A Survey of Cryptographic Algorithms for IoT Devices

Internet of things

The Internet of Things describes physical objects that are embedded with sensors, processing ability, software, and other technologies, and that connect and exchange data with other devices and systems over the Internet or other communications networks.

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, Lightweight cryptography, NOEKEON, PES, PRESENT, mCrypton, Raspberry Pi, RC2, RC6, RSA, SEA, Skipjack, Simon and Speck, Symmetric and Asymmetric algorithms, TEA, XTEA and TWINE

LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS

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

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

* DESL

is the lightweight version of classical DES algorithm and DESXL is a lightweight version of the DESX algorithm where both use 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

* 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 a 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

* 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 are 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 provide required nonlinearity. • They process small blocks of data which are from 32 to 64 bits; • KTANTAN’s key schedule is simpleKATAN & 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

* 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 have 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 the use of 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.

* 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

* 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 lowperforming 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. 5 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 the following 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

* TWINE

TWINE, 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 lowcost, 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.

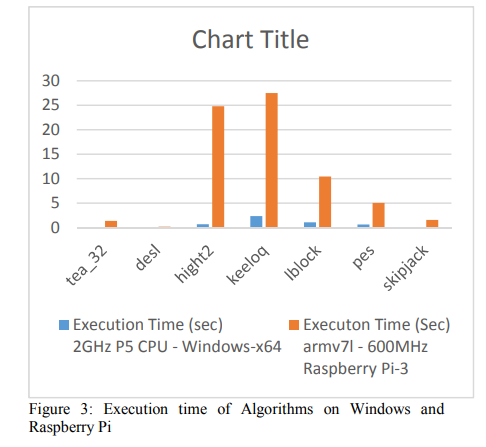
• KeeLoq is a lightweight block cipher with a 32-bit block size and a 64-bit key proposed by Bogdanov in 2007. Despite its short key size, it is widely used in remote key less entry systems and other wireless authentication applications. It has been noticed that block ciphers such as DESL, HIGHT, PRESENT 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

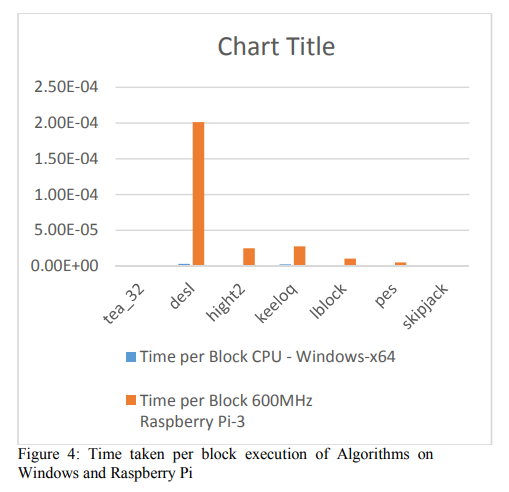
Cryptanalysis uses the weaknesses in cryptographic algorithms to breach their security and access the content of any cipher text. As discussed above, the main challenge in light weight algorithms is how to balance between low resources requirements in constrained devices, performance, and security. As 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.

PERFORMANCE OF LIGHT WEIGHT ALGORITHMS

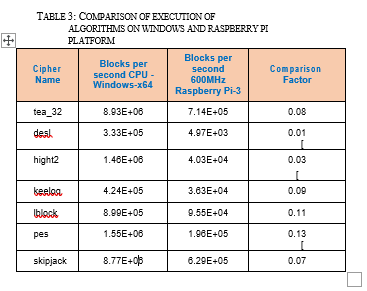
It can be noticed that execution time on the embedded Raspberry Pi is lot higher when compared to the Windows execution time. Even though keeloq and hight2 execution time is high it should be noticed that the number of iterations were 1,000,000 whereas the execution time of DESL was recorded just for 1000 iterations. So it is safe to assume DESL execution time is higher than the rest of these algorithms.

Execution time of Algorithms on Windows and Raspberry Pi 

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.

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

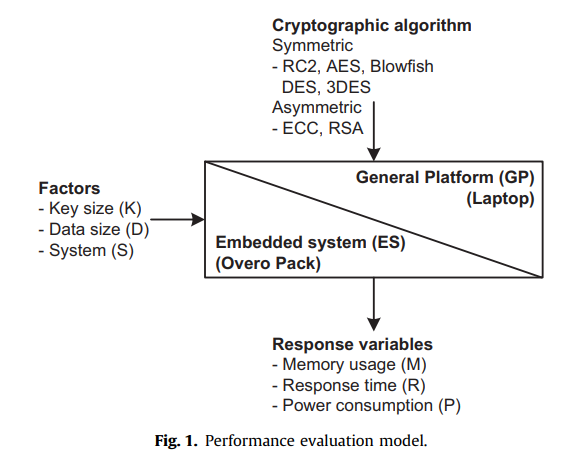
The reverse of time per block gives you the value of blocks executed per second. The Figure 5 graph clearly shows that the Windows platform output outperforms the embedded platform for these algorithms.

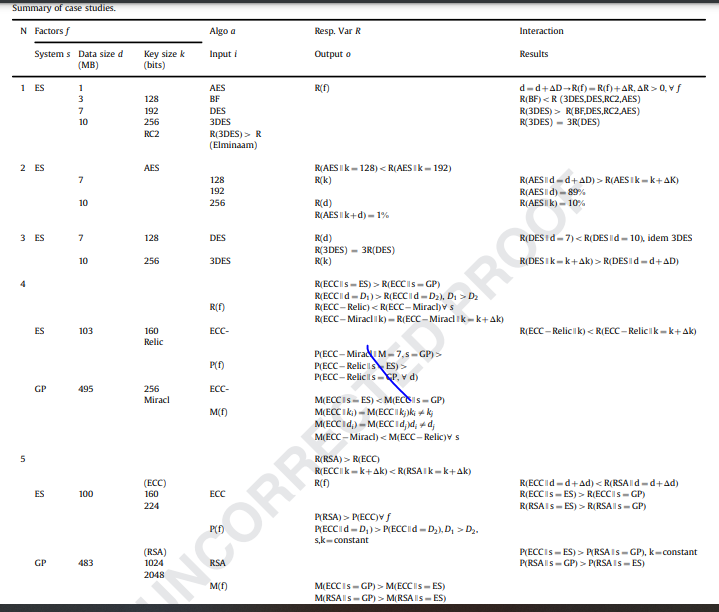
COMPARISON OF EXECUTION OF ALGORITHMS ON WINDOWS AND RASPBERRY PI PLATFORM

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

**Case studies of performance evaluation of cryptographic algorithms for an embedded system and a general purpose computer**

This paper presents a performance evaluation analysis of cryptographic algorithms in embedded systems (namely RC2, AES, Blowfish, DES, 3DES, ECC and RSA). Parameters considered in the analysis are average processor and memory usage, response time and power consumption. The results show that symmetric and asymmetric algorithms such as Blowfish and ECC have a good performance in embedded systems when properly chosen for each situation.

****

****

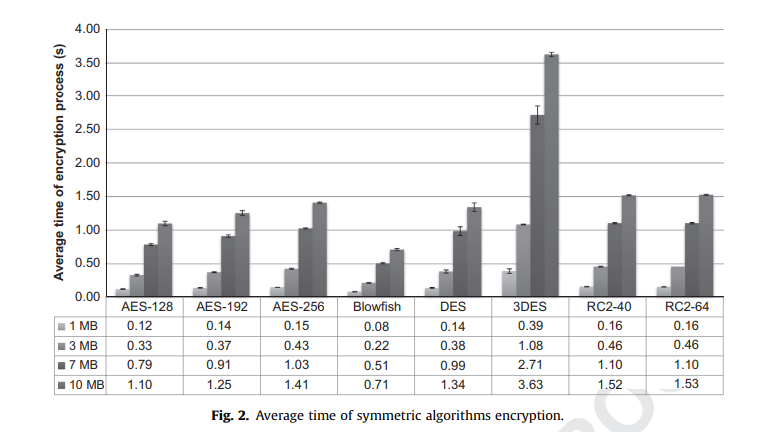
**As expected, as we increased the message (data) size the average response time has also increased.**

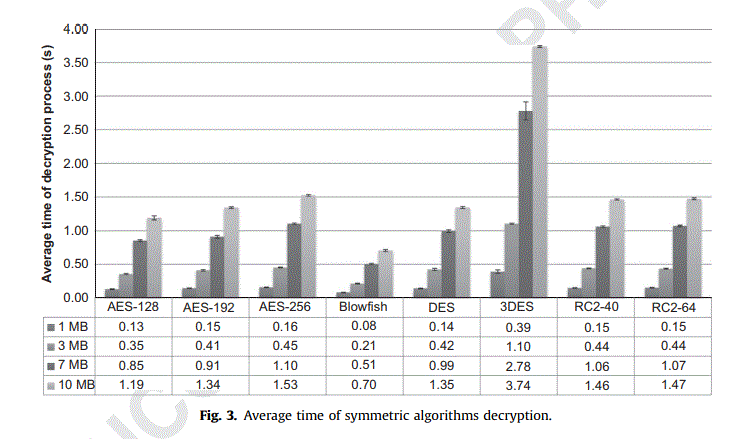
**Blowfish was the algorithm with the shortest response time.**

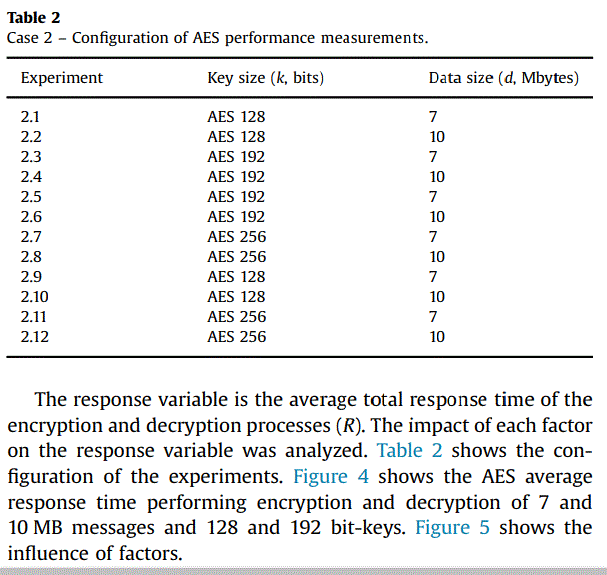
**3DES produced the largest response time from all algorithms compared.3**

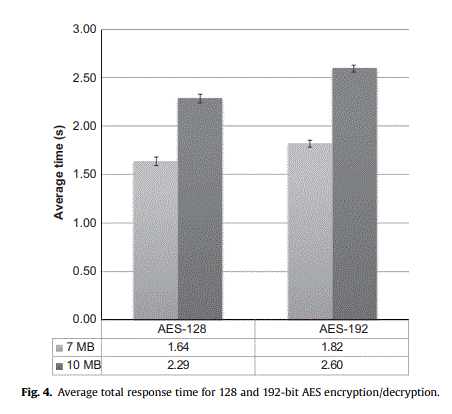
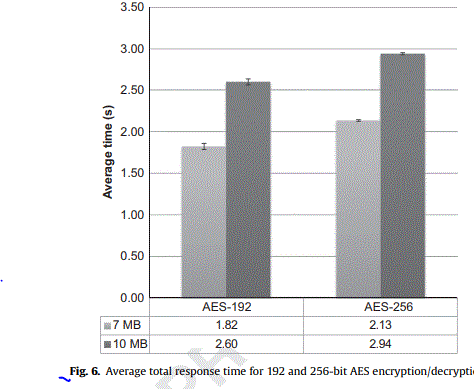
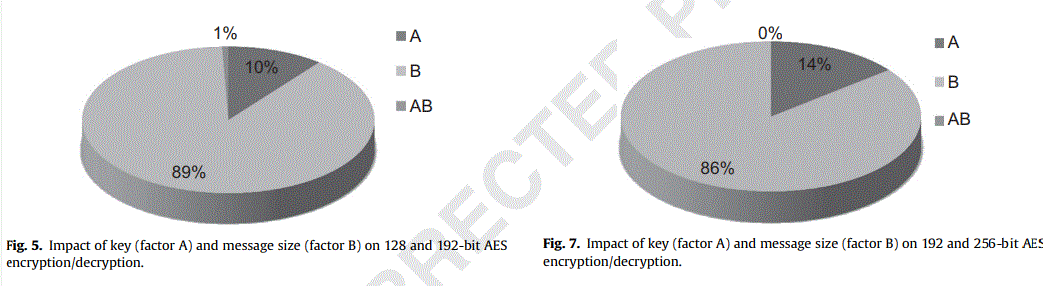
**3DES has a response time R three times larger than the one presented by DES, as shown in Fig. 2. This is due to the fact that the 3DES encryption process is composed of three steps: firstly, it encrypts data with key K1; secondly, it decrypts this data using K2; and finally, it encrypts the same data using K1 again or a third key K3. 4 The process of decryption does the opposite. Clearly, these three steps increase the security strength of the 3DES and solve the weakness (i.e. security limitations) of DES.**

**Naturally, the response time does not mean that an algorithm is better than the others. Once it is necessary to consider mathematical operations and the key size as part of the elements, those will determine the strength of an encryption solution. However, it is important to evaluate the time spent to process information because in some cases, less stronger solutions may be applicable even with smaller (footnote continued) confidence levels, whereas stronger solutions are not feasible due to the resourceconstrained system. 4 i.e. assuming that K1, K2 and K3 are three arbitrary keys.**



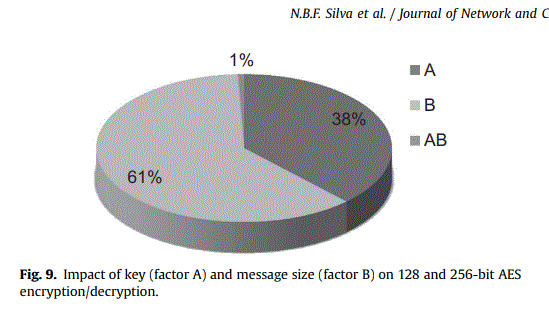
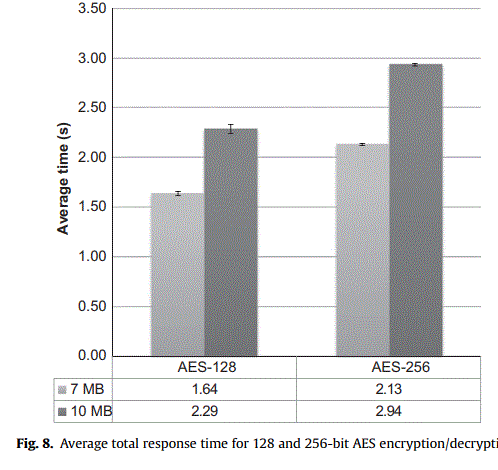


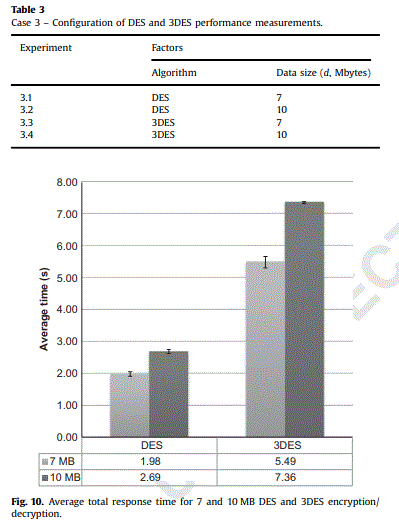


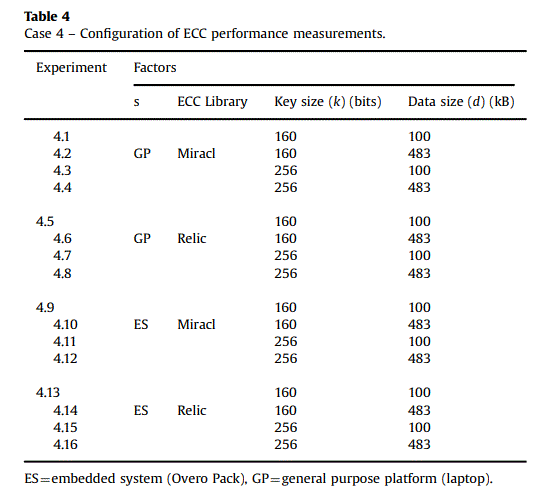
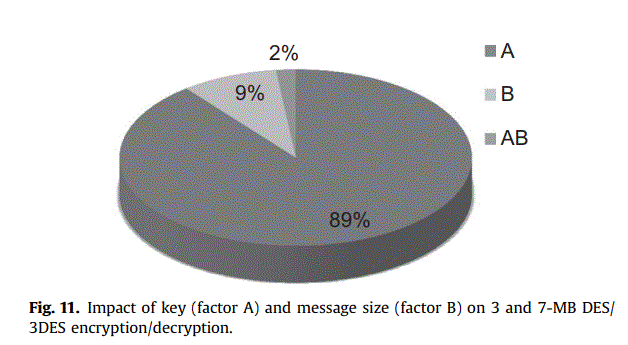


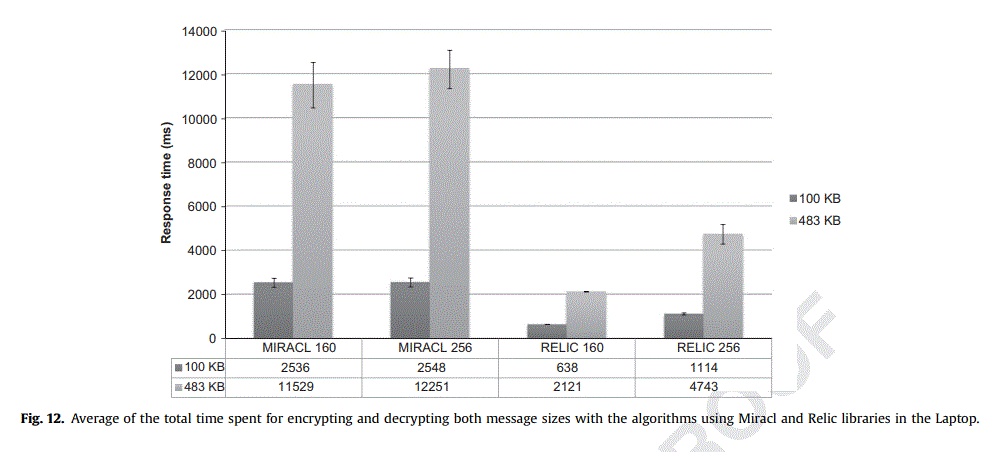
**We noticed the following behavior:**

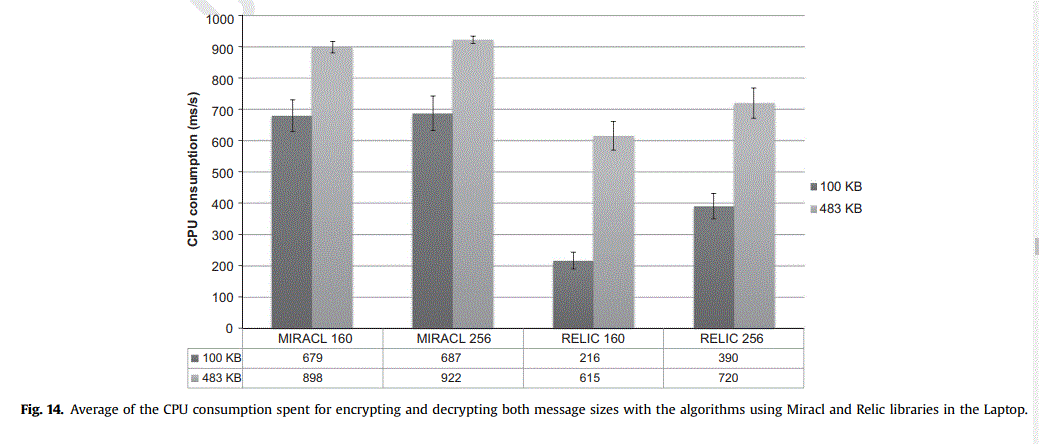
**As expected, it is possible to verify a small difference between AES-128 and AES-192 regarding the response time, due to the key size (i.e. increased reliability). Compared to key size, the data size (d) (i.e. message size) is the most prominent factor affecting the total response (Fig. 5). The 3 MB difference between messages justifies the impact of 89% on the result (since the encryption and decryption processes are relatively fast). Key size exerted an influence of 10%. The association of both factors (key size and message size) impacted only 1%.**

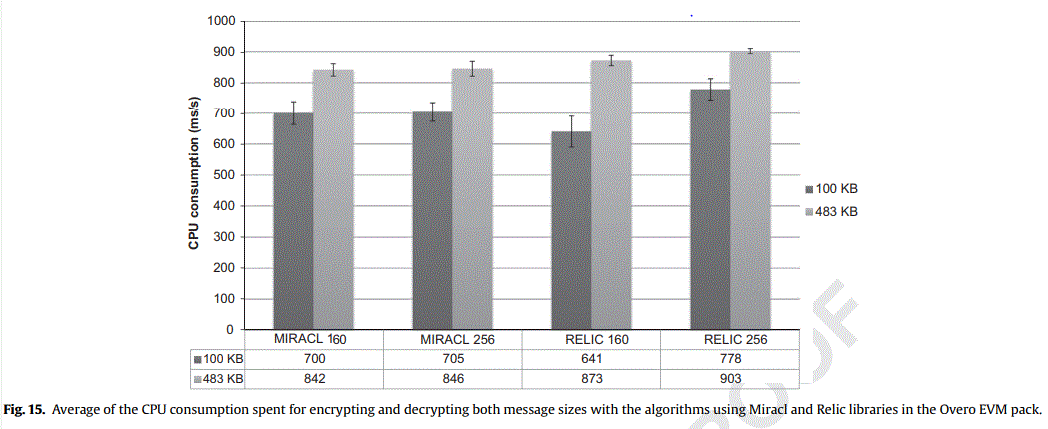
****

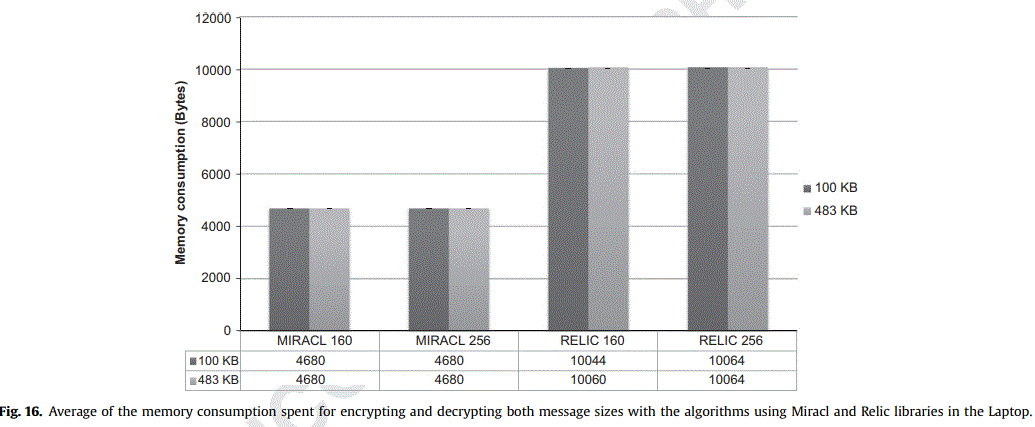
****

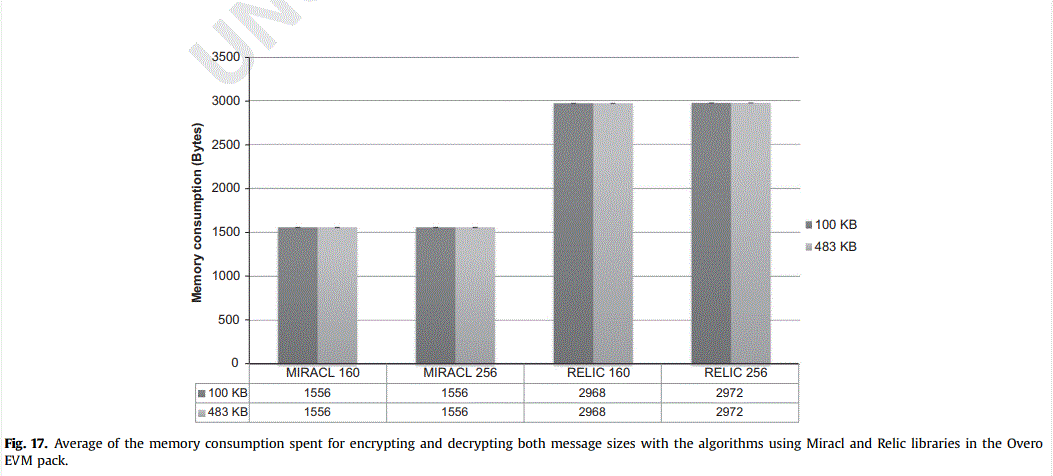
****

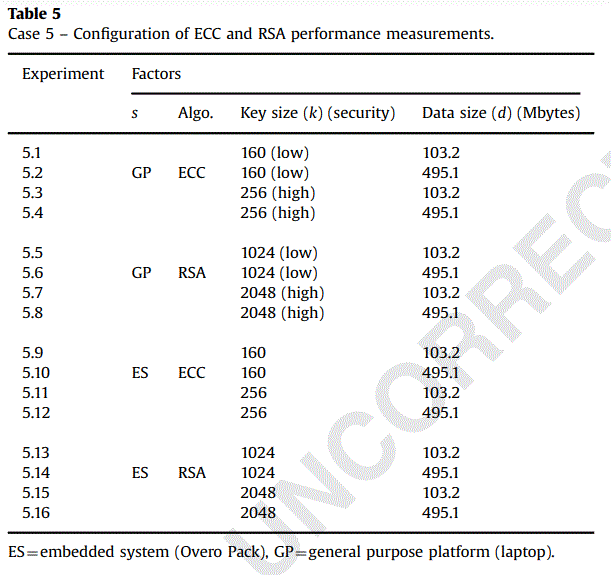
****

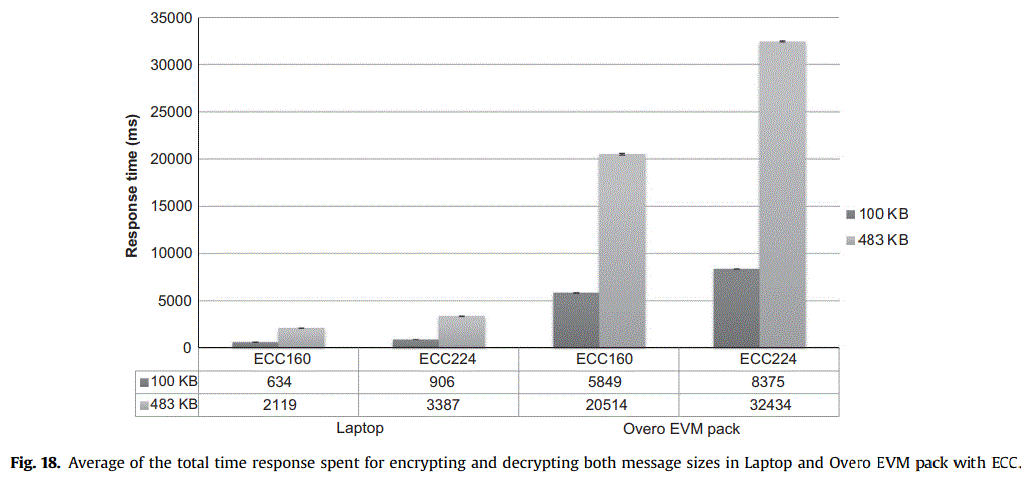
****

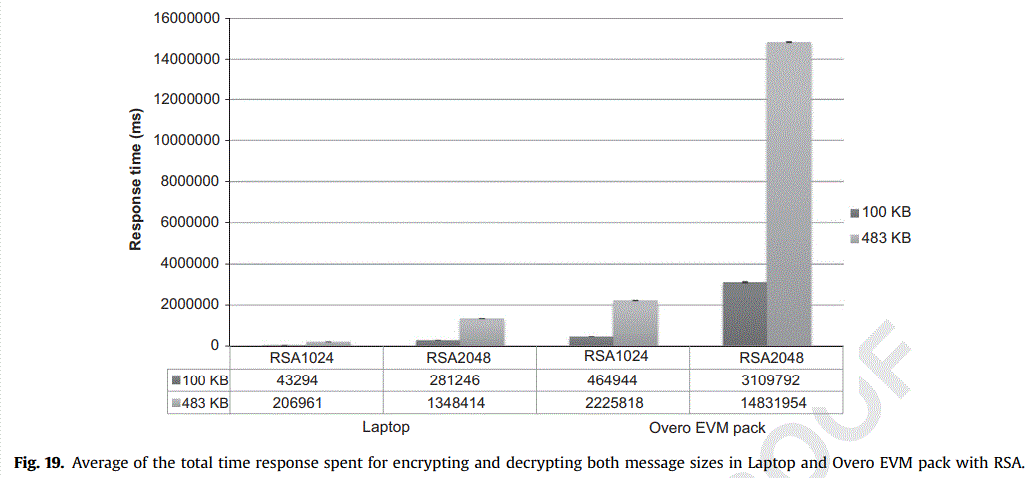
****

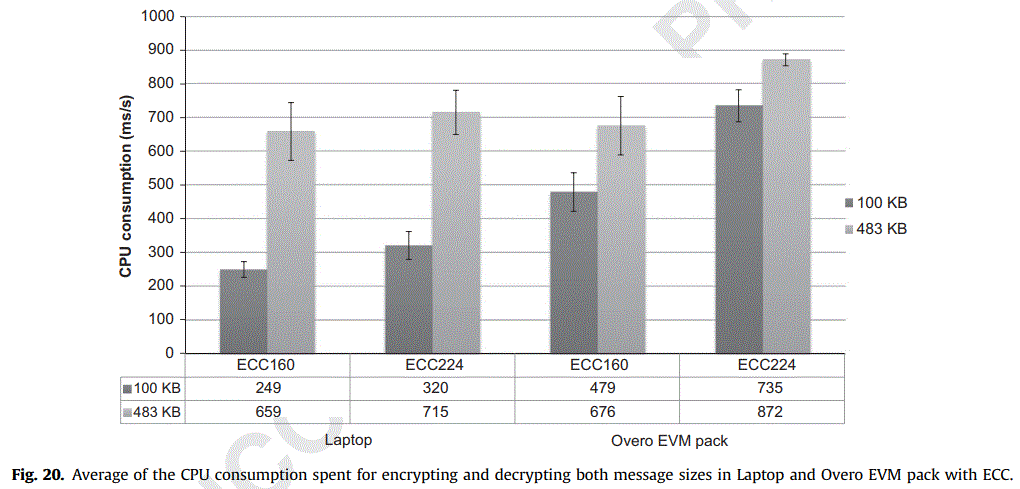
****

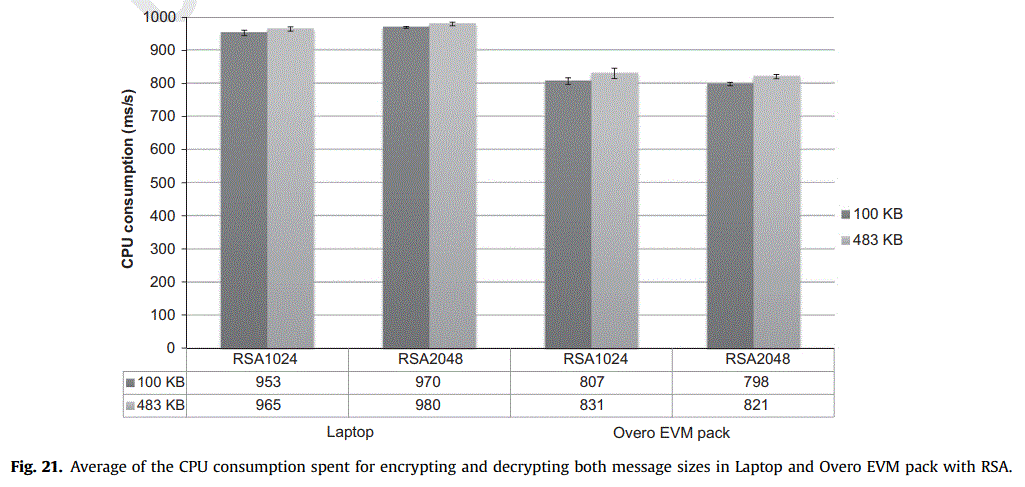
****

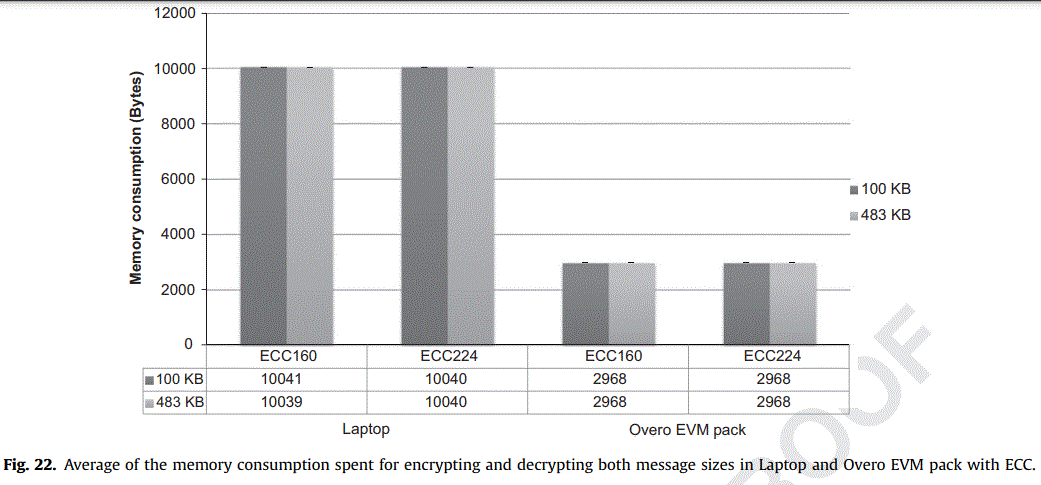
****

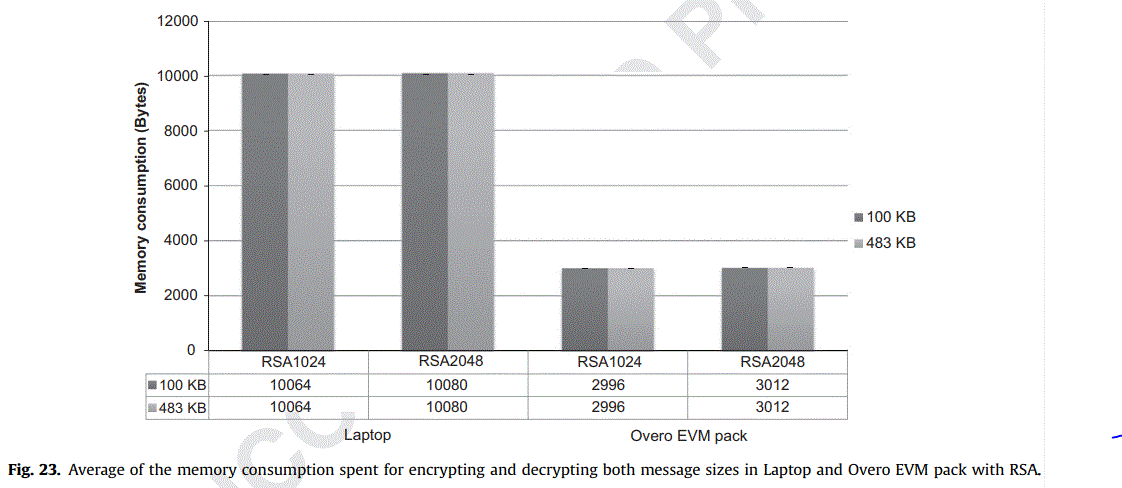
****

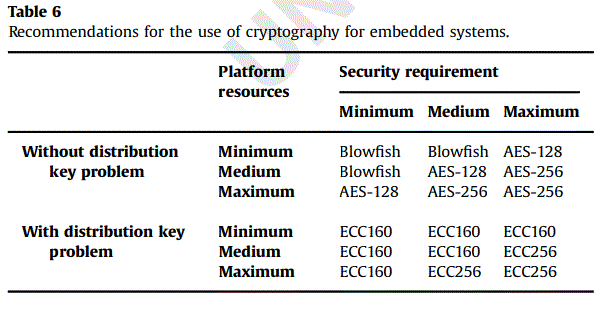
****

****

****

****

****

****

**A Survey on Lightweight Cryptographic Algorithms**

**The emergence of Internet of Things (IoT) devices is challenging the conventional design targets for integrated systems such as energy efficiency, cost, noise, and performance. With the prospected proliferation of IoT devices with 5G networks, ensuring safe margins for these design targets will become even more crucial due to the limited battery life and significant physical constraints.**

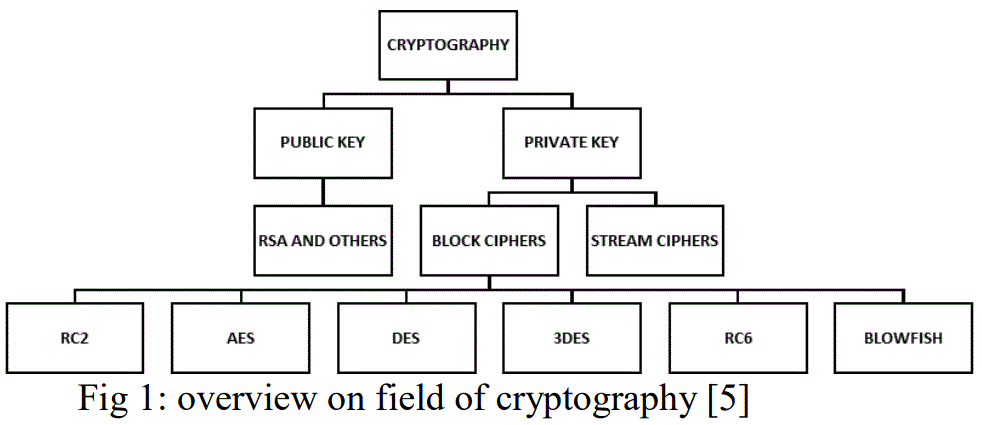
**IoT devices are quite vulnerable to hardware attacks since they are typically more accessible to an attacker as compared to the other general purpose computing devices.**

**a survey is conducted to compare between selected lightweight cryptographic algorithms. There are two types of lightweight cryptography algorithms know as block ciphers and stream ciphers, both are presented in this paper. Their security features and performances of hardware implementations are also analyzed.**

**A block cipher is an encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers. For example, a common block cipher, AES, encrypts 128 bit blocks with a key of predetermined length: 128, 192, or 256 bits**

**A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream. In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream.**

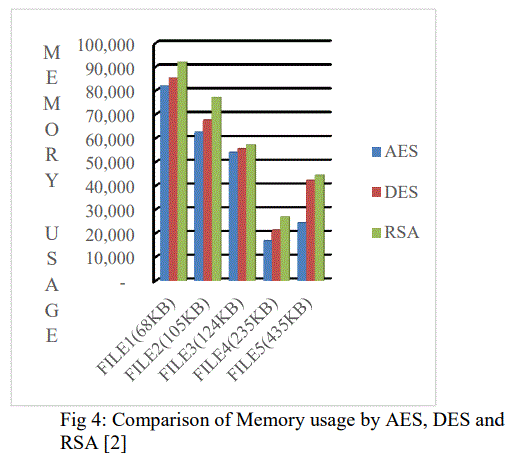
**Review of encryption algorithms First, we take a review of encryption algorithms. Encryption algorithms use either one of two techniques: Public Key or Private Key**

****

**Resources Consumption**

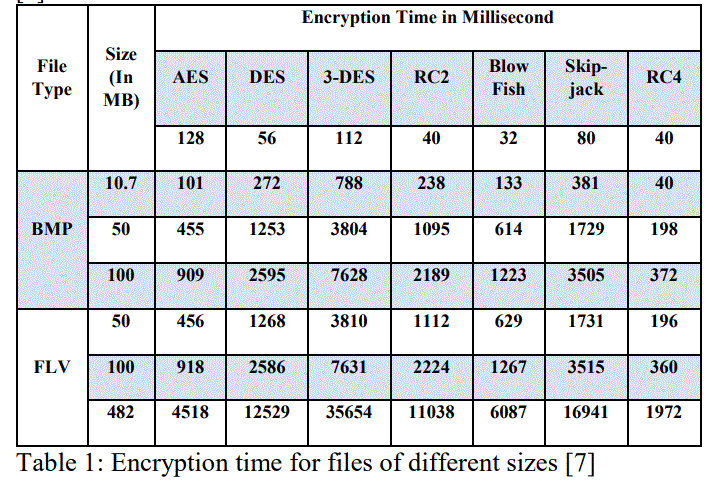
**Encryption algorithms consume a significant amount of computing resources such as CPU time, memory, and battery power. Battery technology is increasing at a slower rate than other technologies. This causes a “battery gap” F**

**LIGHTWEIGHT CRYPTOGRAPHY ALGORITHMS**

****

**Lightweight cryptography does not determine strict criteria for classifying a cryptographic algorithm as lightweight, but the common features of lightweight algorithms are extremely low requirements to essential resources of target devices, including the following: Size required for hardware implementation; Computational power of microprocessors or microcontrollers; Random access memory (RAM); Read-only memory (ROM) etc**

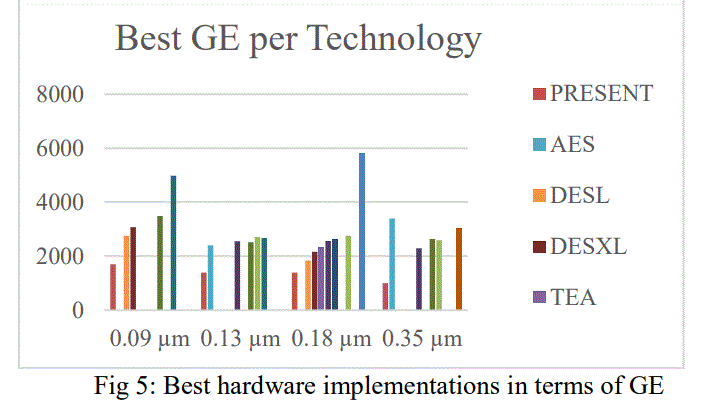
**Comparison Results**

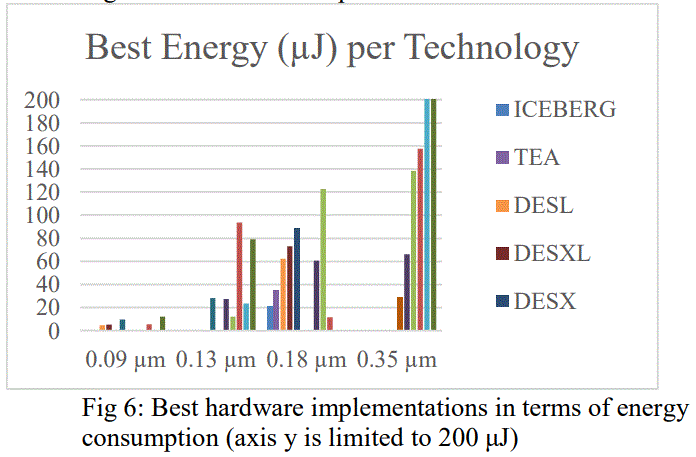
****

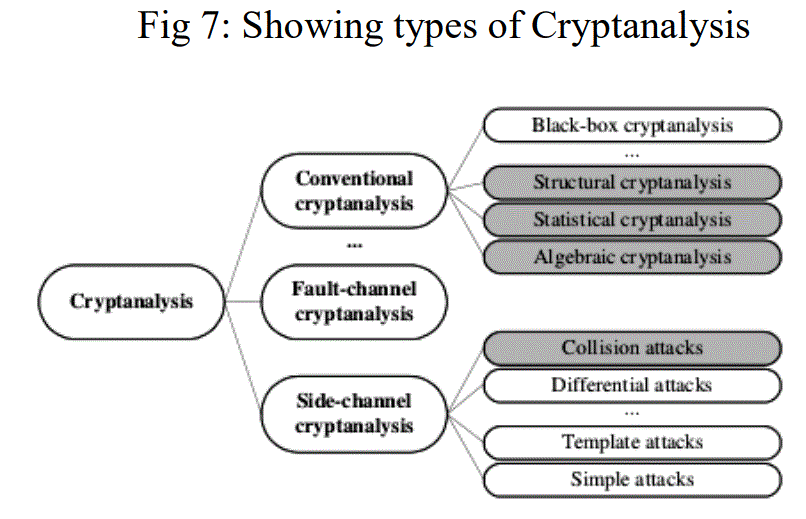
**The block ciphers presented in this paper are AES, DESL, DESX, DESLX, HIGHT, ICEBERG, CLEFIA, mCRYPTON, TEA, XTEA, and PRESENT. The stream ciphers presented in this paper are Trivium and Grain. Hummingbird is having the properties of both [13] [15]. In lightweight block ciphers minimizing the cost is the primary concern. That is why the cost is used in combination with performance and security to achieve the goal of lightweight block cipher**

**Comparison Results**

**All proposals for the cipher ICEBERG exceed the boundary of 3000GE and is, therefore, not considered efficient Fig 5. HIGHT, TEA, AES, DES, and DESX consume high energy per bit Fig 6. DESX, DES, and AES produce high latency (144/ 3720 cycles per block). DES, DESX, and HIGHT have higher power requirements than other ciphers. PRESENT, DESL, AES, CLEFIA, and XTEA, own inverse, f(f(x)) = x Proceedings of TENCON 2018 - 2018 IEEE Region 10 Conference (Jeju, Korea, 28-31 October 2018) 1786 consume also low power (around 2.5μW). DESL, DESXL, mCRYPTON, PRESENT, and CLEFIA consume low energy per bit (less than 10 μJ per bit). PRESENT achieve a good overall status. mCRYPTON exhibit low latency and efficient implementations. For lower security, DESL performs well. AES, PRESENT, CLEFIA, and DES variants are the most studied solutions and as a consequence the most acceptable ciphers. PRESENT and CLEFIA are the standardized block ciphers for lightweight cryptography**

****

****

****

**Lightweight and ultra-lightweight block ciphers are designed for various applications that are resource constrained in nature. These ciphers are designed keeping into consideration the very fact that there is a trade-off between how much power is consumed, how much chip area is used, how much time is consumed for encryption and decryption. In short, the speed and security are their primary features and a suitable tradeoff has to be provided for specific applications. According to changing requirements, several new and innovative designs in the last few years were proposed which used new cryptographic primitives and operations. These designs need to be critically analyzed before deployment.**

**Strongest Data Encryption Algorithms**

* **TripleDES.**
* **Twofish encryption algorithm.**
* **Blowfish encryption algorithm.**
* **Advanced Encryption Standard (AES)**
* **IDEA encryption algorithm.**
* **MD5 encryption algorithm.**
* **HMAC encryption algorithm.**
* **RSA security.**

**Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing**