A Survey of Cryptographic Algorithms for IoT Devices

Susha Surendran (NYIT, Abu Dhabi, UAE), Amira Nassef (NYIT, Abu Dhabi, UAE),
Babak D. Beheshti (NYIT, Old Westbury, New York)

Abstract— The future of Internet is "Intrnet of Things" where trillions of physical objects, most of them with low or extremely low resources, communicate with each other without human intervention. Light weight cryptography includes cryptographic algorithms specifically meant for extremely constrained resources. They can be applied not only for encryption but also for hashing and authentication under environments that are highly constrained. In this paper, we first discuss the need of light weight cryptography and their design differences with normal block ciphers. An overview of some of the light weight cryptographic algorithms is discussed after that. Also, we look into different types of attacks that has been studied on some of these ciphers. Finally, we compare the performance of some of these ciphers on Windows and Embedded platform.

***Index Terms*— 3DES, AES, Blowfish, Cryptanalysis, Cryptographic algorithms, Crypton, Curupira, DES, DESL, DESX, DESXL, embedded platform, Feistel Structure, Katan & Ktantan, HIGHT, HIGHT2, Hummingbird, Hummingbird-2, Internet of Things, KEELOQ, LBLOCK, LED, Light weight cryptography, NOEKEON, PES, PRESENT, mCrypton, Raspberry Pi, RC2, RC6, RSA, SEA, Skipjack, Simon and Speck, Symmetric and Asymmetric algorithms, TEA, XTEA and TWINE.**

INTRODUCTION

Soon there will be trillions of devices on the Internet. And the major problems that Internet of Things (IoT) is facing are in the areas of naming, authentication, maintenance, security and support at this large scale. The growth of IoT will be soon in a more general class of cyber-physical systems which leads to technologies such as smart grids, virtual power plants, intelligent transportation, smart homes and smart cities. Researchers are now more focused on specifying, detecting and resolving dependencies across applications.

There will be a vast amount of raw data being continuously collected in an IoT world which requires real-time sensor data streams as well as techniques to convert these raw data to usable knowledge. Also there will be serious questions on data privacy and security. Design criteria of cryptographic algorithms intended for devices with extremely low resources are different from that of commonly used ones. This very specific field leads to a branch of modern cryptography – lightweight cryptography.

NEED FOR LIGHT WEIGHT CRYPTOGRAPHY ALGORITHMS

As internet is growing day-by-day, security is turning out to be the most critical and challenging aspect of it. Cryptography, study of converting normal data into unreadable form, is playing a vital role in information security.

A. Cryptography algorithms

Cryptography is the art and science of keeping a message (such as email messages, credit card information, etc.) secure, while transmitting it in the network by encrypting the data using encryption algorithms. Many encryption algorithms are used in network security. They are divided into three basic types: Symmetric algorithms, Asymmetric (or public-key) algorithms, and Cryptographic protocols. According to number of keys used in encryption and decryption, they are classified to: Symmetric algorithms (or secret key encryption) where one key is used to encrypt and decrypt data, and Asymmetric (or public-key) algorithms which use two keys i.e. private and public keys. Public key is used for encryption and private key is used for decryption.

Some of the important cryptographic algorithms available in the market: Rivest-Shamir-Adleman (RSA), Data Encryption Standard (DES) – no longer considered secure, Triple DES (3DES), Advanced Encryption Standard (AES), Blowfish, RC2, and RC6. Although those algorithms are vital in information systems security, they consume a significant amount of computing resources such as CPU time, memory, and battery power.

Symmetric key encryption strength depends on the size of key used, for example RC2 and DES uses a 64-bit key, Triple DES (3DES) uses two 64-bits keys, AES and RC6 use any of 128, 192 or 256 bits keys and Blowfish uses 32-448 bit range keys (default 128 bits) [1, 2]. In this paper we will compare the performance of cryptographic algorithms in terms of energy, changing data types

such as text or document, power consumption, changing packet size, and changing key size.

Energy consumption of different symmetric algorithms depends on key size, as it needs more energy to perform more operations. For example, it is found that after only 600 encryptions of 5 MB file using 3DES, 55% of battery power is consumed [3, 4, and 5]. In AES as the key size is increased by 64 bits, the energy consumption increased about 8% without any data transfer. In a study to evaluate performance of encryption algorithms on power consumption for wireless devices, Figure 1 graph is derived which shows the power consumption for encrypting text data with different data block size by calculating change in battery left for encryption process without data transmission [3].

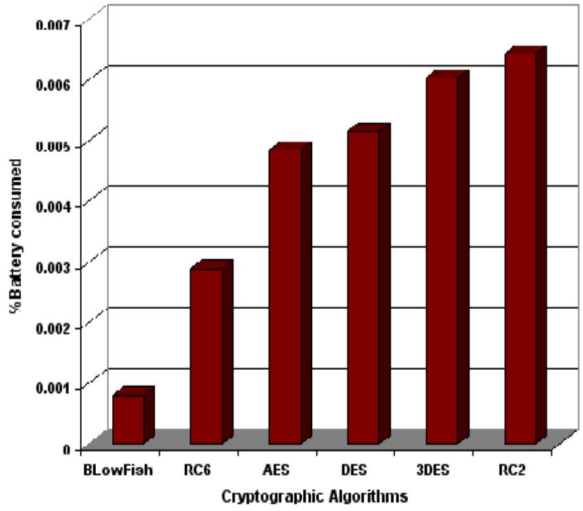

Figure 1: Battery consumed for each encryption algorithm

As seen in Figure 1, most of encryption algorithms consumes energy which affect battery power. Due to the slow increasing rate in battery technology than other technologies we face a "battery gap" [4], so decisions need to be made about energy consumption and security to reduce the consumption of battery powered devices.

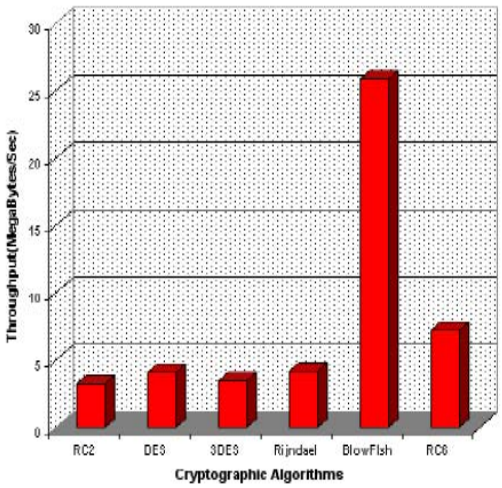

Figure 2: Throughput of each encryption algorithm (Megabyte/Sec)

The throughput of the encryption scheme is calculated by dividing the total size of plaintext in megabytes encrypted on the total encryption time for each algorithm in. As the throughput value is increased, the power consumption and CPU process time of this encryption technique is decreased. CPU Process Time reflects the load of the CPU. This load depends on the CPU time used in the encryption process. Therefore, the more time the CPU will be used in the encryption process, the higher the load of the CPU will be. In Figure 2, it is evident that other than Blowfish algorithm, all other algorithms' throughput is very low and cannot be recommended for low computing systems.

The study in [5] shows that the consumption time of encryption algorithms is increased as the key size and the packet size increased and AES has better performance than RC2, DES, and 3DES. On the other hand, [6] and [7] found that AES requires more space in memory as the baseline version of AES uses 800 bytes memory space for lookup tables and consumes the most energy per byte during encryption and decryption.

B. The Internet of Things (IoT)

The Internet of Things (IoT) is now one of the essential topics in the industry of technology. IoT has changed our world in the recent years in many aspects of life, including industrial components, customer goods, cars, smart phones, TVs, and many of our daily use objects ("things") that have unique identities and are being provided with internet connection in which case can be remotely available. IoT enables highly resource-constrained devices which have lower computational power, smaller memory size, lower power consumption, smaller physical size, lower price to communicate, compute

process and make decision in the communication network [8]. Security is one of the challenging issues in IOT due to the limited resources available in such constrained devices, in other words how to provide confidentiality, data integrity, and authentication to IOT devices, in spite of the fact that most security mechanisms require heavy computation loads and large memory requirements.

As we discussed in part a) the commonly used cryptographic algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power, so the main challenge in IOT as resource constraint devices is a resource-efficient cryptographic algorithms which are lightweight algorithms that are suitable for resource-constrained environments. These include algorithms that are fast and responsive, more energy and storage efficient than conventional encryption and decryption algorithms, and powered by optimized crypto engines [9].

LIGHT WEIGHT CRYPTOGRAPHY ALGORITHMS

Design criteria of cryptographic algorithms to be used in extremely low resource devices are different from that of the commonly used ones. For this, lightweight cryptography algorithms are developed that have extremely low requirements. Even though no strict criteria is defined for lightweight cryptography algorithms, the features usually includes any one or more of

- Minimum size required for hardware implementation;
- Low computational power of microprocessors or microcontrollers;
- Low implementation cost;
- Good security

There is a trade-off between security, costs and performance i.e. in cryptographic algorithms, the key length is correlated with security and cost trade-off, while the number of rounds in encryption provides a security, performance trade-off and hardware architecture[10]. As it is difficult to optimize all the three design goals, usually two of these goals are kept in mind while designing the lightweight algorithms.

A. DESL & DESXL

DESL is the lightweight version of classical DES algorithm and DESXL is a lightweight version of the DESX algorithm where both uses a single S-box (substation block) instead of 8 S-boxes. As there is only a single S-box, memory is saved and the S-box makes them resistant to most of the common cryptanalytic attacks.

B. Curupira

Curupira algorithm is based on the Wide Trail strategy by Joan Daemen [11]. To qualify it as the lightweight algorithm, it has the following features:

- The data block size is 96 bits and is represented as 3 X 4-byte array. The key lengths can be 96, 144 or 192 bits;
- The number of rounds is determined based on the key length;
- The 8 X 8-bit S-box is implemented as two 4 X 4-bit S-boxes. This will reduce the space required to store the S-boxes

C. Katan & Ktantan

KATAN & KTANTAN are from a family of hardware oriented six block ciphers which are divided into 3 KATAN ciphers: KATAN32, KATAN48, and KATAN64 and 3 KTANTAN ciphers: KTANTAN32, KTANTAN48 and KTANTAN64. The number in the algorithm's name represents the block size of the algorithm in bits. They both use 80-bit key size. The difference is that KTANTAN is more compact in hardware where the key is burnt into the target device and cannot be changed. So KTANTAN ciphers are small block ciphers when compared to KATAN and is used in devices which are initialized with one key.

Due to the following features, the resource requirements for Katan & Ktantan algorithm are low:

- The size of the internal state is equivalent to the block size of the algorithm. They use the shift registers and feedback functions which are easy to implement in hardware and provides required nonlinearity.
- They process small blocks of data which are from 32 to 64 bits;
- KTANTAN's key schedule is simple.

D. Present

PRESENT is one of the leanest lightweight algorithms and has obtained the ISO/IEC standard for lightweight cryptography. It is based on the transformation layers of Serpent [13] and DES [12] that has been analyzed in-depth, especially on security and hardware efficiency. It has the following features to consider it as the leanest algorithm.

- It uses very less gate count and less memory.
- It performs 31 rounds on 64-bit data block
- It allows to use 80 or 128-bit keys.
- The most compact hardware implementation of PRESENT needs 1570 (GE) and is therefore competitive with today's leading compact stream ciphers, which need 1300-2600 GE.

PRESENT was designed for hardware performance but can be implemented in software. The applications that mainly uses PRESENT algorithm is for encrypting small or reasonable amount of data.

E. Hummingbird

Hummingbird is a hybrid algorithm of both block and stream ciphers. It encrypts

- 16-bit blocks of data
- Uses a 256-bit key
- Has 80-bit internal state and
- Simple logic and arithmetic operations.

Because it uses a small block size, it has minimum response time and power consumption requirements and is suitable for RFID tags or wireless sensors without any modification of the current standard.

Even though Hummingbird performs operations on short 16-bit block size, when compared to PRESENT, it has higher latency and execution time. So it has less encryption speed and is less efficient for authentication mechanisms.

Later Hummingbird-2 was designed which can optionally produce an authentication tag for each message. In comparison to its predecessor,

- It operates on 16-bit blocks
- The key size is 128 bit and
- Its internal state r, with size 128 bit, is initialized using 64 bit initialization vector iv.

To authenticate any associated data that travels with cipher text, Hummingbird-2 uses a method called Authenticated Encryption with Associated Data. Processing of associated data happens only after the processing of entire encrypted payload. For messages with size less than 16 bits it's better to communicate without message expansion. Advantage of Hummingbird-2 is its low power consumption and processing speed is faster.

F. Simon and Speck

Simon and Speck is a family of lightweight block ciphers developed by the National Security Agency (NSA) and released in June 2013. Simon and Speck algorithm aims to be generalist block cipher so that it can be recommended for future applications of IoT [14].

Even though Simon is optimized for hardware implementations and Speck is optimized for software implementations both have advantages such as:

- Offers excellent performance on hardware and software platforms
- Very simple constructed and so it is very easy to find efficient implementations.
- Flexible enough to construct a variety of implementations on a given platform, and
- Open to analysis using existing techniques.

Both Simon and Speck come with ten distinct block ciphers with differing block and key sizes. Simon is denoted as Simon2n, for 2n-bit block and n is required to be 16, 24, 32, 48, or 64. Simon2n with an m-word (mn-bit) key will be referred to as Simon2n/mn. For example, Simon64/128 refers to the version of Simon acting on 64-bit plaintext blocks and using a 128-bit key. The analogous notation is used for Speck. The range of block and key sizes goes from tiny to large: a 32bit block with a 64-bit key at the low end, to a 128-bit block with a 256-bit key at the high end.

G. LED

Light Encryption Device is a symmetric block cipher that is lightweight and can be implemented in hardware efficiently. A use case of LED is the secure storage and transmission of RFID tags. LED uses a block size of 64 bits.

The key length is 64 bit (LED-64) or 128 bit (LED-128). Even key length between 64 bit and 128 bit is possible in which case the remaining bits will be padded with the prefix of the key.

LED can be used for software implementation.

H. TEA

The Tiny Encryption Algorithm (TEA) was developed with the objective to be used on low-performing small computers. This block cipher is based on a high performance but mathematically simple encryption algorithm which are variants of a Feistel Cipher.

- TEA encrypts 64 bit blocks which are divided into 32 bit blocks.
- Uses a 128-bit length key.
- TEA is a round based encryption method. The number of the used rounds are variable but 32 Tea cycles are recommended.
- It is developed based on the assumption that security can be enhanced by increasing the number of iterations.

Even though TEA has 32 rounds, it is faster than DES with 16 rounds and all modes of DES are applicable with it. It can be implemented in all programming languages.

The XTEA (eXtended TEA) algorithm is a further development of TEA. It works with:

- 64 Bit blocks and
- 128 Bit key length
- 64 encryption rounds.

When compared to TEA, XTEA has a more complex key management and a change of the Shift, XOR and addition operations.

Along with XTEA, Block TEA was also released which differs only on the part that it doesn't require a fixed block size but can work with blocks of any size. Block TEA does not need an operation mode to ensure confidentiality and authenticity; and can be applied directly to the entire message

I. SEA

SEA (Scalable Encryption Algorithm) has fthe ollowing features

- Low memory,
- Small code size,
- Limited instruction set. And
- Flexibility to run on any platform as it can be parameterized according to processor size as well as plaintext size and key size

SEA, which is based on Feistel structure, is the most compact cipher due to use of 3-bit S-box. SEA is recommended for small encryption routines.

J. TWINE

TWINE, proposed by Tomoyasu [15, 16], is based on a Generalized Feistel Structure (GFS), which enables small implementations on hardware and software. It can be implemented in hardware with 1.5 KGates and low-end micro-controllers (due to its small memory consumption) but requires several iterations to make the resulting cipher sufficiently secure. To recover this drawback, TWINE employs an improved variant of GFS which results in making it to be ultra-lightweight while keeping sufficient speed.

TWINE is Type-2 generalized Feistel [20] with following features:

- 64 bits block size
- 36 rounds
- TWINE has two types - TWINE-80 and TWINE-128 where the key size is 80 bits and 128 bits respectively.

K. Other Algorithms

Other notable algorithms are listed below:

- Skipjack [17] is a lightweight block cipher based on an unbalanced Feistel network designed by U.S. NSA for embedded applications. It operates on 64-bit block length with 80-bit key.
- NOEKEON is a hardware-efficient block cipher by Daemen et al. [18].
- HIGHT was designed by Hong et al. [19] which a generalized Feistel-like cipher as it possesses 64-bit block length and 128- bit key length to be suitable for low-cost, low-power, and ultralight implementation and it undergoes 32-round iterative structure.
- By redesigning Crypton by compact implementation of both hardware and software, mCrypton is created.
- KeeLoq is a lightweight block cipher with a 32-bit block size and a 64-bit key proposed by Bogdanov in 2007. Despite its short key size, it is widely used in remote key less entry systems and other wireless authentication applications.

It has been noticed that block ciphers such as DESL, HIGHT, PRESENT are more suitable for resource constrained environments when compared to stream ciphers. KATAN, LED, SIMON; and PRESENT has been optimized for performance on hardware devices and SPECK, SEA and TEA for performance in software.

ATTACKS ON LIGHTWEIGHT CIPHERS

Cryptanalysis uses the weaknesses in cryptographic algorithms to breach their security and access the content of any cipher text. As discussed above, the main challenge in light weight algorithms is how to balance between low resources requirements in constrained devices, performance, and security. As a result, the risk content is more in light weight ciphers that need to be identified and analyzed before deployment and requires a lot of cryptanalysis work. In this section we survey the dedicated attacks on some light weight crypto algorithms:

A. DESL

DESL is more secure against certain types of linear and di erential cryptanalyses (attack based on how well differences in the input propagate to output differences) and the Davies-Murphy attack (dedicated statistical cryptanalysis method for attacking the Data Encryption Standard (DES)) because it uses a single S-box repeated eight times to minimize the probability of collisions at the output of the S-boxes and thus at the output of the f-function. But there is possibility to have a collision in three adjacent S-boxes leads to successful differential attack based on a 2-round iterative characteristic with probability 1/234 [21].

B. KATAN and KTANTAN

The KATAN and the KTANTAN families are secure against di erential and linear attacks (linear cryptanalysis is based on how well the algorithm transformation can be approximated by a linear mapping) but they are possible to be attacked by Slide Attacks (based on finding two messages such

that they share most of the encryption process given the fact that there is a difference between the deployed round functions) which is possible only for a very small number of rounds [22].

KTANTAN families are susceptible to Cube Attacks and Algebraic Attacks (Algebraic cryptanalysis solves linear and nonlinear equations on input, output and key variables using algebraic representations of the algorithm transformation [10]) by low algebraic degree of the combining function after 160 rounds.

C. *PRESENT*

In PRESENT, linear attacks were more successful in breaking more rounds than di□erential attacks [24] due to the following facts:

- Bitwise permutation of PRESENT
- The design criteria of the PRESENT s-box allows the existence of linear characteristics with one active s-box per round and prevents the existence of di□erential characteristics with one active s-box per round
- The existence of eight linear approximations in the PRESENT Sbox with input and output mask Hamming weight one

As it exhibits a particular weakness in its di□usion layer, the PRESENT cipher is targeted by statistical saturation attack proposed by Bogdanov et al. at CHES 2007 [25]. Also related-key attacks and slide attacks are two of the most effective attacks on PRESENT cipher [10].

D. *TEA & HUMMINGBIRD*

The simplicity of TEA key schedule (key size is only 126 bits) make it exposed to several attacks like equivalent keys attack which exploits the weakness that each key is equivalent to three others. TEA is also can be attacked by related-key and slide attacks. But these weakness points are modified in a new version called XTEA algorithm [10, 26].

Hummingbird cipher has a hybrid mode of block cipher and stream cipher and researchers in [27] analyze that it is resistant to the most common attacks to block ciphers and stream ciphers including birthday attack, di□erential and linear cryptanalysis. But other studies [10] proposed that there is a high probability that this cipher can be admitted to cube attack if the degree of the internal state transition function in a stream cipher is low.

E. *HIGHT (high security and light weight)*

HIGHT is exposed to saturation attack in which saturated multi-set of plaintexts is used, as the saturation characteristic (property of XOR sum should be known that XOR sum of particular parts of the corresponding cipher texts is zero) are found in block ciphers which applies on 16-round of HIGHT [10,28]. The Boomerang attack is another attack applicable on HIGHT [10].

As a conclusion for this section, attacks on lightweight ciphers is an important area that requires more focus as the era of IoT is strongly depended on security.

PERFORMANCE ANALYSIS OF LIGHT WEIGHT CIPHERS ON AN EMBEDDED PLATFORM

In case of large electrical or mechanical systems, there can be one or more computer systems, each taking care of a specific function. When these computers are embedded as part of a complete device, they are called embedded systems. Embedded systems are used in home automation to control lights, sensors, AV systems and also in GPS, ATMs, networking equipment, digital video cameras, mobile phones, aerospace applications, telecom applications, etc. Currently embedded system market is aiming to make certain transformations into their products to take advantage of IoT world. But the future of embedded systems and IoT lies in the advancement of technologies that enable faster communication with high interwoven connections between different devices.

The Raspberry Pi is an embedded Linux system consisting of a small single-board computer. The Raspberry Pi has built in booting and kernel building modules, and is especially well suited for teaching applications programming.

In this section we present the performance analysis of light weight ciphers on an Intel based laptop and on Raspberry Pi system. The cryptographic algorithms for which the performance analysis was conducted were TEA (32-bit), DESL, HIGHT2, KEELOQ, LBLOCK, PES and SKIPJACK. Tables 1 and 2 show the execution time and time per block for these light weight cryptographic algorithms. For each algorithm, 10,000,000 iterations were conduction to find the execution time on Intel based platform as well as Raspberry PI based platform except for DESL where only 1000 iterations were conducted.

TABLE 1: PERFORMANCE OF LIGHT WEIGHT ALGORITHMS ON WINDOWS PLATFORM

Cipher Name	Execution Time (sec)	Time per Block	Blocks per second
tea_32	0.112	1.12E-07	8.93E+06
Desl	0.003	3.00E-06	3.33E+05
hight2	0.686	6.86E-07	1.46E+06
Keeloq	2.3564	2.36E-06	4.24E+05
Lblock	1.112	1.11E-06	8.99E+05

Pes	0.646	6.46E-07	1.55E+06
Skipjack (encryption)	0.114	1.14E-07	8.77E+06
Skipjack (decryption)	0.126		

TABLE 2: PERFORMANCE OF LIGHT WEIGHT ALGORITHMS ON RASPBERRY PI PLATFORM

Cipher Name	Execution Time (Sec)	Time per Block	Blocks per second
tea_32	1.399904	1.40E-06	7.14E+05
Desl	0.20139	2.01E-04	4.97E+03
hight2	24.79685	2.48E-05	4.03E+04
Keeloq	27.52748	2.75E-05	3.63E+04
Lblock	10.46632	1.05E-05	9.55E+04
pes	5.09033	5.09E-06	1.96E+05
Skipjack (encryption)	1.58902	1.59E-06	6.29E+05
Skipjack (decryption)	1.64537		

The below figure 3 shows the graph derived from the above two tables indicating the execution time with respect to the light weight ciphers being analyzed. It can be noticed that execution time on the embedded Raspberry Pi is lot higher when compared to the Windows execution time. Even though keeloq and hight2 execution time is high it should be noticed that the number of iterations were 1,000,000 whereas the execution time of DESL was recorded just for 1000 iterations. So it is safe to assume DESL execution time is higher than the rest of these algorithms.

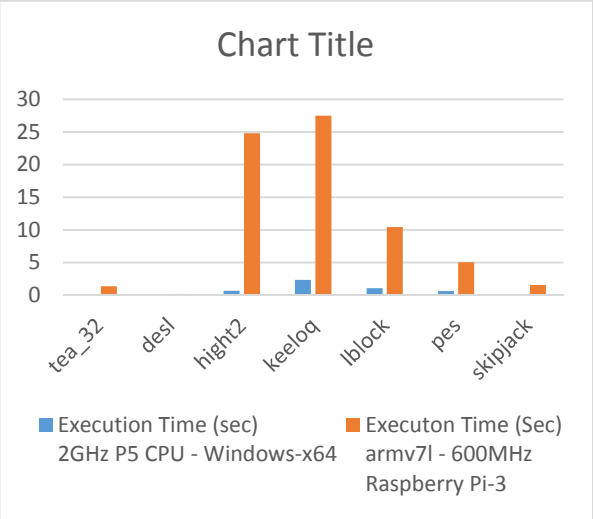

Figure 3: Execution time of Algorithms on Windows and Raspberry Pi

Time per block is calculated as execution time divided by number of iterations. When comparing the time per block of these algorithms, the chart in Figure 4 shows DESL on raspberry pi platform shoots up. But in case of Windows platform, DESL's time is somewhat within the range of other algorithms.

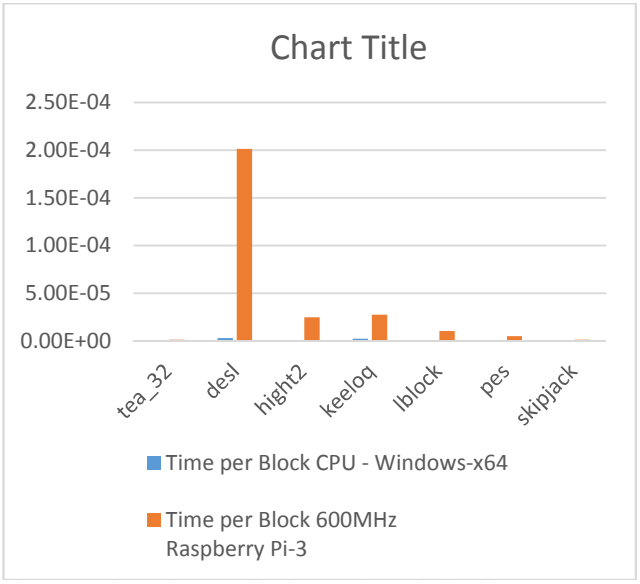

Figure 4: Time taken per block execution of Algorithms on Windows and Raspberry Pi

The reverse of time per block gives you the value of blocks executed per second. The Figure 5 graph clearly shows that the Windows platform output outperforms the embedded platform for these algorithms.

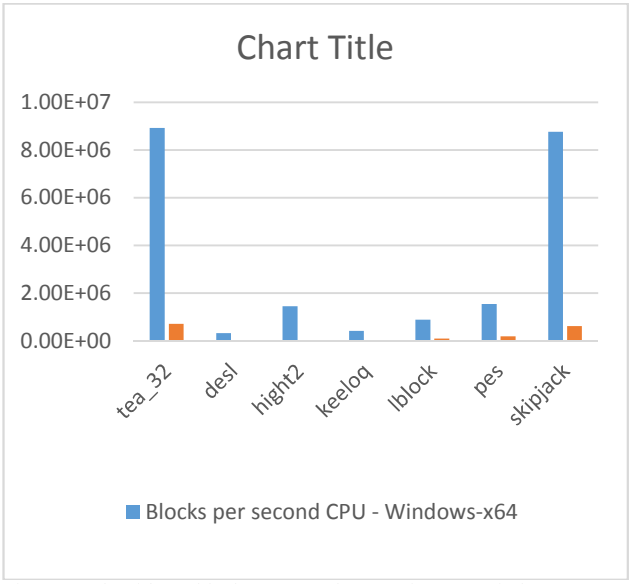

Figure 5: Algorithms' block per second comparison on Windows and Raspberry Pi platform

TABLE 3: COMPARISON OF EXECUTION OF ALGORITHMS ON WINDOWS AND RASPBERRY PI PLATFORM

Cipher Name	Blocks per second CPU - Windows-x64	Blocks per second 600MHz Raspberry Pi-3	Comparison Factor
tea_32	8.93E+06	7.14E+05	0.08

desl	3.33E+05	4.97E+03	0.01
hight2	1.46E+06	4.03E+04	0.03
keeloq	4.24E+05	3.63E+04	0.09
lblock	8.99E+05	9.55E+04	0.11
pes	1.55E+06	1.96E+05	0.13
skipjack	8.77E+06	6.29E+05	0.07

Finally, the Table 3 shows the comparison table for the light weight cryptographic algorithms on windows and embedded platform.

These charts and tables indicate that the light weight ciphers have better performance in Windows platform when compared to embedded platform. So there is a need of further more research in the area of light weight ciphers in embedded platform as we are looking to a future where IoT and Embedded systems can go hand-in-hand.

REFERENCES

[1] W. Stallings, Cryptography and Network Security, Prentice Hall, pp. 58-309, 4th Ed, 2005.

[2] Paar, Christof, Pelzl, Jan; Understanding Cryptography, A Textbook for Students and Practitioners; First Edition, 2010. ISBN 978-3-642-04100-6 e-ISBN 978-3-642-04101-3 DOI 10.1007/978-3-642-04101-3.

[3] Studying the Effects of Most Common Encryption Algorithms, Diaa Salama, Hatem Abdual Kader, and Mohiy Hadhoud Jazan University, Kingdom of Saudi Arabia Minufiya University, Egypt, International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011.

[4] Evaluating the Performance of Symmetric Encryption Algorithms, Diaa Salama Abd Elminaam1, Hatem Mohamed Abdual Kader2, and Mohiy Mohamed Hadhoud2, International Journal of Network Security, Vol.10, No.3, PP.213 {219, May 2010.

[5] Idrus.S.Z, Aljunid.S.A, Asi.S.M (2008), "Performance Analysis of Encryption Algorithms Text Length Size on WebBrowsers," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, PP 20-25.

[6] C. T. R. Hager, S. F. Midkiff, J. M. Park, and T.L. Martin, "Performance and energy efficiency of block ciphers in personal digital assistants," Third IEEE International Conference on Pervasive Computing and Communications, pp. 127-136, Mar. 8-12, 2005.

[7] Analytical Comparison of Cryptographic Techniques for Resource-Constrained Wireless Security, M. Razvi Doomun and KMS Soyjaudah, International Journal of Network Security, Vol.9, No.1, PP.82–94, July 2009.

[8] Enterprise IoT: Strategies and Best Practices for Connected Products and ... By Dirk Slama, Frank Puhlmann, Jim Morrish, Rishi M Bhatnagar first edition

[9] Lightweight Cryptography: Underlying Principles and Approaches International Journal of Computer Theory and Engineering, Vol. 3, No. 4, August 2011.

[10] Anjali Arora, Priyanka, Saibal Kumar Pal, "A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers," IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.2, April 2012

[11] J. Daemen. Cipher and hash function design strategies based on linear and differential cryptanalysis. Doctoral Dissertation, March 1995, K. U. Leuven.

[12] FIPS Publication 46-3. Data Encryption Standard (DES). U. S. Department of Commerce / National Institute of Standards and Technology. Reaffirmed 1999 October 25.

[13] R. J. Anderson, E. Biham, and L. R. Knudsen. Serpent: A Proposal for the Advanced Encryption Standard. Available at http://www.cl.cam.ac.uk.

[14] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. Simon and speck: Block ciphers for the internet of things. Cryptology ePrint Archive, Report 2015/585, 2015. http://eprint.iacr.org/.

[15] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi, "TWINE: A Lightweight, Versatile Block Cipher".

[16] Tomoyasu Suzaki, Kazuhiko Minematsu, Sumio Morioka, and Eita Kobayashi. TWINE: A lightweight block cipher for multiple platforms. In LarsR. Knudsen and HuapengWu, editors, Selected Areas in Cryptography, volume 7707 of Lecture Notes in Computer Science, pages 339–354. Springer Berlin Heidelberg, 2013.

[17] National Institute of Standards and Technology. Skipjack and kea algorithm specifications (version 2.0). NIST online document. Available http://csrc.nist.gov/groups/ST/toolkit/documents/skipjack/skipjack.pdf, May 1998.

[18] J. Daemen, M. Peeters, G. Van Assche, and V. Rijmen. The Noekeon block cipher. The NESSIE Proposal, 2000.

[19] D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B. Koo, C. Lee, D. Chang, J.Lee, K. Jeong, H. Kim, J. Kim, and S. Chee. HIGHT: A new block cipher suitable for low-resource device. In L. Goubin and M. Matsui, editors, Cryptographic Hardware and Embedded Systems – CHES 2006, volume LNCS 4249, pages 46–59. Springer, 2006.

[20] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In Gilles Brassard, editor, Advances in Cryptology CRYPTO 89 Proceedings, volume 435 of Lecture Notes in Computer Science, pages 461–480. Springer New York, 1990.

[21] Gregor Leander, Christof Paar, Axel Poschmann, and Kai Schramm, "New Lightweight DES Variants", RFIDSec '06, 2006.

[22] Christophe De Canni`ere and Orr Dunkelman, Miroslav Kne˘zevi´c, "KATAN & KTANTAN — A Family of Small and Efficient Hardware-Oriented Block Ciphers".

[23] A. Bogdanov, L.R. Knudsen, "PRESENT: An Ultra-Lightweight Block Cipher"

[24] Mohamed Ahmed A. M. A. Abdelraheem, "Cryptanalysis of Some Lightweight Symmetric Ciphers", Department of Mathematics in The Technical University of Denmark, December 2012.

[25] B. Collard and F.-X. Standaert, "A Statistical Saturation Attack against the Block Cipher PRESENT"

[26] B. Collard and F.-X. Standaert, David J.Wheeler, Roger Needham, "A Tiny Encryption Algorithm".

[27] Daniel Engels, Xinxin Fan, Guang Gong, Honggang Hu, and Eric M. Smith, "Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices."

[28] Peng Zhang1, Bing Sun1, and Chao Li1, "Saturation Attack on the Block Cipher HIGHT", Department of Mathematics and System Science, Science College of National, University of Defense Technology, Changsha, 410073, China.