AN ENHANCED LIGHTWEIGHT CRYPTO-HASH FUNCTION TECHNIQUE USING NEW MERSENNE NUMBER TRANSFORM FOR INTERNET OF THINGS SECURITY

BY

NUBILA JALEEL

A thesis submitted in fulfilment of the requirements for the degree of Doctor of Philosophy (Engineering)

Kulliyyah of Engineering
International Islamic University Malaysia

SEPTEMBER 2022

ABSTRACT

Internet of Things is a concept that describes the idea of connecting everyday physical objects to the internet. So no longer objects are just related to their user, but now it is connected to surrounding objects and database. The main challenge in designing IoT applications is in the field of security. IoT contains resource-constrained devices such as sensors, actuators, and Radio Frequency Identification (RFID) in the edge layer. In order to implement the security mechanism in these types of devices, lightweight cryptographic techniques are the obvious solution. There are several lightweight hashing techniques available today. Examples are PHOTON, QUARK, SPONGENT, GLUON, etc. These all are fixed length block sized and key sized lightweight hashing techniques.

The existing lightweight hash family uses Maximum Distance Separable (MDS), Mixed column transformation or by using some registers for the desired diffusion. All transformation methods available only support fixed block size and key and require high hardware requirements.

This thesis proposes a Novel New Mersenne Number Transform (NMNT) based Lightweight hash function for IoT applications. This proposed Lightweight hash uses New Mersenne Number Transform, which provides good diffusion property and employs a fast algorithm to compute the transform. Further, the hash function's New Mersenne Number Transform supports the powerful property of variable transform length (powers of two). These properties make New Mersenne Number Transform suitable for the design of new Lightweight hashing technique. The proposed lightweight hash function is named lightweight New Mersenne number transform hash function (LNMNT) and it is evaluated in terms randomness, confusion and diffusion, distribution of hash function and different attacks. The randomness analysis testing is done using standardized NIST test suit. The hash function was evaluated by means of COOJA simulator and numerical models and was benchmarked against lightweight hash function PHOTON and the proposed system shows about 65 percentage of improvement in time of execution and 25 percentage improvement in randomness property. And also did some comparisons on other todays available lightweight hash function QUARK, SPONGENT, GLUON in a testbed implemented using Contiki OS platform running on Zolertia Z1 motes in terms of time of execution, cycles per byte and memory usage. The analysis result showed that our new lightweight hash function has good random property and is highly sensitive to a slight change in the input message and it consumed very low resources where the time of execution is only 1.3 seconds while the power consumption is 6.7 µW.

The proposed LNMNT uses 54042 cycles per byte for the hash length of 128 bits making it compete very well in comparison with other standardized industry-adopted lightweight hash functions, in terms of cycles per byte and execution speed. Furthermore, other LWT hash functions are not adaptable to different hash digest lengths. However, with LNMNT, transform length can be changed and create variable-length hash digests without increasing the number of rounds.

خلاصة البحث

إنترنت الأشياء هو مفهوم يصف فكرة توصيل الأشياء المادية اليومية بالإنترنت. لذلك لم تعد الكائنات مرتبطة فقط بمستخدمها ، ولكنها الآن متصلة بالكائنات المحيطة وقاعدة البيانات. يكمن التحدي الرئيسي في تصميم تطبيقات إنترنت الأشياء في مجال الأمن. يحتوي إنترنت الأشياء على أجهزة محدودة الموارد مثل أجهزة الاستشعار والمشغلات وتحديد الترددات الراديوية (RFID) في طبقة الحافة. من أجل تنفيذ آلية الأمان في هذه الأنواع من الأجهزة ، فإن تقنيات التشفير خفيفة الوزن هي الحل الواضح. هناك العديد من تقنيات التجزئة الخفيفة المتاحة اليوم. ومن الأمثلة على ذلك PHOTON ، و QUARK ، و SPONGENT ، و GLUON ، وما إلى ذلك ، وكلها تقنيات ذات حجم كتلة ذات طول ثابت وتقنيات تجزئة خفيفة الوزن ذات حجم رئيسي.

تستخدم عائلة التجزئة خفيفة الوزنالحالية أقصى مسافة يمكن فصلها (MDS) أو تحويل العمود المختلط أو باستخدام بعض السجلات للانتشار المطلوب. جميع طرق التحويل المتاحة تدعم فقط حجم الكتلة الثابتة والمفتاح وتتطلب متطلبات عالية للأجهزة.

تقترح هذه الرسالة وظيفة تجزئة خفيفة الوزن تعتمد على تحويل أرقام مرسين الجديدة (NMNT) لتطبيقات إنترنت الأشياء. تستخدم هذه التجزئة خفيفة الوزن المقترحة تحويل رقم Mersenne الجديد ، والذي يوفر خاصية انتشار جيدة ويستخدم خوارزمية سريعة لحساب التحويل. علاوة على ذلك ، يدعم تحويل رقم Mersenne الجديد لوظيفة التجزئة الخاصية القوية لطول التحويل المتغير (قوى اثنين). هذه الخصائص تجعل New Mersenne Number Transform مناسبًا لتصميم تقنية التجزئة خفيفة الوزن الجديدة. تسمى دالة التجزئة خفيفة الوزن المقترحة وظيفة تجزئة تحويل رقم Mersenne خفيفة الوزن (LNMNT) ويتم تقييمها من حيث العشوائية والارتباك والانتشار وتوزيع دالة التجزئة والهجمات المختلفة. يتم إجراء اختبار تحليل العشوائية باستخدام بدلة اختبار NIST الموحدة. تم تقييم وظيفة التجزئة عن طريق محاكاة COOJA والنماذج العددية وتم قياسها مقابل دالة التجزئة خفيفة الوزن PHOTON ويظهر النظام المقترح حوالي 65 بالمائة من التحسن في وقت التنفيذ و 25 بالمائة من التحسن في خاصية العشوائية. كما أجرى بعض المقارنات مع وظائف التجزئة خفيفة الوزن الأخرى المتاحة اليوم QUARK و SPONGENT و GLUON في اختبار تم تنفيذه باستخدام منصة Contiki OS التي تعمل على محركات Zolertia Z1 من حيث وقت التنفيذ والدورات لكل بايت واستخدام الذاكرة. أظهرت نتيجة التحليل أن وظيفة التجزئة خفيفة الوزن الجديدة لدينا لها خاصية عشوائية جيدة وحساسة للغاية لتغيير طفيف في رسالة الإدخال وتستهلك موارد منخفضة للغاية حيث يبلغ وقت التنفيذ 1.3 ثانية فقط بينما يبلغ استهلاك الطاقة 6.7 ميغاواط.

يستخدم LNMNT المقترح 54042 دورة لكل بايت لطول التجزئة البالغ 128 بتًا مما يجعله يتنافس بشكل جيد للغاية مقارنة بوظائف التجزئة خفيفة الوزن الأخرى المعتمدة في الصناعة ، من حيث الدورات لكل بايت وسرعة التنفيذ. علاوة على ذلك ، فإن وظائف تجزئة LWT الأخرى غير قابلة للتكيف مع أطوال مختلفة لهضم التجزئة. ومع ذلك ، مع LNMNT ، يمكن تغيير طول التحويل وإنشاء ملخصات تجزئة متغيرة الطول دون زيادة عدد الجولات.

APPROVAL PAGE

The thesis of Nubila Jaleel has been approved by the following:

Mohammed Hadi Habaebi

Supervisor

_____

Mohammmad Rafiqul Islam

Co-Supervisor

_____

Internal Examiner

_____

External Examiner

_____

Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Nubila Jaleel

Signature  Date: 12/09/2022

....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

A MERSENNE NUMBER TRANSFORM BASED ONE-WAY LIGHTWEIGHT CRYPTO-HASH FUNCTION FOR INTERNET OF THINGS

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Nubila Jaleel

12/09/2022

……..…….. ……..

Signature Date

ACKNOWLEDGEMENTS

First and foremost, I am thankful and grateful to the Almighty Allah SWT, the Creator and Sustainer of the universe, the most beneficent and most merciful, for His guidance and blessings, and for granting me the knowledge, health, patience and perseverance necessary to accomplish this research.

The advice and directions of my supervisor, Professor Dr. Mohamed Hadi Habaebi, can never be forgotten. He pushed me to reach my limits in a very gentle and polite way. His continuous encouragement, invaluable comments, fruitful suggestions, and consistent guidance are highly appreciated. I have learned a lot from working with him. I owe my thanks to him for all that. I would like to express my deep and grateful thanks to my co-supervisor Prof. Dr. Md. Rafiqul Islam and Prof. Dr. Shihab Hammed for their excellent help, timely suggestion, guidance and active support.

My sincere thanks go to every person who cooperated with me to finish this study, especially Dr Samer Zain, Mohd Shukur Ahmad, Abdul Rahmat Abdul Latiff, Mohd Norazizi Bin Hamzah, Ali Lwas, Mohammed Al shibly, and Ahmed Badawi. May Allah reward them all.

Finally special thanks are due to parents and words also fall short to express the appreciation and pride that I hold towards my husband to have the strength to uphold the ethical, and constantly support my initiatives for knowledge seeking. I would like to express appreciation to my family and friends, for their support and comments on my research work and above all to Allah alone.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATION

AES	Advanced Encryption Standard
DES	Data Encryption Standard
DSP	Digital Signal Processors
ECC	Elliptic Curve Cryptography
FNT	Fermat Number Transform
FFT	Fast Fourier Transform
FPGA	Field Programmable Gate Array
HBS	Hash Based Signature
ICT	Information Technology
IOT	Internet Of Things
IPsec	Internet Protocol Security
TLS	Transport Layer Security
IV	Initialization Vector
LFSR	Linear Feedback Shift Register
LNMNT	Lightweight New Mersenne Number Transform
LW	Lightweight
LWC	Lightweight Cryptography
LWH	Lightweight Hash
LWT	Lightweight
MAC	Message Authentication Code
MAL	Media Access Layer
MD5	Message-Digest algorithm 5
MDS	Maximum Distance Separable
MNP	Mersenne Number Prime
MPN	Mersenne Prime Number
MSP	Managed service provider
NIST	National Institute of Standards and Technology
NMNT	New Mersenne Number Transform
NFSR	Non-Linear Feedback Shift Registers
NLFSR	Non-Linear Feedback Shift Registers
NTT	Number Theoretic Transforms
PDR	Packet Delivery Ratio
PH	PHOTON
RFID	Radio Frequency Identification
RIOT	IOT OS
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
QK	QUARK

LIST OF SYMBOLS

b	Bit rate
c	Capacity
f, g, h	Boolean functions
h(x)	Hash function of x
I	Integer
K	Transform length
N	array length
mnp	Mersenne number prime
Nmax	Maximum Mransform Length
p	prime number
r	bitrate
X(k)	Integer array
β1, β2, α1, α2, q	Transform parameters

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND

The world is heading to a situation where objects are given life. Each object is able to communicate, act as storage and also think on its own. IoT describes the concept of connecting everyday physical objects to the internet (Ding et al., 2020). Thus, the objects no longer are related to only user but also is connected to surrounding objects and databases. IoT applications not only lessened the work burden, it improved the maximum utilization of resources. Figure 1.1 shows IoT applications, where the world empowered with IoT is about to arrive (Jasim & ALRikabi, 2021). The data produced by this world can be beneficial and contains consequences to the society. The main drawbacks arise in the field of security and privacy. Hence, a better security mechanisms for IoT is needed (Sharma et al., 2018).

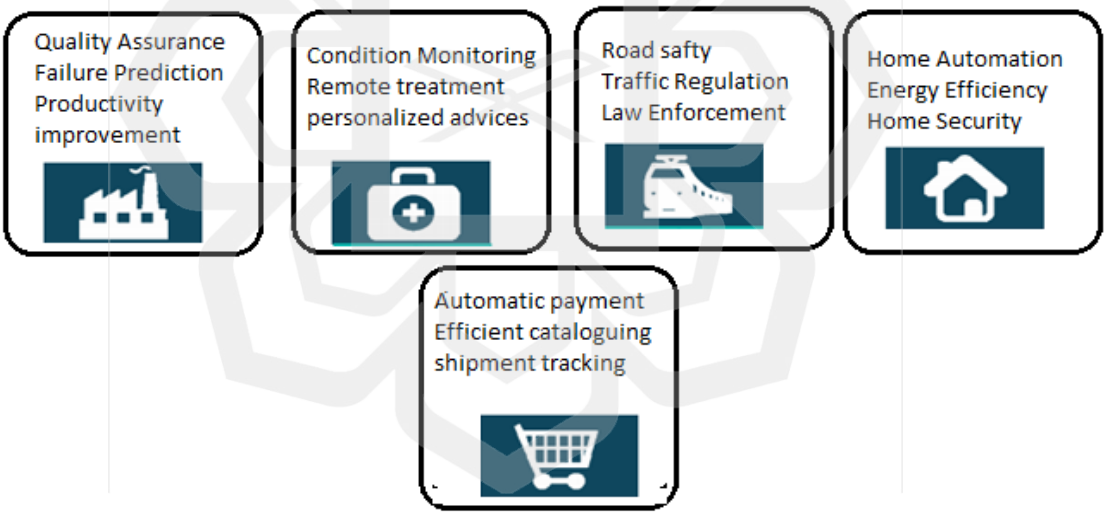

Figure 1.1 IoT Applications

In today's networking concept everything is mobile, dynamic and virtually connected to everything. IoT has been successfully applied to many fields such as medical health, military applications, security assurance, agricultural field etc (Ashibani & Mahmoud, 2018). Basically, IoT is based on the wireless network which are easily attacked by attackers. Moreover, the sensor nodes and gateways are located in open environment, which are vulnerable to different security problems. The security

guarantee for the communication between links need to be maintained. Failing in security aspects can lead the attacker to attack the links and devices, collect information and destroy the communication.

In case of IoT security (Suchitra & Vandana, 2016), one should start from lower level security to higher levels (X. Li et al., 2011). Lower-level means starting from the sensor nodes and gateways level. Hence, security of edge devices while connecting to network is considered. The main issue related to the security of edge devices is that these are very resource constrained devices which means they possess very little computational power, small memory, and are power constrained devices in nature. In order to implement the security mechanism in these types of devices, developing of lightweight security mechanisms (Ukil et al., 2011) is required.

1.2 IOT FUNDAMENTAL DESIGN AND OPERATIONAL CONSTRAINTS

Researchers have been working hard to develop hash functions that are suitable to run on the given system requirements (Kenji et al., 2015). The newly proposed hash algorithm, investigated in this research work, must manage to run with low resource load and overcome issues of security and throughput. In cipher design, a trade-off between cost and security is necessary. Due to non-criticality of data transmitted by single RFID chip, complete mass of all RFID chip's data is critical. Therefore, the data transmitted to other chips or servers should not be transmitted in clear format.

For example, a small cipher with reduced security still secures enough because attacker must compromise the hashed data of all RFIDs. It is challenging with the presented hash functions. Typically, in IoT scenarios, availability might be more important than confidentiality. But it depends on the use case. Latest Trends and Current LWT Crypto-Functions Standardization Efforts Internet-of-Things (IoT) applications often require constrained devices to be deployed in field for several years, even decades. Protection of these tiny motes is crucial for end-to-end IoT security. Secure boot and attestation techniques are critical requirements in IoT devices expected to be deployed in field for several year, even decades. Such devices which rely on public key Sign/Verify operations. In not-so-distant future, quantum computers are expected to break traditional public key Sign/Verify functions (e.g. RSA and ECC signatures).

Hash Based Signatures (HBS) schemes, on the other hand, are promising quantum-resistant alternatives. Their security is based on security of cryptographic hash

function which is known to be secure against quantum computers. The XMSS signature scheme (Ghosh et al., n.d.) is a modern HBS construction with several advantages, but it requires thousands of hash operations per Sign/Verify operation, which could be challenging in resource constrained IoT motes. A latency-area optimized XMSS Sign or Verify scheme with 128-bit post-quantum security was proposed in and an appropriate HW-SW architecture has been designed and implemented in FPGA and Silicon, where it spans out to 1521 ALMs and 13.5k gates respectively. In total, each XMSS Sign/Verify operation takes 4.8 million clock cycles in the HW-SW hybrid design approach which is 5.35 times faster than its pure SW execution latency on a 32-bit microcontroller.

The main goal of LWT cryptography (Dutta, 2019) is to use less memory, computing resource, power supply to provide security solution that can work over resource-limited devices. The LWT cryptography is expected to be simpler and faster implementation compared to conventional cryptography. Because of weakness and problems in standard hash algorithms, designing a new cryptographic hash function is an active research topic. This thesis research basically deals with construction of New Mersenne Number Transform (Boussakta et al., 2003) based on new LWT hashing techniques suitable for resource constrained devices. The main advantages of using Mersenne numbers Transforms are:

1. Any arithmetic modulo Mersenne number is hamming weight preserving. Always use low hamming weight numbers for key generation, so any number modulo Mersenne number keep low hamming weight. With low hamming weight, there need only low computation power.
2. Calculation of any number modulo Mersenne number operation can be done within shorter time.
3. Use variable transform length (powers of two).
4. Use variable block size.
5. Use fast algorithm to compute the transform.
6. Attain good diffusion property.

1.3 ARCHITECTURE OF IOT

The architecture of IoT applications is shown in figure 1.2 consisting of four layers. The device layer consists of sensors, actuators, RFIDs and gateways (Qian et al.,

2016). Gateways collect the data from the above-mentioned devices for further processing. This layer consists of resource constrained devices. Second layer, Network Layer, provides transport and networking capabilities for routing the data. Third Layer is a middle layer which hides the complexity of lower layers to higher layer and provides also storage and further processing of data. The Application layer caters for different IoT applications like Smart city, Smart industry and smart health.

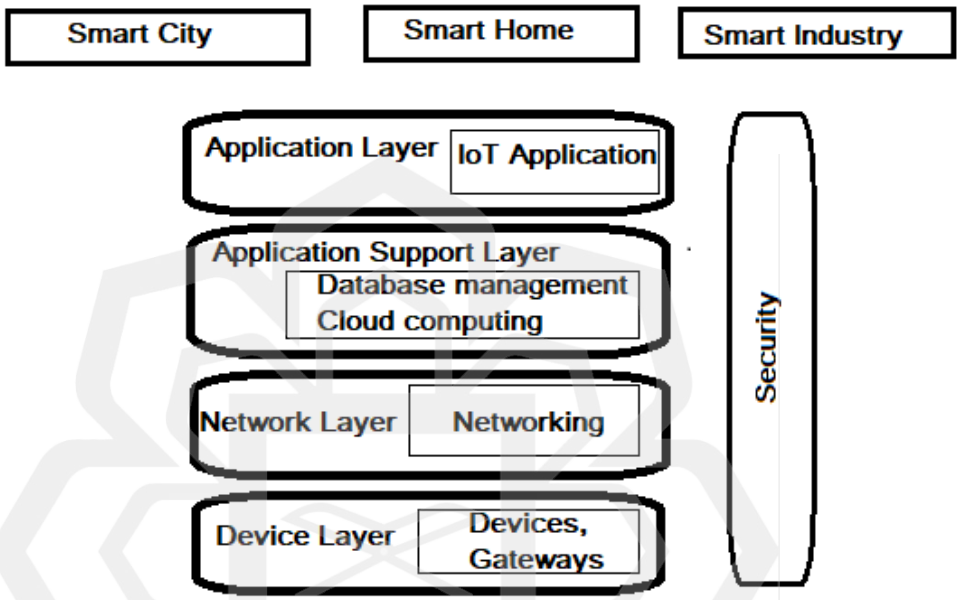

Figure 1.2 Architecture view of IoT

The security module provides necessary security features to each layer. It is known, the device layer consists of resource constrained devices. In order to implement a security mechanism in this layer LWT cryptographic techniques is required. The main factors that needed to be consider for LWT cryptography includes memory usage, power consumption and processing speed. The implementation of conventional cryptographic techniques, such as SHA, AES are impossible in these kinds of devices due to complexity associated with techniques. RFID tags have total gate count of 1000-10000, with only 200-2000 gates set for security. Most of the conventional cryptographic techniques needs more than 10000 gate equivalents for its implementation (Naru et al., 2017).

For LWT cryptography, PH (Guo et al., 2011), QK (Aumasson et al., 2013), SPONGENT (Bogdanov et al., 2013) , hash one (Mukundan et al., 2016) and Lesamanta-LW (Akhimullah & Hirose, 2017) are defined as hashing methods in ISO/IEC 29192-5:2016, PRESENT and CLEFIA for block ciphers in ISO/IEC 29192-

2:2012, and Enocoro and Trivium are defined stream methods in ISO/IEC 29192-3:2012.

1.4 LIGHTWEIGHT HASH FUNCTIONS CHALLENGES

Most of the LWT hash function family known so far managed to run on resource constrained devices but have some issues in terms of security and throughput. Consequently, it is necessary to develop new approaches to hash function algorithm design that is able to prevent attacks effectively in comparison to existing algorithms, as they do not totally meet the requirement of latest technologies and security concern of IoT. Furthermore, these issues are always considered in greater perspective of the ICT rather than specific application domain of IoT (Zhang & Zhu, 2011).

Recently, there are many options followings for lowering of resource requirements of hash functions, such as reducing the block size reducing the key size or reducing the computations. However, making hash function LWT by reducing the block size can be a serious concern against security, because there is increase in the probability of guessing the random IV by the attackers, so that probability of recovering the plaintext block by block by using chosen –plaintext attack increases. From this it is clear to say that LWT is not meant to be weak cryptography. More from less availability is required, so that weakening conventional cryptography is not good practice to achieve design goal of LWT cryptography. Hence, an alternate method to achieve the LWT goal is needed. There are many possibilities of side channel attacks, and is vital to consider countermeasures at the implementation level.

Two main principles to secure cryptographic systems are diffusion and confusion property. Confusion tries to make complication between plaintext and cipher text. Diffusion is the process to rearranges plaintext into cipher text. The strength of diffusion is measured by how plaintext is rearranged into cipher text. A small change in plaintext should have a significant change in cipher text. This effect is called avalanche effect. The cryptosystem should have good avalanche effect in such a way that half of cipher text should chance for a single change in plaintext. Currently, AES algorithm uses Mix Column Transformation in its diffusion layer. Mix Column transformation is powerful for diffusion property. However, this transformation is fixed in terms of their length. So that one cannot make significant change in the algorithm to make it completely adequate for IoT devices. Thus, there is need for an alternative method in

order to satisfy the requirements of IoT devices. One major solution is to use parameter-based transformation which supports variable block length and key size by changing the transform length accordingly.

In this research, a new LWT hash function LNMNT is described, which uses New Mersenne Number transform (NMNT) in its diffusion layer based on the advantages of NMNT described above. Sponge construction method is chosen in order to reduce the internal memory size as possible. This research also includes NIST test result of our new LWT hash function.

1.5 PROBLEM STATEMENT

The main challenge in the design of security system of IoT is in the device layer. This is due to the fact that the device layer consists of resource-constrained devices. There are many lightweight hashing techniques available today such as PH (Li et al., 2018) (Meuser et al., n.d.), QK (Aumasson et al., 2013), SPONGENT (X. Wang et al., 2016), GLUON (Tareq Hammad, Jamil, Ezanee Rusli, & Reza, 2017) and SPN-HASH (Canteaut, Anne & Roué, Joëlle. 2015) etc. However, their major drawback is that they only support fixed block size or fixed parameter-based hash functions.

A balancing of resource requirements and security is a challenging problem in LWT cryptographic design. The majority of LWT hashing approaches attempt to simplify existing cryptographic techniques which is a bad practice because ‘‘lightweight’’ does not imply ‘‘weak’’ or ‘‘light’’ cryptography. LWT designs require same or better level of security features than conventional cryptography. Most of LWT hash function family known so far managed to run on resource-constrained devices, but do have some issues in terms of security level achieved and throughput. Consequently, it is necessary to develop new approaches to hash function design that can prevent attacks effectively in comparison to existing algorithms as they are not sufficient to meet requirement of latest technologies and security concerns of IoT applications. There are more than fifty symmetric LWT cryptographic algorithms proposed by various sectors. However, the design focuses on how to reduce cost and enhance hardware and software performance. Furthermore, many of them do not properly consider mitigating security attacks. The ideal LWT cryptographic technique should reduce the conflict and strike a balance between cost, performance, and security. To reach these three often contradicting properties all together is a challenging design problem. Security problems

arise often when key or block sizes are reduced, and when algorithm design is simplified. Making a hash function LWT by reducing the block size can be of serious concern against security because there is an increase in probability of guessing random IV by attackers (e.g., the probability of recovering the plaintext block by block by using chosen plaintext attack increases). LWT does not mean weak cryptography, as more from less availability is needed. Hence, weakening conventional cryptography is not a good practice to achieve design goal of LWT cryptography and an alternative design approach should be considered. There are many possibilities of side-channel attacks, and it is vital to consider countermeasures at implementation level. Two main principles for secure cryptographic systems are diffusion and confusion property. Confusion tries to make complications between plaintext and ciphertext. Diffusion is the process in which plaintext is rearranged into ciphertext. The strength of diffusion is measured by how the plaintext is rearranged into ciphertext. A small change in the plaintext should have a significant change in ciphertext (e.g., the avalanche effect). The crypto system should have good avalanche effect in such a way that half of the ciphertext should change for a single change in the plaintext. Currently, the AES algorithm uses Mix Column Transformation in its diffusion layer. Mix Column transformation is powerful for diffusion property. However, this transformation is fixed in terms of their length such that a significant change in the algorithm to make it completely adequate for IoT applications cannot be made. As a result, an alternate technique to meet the needs of resource-constrained IoT devices is the usage of parameter-based transformation, which permits changeable block length and key size by adjusting the transform length.

1.6 RESEARCH OBJECTIVES

The proposed new hash function is expected to support variable length hash block for applications to the domain of IoT. The main features of the proposed novel hash function are being lightweight, produce variable hash size, low cost, possess reduced implementation complexity and has good diffusion.

The research specific objectives are:

1. A new design approach is required for the construction of a LWT hash function, where simplification of existing conventional cryptographic techniques is not recommended. As a result, by using NMNT design a lightweight one-way hash function for resource-constrained IoT devices.