Computationally secure threshold secret sharing scheme with minimal redundancy

M Babenko[1], A Tchernykh[2,3,4], E Golimblevskaia[1], Nguyen Viet Hung[5] and V K Chaurasiya[5]

[1]North-Caucasus Federal University, Stavropol, Russia
[2]CICESE Research Center, Ensenada, BC, México
[3]South Ural State University, Chelyabinsk, Russia
[4]Ivannikov Institute for System Programming, Moscow, Russia
[5]LeQuyDon Technical University, Hanoi, Vietnam
[6]Indian Institute of Information Technology, Allahabad, India

E-mail: chernykh@cicese.mx

Abstract. When designing and using distributed storage systems with cloud technology, the security issues become crucial. One of the promising mechanisms is the computationally secure threshold secret sharing scheme. We propose a computationally secure secret sharing scheme based on the minimally redundant modular code. It reduces the computational complexity of data encoding and decoding and reduce data redundancy. We show that it is computationally secure and provides data redundancy equivalent to the redundancy of the Rabin system. We demonstrate that the minimally redundant modular code does not satisfy the criterion of compactness of a sequence, but it can be used as an asymptotically ideal secret sharing scheme.

1. Introduction

The cloud technologies require users to take into account the increased risks of data security and reliability. To reduce the likelihood of theft, loss or distortion of data stored in clouds, two mechanisms can be used: secret sharing schemes and hash functions. Residue Number System (RNS) as the basis for the design of distributed storage systems combines these two mechanisms into one, since RNS on the one hand is a secret sharing scheme, and, on the other hand, it has properties of error detection and correction.

Secret sharing schemes on RNS provide the same level of security as schemes built on Lagrange interpolation, however, have higher redundancy. To solve this problem, compact sequences as RNS moduli that satisfy the condition $p_1 < p_2 < \cdots < p_n < 2p_n$ are proposed [1].

Compact sequences highlight a class of asymptotically ideal Asmuth-Bloom secret sharing schemes [2, 3], which ensure a high level of data reliability and security. But this approach is not applicable in practice for storing big data, since data redundancy is higher than data replication and symmetric encryption.

AC-RRNS [4] modification of the Asmuth-Bloom scheme uses compact sequences to reduce data redundancy while ensuring computational security. However, using a prime number p_0 as a key satisfying the condition: $\beta = \prod_{i=1}^{k} p_i > p_0 > \prod_{i=0}^{k-2} p_{n-i} = \alpha$ leads to increasing the complexity of the

encoding and decoding algorithm from linear-logarithmic to quadratic. It does not allow its efficient use.

An alternative solution to the problem is to use minimally redundant modular code, which, on the one hand, satisfies the criteria of compactness of a sequence, and, on the other hand, reduces the computational complexity of encoding and decoding while maintaining reliability and security at the same level.

The rest of the paper is structured as follows. Section 2 discusses the properties of RNS. Section 3 describes RNS-based minimally redundant code. Section 4 discusses our secret sharing scheme modification. Section 5 explores the security issues of the proposed scheme. Section 6 concludes the paper.

2. RNS and its properties

RNS is a non-positional number system that allows splitting long numbers into a series of independent digits of small length, speeding up the calculations and organizing their parallelism. The main advantage of RNS is the ability to perform addition and multiplication operations fast compared to all other number systems. It causes a great interest in RNS in those areas in which large amounts of computation are required.

RNS is defined by a system of mutually prime moduli $\beta = \{p_1, p_2, \dots, p_n\}$. The positive number X in the RNS for these moduli is represented as a tuple of numbers $X = (x_1, x_2, \dots, x_n)$, where $x_i = |X|_{pi} = X \bmod p_i$ [5] for $i = 1,2, \dots, n$. Such a representation of the number X is unique, if $0 \le X < P$, where $P = \prod_{i=1}^{n} p_i$, and is called the RNS range.

The operations of addition, subtraction and multiplication in the RNS for the numbers $A = (a_1, a_2, \dots, a_n)$ and $B = (b_1, b_2, \dots, b_n)$ are determined by the formulas:

$$A \pm B = \left(|a_1 \pm b_1|_{p_1}, \dots, |a_n \pm b_n|_{p_n}\right) \quad (1)$$

$$A \times B = \left(|a_1 \times b_1|_{p_1}, \dots, |a_n \times b_n|_{p_n}\right) \quad (2)$$

The equalities (1) and (2) show the parallel nature of RNS, free from bitwise transfers. In addition, the numbers a_i and b_i have much smaller number of digits than the original numbers A and B.

In modern technology, one of the most popular properties of algorithms is their parallelism. This fact is due to the development of many parallel systems, from multiprocessor clusters to embedded systems for special purposes.

The most common way to reconstruct the positional value of a number based on its residual representation is the Chinese Remainder Theorem (CRT), the classical form of which we will designate as CRTc.

Let the number X be given in the form $(x_1, x_2, \dots, x_n)$ in the CRT by moduli $(p_1, p_2, \dots, p_n)$. Then:

$$X = \left|\sum_{i=1}^{n} \left|P_i^{-1}\right|_{p_i} P_i x_i\right|_P \quad (3)$$

where $P_i = P/p_i$, $\left|P_i^{-1}\right|_{p_i}$ is the multiplicative inversion of P_i modulo p_i for $i = 1, \dots, n$.

This method is computationally complex, since it leads to calculations that fall outside the range of P, and its implementation requires the operation of calculating the residue of the division by a large number of P, which greatly complicates the calculation scheme. The calculation of the residue of the division in any computer system is traditionally one of the most expensive operations. The implementation of this operation on the FPGA leads to a significant increase in the hardware costs of the algorithm and an increase in the delay in operation.

One approach to get rid of calculating the residue of dividing by the RNS range is an approach using a Mixed-Radix System (MRS) [6-8]. By MRS with moduli $p_1, p_2, \dots, p_n$ we mean a system in which the integer X is represented as:

$$X = a_n p_{n-1} p_{n-2} \dots p_2 p_1 + a_{n-1} p_{n-2} p_{n-3} \dots p_2 p_1 + \dots + a_2 p_1 + a_1,$$

where a_j are the numbers $0,1,\dots,p_{j-1}$. MRS numbers a_j can be found by the formulas.

$a_1 = x_1 \ mod \ p_1;$
$a_2 = (x_2 - a_1)c_{12} \ mod \ p_2$
….
$a_3 = \big((x_3 - a_1)c_{13} - a_2\big)c_{23} \ mod \ p_3$
$a_n = \big(\dots\big((x_n - a_1)c_{1n} - a_2\big)c_{2n} - \dots - a_{n-1}\big)c_{n-1,n} \ mod \ p_n$

The constants c_{ij} are multiplicative inverse elements for p_i modulo p_j for all $1 \le i \le j \le n$, i.e. $c_{ij} \cdot p_i = 1 \ mod \ p_j$ for $1 \le i \le n$, and can be calculated, for example, using the Euclidean algorithm.

The main advantage of MRS is the transition to the use of low-bit operations. Most operands for addition and multiplication operations are numbers whose bit capacity is equal to the capacity of the moduli, which allows constructing simpler schemes than when using CRT. In addition, the considered method can be presented in parallel form [9]. However, a decrease in the capacity of operands leads to an increase in the number of operations, including operations for calculating the residue of the division, which leads to an overall decrease in the operating time of the algorithm.

Next, we consider a modification of the Chinese remainder theorem using fractional quantities, which we will denote CRTd [10-12]. If both parts of formula (3) are divided by P, then we obtain the relation

$$\bar{X} = \frac{X}{P} = \left| \sum_{i=1}^{n} \frac{\left|P_i^{-1}\right|_{p_i}}{p_i} x_i \right|_1 \tag{4}$$

where the operation $|\cdot|_1$ means discarding the integer part of the number and the numbers

$$k_i = \frac{\left|P_i^{-1}\right|_{p_i}}{p_i}, i = 1,2,\dots,n \tag{5}$$

are constants of RNS and can be calculated in advance. In this case, the value of each sum will be in the range $[0,1)$, which gives enough information to evaluate the sign and value of the number represented in the RNS.

Such a transition allows replacing the exact number with its fractional characteristic, making it possible to control the accuracy of the presentation depending on the available resources and the task. The value $\bar{X}$ can be considered as a positional characteristic of the number X, while the number X can be found by the formula

$$X = \bar{X}P \tag{6}$$

However, in the case of machine calculations, we can use only limited accuracy, which requires rounding or discarding the least significant bits of the fraction. Let us estimate the number of bits that make it possible to uniquely determine the fractional characteristic of the number X. Let $\overline{k_\iota}$ be a finite fraction containing N bits that coincide with the first N bits of the number k_i for all $i = 1,2,\dots,n$. In other words $\overline{k_\iota} = \lfloor k_i \rfloor_{2^{-N}}$, where the operation means rounding the number down. The approximate value of the number $\bar{X}$ will not be more accurate, since $k_i \ge \overline{k_\iota}$. The exact value of X can be restored by multiplying $\bar{X}$ by P, discarding the fractional part with rounding up. Let us estimate the required calculation accuracy N, at which the value $\bar{X}$ reconstructed using $\overline{k_\iota}$ will not lead to errors when restoring the exact value of X. For this, the relation

$$\frac{X-1}{P} < \left| \sum_{i=1}^{n} \overline{k_\iota} x_i \right|_1 \le \frac{X}{P} \tag{7}$$

shows the uniqueness of the positional characteristic $\bar{X}$ for different numbers of RNS. The transformation of expression (7) using formula (4) leads to the inequality

$$0 \le \left| \sum_{i=1}^{n} \left(k_i - \overline{k_\iota}\right) x_i \right|_1 < \frac{1}{P} \tag{8}$$

Since $k_i - \overline{k_\iota} = \frac{|P_i^{-1}|_{p_i}}{p_i} - \frac{2^N|P_i^{-1}|_{p_i} - \left|2^N|P_i^{-1}|_{p_i}\right|_{p_i}}{2^N \cdot p_i} = \frac{\left|2^N|P_i^{-1}|_{p_i}\right|_{p_i}}{2^N \cdot p_i}$, then

$$\sum_{i=1}^{n}\left(k_i - \overline{k_\iota}\right)x_i = \sum_{i=1}^{n}\frac{\left|2^N|P_i^{-1}|_{p_i}\right|_{p_i}}{2^N \cdot p_i}x_i. \tag{9}$$

Considering $x_i \le p_i - 1$, the left side of equality (9) satisfies the inequality:

$$\sum_{i=1}^{n}\frac{\left|2^N|P_i^{-1}|_{p_i}\right|_{p_i}}{2^N \cdot p_i}x_i \le \frac{1}{2^N}\left(\sum_{i=1}^{n}\left|2^N\left|P_i^{-1}\right|_{p_i}\right|_{p_i} - \sum_{i=1}^{n}\frac{\left|2^N|P_i^{-1}|_{p_i}\right|_{p_i}}{p_i}\right) \tag{10}$$

It follows from (8) and (10) that N satisfies the inequality:

$$2^N \le P\left(\sum_{i=1}^{n}\left|2^N\left|P_i^{-1}\right|_{p_i}\right|_{p_i} - \sum_{i=1}^{n}\frac{\left|2^N|P_i^{-1}|_{p_i}\right|_{p_i}}{p_i}\right) \le -\mathrm{SQ} + P\sum_{i=1}^{n}(p_i - 1). \tag{11}$$

where $SQ = \sum_{i=1}^{n} P_i$.

Denoting $\rho = \sum_{i=1}^{n}(p_i - 1)$, from formula (11) we get that when choosing N equal to $N = \lceil \log_2(P \cdot \rho - SQ)\rceil$, the resulting estimate is the estimate refinement obtained in [12], where $N = \lceil \log_2(P \cdot \rho)\rceil$. Using the approximate method allows getting away from calculating the residue of the division by the RNS range, by increasing the dimension of the coefficients. An alternative solution is to use minimally redundant code, which imposes additional restrictions on the moduli, but at the same time reduces the complexity of decoding.

3. Minimally redundant code and its properties

In the following, we assume that the RNS moduli are ordered in increasing order $p_1 < p_2 < \cdots < p_n$. The number X can be restored using the properties of the modular code, according to the following formula:

$$X = \sum_{i=1}^{n-1} M_i\left|M_i^{-1} \cdot x_i\right|_{p_i} + P_n \cdot I(X), \tag{12}$$

where for any $i \in [1, n-1]$: $M_i = P_n/p_i$, and $I(X)$ is an interval characteristic that is determined using the following Theorem 1.

Theorem 1 [13]. If the RNS moduli satisfy the condition $p_n \ge 2p_1 + n - 2$, then the interval characteristic $I(X)$ is calculated using the following formula:

$$I(X) = \begin{cases} \hat{I}(X) \; if \; \hat{I}(X) < p_1 \\ \hat{I}(X) - p_n \; if \; \hat{I}(X) \ge p_n - p_1 - n + 2 \end{cases} \tag{13}$$

where $\hat{I}(X) = \left|\left|\frac{x_n}{P_n}\right|_{p_n} - \cdot \sum_{i=1}^{n-1}\left|\frac{1}{p_i}\right|_{p_n} \cdot \left|M_i^{-1} \cdot x_i\right|_{p_i}\right|_{p_n}$.

As shown in Chernyavsky & Kolyada, 2009 [13], for RNS moduli to be minimally redundant modular code, it is necessary and sufficient that

$$p_n = 2p_1 + n + |p_n - n|_2 + 2 \tag{14}$$

We consider four cases:

Case 1, p_n and n are even numbers, $p_n = 2p_1 + n + 2$,

Case 2, p_n and n are odd numbers, $p_n = 2p_1 + n + 2$,

Case 3, p_n is even number and n is odd number, $p_n = 2p_1 + n + 3$,

Case 4, p_n is odd number and n is even number, $p_n = 2p_1 + n + 3$.

Considering four cases, we can conclude that if $p_n > 2p_1$, then the minimally redundant code does not satisfy the compactness criterion.

Using (12) we can reduce the computational complexity of the data decoding algorithm.

4. Modification of the secret sharing scheme

To formalize the proposed scheme, we use the following notations. $S \in Z_Q$ is a secret, $p_1, p_2, \dots, p_n$ are prime numbers (RNS moduli set), with properties of the minimum redundant modular code, where $\mathrm{Q} = q_1, q_2, \dots, q_m$ is secret key and q_i is prime numbers and compact sequence, i.e. $q_1 < q_2 < \cdots < q_m < 2q_1$.

We perform a masking transformation that translates S to $\bar{S} = S + Q \cdot rand$, where $rand$ is a random number and $\bar{S} < \prod_{i=1}^{k} p_i$. To calculate the chunks, we get $c_i = |\bar{S}|_{p_i}$.

It follows from the condition $\bar{S} < \prod_{i=1}^{k} p_i = \beta$ that $S + Q \cdot rand < \beta$, which means that $S < \beta - Q \cdot rand$. Let $rand$ be bounded above $rand \le r$. We have

$$S < \beta - Q \cdot r \tag{15}$$

On the other hand, $S = |\bar{S}|_Q$ so that we can uniquely decode data if

$$S < Q \tag{16}$$

Multiplying inequality (16) by r and adding to (15), we have

$$(r+1) \cdot S < \beta \tag{17}$$

Hence,

$$S < \frac{\beta}{r+1} \tag{18}$$

Since S must satisfy two conditions (16) and (18), therefore:

$$S < \min\left(Q, \frac{\beta}{r+1}\right) \tag{19}$$

We consider two cases:

Case 1: $Q < \frac{\beta}{r+1}$, then $S < Q$ and redundancy is equal to

$$R \approx \frac{\log_2 \prod_{i=1}^{n} p_i}{\log_2 Q} > \frac{\log_2 \prod_{i=1}^{n} p_i}{\log_2 \prod_{i=1}^{k} p_i - \log_2(r+1)} = 1 + \frac{\log_2(r+1) + \log_2 \prod_{i=k+1}^{n} p_i}{\log_2 \prod_{i=1}^{k} p_i - \log_2(r+1)} \tag{20}$$

Case 2: $Q \ge \frac{\beta}{r+1}$, then $S < \frac{\beta}{r+1}$

$$R \approx \frac{\log_2 \prod_{i=1}^{n} p_i}{\log_2 \beta - \log_2(r+1)} = \frac{\log_2 \prod_{i=1}^{n} p_i}{\log_2 \prod_{i=1}^{k} p_i - \log_2(r+1)} = 1 + \frac{\log_2(r+1) + \log_2 \prod_{i=k+1}^{n} p_i}{\log_2 \prod_{i=1}^{k} p_i - \log_2(r+1)} \tag{21}$$

From (20) and (21), it follows that the secret sharing scheme has optimal redundancy (21). If the condition $Q \ge \frac{\beta}{r+1}$ is fulfilled, then $(r+1)Q \ge \beta$. On the other hand, from (15) $r \cdot Q \le \beta$ follows, therefore β satisfies the condition:

$$r \cdot Q \le \beta \le (r+1)Q \tag{22}$$

Dividing (22) by Q, we get:

$$r \le \frac{\beta}{Q} \le r + 1 \tag{23}$$

From (23), it follows that the value $r = \left\lfloor \frac{\beta}{Q} \right\rfloor$. Since, from the point of view of safety, r satisfies the condition $r \ge 1$, then $Q < \beta/2$. Therefore, the scheme parameters must satisfy the following conditions:

Condition 1: $\beta > \prod_{i=0}^{k-2} p_{n-i}$ (determines that the proposed scheme is a threshold)

Condition 2: $Q < \frac{\beta}{2}$ and $\gcd(Q, \beta) = 1$.

Condition 3: $r = \left\lfloor \frac{\beta}{Q} \right\rfloor$.

Condition 4. $2^{l-1} < p_1 < p_2 < \cdots < p_n$ is the minimum redundant modular code.

In contrast to the Asmuth-Bloom scheme [14], the proposed scheme provides data security with minimum redundancy.

5. Properties of the proposed scheme

In this section, we examine the security parameters of the proposed scheme. Condition 4 states that RRNS moduli set is a minimum redundant modular code. Hence, each user has approximately the same amount of information about the original data. Now, we show that proposed scheme minimizes the probability of access to data by collusion of adversaries. To this end, we prove the following statements, corollary, and theorem.

Statement 1. *In proposed* (k, n) *secret sharing scheme, if an adversary coalition knows less than* k *secret shares and secret key* Q*, then the probability obtaining the secret is less than* $1/2^{(l-1)}$.

Proof. For the set $I \subset \{1,2, \dots, n\}$ with the cardinality less than k, we can compute the value S^* that satisfies the equality $S^* = |S|_{P_I}$, where $P_I = \prod_{i \in I} p_i$. Therefore, S can be represented as: $S = S^* + P_I \cdot w$, where integer $w \in [0, \lfloor \beta / P_I \rfloor]$. Each value of w corresponds the value of C_w^* calculated by the following formula: $C_w^* = |S^* + P_I \cdot w|_{p_0}$.

Taking into account Condition 1, P_I satisfies the condition $P_I \leq \prod_{i=0}^{k-2} p_{n-i}$. Consequently, the probability to compute S with the known S^*, satisfies the equality $Pr(I) \leq \frac{1}{\left\lfloor \frac{\beta}{P_I} \right\rfloor} \leq \frac{1}{p_{n-k+1}} < \frac{1}{2^{l-1}}$

Statement 2. *In the proposed* (k, n) *scheme, probability to obtain the secret based on known* k *or more secret shares without secret key is less than* $\frac{2}{\phi(\beta) - 2^{k+1}}$*, where* $\phi(x)$ *is Euler function.*

Proof. Knowing k or more secret shares using the Chinese remainder theorem, we can restore the value of $\bar{S}$**.** In order to calculate S from $\bar{S}$ it is necessary to sort out the whole set of possible values of Q. Since from Condition 2 $\gcd(Q, \beta) = 1$ and $Q < \frac{\beta}{2}$, then Q represented in RNS by the moduli $p_1, p_2, \dots, p_k$ should not contain a single residue from the division equal to zero. Let us consider the values of the form X_E, the smallest of the numbers which in the representation of the moduli P contains $e \leq k$ different zero values at the positions $E = \{i_1, i_2, \dots, i_e\}$, respectively, then the number of numbers containing at the positions $\{i_1, i_2, \dots, i_e\}$ zeros and $\frac{\beta}{2}$ is $\left\lfloor \frac{\beta}{2X_E} \right\rfloor$. Therefore, the number of non-coprime to β numbers is $\sum_{E \in I} \left\lfloor \frac{\beta}{2X_E} \right\rfloor$. Considering that the cardinality of the set I is 2^k, then

$$\sum_{E \in I} \left\lfloor \frac{\beta}{2X_E} \right\rfloor < \sum_{E \in I} \frac{\beta}{2X_E} = \frac{1}{2} \sum_{E \in I} \frac{\beta}{X_E} - 2^k < \frac{1}{2} \sum_{E \in I} \left\lfloor \frac{\beta}{X_E} \right\rfloor + 2^k \tag{24}$$

Since the number of numbers that are non-coprime to β and smaller β is, on the one hand, equal to $\sum_{E \in I} \left\lfloor \frac{\beta}{X_E} \right\rfloor$, on the other hand, substituting $\beta - \phi(\beta)$ in (24), we find that the number of numbers non-coprime to β and less than $\frac{\beta}{2}$ is less then:

$$\frac{1}{2}\big(\beta - \phi(\beta)\big) + 2^k \tag{25}$$

Therefore, the number of numbers coprime to β and less than $\frac{\beta}{2}$ is greater than or equal to:

$$\frac{\beta}{2} - \left(\frac{1}{2}\big(\beta - \phi(\beta)\big) + 2^k\right) = \frac{1}{2}\phi(\beta) - 2^k = \frac{\phi(\beta) - 2^{k+1}}{2} \tag{26}$$

Hence, the probability to obtain Q is less than $\frac{2}{\phi(\beta)-2^{k+1}}$.

Now, we show the computational security of the proposed scheme. The concept of computational security is based on the following idea: information cannot be effectively restored if there is no complete information. Therefore, the scheme is computationally secure, if the adversary knows the secrets $S^{(1)}, S^{(2)}$ and incomplete sets of shares $C^{(1)}, C^{(2)}$, but cannot map $\left(S^{(1)}, C^{(1)}\right)$ and $\left(S^{(2)}, C^{(2)}\right)$ unambiguously.

Computational security for secret sharing schemes can be defined in more strong way [15]. It is based on the polynomial indistinguishability concept [16-23]. For any probability distribution $D(C,S)$, a secret sharing scheme is computationally secure if, for any pair of secrets $S^{(1)}, S^{(2)}$ and incomplete subsets of shares $C^{(1)}$ and $C^{(2)}$, the distributions $D\left(C^{(1)}, S^{(1)}\right)$ and $D\left(C^{(1)}, S^{(1)}\right)$ are polynomial indistinguishable, i.e. for any probabilistic algorithm A

$$\left|\Pr\left(A\left(D\left(C^{(1)}, S^{(1)}\right)\right)=1\right)-\Pr\left(A\left(D\left(C^{(2)}, S^{(2)}\right)\right)=1\right)\right|<\frac{1}{poly(n,k)},$$

where $poly(n,k)$ is the some polynomial over the amount of possible shares.

Theorem 2. *The proposed scheme is computationally secure if* $k \leq 4$.

Proof. To prove the computational security of proposed scheme, we use the auxiliary inequality.

$$\forall\, a,b,c \in R: |a-b| \leq |a-c| + |b-c| \tag{27}$$

Let $= \Pr\left(A\left(D\left(C^{(1)}, S^{(1)}\right)\right)=1\right),\ b = \Pr\left(A\left(D\left(C^{(2)}, S^{(2)}\right)\right)=1\right),\ c = \Pr\left(D\left(C^{(1)}, S^{(1)}\right)=1\right)$. We have:

$$\begin{aligned}
&\left|\Pr\left(\mathrm{A}\left(\mathrm{D}\left(\mathrm{C}^{(1)}, \mathrm{S}^{(1)}\right)\right)=1\right)-\Pr\left(\mathrm{A}\left(\mathrm{D}\left(\mathrm{C}^{(2)}, \mathrm{S}^{(2)}\right)\right)=1\right)\right| \\
&\leq \left|\Pr\left(\mathrm{A}\left(\mathrm{D}\left(\mathrm{C}^{(1)}, \mathrm{S}^{(1)}\right)\right)=1\right)-\Pr\left(\mathrm{D}\left(\mathrm{C}^{(1)}, \mathrm{S}^{(1)}\right)=1\right)\right| \\
&\quad+\left|\Pr\left(\mathrm{A}\left(\mathrm{D}\left(\mathrm{C}^{(2)}, \mathrm{S}^{(2)}\right)\right)=1\right)-\Pr\left(\mathrm{D}\left(\mathrm{C}^{(1)}, \mathrm{S}^{(1)}\right)=1\right)\right|
\end{aligned} \tag{28}$$

where $\Pr\left(D\left(C^{(1)}, S^{(1)}\right)=1\right)$ is the probability of obtaining the secret using the first k shares.

Since the number of desired outcomes is less than or equal to $\prod_{i=1}^{k} p_i$ and the total number of all outcomes is $\prod_{i=1}^{n} p_i$, then the probability is

$$\Pr\left(\mathrm{A}\left(\mathrm{D}\left(\mathrm{C}^{(1)}, \mathrm{S}^{(1)}\right)\right)=1\right) \leq \frac{\prod_{i=1}^{k} p_i}{\prod_{i=1}^{n} p_i} = \frac{1}{\prod_{i=k+1}^{n} p_i},$$

$$\Pr\left(\mathrm{A}\left(\mathrm{D}\left(\mathrm{C}^{(2)}, \mathrm{S}^{(2)}\right)\right)=1\right) \leq \frac{\prod_{i=1}^{k} p_i}{\prod_{i=1}^{n} p_i} = \frac{1}{\prod_{i=k+1}^{n} p_i},$$

$$\Pr\left(\mathrm{D}\left(\mathrm{C}^{(1)}, \mathrm{S}^{(1)}\right)=1\right) = \frac{1}{\prod_{i=1}^{k} p_i}.$$

From Condition 4 and $\mathrm{k} \geq 4$, it follows that $\mathrm{p}_1^{\mathrm{k}} < \prod_{\mathrm{i}=1}^{\mathrm{k}} \mathrm{p_i} < 2^{\mathrm{k}} \mathrm{p}_1^{\mathrm{k}}$ and $\mathrm{p}_1^{\mathrm{n-k}} < \prod_{\mathrm{i}=\mathrm{k}+1}^{\mathrm{n}} \mathrm{p_i} < 2^{\mathrm{n-k}} \mathrm{p}_1^{\mathrm{n-k}}$.

Therefore, $\frac{1}{2^k p_1^k} < \frac{1}{\prod_{i=1}^{k} p_i} < \frac{1}{p_1^k}$ and $\frac{1}{2^{n-k} p_1^{n-k}} < \frac{1}{\prod_{i=k+1}^{n} p_i} < \frac{1}{p_1^{n-k}}$.

Let us estimate terms of (28):

$$\left|\Pr\left(\mathrm{A}\left(\mathrm{D}\left(\mathrm{C}^{(1)}, \mathrm{S}^{(1)}\right)\right)=1\right)-\Pr\left(\mathrm{D}\left(\mathrm{C}^{(1)}, \mathrm{S}^{(1)}\right)=1\right)\right| < \max\left\{\frac{1}{p_1^{n-k}}-\frac{1}{2^k p_1^k}, \frac{1}{p_1^k}-\frac{1}{2^{n-k} p_1^{n-k}}\right\} \tag{29}$$

$$\left|\Pr\left(\mathrm{A}\left(\mathrm{D}\left(\mathrm{C}^{(2)}, \mathrm{S}^{(2)}\right)\right)=1\right)-\Pr\left(\mathrm{D}\left(\mathrm{C}^{(1)}, \mathrm{S}^{(1)}\right)=1\right)\right| < \max\left\{\frac{1}{p_1^{n-k}}-\frac{1}{2^k p_1^k}, \frac{1}{p_1^k}-\frac{1}{2^{n-k} p_1^{n-k}}\right\}.$$

By substituting (29) in (28), we obtain:

$$\left|\Pr\left(A\left(D\left(C^{(1)},S^{(1)}\right)\right)=1\right)-\Pr\left(A\left(D\left(C^{(2)},S^{(2)}\right)\right)=1\right)\right| \tag{30}$$
$$<2\cdot\max\left\{\frac{1}{p_1^{n-k}}-\frac{1}{2^k p_1^k},\frac{1}{p_1^k}-\frac{1}{2^{n-k}p_1^{n-k}}\right\}.$$

It means that the proposed scheme satisfies the formal definition of computational security.

The theorem is proven.

Theorem 2 has a significant practical importance. It states that the adversary cannot obtain any information from an incomplete set of shares.

Let $(S^{(1)},C^{(1)})$ and $(S^{(2)},C^{(2)})$ satisfy the following assertions for all $i\in[1,\dots,n]$:

$$c_i^{(1)}=\left|S^{(1)}+\mathrm{Q}\cdot rand_1\right|_{p_i},c_i^{(2)}=\left|S^{(2)}+Q\cdot rand_2\right|_{p_i} \tag{31}$$

Since for all $\in[1,\dots,n]$ $\gcd(\mathrm{Q},p_i)=1$, there exist $rand_1'$, $rand_2'$, Q' such that the following equations are satisfied:

$$c_i^{(1)}=\left|S^{(2)}+\mathrm{Q}'\cdot rand_2'\right|_{p_i},c_i^{(2)}=\left|S^{(1)}+\mathrm{Q}'\cdot rand_1'\right|_{p_i}. \tag{32}$$

From (31) and (32), it follows that to unambiguously map $(S^{(1)},C^{(1)})$ and $(S^{(2)},C^{(2)})$, Q is required. Since Q is not known, our scheme is computationally secure.

6. Conclusion

We propose and analyze computationally secure threshold secret sharing schemes based on the minimally redundant modular code. We show that a minimally redundant modular code does not possess the compact sequence property. We study the selection of circuit parameters to minimize redundancy while ensuring data security. We demonstrate that a scheme has minimal redundancy if it satisfies Conditions 2 and 3.

We prove the security property of the proposed modification of the secret sharing scheme. The probability of a secret being obtained by an attacker is provided, as well as we prove the computational security of this scheme. This information shows a possible level of security that allows working out a more detailed strategy for protecting data in cloud storages when applying this modification.

In the future work, we plan to study the applicability of the proposed scheme in different areas: homomorphic data encryption; efficient implementation of data encoding and decoding algorithms using artificial neural networks and minimally redundant modular code; generating moduli with the property of minimally redundant modular code; implementing safe and reliable storage systems for processing and transmitting data in cloud computing; building devices of low-power devices for use in the design of smart Internet of things, etc.

Acknowledgments

This work was supported by a grant from the Russian Science Foundation Grant No. 19-71-10033.

References

[1] Ţiplea F L and Drăgan C C 2014 A necessary and sufficient condition for the asymptotic idealness of the GRS threshold secret sharing scheme *Inf. Process. Lett.* **114** 299–303

[2] Drăgan C C and Tiplea F L 2018 On the asymptotic idealness of the Asmuth-Bloom threshold secret sharing scheme *Inf. Sci. (Ny).* **463–464** 75–85

[3] Muhammad Y I, Kaiiali M, Habbal A, Wazan A S and Sani Ilyasu A 2016 A secure data outsourcing scheme based on Asmuth-Bloom secret sharing *Enterp. Inf. Syst.* **10** 1001–1023

[4] Tchernykh A, Babenko M, Chervyakov N, Miranda-López V, Kuchukov V, Cortés-Mendoza J M, Deryabin M, Kucherov N, Radchenko G and Avetisyan A 2018 AC-RRNS: Anti-collusion secured data sharing scheme for cloud storage *Int. J. Approx.Reason.* **102** 60–73
[5] Barsi F and Maestrini P 1973 Error Correcting Properties of Redundant Residue Number Systems *IEEE Trans. Comput.* **C–22** 307–315
[6] Huang 1983 A Fully Parallel Mixed-Radix Conversion Algorithm for Residue Number Applications *IEEE Trans. Comput.* **C–32** 398–402
[7] Gbolagade K A and Cotofana S D 2009 An O(n) Residue Number System to Mixed Radix Conversion technique *2009 IEEE International Symposium on Circuits and Systems* (IEEE) pp 521–524
[8] Tchernykh A, Babenko M, Chervyakov N, Miranda-Lopez V, Avetisyan A, Drozdov A Y, Rivera-Rodriguez R, Radchenko G and Du Z 2020 Scalable Data Storage Design for Non-Stationary IoT Environment with Adaptive Security and Reliability *IEEE Internet Things J.*
[9] Sung-Ming Yen, Seungjoo Kim, Seongan Lim and Sang-Jae Moon 2003 RSA speedup with chinese remainder theorem immune against hardware fault cryptanalysis *IEEE Trans. Comput.* **52** 461–472
[10] Chervyakov N, Babenko M, Tchernykh A, Kucherov N, Miranda-López V and Cortés-Mendoza J M 2019 AR-RRNS: Configurable reliable distributed data storage systems for Internet of Things to ensure security *Futur. Gener. Comput. Syst.* **92** 1080–1092
[11] Chervyakov N I, Molahosseini A S, Lyakhov P A, Babenko M G and Deryabin M A 2017 Residue-to-binary conversion for general moduli sets based on approximate Chinese remainder theorem *Int. J. Comput. Math.* **94** 1833–1849
[12] Chervyakov N I, Babenko M G, Lyakhov P A and Lavrinenko I N 2014 An Approximate Method for Comparing Modular Numbers and its Application to the Division of Numbers in Residue Number Systems* *Cybern. Syst. Anal.* **50** 977–984
[13] Chernyavsky A F, Kolyada A A 2009 Scaling Method and Algorithm in the Minimum Redundant Modular Counting System *Reports of the NAS of Belarus* **53** 29–37
[14] Asmuth C and Bloom J 1983 A modular approach to key safeguarding *IEEE Trans. Inf. Theory* **29** 208–210
[15] Krawczyk H 1993 Secret Sharing Made Short *Proceedings in the 13th Annual International Cryptology Conference*, **93** 136-146
[16] Quisquater M, Preneel B, Vandewalle J 2002 On the security of the threshold scheme based on the Chinese remainder theorem *Proceedings in the International Workshop on Public Key Cryptography* 199-210.
[17] Babenko M, Tchernykh A, Chervyakov N, Kuchukov V, Miranda-López V, Rivera-Rodriguez R, Du Z and Talbi E-G 2019 Positional Characteristics for Efficient Number Comparison over the Homomorphic Encryption *Program. Comput. Softw.* **45** 532–543
[18] Tchernykh A, Miranda-López V, Babenko M, Armenta-Cano F, Radchenko G, Drozdov A Y and Avetisyan A 2019 Performance evaluation of secret sharing schemes with data recovery in secured and reliable heterogeneous multi-cloud storage *Cluster Comput.* **22** 1173–1185
[19] Tchernykh A, Schwiegelsohn U, Talbi E and Babenko M 2019 Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability *J. Comput. Sci.* **36** 100581
[20] Lopez-Falcon E C, Miranda-López V, Tchernykh A, Babenko M and Avetisyan A 2019 Bi-objective Analysis of an Adaptive Secure Data Storage in a Multi-cloud *Communications in Computer and Information Science* **979** pp 307–321
[21] García-Hernández L E, Tchernykh A, Miranda-López V, Babenko M, Avetisyan A, Rivera-Rodriguez R, Radchenko G, Barrios-Hernandez C J, Castro H and Drozdov A Y 2020 Multi-objective Configuration of a Secured Distributed Cloud Data Storage *Communications in Computer and Information Science* **1087** pp 78–93

[22] Miranda-López V, Tchernykh A, Cortés-Mendoza J M, Babenko M, Radchenko G, Nesmachnow S and Du Z 2018 Experimental Analysis of Secret Sharing Schemes for Cloud Storage Based on RNS *Communications in Computer and Information Science* **796** pp 370–383

[23] Tchernykh A, Cortés-Mendoza J M, Bychkov I, Feoktistov A, Didelot L, Bouvry P, Radchenko G and Borodulin K 2019 Configurable cost-quality optimization of cloud-based VoIP *J. Parallel Distrib. Comput.* **133** 319–336