INFORMATION CONTROL SYSTEMS AND INTELLIGENT TECHNOLOGIES. ADVANCES AND APPLICATIONS

Section 1. Information control systems

UDC 004.056.5:519.725
DOI https://doi.org/10.36059/978-966-397-538-2-1

IMPLEMENTATION OF CRYPTOGRAPHIC TRANSFORMATIONS BASED ON THE RESIDUE NUMBER SYSTEM TO ENHANCE DIGITAL SECURITY

Ph.D. A. Yanko[0000-0003-2876-9316]**, Dr.Sci. V. Krasnobayev**[0000-0001-5192-9918]**,**
Ph.D. A. Hlushko[0000-0002-4086-1513]**, M. Myziura**[0009-0009-9301-2054]
National University «Yuri Kondratyuk Poltava Polytechnic», Ukraine
EMAIL:al9_yanko@ukr.net

Abstract. *The paper addresses the critical 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.*

Problem Statement. In today's world of rapid digitalization of society and globalization of economic processes, digital security is a fundamental prerequisite for the stable functioning of all sectors – from public administration and finance to industrial production and critical infrastructure. The constant growth in the volume of data processed and the introduction of Internet of Things (IoT), artificial intelligence (AI), and cloud computing technologies create not only new opportunities for the development of business and socio-economic systems, but also new vectors of vulnerability [1]. In these conditions, the risks of unauthorized access, distortion, or destruction of information become a critical factor that can lead to large-scale economic losses, disruption of business processes, and loss of trust from consumers and partners.

Ensuring digital security goes far beyond technical issues and has become a complex interdisciplinary task that combines scientific research in the fields of cryptography, mathematical modeling, cybernetics, and risk management [2]. At the same time, in practical terms, it involves the development and implementation of innovative solutions capable of countering increasingly complex cyber threats, in particular by adapting modern cryptographic transformations and optimizing computing processes.

In this context, research aimed at improving the effectiveness of information protection systems by using residual number systems (RNS) as a tool for increasing the resistance of cryptographic algorithms to attacks and reducing computational costs is of particular importance [3]. Such research responds both to significant scientific challenges – the search for new mathematical models and encryption methods – and to the practical tasks of digital transformation of the economy, the formation of a secure cyberspace, and the reduction of threats to strategically important objects.

Analysis of Previous Studies. The digital transformation, which now encompasses virtually all sectors of the economy and society, is bringing about a fundamental change in approaches to data processing, storage, and transmission. The introduction of intelligent information systems, cloud services, IoT, AI, and blockchain technologies opens up new opportunities for improving the efficiency of business processes, optimizing management decisions, and increasing the competitiveness of organizations [4]. However, along with these advantages, the range of cyber threats is also growing, putting the issue of ensuring reliable protection of digital assets on the agenda.

The issue of digital security, particularly through cryptographic mechanisms, is key to ensuring trust in transformed digital processes. Research shows that the degree of integration of information security into business processes directly affects the stability and performance of organizations. One example is the analysis of the impact of digital transformation on business security and recommendations for strengthening its cyber resilience [5].

In scientific discourse, digital security is being rethought as a growing component of digital transformation that requires comprehensive solutions – from technological to managerial [6]. In addition, the growth of computing capabilities, especially with the approach of the era of quantum computing, is forcing a rethinking of traditional cryptographic approaches. In this context, post-quantum cryptography (PQC) is becoming critically important for protecting data today – to avoid “collect now, decrypt later” attacks – and to minimize the risks of future code breakthroughs [7].

From a scientific point of view, digital security challenges require innovative scientific solutions, such as combining cryptographic transformations with blockchain technologies that ensure data resilience, transparency, and authenticity in decentralized systems [8].

Contemporary public-key cryptosystems widely utilize algebraic curve-based transformations, including elliptic curves (EC), hyperelliptic curves (HEC) [9, 10], Picard curves (PC), and superelliptic curves (SEC) [11], in addition to the traditional RSA scheme. The practical implementation of these systems relies on various scalar multiplication algorithms, such as the Kantor divisor addition method, the Koblitz method, arithmetic transformation techniques for HEC Jacobian divisors, weighted divisor addition methods, the Karatsuba algorithm for modular multiplication, polynomial function field reduction, and approaches based on the Chinese Remainder Theorem. However, many of these methods do not fully meet the high efficiency requirements of modern cryptographic applications. In contrast, recent studies [12, 13] demonstrate that modular arithmetic codes, particularly those based on the Residue Number System (RNS), offer significant advantages in accelerating digital information processing, including tasks such as digital filtering, Fast Fourier Transform (FFT), and Discrete Fourier Transform (DFT) computations.

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 [14, 15, 16].

The primary goal of the studies documented in [17, 18] 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 [19] 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 [20] 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) [21]; 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 [22] presents a key benefit.

Unresolved Issues. 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. 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. Consequently, there is a pressing need for the development of techniques that enhance the efficiency, reliability, and security of cryptographic transformations.

Objective of the Article. The objective of this article is to investigate methods for enhancing the performance and security of public-key cryptographic systems. The work focuses on the RSA cryptosystem, which remains a fundamental mechanism for data protection. A primary goal is to address the issue of computational latency that arises from the need for increasingly long key lengths, which in turn diminishes the processing speed of cryptographic transformations.

To achieve this, the article aims to develop and substantiate a novel approach based on the RNS. The proposed method involves the implementation of a cyclic shift mechanism utilizing modular arithmetic, entirely within the RNS framework. This approach is designed to accelerate core cryptographic operations, such as modular multiplication and exponentiation, which are the most computationally intensive components of the RSA algorithm.

Ultimately, the research seeks to demonstrate that the application of RNS can provide a more efficient and reliable solution for high-speed crypto accelerators. The findings are intended to offer a practical and academically sound contribution to the field of information security, paving the way for the development of more robust and responsive digital security infrastructure.

Main Content. 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 [23]. 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 [24]. This independence facilitates the development of novel machine arithmetic and fundamentally new HSCA architectures, thereby expanding the applicability of machine arithmetic. Numerous studies [25, 26, 27] 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.

The primary bottleneck in high-speed digital systems, including crypto accelerators, is the "carry propagation problem" inherent in positional number systems. In PNS, the calculation of each digit in an arithmetic operation, such as addition or multiplication, depends on the carry from the preceding position. This sequential dependency creates a critical path that directly limits the maximum operating frequency and overall processing speed. This issue is particularly pronounced when dealing with the large bit-length numbers required for modern, secure cryptographic algorithms like RSA. As key sizes increase, the carry propagation delay scales almost linearly, creating a fundamental barrier to achieving real-time performance in resource-constrained environments. This fundamental limitation of PNS makes alternative number systems, such as the RNS, highly attractive for high-performance applications where parallel processing can be leveraged.

To further illustrate the effectiveness of the proposed approach, let's consider a simple example of adding two large numbers in a traditional binary system (PNS) versus in the Residue Number System (RNS). Suppose we need to compute the sum of two 64-bit numbers, for example, *Y* and *U*.

1. The Traditional Approach (PNS): In the binary system, addition is performed sequentially, bit by bit. Each subsequent bit's value depends on the carry from the previous position. For a 64-bit number, the result in the 64th bit cannot be computed until all intermediate carries from the 1st to the 63rd bit are known. This dependency on carry propagation is the primary factor limiting the computation speed. The addition time is the sum of the time required to process each bit, which can be notionally represented as $T_{PNS} = 64 \times T_{gate}$, where T_{gate} – is the switching time of a single logic gate.

2. The Proposed Approach (RNS): In contrast, let's use the RNS with a set of relatively prime moduli. For a 64-bit number, this could be a set of 8-bit moduli. Adding the numbers Y and U in RNS is performed in parallel for each modulus, with no carry propagation between them. The calculations are performed as follows $\left((y_1+u_1)(\mathrm{mod}\, m_1),(y_2+u_2)(\mathrm{mod}\, m_2),...,(y_n+u_n)(\mathrm{mod}\, m_n)\right).$ Each of these calculations is executed independently in a separate arithmetic processing unit (APU). The proposed ring shift mechanism (RSM) allows each remainder to be computed in a time that depends only on the size of its respective modulus, not on the total length of the number.

This example demonstrates that while PNS speed is limited by the number's length, RNS calculations occur in parallel. This parallelism eliminates the delay caused by carry propagation, achieving a significant speedup that is critical for high-performance cryptographic applications.

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 [28].

Research presented in [29] 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 [30].

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 $GF(p_n)$ [32].

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: $+,-,\times$) [33]. 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 [34]. 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 [35].

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 [36].

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 [37], 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 [38], 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 [39]. 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.

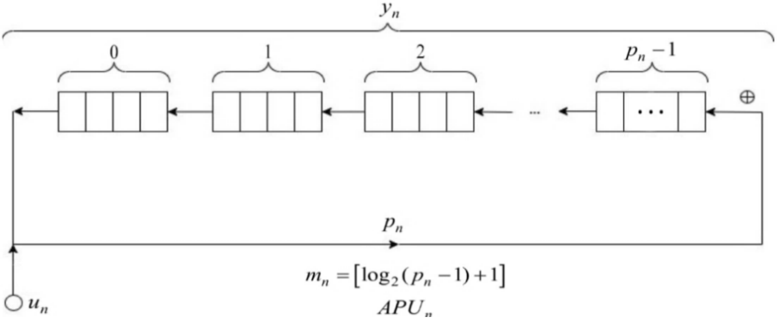


Figure 1. Primary digital structure of the CSA for modulus p_n in RNS

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):

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

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

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.

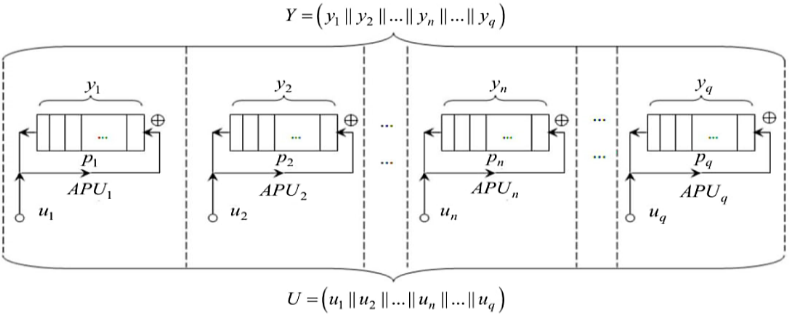

$Y=\left(y_1 \| y_2 \| \ldots \| y_n \| \ldots \| y_q\right)$
y_1
p_1
APU_1
u_1
y_2
p_2
APU_2
u_2
y_n
p_n
APU_n
u_n
y_q
p_q
APU_q
u_q
$U=\left(u_1 \| u_2 \| \ldots \| u_n \| \ldots \| u_q\right)$

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 $Y=\left(y_1 \| y_2 \| \ldots \| y_n \| \ldots \| y_q\right)$ and $U=\left(u_1 \| u_2 \| \ldots \| u_n \| \ldots \| u_q\right)$, 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 $(y_n+u_n) \bmod p_n \quad (n=\overline{1,\ q})$, 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 [40], 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:

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

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 [24, 40], 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.

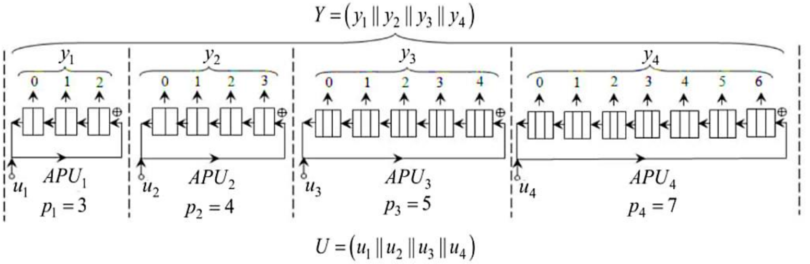


Figure 3. Simplified HSCA OU scheme of low-bit representation of numbers in RNS [40]

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 $D = \prod_{n=1}^{q} p_n = 11 \cdot 13 \cdot 15 \cdot 19 = 40755$ 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: $V_1 = 7$, $m_1 = [\log_2(p_1 - 1) + 1] = [\log_2(11 - 1) + 1] = 4$ and $V_1 \cdot m_1 = 7 \cdot 4 = 28.$

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

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

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

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:

$$\theta_{RNS} = V_1 \cdot [\log_2(p_1 - 1) + 1] \cdot 3 \cdot t' = 7 \cdot 4 \cdot 3 \cdot t' = 84 \cdot t'.$$

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: $V_1 = 1$, $m_1 = [\log_2(p_1 - 1) + 1] = [\log_2(11 - 1) + 1] = 4$ and $V_1 \cdot m_1 = 1 \cdot 4 = 4.$

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

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

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

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

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:

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

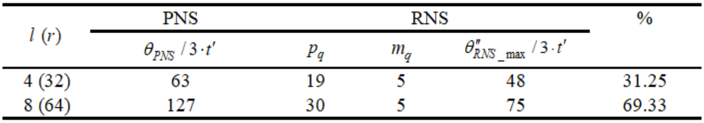
The ratio of addition operation execution times in PNS and RNS will be represented by a coefficient, namely:

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

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.

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

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.

Conclusions and Prospects. Digital transformation necessitates a rethinking of existing approaches to digital security. To strengthen the ability of entities to counter dynamic and growing risks in the field of cyber security, existing tools and technologies need to be improved. Of particular importance in this context is the modernization of the RSA cryptosystem as one of the basic mechanisms for data protection, which ensures resistance to modern cyber threats and increases the level of trust in digital services.

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. The core advantage of this approach lies in its inherent parallelism, which fundamentally bypasses the carry propagation bottleneck that limits the speed of traditional positional number systems. This enables modular operations to be executed in constant time, regardless of the operand's bit length, a critical achievement for modern, high-bit-length cryptographic keys.

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.

The research findings offer significant potential for application in resource-constrained systems, such as embedded devices, Internet of Things (IoT), and industrial control systems, where high performance must be achieved with limited computational power. 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. Moreover, the core principles of RNS-based modular arithmetic and the cyclic shift mechanism are inherently adaptable to other public-key cryptographic algorithms that heavily rely on modular exponentiation and multiplication, such as ElGamal and Diffie-Hellman. Further research will also investigate the method's applicability to post-quantum cryptography (PQC), which demands exceptional computational efficiency for its large-integer-based algorithms.

References

1. Onyshchenko, S., Yanko, A., Hlushko, A., & Sivitska, S. (2020). Conceptual principles of providing the information security of the national economy of Ukraine in the conditions of digitalization. *International Journal of Management, 11*(12), 1709–1726. https://doi.org/10.34218/IJM.11.12.2020.157

2. Kharchenko, V., et al. (2022). Combining Markov and semi-Markov modelling for assessing availability and cybersecurity of cloud and IoT systems. *Cryptography, 6*(3), 44. https://doi.org/10.3390/cryptography6030044

3. Hlushko, A. D., & Yanko, A. S. (2019). Optimal reservation of data in the system of residual classes in the direction of ensuring information security of the

national economy. *Economics and Region, (4)75,* 35–44. https://doi.org/10.26906/EiR.2019.4(75).1814

4. Hlushko, A., Yanko, A., & Bilko, S. (2025). Digital transformation of business processes: Security aspect. *Digital Economy and Economic Security, 2*(17). https://doi.org/10.32782/dees.17-26

5. Saeed, S., et al. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors, 23*(15), 6666. https://doi.org/10.3390/s23156666

6. Shahim, A. (2021). Security of the digital transformation. *Computers & Security*, *108*, 102345. https://doi.org/10.1016/j.cose.2021.102345

7. Monroe, D. (2023). Post-quantum cryptography. *Communications of the ACM*, *66*(2), 15–17. https://doi.org/10.1145/3575664

8. Kuznetsov, A., et al. (2022). Cryptographic transformations in a decentralized blockchain environment. In *Information Security Technologies in the Decentralized Distributed Networks* (pp. 89–113). Cham. https://doi.org/10.1007/978-3-030-95161-0_4

9. Pasumponpandian, D. (2020). Development of secure cloud-based storage using the Elgamal hyper elliptic curve cryptography with fuzzy logic based integer selection. *Journal of Soft Computing Paradigm, 2*(1), 24–35. https://doi.org/10.36548/jscp.2020.1.003

10. Ullah, S., & Din, N. (2021). Blind signcryption scheme based on hyper elliptic curves cryptosystem. *Peer-to-Peer Networking and Applications, 14*(2), 917–932. https://doi.org/10.1007/s12083-020-01044-8

11. Berini, A. D. e., et al. (2023). HCALA: Hyperelliptic curve-based anonymous lightweight authentication scheme for Internet of Drones. *Pervasive and Mobile Computing, 101798.* https://doi.org/10.1016/j.pmcj.2023.101798

12. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O., & Cherviak, A. (2023). Cybersecurity and improvement of the information security system. *Journal of the Balkan Tribological Association, 29*(5), 818–835. https://scibulcom.net/en/article/L8nV7It2dVTBPX09mzWB

13. Albusifi, S., Mugassab, S., & Elferjani, A. (2021). RSA cryptography algorithm and its applications to security system by using linear congruence. *International Journal of Multidisciplinary Sciences and Advanced Technology, Special 1,* 558–564. https://www.researchgate.net/publication/380320192_RSA_Cryptography_Algorithm_and_its_Applications_to_Security_System_by_Using_Linear_Congruence/stats

14. Al-Hamami, A. H., & Aldariseh, I. A. (2012, November 26–28). Enhanced method for RSA cryptosystem algorithm. *2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT).* Kuala Lumpur, Malaysia. https://doi.org/10.1109/acsat.2012.102

15. Mammadov, F. K. (2023). New approach to book cipher: Web pages as a cryptographic key. *Advanced Information Systems, 7*(1), 59–65. https://doi.org/10.20998/2522-9052.2023.1.10

16. Shang, Y., et al. (2008). Study on the scheme for RSA iterative encryption system. *Computer and Information Science, 1*(3). https://doi.org/ 10.5539/ cis.v1n3p120

17. Barker, E., & Roginsky, A. (2019). Transitioning the use of cryptographic algorithms and key lengths. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/nist.sp.800-131ar2

18. Vorobets, H., Vorobets, O., Luchyk, O., & Rusyn, V. (2023). Information technology and software for simulation, synthesis and research of data crypto protection methods. *Security of Infocommunication Systems and Internet of Things, 1*(2), 02011. https://doi.org/10.31861/sisiot2023.2.02011

19. Nan, L., et al. (2019). A VLIW architecture stream cryptographic processor for information security. *China Communications, 16*(6), 185–199. https://doi.org/10.23919/jcc.2019.06.015

20. Krasnobayev, V., Yanko, A., Martynenko, A., & Kovalchuk, D. (2023). Method for computing exponentiation modulo the positive and negative integers. In *XI International Scientific and Practical Conference on Information Control Systems & Technologies (ICST-2023)* (pp. 374–383). Odessa, Ukraine: CEUR. https://ceur-ws.org/Vol-3513/paper31.pdf

21. Zhang, J., Liu, J., & He, J. (2023). Composing parameter-efficient modules with arithmetic operation. *Advances in Neural Information Processing Systems, 36,* 12589–12610. https://doi.org/10.48550/arXiv.2306.14870

22. Vollala, S., et al. (2014, February 21–22). Efficient modular multiplication algorithms for public key cryptography. *2014 IEEE International Advance Computing Conference (IACC).* Gurgaon, India. https://doi.org/ 10.1109/ iadcc.2014.6779297

23. Kochan, R., et al. (2020, September 17–18). Development of methods for improving crypto transformations in the block-symmetric code. *2020 IEEE 5th International Symposium on Smart and Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS).* Dortmund. https://doi.org/10.1109/idaacs-sws50031.2020.9297102

24. Onyshchenko, S., Yanko, A., & Hlushko, A. (2023). 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)), 63–73. https://doi.org/10.15587/1729-4061.2023.289185

25. Wang, X., et al. (2021). Processing methods for digital image data based on the geographic information system. *Co* [26] 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). https://doi.org/10.56042/ijems.v31i1.4887

27. Hofheinz, D., Hövelmanns, K., & Kiltz, E. (2017). A modular analysis of the Fujisaki-Okamoto transformation. In Y. Kalai & L. Reyzin (Eds.), *Proceedings of the Theory of Cryptography, TCC 2017* (Lecture Notes in Computer Science, Vol. 10677, pp. 341–371). Cham: Springer. https://doi.org/10.1007/978-3-319-70500-2_12

28. Nguyen, D. C., & Pershin, Y. (2024). Fully parallel implementation of digital memcomputing on FPGA. In *2024 IEEE 67th International Midwest Symposium on Circuits and Systems (MWSCAS)* (pp. 263–266). Springfield, MA, USA: IEEE. https://doi.org/10.1109/MWSCAS60917.2024.10658882

29. Krasnobayev, V., Kuznetsov, A., Yanko, A., Akhmetov, B., & Kuznetsova, T. (2021). 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* (Lecture Notes on Data Engineering and Communications Technologies, Vol. 48, pp. 529–555). Cham: Springer. https://doi.org/10.1007/978-3-030-43070-2_24

30. Liu, N., & Wang, H. (2021). The characterizations of WG matrix and its generalized Cayley–Hamilton theorem. *Journal of Mathematics*, 2, 1–10. https://doi.org/10.1155/2021/4952943

31. Kovács, I., & Kwon, Y. (2021). Regular Cayley maps for dihedral groups. *Journal of Combinatorial Theory, Series B*, 148, 84–124. https://doi.org/10.1016/j.jctb.2020.12.002

32. Brown, S. (2024). Distance between consecutive elements of the multiplicative group of integers modulo n. *Notes on Number Theory and Discrete Mathematics*, 30(1), 81–99. https://doi.org/10.7546/nntdm.2024.30.1.81-99

33. Kress, J., Schöbel, K., & Vollmer, A. (2023). An algebraic geometric foundation for a classification of second-order superintegrable systems in arbitrary dimension. *The Journal of Geometric Analysis*, 33(11). https://doi.org/10.1007/s12220-023-01413-8

34. Singh, P., Pranav, P., Anwar, S., & Dutta, S. (2024). Leveraging generative adversarial networks for enhanced cryptographic key generation. *Concurrency and Computation: Practice and Experience*, 36(22). https://doi.org/10.1002/cpe.8226

35. Antão, S., & Sousa, L. (2013). An RNS-based architecture targeting hardware accelerators for modular arithmetic. In *2013 IEEE International Conference on Acoustics, Speech and Signal Processing* (pp. 2572–2576). Vancouver, BC, Canada: IEEE. https://doi.org/10.1109/ICASSP.2013.6638120

36. Krasnobayev, V., Kuznetsov, A., Yanko, A., & Kuznetsova, T. (2020). 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)* (pp. 580–593). Zaporizhzhia, Ukraine: CEUR. https://doi.org/10.32782/cmis/2608-45

37. Adigun, A. A., Abolarinwa, M. O., Ojo, O. E., Oladimeji, A. I., & Bakare, O. S. (2024). Enhanced local binary pattern algorithm for facial recognition using Chinese remainder theorem. *Dutse Journal of Pure and Applied Sciences*, 10(1c), 255–262. https://doi.org/10.4314/dujopas.v10i1c.24

38. Jackiewicz, W., & Jackiewicz, K. (2024). Algorithmic sequencing of remainders for hyperbolic functions in discrete space (pp. 1–16). https://doi.org/10.13140/RG.2.2.15943.92328

39. Liu, R., Li, Z., Zhang, X., Li, W., Shen, L., Tang, R., Luo, Z., Chen, X., Han, Y., & Tang, M. (2024). Crypto-DSEDA: A domain-specific EDA flow for

CiM-based cryptographic accelerators. *IEEE Design & Test*, 4(5), 46–54. https://doi.org/10.1109/MDAT.2024.3395987

40. Krasnobayev, V., Yanko, A., & Koshman, S. (2016). Conception of realization of cryptographic RSA transformations with using of the residue number system. *Computer Science and Cybersecurity*, 2, 5–12. Retrieved from https://periodicals.karazin.ua/cscs/article/download/6207/5745/*mplexity, 2021,* 1–12. https://doi.org/10.1155/2021/2319314

ВПРОВАДЖЕННЯ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ НА ОСНОВІ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ ДЛЯ ПІДВИЩЕННЯ ЦИФРОВОЇ БЕЗПЕКИ

Ph.D. А. Янко[0000-0003-2876-9316], **Dr.Sci. В. Краснобаєв**[0000-0001-5192-9918], **Ph.D. А. Глушко**[0000-0002-4086-1513], **М. Мизюра** [0009-0009-9301-2054]
Національний університет «Полтавська політехніка імені Юрія Кондратюка», Україна
EMAIL: al9_yanko@ukr.net

Анотація. *У роботі розглядаються критичні питання посилення безпеки бізнесу в умовах цифрової трансформації. Автори демонструють, що розширення процесів цифровізації вимагає перегляду концепції економічної безпеки. Обґрунтовано, що для зміцнення стійкості бізнесу до ризиків та загроз цифровій безпеці необхідно впроваджувати низку заходів, спрямованих на захист конфіденційності, цілісності та доступності інформації. Було проведено дослідження кіберзагроз для суб'єктів національної економіки та громадян, у тому числі з використанням інструментів штучного інтелекту. Це дало змогу визначити пріоритетну сферу захисту даних – удосконалення RSA-криптосистеми. У дослідженні деталізовано розробку ефективних стратегій обробки інформації для зменшення затримки криптографічних функцій RSA. Для прискорення криптографічних перетворень RSA в цьому дослідженні запропоновано методи високошвидкісної обробки інформації. Основа запропонованого методу включає реалізацію механізму циклічного (кільцевого) зсуву з використанням модулярної арифметики, повністю реалізованого системою залишкових класів (СЗК). Застосування СЗК демонструє її ефективність у структуруванні процесу реалізації модулярних цілочислових арифметичних операцій для прискорення криптографічних перетворень з відкритим ключем.*

Ключові слова: *техніка представлення двійкового залишку, криптографічний захист інформації, алгоритм криптографії, масиви циклічного зсуву, цифрова трансформація, високошвидкісні криптографічні прискорювачі, модулярні арифметичні коди, система залишкових класів, механізм кільцевого зсуву.*