A New Lightweight AES for IoT

Liana Qabajeh
Deanship of Graduated Studies
Palestine Polytechnic University
Hebron, Palestine
liana_tamimi@ppu.edu

Radwan Tahboub
Deanship of Graduated Studies
Palestine Polytechnic University
Hebron, Palestine
radwant@ppu.edu

Mohammed AbuJoodeh
Deanship of Graduated Studies
Palestine Polytechnic University
Hebron, Palestine
131089@ppu.edu.ps

Abstract-Internet of Things (IoT) introduces new security algorithms requirements and trends since the algorithms should be lightweight to adapt with IoT devices capabilities. In this paper, we explored the results of security and performance of the AES algorithm by changing AES core parameters and functions including MixColumns operation and number of rounds. In the case of changing MixColumns, the results showed that the security has been adversely affected. While changing the number of rounds provides a promising result to improve the algorithm performance while keeping an acceptable security level which makes it more adaptable to IoT devices. In general, the results showed that running three rounds of standard AES maintains the same level of security practically under specific criteria with a 386% improvement in performance indicators. Accordingly, we proposed a New Lightweight AES (NLW-AES) which maintains the standard AES-MixColumns with three rounds of AES. Finally, we tested both the Standard AES and the New Lightweight AES on Raspberry Pi as an IoT model, and we obtained compatible results with the explored scenarios.

Keywords- IoT, IoT security, Cryptography, AES, Lightweight Cryptography.

I. INTRODUCTION

Our current reality is witnessing an increasing explosion in the development of information systems. The concept of the Internet of Things (IoT) has become very prevalent in our daily lives [1-3].

The security of information is at the forefront of the most important factors for individuals, and from here comes the emphasis on the inability to compromise information security, which includes maintaining the confidentiality of data, integrity, and availability while ensuring the verification, authorization, and accountability [1,2-4].

The confidentiality of information is ensured through cryptography, which is based on encrypting information in various ways.

Cryptography can be categorized as *Symmetric and asymmetric cipher*. In symmetric cipher, the same key is used in the encryption and decryption process, which can be used in the two encryption approaches: *Stream Cipher* and *Block Cipher*. The best-known examples of symmetric cipher are Data Encryption Standard (DES) and Advanced Encryption Standard (AES). In *asymmetric encryption*, two different keys are used. This encryption is known as Public Key cryptography. It is characterized by being better at the level of security, but it requires high resources, the most prominent examples of which are ElGamal, and Rivest-Shamir-Adleman (RSA) [1,2].

Lightweight Cryptography (LWC) can be summarized as the application of traditional security and cryptography concepts, but in an improved manner that ensures its suitability for devices with limited capabilities, such as IoT devices. PRESENT, RECTANGLE, and GIFT are the most common examples of LWC algorithms [1,2-6].

AES is one of the most popular block symmetric encryption algorithms, it provides a very good security level with an acceptable degree of performance [1,2].

The rest of the paper is organized as follows. We provide some researches related to LWC, and AES in section II. Section III discusses the AES explored scenarios in different scenarios regarding changes in its some core parameters. In section IV, we evaluate the proposed explored AES scenarios in the case of their security and performance. Section V summarizes and discusses the results of AES and the explored scenarios and the recommendations and findings are discussed. In section VI, the proposed New Lightweight AES is presented. Finally, we conclude the paper and present a vision for future work in section VII.

II. LITERATURE REVIEW

This section discusses some state-of-the-art researches that are related to the field of LWC and AES.

AbuJoodeh et al. [1], discuss many cryptographies and LWC algorithms with focusing on AES, the study showed that the AES achieved promising results, which opens the way to improve its internal structure for the possibility of its compatibility with the requirements of LWC algorithms that are compatible with the IoT devices.

Hassan et al. [7], the researchers proposed a lightweight stream cipher. This design derives its security strength from the dynamic key. This design is based on simple operations that do not require high capabilities such as XOR and LFSR in resource consumption. The dynamic key of this algorithm is a function of a secret key and nouns. The S-boxes depend on this key, making it more difficult to detect. Based on what the researchers put forward, this algorithm is characterized by

979-8-3503-2006-0/23/$31.00 ©2023 IEEE

low overhead by relying on simple operations and low sequencing, variable cipher primitive that changes after each time, low error propagation, and a simple implementation that does not require large memory.

Khalifa et al. [8], after discussing the challenge resulting from changing objects places, a new method has been proposed to protect the IoT system from address modification attack and heap penetration by encrypting the object during runtime using the ECC besides the cryptographic hash function. The results proved that this method is powerful, effective, and provides a good level of security. The researchers also proposed an authentication system intending to verify devices and collect their behavior dynamically to detect any unusual activity in the system using machine learning algorithms.

Farooq et al. [9] tested AES using different techniques depending on the resources of the target devices, the results were characterized by varying in nature according to the techniques used. Among these techniques are Parallelization and storage of s-box and key expansion. As it has been noted that the introduction of such technologies helps in optimizing the exploitation of resources to provide better results.

Freyre et al [10], provided an understanding of the dynamic AES algorithm, by changing the core AES operations represented by: SubBytes, ShiftRows, MixColumns, and AddRoundKey which were compensated by random key-dependent transformations of RandomSubBytes, RandomShiftRows, RandomMixColumns, RandomAffineTransfKey respectively. The contribution of this study represented by these fundamental changes helps to provide better security with more random properties.

Salim et al. [11] presented the development of an AES algorithm called multi-key AES. The name came concerning the fact that this proposal uses the AES algorithm while using several keys as the secret key is used to configure a variable number of keys using ECC. The study specialized in implementing this algorithm in the IoT, provided that it is used on devices capable of running this algorithm. The results indicated that this modification did not affect the algorithm's performance, but it contributed to improving its security.

Singh et al. [12], tested both a strict crash rate and a bit independence criterion of eight rounds AES algorithm with a dynamic S-Box used to verify that it maintains its security level. The results showed an improvement in the level of performance due to the reduction in the number of rounds, in addition to the improvement in the level of security compared to its reliance on this improved S-Box.

Pan et al [13], proposed a new model for representing AES by introducing some extended operations such as using DRAM, which reduces runtime by providing parallelism between encryption and access to the system. The results indicate a significant improvement in the effectiveness of the algorithm by reducing the encryption time. However, on the contrary, this has increased in energy consumption.

III. Proposed AES EXPLORATION

Based on the time-consuming analysis of the AES algorithm, we found that a large proportion of the time is consumed in the number of rounds and MixColumns operations.

By running AES, we found that MixColumns operation takes about 50% of the running time, while rounds take about 77% of the running time. Therefore, these two factors have been chosen as critical points to be manipulated for the performance improvement to be of good value and noticeable. *Fig. 1* presents the time analysis of the AES algorithm.

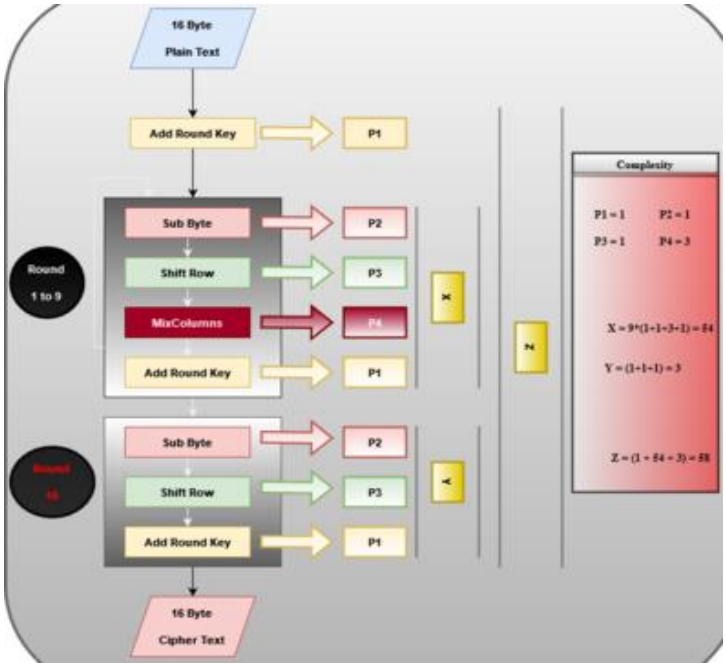

Fig. 1. Time analysis of the AES algorithm

A. Exploration Scenarios

AES explored scenarios focus on changing the number of rounds, MixColumns operation, or both. Hence the following scenarios have been studied:

- 10-Rounds AES with Half MixColumns(10H).
- 10-Rounds AES without MixColumns(10N).
- 5-Rounds AES with Half MixColumns(5H).
- 5-Rounds AES without MixColumns(5N).
- 5-Rounds AES with MixColumns(5F).
- 3-Rounds AES with MixColumns(3F).
- 2-Rounds AES with MixColumns(2F).

The Data proceed as a 4*4 Matrix (M) in each operation. After the ShiftRow operation, each column of the Matrix is multiplied by a fixed matrix in the MixColumn operation to generate a new Matrix (M'). *Fig. 2* presents the process of MixColumn operation.

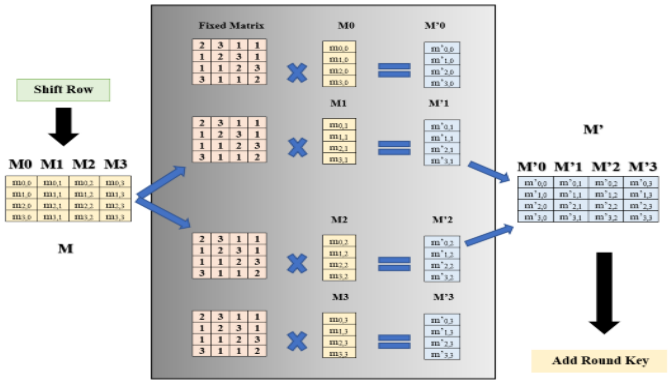

Fig. 2. MixColumn Operation

In Half-MixColumn, we mean that not all M columns will be multiplied by the fixed matrix. Only two columns will proceed in MixColumn operation, and the other two columns will transform to the M' without and changes. We explored all possible possibilities of the chosen column. *Fig. 3* presents the process of Half-MixColumn operation.

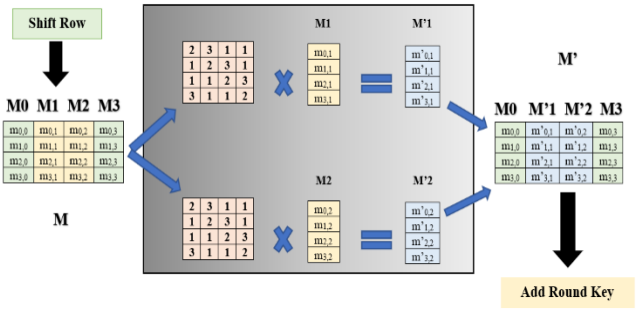

Fig. 3. Half-MixColumn Operation

Without MixColumns means completely eliminating MixColumns, while Half-MixColumns means that the MixColumns are applied only on two columns of ciphertext matrix instead of the four columns.

B. *Evaluation Metrices*

The evaluation process should address performance evaluation and security evaluation to ensure the power of the algorithm. To evaluate *performance*, we will initially need to calculate the following:

- ***Execution Time***: is one of the essential parameters for evaluation performance. It measures the time needed to encrypt and decrypt a specific data size [1-2, 14-15].
- ***Throughput***: it reflects how much data can be processed during a time. It presents the average of data in kb divided by the average Encryption or Decryption time.

As for s*ecurity*, we will initially need to account for:

- ***Key / Time Security:*** the time to attack the algorithm using brute force which is related to key size [1-2, 14-15].
- ***Histogram****:* study the uniformity of data distribution [14-15].
- ***Confusion:*** study the relationship between *ciphertext* and *key*; this relation should be robust. In simple words, the changing of 1-bit in the secret key should lead to a significant change in ciphertext [14-15].
- ***Diffusion:*** study the relationship between *ciphertext* and *plain text*; in simple words, changing a 1-bit in plain text should affect the ciphertext highly [14-15].
- ***NIST Tests****:* These tests attempt to test the randomness of binary sequences produced by an algorithm. These tests focus on different types of non-randomness that could exist in a binary sequence. It was released by the National Institution of Standards and Technology (NIST) as a suite for testing PRNGs that contains 188 tests, including 15 main tests [1-2], [14-15].

IV. EVALUATION AND DISCUSSION

This section deals with evaluating AES and some scenarios along with a brief discussion of this evaluation.

A. *AES Evaluation Summary*

In this section, we summarize the result of testing the standard AES. We define some variable to facilitate the comparison process as follow:

- a, b, Xi: it indicates the size of the data. Where (a) = 155KB, (b) = 31MB, and (x) is the encryption time.
- W: it is a score that takes a value from a specific range.
- In performance, the range from 1 to 8 according to the number of AES versions that are implemented. The values are generated by changing the range to which the values belong in fixed proportions.
- G: the score of each test in the range of W.
- The improvement percentage is calculated by measuring the gain based on the following formula:

$$Gain = \pm \frac{Scenario\ Score - AES\ Score}{AES\ Score} * 100\% \quad (11)$$

  - (+) indicates that we have an improvement in results, while (–) indicates that the results have been drawn back.
- The Security Score in Security Summary for each mode is Calculated based on formula 12:

$$Mode\ Security\ Score = \sum_{Mapping}^{NIST} G \quad (12)$$

- The total Security Score for each Scenario is calculated based on formula 13:

$$Security\ score = \frac{(CBC\&CFB\ score) + ECB\ score + OFB\ score + CTR\ core}{4} \quad (13)$$

Where,

$$CBC\&CFB\ score = \frac{CBC\ score + CFB\ score}{2} \quad (14)$$

TABLE I summarizes the security tests result obtained from this implementation, while *TABLE II* summarizes the performance tests result.

TABLE I. summarizes the security tests results of AES

	W	ECB		G	CBC	G	CFB	G	OFB	G	CTR	G
Mapping	1		uniform	1	uniform	1	uniform	1	uniform	1	uniform	1
Histogram	1		8194.44	0	240.912	1	251.804	1	274.401	1	257.439	1
Correlation	1		0.00155	0	0.00010	1	0.00056	1	0.00050	1	0.00029	1
Confusion	1	a	50.082	1	50.035	1	49.928	1	50.106	1	49.948	1
	1	b	50.008	1	50.003	1	50.005	1	49.999	1	50.003	1
Diffusion	1	a	0.082	0	50.158	1	49.822	1	0.004	0	0.004	0
	1	b	0.00003	0	49.998	1	49.998	1	0.000002	0	0.000002	0
Key Security	1	$2^{128} * \chi_{AES}$										1
NIST	15	13			15		15		15		15	
Security Score	**23**	**17**			**23**		**23**		**21**		**21**	

TABLE II. summarizes the performance tests results of AES

	W	ECB		CBC	CFB	OFB	CTR	G
Enc. Time	8	a	1.136	1.132	1.224	1.374	1.355	1
	8	b	228.899	243.123	246.811	242.619	241.472	1
Dec. Time	8	a	1.321	1.414	1.141	1.054	1.120	1
	8	b	299.262	306.895	242.756	248.475	244.634	1
Enc. Throughput	8	a	1278.240	1063.874	1098.200	1192.912	1132.802	1
	8	b	1134.554	1037.381	1028.120	1051.146	1046.477	1
Dec. Throughput	8	a	987.111	866.452	1091.376	1169.090	1113.619	1
	8	b	885.729	826.893	1038.351	1047.640	1040.165	1
# Of Processes	8	a	32					1
CPU Usage	8	a	16.5%					4
RAM Usage	8	a	1.463					1
Performance Score	**88**	**14**						

After presenting the results of Mapping, Histogram and Chi-Square, Correlation, NIST, Confusion and Diffusion, and Key security test. These results are summarized as follows:

- AES passes the Mapping test in all modes.
- AES passes the Histogram test in all modes except ECB.
- AES passes the Correlation test in all modes except ECB.
- AES passes NIST tests in all modes except ECB.
- AES passes the Confusion test in all modes.
- AES passes the Diffusion test only in CBC /CFB modes.
- AES Key is secure against brute force attack with complexity $\approx \mathbf{2^{128}}$.

B. AES Exploring Results and Discussion

a. 10-Rounds AES with Half MixColumns(10H).

In this section, we implement the AES by modifying the MixColumns to operate on two columns instead of four with the same rounds of Standard AES. Compared to AES, in the case of studying security, we found that:

- In addition to ECB mode, 10H fails in the CTR mode mapping test, while it passes the mapping test in all other modes.
- 10H passes the Histogram test only in CBC and CFB modes.
- Only CBC and CFB pass the correlation test with accepted results.
- 10H passes the confusion test in All modes.
- 10H failed in the diffusion test in all modes.
- Only CBC and CFB modes pass all NIST tests.
- OFB mode has good NIST results.
- 10H maintains the same level of key security compared with AES.

In the case of studying performance, we found that:

- 10H provides better encryption and decryption time with a 44.25% improvement.
- 10H provides better encryption and decryption throughput with a 79.75% improvement.
- 10H requires a smaller number of processes with an 18.75% improvement.
- 10H requires less RAM with a 4.81% improvement but requires 5.74% more CPU.

b. 10-Rounds AES without MixColumns(10N)

In this scenario, we implement the AES by ignoring the MixColumns operation with the same rounds of Standard AES. Compared to AES, in the case of studying security, from we found that:

- In addition to ECB mode, 10N fails in the CTR mode mapping test, while it passes the mapping test in all other modes.
- 10N passes the Histogram test only in CBC and CFB modes.
- Only CBC and CFB pass the correlation test with accepted results.
- 10N passes the confusion test in All modes.
- 10N failed in the diffusion test in all modes.
- Only CBC and CFB modes pass all NIST tests.
- OFB mode has good NIST results.
- 10N maintains the same level of key security compared with AES.

In the case of studying performance, we found that:

- 10N provides better encryption and decryption time with a 22% improvement.
- 10N provides better encryption and decryption throughput with a 28% improvement.
- 10N requires a smaller number of processes with a 34.38% improvement.
- 10N requires less CPU and RAM usage with a 0.69% and 6.46% improvement, respectively.

c. 5-Rounds AES with Half MixColumns(5H)

In this section, we implement the AES by modifying the MixColumns to operate on two columns instead of four with five rounds of Standard AES. Compared to AES, in the case of studying security, we found that:

- In addition to ECB mode, 5H fails in the CTR mode mapping test, while it passes the mapping test in all other modes.
- 5H passes the Histogram test only in CBC and CFB modes.
- Only ECB and CTR modes failed in the correlation test.
- 5H passes the confusion test in All modes.
- 5H failed in the diffusion test in all modes.
- Only CBC and CFB modes pass all NIST tests.
- 5H maintains the same level of key security compared with AES.

In the case of studying performance, we found that:

- 5H provides better encryption and decryption time with a 60.25% improvement.

- 5H provides better encryption and decryption throughput with a 155% improvement.
- 5H requires a smaller number of processes with a 46.88% improvement.
- 5H requires less CPU and RAM usage with a 3.13% and 1.34% improvement, respectively.

d. 5-Rounds AES without MixColumns(5N)

In this section, we implement the AES by ignoring the MixColumns operation with five rounds of Standard AES. Compared to AES, in the case of studying security, we found that:

- In addition to ECB mode, 5N fails in the CTR mode mapping test, while it passes the mapping test in all other modes.
- 5N passes the Histogram test only in CBC and CFB modes.
- Only CBC and CFB pass the correlation test with accepted results.
- All modes except ECB pass the confusion test.
- 5N failed in the diffusion test in all modes.
- Only CBC and CFB modes pass all NIST tests.
- OFB mode has good NIST results.
- 5N maintains the same level of key security compared with AES.

In the case of studying performance, we found that:

- 5N provides better encryption and decryption time with a 68.5% improvement.
- 5N provides better encryption and decryption throughput with a 226% improvement.
- 5N requires a smaller number of processes with a 46.88% improvement.
- 5N requires less CPU and RAM usage with a 3.05% and 2.45% improvement, respectively.

e. 5-Rounds AES with MixColumns(5F)

In this section, we implement the AES by using five rounds of Standard AES. Compared to AES, in the case of studying security, we found that:

- 5F maintains the same level of security compared with AES **practically under specific criteria**.
- In the case of studying performance, we found that:
- 5F provides better encryption and decryption time with a 50.5% improvement.
- 5F provides better encryption and decryption throughput with a 103.25% improvement.
- 5F requires a smaller number of processes with a 37.5% improvement.
- 5F requires less RAM with a 1.22% improvement but requires 4.04% more CPU.
- 5F has a 207% improvement in performance compared with AES.

f. 3-Rounds AES with MixColumns(3F)

In this section, we implement the AES by using three rounds of Standard AES. Compared to AES, in the case of studying security, we found that:

- 3F maintains the same level of security compared with AES practically under specific criteria.

In the case of studying performance, we found that:

- 3F provides better encryption and decryption time with a 69.25% improvement.
- 3F provides better encryption and decryption throughput with a 224% improvement.
- 3F requires a smaller number of processes with a 50% improvement.
- 3F requires less CPU and RAM usage with a 4.2% and 2.54% improvement, respectively.
- 3F has a 386% improvement in performance compared with AES.

g. 2-Rounds AES with MixColumns(2F)

In this section, we implement the AES by using two rounds of Standard AES. Compared to AES, in the case of studying security, we found that:

- 2F fails in the CTR mode mapping test, while it passes the mapping test in all other modes.
- In addition to ECB mode, 2F fails in the CTR mode histogram test, while it passes the histogram test in all other modes.
- In addition to ECB mode, 2F fails in the CTR mode correlation test, while it passes the correlation test in all other modes.
- ECB and CTR modes failed in the confusion test.
- 2F failed in the diffusion test in all modes.
- CBC, CFB, and OFB modes pass all NIST tests.
- 2F maintains the same level of key security compared with AES.

In the case of studying performance, we found that:

- 2F provides better encryption and decryption time with a 78.5% improvement.
- 2F provides better encryption and decryption throughput with a 357.5% improvement.
- 2F requires a smaller number of processes with a 62.5% improvement.
- 2F requires less CPU and RAM usage with a 9% and 3.34% improvement, respectively.
- 2F has a 507% improvement in performance compared with AES.

V. AES Exploring Results Summary

In this section, we present a brief summary of the results of the explored scenarios and scientifically discuss these results. *Table III* summarizes the results scientifically and mathematically to facilitate the process of extrapolating recommendations and can be summarized as follow:

- The ECB mode fails in most security tests due to the way of data handling in the encryption process. Since each block in plaintext is isolated from other blocks, that means each block in plaintext has an identical block in the cipher.

TABLE III. AES Exploring Results Summary

	AES	10H	10N	5H	5N	5F	3F	2F
Key Security	Pass	No changes						
NIST	Pass	Moderate	Fail	Moderate	Fail	No Changes		
Diffusion	Pass	Fail				No Changes		
Confusion	Pass	Acceptable				No Changes		Acceptable
Correlation	Pass	Moderate	Fail	Moderate	Fail	No Changes		
Histogram	Pass	Moderate	Fail	Moderate	Fail	No Changes		
Mapping	Pass	Moderate	Fail	Moderate	Fail	No Changes		
Dec. Throughput	Good	+89 %	31 %	+158.5 %	+242.5 %	+105.5 %	+228 %	+374.5 %
Enc. Throughput	Good	+70.5%	25%	+151.5 %	+209.5 %	+101%	+220 %	+340.5%
Dec. Time	Good	+47.5 %	24.5%	+61 %	+70 %	+51%	+69.5 %	+79.5 %
Enc. Time	Good	+41 %	+19.5%	+59.5 %	+67%	+50%	+69%	+77.5%
Security Score	20.5	17.25	15.5	12.375	13.875	20.5	20.5	15.5
Performance Score	14	29	47	55	65	37	68	85

- CBC and CFB modes are the best modes to be used during their results in security tests.
- MixColumn operation improves the security of the algorithm, especially in Diffusion. Since it provides dynamic changes to the results.
- 10H has a 24% loss in security compared with AES. While it provides a 93% improvement in performance.
- 10N has a 40% loss in security compared with AES. While it has a 220% improvement in performance.
- 5H has a 38% loss in security compared with AES. While it provides a 28% improvement in performance with AES.
- 5N has a 32% loss in security compared with AES. While it has a 347% improvement in performance.
- 5F maintains the same level of security, practically under specific criteria, compared with AES and provides a 147% improvement in performance with AES.
- 3F maintains the same level of security compared with AES, practically under specific criteria, and provides a 386% improvement in performance compared with AES.
- 2F has a 24% loss in security compared with AES. While it has a 467% improvement in performance compared with AES.

In this section, we discussed the results of AES, 10H, 10N, 5H, 5N, 5F, 3F, and 2F scenarios in terms of performance and security. While 3F provides the best performance scenarios for maintaining the level of security practically, *TABLE IV* summarizes the security test results obtained from this implementation, and *TABLE V* summarizes the performance tests result.

TABLE IV. summarizes the security tests results of 3F scenario

	W	ECB		G	CBC	G	CFB	G	OFB	G	CTR	G
Mapping	1		Uniform	1	uniform	1	uniform	1	uniform	1	uniform	1
Histogram	1		63946	0	256.531	1	256.922	1	247.026	1	253.986	1
Correlation	1		-0.00262	0	0.00002	1	-0.0005	1	-0.0007	1	0.00017	1
Confusion	1	a	50.081	1	50.034	1	49.955	1	49.995	1	50.190	1
	1	b	50.044	1	50.000	1	49.991	1	50.003	1	50.168	1
Diffusion	1	a	0.0082	0	50.0186	1	50.0037	1	0.00024	0	0.00024	0
	1	b	0.000160	0	50.0185	1	49.9925	1	0.000005	0	0.000005	0
Key Security	1	$2^{128} * x_{AES}$										1
NIST	15	13			15		15		15		15	
Security Score	**23**	**17**			**23**		**23**		**21**		**21**	

TABLE V. summarizes the performance tests results of 3F scenario

	W	ECB		CBC	CFB	OFB	CTR	G
Enc. Time	8	a	0.312	0.322	0.326	0.381	0.342	7
	8	b	70.500	74.601	75.950	75.309	79.786	7
Dec. Time	8	a	0.364	0.382	0.365	0.417	0.350	7
	8	b	84.030	89.429	75.789	76.506	78.163	7
Enc. Throughput	8	a	4121.117	3812.127	3830.001	3232.544	3603.957	6
	8	b	3713.571	3245.844	3278.260	3418.138	3160.745	5
Dec. Throughput	8	a	3490.198	3246.598	3700.335	3139.058	3495.501	6
	8	b	3098.007	2762.357	3382.161	3421.635	3236.305	6
# Of Processes	8	a	16					7
CPU Usage	8	a	15.81%					6
RAM Usage	8	a	1.426					4
Performance Score	88		68					

Due to the results of the 3F scenario, which outperformed other scenarios, we have conducted new tests, *TABLE VI* compares it with AES in terms of Average Power Consumption (APC). While *TABLE VII* compares it with AES in terms of UACI and NPCR tests.

TABLE VI. APC

	AES	3F	Gain
Average Power consumption (Watt)	13.31	12.446	6%

From *TABLE VI*, we found that 3F provides better APC with a 6% improvement.

Unified Averaged Changed Intensity (UACI) and Number of Pixel Change Rate (NPCR) represent two important criteria in studying this change, which study the change in the encrypted image when changing one pixel in the original image. NPCR measures the percentage of different pixels. UACI measures the average intensity of the difference between the two encoded images.

TABLE VII. UACI and NPCR for 512 × 512 Lena image

	AES	3F	Similarity
UACI	33.465	33.477	Almost, a perfect match in the results
NPCR	99.609	99.612	

From *TABLE VII*, we found that AES has good UACI and NCPR values, since the changing of 1 pixel has infected the entire image, and hence the encryption algorithm has a good avalanche effect, so the algorithm is resistant against differential attack.

- There is no real change between AES and 3F in UACI and NPCR results. In other words, 3F maintains the same level of UACI and NPCR practically.

Furthermore, we implemented this scenario and tested it on Raspberry Pi (RP) as a working model on IoT devices. Where the results were as follows:

Compared to AES on RP, in the case of studying performance, we found that:

- 3F provides better encryption and decryption time with a 67.5% improvement.
- 3F provides better encryption and decryption throughput with a 213.5% improvement.
  - These two results are relatively consistent with the results that have been shown *in section IV. B. f.*
- 3F has a 100% improvement in performance with AES. The change in total improvement occurred because not all factors were taken into account in the calculation.
- 3F has a better APC on RP with a 7.38% improvement.

VI. A New Lightweight AES

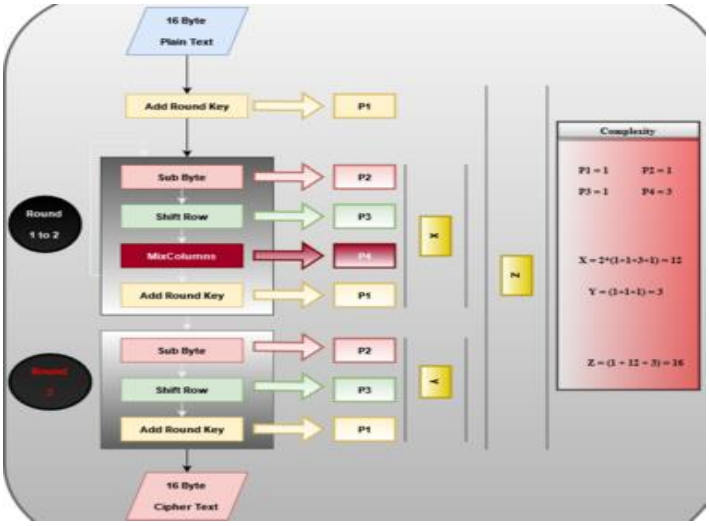

Fig. 4. NLW-AES Time Analysis

Based on the result and comparison that have been done in section 5, we found:

- The results indicate that running three rounds of AES at least is sufficient to maintain the level of security and that this algorithm optimization achieves a significant performance advantage by 386%.
- The standard AES algorithm loses some security level when run at one or two rounds due to the lack of changes to the original text during encryption. Thus, it is important to devise a mechanism to complicate and increase this effect, provided it does not require a lot of time.

- AES loses more security when reducing the MixColumns operation. AES loses much more security when ignoring the MixColumns operation.
- *Fig. 4* presents the time analysis of the NLW-AES which mathematically show that it provides a 72.4% improvement in the encryption time based on equation 11. Which is consistent with the results obtained practically.

Based on the results, we choose 3F as the New Lightweight AES Algorithm (NLW-AES),

VII. CONCLUSIONS

In this paper, we presented the results of testing the AES algorithm according to the specified criteria. We have undertaken an extensive exploration of a set of AES scenarios to study their results. These scenarios are generated by changing some AES core parameters such as the change in the number of rounds and in the MixColumns operation.

The results of the explored scenarios testing process varied in terms of performance enhancement along with decreasing the level of security, or improving performance while maintaining the same level of security. We found that the change in the MixColumns operation led to a significant decline in the level of security, while the change in the number of rounds preserved the core function of AES maintaining the same level of security considering three to ten rounds practically. Upon testing two rounds and one round of AES, the level of security has declined significantly.

Based on the need of maintaining the level of security, the explored scenarios have been limited to 5F and 3F. These two scenarios maintain the same level of security as AES practically under specific criteria with different performance levels. Finally, through a detailed comparison process based on the level of performance, we found that the results showed that running three rounds of standard AES lead us to propose the NLW-AES which maintains the same level of security as AES practically under specific criteria with a 386% improvement in performance.

Upon our exploration and depending on the conducted experiments and results, we can say that "NLW-AES is a suitable choice for securing real-time IoT applications".

Future Work

In light of the obtained promising results and confirming the consequences of what was discussed in the previous studies, our next step is to work on improving the AES algorithm security when run over one or two rounds by combining AES with another lightweight operation to compensate for the level of security and increase the effectiveness of the one and two rounds on the text being processed. One of the suggested enhancements that should be taken into account, is to replace the S-Box with a more efficient one. Furthermore, we should look if there are any other security tests that can be studied to evaluate AES and the NLW-AES in terms of security. Also, the attacks such as Meet-in-the-Middle-attack, and Quantum attack should be applied on AES and NLW-AES to compare the effect of reducing the number of rounds from ten to three. Finally, we recommend a new work including the study of a complete security system based on NLW-AES with suitable hashing, and digital signature algorithms.

REFERENCES

[1] M. Abujoodeh, L. Tamimi, and R. Tahboub. "Exploring and Adapting AES Algorithm for Optimal Use as a Lightweight IoT Crypto Algorithm, 2022. [Master Thesis, Palestine Polytechnic University].Available:https://scholar.ppu.edu/handle/123456789/8635.

[2] M. Abujoodeh, L. Tamimi, and R. Tahboub, 'Toward Lightweight Cryptography: A Survey', Computational Semantics. IntechOpen, Jan. 05, 2023. doi: 10.5772/intechopen.109334.

[3] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson. "The industrial internet of things (IIoT): An analysis framework. Computers in industry", Computers in Industry, vol. 101, pp.1-12, 2018.

[4] H. Mohammed, A, Al-adhami, Y. Yaseen, and L. Abed, "A Developed Cryptographic Model Based on AES Cryptosystem". In AIP Conference Proceedings 31 October 2022; 2400 (1): 020013, Anbar, Iraq. 2022. https://doi.org/10.1063/5.0112123.

[5] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks", Journal of Information Security and Applications, vol. 38, pp.8-27, 2022.

[6] P. Krishnakumar, "Lightweight Cryptography and its Algorithms in Internet of Things: An Overview", International Journal of Innovative Research in Science Engineering and Technology. vol. 10, pp.4900-4904, 2021.

[7] N. Hassan, C. Raphaël, P. Congduc, and C. Ali, "Lightweight Stream Cipher Scheme for Resource-Constrained IoT Devices", in 15th IEEE WiMob 2019At conf, Barcelona, Spain, 2019.

[8] M. Khalifa, F. Algarni, M. Khan, A. Ullah, and K. Aloufi, "A lightweight cryptography (LWC) framework to secure memory heap in Internet of Things", Alexandria Engineering Journal, vol. 60, pp. 1489-1497, 2020.

[9] U. Farooq, and F. Aslam, "Comparative analysis of different AES implementation techniques for efficient resource usage and better performance of an FPGA", Journal of King Saud University - Computer and Information Sciences, vol. 29, pp. 295-302, 2017.

[10] P. Freyre, O. Cuellar, N. Díaz, and A. Alfonso, "From AES to Dynamic AES", Journal of Science and Technology on Information security, vol. 1, pp. 11-22, 2020.

[11] K. Salim, S. Alalak, and M. Jawad, "Improved Image Security in Internet of Thing (IoT) Using Multiple Key AES", *Baghdad Science Journal*, vol. 18, pp. 417-429, 2021.

[12] A. Singh," Comparative Analysis of Reduced Round Dynamic AES with Standard AES Algorithm", *International Journal of Computer Applications*, vol. 183, pp. 41-49, 2021.

[13] L. Pan, G. Tu, S. Liu, Z. Cai, and X. Xiong, "A Lightweight AES Coprocessor Based on RISC-V Custom Instructions", *Security and Communication Networks*, vol. 2021, pp.1-13, 2.

[14] O. Salhab, N. Jweihan, M. abuJoodeh, M. Abutaha and M. Farajallah "Survey paper: Pseudo-random number generators and security tests", Journal of Theoretical and Applied Information Technology. vol.96, pp. 1951-1970, 2018.

[15] M. Farajallah, M. Abutaha, M. Abujoodeh, O. Salhab and N. Jweihan, "PSEUDO-RANDOM NUMBER GENERATOR BASED ON LOOK-UP TABLE AND CHAOTIC MAPS", Journal of Theoretical and Applied Information Technology, Vol 98. 3130, 2020.