MULTI-SHAPE SYMMETRIC ENCRYPTION MECHANISM FOR NON-GENERIC ATTACKS MITIGATION

ABDELRAHMAN ABDELGADER ALTIGANI ABDELGADER

UNIVERSITI TEKNOLOGI MALAYSIA

MULTI-SHAPE SYMMETRIC ENCRYPTION MECHANISM FOR NON-GENERIC ATTACKS MITIGATION

ABDELRAHMAN ABDELGADER ALTIGANI ABDELGADER

A thesis submitted in fulfilment of the
requirements for the award of the degree of
Doctor of Philosophy

School of Computing
Faculty of Engineering
Universiti Teknologi Malaysia

JULY 2022

ACKNOWLEDGEMENT

First and foremost, “Alhamdulillah”. I also wish to thank my wonderful wife, Shiraz, for her endless love and support. Special thanks to my supervisors Dr Shafaatunnur binti Hassan and Assoc. Prof. Dr Bazara Barry, for their patience, guidance and support. Furthermore, I would like to express my deepest appreciation to my friends Dr Abubakar Elsafi, Dr Akram Osman, Dr Ahmed Elkhateeb, Dr Samah Gubara and all those who supported me in one way or another. Last but not least, I wish to express my appreciation to Prof Dr Siti Mariyam Shamsuddin and pray for our mighty Allah to have mercy upon her soul.

ABSTRACT

Static cyphers use static transformations for encryption and decryption. Therefore, the attacker will have some knowledge that can be exploited to construct assaults since the transformations are static. The class of attacks which target a specific cypher design are called Non-Generic Attacks. Whereby, dynamic cyphers can be utilised to mitigate non-generic attacks. Dynamic cyphers aim at mitigating non-generic attacks by changing how the cyphers work according to the value of the encryption key. However, existing dynamic cyphers either degrade the performance or decrease the cypher's actual security. Hence, this thesis introduces a Multi-Shape Symmetric Encryption Mechanism (MSSEM) which is capable of mitigating non-generic attacks by eliminating the opponents' leverage of accessing the exact operation details. The base cyphers that have been applied in the proposed MSSEM are the Advanced Encryption Standard (AES) competition finalists, namely Rijndael, Serpent, MARS, Twofish, and RC6. These cyphers satisfy three essential criteria, such as security, performance, and expert input. Moreover, the modes of operation used by the MSSEM are the secure modes suggested by the National Institute of Standards and Technology, namely, *Cipher Block Chaining (CBC), Cipher Feedback Mode (CFB), Output Feedback Mode (OFB),* and *Counter (CTR)*. For the proposed MSSEM implementation, the sender initially generates a random key using a pseudorandom number generator such as Blum Blum Shub (BBS) or a Linear Congruential Generator (LCG). Subsequently, the sender securely shares the key with the legitimate receiver. Besides that, the proposed MSSEM has an entity called the operation table that includes sixty different cypher suites. Each cypher suite has a specific cypher and mode of operation. During the run-time, one cypher suite is randomly selected from the operation table, and a new key is extracted from the master key with the assistance of SHA-256. The suite, as well as the new key, is allowed to encrypt one message. While each of the messages produces a new key and cypher suite. Thus, no one except communicating parties can access the encryption keys or the cypher suites. Furthermore, the security of MSSEM has been evaluated and mathematically proven to resist known and unknown attacks. As a result, the proposed MSSEM successfully mitigates unknown non-generic attacks by a factor of 2^{-6}. In addition, the proposed MSSEM performance is better than MODEM since MODEM generates 4650 milliseconds to encrypt approximately 1000 bytes, whereas MSSEM needs only 0.14 milliseconds. Finally, a banking system simulation has been tested with the proposed MSSEM in order to secure inbound and outbound system traffic.

ABSTRAK

Sifer statik menggunakan transformasi statik untuk penyulitan dan penyahsulitan. Olehitu, penyerang akan mempunyai beberapa pengetahuan yang boleh dieksploitasi untuk membina serangan kerana transformasi adalah statik. Kelas serangan yang menyasarkan reka bentuk sifer tertentu dipanggil Serangan Bukan Generik. Di mana, sifer dinamik boleh digunakan untuk mengurangkan serangan bukan generik. Sifer dinamik bertujuan untuk mengurangkan serangan bukan generik dengan menukar cara sifer berfungsi mengikut nilai kunci penyulitan. Walau bagaimanapun, sifer dinamik sedia ada sama ada merendahkan prestasi atau mengurangkan keselamatan sebenar sifer. Oleh itu, kajian ini memperkenalkan Mekanisme Penyulitan Simetri Pelbagai Bentuk (MSSEM) yang mampu mengurangkan serangan bukan generik dengan menghapuskan pengaruh pihak lawan untuk mengakses butiran operasi yang tepat. Sifer asas yang telah diaplikasikan dalam MSSEM yang dicadangkan ialah finalis pertandingan *Advanced Encryption Standard* (AES) iaitu Rijndael, Serpent, MARS, Twofish, dan RC6. Sifer ini memenuhi tiga kriteria penting, iaitu keselamatan,prestasi dan input pakar. Selain itu, mod operasi yang digunakan oleh MSSEM adalah mod selamat yang dicadangkan oleh Institut Piawaian dan Teknologi Kebangsaan, iaitu, *Cipher Block Chaining* (CBC), *Cipher Feedback Mode* (CFB), *Output Feedback Mode* (OFB), dan *Counter* (CTR). Bagi pelaksanaan MSSEM yang dicadangkan, pengirim pada awalnya menjana kunci rawak menggunakan penjana nombor rawak seperti *Blum Blum Shub* (BBS) atau *Linear Congruential Generator* (LCG). Selepas itu, pengirim dengan selamat berkongsi kunci dengan penerima yang sah. Selain itu, MSSEM yang dicadangkan mempunyai entiti yang dipanggil jadual operasi yang merangkumi enam puluh sut sifer yang berbeza. Setiap sut sifer mempunyai sifer dan mod operasi tertentu. Semasa masa jalanan dilaksanakan, satu sut sifer dipilih secara rawak daripada jadual operasi, dan kunci baharu diekstrak daripada kunci induk dengan bantuan SHA-256. Sut, serta kunci baharu dibenarkan untuk menyulitkan satu mesej. Manakala, setiap mesej menghasilkan sut kunci dan sifer baharu. Oleh itu, tiadasesiapa kecuali pihak yang berkomunikasi boleh mengakses kunci penyulitan atau sut sifer. Tambahan pula, keselamatan MSSEM telah dinilai dan terbukti secara matematik untukmenentang serangan yang diketahui dan tidak diketahui. Hasilnya, MSSEM yang dicadangkan berjaya mengurangkan serangan bukan generik yang tidak diketahui dengan faktor 2^{-6}. Di samping itu, prestasi MSSEM yang dicadangkan adalah lebih baik daripada MODEM kerana MODEM menjana 4650 milisaat untuk menyulitkan kira-kira 1000 bait, manakala MSSEM hanya memerlukan 0.14 milisaat. Akhir sekali, simulasi sistem perbankan telah diuji dengan MSSEM yang dicadangkan untuk mendapatkan sistem trafik masuk dan keluar yang selamat.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AES	-	Advanced Encryption Standard
API	-	Application Programming Interface
ASCII	-	American Standard Code for Information Interchange
BBS	-	Blum Blum Shub
CBC	-	Cypher block chaining
CFB	-	Cypher feedback
CI	-	Confidence Interval
CTR	-	Counter
DDBM	-	Dynamic Data Blocking Mechanism
DEA	-	Data Encryption Algorithm
DES	-	Data Encryption Standard
DK	-	Dynamic Key
DNA	-	DeoxyriboNucleic Acid structure
DS	-	Dataset
ECB	-	Electronic Codebook
FBI	-	Federal Bureau of Investigation
FPGA	-	Field-Programmable Gate Array
ICT	-	Information and Communication Technology
IP	-	Initial Permutation
IV	-	Initialisation Vector
LCG	-	Linear Congruential Generator
MDS	-	Maximum Distance Separable
MODEM	-	Multi Operation Data Encryption Mechanism
MSSEM	-	Multi-Shape Symmetric Encryption Mechanism
NIST	-	National Institute for Standards and Technology
NSA	-	National Security Agency
OFB	-	Output feedback
OP-CODE	-	Operation Code
OTP	-	One Time Pad

PHT	-	Pseudo–Hadamard Transform
PRNG	-	Pseudorandom Number Generator
PT	-	Plaintext
RSM	-	Randomised Substitution Mechanism
SAC	-	Strict Avalanche Criterion
SHA	-	Secure Hash Algorithm
SK	-	Session Key
SSL	-	Secure Sockets Layer
STS	-	Statistical Test Suite
TID	-	Tailoring ID
TRNG	-	True Random Numbers Generator

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

Information and Communication Technology (ICT) has significantly changed our lives in almost all respects. Many systems have been computerised to promote the quality of services and to increase convenience for customers, businesses owners, and employees. However, when providing a service electronically, adequate security should be in place, or it will jeopardise all involved parties. For instance, a press report had been published by the Federal Bureau of Investigation (FBI) stating that the total amount of losses inside the United States due to cybercrimes is estimated at 6.9 billion U.S. Dollars only in 2021 (FBI, 2022).

To counter a wide range of cybercrimes, cryptographic techniques such as asymmetric encryption algorithms, symmetric encryption algorithms as well as hashing and MACing algorithms are usually used to maintain the *Confidentiality*, *Integrity* and *Authenticity*, *Non-Repudiation*, and *Access Control* of the data (Abomhara *et al.*, 2011; Bhattarai and Wang, 2018; Park *et al.*, 2021; Utakrit and Utakrit, 2021).

The *confidentiality* security service is typically achieved using encryption algorithms. Encryption algorithms can be classified into *symmetric* and *asymmetric* algorithms. The *symmetric* encryption algorithm uses the same key for encrypting (i.e. encoding) and decrypting (i.e. decoding) the secret data (Abomhara *et al.*, 2022). In symmetric encryption, there is a need to share the secret key between communicating parties securely. Sharing the secret key or key exchange is the main limitation of using symmetric encryption (Baldi *et al.*, 2019; Carlson, 2019).

Asymmetric encryption algorithms overcome the key exchange problem by proposing two keys per user, a *public key* and a *private key*. The public key for any user (e.g. Alice) is typically accessible by any other user (e.g. Bob). However, the corresponding private key is only accessible to the key owner (i.e. Alice). If any data is encrypted using Alice's public key, no one except the corresponding private key holder (i.e. Alice) can decrypt the data.

Asymmetric encryption algorithms resolved the key exchange problem. Nevertheless, its performance is lower compared to symmetric algorithms. The cypher performance refers to the encryption and decryption speed (Gnatyuk *et al.*, 2018; Yuan *et al.*, 2018). Asymmetric cyphers' performance is generally low because they depend on time-consuming mathematical operations to carry the encryption and decryption. As an example, to retrieve the plaintext *P* from the cyphertext *C* using the RSA, the following equation is used:

$$P = C^d \ mod \ n \tag{1.1}$$

where both *d* and *n* are large integers. Modular exponentiation is an inherently time-consuming operation, which decreases the performance of the RSA, as well as many other asymmetric cyphers (Bajpai and Enbody, 2020; Fathy *et al.*, 2018). In general, asymmetric cyphers can be 1000 times slower than symmetric cyphers (de Ree *et al.*, 2021; Haque *et al.*, 2018; Thapar and Sarangal, 2018).

Nonetheless, asymmetric encryption algorithms are widely used in applications such as email security, web security and other applications which require a key exchange. In general, *symmetric* and *asymmetric* encryption algorithms are integrated, where the message content (i.e. payload) is encrypted using a symmetric cypher, and the symmetric key used for encrypting the payload is shared after being encrypted using an asymmetric cypher (Alwazzeh *et al.*, 2020; Devarakonda Krishna and Krishna; Schillinger and Schindelhauer, 2020).

Encryption algorithms were previously considered a national security asset. No one except the sender and the legitimate receiver, in addition to a few other trusted

experts, has complete knowledge about how it works. This convention has been widely abandoned, and the current dominant trend in cryptology is to use standard encryption algorithms that use known transformations. This property was introduced by Auguste Kerckhoffs, who stated that the cryptosystem should remain secure even if it has fallen into the enemy's hands (Ergün and Acar, 2020). Since then, this property has gained a significant consensus among cryptographers. Although Kerckhoffs did not state that the encryption algorithm must be disclosed, standardisation bodies like the National Institute for Standards and Technology (NIST) urge the use of standard (i.e. known) encryption algorithms. The intuitive justification is to maximise interoperability and to expose the algorithm for testing by experts from all over the world. Hence, interoperability is the ability to exchange information between two different systems (Khisro, 2020; Vandana and BJ, 2020). In other words, it means the ability to exchange encrypted messages between different systems.

1.2 Problem Background

Symmetric cyphers are in wide use (Nurgaliyev and Wang, 2021; Xu and Tian, 2019). This is due to two main reasons. The first reason is that symmetric cyphers provide high performance compared to asymmetric cyphers. The second reason is that well-known symmetric cyphers are hard to break (i.e. secure) when the encryption key has a sufficiently large size (Abomhara *et al.*, 2010). For these reasons, many systems and applications use symmetric cyphers to provide the confidentiality security service. This includes sensitive systems such as banking systems (Islam *et al.*, 2021). For these reasons, this thesis focuses on symmetric encryption.

Strong encryption is needed in almost all electronic transactions. Nonetheless, the confidentiality of the transactions related to financial applications has especial importance. This is because end users are generally sceptical of using the technology when the transaction involves some sort of payment unless they can fully trust it (Akinbowale *et al.*, 2020; De Kimpe *et al.*, 2020). Assuring the users that strong encryption is used will assist in gaining their confidence and trust (Akinyede and Esese, 2017).

According to Pupezescu *et al.* (2017), in banking systems, it is important to use well-known encryption algorithms to provide the confidentiality security service. This is because banking systems are extremely sensitive systems that cannot tolerate the use of new cyphers which have not been rigorously tested. Furthermore, financial institutions process large volumes of data daily. Therefore, there is a need to use a high-performance cypher to maximise resources utilisation (Ammari and Lu, 2017).

In the last five decades, standard *symmetric* encryption algorithms such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) have been widely used to provide the confidentiality security service. Both the DES and the AES are *static* cyphers. This means they use the same known transformations to encrypt or decrypt a given message (Cardona, 2019; Jose and George, 2019). Since everyone knows the exact transformations used by the cypher to encrypt or decrypt any given message, they can be vulnerable to future attacks that target their fixed structure (Couturier *et al.*, 2020; Noura *et al.*, 2018; Noura *et al.*, 2020a; Noura *et al.*, 2020b).

Several attacks have been designed to penetrate the AES or a simplified version of the AES (Bar-On *et al.*, 2020; Bardeh and Rønjom, 2019; Grassi *et al.*, 2017; Kakarla *et al.*, 2017; Zhao *et al.*, 2017). Although these attempts are still considered impractical, they have achieved a partial success. These attacks are discussed in further detail in section 2.8. It is worth mentioning that the common factor among all these attacks is that it is designed solely to target a specific static cypher design. The algorithm which has a static behaviour lends the potential attacker a starting point to design and launch attacks since the steps used for encryption are always the same (Couturier *et al.*, 2020; Noura *et al.*, 2020a; Noura *et al.*, 2020b). The attacks which target a specific static cypher design are called “Non-Generic Attacks” (Sehrawat and Gill, 2018).

There are several cyphers’ designs that aim at resisting non-generic attacks. Such cyphers are called dynamic cyphers (Tang *et al.*, 2018). The common design philosophy of dynamic cyphers is to change the static nature of the cypher into a dynamic one. This means the encryption transformations used by the dynamic cypher

will change according to the encryption key value. In other words, the dynamic cypher has several variants, and the attacker will not be certain which variant is used for encrypting a given message. This technique makes the dynamic cypher capable of mitigating the efficacy of non-generic attacks.

To use a dynamic cypher, it is essential to ensure that all the variants of the dynamic cypher are capable of resisting known attacks. This includes brute force, linear cryptanalysis, differential cryptanalysis, related key, timing, and side-channel attacks. *Brute force* is the simplest attack that aims at penetrating the cypher by trying all possible values of the encryption key. *Linear Attacks* work by tracking the parity of the bits between the input and the output. Linear attacks can be effective if the bias of a specific parity between the input and the output is significantly high. *Differential Attacks* work by passing pairs of chosen inputs to the cypher. The chosen inputs must have a constant *difference*. The differential attacks can be effective in a given cypher if there is a high probability that a constant input difference will lead to a constant output difference. *Related-key attacks* are a class of cryptanalysis in which the attacker can monitor the operation of the encryption algorithm under various keys whose values are unknown, but there is a mathematical relationship that connects these keys. Moreover, it is assumed that the mathematical relationship is known to the attacker. *Side-channel attacks* are a non-invasive form of attack that aims at revealing the secret key of a given cypher by analysing the leaked physical information (Gui *et al.*, 2020). *Timing attacks* aim at deducing information about the plaintext or the key using the time elapsed for encryption or decryption (Liu *et al.*, 2021b). Timing attacks are a common example of side-channel attacks.

In addition, two other security requirements should be satisfied by all the variants of the dynamic cypher. These requirements are the output randomness and the cypher's avalanche. The output randomness means that the cypher output is statistically indistinguishable from truly random data. This can be tested using the Statistical Test Suite (STS) suggested by the National Institute of Standards and Technology (NIST). The other requirement is the cypher's avalanche. This means a small change in the cypher input will lead to a large and unpredictable change in the cypher output.

Moreover, the cypher performance is a critical requirement too. In the context of this thesis, cypher performance refers to the encryption and decryption speed (Gnatyuk *et al.*, 2018; Yuan *et al.*, 2018). Ideally, systems' users should not experience any sluggishness in fulfilling their tasks when applying the encryption. Encryption algorithms with poor performance will be abandoned regardless of what good security they provide.

There are several examples of dynamic cyphers in the literature. For instance, in the designs suggested by Bhavani *et al.* (2019), Chauhan and Sasamal (2019), and Rahaman *et al.* (2020), the SubBytes transformation in the AES has been manipulated. This means the S-Box entries values will depend on the encryption key value.

It can be argued that there is no practical technique to investigate the avalanche criterion and the output randomness for all AES variants with key-dependent S-Boxes. Moreover, a related-key attack that has a complexity of 2^{96} has been devised on the AES key scheduler using 2^{35} related keys (Biryukov *et al.*, 2009). Furthermore, no special arrangements have been used to immune the cypher against zero-day attacks, timing attacks and other side-channel attacks. Another concern is that the technique used to manipulate the S-Box may introduce significant performance degradation. For instance, in (Malik *et al.*, 2020), it has been suggested to use chaotic maps to dynamise the S-Box. Nevertheless, chaotic maps are known for increasing the time complexity (Akhavan *et al.*, 2017).

Another dynamic encryption approach is based on DES and matrices multiplication. In this model, the plaintext x is initially multiplied in a binary invertible matrix k_a. Consequently, the DES cypher is invoked to encrypt the output of the latter phase. The outcome of the DES encryption is multiplied in another binary invertible matrix k_c. The details of generating k_a, k_c, as well as the routine used to update k_c, are thoroughly elaborated in (Tang *et al.*, 2018).

An essential step suggested in the aforementioned study is to update the matrix k_c before sending new messages. Consequently, even if the same message has been sent twice using this model, the outcome will be different, even without the help of the

block cypher mode of operation. This change makes the cypher a dynamic cypher. The process of updating k_c is called a partial key update. This is because the 64 bits DES key, k_a, and k_c are together used as a key for this new cypher.

The capability of the cypher to resist linear and differential attacks has not been discussed. Furthermore, there is no discussion on the avalanche criterion or the output randomness. Moreover, no special arrangements have been used to immune the cypher against related-key attacks, zero-day attacks, timing attacks and other side-channel attacks. In fact, the authors of this approach stated that the security of this mechanism needs more investigation which has been left as future work. Moreover, as per the statement of the designers, the performance of this model can be compared to the performance of the 3-DES. However, 3-DES was known to be a sluggish cypher (Yang *et al.*, 2019).

Another example of a dynamic encryption algorithm has been introduced in (Noura *et al.*, 2019b). In this algorithm, it is assumed that the communicating parties have exchanged a secret Session Key (SK) a priori to establishing their communication. Using SK, an XOR operation is carried out with 512 bits nonce. The resulting 512 bits are hashed using SHA-512. The result is 512 bits. These bits will change with every new nonce. Hence, it will be called the Dynamic Key (DK). DK is divided into five sub-keys: $\{k_{S1}, k_{S2}, k_P, k_{RK}, k_{SRK}\}$. k_{S1} and k_{S2} are used to construct two different key-dependent substitution tables S_1 and S_2 using the key setup algorithm of the RC4 cypher. k_P is used to construct a permutation table π. k_{RK} will seed a stream cypher to generate a random sequence of bits. These randomly generated bits are divided into *m* blocks, where *m* represents the number of blocks of the plaintext. Every block of these *m* blocks will be used as a sub-key to be XORed with one block in the plaintext. The k_{SRK} will be used to generate a selection table that specifies which sub-key to be XORed with which plaintext block. All the cypher's building blocks are key-dependent. Hence, any change in any part of the key will lead to a major and unpredictable change in the output.

The cypher processes two blocks at a time. The first block is XORed with a sub-key selected using the selection table. Consequently, the result undergoes a byte

substitution process using S_1. The outcome of this substitution is XORed with the second plain block, and the result undergoes a byte substitution process using S_2. The result is the cyphered version of the first block. The second plain block undergoes a slightly different process (Noura *et al.*, 2019b).

The length of the Secret Key (SK) has not been specified. Unless the SK was lengthy enough, the cypher might be vulnerable to a brute-force attack. Moreover, the authors claimed that the cypher is capable of resisting linear and differential attacks. However, the conventional approach to assure the cypher's resistance against these attacks is to employ many rounds to decrease the prop-ratio and the correlation. Given that this cypher has only one round, there is no compelling argument that it can resist linear and differential attacks.

In terms of ciphertext randomness, the output randomness should be evaluated using the Statistical Test Suite (STS). The STS has not been used to evaluate the output randomness of this cypher. In addition, no special arrangements have been used to immune the cypher against related-key attacks, zero-day attacks, timing attacks and other side-channel attacks.

In terms of performance, the authors analysed the performance of the cypher, and compare it to the AES. The experiment has been carried out in different models of Raspberry Pi. The experiments concluded that the introduced cypher performance is about two times better than the AES-CBC and AES-CTR. It is worth mentioning that, these experiments have been purposefully carried on environments that have constrained resources (i.e. Raspberry PI0 and Raspberry PI3). The experimentation platform choice is rationale since the introduced cypher targets such constrained environments. However, normal computers are widely used. Therefore, it is important to evaluate the performance of the suggested cypher against the AES and other cyphers over normal computers. Otherwise, the comparison will not have adequate significance.

Moreover, Shoukat (2016) suggested a dynamic encryption mechanism. In this mechanism, rather than processing blocks of fixed size, a Dynamic Data Blocking

Mechanism (DDBM) is used to generate dynamic sized data blocks. In addition, a Randomised Substitution Mechanism (RSM) is employed to modify the keys and the blocks of the plaintext unpredictably. Consequently, a Multi Operation Data Encryption Mechanism (MODEM) is used. The MODEM operates by dynamically picking a group of encryption transformations among several other groups. Each group includes a set of operations such as XOR, permutations, random substitution, shifting, and logical operations. The process of selecting which group to be used is key-dependent, which qualifies this cypher to be considered a dynamic cypher.

MODEM has several issues. For instance, the author tried to prove the resistance of MODEM against chosen plaintext and cyphertext attacks, which implies the resistance of MODEM against linear and differential cryptanalysis. However, the proof depends on comparing the XOR result between parts of the plaintext and the parts of the cyphertext $(ßD \oplus Ć)$ or its complement $\sim(ßD \oplus Ć)$ to the corresponding parts of the encryption key K, and the corresponding parts of the session key ΔK. This is not sufficient to prove the resistance of MODEM against linear and differential attacks.

Moreover, no special arrangements have been used to immune the cypher against related-key attacks, zero-day attacks, timing attacks and other side-channel attacks. The key avalanche of MODEM is 41.57%, whereas the plaintext avalanche is just 2.14%. Both scores, especially the latter score, show a significant deviation from the value 50%. This indicates that MODEM has a poor avalanche.

In addition, this mechanism has a significantly poor performance. For instance, to employ this cypher for processing approximately 1.6 Kilo Bytes in a PC with average specifications, it takes 21.21 seconds and 124.49 seconds for encryption and decryption, respectively. Hence, it can be concluded that this dynamic encryption mechanism is neither secure nor has an acceptable performance.

From the above discussion, it can be concluded that there are several attempts to design *dynamic* cyphers that can counter or mitigate non-generic attacks. However, existing dynamic cyphers either have deficient performance or do not meet all the

security requirements including the avalanche criterion, output randomness, resistance against known attacks such as brute force, linear cryptanalysis, differential cryptanalysis, related-key, timing, and side-channel attacks.

1.3 Problem Statement

Symmetric encryption is widely used to provide the *confidentiality* security service. Nowadays, the most popular symmetric cypher is the AES. The AES and many other symmetric cyphers have a static structure. Although using a static cypher can be practical, it can render the cypher vulnerable to future potential attacks which would target its static nature to recover the secret key (Couturier *et al.*, 2020; Noura *et al.*, 2020a; Noura *et al.*, 2020b). Most of the existing cryptanalysis techniques aim at exploiting the known and static transformations used by the targeted cypher. Such attacks are called *non-generic attacks* (Sehrawat and Gill, 2018).

There are several non-generic attacks that have been designed to penetrate the AES. These attacks includes Grassi's Distinguisher (Grassi, 2018), which has been used to mount an attack on five rounds AES with the knowledge of 2^{32} chosen plaintexts. It also includes the attack suggested in (Bar-On *et al.*, 2020) which reduced the amount of needed chosen texts from 2^{32} to 2^{22} to attain the same results. In addition, In (Biryukov and Khovratovich, 2009) a related-key attack that has a complexity of 2^{96} has also been devised on the AES key scheduler using 2^{35} related keys. These are just a few examples. However, there are many other attempts to attack the AES such as (Bardeh and Rønjom, 2019; Kakarla *et al.*, 2017; Zhao *et al.*, 2017).

The common aspect of these attacks is that they utilise the static nature of the AES. These attacks are still impractical or only effective on a simplified version of the AES. However, it can lead to more effective attacks in the future.

To mitigate non-generic attacks, several dynamic cyphers have been suggested. In the context of this thesis, the term "attacks mitigation" means the measures used to counter or decrease the success possibilities of a given attack (Gui *et al.*, 2020;

Meadows *et al.*, 2020). Dynamic cyphers aim at mitigating non-generic attacks by changing how the cypher works according to the encryption key value. In other words, the dynamic cypher has different variants. Each variant uses different transformations to carry the encryption. The variant used for encrypting a given message is selected randomly according to the encryption key value.

When using a dynamic cypher, it is not enough to rely on the unknowingness or the ambiguity of the encryption transformations (i.e. dynamism) to prove the cypher security. As clarified by Ergün and Acar (2020), to comply with Kerckhoffs's principle, each variant of the dynamic cypher variants must be secure on its own. In other words, it is essential to ensure that all of the dynamic cypher variants are capable of providing the confidentiality security and resisting known attacks such as brute force, linear cryptanalysis, differential cryptanalysis, related key, timing, and side-channel attacks. Similarly, the output for each variant of the dynamic cypher must be statically indistinguishable from random data. Moreover, each of the dynamic cypher variants must satisfy the avalanche criterion.

In addition, sensitive systems such as the banking systems require the use of a well-known cypher (Pupezescu *et al.*, 2017). This is because such sensitive systems cannot tolerate using an encryption algorithm that has not been extensively investigated. To meet this requirement, all the variants of a dynamic cypher must be well-known cyphers.

On the other hand, the performance of the used cypher is an essential factor. Although it is possible to argue that the additional layer of dynamism or ambiguity will incur some delay, a cypher with a significant performance degradation is useless. In the context of this thesis, cypher performance refers to the time needed to carry out the encryption and decryption (Gnatyuk *et al.*, 2018; Yuan *et al.*, 2018).

Existing dynamic cyphers do not meet the security and performance requirements. For instance, the algorithms suggested by Bhavani *et al.* (2019), Chauhan and Sasamal (2019), and Rahaman *et al.* (2020) have security concerns. This is because there is no practical technique to investigate the avalanche criterion and the

output randomness. Moreover, these algorithms are vulnerable to a related-key attack that has a complexity of 2^{96} using 2^{35} related keys (Biryukov *et al.*, 2009). Furthermore, no arrangements have been used to immune these cyphers against zero-day attacks, timing attacks and other side-channel attacks. Similarly, in the algorithm suggested in Noura *et al.* (2019b), the length of the Secret Key (SK) has not been specified which may render the cypher vulnerable to a brute-force attack unless the key length was sufficient. Moreover, the cypher has only one round. Therefore, there is no compelling argument that it can resist linear and differential attacks. In addition, the ciphertext randomness has not been evaluated using the Statistical Test Suite (STS). Furthermore, no special arrangements have been used to immune the cypher against related-key attacks, zero-day attacks, timing attacks and other side-channel attacks.

Moreover, the dynamic encryption algorithms designed by Shoukat (2016) has numerous issues, including the cypher resistance against linear and differential cryptanalysis, related-key attack, zero-day attacks, timing attacks and other side-channel attacks. Moreover, the key avalanche of MODEM is 41.57%, where the plaintext avalanche is just 2.14%. Both scores show a significant deviation from the value 50%. This indicates that MODEM has a poor avalanche. Moreover, MODEM has a significantly poor performance. For instance, to employ this cypher for processing approximately 1.6 Kilo Bytes it takes 21.21 seconds and 124.49 seconds for encryption and decryption, respectively.

It can be concluded that there is a need to devise a dynamic cypher that has a good performance and meets all the security requirements including the avalanche criterion, output randomness, resistance against known attacks such as brute force, linear cryptanalysis, differential cryptanalysis, related key, timing, and side-channel attacks. This constitutes the primary research question as below:

> How to design a Multi-Shape Symmetric Encryption Mechanism (MSSEM) that is capable of mitigating non-generic attacks without compromising the actual security or significantly decreasing the performance?

In the context of this thesis, the phrase "*multi-shape symmetric cypher*" means a symmetric dynamic cypher that operates differently according to the encryption key value. In other words, the encryption transformations used to encrypt a given message depend on the encryption key value. The above primary question has led to the secondary research questions as given below:

i) *How to investigate the output randomness, avalanche criterion, resistance against known attacks, and the performance of the base cyphers that will be used in the Multi-Shape Symmetric Encryption Mechanism?*

ii) *How can these base cyphers be integrated to form the Multi-Shape Symmetric Encryption Mechanism?*

iii) *How are the performance and the security of the proposed MSSEM?*

1.4 Research Aim

This research aims to propose a Multi-Shape Symmetric Encryption Mechanism (MSSEM) that operates dynamically to mitigate non-generic attacks. This means the exact steps used to encrypt a given message will be unknown to the potential opponents. The approach should have provable security. This means the actual security of this approach should not depend on the dynamism of the approach. Moreover, the proposed approach should not render a significant performance degradation.

1.5 Research Objectives

To achieve the aim of the study, the following three objectives have been determined:

1. To investigate the output randomness, avalanche criterion, resistance against known attacks, and the performance of the selected base cyphers that will be used in the Multi-Shape Symmetric Encryption Mechanism.

2. To design a Multi-Shape Symmetric Encryption Mechanism (MSSEM) by integrating the selected base cyphers.

3. To evaluate the security and the cypher performance of the proposed Multi-Shape Symmetric Encryption Mechanism (MSSEM).

1.6 Research Scope

1. This research focuses on designing a Multi-Shape Symmetric Encryption Mechanism (MSSEM) that is capable of mitigating non-generic attacks.

2. The criteria that will be used to evaluate the devised approach are security and cypher performance. Security includes resistance against brute-force attacks, linear and differential cryptanalysis, related-key attacks, timing attacks, side-channel attacks, zero-day attacks, avalanche criterion, and output randomness. In the context of this thesis, the cypher performance means the time elapsed to carry the encryption and decryption (Gnatyuk *et al.*, 2018; Yuan *et al.*, 2018).

3. In the design of the proposed mechanism, only known and secure cyphers, modes of operations, and hashing algorithms are used. This includes the cyphers: AES, Serpent, MARS, Twofish and RC6. The modes of operation: CBC, CFB, OFB and CTR. The Hashing algorithm SHA-265. These design choices are made to avoid using a new encryption algorithm, mode of operation or hashing algorithm that has not been adequately scrutinized by the cryptography community.

4. The proposed mechanism requires that five cyphers (AES, Serpent, Twofish, MARS and RC6) and four modes of operation (CBC, CFB, OFB, and CTR) to be implemented. This will be feasible for general-purpose computers, and most other environments. However, it might be unfeasible for environments with

constrained memory and processing resources such as in embedded control systems (e.g. fitness trackers, domestic appliances, etc).

1.7 Research Significance

Nowadays, symmetric encryption algorithms form the security backbone for the majority of daily electronic services. Symmetric cyphers, which are currently in wide use, are static. This includes the DES, AES, 3DES and many other cyphers. According to Couturier *et al.* (2020), Noura *et al.* (2020b) and Noura *et al.* (2020a), such static cyphers might be vulnerable to future attacks that utilises their static nature. The attacks that target a specific cypher design are called non-generic attacks (Sehrawat and Gill, 2018).

To mitigate non-generic attacks, the mechanism used to perform the encryption should become dynamic. Consequently, the cypher will perform different encryption transformations according to the key value. This will decrease the attackers' capabilities of designing and launching effective attacks.

Several dynamic cyphers' designs have been suggested in the literature. However, existing dynamic cyphers have either poor performance as mentioned by Shoukat (2016) and Tang *et al.* (2018), or unprovable security as stated by Bhavani *et al.* (2019), Chauhan and Sasamal (2019), Rahaman *et al.* (2020) and Noura *et al.* (2019b). Hence, the significance of this thesis relies on suggesting a mechanism that can mitigate non-generic attacks without compromising the actual security or incurring intolerable performance degradation.

1.8 Research Contribution

This study proposes a Multi-Shape Symmetric Encryption Mechanism (MSSEM) that operates dynamically to mitigate non-generic attacks. Since the proposed MSSEM selects the encryption transformations dynamically, the opponent

will not be able to predict them. The proposed MSSEM integrates five cyphers and four block cypher modes of operation. The cyphers are AES, Serpent, Twofish, RC6 and MARS. These cyphers have been selected because they are secure, well-known and have good performance (Daemen and Rijmen, 2020). Moreover, the modes of operation used with this model are Cypher Block Chaining (CBC), Cypher Feedback (CFB), Output Feedback (OFB) and Counter (CTR). These are secure modes of operation recommended by the National Institute of Standards and Technology (NIST).

In this study, a random encryption algorithm, mode of operation and key length are selected based on the encryption key value. No one, except communicating parties, will be able to identify the used encryption algorithm mode of operation or key length. This renders the proposed MSSEM capable of mitigating non-generic attacks since the attacker cannot identify the used encryption algorithm and mode of operation. On the other hand, since only secure encryption algorithms and modes of operation have been used, the actual security of the encrypted message is maintained.

The contribution of the proposed MSSEM to security is its *dynamism*. In the context of this thesis, dynamism means the ability of the cypher to use different transformations (i.e. cryptographic suite) to encrypt a given message. The exact cryptographic suite used by the proposed MSSEM to encrypt a given message depends on the encryption key value. This dynamism enables the proposed MSSEM to mitigate the efficacy of non-generic attacks. This is because non-generic attacks target a fixed and known cypher structure. Since the proposed MSSEM work differently according to the encryption key value, the efficacy of a given non-generic attack will decrease accordingly. The proposed MSSEM has sixty different sets of encryption transformations. Moreover, assume a given non-generic attack has the success probability P_S on one of the sixty possible encryption transformations. Since the attacker cannot be sure which of the sixty possible encryption transformations has been used, the success probability of the attack will decrease to $\frac{P_S}{60}$.

The performance of the proposed MSSEM depends on the performance of its base cyphers. Needless to say, the proposed MSSEM carries some processing to select

the cryptographic suite in addition to the time needed for encrypting the payload. Consequently, the proposed MSSEM will be slower compared to its base cypher. However, to ensure that the overall performance of the MSSEM will not decrease significantly, two aspects have been considered. The first consideration is selecting only high-performance base cyphers in the design of the proposed MSSEM. The second consideration is to carefully consider the performance of the module responsible for providing the dynamism (e.g. the module responsible for cooking the cryptographic suite that will be used for encrypting a given message). By considering these two factors, the overall performance of the dynamic cypher will be good.

In conclusion, the main contribution of this study is proposing a *secure dynamic* symmetric encryption approach that has a *reasonable performance* and is *capable of mitigating non-generic attacks*.

1.9 Thesis Organisation

This thesis consists of seven chapters. Chapter 1 presents the overview, problem background, research aim and objectives as well as the contribution of the study. Chapter 2 provides a general overview of cryptography and highlights the widely known cyphers. It also highlights non-generic attacks and discusses the parameters used for evaluating symmetric cyphers. This is followed by exploring the design of several dynamic cyphers and mechanisms suggested for mitigating non-generic attacks. The research framework, the overall research plan, and the steps of testing, evaluation and validation methods are provided in Chapter 3. Subsequently, the experimental result, design details, analysis and discussions for the proposed study are demonstrated in Chapters 4, 5 and 6, respectively. In Chapter 7, the thesis summary, research contributions and future works are discussed accordingly.

REFERENCES

Abdullah, A. (2017). Advanced encryption standard (aes) algorithm to encrypt and decrypt data. *Cryptography and Network Security, 16*.

Abomhara, M., Khalifa, O. O., Zaidan, A., Zaidan, B., Zakaria, O., and Gani, A. (2011). An experiment of scalable video security solution using H. 264/AVC and advanced encryption standard (AES): Selective cryptography. *International Journal of the Physical Sciences, 6*(16), 4053-4063.

Abomhara, M., Zakaria, O., and Khalifa, O. O. (2010). An overview of video encryption techniques. *International Journal of Computer Theory and Engineering, 2*(1), 103.

Abomhara, M., Zakaria, O., Khalifa, O. O., Zaidan, A., and Zaidan, B. (2022). Enhancing selective encryption for H. 264/AVC using advanced encryption standard. *arXiv preprint arXiv:2201.03391*.

Ahmadova, U., Mammadova, L., and Kalejahi, B. K. (2019). Implementation of encryption on telemedicine. *arXiv preprint arXiv:1912.09572*.

Akhavan, A., Samsudin, A., and Akhshani, A. (2017). Cryptanalysis of an image encryption algorithm based on DNA encoding. *Optics & Laser Technology, 95*, 94-99.

Akinbowale, O. E., Klingelhöfer, H. E., and Zerihun, M. F. (2020). Analysis of cyber-crime effects on the banking sector using balance score card: a survey of literature. *Journal of Financial Crime*.

Akinyede, R. O., and Esese, O. A. (2017). Development of a secure mobile e-banking system. *International Journal of Computer (IJC), 26*(1), 23-42.

Al-Wattar, A. H., Mahmod, R., Zukarnain, Z. A., and Udzir, N. I. (2015). A New DNA-Based Approach of Generating Key-dependent ShiftRows Transformation. *arXiv preprint arXiv:1502.03544*.

Alagic, G., Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., et al. (2019). *Status report on the first round of the NIST post-quantum cryptography standardization process*: US Department of Commerce, National Institute of Standards and Technology ….

Alruily, M., Shahin, O. R., Al-Mahdi, H., and Taloba, A. I. (2021). Asymmetric DNA encryption and decryption technique for Arabic plaintext. *Journal of Ambient Intelligence and Humanized Computing*, 1-17.

Alwazzeh, M., Karaman, S., and Shamma, M. N. (2020). Man in The Middle Attacks Against SSL/TLS: Mitigation and Defeat. *Journal of Cyber Security and Mobility*, 449–468-449–468.

Amato, D., Juan, P., and Vénere, M. J. (2014). Encrypting video and image streams using OpenCL code on-demand. *CLEI Electronic Journal, 17*(1), 6-6.

Amer, S. (2021). Security of DBMSs. In *Advances in Security, Networks, and Internet of Things* (pp. 449-461): Springer.

Ammari, F. T., and Lu, J. (2017). Securing Financial XML Transactions Using Intelligent Fuzzy Classification Techniques: A Smart Fuzzy-Based Model for Financial XML Transactions Security Using XML Encryption. In *Ontologies and Big Data Considerations for Effective Intelligence* (pp. 214-326): IGI Global.

Anderson, R., Biham, E., and Knudsen, L. (1998). Serpent: A proposal for the advanced encryption standard. *NIST AES Proposal, 174*, 1-23.

Antonio, R. B., Sison, A. M., and Medina, R. P. (2019). *Performance Analysis of the Modified Generated S-Box for Advanced Encryption Standards.* Paper presented at the Proceedings of the 2019 2nd International Conference on Data Science and Information Technology, 117-121.

Arciuolo, T., and Elleithy, K. M. (2021). *Parallel, True Random Number Generator (P-TRNG): Using Parallelism for Fast True Random Number Generation in Hardware.* Paper presented at the 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 0987-0992.

Arshad, B., and Siddiqui, N. (2020). Construction of Highly Nonlinear Substitution Boxes (S-Boxes) Based on Connected Regular Graphs. *International Journal of Computer Science and Information Security (IJCSIS), 18*(4).

Arvedal, D. (2017). Analyzing network monitoring systems and objects for a telecommunications company.

Ashokkumar, C., Roy, B., Venkatesh, M. B. S., and Menezes, B. L. (2019). "S-Box" Implementation of AES is NOT side channel resistant. *Journal of Hardware and Systems Security*, 1-12.

Atici, A. C., Yilmaz, C., and Savaş, E. (2018). Cache-timing attacks without a profiling phase. *Turkish Journal of Electrical Engineering & Computer Sciences, 26*(4), 1953-1966.

Aumasson, J.-P. (2019). Too Much Crypto. *IACR Cryptol. ePrint Arch., 2019*, 1492.

Bachtiar, M. M., Ditanaya, T. H., Wasista, S., and Perdana, R. R. K. (2018). *Security enhancement of AES based encryption using dynamic salt algorithm.* Paper presented at the 2018 International Conference on Applied Engineering (ICAE), 1-6.

Bajpai, P., and Enbody, R. (2020). *An empirical study of key generation in cryptographic ransomware.* Paper presented at the 2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 1-8.

Baldi, M., Chiaraluce, F., Incipini, L., and Ruffini, M. (2019). Code-based physical layer secret key generation in passive optical networks. *Ad Hoc Networks*.

Balli, S., and Yilmaz, M. (2020). Multi-criteria usability evaluation of symmetric data encryption algorithms in fuzzy environment. *SN Applied Sciences, 2*(8), 1-12.

Bar-On, A., Dunkelman, O., Keller, N., Ronen, E., and Shamir, A. (2020). Improved key recovery attacks on reduced-round AES with practical data and memory complexities. *Journal of Cryptology, 33*(3), 1003-1043.

Bardeh, N. G., and Rønjom, S. (2019). *Practical Attacks on Reduced-Round AES.* Paper presented at the International Conference on Cryptology in Africa, 297-310.

Baz, M. (2018). Digital Image Encryption using Logistic Chaotic Key-based RC6. *Int. J. Comput. Appl, 182*(2), 17-23.

Bejar, E., Saldaña, J., Raygada, E., and Silva, C. (2017). *On the jitter-to-fast-clock-period ratio in oscillator-based true random number generators.* Paper presented at the 2017 24th IEEE International Conference on Electronics, Circuits and Systems (ICECS), 243-246.

Benhadjyoussef, N., Karmani, M., and Machhout, M. (2021). Power-based Side-Channel Analysis against AES Implementations: Evaluation and Comparison. *International Journal of Computer Science & Network Security, 21*(4), 264-271.

Bhattarai, S., and Wang, Y. (2018). End-to-end trust and security for Internet of Things applications. *Computer, 51*(4), 20-27.

Bhavani, Y., Puppala, S. S., Krishna, B. J., and Madarapu, S. (2019). *Modified AES using Dynamic S-Box and DNA Cryptography*. Paper presented at the 2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 164-168.

Bhowmik, A., Karforma, S., Dey, J., and Sarkar, A. (2020). *Fuzzy-Based Session Key as Restorative Power of Symmetric Key Encryption for Secured Wireless Communication.* Paper presented at the Proceedings of the 2nd International Conference on Communication, Devices and Computing, 171-183.

Biham, E., Anderson, R., and Knudsen, L. (1998). *Serpent: A new block cipher proposal*. Paper presented at the International Workshop on Fast Software Encryption, 222-238.

Biryukov, A., and Khovratovich, D. (2009). Related-key cryptanalysis of the full AES-192 and AES-256. *Advances in Cryptology–ASIACRYPT 2009*, 1-18.

Biryukov, A., Khovratovich, D., and Nikolić, I. (2009). *Distinguisher and related-key attack on the full AES-256.* Paper presented at the Annual International Cryptology Conference, 231-249.

Borrello, P., D'Elia, D. C., Querzoni, L., and Giuffrida, C. (2021). Constantine: Automatic Side-Channel Resistance Using Efficient Control and Data Flow Linearization. *arXiv preprint arXiv:2104.10749*.

Briongos, S., Malagón, P., de Goyeneche, J.-M., and Moya, J. M. (2019). Cache misses and the recovery of the full AES 256 key. *Applied Sciences, 9*(5), 944.

Buell, D. (2021). Modern Symmetric Ciphers—DES and AES. In *Fundamentals of Cryptography* (pp. 123-147): Springer.

Bujari, D., and Aribas, E. (2017). *Comparative analysis of block cipher modes of operation.* Paper presented at the International Advanced Researches & Engineering Congress, 1-4.

Burwick, C., Coppersmith, D., D'Avignon, E., Gennaro, R., Halevi, S., Jutla, C., et al. (1998). MARS-a candidate cipher for AES. *NIST AES Proposal, 268*, 80.

Canteaut, A., Lambooij, E., Neves, S., Rasoolzadeh, S., Sasaki, Y., and Stevens, M. (2017). Refined probability of differential characteristics including dependency between multiple rounds. *IACR Transactions on Symmetric Cryptology*, 203-227.

Cardona, D. (2019). Live streaming-TV content, acquisition, transformation, encryption, and distribution system, and method for its use: Google Patents.

Carlson, J. A. (2019). Method for secure communication using asymmetric and symmetric encryption over insecure communications: Google Patents.

Chandel, A., Aggarwal, A., Mittal, A., and Choudhury, T. (2019). *Comparative Analysis of AES & RSA Cryptographic Techniques.* Paper presented at the 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 410-414.

Chauhan, Y. S., and Sasamal, T. (2019). *Enhancing Security of AES Using Key Dependent Dynamic Sbox.* Paper presented at the 2019 International Conference on Communication and Electronics Systems (ICCES), 468-473.

Clark, S. (2021). Measuring up the universe. *New Scientist, 249*(3315), 32-38.

Couturier, R., Noura, H. N., and Chehab, A. (2020). ESSENCE: GPU-based and dynamic key-dependent efficient stream cipher for multimedia contents. *Multimedia Tools and Applications, 79*(19), 13559-13579.

Dabra, V., Bala, A., and Kumari, S. (2021). Reconciliation based key exchange schemes using lattices: a review. *Telecommunication Systems*, 1-22.

Daemen, J., and Rijmen, V. (1999). AES proposal: Rijndael.

Daemen, J., and Rijmen, V. (2020). The Advanced Encryption Standard Process. In *The Design of Rijndael* (pp. 1-8): Springer.

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L., and Hardyns, W. (2020). Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims. *Computers in Human Behavior, 108*, 106310.

De Meyer, L., De Mulder, E., and Tunstall, M. (2020). On the Effect of the (Micro) Architecture on the Development of Side-Channel Resistant Software. *IACR Cryptol. ePrint Arch., 2020*, 1297.

de Ree, M., Mantas, G., Rodriguez, J., Althunibat, S., Qaraqe, M. K., Alhasanat, A., et al. (2021). *Data Confidentiality for IoT Networks: Cryptographic Gaps and Physical-Layer Opportunities.* Paper presented at the 2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 1-6.

Degada, A., and Thapliyal, H. (2020). *Harnessing Uncertainty in Photoresistor Sensor for True Random Number Generation in IoT Devices.* Paper presented at the 2020 IEEE International Conference on Consumer Electronics (ICCE), 1-5.

Devarakonda Krishna, S., and Krishna, G. R. An Efficient Review on Encryption Algorithms used in Network Security.

Easttom, W. (2021). Asymmetric Algorithms. In *Modern Cryptography* (pp. 225-244): Springer.

Ergün, S., and Acar, B. (2020). *Revealing the Secret Parameters of an FPGA-Based "True" Random Number Generator.* Paper presented at the 2020 IEEE International Symposium on Circuits and Systems (ISCAS), 1-4.

Fathy, K. A., Bahig, H. M., and Ragab, A. (2018). A fast parallel modular exponentiation algorithm. *Arabian Journal for Science and Engineering, 43*(2), 903-911.

FBI. (2022). Federal Bureau of Investigation Internet Crime Report.

Ferguson, N., Kelsey, J., Schneier, B., and Whiting, D. (2000). *A Twofish Retreat: Related-Key Attacks Against Reduced-Round Twofish*: Twofish Technical Reporto. Document Number)

Freyre, P., Cuellar, O., Díaz, N., and Alfonso, A. (2020). From AES to Dynamic AES. *Journal of Science and Technology on Information security*, *1*(11), 11-22.

Furkan Altınok, K., Peker, A., Tezcan, C., and Temizel, A. GPU accelerated 3DES encryption. *Concurrency and Computation: Practice and Experience*, e6507.

Gnatyuk, S., Kinzeryavyy, V., Iavich, M., Prysiazhnyi, D., and Yubuzova, K. (2018). *High-Performance Reliable Block Encryption Algorithms Secured against Linear and Differential Cryptanalytic Attacks.* Paper presented at the ICTERI Workshops, 657-668.

Grassi, L. (2018). Mixture differential cryptanalysis: a new approach to distinguishers and attacks on round-reduced AES. *IACR Transactions on Symmetric Cryptology*, 133-160.

Grassi, L., Rechberger, C., and Rønjom, S. (2017). Subspace trail cryptanalysis and its applications to AES. *IACR Transactions on Symmetric Cryptology, 2016*(2), 192-225.

Gui, Y., Tamore, S. M., Siddiqui, A. S., and Saqib, F. (2020). Key Update Countermeasure for Correlation-Based Side-Channel Attacks. *Journal of Hardware and Systems Security*, *4*, 167-179.

Gupta, D. R. (2020). A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function. *European Journal of Molecular & Clinical Medicine*, *7*(7), 3397-3408.

Hammad, B. T., Sagheer, A. M., Ahmed, I. T., and Jamil, N. (2020). A comparative review on symmetric and asymmetric DNA-based cryptography. *Bulletin of Electrical Engineering and Informatics, 9*(6), 2484-2491.

Hammood, W. A., Abdullah, R., Hammood, O. A., Asmara, S. M., Al-Sharafi, M. A., and Hasan, A. M. (2020). *A review of user authentication model for online banking system based on mobile IMEI number.* Paper presented at the IOP Conference Series: Materials Science and Engineering, 012061.

Haque, M. E., Zobaed, S., Islam, M. U., and Areef, F. M. (2018). *Performance analysis of cryptographic algorithms for selecting better utilization on resource constraint devices.* Paper presented at the 2018 21st International Conference of Computer and Information Technology (ICCIT), 1-6.

Hell, M., and Westman, O. (2020). Electromagnetic Side-Channel Attack on AES using Low-end Equipment. *ECTI Transactions on Computer and Information Technology (ECTI-CIT), 14*(2), 139-148.

Hussain, A., Lasrado, L. A., Mukkamala, R. R., and Tanveer, U. (2021). Sharing Is Caring–Design and Demonstration of a Data Privacy Tool for Interorganizational Transfer of Data. *Procedia Computer Science, 181*, 394-402.

Hussain, I., Anees, A., AlKhaldi, A. H., Algarni, A., and Aslam, M. (2018a). Construction of chaotic quantum magnets and matrix Lorenz systems S-boxes and their applications. *Chinese Journal of Physics*.

Hussain, I., Anees, A., Aslam, M., Ahmed, R., and Siddiqui, N. (2018b). A noise resistant symmetric key cryptosystem based on S 8 S-boxes and chaotic maps. *The European Physical Journal Plus, 133*, 1-23.

Ibor, A. E., Oladeji, F. A., Okunoye, O. B., and Uwadia, C. O. (2021). Novel adaptive cyberattack prediction model using an enhanced genetic algorithm and deep learning (AdacDeep). *Information Security Journal: A Global Perspective*, 1-20.

Islam, A., Kobita, A. A., Sagar Hossen, M., Rumi, L. S., Karim, R., and Tabassum, T. (2021). Data Security System for A Bank Based on Two Different Asymmetric Algorithms Cryptography. In *Evolutionary Computing and Mobile Sustainable Networks* (pp. 837-844): Springer.

Jose, J., and George, D. S. (2019). Hardware Efficient Crypto-Coder Systems for Wireless Channels. *IETE Journal of Research, 65*(4), 494-501.

Kakarla, S., Mandava, S., Saha, D., and Chowdhury, D. R. (2017). *On the practical implementation of impossible differential cryptanalysis on reduced-round AES.* Paper presented at the International Conference on Applications and Techniques in Information Security, 58-72.

Kapoor, J., and Thakur, D. (2022). Analysis of Symmetric and Asymmetric Key Algorithms. In *ICT Analysis and Applications* (pp. 133-143): Springer.

Kaur, G., Singh, K., and Gill, H. S. (2021). Chaos-based joint speech encryption scheme using SHA-1. *Multimedia Tools and Applications, 80*(7), 10927-10947.

Khashan, O. A. (2020). Hybrid lightweight proxy re-encryption scheme for secure fog-to-things environment. *IEEE Access, 8*, 66878-66887.

Khisro, J. (2020). Understanding The Relation Between Interoperability And Data Quality: A Study Of Data Hub Development In Swedish Electricity Market. *International Journal of Public Information Systems, 14*(1).

KILIÇ, M. B. (2021). Encryption Methods and Comparison of Popular Chat Applications. *Advances in Artificial Intelligence Research, 1*(2), 52-59.

Kim, E., Lee, M., and Kim, J.-J. (2017). *8.2 8Mb/s 28Mb/mJ robust true-random-number generator in 65nm CMOS based on differential ring oscillator with feedback resistors.* Paper presented at the 2017 IEEE International Solid-State Circuits Conference (ISSCC), 144-145.

Kim, H., Hahn, C., and Hur, J. (2021). *Real-time Detection of Cache Side-channel Attack Using Non-cache Hardware Events.* Paper presented at the 2021 International Conference on Information Networking (ICOIN), 28-31.

Kumar, V., and Sinha, D. (2021). A robust intelligent zero-day cyber-attack detection technique. *Complex & Intelligent Systems*, 1-24.

Kuppuswamy, P., and John, R. (2020). *A Novel approach of Designing E-commerce authentication scheme using Hybrid Cryptography based on Simple symmetric key and extended Linear block cipher algorithm.* Paper presented at the 2020 International Conference on Computing and Information Technology (ICCIT-1441), 1-6.

Lipp, M., Kogler, A., Oswald, D., Schwarz, M., Easdon, C., Canella, C., et al. (2021). *PLATYPUS: Software-based power side-channel attacks on x86.* Paper presented at the IEEE Symposium on Security and Privacy (SP).

Liu, F., Cruz, W., and Michel, L. (2018). *A complete tolerant algebraic side-channel attack for AES with CP*. Paper presented at the International Conference on Principles and Practice of Constraint Programming, 259-275.

Liu, H., Wang, X., and Kadir, A. (2021a). Constructing chaos-based hash function via parallel impulse perturbation. *Soft Computing*, 1-10.

Liu, J., Tong, X., Zhang, M., and Wang, Z. (2020a). *The Design of S-box Based on Combined Chaotic Map.* Paper presented at the 2020 3rd International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE), 350-353.

Liu, X., Richardson, A. G., and Van der Spiegel, J. (2021b). An Energy-efficient Compressed Sensing Based Encryption Scheme for Wireless Neural Recording. *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*.

Liu, Y., Zhang, W., Sun, B., Rijmen, V., Liu, G., Li, C., et al. (2020b). The phantom of differential characteristics. *Designs, Codes and Cryptography, 88*(11), 2289-2311.

Lizama-Perez, L. A., and López R, J. M. (2021). Non-Invertible Public Key Certificates. *Entropy, 23*(2), 226.

Ma, L., Xu, J., Sun, J., Zhou, Y., Xie, X., Shen, W., et al. (2021). Revisiting Challenges for Selective Data Protection of Real Applications. *arXiv preprint arXiv:2105.14251*.

Malik, M. S. M., Ali, M. A., Khan, M. A., Ehatisham-Ul-Haq, M., Shah, S. N. M., Rehman, M., et al. (2020). Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. *IEEE Access, 8*, 35682-35695.

ManJiang, D., Kai, C., ZengXi, W., and LiPeng, Z. (2020). *Design of a Cloud Storage Security Encryption Algorithm for Power Bidding System.* Paper presented at the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 1875-1879.

Mansouri, A., and Wang, X. (2020). Image encryption using shuffled Arnold map and multiple values manipulations. *The Visual Computer*, 1-12.

Meadows, B., Edwards, N., and Chang, S.-Y. (2020). *On-Chip Randomization for Memory Protection Against Hardware Supply Chain Attacks to DRAM.* Paper presented at the 2020 IEEE Security and Privacy Workshops (SPW), 171-180.

Mekki, N., Hamdi, M., Aguili, T., and Kim, T.-h. (2018). *A real-time chaotic encryption for multimedia data and application to secure surveillance framework for IoT system.* Paper presented at the 2018 International Conference on Advanced Communication Technologies and Networking (CommNet), 1-10.

Menezes, A., and Stebila, D. (2021). The Advanced Encryption Standard: 20 Years Later. *IEEE Security & Privacy, 19*(6), 98-102.

Mewada, S., Sharma, P., and Gautam, S. (2016). Classification of efficient symmetric key cryptography algorithms. *International Journal of Computer Science and Information Security, 14*(2), 105.

Mihailescu, M. I., and Nita, S. L. (2021). Cryptanalysis Attacks and Techniques. In *Pro Cryptography and Cryptanalysis* (pp. 447-456): Springer.

More, P., Chandugade, S., Rafiq, S. M. S., and Pise, P. (2018). *Hybrid encryption techniques for secure sharing of a sensitive data for banking systems over cloud.* Paper presented at the 2018 International Conference on Advances in Communication and Computing Technology (ICACCT), 93-96.

Mushtaq, M., Akram, A., Bhatti, M. K., Rais, R. N. B., Lapotre, V., and Gogniat, G. (2018). *Run-time detection of prime+ probe side-channel attack on AES encryption algorithm.* Paper presented at the 2018 Global Information Infrastructure and Networking Symposium (GIIS), 1-5.

Muthalagu, R., and Jain, S. (2018). Modifying the structure KASUMI to improve its resistance towards attacks by inserting FSM and S-Box. *Journal of Cyber Security Technology, 2*(1), 37-50.

Nanda, A., Nanda, P., He, X., Jamdagni, A., and Puthal, D. (2020). A hybrid encryption technique for Secure-GLOR: The adaptive secure routing protocol for dynamic wireless mesh networks. *Future Generation Computer Systems, 109*, 521-530.

Noura, H., Chehab, A., and Couturier, R. (2019a). *Lightweight dynamic key-dependent and flexible cipher scheme for IoT devices.* Paper presented at the 2019 IEEE Wireless Communications and Networking Conference (WCNC), 1-8.

Noura, H., Chehab, A., Sleem, L., Noura, M., Couturier, R., and Mansour, M. M. (2018). One round cipher algorithm for multimedia IoT devices. *Multimedia tools and applications, 77*(14), 18383-18413.

Noura, H. N., Chehab, A., and Couturier, R. (2019b). Efficient & secure cipher scheme with dynamic key-dependent mode of operation. *Signal Processing: Image Communication, 78*, 448-464.

Noura, H. N., Chehab, A., and Couturier, R. (2020a). *Overview of Efficient Symmetric Cryptography: Dynamic vs Static Approaches.* Paper presented at the 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 1-6.

Noura, H. N., Salman, O., Kaaniche, N., Sklavos, N., Chehab, A., and Couturier, R. (2020b). TRESC: Towards redesigning existing symmetric ciphers. *Microprocessors and Microsystems*, 103478.

Nurgaliyev, A., and Wang, H. (2021). *Comparative study of symmetric cryptographic algorithms.* Paper presented at the 2021 International Conference on Networking and Network Applications (NaNA), 107-112.

Park, J. H., Rathore, S., Singh, S. K., Salim, M. M., Azzaoui, A., Kim, T. W., et al. (2021). A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions. *Hum.-Centric Comput. Inf. Sci, 11*(3).

Patil, J., Bansod, G., and Kant, K. S. (2017). *LiCi: A new ultra-lightweight block cipher*. Paper presented at the 2017 International Conference on Emerging Trends & Innovation in ICT (ICEI), 40-45.

PÉREZ, F. M. (2020). Multichannel audiovisual composition using audiovisual sampling, synchronous granular synthesis and pseudorandom number generator algorithms.

Pham, T. T. (2017). Comparative Study of the Characteristics of Modern Asymmetric Encryptions. *Revista Tecnologia da Informação e Comunicação: Teoria e Prática, 1*(1).

Prajwalasimha, S., and Surendra, U. (2017). *Multimedia data encryption based on discrete dyadic transformation.* Paper presented at the 2017 International Conference on Signal Processing and Communication (ICSPC), 492-495.

Premkumar, P., and Shanthi, D. (2016). Block Level Data Integrity Assurance Using Matrix Dialing Method towards High Performance Data Security on Cloud Storage. *Circuits and Systems, 7*(11), 3626.

Pupezescu, V., RĂDESCU, R., and PAŞCA, S. (2017). Design And Implementation Of An Online Learning Application To Study A Virtual E-Banking System. *eLearning & Software for Education, 2*.

Qasaimeh, M., Al-Qassas, R. S., and Tedmori, S. (2018). Software randomness analysis and evaluation of lightweight ciphers: the prospective for IoT security. *Multimedia Tools and Applications, 77*(14), 18415-18449.

Rahaman, Z., Corraya, A. D., Sumi, M. A., and Bahar, A. N. (2020). A novel structure of advance encryption standard with 3-dimensional dynamic S-Box and key generation matrix. *arXiv preprint arXiv:2005.00157*.

Reinbrecht, C., Forlin, B., and Sepúlveda, J. (2019). Cache timing attacks on NoC-based MPSoCs. *Microprocessors and Microsystems, 66*, 1-9.

Rezk, A. A., Madian, A. H., Radwan, A. G., and Soliman, A. M. (2019). Reconfigurable chaotic pseudo random number generator based on FPGA. *AEU-international Journal of Electronics and Communications, 98*, 174-180.

Rivest, R. L., Robshaw, M. J., Sidney, R., and Yin, Y. L. (1998). *The RC6 block cipher*. Paper presented at the in First Advanced Encryption Standard (AES) Conference.

Rivest, R. L., Robshaw, M. J., and Yin, Y. L. (2000). *RC6 as the AES.* Paper presented at the AES Candidate Conference, 337-342.

Roellgen, C. B. (2013). The Polymorphic Medley Cipher Version 2: 128 bit block length,128 .. 1024 bit key length.

Sahi, A., Lai, D., and Li, Y. (2018). *An Efficient Hash Based Parallel Block Cipher Mode of Operation.* Paper presented at the 2018 3rd International Conference on Computer and Communication Systems (ICCCS), 33-40.

Saleem, J., and Hammoudeh, M. (2018). Defense methods against social engineering attacks. In *Computer and network security essentials* (pp. 603-618): Springer.

Saqib, N. A., Shakeel, Y., Khan, M. A., Mehmood, H., and Zia, M. (2017). An effective empirical approach to VoIP traffic classification. *Turkish Journal of Electrical Engineering & Computer Sciences, 25*(2), 888-900.

Sarode, R. P., and Bhalla, S. (2019). *Data Security in Mobile Cloud Computing.* Paper presented at the Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.

Schillinger, F., and Schindelhauer, C. (2020). *Revocable Access to Encrypted Message Boards.* Paper presented at the International Workshop on Security and Trust Management, 57-72.

Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C., and Ferguson, N. (1998). Twofish: A 128-bit block cipher. *NIST AES Proposal*, *15*(1), 23-91.

Seghier, A., and Li, J. (2019). *AES Based on Key Dependently Nonlinear Redundant S-Box.* Paper presented at the ICC 2019-2019 IEEE International Conference on Communications (ICC), 1-6.

Seghier, A., Li, J., and Sun, D. Z. (2019). Advanced encryption standard based on key dependent S-Box cube. *IET Information Security*.

Sehrawat, D., and Gill, N. S. (2018). Analysis of Security Attacks on Lightweight Block Ciphers and their Countermeasures. *Journal of Engineering and Applied Sciences, 13*(20), 8439-8447.

Shakiba, A. (2021). A novel 2D cascade modulation couple hyperchaotic mapping for randomized image encryption. *Multimedia Tools and Applications, 80*(12), 17983-18006.

Shoukat, I. A. (2016). *Muli-operation Data Encryption Mechanism Using Dynamic Data Blocking and Randomized Substitution.* Universiti Teknologi Malaysia.

Srivastava, S., and Prakash, S. (2020). *Security Enhancement of IoT Based Smart Home Using Hybrid Technique.* Paper presented at the International Conference on Machine Learning, Image Processing, Network Security and Data Sciences, 543-558.

Stallings, W. (2016). *Cryptography and network security: principles and practice*: Pearson.

Sultan, I., Mir, B. J., and Banday, M. T. (2020). *Analysis and optimization of advanced encryption standard for the Internet of things.* Paper presented at the 2020 7th International Conference on Signal Processing and Integrated Networks (SPIN), 571-575.

Tang, H., Sun, Q. T., Yang, X., and Long, K. (2018). A network coding and DES based dynamic encryption scheme for moving target defense. *IEEE Access, 6*, 26059-26068.

Tayel, M., Dawood, G., and Shawky, H. (2018). *A proposed serpent-elliptic hybrid cryptosystem for multimedia protection.* Paper presented at the 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 387-391.

Thapar, S. S., and Sarangal, H. (2018). *A study of data threats and the role of cryptography algorithms.* Paper presented at the 2018 IEEE 9th Annual

Information Technology, Electronics and Mobile Communication Conference (IEMCON), 819-824.

Utakrit, N., and Utakrit, N. (2021). Similarity and Dissimilarity between Information Security and Information Assurance. *Information Technology Journal, 17*(2), 46-56.

Valencia, J. A. V., and Rey, B. A. R. (2019). Phase chaotic encryption and efficiency evaluation for an image multiplexing method. *Optics and Lasers in Engineering, 121*, 464-472.

Vandana, R., and BJ, S. K. (2020). *Integrity based Authentication and Secure Information Transfer Over Cloud for Hospital Management System.* Paper presented at the 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), 139-144.

Wang, H. (2019). Side-channel analysis of AES based on deep learning.

Wang, J., Liu, G., Chen, Y., and Wang, S. (2021). Construction and Analysis of SHA-256 Compression Function Based on Chaos S-Box. *IEEE Access*.

Wang, M., Wang, X., Zhang, Y., and Gao, Z. (2018). A novel chaotic encryption scheme based on image segmentation and multiple diffusion models. *Optics & Laser Technology, 108*, 558-573.

Wu, T., Zhang, C., Chen, Y., Cui, M., Huang, H., Zhang, Z., et al. (2021). Compressive sensing chaotic encryption algorithms for OFDM-PON data transmission. *Optics Express, 29*(3), 3669-3684.

Xing, B., Wang, D., Yang, Y., Wei, Z., Wu, J., and He, C. (2021). Accelerating DES and AES Algorithms for a Heterogeneous Many-core Processor. *International Journal of Parallel Programming, 49*(3), 463-486.

Xu, X., and Tian, N. (2019). *The search and improvement of DES algorithm for data transmission security in SCADA.* Paper presented at the 2019 International Conference on Intelligent Computing, Automation and Systems (ICICAS), 275-279.

Yang, W., Peisong, Y., and Qianchuan, Z. (2019). *Industry Trusted Network Communication Based on Quantum Encryption.* Paper presented at the 2019 Chinese Control Conference (CCC), 7016-7022.

Yildirim, N., and Varol, A. (2019). *A research on security vulnerabilities in online and mobile banking systems.* Paper presented at the 2019 7th International Symposium on Digital Forensics and Security (ISDFS), 1-5.

Yu, F., Li, L., He, B., Liu, L., Qian, S., Huang, Y., et al. (2019a). Design and FPGA implementation of a pseudorandom number generator based on a four-wing memristive hyperchaotic system and Bernoulli map. *IEEE Access, 7*, 181884-181898.

Yu, F., Li, L., Tang, Q., Cai, S., Song, Y., and Xu, Q. (2019b). A survey on true random number generators based on chaos. *Discrete Dynamics in Nature and Society, 2019*.

Yuan, Y., Yang, Y., Wu, L., and Zhang, X. (2018). *A high performance encryption system based on AES algorithm with novel hardware implementation.* Paper presented at the 2018 IEEE International Conference on Electron Devices and Solid State Circuits (EDSSC), 1-2.

Zhang, N. (2021). *Research on the Application of Data Encryption Technology Based on Network Security Maintenance in Computer Network Security*. Paper presented at the Journal of Physics: Conference Series, 022060.

Zhang, X., Ruizhen, W., Wang, M., and Wang, L. (2019). *A high-performance parallel computation hardware architecture in ASIC of SHA-256 hash.* Paper presented at the 2019 21st International Conference on Advanced Communication Technology (ICACT), 52-55.

Zhao, K., Cui, J., and Xie, Z. (2017). Algebraic Cryptanalysis Scheme of AES-256 Using Gröbner Basis. *Journal of Electrical and Computer Engineering, 2017*.

Zhao, Y., Yu, W., and Guo, C. (2021). Related-Key Analysis of Generalized Feistel Networks with Expanding Round Functions. *IACR Cryptol. ePrint Arch., 2021*, 425.

Zhu, C., Wang, G., and Sun, K. (2018). Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box. *Symmetry, 10*(9), 399.

LIST OF PUBLICATIONS

Indexed Journals with Impact Factors

1. **Altigani, A.**, Hasan, S., Barry, B., Naserelden, S., Elsadig, M.A. and Elshoush, H.T., 2021. A Polymorphic Advanced Encryption Standard–A Novel Approach. IEEE Access, 9, pp.20191-20207 **(Q1, IF: 3.367)**
2. **Altigani, A.**, Hasan, S., Shamsuddin, S.M. and Barry, B., 2019. A multi-shape hybrid symmetric encryption algorithm to thwart attacks based on the knowledge of the used cryptographic suite. Journal of Information Security and Applications, 46, pp.210-221 **(Q1, IF: 4.96)**

Indexed Journals

1. **Altigani, A.**, Hasan, S., Shamsuddin, S.M. and Barry, B., 2020.THE NEED FOR POLYMORPHIC ENCRYPTION ALGORITHMS: A REVIEW PAPER, Journal of Theoretical and Applied Information Technology, 98(3), pp.360-377 **(Q4, Indexed by Scopus)**

Indexed Conference Proceedings

1. **Altigani, A.**, Hasan, S., Barry, B. and Shamsuddin, S.M., 2018, August. Key-dependent Advanced Encryption Standard. In 2018 International Conference on Computer, Control, Electrical, and Electronics Engineering (ICCCEEE) (pp. 1-5). IEEE **(Indexed by Scopus)**