International Journal of Computer and Organization Trends
ISSN: 2249 – 2593 / https://doi.org/10.14445/22492593/IJCOT-V14I1P302

Volume 14 Issue 1, 12-18, Jan-Apr 2024
© 2024 Seventh Sense Research Group®

Review Article

A Modified RSA Cryptosystem for Cloud Security Using Residue Numbers System

Abdul-Ganiwu Yahaya[1], Peter Awonnatemi Agbedemnab[2], Edem Kwadzo Bankas[3]

[1]Department of Computer Science, School of Computing and Information Sciences, C. K Tedam University of Technology and Applied Sciences Navrongo, Ghana.
[2]Department of Information Systems and Technology, School of Computing and Information Sciences, C. K Tedam University of Technology and Applied Sciences Navrongo, Ghana.
[3]Department of Business Computing, School of Computing and Information Sciences, C. K Tedam University of Technology and Applied Sciences Navrongo, Ghana.

[1]Corresponding Author : agyahaya.stu@cktutas.edu.gh

Received: 01 February 2024 Revised: 02 March 2024 Accepted: 20 March 2024 Published: 06 April 2024

Abstract *- Securing transmitted data on a cloud is an important issue. Integer factorization and discrete logarithm issues are two examples of number theory applications that are crucial to public-key cryptosystems. In the majority of applications, these systems make a great choice, and their security is well-defined and understood. The drawbacks of computational complexity are one of the main issues. Consequently, a different strategy that would improve computing efficiency and security is required. This paper proposes an efficient asymmetric cryptographic scheme by utilizing the inherent properties of the Residue Number System (RNS) and the existing RSA Cryptosystem to encrypt any data size suitable for securing data on cloud systems. The generation of the public and private keys is determined by the selected moduli, which also contains the secret information. These moduli are sensitive to any slight modification resulting in corrupt information when decrypted. The obtained results of the simulation indicate substantial improvement over the best-known equivalent state of the art in terms of computation, power consumption, and runtime. The proposed approach has the ability to identify and rectify errors that may occur in the encrypted data.*

Keywords *- Cloud, Cryptography, RSA Cryptosystem, Residue Number System (RNS), Data Security*.

1. Introduction

The continuous advancements in science have led to significant changes in our way of life, with data playing a crucial role in shaping our modern society. The advancement of communication technologies has led multiple devices to be interconnected to deliver communication and services to humans. Over the previous decades, most developments in all scientific areas have been predicated on the extraction, management, and assessment of data in order to give cutting-edge intelligence.

Due to this, the necessity for the generation of massive amounts of data has increased. Because of the complexity, there is an ongoing need to develop, test and use theoretical concepts, methodologies, and tools in order to successfully combine multidisciplinary approaches to address such problems. As a result, theory is always improving to give the required tools for extracting relevant and correct data in order to promote a successful outcome.

The primary function of a computer involves computation, which revolves around numbers. However, the inherent limitations of binary and decimal numeral systems restrict the efficiency of the arithmetic unit and the processor constructed using these systems. Due to this limitation, there has been a continuing research interest in improving the speed reducing the area cost and power consumption of digital systems. One of the challenges in improving the performance of digital systems from the computational point of view is the carry propagation problem, which is characteristic of conventional number systems (binary and decimal number systems). This is due to the fact that carry propagation limits the performance of arithmetic operations. This carry propagation problem is the major contributor to the internal delay of processors built with conventional number systems [2],[5] & [6]. The growing recognition and choice of unconventional number systems for fast computation is really necessary.

Residue Number System (RNS) is a weightless numerical system that operates without assigning weights, and it is characterized by a set of relatively prime integers $w_1, w_2, \dots w_n$. known as moduli sets. The condition for the moduli sets is that the greatest common divisor

$\gcd(w_1, w_2, \dots w_n) = 1$ for $i \neq j$. The system's Dynamic Range (DR) is denoted as $[0, W]$, where $W = \prod_{i=1}^{n} w_i$, ensuring that any integer $X \in [0, W]$ possesses a unique RNS representation denoted by the ordered set of residues $x = (x_1, x_2, \dots x_n)$, $[X]w_i$ $i = 1,2, \dots.$. RNS has found application in various domains, including cryptography. The advent of public key cryptography, introduced by Diffie and Hellman in 1976, led to the proposal of numerous cryptographic algorithms. The security of these algorithms hinges on mathematically intricate problems like integer factorization and discrete logarithms. A cryptographic scheme is deemed secure if it can withstand cryptographic attacks over a significant period. However, since certain schemes may take several years before being widely studied, making them vulnerable as time passes. Conversely, a cryptographic scheme is considered provable if it can resist cryptographic attacks relying on mathematical assumptions and can be easily adapted to diverse cryptographic groups.

Recently, numerous research endeavors have focused on enhancing the security of the RSA cryptosystem. This has been achieved through a combination with other approaches or by introducing a modification to the existing cryptosystem. However, the effectiveness of these methods alone may not be adequate for definitively establishing the superiority of an algorithm. In the realm of cloud security, the escalating demand for substantial volumes of data and applications essential for personal, health, commercial, and governmental purposes has become pervasive. Safeguarding the extensive data stored in cloud storage from unauthorized tampering is imperative. Therefore, one feasible option is to enhance the RSA cryptographic scheme by integrating a carry-free arithmetic system. This system is designed to robustly withstand cryptographic attacks, boost speed, diminish area costs, minimize power consumption, and ensure the integrity and confidentiality of presumed data. It can be seamlessly implemented in various hardware security modules, addressing the requirement of cloud providers handling vast amounts of data and applications. The subsequent sections are as follows: Section 2 details the methodologies employed to derive the results, and Section 3 provides an analysis of the outcome of the proposed scheme with a conclusion remark in Section 4.

2. Proposed Scheme

Currently, there exist several encryption algorithms for securing data. However, by employing some cryptanalyst techniques, unauthorized individuals are able to bypass these algorithms. In the context of cloud security, this paper suggests an unconventional mathematical model of the RNS system based on the RSA cryptosystem. This security method, or cryptography strategy, is distinct and novel in this field, which can cause the third party to become completely perplexed. It, therefore employed the RNS-based technique to secure the cloud, which is less vulnerable than other existing solutions, in order to prevent the unwanted access of the data. It is known that all data in computing technology is stored in digitized or binary form. To ensure data security, the binary number system is basically changed, in this case, into the residue number system before transferring the information into the cloud. Different cloud services present distinct sets of moduli that RNS offer, and these various sets of moduli can be stored there. The moduli set $\{2^n - 3, 2^n - 1, 2^n + 1\}$ will be used for the hardware realization and simulation process for the proposed scheme. The size of the cipher text will be larger or the same as the plaintext in the cloud environment, which can help maintain security.

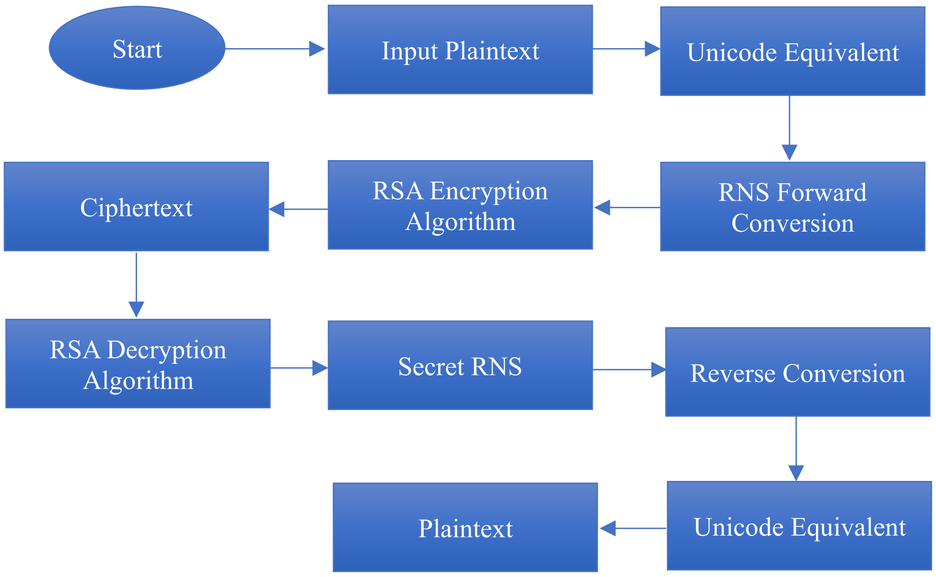

Fig. 1 Flow diagram for the proposed scheme

2.1. Algorithm of the Proposed Scheme

Let $P \rightarrow E \in Z_h$ and $p = 2^n - 3$, $q = 2^n - 1$ and $r = 2^n + 1$, where $p \neq q \neq r$ are relatively prime numbers from the chosen moduli set, for $h = pqr$ and $\varphi(h) = \frac{(p-1)(q-1)(r-1)}{2}$, the encryption key (e), such that $(1 < e < \varphi(h)$ so that $\gcd(e, \varphi(h) = 1)$, and $d \leftarrow e^{-1} mod \varphi(h)$ for $ed \equiv 1(mod \varphi(h))$ where the public keys are (h, e) and the private keys are (p, q, r, d).

Figure 1 represents the architecture of the proposed cryptosystem, wherein both the start and end of the method utilize information conversion based on RNS. Whilst RSA Encryption comes after the forward conversion with the public key, which is then followed by the Decryption process with the private key before the reverse conversion of the decrypted data.

2.1.1. Forward Conversion

For the scheme, the moduli set $\{2^n - 3, 2^n - 1, 2^n + 1\}$ is used for the implementation. The moduli set is relatively co-prime and exhibits interesting features. For the message M such that $C = M^e < h$, whiles the data undergoes the encryption phase, the encryption process transform M^e into another representation, which will be expressed in the form $(r_1^e < h)$. Therefore, the Proposed Scheme is suitable and has the inherent feature of enhancing the throughput. When computing the residue of an arbitrary integer X with respect to a modulus m, X is represented as an n-bit binary number $(x_{n-1}, x_{n-2}, \dots x_0)$. The residue of X with respect to m can be expressed as.

$$|X|_m = |x_{n-1}x_{n-2}x_{n-3}, \dots x_0|_m \qquad (1)$$

Which can also be computed as;

$$|X|_m = |2^{n-1}x_{n-1} + 2^{n-2} + 2^{n-3}x_{n-3} +, \dots 2^0 x_0|_m \qquad (2)$$

such that;

$$|X|_m = ||2^{n-1}x_{n-1}|_m + |2^{n-2}x_{n-2}|_m + |2^{n-3}x_{n-3}|_m, \dots + |2^0 x_0|_m|_m \qquad (3)$$

Given that x_1 can only take on values of 0 or 1, the process of computing the residue X entails the assessment of values $|2^i|_m$. These values are subsequently aggregated using a reduction in relation to the modulus. To determine the remainder of the integer X, the binary representation of the input is represented as a 3n-bit value. Subsequently, the performance partial reduction is calculated for each subset of n-bit utilizing the moduli set $\{2^n - 3, 2^n - 1, 2^n + 1\}$. This involves computing three residues, each corresponding to one of the moduli. Figure 2 depicts the schematic diagram of the forward converter.

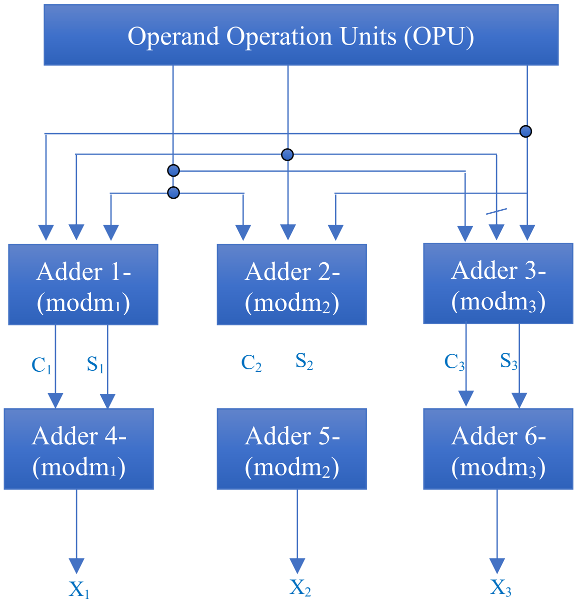

Fig. 2 Schematic drawing of forward converter for the proposed scheme

2.1.2. Reverse Conversion

The reverse conversion is implemented in order to minimize the delay generated. The moduli set used can invade the imbalance issue due to its utilization of either n or (n + 1) −bit width to represent the large residue within the moduli set. Employing this approach, greater parallelism is achieved without introducing significant hardware redundancy. To invert an RNS number using the given moduli set, the simplified CRT is presented using the chosen moduli set.

$$X = \sum_{i=1}^{n} a_i x_i u_i mod M \qquad (4)$$

Were

$$M = \prod_{i=1}^{n} m_i \,, a_i = \frac{M}{m_i}, u_i = a_i^{-1} mod m_i$$

and

$$x_i = (x_1, x_2, x_3, \dots x_n)$$

Therefore

$$X = \left|a_1\left[|u_1 \times x_1|_{m_1}\right] + a_2\left[|u_2 \times x_2|_{m_2}\right] + \cdots a_n\left[|u_n \times x_n|_{m_n}\right]\right|_M \qquad (5)$$

$$= |A + B + C|_M \qquad (6)$$

Where

$$A = |(2^n - 1)(2^n + 1)(2^{n-1})|_{m_1} = (x_{1,0}, x_{1,n-1}, \dots x_1 x_0)$$

$$B = |(2^n-3)(2^n+1)(2^n-3)|_{m_2} = (x_{2,0}, x_{2,n-1}, \dots x_2 x_{2,n-1} \dots x_2 x_0)$$

$$C = |(2^n-3)(2^n-1)(2^n)|_{m_3} = (x_{3,0}, x_{3,n-1}, \dots x_3 x_{3,n-1}, \dots x_3 x_0)$$

Since the representation of x_1, x_2 and x_3 have a bit length of n. Then, the above can be computed as the sum of 3n-bit formed by concatenation and rotation. The two-level architecture realized by the Chinese Remainder Theory (CRT) method can lead to an efficient implementation of RNS to binary converter of the moduli set $M = \{2^n-3, 2^n-1, 2^n+1\}$.

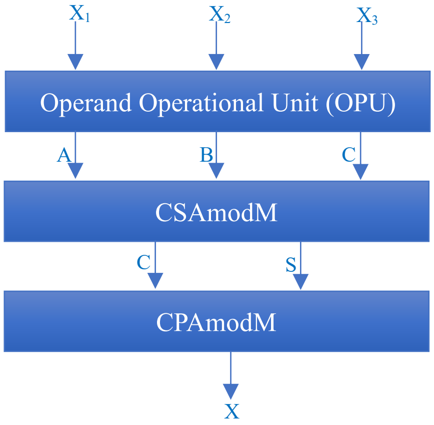

Fig. 3 Flow diagram of the reverse conversion for the proposed scheme

The proposed moduli set incorporates the use of both Carry Save Adder (CSA) and Carry Propagated Adder (CPA). An optimized structure has been proposed by several authors [3]-[7] on modulo (2^n-1) and (2^n+1). The circuit area required by this structure is given as $A_{CSA} = n \times A_{FA}$ for modulo (2^n-1) and $A_{CSA} = n \times A_{FA} + A_{not}$ for (2^n+1) where n represents the number of bits and A_{FA} represent Full Adder and A_{not} are a represent Not gate. The critical path is determined by the delay of an FA for the modulo (2^n-1), and for modulo (2^n+1) an additional delay from the NOT gate is considered. This leads to a theoretical, critical path of $\Delta_{CSA} = \Delta_{FA} + \Delta_{Not}$. For modulo (2^n-3) no delay overhead is experienced, and overall latency and area consumption are reduced. The moduli set leads us to a better internal hardware implementation. Therefore, in comparison to the moduli set architecture, optimizing our design resulted in improved performance, reduced hardware complexity, and enhanced energy efficiency, leading to lower power consumption.

3. Results and Discussion

The paper categorized the different types of cryptography based on their strengths and weaknesses; information about the method's performance and benefits is needed to implement the algorithm in a way that is appropriate for the application. Therefore, the algorithms were tested based on a variety of criteria, and it's important as follows.

- Encryption Time: In the context of the proposed system experiment, it is quantified in milliseconds and denotes the duration needed to convert plaintext into ciphertext.
- Decryption Time: As indicated in the proposed system, it refers to the time taken to decrypt ciphertext to retrieve plaintext, measured in milliseconds.
- Expansion Rate: This refers to the size of the new file after separating the plaintext's (P) size from the ciphertext's (C) size. The proposed scheme's tests estimate the expansion rate in kilobytes.

3.1. Performance Evaluation

In the conventional RSA cryptosystem, for a message M such that $C = M^e < h$, then M can be recovered from C by $M = C^d < h$. However, with the proposed scheme M passes through a second stage of $M_{RNS} \to (x_1, x_2, x_3)$ and the encryption system $C = x_1^e$ the encryption process transform M^e into another representation, which will be expressed in the form x_{ii}, then after decrypting, x_{11} is obtained then $|x|_{m_i}$, is taken and calling back $(x_1, x_2) \to (x_1, x_2, x_3)$. The proposed system will transform M to x_i, using the moduli set and only the knowledge of the moduli set together with the private key can recover the original message.

NB: x_2 or x_3 should be used for the encryption process since x_1 must be part of the secret RNS.

3.2. Theoretical Evaluation

The theoretical encryption and decryption of the conventional RSA cryptosystem and the RNS-RSA were tested using the same parameters. Excellent encryption and decryption results were achieved based on the time it takes for the encryption and decryption process to complete. During the testing, the proposed method can take a file of any size depending upon the value of n for n is even and n > 2 used for the moduli set, the size of the plaintext decreases and also uses many secret keys, which makes the proposed scheme faster and very vulnerable and have less expansion rate than the conventional RSA cryptosystem as shown in the tables below.

Table 1. Parameter for Conventional RSA and the RNS-RSA Cryptosystem

Parameter	Bits	
	Conventional RSA	RNS- RSA
Dynamic Range	3315	3315
Encryption Exponent (e)	701	701
Decryption Exponent (d)	533	533

Table 1 Displays the parameters used for encryption and decryption. To ensure a fair comparison, both schemes were configured with an equal number of bits.

Table 2. RSA-Cryptographic Process

Data	Encryption (Time)	Ciphertext	Decryption (Time)	Plaintext
115	1466.50	1645	5466.50	115
330	2932.93	720	4888.21	330
450	2932.93	60	1010.65	450
560	4888.21	560	4888.21	560
650	4888.21	650	4888.21	650
780	4888.21	2535	6843.83	780

Table 2 Presents the encryption and decryption times of the conventional RSA cryptosystem.

Table 3. RNS-RSA-Proposed scheme

Data	Encryption (Time)	Ciphertext	Decryption (Time)	Decrypted text (secret with RNS)
115	460.75	10	460.75	10
330	160.75	0	160.75	0
450	160.75	0	160.75	0
560	335.67	5	335.67	5
650	335.67	5	335.67	5
780	160.75	0	160.75	0

Table 3 illustrates the encryption and decryption times of the proposed RNS-RSA cryptosystem.

Table 4. Comparison of encryption time

Data	RSA En Time	RNA-RSA En Time	Time Diff	Percentage
115	1466.50	460.75	1005.75	68.582
330	2932.93	160.75	2772.18	94.519
450	2932.93	160.75	2772.18	94.519
560	4888.21	335.67	4552.54	93.133
650	4888.21	335.67	4552.54	93.133
780	4888.21	160.75	4727.46	96.711

Tables 4 and 5 offer a comparison of the encryption and decryption times between the RSA cryptosystem and the RNS-RSA cryptosystem.

Table 5. Comparison of decryption time

Data	RSA Dn Time	RNA-RSA Dn Time	Time Diff	Percentage
115	5466.50	460.75	5005.75	91.57
330	4888.21	160.75	4727.46	96.711
450	1010.65	160.75	849.90	84.094
560	4888.21	335.67	4552.84	93.14
650	4888.21	335.67	4552.54	93.14
780	6843.83	160.75	6683.08	97.651

Figure 4 shows encryption time with Data size of the Proposed RNS-RSA cryptosystem and conventional RSA cryptosystem. The figure clearly reveals that there is a reduction in the time taken to encrypt the plaintext. This shows that the speed of encryption of the proposed RNS-RSA cryptosystem outperformed that of the conventional RSA cryptosystem.

Figure 5 shows the decryption time with Data size of the Proposed RNS-RSA cryptosystem and conventional RSA cryptosystem. It can be observed that the decryption time has reduced due to the modulus reduction, which has improved the speed and increased the strength of security.

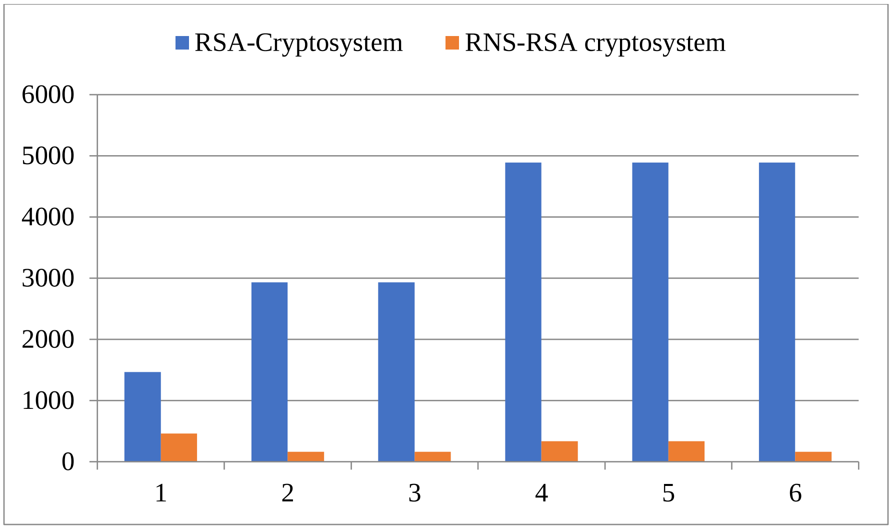

Fig. 4 Encryption time

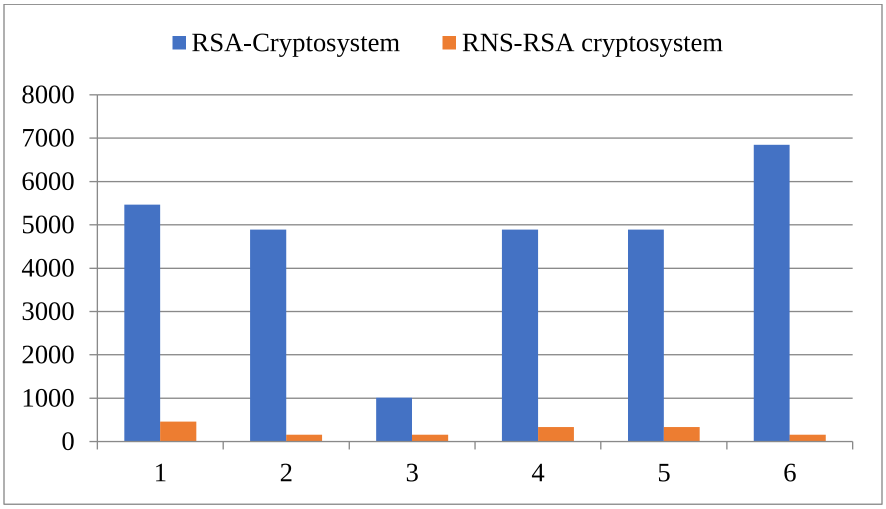

Fig. 5 Decryption Time

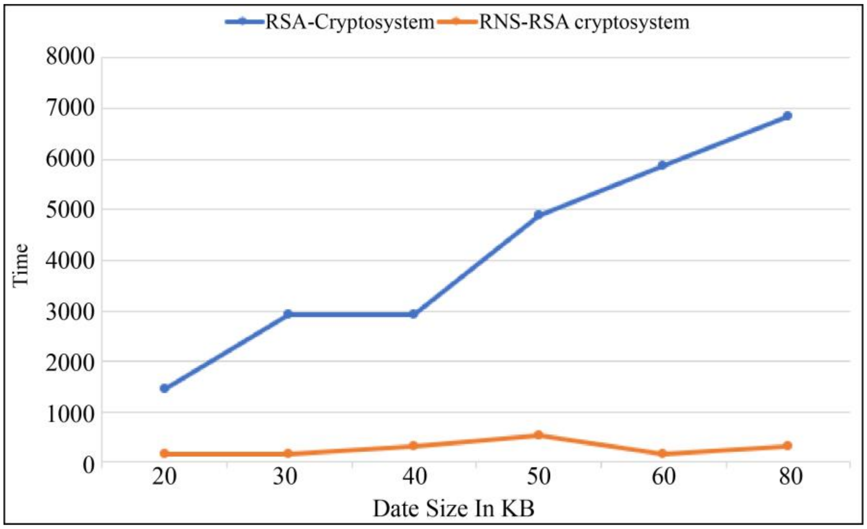

Fig. 6 Expansion rate

Figure 6 Expansion Rate with Data size of the Proposed RNS-RSA cryptosystem and conventional RSA cryptosystem. The results demonstrate that the proposed RNS-RSA cryptosystem performs at a faster rate in both encryption and decryption. It is evident that the size of the plaintext is reduced to enhance encryption. This accelerated encryption speed makes the RNS-RSA scheme the most reliable choice for cloud applications, especially when handling large amounts of data in real-time computation.

The comparison of execution times is mostly intended to demonstrate how quickly the suggested strategy can be implemented. Nevertheless, it can retrieve the plaintext at a higher level. An attacker who can compromise the system must be aware of the moduli set requirements, the key, and the modulo utilized order.

4. Conclusion

The effectiveness of information security significantly impacts the quality of service in data transmission. Perfect security is impossible; instead, we should focus more on protecting our data from theft and interpreting it. To protect data from illegal access and other dangerous actions, the RSA encryption method is the most popular public key encryption technique. The power-of-two moduli set, which has grown in popularity, generated efficient hardware implementation and resulted in ROM-less reverse conversion [2], was used in this research aims to design and construct an enhanced version of the conventional RSA cryptosystem, which requires quick speeds for both encryption and decryption. The messages are processed by the moduli defined in the initial stage to obtaining the residue, which is encrypted. This will help reduce the vulnerability to attack.

References

[1] Abeer Abdel-Jabbar Abu-Zayed et al., *Netnography Internet Research Methodology into the Internet of Toys*, Reconciliation, Heritage and Social Inclusion in the Middle East and North Africa, Springer, Cham, pp. 87–98, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Iqbal Ahmed, “A Brief Review: Security Issues in Cloud Computing and their Solutions,” *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 17, no. 6, pp. 2812–2817, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] Aljwhrh Almtrf, Yasamin Alagrash, and Mohamed Zohdy, “Framework Modeling for User Privacy in Cloud Computing,” *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC),* Las Vegas, NV, USA, pp. 819–826, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[4] B. Angel Rubavathy, “Heterogeneous Security Determination System Inculcating Elgamal Cryptosystem,” *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 11, pp. 2353–2358, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Edem Kwedzo Bankas, Kazeem Alagbe Gbolagade, and Sorin Dan Cotofana, “An Effective New CRT Based Reverse Converter for Novel Moduli set {2 2n+ 1- 1, 2 2n+ 1, 2 2n- 1},” *2013 IEEE 24th International Conference on Application-Specific Systems, Architectures and Processors*, Washington, DC, USA, pp. 142-146, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[6] Mebiratu Beyene, and K. Raja Shekar, “Performance Analysis of Homomorphic Cryptosystem on Data Security in Cloud Computing,” *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–7, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] Manoj Kumar Chande, “Modified Elgamal Signature with Secret Key Pair and Additional Random Number,” *Serdica Mathematical Journal*, vol. 47, no. 4, 2021. [Google Scholar] [Publisher Link]

[8] Qusay Kanaan Kadhim et al., “A Review Study on Cloud Computing Issues,” *Journal of Physics: Conference Series*, vol. 1018, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[9] Israel Koren, Computer Arithmetic Algorithms, 2nd ed., *North Africa: AK Peters/CRC Press*, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[10] Hongyu Li et al., “Blockchain-Based Data Preservation System for Medical Data,” *Journal of Medical Systems*, vol. 42, no. 141, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[11] M.V. Valueva et al., “Application of the Residue Number System to Reduce Hardware Costs of the Convolutional Neural Network Implementation,” *Mathematics and Computers in Simulation*, vol. 177, pp. 232-243, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[12] Beerendra K. Patel, and Jitendra Kanungo, “Area Efficient Diminished 2^n-1 Modulo Adder Using Parallel Prefix Adder,” *Journal of Engineering Research - ICAPIE Special Issue*, pp. 8-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] Mikhail Selianinau, and Yuriy Povstenko, “An Efficient CRT-Base Power-of-Two Scaling in Minimally Redundant Residue Number System,” *Entropy*, vol. 24, no. 12, pp. 1-22, 2022. [CrossRef] [Google Scholar] [Publisher Link]