Implementation of Cryptographic Transformations for Digital Security Using the Residue Number System

Alina Yanko [1,*,†], Victor Krasnobayev [1,†], Alina Hlushko [1,†] and Mykhailo Myziura [1,†]

[1] National University «Yuri Kondratyuk Poltava Polytechnic», Pershotravnevyj Ave 24, Poltava, 36011, Ukraine

Abstract

This paper investigates the issues of strengthening business security during digital transformation. The authors demonstrate that the expansion of digitalization processes necessitates a reevaluation of the economic security concept. It is substantiated that in order to strengthen business resilience to risks and threats to digital security, it is necessary to implement a number of measures aimed at protecting the confidentiality, integrity and availability of information. A study of cyber threats to national economic entities and citizens was conducted, including with the use of artificial intelligence tools. This made it possible to identify a priority area of data protection – improving the RSA cryptosystem. This research details the development of efficient information processing strategies for reducing the latency of RSA cryptographic functions. To accelerate RSA cryptographic transformations, this study introduces methods for high-speed information processing. The core of suggested method involves the realization of a cyclic shift mechanism utilizing modular arithmetic, entirely implemented by the residue number system (RNS). The application of RNS demonstrates its effectiveness in structuring the process of implementing modular integer arithmetic operations for accelerating public-key cryptographic transformations.

Keywords

binary remainder representation technique, cryptographic information protection, cryptography algorithm, cyclic shift arrays, digital transformation, high-speed crypto accelerators, modular arithmetic codes, residue number system, ring shift mechanism

1. Introduction

The concept of ensuring economic security of Ukrainian business in active digital transformation has undergone a significant rethinking. Despite the unprecedented challenges and threats posed by Russia's military invasion, government regulatory measures to support all sectors of the national economy [1] continued with a new vector to increase business resilience by accelerating digital transformation. Digitalization has become a key tool in overcoming war risks and ensuring the adaptability of business entities in the face of uncertainty. At the same time, the digital economy is raising the issue of countering digital security threats [2].

Ukrainian business remains particularly vulnerable to digital security risks in the constant growth of cyberattacks from the aggressor country. Digital security incidents have significant economic and social consequences, including damage to reputation, financial losses, recovery costs, etc. [3]. Cyber incidents threaten the availability, integrity, and confidentiality of information and systems. In this context, the need to improve the level of digital security of business is undeniable.

One of the most relevant areas is the improvement of cryptographic information security systems.

ICST-2025: Information Control Systems & Technologies, September 24-26, 2025, Odesa, Ukraine
* Corresponding author.
† These authors contributed equally.
al9_yanko@ukr.net (A. Yanko); v.a.krasnobaev@gmail.com (V. Krasnobayev); glushk.alina@gmail.com (A. Hlushko); myziura.work@gmail.com (M. Myziura)
0000-0003-2876-9316 (A. Yanko); 0000-0001-5192-9918 (V. Krasnobayev); 0000-0002-4086-1513 (A. Hlushko); 0009-0009-9301-2054 (M. Myziura)

Contemporary public-key cryptosystems commonly employ transformations based on algebraic curves, including elliptic curves (EC), hyperelliptic curves (HEC) [4, 5], Picard curves (PC), and superelliptic curves (SEC) [6], alongside traditional RSA systems. A prevailing direction in cryptographic information processing research focuses on extending key lengths. However, this approach inherently leads to a reduction in the processing speed of public-key cryptosystems [7, 8]. This slowdown is particularly problematic when implementing EC-based cryptosystems in resource-constrained environments, such as specialized systems and devices where the use of high-performance, multi-precision computers is not feasible [9]. Consequently, there is a pressing need for the development of techniques that enhance the efficiency, reliability, and security of cryptographic transformations [10]. The proposed approach, which leverages the residue number system (RNS), offers a significant advantage over existing hardware implementations of RSA by fundamentally altering the arithmetic operation paradigm. Unlike traditional positional number systems that rely on sequential digit processing and suffer from inter-digit carry propagation; RNS enables highly parallel execution of modular arithmetic operations. This inherent parallelism, particularly for modular multiplication and squaring which dominate RSA computations, allows for a substantial reduction in latency and an increase in throughput, making it a promising solution for high-speed crypto accelerators in real-time applications. For a comprehensive evaluation of novel cryptographic acceleration methods, comparative performance indicators against established techniques are essential for objectively assessing their practical utility and superiority.

2. Analysis of the problem of cryptographic information protection to strengthen business security in a digital transformation

Since the beginning of Russia's full-scale invasion, the number of cyberattacks against Ukraine has been steadily increasing [11]. According to official data from Forbes Ukraine, the losses caused by cybercrime to Ukrainian businesses in 2022 increased by 96% compared to 2021. Their absolute value amounted to UAH 1 billion (EUR 24 million) [12]. Average losses per cyberattack increased by 49% to UAH 7,900 (EUR 190). According to the Ministry of Digital Transformation of Ukraine, the problem of information security increased by 14% in 2021-2023. In 2022, 60% of the adult population and every 8 out of 10 adolescents experienced a data security breach [13]. Unfortunately, official data on the frequency and type of digital security incidents after the full-scale Russian invasion are not available. However, data collected prior to this period shows an increase in the vulnerability of Ukrainian businesses to digital security threats.

During the war, cybercriminals scaled up their criminal business using artificial intelligence [14, 15]. One of the most common types of crimes is the issuance of loans for missing military personnel and citizens who have traveled abroad [16], including through the forgery of an electronic digital signature. Accordingly, the issue of cryptographic protection of information to strengthen the security of business and citizens is relevant and supported by existing research and development.

A comprehensive examination of techniques aimed at enhancing the efficiency of scalar multiplication (SC) within the Jacobian of hyperelliptic curves (HEC) provides both theoretical and empirical justification for the dependence of SC operation performance on several key factors. These factors include: the implementation modality of cryptographic transformations (software, hardware, or hybrid); the specific algorithm employed for HEC divisors; the underlying base field over which the curve is defined; the curve's type and coefficient values; the chosen coordinate system for representing Jacobian divisors (affine, projective, weighted, or hybrid); and the selected arithmetic transformation method within the Jacobian.

Existing methodologies for implementing scalar multiplication algorithms, such as the Kantor divisor addition method, the Koblitz method, various arithmetic transformation methods for HEC Jacobian divisors, weighted divisor addition techniques, the Karatsuba method for modular multiplication and polynomial function field reduction, and methods leveraging aspects of the Chinese Remainder Theorem, often fail to meet the stringent efficiency requirements of modern

cryptographic applications. Conversely, the literature [17, 18] highlights the substantial advantages of modular arithmetic codes, specifically the RNS, for accelerating digital information processing tasks, including digital filtering, Fast Fourier Transform (FFT), and Discrete Fourier Transform (DFT) implementations.

This context underscores the critical importance and timeliness of developing novel approaches to improve the performance of cryptographic transformations, particularly RSA, through the utilization of RNS. The RSA system, initially proposed in 1977, remains the most prevalent public-key cryptosystem in use today [19-21].

The primary goal of the studies documented in [22, 23] is to formulate a method for rapid execution of public-key cryptographic transformations and to design a structural model for the operating unit (OU) of a high-speed cryptographic coprocessor, leveraging the capabilities of RNS. The research [24] presents a modified stream cipher cryptographic processor equipped with specialized instructions based on the VLIW architecture. The proposed system utilizes a distributed (clustered) memory structure and is designed for efficient execution of stream cipher operations. Such architecture ensures high performance in processing stream cryptographic algorithms.

Research in [25] investigates the impact of fundamental properties of the modular number system (MNS), such as remainder independence, equality, and the presence of low-order digits, on the architecture and operational principles of crypto accelerator systems utilizing MNS. Specifically, it highlights that the presence of low-order digits in modular representations allows for a wide array of system and technical design choices when implementing integer modular arithmetic operations.

There are four primary methodologies for performing arithmetic operations within RNS: the summation method (utilizing low-order bits of binary adders modulo RNS); the table lookup method (employing read-only memory); the direct logical method, which involves defining and implementing modular operations at the switching function level to generate result values (systolic arrays, programmable logic matrices, and programmable logic devices (PLDs) are suitable hardware platforms for this approach) [26]; and the ring shift mechanism (RSM), which leverages cyclic shift arrays (CSA).

A significant and highly advantageous characteristic of RNS, when based on modular multiplication algorithms, is the absence of inter-remainder carry propagation during cryptographic transformations within the cryptographic coprocessors employing the ring shift mechanism (RSM). While intra-remainder carries exist between binary digits within each modulus p_n, the elimination of carry propagation between remainders during modular operations [27] presents a key benefit.

3. Methodological approach to improving the RSA cryptosystem

In a positional number system (PNS), arithmetic operations necessitate sequential digit processing due to operation-specific rules, preventing completion until all intermediate results, reflecting inter-digit dependencies, are determined. Consequently, PNS, prevalent in contemporary high-speed crypto accelerators (HSCA), suffers from inherent inter-digit connections that complicate arithmetic operation implementation, demand complex hardware, compromise computational reliability, and limit cryptographic transformation speed [28]. Therefore, a number system devoid of inter-digit dependencies is desirable. The RNS offers this advantage, possessing a unique property: the independence of remainders based on the chosen base [29]. This independence facilitates the development of novel machine arithmetic and fundamentally new HSCA architectures, thereby expanding the applicability of machine arithmetic. Numerous studies [30-32] suggest that adopting non-traditional data representation and parallel processing in digital systems enhances computational efficiency, particularly in modular arithmetic, which exhibit maximum internal parallelism during information processing. RNS falls within this category.

Several factors support the effective utilization of RNS in HSCA: HSCA, like RNS, processes only integer data; HSCA primarily performs modular arithmetic operations; RNS excels in

executing modular multiplication and squaring operations, which constitute over 95% of RSA cryptosystem operations, particularly in modulus p_n; as the word length (W) of HSCA processors increases, a trend in modern RSA system development, RNS application efficiency improves; the widespread use of CSA in HSCA for RSA transformations; the limitations of PNS in achieving significant HSCA efficiency and reliability gains; and promising preliminary results demonstrating RNS's effectiveness in enhancing real-time HSCA performance and reliability [33].

Research presented in [34] elucidates the operational principle of integer residual arithmetic, specifically the ring shift mechanism (RSM). This mechanism is distinguished by its ability to determine the result of arithmetic operations, such as $(y_n \pm u_n) \bmod p_n$, for any modulus p_n within the RNS base set $\{p_n\}$ $(n = \overline{1, q})$, without necessitating the computation of partial sums S_n or carry values C_n from binary adders in PNS. Instead, the result is derived through cyclic shifts of a predefined digital structure. This approach is grounded in Cayley's theorem, which establishes an isomorphism between the elements of a finite abelian group and those of a permutation group [35].

From Cayley's theorem, it can be inferred that the action of abelian group elements on the group of integers is homomorphic [36]. This property enables the organization of arithmetic operation result determination in RNS through the application of RSM. Thus, an operand in RNS is represented as a set of q remainders $\{y_n\}$ $(n = \overline{1, q})$, obtained by successively dividing an initial number Y by n pairwise prime numbers $\{p_n\}$. In this context, the collection of remainders $\{y_n\}$ directly corresponds to the sum of q simple Galois fields $GF(p_n)$ [37].

An algebraic system (A) consists of a plural (P) and a set of operations (F) defined on this set. This system is denoted as $A = (P, F)$, where P is a non-empty plural of integers (Z); F is a set of binary operations (specifically, in RNS implementation, the operations executed in a single clock cycle are the arithmetic operations: $+, -, \times$) [38]. That is, F is the set of operations addition (+), subtraction $(-)$, multiplication $(\times)$ for any $y_n, u_n \in Z$, $y_n + u_n$, $y_n - u_n$, $y_n \times u_n$ also belong to Z. It is important that the operations be closed on the plural P, that is, the result of the operation on elements from P also belongs to P. Therefore, it is very important that the range of representation of numbers in the MSN $D = \prod_{n=1}^{q} p_n$ overlaps the set P, that is, that the elements a and b themselves, and the result of the arithmetic operations $+, -, \times$, lie in this range. In cryptography, where information security is a key aspect, the use of large numbers becomes necessary to ensure the reliability and robustness of cryptographic systems. The larger the number of bits, the more difficult it is to break a cryptographic algorithm, as the number of possible combinations grows exponentially. Asymmetric cryptography algorithms, such as RSA, DSA, and ECC, are based on the use of large prime numbers to generate cryptographic keys [39]. The key operations in these algorithms are modular multiplication and exponentiation, which are performed on large-bit numbers. Given the increasing requirements for the speed of cryptographic systems, the optimization of these operations is a relevant area of research. In this context, the goal of our research is to develop and analyze a method for ultrafast execution of the modular addition operation in RNS, which can serve as an effective replacement for the modular multiplication and exponentiation operations, ensuring increased performance of cryptographic transformations [40].

Algebraic systems A is a plural P with operations F forming an algebraic system, for example, a group, ring, or field. Groups, rings, and fields are fundamental structures in abstract algebra, each defined by a set of axioms that specify the properties of operations. These structures are used to model a variety of mathematical objects and processes, from simple arithmetic operations to complex cryptographic algorithms.

One of the important directions in the study of algebraic systems is the study of factor structures, which allow us to build new algebraic objects based on existing ones. In particular, in the case of rings, we can construct a ring of subtraction classes, or a factor ring, which is a

powerful tool for analyzing the structure of rings and their properties.

Let us consider in more detail the process of constructing a ring of subtraction classes. Let R be a ring with the operations of addition (+) and multiplication ($\times$) defined on it, and J be an ideal of the ring R. The ideal J is a subset of R that satisfies certain conditions that allow us to partition R into subtraction classes. The subtraction class containing an element $y_n \in R$ is defined as the set $y_n + J = \{y_n + j \mid j \in J\}$. The set of all subtraction classes forms a new ring, called the subtraction class ring or factor ring, and is denoted by R/J. The operations of addition and multiplication in R/J are defined in terms of the operations in R, allowing us to inherit many properties from the original ring.

Subtraction class rings are an important tool for studying the structure of rings and their applications in various fields of mathematics and computer science, including cryptography, number theory, and algebraic geometry.

The factor ring R/J can be expressed as Z/p_n, where V represents the set of integers. When p_n, the base of the RNS, is a prime number, Z/p_n forms a finite field. Given the methodology for performing arithmetic operations within the RNS, it is advantageous to focus on an arbitrary finite Galois field $GF(p_n)$, where n remains constant, corresponding to a specific defined residue system. Leveraging the aforementioned properties, modular addition and subtraction operations in RNS can be implemented without inter-digit carry propagation using the RSM through q CSAs with a range of with a range of elements representation D, effectively achieved through ring shifts of digit representations utilizing bit shift registers [41].

4. Method for cryptographic transformation implementation

Based on the RSM proposed in the research, a method for performing arithmetic operations within the RNS is introduced, namely the binary remainder representation technique (BRRT). This approach, grounded in the principles of RNS, which originates from the Chinese remainder theorem [42], facilitates efficient execution of arithmetic operations, including addition, subtraction, and multiplication, on large-bit numbers. A key feature of BRRT is the utilization of binary representations for remainders [43], which allows for the substitution of complex multiplication and exponentiation operations with simpler shift and addition operations. This significantly enhances the speed of arithmetic computations, a critical factor for cryptographic algorithms where computational efficiency is paramount. Furthermore, BRRT enables parallel processing, further accelerating operation execution. These advantages render the proposed method highly promising for cryptographic systems that demand high performance and reliability [44]. Utilizing this approach, the primary (foundational) digital structure of the CSA for each modulus p_n of RNS is represented by the initial row (column) of the Cayley addition table, specifically $(y_n + u_n) \bmod p_n$, as illustrated in Fig. 1.

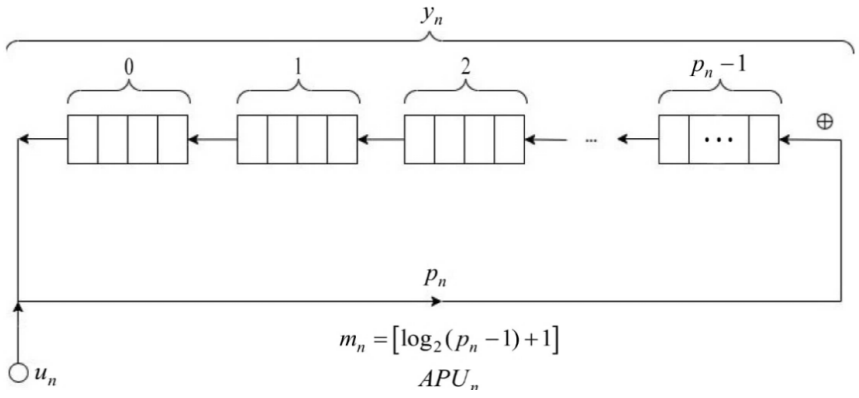

Figure 1: Primary digital structure of the CSA for modulus p_n in RNS

The primary digital structure of the CSA content for each modulus p_n can be expressed as:

$$B\_p_n = \left(B\_y_0 \,\|\, B\_y_1 \,\|\, \ldots \,\|\, B\_y_{p_n-1}\right), \tag{1}$$

where symbol $\|$ denotes the concatenation operation (combining, merging); B_y_j is a *m*-bit binary representation of the number y_j (while y_j iterates from 0 to $p_n - 1$) for modulus p_n.

The bit width *m* of the binary code of the primary digital structure of the CSA is determined by:

$$m_n = \left[\log_2(p_n - 1) + 1\right], \tag{2}$$

where square brackets [x] denotes the integer part of x, discarding the fractional part.

Given a specific modulus $p_n = 7$, the primary digital structure of the CSA content, derived from mathematical expression (1), is as follows:

$$B\_7 = \left(000 \,\|\, 001 \,\|\, 010 \,\|\, 011 \,\|\, 100 \,\|\, 101 \,\|\, 110\right).$$

Therefore, leveraging CSA, which are prevalent in binary PNS, especially within cryptography, facilitates the straightforward implementation of addition operations in the RNS. The degree *k* of cyclic displacements (shift) is established through the following expression, as per structure (1):

$$\left[B\_y_0 \,\|\, B\_y_1 \,\|\, \ldots \,\|\, B\_y_{p_n-1}\right] = \\ = \left[B\_y_k \,\|\, B\_y_{k+1} \,\|\, \ldots \,\|\, B\_y_0 \,\|\, \ldots \,\|\, B\_y_{p_n-1}\right]^k, \tag{3}$$

$$\left[B\_y_0 \,\|\, B\_y_1 \,\|\, \ldots \,\|\, B\_y_{p_n-1}\right]^{-k} = \\ = \left[B\_y_{p_n-1-k} \,\|\, B\_y_{p_n-k} \,\|\, \ldots \,\|\, B\_y_0 \,\|\, B\_y_1 \,\|\, \ldots \,\|\, B\_y_{p_n-k-2}\right]. \tag{4}$$

It is noteworthy that $\left[B\_y_0 \,\|\, B\_y_1 \,\|\, \ldots \,\|\, B\_y_{p_n-1}\right]^{p_n}$, implying that when $k = p_n$, all elements of the ordered set $\{B\_y_j\}$ remain in their original positions.

For the practical realization of this approach, the first term y_n indicates the quantity of CSA digit positions that hold the result of the modular operation $(y_n + u_n) \bmod p_n$, while the second term u_n indicates the number *k* shifts CSA applied to the primary CSA content (1), as defined by expressions (3)-(4). The number of shifts equals the product of the second term u_n and the bit width m_n of the CSA's primary digital structure binary code, i.e. $u_n \cdot m_n$ – the total binary digit displacement in a positive direction within the CSA Figure 2 depicts a potential operational architecture for the HSCA operating unit (OU) within the RNS.

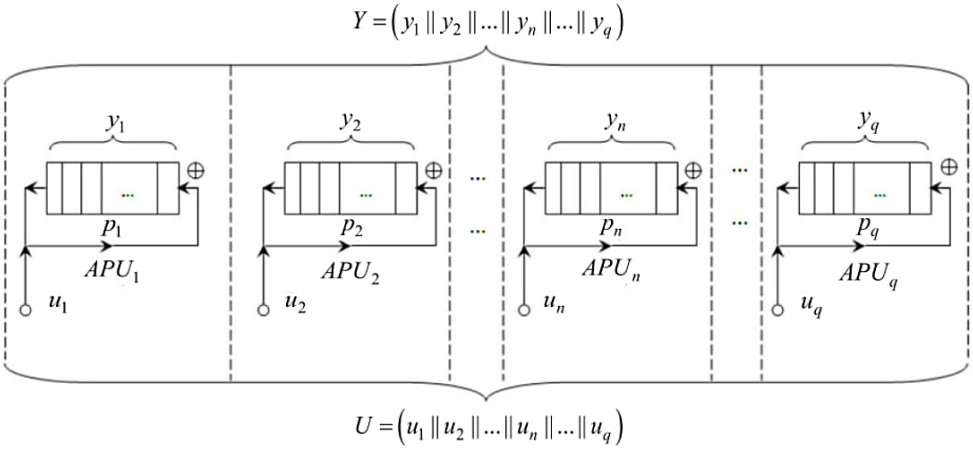

Figure 2: HSCA OU operation scheme for arbitrary RNS

For a comparative analysis of the execution time of integer addition in binary PNS and the RNS, it is necessary to determine the time required to add two numbers $Y=\left(y_1\|y_2\|...\|y_n\|...\|y_q\right)$ and $U=\left(u_1\|u_2\|...\|u_n\|...\|u_q\right)$, within the SRC utilizing the RSM. In the RSM, the time θ for modular addition of two remainders y_n and u_n, specifically in the circuit that calculates $(y_n+u_n)\bmod p_n$ $(n=\overline{1,\ q})$, is primarily governed by the time $\underset{\rightarrow}{\theta}$ needed to shift the primary contents of CSA digit positions (hereafter, we assume $\theta=\underset{\rightarrow}{\theta}$). The time of a single bit shift (trigger activation time) of the digital contents of CSA digit positions is given by the expression:

$$\underset{\rightarrow}{\theta}=3\cdot t', \tag{5}$$

where t' – switching time of a single logic gate (an AND, NOT, or OR gate).

Building upon prior research [45], the processing time for the modular addition of remainders y_n and u_n, specifically $(y_n+u_n)\bmod p_n$, within the RNS can be expressed by the ensuing expression:

$$\theta_{RNS}=V_n\cdot m_n\cdot\underset{\rightarrow}{\theta}, \tag{6}$$

where V_n – the second term u_n in the modular addition $(y_n+u_n)\bmod p_n$, which indicating the quantity of CSA digits cyclically shifted counterclockwise from the CSA's initial state, i.e. $V_n=\overline{0,\ p_n-1}$.

Thus, based on expressions (5) and (6), for an arbitrary modulus p_n of RNS, the addition time of two remainders y_n and u_n modulo p_n is defined by:

$$\theta_{RNS}=V_n\cdot\left[\log_2(p_n-1)+1\right]\cdot 3\cdot t'. \tag{7}$$

In this case, the maximum possible value of expression (7) for the arbitrary modulus m_i of RNS is defined by:

$$\theta_{RNS\_\max}=(p_n-1)\left[\log_2(p_n-1)+1\right]\cdot 3\cdot t'. \tag{8}$$

However, for the specified RNS, the maximum addition time of two numbers $Y=\left(y_1\|y_2\|...\|y_n\|...\|y_q\right)$ and $U=\left(u_1\|u_2\|...\|u_n\|...\|u_q\right)$ is determined by the maximum value of modulus p_q:

$$\theta'_{RNS\_\max}=(p_q-1)\left[\log_2(p_q-1)+1\right]\cdot 3\cdot t'. \tag{9}$$

In general, the addition time of two numbers $Y=\left(y_1\|y_2\|...\|y_n\|...\|y_q\right)$ and $U=\left(u_1\|u_2\|...\|u_n\|...\|u_q\right)$ in RNS is determined by the time (8) of realization of module operation $(y_n+u_n)\bmod p_n$ in *n*-th arithmetic processing unit (*APU*$_n$), i.e. in HSCA, in which instance $V_n\cdot m_n$ is reaches its peak $(V_n\cdot m_n=\max)$ across all $APU_e(e=\overline{1,q};\ n\neq e)$.

Previous studies [29, 45], focused on the optimization of the RSA cryptographic algorithm through the utilization of the RNS, have thoroughly examined the implementation of modular addition for one- and two-byte digit numbers. A simplified OD scheme for a one-byte HSCA processor in RNS is presented in Fig. 3.

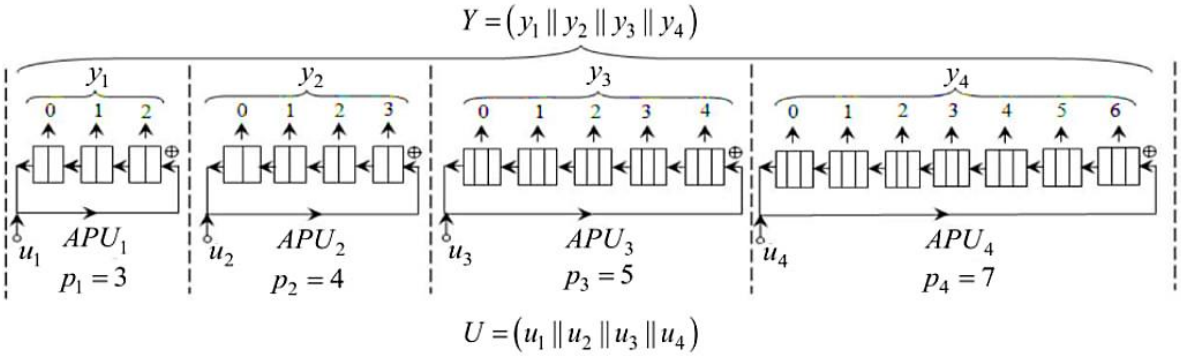

Figure 3: Simplified HSCA OU scheme of low-bit representation of numbers in RNS [45]

However, given the substantial range of number representation required for ensuring the robustness of the RSA cryptographic algorithm, there arises a necessity to investigate the effectiveness of RNS in processing large data arrays. A comprehensive analysis and illustrative examples demonstrating the advantages of employing RNS for modular addition of large-digit numbers will be presented.

Cases where operand sizes reach values typical for contemporary cryptographic applications will be considered, and results will be compared with conventional computational methods. This will enable the evaluation of the practical value of RNS for enhancing the performance of cryptographic systems.

Concrete example of implementing the addition operation for two numbers within the RNS are presented, utilizing the following set of moduli: $p_1=11$, $p_2=13$, $p_3=15$, and $p_4=p_q=19$, which provides a number representation range from 0 to $D=\prod_{n=1}^{q} p_n=11\cdot13\cdot15\cdot19=40755$ in the RNS. According to equation (8), the modular addition operation's execution time depends on the second addend and the modulus p_n of the respective APU_n, under the condition that $V_n\cdot m_n=\max$.

Example 1. If the second number $(U_{10}=95)$ is equal to $U_{RNS}=(111\|100\|101\|000)_2=$ $=(7\|4\|5\|0)_{10}$, then it is necessary to find the APU with the largest product value $V_n\cdot m_n$, therefore:

In the APU_1 with modulus $p_1=11$, the following values are obtained: $V_1=7$, $m_1=\left[\log_2(p_1-1)+1\right]=\left[\log_2(11-1)+1\right]=4$ and $V_1\cdot m_1=7\cdot4=28$.

In the APU_2 with modulus $p_2=13$, the following values are obtained: $V_2=4$, $m_2=\left[\log_2(p_2-1)+1\right]=\left[\log_2(13-1)+1\right]=4$ and $V_2\cdot m_2=4\cdot4=16$.

In the APU_3 with modulus $p_3=15$, the following values are obtained: $V_3=5$, $m_3=\left[\log_2(p_3-1)+1\right]=\left[\log_2(15-1)+1\right]=4$ and $V_3\cdot m_3=5\cdot4=20$.

In the APU_4 with modulus $p_4=19$, the following values are obtained: $V_4=0$, $m_4=\left[\log_2(p_4-1)+1\right]=\left[\log_2(19-1)+1\right]=5$ and $V_4\cdot m_4=0\cdot5=0$.

It is evident that the maximum binary digit shift, amounting to 28, is observed within the first arithmetic processing unit (APU_1). Consequently, the execution time for the addition of two numbers *Y* and *U*, represented in the RNS utilizing the ring shift mechanism, is determined by the value of the second term *U* and is equivalent to:

$$\theta_{RNS}=V_1\cdot\left[\log_2(p_1-1)+1\right]\cdot3\cdot t'=7\cdot4\cdot3\cdot t'=84\cdot t'.$$

Example 2. If the second number $(U_{10}=78)$ is equal to $U_{RNS}=(001\|000\|011\|010)_2=$ $=(1\|0\|3\|2)_{10}$, then it is necessary to find the APU with the largest product value $V_n\cdot m_n$,

therefore:

In the APU_1 with modulus $p_1 = 11$, the following values are obtained: $V_1 = 1$, $m_1 = \left[\log_2(p_1 - 1) + 1\right] = \left[\log_2(11 - 1) + 1\right] = 4$ and $V_1 \cdot m_1 = 1 \cdot 4 = 4$.

In the APU_2 with modulus $p_2 = 13$, the following values are obtained: $V_2 = 0$, $m_2 = \left[\log_2(p_2 - 1) + 1\right] = \left[\log_2(13 - 1) + 1\right] = 4$ and $V_2 \cdot m_2 = 0 \cdot 4 = 0$.

In the APU_3 with modulus $p_3 = 15$, the following values are obtained: $V_3 = 3$, $m_3 = \left[\log_2(p_3 - 1) + 1\right] = \left[\log_2(15 - 1) + 1\right] = 4$ and $V_3 \cdot m_3 = 3 \cdot 4 = 12$.

In the APU_4 with modulus $p_4 = 19$, the following values are obtained: $V_4 = 2$, $m_4 = \left[\log_2(p_4 - 1) + 1\right] = \left[\log_2(19 - 1) + 1\right] = 5$ and $V_4 \cdot m_4 = 2 \cdot 5 = 10$.

It is evident that the maximum binary digit shift, amounting to 12, is observed within the third arithmetic processing unit (APU_3). The execution time for the addition of two numbers *Y* and *U*, represented in the RNS utilizing the RSM, is equivalent to:

$$\theta_{RNS} = V_3 \cdot \left[\log_2(p_3 - 1) + 1\right] \cdot 3 \cdot t' = 3 \cdot 4 \cdot 3 \cdot t' = 36 \cdot t'.$$

An analysis comparing the time required to perform the addition of two numbers *Y* and *U* between PNS and RNS is provided. The addition time of numbers *Y* and *U* in PNS is:

$$\theta_{PNS} = \underset{\rightarrow}{\theta} \cdot (2 \cdot r - 1) = 3 \cdot t'(16 \cdot l - 1), \tag{10}$$

where $r = 8 \cdot l$ – the number of bits for an *l*-byte data unit; $\underset{\rightarrow}{\theta} = 3 \cdot t'$ – the summation time in the (*n*+1)th binary place of the positional adder for partial sum values S_{n+1} and carry values C_{n+1}.

Recognizing that an existing method achieves a two-fold shortening of the maximum operation time for modular addition in RNS, the following applies to RSM:

$$\theta''_{RNS\_\max} = \theta'_{RNS\_\max} / 2. \tag{11}$$

The ratio of addition operation execution times in PNS and RNS will be represented by a coefficient, namely:

$$\begin{gathered} \gamma = \theta_{PNS} / \theta''_{RNS\_\max} = \\ = \frac{(16 \cdot l - 1) \cdot 3 \cdot \underset{\rightarrow}{\theta} \cdot 2}{(p_q - 1) \cdot \left[\log_2(p_q - 1) + 1\right] \cdot 3 \cdot \underset{\rightarrow}{\theta}} = \\ = \frac{2 \cdot (16 \cdot l - 1)}{(p_q - 1) \cdot \left[\log_2(p_q - 1) + 1\right]}. \end{gathered} \tag{12}$$

The computational assessment and comparative evaluation of arithmetic operation execution times during cryptographic transformations demonstrated the significant effectiveness of the BRRT method, which utilizes the RSM within the RNS, when contrasted with a method employed in PNS (see Table 1).

It is important to note that Table 1 specifically presents a comparative analysis of the modular addition operation within the RNS versus the PNS. While these results highlight the efficiency gains at the fundamental arithmetic level, a direct comparative analysis of the overall RSA cryptosystem's performance using the proposed RNS-based acceleration against other established RSA acceleration methods (e.g., Montgomery multiplication, Karatsuba algorithm, or dedicated hardware implementations) is a complex task that requires specific experimental setups and is beyond the scope of this initial theoretical and methodological paper.

The presented data are derived without the inclusion of supplementary algorithms, which, if implemented, could expedite the execution of modular arithmetic operations. The resulting mathematical expressions (7)–(9) and (12), along with the determined operational times for arithmetic operations in RNS, can be utilized for evaluating and comparing the computational complexity of RSA cryptographic transformation algorithms.

Table 1
Data of comparative analysis of time of addition operation

$l\ (r)$	PNS	RNS			%
	$\theta_{PNS}\ /\ 3\cdot t'$	p_q	m_q	$\theta''_{RNS\_\max}\ /\ 3\cdot t'$	
4 (32)	63	19	5	48	31.25
8 (64)	127	30	5	75	69.33

5. Conclusion

Economic security of businesses undergoing digital transformation necessitates a paradigm shift in our conceptual approach. In the face of martial law threats, Ukraine's national economy has demonstrated a commendable level of cyber resilience. However, to bolster business resilience against evolving digital security risks, the current approach requires augmentation. Specifically, enhancing the RSA cryptosystem is crucial.

This paper introduced a novel method for accelerating cryptographic transformations within Galois fields, focusing on improving the efficiency of RSA cryptosystems with public keys. The proposed method leverages the RNS. By exploiting the fundamental theoretical properties of RNS, we have effectively streamlined the execution of modular operations essential for cryptographic tasks.

Furthermore, we have presented a practical method for realizing arithmetic operations in RNS based on a ring shift mechanism, namely the binary remainder representation technique. The efficiency analysis and concrete technical implementation examples of modular arithmetic operations substantiate the practical feasibility of this approach. This method of information processing is highly recommended for crypto accelerators enabling real-time security surveillance and secure authentication.

The application of the proposed method significantly reduces the execution time of operations, which is critical for ensuring real-time security. The obtained results confirm the practical value of RNS in enhancing the performance of cryptographic systems, particularly when processing large data arrays, which is typical for modern cryptographic applications.

The research findings offer significant potential for application in systems and devices designed for high-throughput, real-time digital information processing. Practical examples confirm its feasibility for real-time applications, strengthening digital security infrastructure, especially in dynamic environments. The implementation of this method not only improves the speed of critical cryptographic processes, but also enhances the overall security posture of digital systems. Moreover, while this study specifically focuses on RSA, the core principles of RNS-based modular arithmetic and the cyclic shift mechanism are inherently adaptable to other cryptographic algorithms that heavily rely on modular exponentiation and multiplication, such as ElGamal, Diffie-Hellman, and various elliptic curve cryptography (ECC) schemes. The parallel processing capabilities offered by RNS make it a versatile foundation for accelerating a broad spectrum of public-key cryptographic operations beyond RSA. As such, it represents a substantial advancement in the field of secure computation. By enhancing the speed and efficiency of cryptographic operations, this method contributes to strengthening the digital security infrastructure, particularly critical in dynamic and challenging environments.

Future work will focus on a comprehensive experimental evaluation of the proposed RNS-based RSA acceleration method against state-of-the-art hardware and software implementations of RSA, including detailed comparative performance indicators such as throughput, latency, and resource utilization. This will provide a more objective and complete assessment of its practical advantages and potential for real-world deployment.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] L. Svistun, A. Glushko, K. Shtepenko, Organizational aspects of development projects implement at the real estate market in Ukraine, International Journal of Engineering and Technology (UAE) 7 (2018) 447–452. doi:10.14419/ijet.v7i3.2.14569.

[2] V. Kharchenko, Y. Ponochovnyi, O. Ivanchenko, H. Fesenko, O. Illiashenko, Combining Markov and Semi-Markov Modelling for Assessing Availability and Cybersecurity of Cloud and IoT Systems, Cryptography, 6(3) (2022) 1–33. doi:10.3390/cryptography6030044.

[3] OECD, Enhancing Resilience by Boosting Digital Business Transformation in Ukraine, 2024. URL: https://www.oecd.org/en/publications/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_4b13b0bb-en.html.

[4] Dr. Pasumpon Pandian A., Development of Secure Cloud Based Storage Using the Elgamal HyperElliptic Curve Cryptography with Fuzzy Logic Based Integer Selection, Journal of Soft Computing Paradigm (JSCP), 2(1) (2020) 24–35. doi:10.36548/jscp.2020.1.003.

[5] U. Shamsher, D. Nizamud, Blind signcryption scheme based on hyper elliptic curvescryptosystem, Peer-to-Peer Networking and Applications, 14 (2021) 917–932. doi:10.1007/s12083-020-01044-8.

[6] A. Dia E. Beriniet, M. A. Ferrag, B. Farou, H. Seridi, HCALA: Hyperelliptic curve-based anonymous lightweight authentication scheme for Internet of Drones, Pervasive and Mobile Computing 92 (2023) 101798. doi:10.1016/j.pmcj.2023.101798.

[7] R. Kochan, S. Yevseiev, R. Korolyov, S. Milevskyi, I. Ireifidzh, T. Gancarczyk, Development of Methods for Improving Crypto Transformations in the Block-Symmetric Code, in: 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), IEEE, Dortmund, Germany, 2020, pp. 1–9. doi:10.1109/IDAACS-SWS50031.2020.9297102.

[8] O. Laktionov, L. Lievi, A.Tretia, M. Movin, Investigation of combined ensemble methods for diagnostics of the quality of interaction of human-machine systems, Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu 4 (2023) 138–143. doi:10.33271/nvngu/2023-4/138.

[9] Yu. Horbenko, M. Yesina, V. Onoprienko, G. Maleeva, Threat models for asymmetric cryptotransformations of the promising electronic signature, Radiotekhnika, 3(202) (2020) 72–78. doi:10.30837/rt.2020.3.202.07.

[10] K. Abirami, R. Srikanth, R. Kavitha, Comparative Analysis of Elliptic Curve Cryptography Methods and Survey of Its Applications, International Journal of Intelligent Systems and Applications in Engineering, 11(11s) (2023) 430–434. URL: https://ijisae.org/index.php/IJISAE/article/view/3509.

[11] V. Krasnobayev, A. Yanko, A. Hlushko, O. Kruk, O. Kruk, V. Gakh, Cyberspace protection system based on the data comparison method, in: Economic and cyber security. Kharkiv: PC TECHNOLOGY CENTER, 2023, pp. 3–29. doi:10.15587/978-617-7319-98-5.ch1.

[12] Forbes, The losses of Ukrainians from cybercrime increased to UAH 1 billion lastyear - EMA research, 2023. URL: https://forbes.ua/news/zbitki-ukraintsiv-vid-kiberzlochinnosti-torik-zroslido-1-mlrd-grn-doslidzhennya-ema-21022023-11884.

[13] Ministry of Digital Transformation of Ukraine, Digital Literacy Research – 2023, 2023. URL: https://osvita.diia.gov.ua/uploads/1/8801-en_cifrova_gramotnist_naselenna_ukraini_ 2023.pdf.

[14] O. Shefer, O. Laktionov, V. Pents, A. Hlushko, N. Kuchuk, Practical principles of integrating artificial intelligence into the technology of regional security predicting, Advanced Information Systems, 8 (1) (2024) 86–93. doi:10.20998/2522-9052.2024.1.11.

[15] V. Onyshchenko, S. Yehorycheva, O. Maslii, N. Yurkiv, Impact of Innovation and Digital Technologies on the Financial Security of the State, in: V. Onyshchenko, G. Mammadova, S.

Sivitska, A. Gasimov (Eds.), Proceedings of the 3rd International Conference on Building Innovations (ICBI 2020), volume 181 of Lecture Notes in Civil Engineering, Springer, Cham, 2022, pp. 749–759. doi:10.1007/978-3-030-85043-2_69.
[16] Government of Ukraine, Strategy for the recovery, sustainable development and digital transformation of small and medium-sized enterprises for the period up to 2027, 2024. URL: https://uaeumeter.com.ua/en/laws/.
[17] S. Onyshchenko, A. Yanko, A. Hlushko, O. Maslii, A. Cherviak, Cybersecurity and improvement of the information security system, Journal of the Balkan Tribological Association, 29(5) (2023) 818–835. URL: https://scibulcom.net/en/article/L8nV7It2dVTBPX09mzWB.
[18] S. Albusifi, S. Mugassab, A. Elferjani, RSA Cryptography Algorithm and its Applications to Security System by Using Linear Congruence, International Journal of Multidisciplinary Sciences and Advanced Technology Special 1 (2021) 558–564. URL: https://www.researchgate.net/publication/380320192_RSA_Cryptography_Algorithm_and_its_Applications_to_Security_System_by_Using_Linear_Congruence/stats.
[19] M. Al-Hamami, I. Aldariseh, Enhanced Method for RSA Cryptosystem Algorithm, in: Proceedings of the International Conference on Advanced Computer Science Applications and Technologies, Kuala Lumpur, 2012, pp. 402–408. doi:10.1109/ACSAT.2012.102.
[20] F. K. Mammadov, New approach to book cipher: web pages as a cryptographic key, Advanced Information Systems 7(1) (2023) 59–65. doi:10.20998/2522-9052.2023.1.10.
[21] S. Yulian, J. Wuyuan, L. Peng, Z. Pengfei, Study on the Scheme for RSA Iterative Encryption System, Computer and Information Science 1 (2024) 120–120. doi:10.5539/cis.v1n3p120.
[22] E. Barker, R. Allen, Transitioning the use of cryptographic algorithms and key lengths. No. NIST Special Publication (SP) 800-131A Rev. 2 (Draft). National Institute of Standards and Technology (NIST), 2018.
[23] H. Vorobets, O. Vorobets, O. Luchyk, and V. Rusyn, Information Technology and Software for Simulation, Synthesis and Research of Data Crypto Protection Methods, Security of Infocommunication Systems and Internet of Things 1(2) (2023) 02011. doi:10.31861/sisiot2023.2.02011.
[24] L. Nan, X. Yang, X. Zeng, W. Li, Yi. Du, Z. Dai, A VLIW architecture stream cryptographic processor for information security, China Communications 16 (2019) 185–199. doi:10.23919/JCC.2019.06.015.
[25] V. Krasnobayev, A. Yanko, A. Martynenko, D. Kovalchuk, Method for computing exponentiation modulo the positive and negative integers, in: XI International Scientific and Practical Conference on Information Control Systems &Technologies (ICST-2023), CEUR, Odessa, Ukraine, 2023, pp. 374–383. URL: https://ceur-ws.org/Vol-3513/paper31.pdf .
[26] J. Zhang, S. Chen, J. Liu, J. He, Composing Parameter-Efficient Modules with Arithmetic Operations, in: 37th Conference on Neural Information Processing Systems (NeurIPS 2023), 2023, pp. 1–22. doi:10.48550/arXiv.2306.14870.
[27] S. Vollala, V. V. Varadhan, K. Geetha and N. Ramasubramanian, Efficient modular multiplication algorithms for public key cryptography, in: 2014 IEEE International Advance Computing Conference (IACC), IEEE, Gurgaon, India, 2014, pp. 74–78, doi:10.1109/IAdCC.2014.6779297.
[28] R. Kochan, S. Yevseiev, R. Korolov, S. Milevskyi, I. Ireifidzh, T. Gancarczyk, R. Szklarczyk, Development of Methods for Improving Crypto Transformations in the Block-Symmetric Code, in: 2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS), IEEE, Dortmund, Germany, 2020, pp. 1–9. doi:10.1109/IDAACS-SWS50031.2020.9297102.
[29] S. Onyshchenko, A. Yanko, A. Hlushko, Improving the efficiency of diagnosing errors in computer devices for processing economic data functioning in the class of residuals, Eastern-European Journal of Enterprise Technologies 5(4(125)) (2023) 63–73. doi:10.15587/1729-4061.2023.289185.

[30] X. Wang, T. Chen, D. Li, Sh. Yu, Processing Methods for Digital Image Data Based on the Geographic Information System, Complexity, 16 (2021) 1–12. doi:10.1155/2021/2319314.
[31] G. Moona, A. Singh, S. Bishnoi, V. Kumar, R. Sharma, H. Kumar, A comparative investigation for flatness and parallelism measurement uncertainty evaluation using laser interferometry and image processing, Indian Journal of Engineering and Materials Sciences 31(1) (2024) 51–57. doi:10.56042/ijems.v31i1.4887.
[32] D. Hofheinz, K. Hövelmanns, E. Kiltz, A Modular Analysis of the Fujisaki-Okamoto Transformation, in: Kalai, Y., Reyzin, L. (eds), Proceedings of the Theory of Cryptography, TCC 2017, volume 10677 of Lecture Notes in Computer Science, Springer, Cham, 2017, pp. 341–371. doi:10.1007/978-3-319-70500-2_12.
[33] D. C. Nguyen, Y. Pershin, Fully parallel implementation of digital memcomputing on FPGA, in: 2024 IEEE 67th International Midwest Symposium on Circuits and Systems (MWSCAS), Springfield, MA, USA, 2024, pp. 263-266. doi:10.1109/MWSCAS60917.2024.10658882.
[34] V. Krasnobayev, A. Kuznetsov, A. Yanko, B. Akhmetov, T. Kuznetsova, Processing of the Residuals of Numbers in Real and Complex Numerical Domains, in: T. Radivilova, D. Ageyev, N. Kryvinska (eds), Data-Centric Business and Applications, volume 48 of Lecture Notes on Data Engineering and Communications Technologies, Springer, Cham, 2021, pp. 529–555. doi:10.1007/978-3-030-43070-2_24.
[35] N. Liu, H. Wang, The Characterizations of WG Matrix and Its Generalized Cayley–Hamilton Theorem, Journal of Mathematics (2) (2021) 1–10. doi:10.1155/2021/4952943.
[36] I. Kovács, Y. Kwon, Regular Cayley maps for dihedral groups, Journal of Combinatorial Theory, Series B 148 (2021) 84–124. doi:10.1016/j.jctb.2020.12.002.
[37] S. Brown, Distance between consecutive elements of the multiplicative group of integers modulo n, Notes on Number Theory and Discrete Mathematics 30(1) (2024) 81–99. doi:10.7546/nntdm.2024.30.1.81-99.
[38] J. Kress, K. Schöbel, A. Vollmer, An Algebraic Geometric Foundation for a Classification of Second-Order Superintegrable Systems in Arbitrary Dimension, The Journal of Geometric Analysis 33(11) (2023). doi:10.1007/s12220-023-01413-8.
[39] P. Singh, P. Pranav, S. Anwar, S. Dutta, Leveraging generative adversarial networks for enhanced cryptographic key generation, Concurrency and Computation Practice and Experience 36(22) (2024). doi:10.1002/cpe.8226.
[40] S. Antão, L. Sousa, An RNS-based architecture targeting hardware accelerators for modular arithmetic, in: 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, IEEE, Vancouver, BC, Canada, 2013, pp. 2572–2576. doi:10.1109/ICASSP.2013.6638120.
[41] V. Krasnobayev, A. Kuznetsov, A. Yanko, T. Kuznetsova, The data errors control in the modular number system based on the nullification procedure, in: 3rd International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), CEUR, Zaporizhzhia, Ukraine, 2020, pp. 580–593. doi:10.32782/cmis/2608-45.
[42] A.A. Adigun, M.O. Abolarinwa, O.E. Ojo, A.I. Oladimeji, O.S. Bakare, Enhanced Local Binary Pattern Algorithm for Facial Recognition Using Chinese Remainder Theorem, Dutse Journal of Pure and Applied Sciences 10(1c) (2024) 255–262. doi:10.4314/dujopas.v10i1c.24.
[43] W. Jackiewicz, K. Jackiewicz, Algorithmic Sequencing of Remainders for Hyperbolic Functions in Discrete Space, (2024) 1–16. doi:10.13140/RG.2.2.15943.92328.
[44] R. Liu, Z. Li, X. Zhang, W. Li, L. Shen, R. Tang, Z. Luo, X. Chen, Y. Han, M. Tang, Crypto-DSEDA: A Domain-Specific EDA Flow for CiM-Based Cryptographic Accelerators, IEEE Design & Test 4(5) (2024) 46–54. doi:10.1109/MDAT.2024.3395987.
[45] V. Krasnobayev, A. Yanko, S. Koshman, Conception of realization of criptographic RSA transformations with using of the residue number system, Computer Science and Cybersecurity 2 (2016) 5–12. URL: https://periodicals.karazin.ua/cscs/article/download/6207/5745/.