Proceedings of the 2nd International Conference on Applied Physics and Mathematical Modeling
DOI: 10.54254/2753-8818/56/20240141

Encryption with Complex Variable and its Capabilities

Jiahong Sun

Collingwood School, West Vancouver, British Columbia, V7S1B2, Canada

luck.sun@mycw.org

Abstract. Cybersecurity is instrumental to the modern world. The most effective protection of data online is cryptography and encryption. There are two main types: symmetric and asymmetric. They employ important mathematical concepts to encode vital information. Nevertheless, the encryption field remains largely within the world of real numbers. This paper analyzes an encryption method presented by George Stergiopoulos et al. utilizing complex numbers and investigates its possible usage. The process involves investigating the necessary complex variable applications and a comparative scoring system which provides vital outlook on the promise of this new methodology. Subsequently, the investigation of the time complexity, security and encryption speeds provides a vital outlook on the practical uses in society. The results are promising feasibility of this new algorithm and the encouragement of further investigation into complex variable applications that encrypt with a more substantial range than any operation in the real numbers. Thus, the explicit novel insightful comparison of both symmetric and asymmetric encryption systems to the proposed complex encryption shows vital promise and further interest in investigation into this field as it opens the possibilities to an infinite array of novel complex operations that were previously inaccessible due to the restraint of real numbers.

Keywords: Complex Variable, Encryption, Decryption, Time Complexity, Network Security.

1. Introduction

Encryption is a rising scientific field in the 21st century. The invention and widespread adoption of the internet have brought along revolutionary practical benefits to society. Nevertheless, it has made our society prone to cyberattacks. The rapid development of artificial intelligence has increased the importance of encryption and cybersecurity more than ever. Strong encryption algorithms not only increase cybersecurity, but also improves authentication of data and user integrity [1]. There are two primary settings: symmetric encryption (private-key) and asymmetric encryption (public-key) [2]. The use of mathematics is fundamental to the field. The field of cybersecurity has crucial influence on relevant fields such as quantum computing and algorithm studies [3]. Nonetheless, since its invention and widespread use, most encryption algorithms deal with only the integer field and real numbers of mathematics. This establishes that the field only places with an axis in a surface and world of complex variables and beyond. There have been efforts to adopt the many branches of mathematics such as functions [4], number theory [5], and Elliptic Curves into cryptography [6].

Complex Encryption have shown its preliminary promise. With the enabling of encrypting data across an entire new world as opposed to just an axis of it in the real world, it unleashes unlimited potential for complex and strong encryptions that may dominate the results of its predecessors.

DOI: 10.54254/2753-8818/56/20240141

This paper addresses a recently proposed method of encryption using complex variables within the established symmetric encryption methodology [7]. The paper compares the results of preliminary complex encryption with well-established symmetric and asymmetric encryption using real numbers. Subsequently, the paper shines light on the promise and future development of using a new mathematical world to improve our cybersecurity.

2. Methodology

2.1. Necessary Complex Variables Background

The notion of complex numbers arises from the following identity [8]:

$$i = \sqrt{-1} \tag{1}$$

The branch of complex numbers that can be utilized in cryptography is exponential and logarithmic functions in the complex field.

The Euler form expresses exponents in the complex field in the following notation:

$$e^{i\phi} = \cos(\phi) + isin(\phi) \tag{2}$$

George found an example using the exponential and logarithmic functions in the complex field to achieve the same effects as real number encryption [7]. Define $cis(\phi) = \cos(\phi) + isin(\phi)$. Let $z = a + bi$ where $z \in \mathbb{C}$ [9].

Thus,

$$e^{(a+bi)} = e^{a}\text{cis}(b) \tag{3}$$

Note this equation belongs in the complex plane. Declare $w = e^{a}\text{cis}(b)$ as a new complex variable.

Note, $w = e^{z}$. Define the modulus of z (a complex number) to be the length from z to the 0 and the notation to be |z|.

Example 2.1: Let $z = 3 + 4i$. Please find the |z|.

Proof: This means that the coordinates of z on a cartesian plane is $(3, 4)$. Since the distance d of a point (x, y) to the origin is:

$$d = \sqrt{x^2 + y^2} \tag{4}$$

Hence, |z|, the distance from z to the origin is:

$$\sqrt{3^2 + 4^2} = 5 \tag{5}$$

Define the principle argument of a complex number z to be the reference angle of the terminal arm that includes z and the notation to be $Arg(z)$.

Example 2.2: Let $z = 3 + 3i$. Please find the Arg(z).

Proof: This means that the coordinates of z on a cartesian plane is $(3, 3)$. Since the reference angle ϕ of the terminal arm including point (x, y) to the origin, d is:

$$\phi = \arctan\left(\frac{\text{y}}{x}\right) \tag{6}$$

Hence, Arg(z), the reference angle of the terminal arm desired is:

$$\arctan\left(\frac{3}{3}\right) = \frac{\pi}{4} \tag{7}$$

Define the argument of a complex number to be the principle argument in additional to all equivalent angles and the notation to be $\arg(z)$. Churchill and Brown described logarithmic operation in the complex plane with the following setup [10]:

$$\log(e^{z}) = \log|e^{z}| + \text{iarg}(e^{z}) \tag{8}$$

DOI: 10.54254/2753-8818/56/20240141

Therefore:

$$\log(w) = \log|w| + i(\mathrm{Arg}(w) + 2\pi k) \tag{9}$$

Here, $k \in \mathbb{Z}$.

Note that in the complex plane, the notation log assumes a base of e similar to ln in the reals.

Additionally, the discrete, but infinite points that form complex functions as shown above with infinite integer possibilities for k, make them applicable to randomization in encryption. George used the complex logarithm function substituting the real logarithm to perform the following 4 encryption steps similar to symmetric encryption (AES) for their complex encryption algorithm [7]:

1. Complex Randomization
2. Initial Round
3. Loop through $i = 0, 1, \ldots, k$
4. Final Round

2.2. Quantitative and Qualitative Scoring System

The author will use a straightforward ranking system to score each category. This means if there are k subjects in a given category, each subject will receive a number with k being the best performing, and 1 being the worst performing. If any ties were to occur, all tied subjects will receive the better scoring in Table 1.

Table 1. Comparing CPUs in a MacBook Pro 2021 [11]

Type of CPU	Intel i5	Apple M1	Apple M1 Pro	Apple M1 Max
RAM (GB)	8	8	16	24

Table 2. Scoring CPUs in a MacBook Pro 2021 [11]

Type of CPU	Intel i5	Apple M1	Apple M1 Pro	Apple M1 Max
RAM (Score)	2	2	3	4

Here, the higher score was given to the CPUs with higher RAM as it is clearly preferable over lower RAM in Table 2.

3. Experimentation

3.1. Time Complexity

Time Complexity (TC) is a method to measure the amount of Computer time used by a given algorithm. Specifically, simplified TC can be measured through analyzing the following [12]:

(i) Arithmetic operations performed count
(ii) Comparison count
(iii) Time through a crucial loop count
(iv) Amount of array elements used

TC is measured in the unit O^(f(n)) where f(n) is the general form of the function detailing the number of steps for the algorithm typically conducts.

The author will use the example of bubble sort as a simple algorithm to demonstrate the concept of TC.

In bubble sort, the algorithm composes of two nested loops. The internal loop conducts a comparing method and the external loop is the loop starting index from the first index: 0 to the last index: n-1. Henceforth, through implementing (ii), one understands that the number of comparisons is:

$$\sum_{i=0}^{n-1}(\mathrm{n} - \mathrm{i}) = \frac{n^2 + n}{2} \tag{10}$$

DOI: 10.54254/2753-8818/56/20240141

Since this polynomial's highest degree is 2, it is trivial that the TC for the bubble sort algorithm is $O\hat{}(n^2)$.

3.2. Comparison of Complex and Conventional Encryption

With the necessary background in TC needed to understand its comparisons, other categories are trivial to comprehend. Specifically, data on Network Security is given through qualitatively listing the means of security each encryption provides. Additionally, Encryption and Decryption speeds are given through qualitative measurements from Slow to Fast.

While the complex encryption and AES used similar encryption procedures in Table 3, as comparison, the author uses RSA, which is asymmetric and based on number theory amongst the integers. Primitively, Caesar cipher is used for comparison of real number encryptions [13].

Table 3. Complex Encryption vs Symmetric Encryption and Asymmetric Encryption [7] [14] [15]

Type of Encryption	Complex Encryption	AES (Symmetric Encryption)	RSA (Asymmetric Encryption)
TC	$O\hat{}(n*(\log n)^2)$	$O\hat{}(\log n)$	$O\hat{}(n^3)$
Network Security	Confidentiality, Integrity, Non-repudiation	Confidentiality, Integrity, Non-repudiation	Confidentiality
Encryption Speed	Fast	Fast	Slow
Decryption Speed	Fast	Fast	Slow

4. Results and Discussion

Complex Encryption has performed with comparable results to EAS in all categories except TC. Specifically, it received the highest score of 3 in Network Security, Encryption Speed and Decryption Speed with an almost perfect score of 2 fore TC in Table 4.

Additionally, Table 4 shows that all scores of the Complex Encryption exceeded the RSA encryption system. With the lowest score of 1 across all metrics, the asymmetric encryption system that is based on number theory should be reconsidered for its wide use in the future. Nevertheless, the perfect score of 3 for all sections for EAS representing symmetric encryption still demonstrates to the author that the modern EAS encryption is far from being outdated and encourages the current wide uses of said encryption methodology. This displays a need for modern developers to reshape their focus on development and innovation. While overall Complex Encryption did not attain the perfect score of 12 achieved by EAS and symmetric encryption, its high promise and potential to open up uncountable algorithms in an entirely new mathematical world desires further development into its algorithm and mathematical problems. A reduced complexity of the complex function used during the randomization process may give Complex Encryption the ability to supersede all other widespread notions of encryption in Cryptography.

Table 4. Scoring Complex Encryption vs Symmetric Encryption vs Asymmetric Encryption

Type of Encryption	Complex Encryption	AES (Symmetric Encryption)	RSA (Asymmetric Encryption)
TC (Score)	2	3	1
Network Security (Score)	3	3	1
Encryption Speed (Score)	3	3	1
Decryption Speed (Score)	3	3	1
Total Score	11	12	4

DOI: 10.54254/2753-8818/56/20240141

5. Conclusion

In conclusion, the proposed methodology for Complex Encryption has provided promising results compared to existing system and even dominates the abilities of certain asymmetric encryptions such as RSA. This comparison provides a clear insight on the potential of this field and a positive future for the encryption field as it branches into an entire new world in mathematics. Nevertheless, preliminary results remain unable to be adopted widely and its results are still lackluster compared to existing symmetric systems such as EAS. Henceforth, future research should investigate more efficient algorithms to decrease the TC of current estimates of a preliminary complex encryption system. Additionally, infinite mathematical operation within the complex worlds remains unexplored. Further research should seek to utilize the complex operations in this world to strengthen current security capabilities. With development, the author sees the possibility that complex encryption may replace all real number encryptions in the future as all real operation remain viable in the complex world. Nevertheless, the utilization of complex integrations and other complex procedures remains unknown. A more time-efficient methodology could potentially provide a revolutionary change in the world of cryptography. The author is interested to see the effect of artificial intelligence on complex encryptions as at this stage, complex mathematics seem to be the weakness of artificial intelligence capabilities, at least compared to most literary subjects. Subsequent inquiries are crucial for the network security and surrounding fields of algorithm and quantum computing. Eventually, significant attention and widespread adoption of complex encryption algorithms may become a reality.

References

[1] A Kaushik B, Malik V and Saroha V 2023 A Review Paper on Data Encryption and Decryption. International Journal for Research in Applied Science and Engineering Technology. 11(4):1986–92.

[2] Bellare M, Desai A, Jokipii E and Rogaway P 1997 A concrete security treatment of symmetric encryption. IEEE Xplore. 394–403.

[3] Gupta A 2023 Advances in Cryptography and Security. Quest Journals Journal of Software Engineering and Simulation. 9(9):2321–3809.

[4] Bhanot R and Hans R 2015 A Review and Comparative Analysis of Various Encryption Algorithms. International Journal of Security and Its Applications. 9(4):289–306.

[5] Jahan I, Asif M and Liton J R 2015 Improved RSA cryptosystem based on the study of number theory and public key cryptosystems. American Journal of Engineering Research. 4(1):143–9.

[6] Ullah S, Zheng J, Din N, Hussain MT, Ullah F and Yousaf M 2023 Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. Computer Science Review. 47:100530.

[7] Stergiopoulos G, Kandias M and Gritzalis D 2015 Approaching Encryption through Complex Number Logarithms.

[8] Forsyth A R 1918 Universal Digital Library. Theory of Functions of a Complex Variable. Cambridge University Press.

[9] Sankanagoudar S 2021 A critical study of complex analysis with special reference to mathematics a branch. International Journal of Creative Research Thoughts. 9(11):2320–882.

[10] Brown J and Churchill R 1943 Complex variables and applications. Eighth Edition. McGraw-Hill Higher Education. New York.

[11] Kasperek D, Podpora M and Kawala-Sterniuk A 2022 Comparison of the Usability of Apple M1 Processors for Various Machine Learning Tasks. Sensors. 22(20):8005.

[12] Mridha P and Kumar D. B 2021 An Algorithm for Analysis the TC for Iterated Local Search (ILS). Quest Journals Journal of Research in Applied Mathematics. 7(6):2394-0735.

[13] Luciano D and Prichett G 1987 Cryptology: From Caesar Ciphers to Public-key Cryptosystems. The College Mathematics Journal. 18(1):2–17.

DOI: 10.54254/2753-8818/56/20240141

[14] Patra J, Joshi B and Chowdhury S 2018 Comparison of TC of Symmetric and Asymmetric Key Cryptographic Algorithms. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 3(4):2456–3307.
[15] Borwein J M and Borwein P B 1988 On the Complexity of Familiar Functions and Numbers. SIAM Review. 30(4):589–601.