JQCM
Journal Of Al-Qadisiyah For Computer Science And Mathematics
University Of AL-Qadisiyah

Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

Multiple approaches to Convert RNS to Decimal Numbers

Nibras Hadi Jawad[a]*, ***Salah Abdulhadi***[b]

[a] *Department of Computer Science, College of Computer Sci. and Math, University of Kufa, Iraq. Email: nibrash.albustani@student.uokufa.edu.iq*

[b] *Department of Computer Science, College of Computer Sci. and Math, University of Kufa, Iraq. Email: salah.albermany@uokufa.edu.iq*

ARTICLE INFO

Article history:
Received: 28 /07/2023
Rrevised form: 21 /09/2023
Accepted : 24 /09/2023
Available online: 30 /09/2023

Keywords:

Residues Number System
Chinese Remainder Theorem
Mixed Radix Conversion Method
Approximation Method
Diagonal Function, Base Extension

ABSTRACT

Improving the performance and speed of encryption algorithms is an important issue in cryptography. One of these improvements is the use of the RNS system. In the research, the RNS system and how to retrieve numbers from the RNS system to WNS weight number system or (decimal number) where discussed in several ways, and after performing multiplication operations, giving illustrative examples and making comparisons between methods.

MSC.

https://doi.org/ 10.29304/jqcm.2023.15.3.1276

1. Introduction

The main goal of conducting development on technologies and algorithms is the speed in executing operations. It is one of the main requirements for the strength and quality of algorithms. As one of the things that speeds up the work of intensive calculations is the representation of numbers using RNS because of its property in simplifying integer numbers into simpler numbers that lead to the speed of calculations. RNS is considered one of the important systems with high effectiveness in improving the implementation of operations especially when used with encryption systems, because of its high speed in conducting operations and obtaining results in less time. This system (RNS) was proposed in [1]. The addition and multiplication operations performed in this system have the same execution time, this is very useful, especially when using algorithms that need to deal with very large numbers, as in asymmetric encryption systems [3],[2]. Homomorphic Encryption is considered one of the encryption systems that RNS has helped in improving its performance and significantly increasing the speed of operations, because RNS has the ability to deal with numbers separately (parallel) [3].

Many researchers have studied the field of RNS and how it works and develops it through putting forward theories, proofs and researches that explain this system. **Kuchukov, V. and et.al. [4] (2022)**, A summary of the techniques used to convert the positional number system from the RNS is provided. Reverse conversion techniques for moduli in general form, including the MRC, the CRT, and the Chinese residue theorem with fractional numbers.

⁎Corresponding author

Email addresses:

Communicated by ‘sub etitor’

the authors' theories derived from reference points and modified mixed-radix conversion. The process of determining the residue of division by a large modulo can be substituted with the sequential computation of the residue in this instance, thanks to the modified approach based on the MRC. By changing the number of moduli of one method and the other, this methodology allows one to strike a balance between the hardware employed and the calculation time. The other research in **[5] (2013), by Karim Bigou, and Arnaud Tisserand**, a new RNS modular inversion technique, based on the plus-minus trick and the extended Euclidean algorithm, is described in the study. the technique replaces expensive computations modulo 4 with comparisons across big RNS values. the researchers made comparisons to an RNS version using Fermat's Little Theorem. achieve a 6–10 times quicker plus-minus RNS modular inversion, with a significant reduction in the amount of elementary modular operations. Where by **Karl C. Posch and Reinhard Posch in [6] (2011)**, present a novel approach that combines RNS with effective modulo reduction techniques. the researchers compare two approaches and thoroughly examine the speedier one. The order of complexity for both approaches is O(log n), where n is the number of registers that are used. They also explain faster ways to multiply and retrieve numbers from RNS. **Umar, A. F. [7] (2011)**, the issue of data conversion in the Residue Number System (RNS) is addressed in this thesis. This system is crucial for embedded CPUs, particularly those in portable devices, where power consumption is the most important design consideration. The goal of this thesis is to create effective methods for converting conventional representations to RNS representations and vice versa. give an overview of some of the conversion techniques and strategies that are currently in use when the signal has a binary form. **Gbolagade, K. A., & Cotofana, S. D. [8] (2008)**, An important issue with using RNS numbers in Digital Signal Processing applications is the conversion of RNS operands to decimal, which the researchers looked into. They introduce an MRC method for effectively converting RNS to decimal, utilizing the moduli set {2n + 2, 2n + 1, 2n}, which shares a factor of 2. Because there is less labor involved in the computations, the multipliers and adders are less complicated.

In this research paper, in the second section, you talk about RNS. Followed by methods for returning numbers to their normal state in the third section. In the fourth section, it explains the procedure of multiplication in RNS and returning the result to a decimal number.

2. Residue Number System (RNS)

Integer $x \in \mathbb{Z}$ to represent in RNS with a set of pairwise coprime integer B={m_1, m_2,....,m_n} and size n [1],[9]. no repeat in all elements of base and must be relatively prime to each other (the GCD between them equal to 1). Represent x with RNS as $\langle x\rangle_{\mathrm{B}}$=$\langle x_1, \dots, x_n\rangle_{\mathrm{B}}$ where x_1=$x \ mod \ m_1$ Likewise for the rest. The condition to represent x must M>x. n = ⌈ l /w ⌉ where l number of bits represent x, and w number of bits for each x mod m_i , and note that x mod m_i = $[\mathrm{x}]_{\mathrm{m_i}}$, The product of all bases let M=$\prod_{i=1}^{n} m_i$, and always M>x. the Fig. 1, illustrate the architecture of RNS.

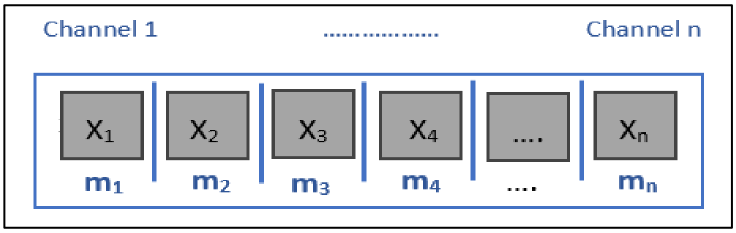

Fig. 1: architecture of RNS

The Fig. 1, explains the integer number divided into multiple small numbers (channels).

Example1: let x=17 to represent it in RNS with bases B={3,5,7}, the GCD between all elements of B equivalent to 1, and M=105 , 0 ≤ x <M. Then the RNS of x:

$$\langle \mathrm{x}\rangle_{\mathrm{B}}=\langle 17 \ mod \ 3, 17 \ mod \ 5, 17 \ mod \ 7\rangle_{\mathrm{B}} \rightarrow \langle 2, 2, 3\rangle_{\mathrm{B}} .$$

If two integers are found and want aplying mathematical operation such as addition or multiplication must represent integers in RNS, before performing operations and compute each channel independent from others. See Fig. 2 .

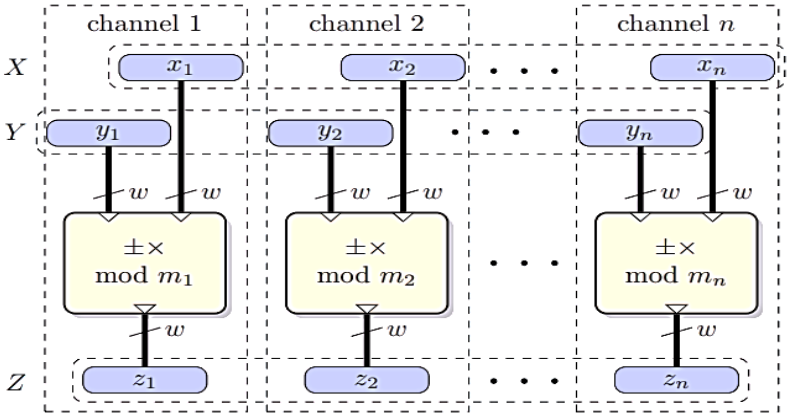

Fig. 2: operations in RNS

Then to compute $\langle x\rangle * \langle y\rangle$ where * is $(\times, +)$.

$$\langle z\rangle = \langle x\rangle * \langle y\rangle = \langle x_1, x_2, \dots, x_n\rangle * \langle y_1, y_2, \dots, y_n\rangle mod\ m_i = \langle (x_1 * y_1)\ mod\ m_1, \dots, (x_n * y_n)\ mod\ m_n \rangle$$

3. Conversion Decimal Number From RNS

To return the integers to their normal state from the RNS, there are several methods proposed by the researchers as follows:

3.1. Chinese Remainder Theorem (CRT)

The main method to convert integer represent in RNS is CRT, [9], [10]. Many researchers based on CRT as the following formula:

$$x = [x]_{\mathrm{M}} = \left[\sum_{i=0}^{n-1}[x_i.\mathrm{M}_i^{-1}]_{m_i} \times \mathrm{M}_i\right]_{\mathrm{M}}$$

As mentioned earlier $0 \le x < \mathrm{M}$, where $\mathrm{M}=\prod_{i=1}^{n} m_i$. Must compute $\mathrm{M}_i = \frac{M}{m_i}$, and M_i^{-1} is multiplicative invers of M_i where $\mathrm{M}_i mod\ m_i$, and $\mathrm{M}_i \times \mathrm{M}_i^{-1} mod\ m_i = 1$,[].

Example2: x=17 , B={3,5,7}, then RNS of x → $\langle x\rangle = \langle 2, 2, 3\rangle_{\mathrm{B}}$

$\mathrm{M}=\prod_{i=1}^{n} m_i \rightarrow$ M=3*5*7=105

$\mathrm{M}_1=\frac{105}{3} = 35$, $\mathrm{M}_1^{-1} = 2$, $\mathrm{M}_2=\frac{105}{5} = 21$, $\mathrm{M}_2^{-1} = 1$, $\mathrm{M}_3=\frac{105}{711} = 15$, $\mathrm{M}_3^{-1} = 1$

$x=[(2*2)_3*35 + (2*1)_5*21 + (3*1)_7*15]_{165}=[110+66+90]_{105}= 17$

3.2. Mixed Radix Conversion Method (MRC)

Based on [11], [12], can use MRC to calculate integer from RNS the with simple operations. Let U_i is conversion coefficient to compute $y_i = (U_i * V_i)_{m_i}$ by increasing series $U_1 = x_1, U_2 = [\, x_2 - x_1]_{m_2}, U3 = [x_3 - x_1 - m_1.U2]_{m_3}$. In the [11],[12] found → $V_1 = 1 , V_2 = \left[\frac{1}{m_1}\right]_{m_2} = 1, V_3 = \left[\frac{1}{m_1 m_2}\right]_{m_3} = 1.$

Example3: B={3,5,7}→{ m1, m2, m3} based on last example , and $\langle x\rangle = \langle 2, 2, 3\rangle_{\mathrm{B}}$, V1 = 1, V2 = 1, and V3 = 1. Must find the coefficients (yi):

$y1$=$(U1 \,.\, V1)_{m1}$ = $[(2.1).1]_3$ =2

$y2$=$(U2 \,.\, V2)_{m2}$ =$[(2\text{-}2).1]_5$ =0

$y3$=$(U3 \,.\, V3)_{m3}$=$[(3\text{-}2\text{-}(3.0)).1]_7$=1

x =y1+y2.m$_1$+y3.m$_1$.m$_2$ =2+(0.3)+(1.3.5)=17

3.3. Approximation Method (AM)

AM is the fast function [13], [14] to calculate integer from RNS by use the flowing:

$$a_i = \left\lceil \frac{[M_i^{-1}]_{m_i}}{m_i} . 2^N \right\rceil \text{ , and N} = \lceil log_2(M.(\textstyle\sum_{i=1}^{n} m_i - n)\,)\rceil \text{ ,} \quad x = \left\lfloor \frac{[\sum_{i=1}^{n} a_i.x_i]_{2^N} .M}{2^N} \right\rfloor$$

Example4: based on last example x=17 , B={3,5,7}, and n=3 (number of element of B) then RNS of x → $\langle x\rangle = \langle 2, 2, 3\rangle_{\mathrm{B}}$,z=$\sum_{i=1}^{n} m_i - n$=(3+5+7)-3=12, M=105, N= ⌈log$_2$ (M*z)⌉= ⌈log$_2$ (105*12)⌉= ⌈10.29920801839⌉=11.

M$_1$=35 , $\mathrm{M}_1^{-1} = 2$, M$_2$=21 , $\mathrm{M}_2^{-1} = 1$, M$_3$=15 , $\mathrm{M}_3^{-1} = 1$.

Then from the coefficient's calculation found the values:

$$a_i = \left\lceil \frac{[M_i^{-1}]_{m_i}.2^N}{m_i} \right\rceil,\ a_1 = \left\lceil \frac{[2]_3.2^{11}}{3} \right\rceil = 1365, a_2 = \left\lceil \frac{[1]_5.2^{11}}{5} \right\rceil = 410,\ a_3 = \left\lceil \frac{[1]_7.2^{11}}{7} \right\rceil = 293$$

$[\sum_{i=1}^{n} a_i.x_i]_{2^N}$ = [1365*2+410*2+293*3]$_{2048}$=[6607]$_{2048}$=333

$$\mathrm{x} = \left\lfloor \frac{[\sum_{i=1}^{n} a_i.x_i]_{2^N} .M}{2^N} \right\rfloor = \left\lfloor \frac{333*105}{2048} \right\rfloor = 17$$

3.4. Diagonal Function (DF)

To calculate integer based on [15], [16] from RNS by using the formula:

$$\mathrm{D(x)}=[\textstyle\sum_{i=1}^{n} d_i.x_i]_{SQ}, d_i = \left(-\frac{1}{m_i}\right)_{SQ},\ \ SQ = M_1 + M_2 + \cdots + M_n = \textstyle\sum_{i=1}^{n} M_i,\ (d_1 + d_2 + \cdots + d_n)_{SQ} = 0\,.$$

The number calculate by: $\mathrm{x} = \frac{M}{SQ}(D(\mathrm{x}) + (\sum_{i=1}^{n} x_i.M_i)) = \frac{(M*D(\mathrm{x}) + (\sum_{i=1}^{n} x_i.M_i))}{SQ}$, and i=1,2,…,n.

Example5: x=17 , B={3,5,7}, and n=3 (number of element of B) then RNS of x → $\langle x\rangle = \langle 2, 2, 3\rangle_{\mathrm{B}}$, M=105, M$_1$=35 , M$_2$=21 , M$_3$=15 .

SQ=35+21+15=71, d$_1$=(-24) mod71=47, d$_2$=(-57)mod71=14, d$_3$=(-61)mod71=10, (47+14+10)$_{71}$=0.

D(x)=(47*2+14*2+10*3)=(152)$_{71}$=10.

x= $\frac{105*10+(2*35+2*21+3*15)}{71}$ = 17.

4. Retrieve the product of the multiplication from the RNS

To multiply two decimal numbers, each number must be represented by an RNS, and then the numbers are multiplied in a simple way, as in the following example:

Example6: let x=12, and y=23, B= {5,7,11} (The base must be chosen so that M is higher than the product of the multiplication in order to retrieve the result correctly) where M=385 , M1=77 , M2=55 , M3=35 , M_1^(-1)=3 , M_2^(-1)=6 , M_3^(-1)=6.

$\langle \boldsymbol{x} \rangle = \langle \mathbf{2, 5, 1} \rangle_{\mathbf{B}}$, $\langle \boldsymbol{y} \rangle = \langle \mathbf{3, 2, 1} \rangle_{\mathbf{B}}$

$\langle \boldsymbol{x} \rangle * \langle \boldsymbol{y} \rangle = \langle (\mathbf{2} * \mathbf{3}) \boldsymbol{mod}\ \mathbf{5}, (\mathbf{5} * \mathbf{2}) \boldsymbol{mod} \mathbf{7}, (\mathbf{1} * \mathbf{1}) \boldsymbol{mod} \mathbf{11} \rangle = \langle \mathbf{1, 3, 1} \rangle_{\boldsymbol{B}}$

To retrieve the decimal number after multiplication from the RNS, it is summarized as in the following Table 1:

Table 1 - retrieve the decimal number after multiplication from the RNS.

parameters	**CRT**	**MRC**	**AM**	**DF**

B={5,7,11}
$\langle x \rangle = \langle 2,5,1 \rangle_B$
$\langle y \rangle = \langle 3,2,1 \rangle_B$
$\langle x \rangle * \langle y \rangle = \langle 1,3,1 \rangle_B$
M=385
	M1=77, M2=55, M3=35 , M_1^(-1)=3 , M_2^(-1)=6 , M_3^(-1)=6
	X=(1*3*77+3*6*55+1*6*35) mod 385=276
		y1=1, y2=2, y3=1,
		X=1+2*5+1*5*7+ 5*2*23 =276
			Z=20,N=13,a1=4916, a2=7022, a3=4469, Σ=5875, X=(5875*385)/213 =276	5. SQ=167, d_1=100, d_2=143,
				6. d_3=91 , D(x)=119 ,
				X=(385*119+ (1*77+3*55+1*35)) /167=276

Time complexity	O(n^2) ,[9],[11]	O(n^2) ,[11]	O((n+1)*$\log_2$(n+1)) ,[13], [14]	O(((n-1)+$\log_2$n$)^2$) ,[15]
Advantage	Reliability, and Easy [9], [10]	Elimination of division [11], [12]	Allow to select approximate coefficient. Reliability [13].	Drive a number's positional characteristic in RNS. Reliability [15],[16].
disadvantage	The calculation time increases as the number gets larger. require to more division [9], [10]	Non-Reliability have many cases in solution [11], [12].	Dealing with large numbers of coefficient [13], [14].	require to more division [15],[16].

To compute large number must be use large M, then more time that' not good. If the complex operation or large number are found, can use more than one base. By using base extension (BE) to convert from one base to another base as the following algorithm1 [17], [18], [19].

algorithm1 : Base Extension in [19]

The Input: $\langle x \rangle_a$, B_a, B_b, σ_0 (fixed as a global parameter)

Precompute.: $\langle M_a^{-1} \rangle_a$, $\langle M_a \rangle_b$, $\langle -M_a \rangle_b$

The Output: $\langle x \rangle_b$

```
$\langle \xi \rangle_a = \langle x \rangle_a * \langle M_a^{-1} \rangle_a$, $\langle x \rangle_b = 0$ , $\sigma = \sigma_0$
for i = 1, . . . , $n_a$ do
```

```
    $σ = σ + trunc(ξ_{a,i})$
    $q = ⌊σ⌋$                (where : q is 0 or 1 )
    $σ = σ − q$
    for j = 1, . . . , $n_b$ do
        $x_{b,j} = [x_{b,j} + ξ_{a,i} * T_{a,i} + q * (−M_a)]_{m_{b,j}}$
return $\langle x\rangle_b$
```

Where the BE formula based on CRT formula as the following:

$$\boldsymbol{x} = \sum_{i=1}^{n_a} \left(\left[x_{a,i} . \mathrm{M}_{a,i}^{-1} \right]_{m_{a,i}} \times \mathrm{M}_{a,i} \right) - q\,\mathrm{M}_a \,, \qquad where\ \boldsymbol{q} = \left\lfloor \sum_{i=1}^{n_a} \frac{\left[x_{a,i} . \mathrm{M}_{a,i}^{-1} \right]_{m_{a,i}}}{m_{a,i}} \right\rfloor = \left\lfloor \sum_{i=1}^{n_a} \frac{\xi_{\ a,i}}{m_{a,i}} \right\rfloor$$

And the (trunc) that function to approximates the devision $\left\lfloor \sum_{i=1}^{n_a} \frac{\xi_{\ a,i}}{m_{a,i}} \right\rfloor$.

Example7:

The Input: $\langle x\rangle_a = \langle 1,3,6\rangle_a$, B_a={2,7,13} , B_b={3,5,1}, $σ_0$=0 , n_a=3, n_b=3

Precompute: $\langle M_a^{-1}\rangle_a = \langle 1,3,1\rangle_a$, $\langle M_a\rangle_b = \langle 2,2,6\rangle_b$, $\langle -M_a\rangle_b = \langle 1,3,5\rangle_a$

want $\langle x\rangle_b$ $(convert\ \langle x\rangle_a \rightarrow \langle x\rangle_b)$

$\langle ξ\rangle_a = \left[x_{a,i} . \mathrm{M}_{a,i}^{-1} \right]_{m_{a,i}}$, $\langle x\rangle_b = \langle 0,0,0\rangle_b$, σ =0

for i = 1, . . . , n_a do

when i=1

$σ = 0 + \frac{ξ_{\ a,i}}{m_{a,i}} = 0 + \frac{(1*1)\ _2}{2} = \frac{1}{2}$, $q = \left\lfloor \frac{1}{2} \right\rfloor = 0$, $σ = σ - q = \frac{1}{2} - 0 = \frac{1}{2}$

for j = 1, . . . , 3 do

j=1 $x_{b1}=[0+1*91+0]_3 = [91]_3 = 1$

j=2 $x_{b2}= [91]_5 = 1$

j=3 $x_{b1}= [91]_{11} = 3$

$\langle x\rangle_b = \langle 1,1,3\rangle_b$

when i=2

$σ = \frac{1}{2} + \frac{(3*3)\ _7}{7} = \frac{11}{14}$, $q = \left\lfloor \frac{11}{14} \right\rfloor = 0$, $σ = \frac{11}{14} - 0 = \frac{11}{14}$

for j = 1, . . . ,3 do

j=1 $x_{b1}=[1+2*26+0]_3 = [53]_3 = 2$

j=2 $x_{b2}=[1+2*26+0]_5 = [53]_5 = 3$

j=3 $x_{b3}=[3+2*26+0]_{11} = [55]_{11} = 0$

$\langle x\rangle_b = \langle 2,3,0\rangle_b$

when i=3

$\sigma = \frac{11}{14} + \frac{6}{13} = \frac{227}{182}$, $q = \left\lfloor \frac{227}{182} \right\rfloor = 1$

for j = 1, . . . ,3 do

j=1 $x_{b1}=[2+6*14+1*1]_3 = [87]_3=0$

j=2 $x_{b2}=[3+6*14+1*3]_5 = [90]_5=0$

j=3 $x_{b3}=[0+6*14+1*5]_{11} = [89]_{11}=1$

The Output: $\langle x \rangle_b = \langle 0,0,1 \rangle_b$

Algorithm1 for two bases with requires ($n_a n_b + n_a$) EMM, if you want use three bases can see in [19].

5. Conclusion

An important improvement that allows for better speed and efficiency is the use of RNS transfers. When representing decimal numbers in such a system, need to return them to their natural state. To return numbers from RNS to decimal, there are several approaches to do this. There is a difference between each method and the other in terms of speed, smooth operations and the application in which it is used. However, the use of RNS remains specific and simple, and to expand its operations to deal with greater complexity, it is preferable to use BE to obtain greater speed.

References

[1] Garner, H. L. *The residue number system*. In Papers presented at the the March 3-5, 1959, western joint computer conference (pp. 146-153). (1959).

[2] Wu, S., Zhao, C., Yuan, Y., Sun, S., Li, J., & Liu, Y. HLG: *A framework for computing graphs in Residue Number System and its application in Fully Homomorphic Encryption.* Cryptology ePrint Archive. (2023).

[3] Gomathisankaran, M., Tyagi, A., & Namuduri, K. HORNS: *A homomorphic encryption scheme for Cloud Computing using Residue Number System.* In 2011 45th Annual Conference on Information Sciences and Systems (pp. 1-5). IEEE. (2011).

[4] Kuchukov, V., Telpukhov, D., Babenko, M., Mkrtchan, I., Stempkovsky, A., Kucherov, N., ... & Grigoryan, M. *Performance Analysis of Hardware Implementations of Reverse Conversion from the Residue Number System.* Applied Sciences, 12(23), 12355. . (2022).

[5] Bigou, K., & Tisserand, A. *Improving modular inversion in RNS using the plus-minus method. In Cryptographic Hardware and Embedded Systems-CHES*, 2013: 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings 15 (pp. 233-249). Springer Berlin Heidelberg. (2013).

[6] Posch, K. C., & Posch, R. *Modulo reduction in residue number systems.* IEEE Transactions on Parallel and Distributed Systems, 6(5), 449-454. (1995).

[7] Umar, A. F. *Data conversion in Residue Number System. Department of Electrical and Computer Engineering Mc Gill University Montreal*. (2011).

[8] Gbolagade, K. A., & Cotofana, S. D. MRC technique for RNS to decimal conversion using the moduli set {2n+ 2, 2n+ 1, 2n}. In PRORISC, Veldhoven, The Netherlands (pp. 318-321). STW. (2008).

[9] Jean C.N. , Kazuhide F. , Thomas P., and Arnaud S. , *Generating Very Large RSA Bases* . IEEE Trans. Emerg. Topics Comput., early access. (2022).

[10] Bigou, K., & Tisserand, A. *Hybrid position-residues number system.* In 2016 IEEE 23nd Symposium on Computer Arithmetic (ARITH) (pp. 126-133). IEEE. (2016).

[11] Gbolagade, K. A., & Cotofana, S. D. *An O (n) residue number system to mixed radix conversion technique.* In 2009 IEEE International Symposium on Circuits and Systems (pp. 521-524). IEEE. (2009).

[12] Chakraborti, Soundararajan, & Reddy. *An implementation of mixed-radix conversion for residue number applications.* IEEE Transactions on computers, 100(8), 762-764. (1986).

[13] Shiriaev, E., Kucherov, N., Babenko, M., & Nazarov, A. *Fast Operation of Determining the Sign of a Number in RNS Using the Akushsky Core Function.* Computation, 11(7), 124. (2023).

[14] Babenko, M., & Golimblevskaia, E. *About One Property of Number Rank in RNS.* In 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus) (pp. 212-216). IEEE. (2021).

[15] Valueva, M., Valuev, G., Semyonova, N., Lyakhov, P., Chervyakov, N., Kaplun, D., & Bogaevskiy, D. *Construction of residue number system using hardware efficient diagonal function*. Electronics, 8(6), 694. (2019).

[16] Ananda Mohan, P. V. *RNS to binary conversion using diagonal function and Pirlo and Impedovo monotonic function*. Circuits, Systems, and Signal Processing, 35, 1063-1076. (2016).

[17] Szabo, N. S., & Tanaka, R. I. *Residue arithmetic and its applications to computer technology*. (1967).

[18] Kawamura, S., Koike, M., Sano, F., & Shimbo, A. *Cox-rower architecture for fast parallel montgomery multiplication.* In Advances in Cryptology—EUROCRYPT 2000: International Conference on the Theory and Application of Cryptographic Techniques Bruges, Belgium, May 14–18, 2000 Proceedings 19 (pp. 523-538). Springer Berlin Heidelberg. (2000).

[19] Bigou, K., & Tisserand, A. *RNS modular multiplication through reduced base extensions*. In 2014 IEEE 25th International Conference on Application-Specific Systems, Architectures and Processors (pp. 57-62). IEEE. (2014).