ISSN 2395-1621

Survey on Efficient Cryptograghic Techniques and Lightweight Encryption Design

[#1]Shalini, [#2]Vidya Lokhande, [#3]Ravinder, [#4]Ashwini Veer, [#5]Prof. NiveditaKadam

[1]shaliniaug941@gmail.com
[2]vidyalokhande23@gmail.com
[3]decentravi94@gmail.com
[4]veer.ashwini8@gmail.com

[#1234]Department of Computer GHRCEM, G.H. Raisoni College of Engineering and Management, Pune

[#5]Assistant Professor of Computer Department, Department of Computer GHRCEM, G.H. Raisoni College of Engineering and Management, Pune

ABSTRACT

Lightweight cryptography is usually called as "the study of secret" that aims to target a very wide variety of devices and can be implemented on a broad range of hardware and software. The focus of lightweight cryptography is on studying new algorithms to overcome the problems that occur in standard cryptographic algorithms as these can be too big, too slow or too energy-consuming. Its implementation should be virtually light as a feather and must hit the perfect balance in providing security, low power consumption, higher throughput and compactness. In this paper we will focus on symmetric-key encryption, the genericsecurity of lightweight constructions, considerations on block cipher, block size and key size. We will also consider software based encryption and hardware based encryption.

Keywords- lightweight cryptography,encryption,decryption,block cipher, blocksize, key size, S-box

ARTICLE INFO

Article History

Received :4th January 2016

Received in revised form :

5th January 2016

Accepted : 6th January,2016

Published online :

6th January, 2016

I. INTRODUCTION

Nowadays, theconcerns about security have been increased due to use of prevalent and widespread devices in the field of electronics.After its human aid, information is an organization's most critical treasure and no framework security controls are 100% effective. As the priority and the value of traded data over the Internet or other media types are booming, the search for the best solution to offer the necessary protection against the data thieves' attacks along with furnishing these services under timely manner is one of the utmost active subjects in the security related communities. In a layered security model, it is much necessary to implement one final prevention control wrapped around sensitive information that is encryption.Efforts to protect systems and networks attempt to achieve three outcomes: data availability, integrity, and confidentiality. In embedded applications, implementing a fully developed cryptographic environment would not be empirical because of the restrictions like power dissipation, area and cost. Due to these constraints, the focus is on using lightweight cryptography that needs as less memory space as possible. The major facet of lightweight cryptographyis to accomplish the security-efficiency trade-offs deep-rooted in implementations of cryptographic algorithms.Cryptography is an art of turning something readable into something unreadable. It is a method of accumulating and imparting data in a particular form so that only those for whom it is planned can read and process .it employs complex mathematics and logic to design strong encryption methods. Cryptography is important because it prohibits criminals from larceny of the information online. When we see a website with HTTPS protocol enabled, that is cryptography at work. It is also at work when you log onto a wifi hotspot or encrypt a file.

The main criterion for the lightweight cipher is to have less memory space and that which would result into a less Gate Equivalent (GEs) count for an efficient hardware implementation without compromising the requirement of strong security properties. An ISO/IEC standard on lightweight cryptography requires that the design be made with 1000-2000 gate equivalents (GEs). For security applications, total GEs available would be approx 2000-3000. Block ciphers should be limited to less GEs in order to fit in lightweight applications.

II. BASIC DEFINITIONS

Encryption:

Encryption is the process of encoding(hiding) the information in a way that only authorized persons can read it that is, the plain text is encoded(encrypted) using an encryption algorithm, generating the cipher text that can only be read if it is decrypted.encryption is being used in military,government and most of the civilian systems to facilitate secret communication and is mainly classified as symmetric key encryption and public key encryption.

Decryption:

Decryption is the process of taking encoded or encrypted text or data and converting(unhiding) it back into text that we or our computer can read and understand. It requires a secret key or password

Cipher:

A cipher is an algorithm for performing encryption.

Decipher:

A cipher is an algorithm for performing decryption.

Block size:

The block size is the smallest size on disk a file can have. If you have a 16 byte Block size,then a file with 16 bytes size occupies a full block on disk.

Block Cipher:

a block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks, with an unvarying transformation that is specified by a symmetric key.it determines how much information we can send before we start having identical blocks.

Key size:

In cryptography, key size or key length is the size measured in bits of the key used in a cryptographic algorithm.

Rounds:

When the techniques or operations like substitution, permutation etc. are used a number of times in iterations called rounds.

S-BOX:

These are basically non-linear substitution tables which basically introduces non-linearity into the encryption so that decryption will be computationally infeasible without the secret key.

III. SOFTWARE BASED AND HARDWARE BASED ENCRYPTION

Software-Based Encryption

software encryption programs can help protect data and provide a good first line of defense but they are vulnerable to a number of decryption attacks. It shares computers resources to encrypt data with other programs on the computer andUses the user's password as the encryption key that creates confusion and makes it difficult to decrypt the data. It can require software updates.responsive to brute force attacks, computer tries to bound the number of decryption endeavor but hackers can access the computer's memory and reset the attempt counter.software based encryption can be economical and profitable in small application environments and it can be implemented on all types of media

Hardware-Based Encryption

Uses the committed processor physically located on the encrypted drive and Processor contains a random number generator to generate an encryption key, which is user's password will unlock, it shield keys and critical security parameters with in crypto_hardware. Authentication takes place on the hardware.It is more profitable in medium and larger application environments and easily adjustable. The Protection against most common attacks, such as cold boot attacks and brute force attacks, Hardware-based encryption offers the stronger defense against the threat models, and it is now available on the new generation of portable data security and authentication devices.

IV. TECHNIQUES

1. DES(data encryption standard)

For more than three decagon, the Data Encryption Standard (DES) was one the mostExtensively used cryptographic algorithms[4][5]. It is still the domineering block cipher for banking applications.it was first published in 1977.it is a symmetric block cipher. Its block size is 64 bit and key length is 56-bits.it was mainly developed for government

communication.DES was originally practical only in hardware implementations.it uses fiestal network that is it divides the block into two halves before going through the encryption steps. Maximum amount of data that can be transferred with a single encryption key is 32 GB.

DES I challenge- it took 85 days to crack the message.
DES II challenge – it took 3 days to crack the message.
DES III challenge- it took 22 hours and 15 minutes to crack the message.

2. **AES(advanced encryption standard)**

It was the first published in year 2001 and it is more mathematically efficient cryptographic algorithm. It is main strength rest in option for various key lengths. It allows to choose 128-bit, 192-bit, or 256-bit key.it is more exponentially stronger than 56-bit key.it uses Permutation-Substitution that involves a series of substitution and permutation steps to create the encrypted block. Substitution is a simply mapping of one value to be another and permutation is the re-ordering of the bit positions for each of the inputs.there can be 2^128,2^192, 2^256 combinations of the key. Maximum amount of data that can be transferred with the single encryption key is 256 billion gigabytes.

3. RSA

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman introduced a cryptographic algorithm
It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also termed aspublic key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the case that finding the factors of an integer is toughthe factoring problem. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message.

4. Hummingbird Algorithm

Hummingbird is a brand-new acutelylight cryptographic algorithm intended for resource forced devices such as Radio Frequency Identification (RFID) tags, smart cards and wireless sensor nodes.it is a search algorithm used by Google.AES algorithm takes more time as compared to hummingbird algorithm. So hummingbird algorithm encrypts and decrypts thebits faster.

Name of the cryptographic algorithm	Key size	No of bits applied	Total no of clock cycles Required to encrypt and decrypt are
AES	128	128	1616
16 BIT HUMMINGBIRD	64	16	4
256 BIT HUMMINGBIRD	1024	256	16

1. CLEFIA

CLEFIA[11][14] is a elixir block cipher algorithm. Its name is taken from the French word clef, meaning "key". The block size is 128 bits and the key size can be 128 bit, 192 bit or 256 bit. It is intended to be used in DRM systems. It is one of the cryptographic techniques referred as candidate for government use by the japanese.

Key size	**Block size**	**Structure**	**Rounds**
128,192,256	128	Fiestal network	18,22,26

1. PRESENT

PRESENT [2][7][9]is an engineered cipher whose S-box is the most compact substitution box among all the light variants and has good linear and differential properties. PRESENT's S-box results in a very compact implementation that consumes merely 21 GEs for a single 4 bit S-box. RAM and Flash memory requirements for PRESENT-GRP implementation results in very less bytes as compared to other lightweight algorithms and even with PRESENT individually. The theorem which shows the effect of differential cryptanalysis on S-box of PRSENT is that "Any five differential characteristics of PRESENT has a minimum number of ten active S-boxes" and results from papers [5]shows that PRESENT has very good and compact S-box. There are 16 Sboxes of PRESENT which are divided into four groups. From papers [5], the characteristics of S-box are outlined below:

1.The input bit to an S-box comes from 4 well defined-boxes of the same group.

2. The input bits to a group of four S-boxes come from 16 different S-boxes.

3. The four output bits from a particular S-box enter into four well defined S-boxes, each of them
belongs to a distinct group of S-boxes in the subsequent round.

4. The output bits of S-boxes in distinct groups will be fed to distinct S-boxes.

V. RELATED WORK

There are many new symmetric ciphers. Forexample, Hight, Clefia, DESXL, and Present—with Special implementation properties proposed. High was designed with good hardware performance in mind. In theirpaper, the authors provide hardware figures for a one roundimplementation—that is,

one round is performed in one cycle and they conclude that Hight is well suited for ubiquitous computing devices such as wireless sensor nodes and RFID tags .t Hight requires marginally the same chip size as the Advanced Encryption Standard (AES) algorithm (3,048 versus 3,400 gate equivalents, or GEs) but is much faster. However, figures for implementations with a smaller footprint in hardware are not yet available. Clefia was designed with a broader application range in mind that is to perform well in both hardware and software implementations. GRP [11] is one of the most complicated bit permutation instructions that make it an obvious choice to be used in cryptographic environment. GRP performs n bit permutation with log2(n) steps while other instructions take O(n) steps [5]. Research in this field and papers [11] have shown the increased strength of cipher RC5 by introducing GRP instructions. GRP scales very efficiently to 2n bits on n bit system by using instruction Shift right pair instruction (SHRP) in PA, RISC and in IA-64processors. Table look up is the second option to bit permutation instructions, but it is slower as it takes 16 cycles on a superscalar processor for the scheduling of permutation instructions, while GRP does it in only 8 cycles. By loading control bits, GRP requires 13 numbers of instructions while a table lookup needs 31 numbers of instructions. Bit permutation instructions are difficult sub word permutation that makes them best suitable in securing an environment. The use of bit permutation instructions like GRP and OMFLIP is useful to design efficient and secure ciphers. Ciphers such as DES, and TWO-FISH uses bit Permutation instruction in its operation. Bit permutation instructions are very effective in obtaining diffusion operation [11].

VI. PROPOSED SYSTEM MECHANISM

Cyber-attacks are continuously emerging, so security specialists stay busy in the lab adding some new schemes to keep them at bay. it is protecting our email communications or stored data, some type of encryption must be included in the lineup of security tools. Successful attacks on the victims show that there is no algorithm 100 percent bulletproof, but without it, we would be offering up convenient access to our data. Because of the embedded systems having limited computing resources and strict power requirements, writing software for embedded devices. It is very specialized field that will requires knowledge of both hardware components and programming. Embedded system security is often the reduction of vulnerabilities and protection against the threats in the software running on embedded devices. Here, we will propose the system whose aim is to provide high level security to be critically important emails that is to textual data by means of the applying lightweight encryption methods. System will be use the hardware based on encryption for the embedded security to overcome the drawback which is occur in most conventional software based encryption techniques.Our focus is on maintaining the time and space complexity of the algorithm and most importantly to reduce the gate equivalents (GE) to make encryption process as efficient and fast as possible. Here we are going to introduce dynamic key generation system which is missing in most of the lightweight encryption algorithms. Proposed system uses symmetric key cryptosystem. That is, the key will be generated from the data itself and it will be a dynamic activity. Basically, we are going to design a circuit using logic gates(mainly EX-OR gate) that will be responsible for calling the key generator and combining the key with the plain text to generate the cipher text(encrypted data).the circuit will then be simulated into a software based circuit using the same logic gates but this time using a programming language.

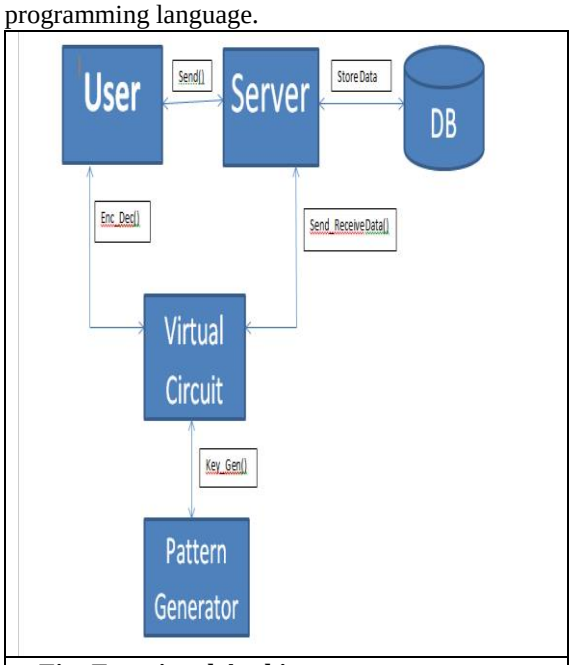

Fig: Functional Architecture

Block ciphers is to be used in the proposed system.GRP (group operation) implementation and use of s-box (required for the substitution in the bits) for creating the obscurity in the data is being employed in the proposed system so that the potential attacker gets confused during the cryptanalysis and fails to recognize the secret key and decrypt the encrypted data back to the plain-text. Also, the proposed system employs Bit permutation instructions which increasesstrength of a block cipher by allowing them to perform any arbitrary permutations efficiently with 'log(n)' steps as compared to 'n'that performs fast bit permutation.

I. Conclusion:-

The paper gives the survey on various lightweight data encryption techniques which is having deep explanation of the how we are going to implement the encryption technique through the system architecture . how to add cryptographic strength to the cipher and also reduce the memory requirements and power. we can provide the stronger and reliable security to highly confidential and private information being transmitted between various applications like, based on military, other government communications, email communication etc.

VII. ACKNOWLEDGMENT

We would like to thank our guide and various technological experts who researches about lightweight encryption techniques and improve the result by implementing new

methods. We would also like to thank Google for providing details on different issues on cryptography and about other related areas and detailed information of encryption and decryption.

VII. REFRENCES

1.K. Finkenzeller, "RFID Handbook: Fundamentals and Applications inContactless Smart Cards and Identification, 2003 John Wiley & Sons.Ltd," ISBN: 0-470-84402-7.

2."Implementation of a New Lightweight Encryption Design for Embedded Security", GauravBansod, NischalRaval, Narayan Pisharoty,2014

3.A. Juels and S. A. Weis, "Authenticating pervasive devices with humanprotocols," In Advances in Cryptology–CRYPTO 2005, pages 293-308.Springer Berlin Heidelberg, 2005.

4.National Bureau of Standards (NBS), "Data Encryption Standard(DES)," Federal Information Processing Standards Publication 46-2,December 1993.

5.National Institute of Standards and Technology, "Data Encryption
Standard (DES)," FIPS 46-3. Available via http://csrc.nist.gov, October
1999.

6.T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel, "ASurvey of Lightweight Cryptography Implementations," IEEE Design &Test of Computers – Special Issue on Secure ICs for Secure EmbeddedComputing, 24(6): 522-533, November/December 2007.

7.A. Bogdanov, G. Leander, L.R. Knudsen, C. Paar, A. Poschmann,M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT - An Ultra-Lightweight Block Cipher," In P. Paillier and I. Verbauwhede, editors,Cryptographic Hardware and Embedded Systems — CHES 2007,number 4727 in Lecture Notes in Computer Science, pages 450-466.Springer-Verlag, 2007.

8.Z. Shi and R. B. Lee, "Bit permutation instructions for acceleratingsoftware cryptography," In *Proceedings of the IEEE InternationalConference on Application Specific Systems, Architectures andProcessors (ASAP 2000)*, pages 138-148, July 2000.

9.A. Bogdanov, G. Leander, L.R. Knudsen, C. Paar, A. Poschmann,M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT - An Ultra-Lightweight Block Cipher," In P. Paillier and I. Verbauwhede, editors,*Cryptographic Hardware and Embedded Systems — CHES 2007*,
number 4727 in *Lecture Notes in Computer Science*, pages 450-466.Springer-Verlag, 2007.

10.A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann,M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultralightweightblock cipher," In *CHES*, Vol. 4727 of *LNCS*, pages 450-466.Springer, 2007.

11.Zhijie Jerry Shi, "Bit Permutation Instructions:Architecture, Implementation andCryptographic Properties", Princeton, June2004.

