Engineering and Technology Journal e-ISSN: 2456-3358

Volume 09 Issue 10 October-2024, Page No.- 5386-5393

DOI: 10.47191/etj/v9i10.19, I.F. – 8.227

© 2024, ETJ

Message Authentication Scheme on Light Weight Parallel Encryption Model with Digit Artithmetic of Covertext using Secure Hash Algorithm

Sariyun Naja Anwar[1], Widiyanto Tri Handoko[2], Eka Ardhianto[3], Edy Supriyanto[4], Dwi Agus Diartono[5]

[1,4]Program Study of Information Management, Faculty of Vocational

[2]Program Study of Information Engineering, Faculty of Information Technology and Industry

[3]Program Study of Information Technology, Faculty of Information Technology and Industry

[5]Program Study of Information Systems, Faculty of Information Technology and Industry

[12345]Univesitas Stikubank, Semarang, Central Java, Indonesia

ABSTRACT: This research aims to enhance message security by developing a Light Weight Parallel Digit Arithmetic of Covertext (PDAC) encryption-based authentication scheme that adopts the Secure Hash Algorithm (SHA) algorithm to ensure message integrity and authentication aspects. Through experiments, tests are conducted on two main aspects: entropy and collision resistance. The experimental results show that the average entropy generated reaches 4.992, or 62.41% of the optimal entropy value. While this result shows a good randomness, there is room for further improvement to reach the optimal level. Collision resistance testing using Google's SHAttered tool showed very positive results. No collisions were found in any of the samples tested, indicating that the PDAC scheme combined with SHA can maintain message integrity well. This indicates that PDAC has strong resistance to hash-based attacks, ensuring that messages remain authentic and safe from manipulation. Thus, this study concludes that PDAC schemes offer a good balance between efficiency, security, and low power consumption, making it suitable for use in resource-constrained environments such as IoT devices and mobile applications.

KEYWORDS: Light Weight PDAC, Secure Hash Algorithm, Message Authentication, Entropy, Collision Resistance

I. INTRODUCTION

Encryption is a technique used to convert a readable message into another format that is difficult to understand. The encryption is also known as a technique that involves the study of mathematics and information protection to secure a message [1], [2]. Aspects of concern in cryptography are Confidentiality, Data Integrity, Authentication, Non-Repudiation [3]. The confidentiality aspect refers to the ethical and legal need to protect confidential information from unauthorised access or disclosure [4]. Confidentiality refers to the use of safeguards to prevent unauthorised persons from accessing confidential information [5]. This suggests that access to sensitive information should be limited to authorised persons or institutions. The aspect of data integrity ensures that data sets or messages are accurate, intact, undamaged, and preserved in their original context [6]. It also describes how records are linked to other related records, with a focus on preventing accidental changes to sensitive information. The non-repudiation aspect is a mechanism that guarantees that the parties sending messages to each other cannot deny [7], [8]. Thus, the message will have a trustworthy legal certainty that the sending party is indeed performing the transaction.

Light weight PDAC is an emerging encryption model that features the merging of cryptographic and steganographic techniques in parallel [9], [10]. Light Weight PDAC is classified as a symmetric cipher, which means it uses the same key for both encryption and decryption. Light weight PDAC has 4 phases of process in it, which are: Covertext Generator, Encryption Key Generator, Encryption, and Finalization. Light Weight PDAC works by converting text characters into binary values. The covertext generator part works to generate the covertext. Covertext in Light Weight PDAC is the value used to hide the encryption key. The Light Weight PDAC covertext also acts as the encryption key. The Light Weight PDAC encryption process is done using the XOR logic process. The XOR operation requires two operands, called: encryption key and secret information. This XOR logic can produce different values by performing the same operation with the same encryption key. The advantage of using XOR logic is that in addition to the common basic operations, XOR has complex operations [11], [12], [13]. The finalization process is used to produce the output in the form of ciphertext. Figure 1 provides an overview of the Light Weight PDAC process [10].

In the literature review, there are several predecessors of the Light Weight PDAC encryption model. Parallel Encryption with Digit Arithmetic of Covertext (PDAC) was the first model in 2013 [14]. This first version of PDAC focuses on the confidentiality aspect. The weakness of this

PDAC is that the output ciphertext produced has a size of 125% of the plaintext size. The development of PDAC is New PDAC [15]. New PDAC focuses on solving the capacity aspect. However, New PDAC is only able to reduce the output capacity to 116.7% of the plaintext size. The next development is the modification of New PDAC [16], which can reduce the ciphertext size to 112% of the plaintext. The modification of PDAC using repeated keys [17], [18], focuses on the ease of use of encryption keys that focus on the confidentiality aspect. Improving the confidentiality aspect of PDAC is done using a fuzzy logic approach [19], [20]. The weakness of this model is that the output ciphertext is still 125% of the plaintext size. The Light Weight PDAC model [9], [10] which focuses on reducing the ciphertext size succeeded in reducing the ciphertext size capacity to 100%. Table 1 summarises the development of PDAC encryption models and their focus.

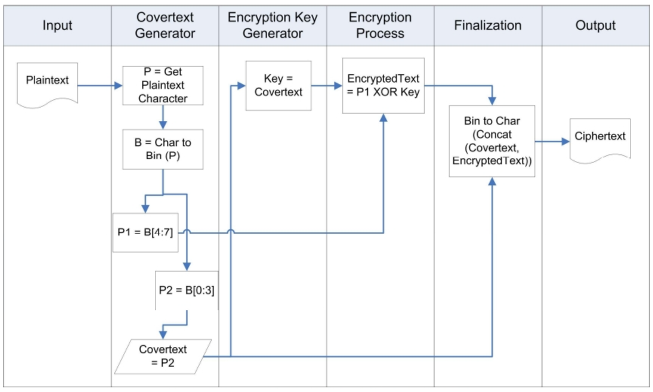

Figure 1. Light Weight PDAC Encryption Process Framework [10].

Table 1. PDAC development and focal aspects of model development.

No	Ecnryption Model	Aspect of Model Development		
		Confidentiality	Capacity	Integrity
1	PDAC [14]	V	-	-
2	New PDAC [15]	-	V	-
3	Modified New PDAC [16]	-	V	-
4	PDAC uses a repeated key [17]	V	-	-
5	Repetitif Covertext PDAC [18]	V	-	-
6	Fuzzy Logic PDAC [19], [20]	V	-	-
7	Light Weight PDAC [9], [10]	-	V	-

Based on Table 1, the integrity aspect of the PDAC encryption model has never been developed. This integrity aspect is considered important because it ensures that the messages sent are not manipulated during the transmission process [21], [22]. With the integrity aspect of the Light Weight PDAC model, the process of securing confidential messages sent by the parties to each other does not worry about the confidentiality of the message itself.

Hash functions are often called one-way functions, message digests, or message authentication codes (MACs). A hash function is a mathematical function that takes a variable length input and converts it into a binary value of a fixed length [23]. One algorithm that can be used to verify the authenticity of a message is the Secure Hash Algorithm (SHA). This SHA algorithm is a one-way hash function that produces a message digest [24]. Figure 2 shows the basic scheme of a hash function. With (M) is a message of free length, (H) is a hash function, and (h) is a message digest of fixed length. The hash function will produce different message digest values for different text message values, so even if the text message has only a small change, the message digest value will also change. By applying the hash function, the text message will be authentic and avoid illegal access by unauthorised entities and parties [25][26].

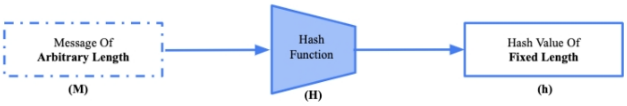

Figure 2. The Hash Function Framework.

This research aims to add integrity aspects to the Light Weight PDAC encryption model. So that the formulation of the problems faced is: 1) How to modify the Light Weight PDAC encryption model framework design by adopting the SHA-1 algorithm as a guarantor of integrity and authentication aspects, 2) How does the new Light Weight PDAC framework modification affect the Confidentiality aspect, and 3) How does the integrity aspect of the Light Weight PDAC encryption model affect collision.

II. THEORETICAL LITERATURE

A. *Symetric Key Cryptography*

A symmetric encryption algorithm is a classic cryptographic algorithm where the key is the same for both encryption and description. The schematic of the symmetric encryption algorithm is shown in Figure 3. A plaintext is encrypted using a key to produce a ciphertext. The ciphertext is decrypted using the same key to produce the plaintext.

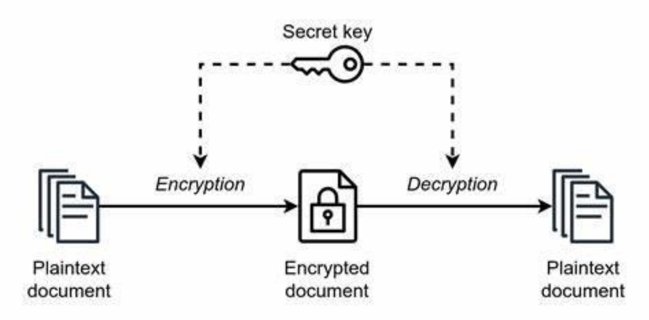

Figure 3. Encryption and Decryption Process in Symmetric Cryptography.

Symmetric cryptographic algorithms are divided into two categories: stream ciphers and block ciphers. Where in the stream algorithm, the encryption process will be oriented towards one bit or byte of data. While in the block algorithm, the encryption process is oriented towards a set of bits or bytes of data (per block).

B. Light Weight PDAC

Light weight PDAC is an encryption model that is being developed and has the feature of combining cryptography and steganography techniques in parallel [9], [10]. Light weight PDAC has 4 stages of process in it, namely: Covertext Generator, Encryption Key Generator, Encryption, and Finalisation. The Light Weight PDAC encryption process is performed using the XOR logic process. The XOR operation requires two operands, namely: encryption key and secret information. This XOR logic can produce different values by performing the same operation with the same encryption key. The advantage of using XOR logic is that in addition to the common basic operations, XOR has complex operations [11], [12], [13]. The finalisation process is used to produce the output in the form of ciphertext. Figure 4 shows the standard PDAC scheme.

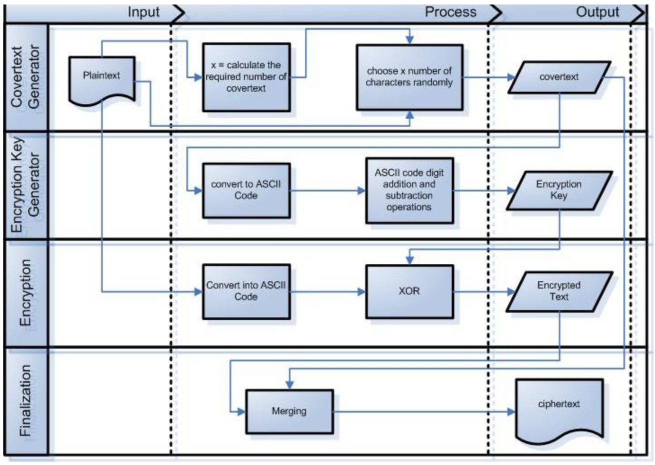

Figure 4. PDAC encryption model.

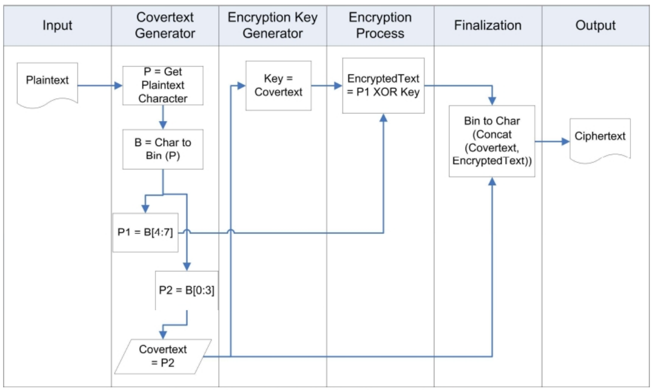

Figure 5. Model Encryption of Light Weiht PDAC.

In the literature review, there are several predecessors of the Light Weight PDAC encryption model. Parallel Encryption with Digit Arithmetic of Covertext (PDAC) was the first model in 2013 [14]. This first version of PDAC focuses on the confidentiality aspect. The weakness of this PDAC is that the outpur ciphertext produced has a size of 125% of the plaintext size. The development of PDAC is New PDAC [15]. New PDAC focuses on solving the capacity aspect. However, New PDAC is only able to reduce the output capacity to 116.7% of the plaintext size. The next development is the modification of New PDAC [16], which can reduce the ciphertext size to 112% of the plaintext. The modification of PDAC using repeated keys [17], [18], focuses on the ease of use of encryption keys that focus on the confidentiality aspect. Improving the confidentiality aspect of PDAC is done using a fuzzy logic approach [19], [20]. The weakness of this model is that the output ciphertext is still 125% of the plaintext size. The Light Weight PDAC model [9], [10] which focuses on reducing the ciphertext size succeeded in reducing the ciphertext size capacity to 100%. Figure 5 shows the scheme of developing PDAC as Light Weight PDAC.

C. SHA-1

SHA stands for Secure Hash Algorithm which is a standard hash function published by NIST (National Institute of Standard and Technology) [21]. SHA is published with several versions including SHA-1 with a digest size of160 bits. The way the SHA-1 cryptography algorithm works is to accept input in the form of a message of arbitrary size and produce a message digest that has a length of 160 bits [24], [25]. The SHA-1 hash function scheme is visualised in Figure 6.

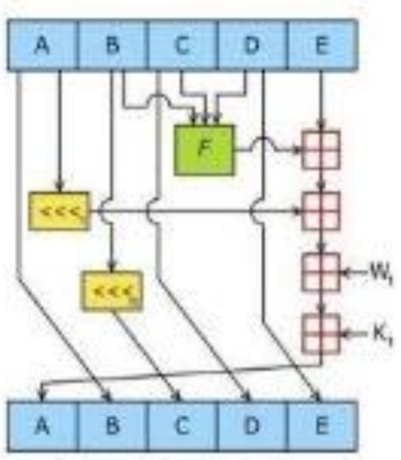

Figure 6. SHA-1 hash scheme.

SHA-1 accepts as input a string with a maximum size of 264bits. For each string, SHA-1 will produce a 160-bit output of that string, and that output is called the message digest. The message digest length can range from 160 to 512-bits depending on the algorithm. SHA-1 is said to be secure because the SHA-1 process is calculated infinitely to find the appropriate string to produce a message digest or it can also be used to find two different strings that will produce the same message digest. In SHA-1 each string block has 512-bits which can be done with 16 sequences of 32 bits. The purpose of string stuffing is to make the total of the stuffed strings a multiplication of 512 bits.

For example, the text to be entered into SHA-1 is ‘halo’, it will produce the value a message digest: ‘33b1eac210971fb02a3b90afce9dbff758be794d’, and text2 is “hallo” by using two “l” characters, it will produce the value of message digest is “fd4cef7a4e607f1fcc920ad6329a6df2df99a4e8”. Both message digests have the same length but different values.

D. Entropy

In the field of information theory, a high entropy value represents true randomness. Data security issues arising from the effect of insufficient entropy show that sufficient randomness is important for security [16]. Entropy is used as a measure of information randomness that reflects the strength of a cryptographic algorithm [13], [14], [16]. The higher the entropy value, the more random the information. This can affect the algorithm's resistance to hacker attacks. To calculate entropy, equation (1) is used.

$$H_m = \sum_{i=0}^{2^n-1} P(m_i) \log_2 \frac{1}{P(m_i)} \qquad (1)$$

III.METHOD

This section describes the research method shown in Figure 7. The research conducted is divided into three stages, namely: 1) Preliminary Experiment, 2) Advanced Experiments, and 3) Evaluation.

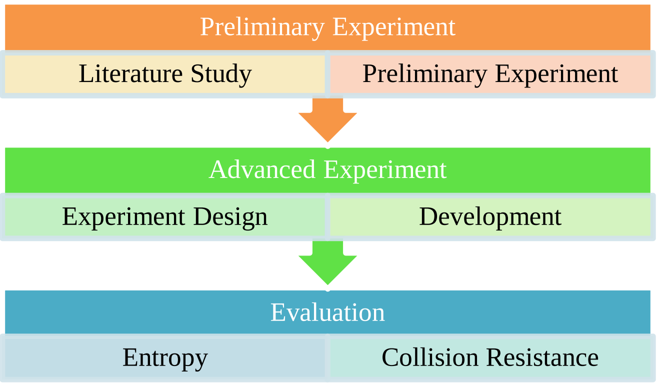

Figure 7. Research Design.

In the preliminary stage of experimentation, we conducted a literacy study on the theoretical basis of cryptography, the development of PDAC encryption models, hash methods, SHA-1, and conducted preliminary experiments to gain in-depth understanding. In the advanced experiments, the research design was made by applying the SHA-1 algorithm to secure the integrity aspect of text messages from the PDAC encryption model. In the follow-up experiments, the same text samples were used as in the initial experiments. Figure 8 shows the design of the proposed new scheme of PDAC development with SHA-1. In the Evaluation section, the average entropy value of the resulting ciphertext is calculated.

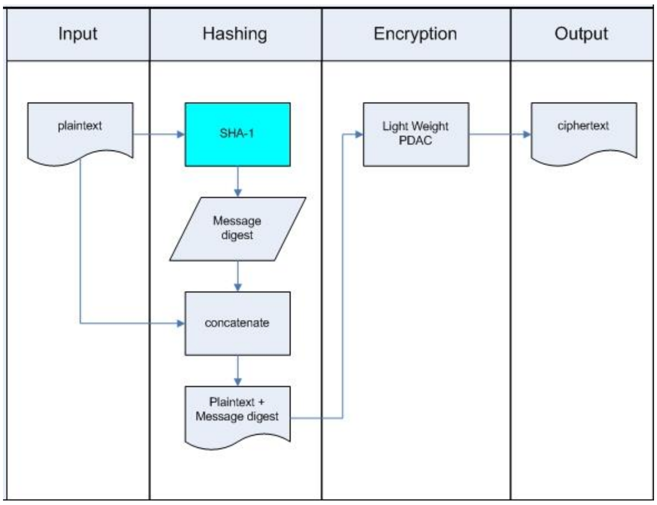

Figure 8. Proposed scheme of Light Weight PDAC using SHA-1.

IV. RESULTS AND DISCUSSIONS

In this experimental research, the data set used comes from the Telegram Astronomer Dataset. The number of datasets used is 14 different file sizes. The various sizes of this data set aim to equate to the state of the form of transmission file sizes that exist in the real world. Table 2 shows the size of the data set used.

Table 2. The size of the dataset used.

File No.	File Size (KB)	Type
1	1	Text ASCII
2	2	Text ASCII
3	3	Text ASCII
4	4	Text ASCII
5	5	Text ASCII
6	6	Text ASCII
7	7	Text ASCII
8	8	Text ASCII
9	9	Text ASCII
10	10	Text ASCII
11	16	Text ASCII
12	32	Text ASCII
13	64	Text ASCII
14	128	Text ASCII

Based on the experiments conducted, several discussions are obtained, namely: the security level of the Light Weight PDAC encryption model, and the measurement of the collision rate against message authentication using SHA-1. More clearly will be discussed in the following subchapters.

A. Security Level in Light Weight PDAC

In the experiment of message security using the Light Weight Parallel Digit Arithmetic of Covertext (PDAC) method, measuring the entropy value is one of the main indicators to evaluate the security level of the encryption scheme. Entropy, which measures the degree of randomness or uncertainty in a cryptographic system, is essential to ensure that encrypted messages are difficult for unauthorised parties to guess or reconstruct. In this experiment, the average entropy resulting from the test was 4.99258. This value indicates a fairly good level of randomness in the context of Light Weight PDAC-based message encryption. Table 3 shows the measurement results of the entropy value of the Light Weight PDAC.

Table 3. PDAC Light Weight Entropy Value.

File No.	File Size (KB)	Entropy Value
1	1	4,96840
2	2	4,91833
3	3	4,74152
4	4	4,81235
5	5	4,81382
6	6	4,95778
7	7	4,90228
8	8	5,04026
9	9	5,00524
10	10	4,98912
11	16	5,12318
12	32	5,01686
13	64	5,01254
14	128	5,59450
Average		4,99258

Although this entropy value is quite high, the entropy achievement is equivalent to 62.41% of the optimal entropy expected under ideal conditions. This value indicates that there is still room for improvement in terms of randomness optimisation. In the context of cryptography, optimal entropy represents the ultimate limit of randomness, meaning that every possible output of the encryption has almost the same probability of occurring. With an entropy of 62.41% of the optimal, the scheme still provides a strong level of randomness, although it has not reached the maximum desired level.

In further analysis, this entropy is affected by the way the data is partitioned and encrypted in parallel. Each part of the message processed through Light Weight PDAC produces a different distribution of numbers, thus increasing the overall level of randomness. However, some message segments may have more predictable patterns, leading to a decrease in the overall entropy. This is a major challenge in lightweight encryption schemes such as PDAC, where the balance between speed, power efficiency and security often lead to some compromises on entropy optimisation.

Nonetheless, achieving 62.41% of the optimal entropy shows that the scheme still provides an adequate level of security in the face of statistical-based attacks, such as frequency attacks or pattern distribution analysis attacks. With an average entropy that is almost close to 5, the system still offers good protection against forced message disclosure attempts. Therefore, although not perfect, the Light Weight PDAC encryption method is reliable enough to be used in applications that require a lightweight form of security such as IoT devices and mobile devices.

B. Collision Resistance in SHA-1 Light Weight PDAC

In message security experiments using Light Weight Parallel Digit Arithmetic of Covertext (PDAC), one important aspect tested is collision resistance, which is the ability of a cryptographic scheme to prevent two different inputs from producing the same hash output. One of the tools used to test this is Google's SHAttered, a well-known tool used to detect potential collisions in hash algorithms, especially those based on Secure Hash Algorithm (SHA), such as SHA-1. Google developed SHAttered to identify weaknesses that cause potential collisions in the SHA-1 hash algorithm, ultimately allowing security exploits by attackers.

In the context of this research, a sample dataset on Light Weight PDAC concatenated with SHA-1 was tested to see if the scheme has collision resistance when measured using Google's SHAttered. The experimental results in Table 4, show that out of all the samples tested, none of them showed a collision. This is a very positive result and illustrates that this PDAC-based encryption method has strong resilience against hash collision-based attacks, at least in tests using this tool.

Table 4. Collision Resistenace Testing.

File No.	File Size (KB)	Collision
1	1	No
2	2	No
3	3	No
4	4	No
5	5	No
6	6	No
7	7	No
8	8	No
9	9	No
10	10	No
11	16	No
12	32	No
13	64	No
14	128	No

The absence of collisions in these experimental results shows that each message processed through Light Weight PDAC encryption produces a unique hash value, even if the encrypted messages are very similar or have almost the same pattern. This is very important because in the world of cryptography, the occurrence of collisions can be a loophole that can be exploited by an attacker to replace the original message with a fake message that has the same hash. Thus, systems that are not collision-resistant will be vulnerable to data integrity attacks, such as man-in-the-middle attacks or digital signature forgery attacks.

The Light Weight PDAC method uses digit arithmetic techniques that play a role in increasing the randomness of the data processed in this encryption scheme. This technique not only helps in speeding up the encryption process through parallelisation, but also ensures that each part of the encrypted message has a high distribution of randomness, thus minimising the chances of collisions. Tests using Google's SHAttered helped verify that even with a lightweight encryption scheme like Light Weight PDAC, which is designed for power- and performance-constrained environments, no significant weaknesses in collision resistance were found.

The fact that no collisions were found in any of the tested samples gives an indication that this encryption method is quite secure in the face of collision-based attacks. However, it is important to note that Google's SHAttered is specifically designed to detect weaknesses in the SHA-1 hash algorithm, and although no collisions were found in this study, further evaluation is needed to test the robustness of this scheme against other hash algorithms that may be used in the future.

From a practical perspective, these results show that Light Weight PDAC and SHA-1 based encryption schemes are reliable in applications that require message integrity protection, such as sensitive data communication, digital signatures, and message authentication. Collision resistance is essential in ensuring that each message has a unique and unforgeable digital footprint, thus preventing attempts at message manipulation by third parties. Moreover, since Light Weight PDAC is a lightweight encryption scheme, this advantage in collision resistance makes it ideal for use in power- and resource-constrained systems, such as IoT devices and mobile applications.

With no collisions detected in this experiment, Light Weight PDAC and SHA-1 provide good security guarantees in terms of resilience against hash-based attacks. However, further evaluation of these schemes needs to be done in the context of using more robust hash algorithms, to ensure that these methods remain relevant in the face of future security challenges.

V. CONCLUSIONS

The conclusion of the experiments combining entropy and collision resistance testing on the Light Weight Parallel Digit Arithmetic of Covertext (PDAC) encryption scheme shows that it offers good security with high efficiency. In the entropy test, the PDAC scheme produced an average entropy value of 4.992, which is equivalent to 62.41% of the optimal entropy. While this value indicates good randomness, there is still room for improvement to achieve a more optimal entropy, which is important to ensure maximum randomness and security in cryptographic systems.

On the other hand, collision resistance testing using Google's SHAttered showed very positive results. No collisions were found in any of the samples tested, which shows that the PDAC scheme can maintain message integrity well. This resistance is crucial in preventing two different inputs from producing the same hash output, thus minimising the possibility of attacks that exploit weaknesses in the encryption process.

With near-optimal entropy and no collisions in the experimental results, PDAC proved to have a good balance between speed, efficiency, and security. This makes it suitable for use in environments that require lightweight encryption, such as IoT and mobile devices, where power consumption and processing capacity are often limited.

Overall, PDAC shows promising performance in terms of message security. However, further research is recommended to optimise the entropy value and test the robustness against stronger hash algorithms, such as SHA-256 or SHA-3, to ensure the relevance of this scheme in the face of growing cryptographic challenges.

REFERENCES

1. M. S. Gayathri and V. Preethi, "Study: Cryptography for information security," 2024, p. 020025. doi: 10.1063/5.0190639.
2. P. Kulkarni and C. Kothari, "Documentation and Data Integrity in Pharmaceutical Industry," in Modern Aspects of Pharmaceutical Quality Assurance, Singapore: Springer Nature Singapore, 2024, pp. 381–403. doi: 10.1007/978-981-99-9271-3_11.
3. S. Pothireddy, N. Peddisetty, P. Yellamma, G. Botta, and K. N. Gottipati, "Data Security in Cloud Environment by Using Hybrid Encryption Technique: A Comprehensive Study on Enhancing Confidentiality and Reliability," International Journal of Intelligent Engineering and Systems, vol. 17, no. 2, pp. 159–170, Apr. 2024, doi: 10.22266/ijies2024.0430.14.
4. O. M. C. Osazuwa, "Confidentiality, Integrity, and Availability in Network Systems: A Review of Related Literature," Int J Innov Sci Res Technol, vol. 8, no. 12, pp. 1946–1955, 2023.
5. Akoh Atadoga, Oluwatoyin Ajoke Farayola, Benjamin Samson Ayinla, Olukunle Oladipupo Amoo, Temitayo Oluwaseun Abrahams, and Femi Osasona, "A COMPARATIVE REVIEW OF DATA ENCRYPTION METHODS IN THE USA AND EUROPE," Computer Science & IT Research Journal, vol. 5, no. 2, pp. 447–460, Feb. 2024, doi: 10.51594/csitrj.v5i2.815.
6. R. Sahbi, S. Ghanemi, and M. A. Ferrag, "Security of internet of vehicles in smart cities: authentication and confidentiality aspects," International Journal of Internet Technology and Secured Transactions, vol. 13, no. 3, pp. 232–269, 2024, doi: 10.1504/IJITST.2024.136655.
7. N. S. Mohammed, O. A. Dawood, A. M. Sagheer, and A. A. Nafea, "Secure Smart Contract Based on Blockchain to Prevent the Non-Repudiation Phenomenon," Baghdad Science Journal, May 2023, doi: 10.21123/bsj.2023.8164.
8. A. Hadabi et al., "Proxy re-encryption with plaintext checkable encryption for integrating digital twins into IIoT," Computers and Electrical Engineering, vol. 116, p. 109164, May 2024, doi: 10.1016/j.compeleceng.2024.109164.
9. E. Ardhianto, W. T. Handoko, and E. Lestariningsih, "New Mechanism of Parallel Encryption with Digit Arithmetic of Cover Text Encryption Model with Reduced Ciphertext Size," ICIC Express Letters, vol. 18, no. 1, pp. 9–15, 2024.
10. W. T. Handoko, E. Ardhianto, H. Murti, and R. S. Redjeki, "A LIGHT WEIGHT OF PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC OF COVERTEXT ENCRYPTION MODEL," J Theor Appl Inf Technol, vol. 101, no. 24, pp. 8028–8037, 2023.
11. R. Chemlal, "A note on combining chaotic dynamical systems using the fuzzy logic XOR operator," Dec. 2020.
12. Y. He, G. Xia, and C. He, "A File cloud sharing method based on XOR operation," IOP Conf Ser Mater Sci Eng, vol. 768, no. 7, p. 072085, Mar. 2020, doi: 10.1088/1757-899X/768/7/072085.
13. C. Singh and E. Baburaj, "XOR Reformed Paillier Encryption Method with Secure De-duplication for Image Scaling and Cropping in Reduced Cloud Storage," International Journal of Intelligent Engineering and Systems, vol. 12, no. 4, pp. 328–337, Aug. 2019, doi: 10.22266/ijies2019.0831.30.
14. S. Kataria, B. Singh, T. Kumar, and H. S. Shekhawat, "PDAC (Parallel Encryption with Digit Arithmetic of Cover Text) Based Text Steganography," in Int. Conf. on Advances in Computer Science, AETACS, 2013, pp. 175–182.
15. M. Gaur and M. Sharma, "A New PDAC (Parallel Encryption with Digit Arithmetic of Cover Text) Based Text Steganography Approach for Cloud Data Security," International Journal on Recent and Innovation Trends in Computing and Communication , vol. 3, no. 3, pp. 1344–1352, 2015, [Online]. Available: http://www.ijritcc.org
16. W. T. Handoko, E. Ardhianto, and E. Supriyanto, "MODIFIKASI NEW PDAC (PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC OF COVER TEXT)," in SENDIU 2020, 2020, pp. 55–59.
17. E. Ardhianto, K. M. A. Pamungkas, E. Supriyanto, and E. Lestariningsih, "MODIFIKASI PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC AND COVERTEXT (PDAC) MENGGUNAKAN KUNCI BERULANG," Jurnal Informatika Universitas Pamulang, vol. 7, no. 2, pp. 308–312, 2022.
18. H. Murti, E. Supriyanto, R. Redjeki, and E. Ardhianto, "ADOPSI REPETITIF COVERTEXT PADA MEODEL ENKRIPSI PDAC," Jurnal Informatika Polinema, vol. 9, no. 1, pp. 1–8, Nov. 2022, doi: 10.33795/jip.v9i1.1152.
19. E. Ardhianto, Y. Heryadi, L. A. Wülandhari, and W. Budiharto, "Covertext Generation using Fuzzy Logic Approach in Parallel Encryption with Digit Arithmetic of Covertext to Improve Information Confidentiality," International Journal of Innovative Computing, Information and Control, vol. 19, no. 4, pp. 1311–1321, Aug. 2023, doi: 10.24507/ijicic.19.04.1311.

20. E. Ardhianto, Y. Heryadi, L. A. Wulandhari, and W. Budiharto, “PARALLEL ENCRYPTION WITH DIGIT ARITHMETIC OF COVERTEXT ENCRYPTION MODEL USING COVERTEXT GENERATOR WITH FUZZY LOGIC APPROACH,” ICIC Express Letters ICIC International, vol. 17, no. 7, pp. 817–824, 2023, doi: 10.24507/icicel.17.07.817.
21. F. Buccafurri, V. De Angelis, and S. Lazzaro, “MQTT-I: Achieving End-to-End Data Flow Integrity in MQTT,” IEEE Trans Dependable Secure Comput, pp. 1–18, 2024, doi: 10.1109/TDSC.2024.3358630.
22. M. Tanveer, A. Aldosary, S. Khokhar, A. K. Das, S. A. Aldossari, and S. A. Chaudhry, “PAF-IoD: PUF-Enabled Authentication Framework for the Internet of Drones,” IEEE Trans Veh Technol, pp. 1–15, 2024, doi: 10.1109/TVT.2024.3365992.
23. Nasution, R. M., “Implementasi Metode Secure Hash Algorithm (SHA-1) Untuk Mendeteksi Orisinalitas File Audio”, BULLETIN OF COMPUTER SCIENCE RESEARCH, vol 2, no 3, pp. 73-84, 2022, doi: 10.47065/bulletincsr.v2i3.140.
24. Al-Layla, H. F., Ibraheem F.N., and Hasan, H. A., “A Review of Hash Function Types and their Applications”, Wasit Journal of Computer and Mathematics Science, vol. 1, no. 3, pp. 75-88, 2022, doi: 10.31185/wjcm.52.
25. Anwar M.R., Apriani, D., and Adianita, I.R., “Hash Algorithm in Verification of Certificate Data Integrity And Security”, Aptisi Transactions on Technopreneurship (ATT), vol. 3, no. 2. pp. 181-188, 2022, doi: 10.34306/att.v3i2.212.
26. Farawn, A.A., Rjeib, H.D., Ali, N.S., and Al-Sadawi, B., “Secured e-payment system based on automated authentication data and iterated salted hash algorithm”, TELKOMNIKA Telecommunication, Computing, Electronics and Control, vol. 18, no. 1, pp. 538-544, 2020, doi: 10.12928/TELKOMNIKA.v18i1.15623.
27. E. Ardhianto, W. Budiharto, Y. Heryadi, and L. A. Wulandhari, “A Comparative Experiment of Document Security Level on Parallel Encryption with Digit Arithmetic of Covertext and Parallel Encryption using Covertext,” in 19th IEEE Student Conference on Research and Development: Sustainable Engineering and Technology towards Industry Revolution, SCOReD 2021, 2021. doi: 10.1109/SCOReD53546.2021.9652746.
28. A. Gutub and B. O. Al-Roithy, “Varying PRNG to improve image cryptography implementation,” Journal of Engineering Research (Kuwait), vol. 9, no. 3, pp. 153–183, Sep. 2021, doi: 10.36909/jer.v9i3A.10111.