, doi: https://doi.org/10.1016/j.ins.2022.02.016

[13] V. P. Binu and A. Sreekumar, "SECURE AND EFFICIENT SECRET SHARING SCHEME WITH GENERAL ACCESS STRUCTURES BASED ON ELLIPTIC CURVE AND PAIRING," *Wireless Personal Communications,* vol. 92, no. 4, pp. 1531-1543, 2017, doi: https://doi.org/10.1007/s11277-016-3619-8

[14] X. Dong, "A MULTI-SECRET SHARING SCHEME BASED ON THE CRT AND RSA," *International Journal of Electronics and Information Engineering,* vol. 2, no. 1, pp. 47-51, 2015, doi: 10.6636/IJEIE.201503.2(1).05.

[15] L. Tan, Y. Lu, X. Yan, L. Liu and L. Li, "WEIGHTED SECRET IMAGE SHARING FOR A (K,N) THRESHOLD BASED ON THE CHINESE REMAINDER THEOREM," *IEEE Access,* vol. 7, pp. 59278-59286, 2019, doi: https://doi.org/10.1109/ACCESS.2019.2914515

[16] K. Meng, F. Miao, Y. Ning, W. Huang, Y. Xiong and C.-C. Chang, "A PROACTIVE SECRET SHARING SCHEME BASED ON CHINESE REMAINDER THEOREM," *Frontiers of Computer Science,* vol. 15, no. 2, pp. 1-10, 2020, doi: https://doi.org/10.1007/s11704-019-9123-z

[17] A. N. Tentu, V. Venkaiah and V. K. Prasad, "CRT BASED MULTI-SECRET SHARING SCHEMES: REVISITED," *International Journal of Security and Networks,* vol. 13, no. 1, pp. 1-9, 2018, doi: https://doi.org/10.1504/IJSN.2018.090637

[18] M. Mignotte and S. , HOW TO SHARE A SECRET, Verlag: Springer, 1983.

[19] C. Asmuth and J. Bloom, "A MODULAR APPROACH TO KEY SAFEGUARDING," *IEEE Transactions on Information Theory,* vol. 29, no. 2, pp. 208-210, 1983, doi: https://doi.org/10.1109/TIT.1983.1056651

[20] K. K. Phiri and H. Kim, "LINEAR (t,n) SECRET SHARING SCHEME WITH REDUCED NUMBER OF POLYNOMIALS," *HINDAWI,* vol. 2019, pp. 1-16, 2019, doi: https://doi.org/10.1155/2019/5134534

[21] Y. Liu, "LINEAR (k, n) SECRET SHARING SCHEME WITH CHEATING DETECTION," *Security and Communication Networks,* vol. 9, no. 13, pp. 2115-2121, 2016, doi: https://doi.org/10.1002/sec.1467

[22] X. Yan, Y. Lu, L. Liu, J. Liu and G. Yang, "CHINESE REMAINDER THEOREM-BASED TWO-IN-ONE IMAGE SECRET SHARING WITH THREE DECODING OPTIONS," *Digital Signal Processing,* vol. 82, pp. 80-90, 2018, doi: https://doi.org/10.1016/j.dsp.2018.07.015

[23] K. H. Rosen, ELEMENTARY NUMBER THEORY AND ITS APPLICATIONS, Reading, Mass. u.a: Addison-Wesley, 1986.

[24] D. M. Burton, ELEMENTARY NUMBER THEORY, New York (US): McGraw-Hill, 2011.

[25] E. Kranakis, PRIMALITY AND CRYPTOGRAPHY, Wiesbaden: Springer, 1986. doi: https://doi.org/10.1007/978-3-322-96647-6

[26] D. Romik, TOPICS IN COMPLEX ANALYSIS, Berlin: De Gruyter, 2023. doi: https://doi.org/10.1515/9783110796810