IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume Vol. 8, Issue 3, March 2019

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.249

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

Light Weight Cryptography Algorithms for Securing IOT Devices

Dr. Rajendra Kumar Bharti

Associate Professor, Computer Science & Engineering, Bipin Tripathi Kumaon Institute of Technology, Dwarahat, Uttarakhand, India

ABSTRACT: The internet of things (IoT) revolution has been sparked by the exponential increase in connected devices caused by recent advances in wireless technology. These embedded devices gather, analyze, and send vast data via the network. Data transmission security is a primary problem in IoT networks. Several lightweight encryption/decryption algorithms have been developed for such resource-constraint devices. One of most effective and fast lightweight encryption algorithms for IoT applications is the Tiny Encryption Algorithm (TEA). TEA has few lines source of codes to implement and based on Feistel structure to provide cryptographic primitive confusion and diffusion features in order to hide statistical aspects of plaintext. However, it is vulnerable to assaults using equivalent and related key attacks. This study suggested modifying TEA by employing a new proposed generating keys function using two Linear Feedback Shift Registers (LFSRs) as a combination to address the security flaw caused by utilizing different keys for each round function. The key sensitivity, Avalanche effect, and a completeness test were used to evaluate its security performance. The key sensitivity of the proposed modified TEA outperforms original TEA by 50.18 % to 44.88 %. The modified TEA avalanche effect outperforms TEA by 52.57 % to 47.69 %, and its completeness test outperforms TEA by 51.75 % to 48.36 %. Experimental results indicates that, the encryption performance of proposed modified TEA is better than original TEA.

KEYWORDS: IoT, data, security, cryptography, light weight, alogarithms, devices, TEA, LFSRs, avalanche, encryption

I. INTRODUCTION

IoT is becoming more common and popular due to its wide range of applications in various domains. They collect data from the real environment and transfer it over the networks. There are many challenges while deploying IoT in a real-world, varying from tiny sensors to servers. Security is considered as the number one challenge in IoT deployments, as most of the IoT devices are physically accessible in the real world and many of them are limited in resources (such as energy, memory, processing power and even physical space). In this paper, we are focusing on these resource-constrained IoT devices[1] (such as RFID tags, sensors, smart cards, etc.) as securing them in such circumstances is a challenging task. The communication from such devices can be secured by a mean of lightweight cryptography, a lighter version of cryptography. More than fifty lightweight cryptography (plain encryption) algorithms are available in the market with a focus on a specific application(s), and another 57 algorithms have been submitted by the researchers to the NIST competition recently.[2] To provide a holistic view of the area, we have compared the existing algorithms in terms of implementation cost, hardware and software performances and attack resistance properties. Also, we have discussed the demand and a direction for new research in the area of lightweight cryptography to optimize balance amongst cost, performance and security. The footprint of the lightweight cryptographic primitives is smaller than the conventional cryptographic ones. The lightweight cryptographic primitives would open possibilities of more network connections with lower resource devices.

A comparison of the lightweight properties with the conventional cryptographic primitives . The comparison in Appendix focuses on hardware properties. Some end-nodes might be able to embed general-purpose microprocessors and software properties are considered important in such platforms. However, lowest cost devices can embed only

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

application-specific ICs due to limited cost and power consumption, where hardware properties are crucially important. Privacy should be an overall priority in smart cities. As it is a new concept for modern societies, privacy is a paramount element to establish smart cities in public opinion. The new technologies should be able to provide confidence to the users, who subsequently will adopt the services offered to them .[3]

Key management will have a prominent role in securing privacy during the authentication process. Especially in the IoT era, lightweight cryptography schemes are necessary to reduce latency and resources. Recently, various lightweight cryptographic primitives have been introduced to substitute the conventional algorithms such as block ciphers, hash functions, and stream ciphers. The proliferation of the connected devices drives the urgency for more flexible solutions in the authentication of users. The performance advantages of lightweight ciphers provide smaller block and key sizes, as well as simpler key schedules.Such schemes can be applied in various aspects of the IoT, apart from machine to machine authentication. Wireless networks could make use of the technology as energy consumption, overhead control, and reduced packet loss rate are key factors for performance enhancement .[4]

Different types of cryptographic solutions are available to protect our important data, but unfortunately, not all of them are suitable for resource-constrained environments like IoT devices.

Both commercial and industrial IoT devices are vulnerable to IoT specific attacks .If we continue to utilize the existing IoT device design flow where security is addressed as an afterthought, we will face many more security disasters in the near future. Lightweight cryptographic solutions are being researched with the goal of creating a strong cryptographic solution for constrained IoT devices.

Lightweight Cryptography. The perceptual layer, network layer, and application layer require data encryption to securely protect the data generated and transferred by the layers. Among these three layers, the perceptual layer has all the constrained components, which demands a lightweight cryptographic system. There are two criteria used to determine the lightweight of a cryptographic algorithm .[5] The first criterion is the software weight of the cipher: this is determined by the cipher's time and memory complexities. Time complexity is the time it takes the cipher to turn plaintext into ciphertext and memory complexity is the amount of memory needed to carry out the task of creating the cipher. The second criterion is the hardware weight of the cipher: this is determined by the cipher's area and power consumption. The area of the cipher is represented by the number of gate equivalencies (GE) used to implement the cipher and power consumption is the power used during the cipher's execution. GE is determined by dividing the area (in micrometer squared: μm^2) by the area of a two-input NAND gate. The algorithm needs to meet the lightweight standards whilst having a similar performance for security attacks and security standards when compared to conventional algorithms. The current cryptographic primitives can be divided into two categories: asymmetric key cryptography and symmetric key cryptography.[6]

Asymmetric Key Cryptography. Few lightweight cryptography researchers have been working on asymmetric cryptographic algorithms, but unfortunately the results are not yet steady and fruitful like symmetric cryptographic algorithms. Lightweight asymmetric cryptographic algorithms are complex in terms of operation, as a result these are often not area or power efficient. With the advancement of attack models, these algorithms are becoming vulnerable .Asymmetric algorithms are typically based on trapdoor functions like, prime and semiprime factorization, and the Euler's totient function . Asymmetric algorithms can be divided into encryption algorithms and key distribution algorithms. A prime example of an asymmetric encryption algorithm is Rivest-Shamir-Adleman (RSA). Elliptical Curve Cryptography (ECC), and Diffie-Hellman are representative examples of asymmetric key distribution algorithms. ECC, and Digital Signature Algorithm (DSA) work in the framework of public key cryptosystems to generate a digital signature.[7]

II. DISCUSSION

A team of security experts at the National Institute of Standards and Technology has decided to standardize Ascon, a group of cryptographic algorithms designed to protect information generated by Internet of Things devices.NIST said Tuesday Ascon will provide lightweight cryptography for miniature technologies used in health care, infrastructure, transportation and other key industries that require protection from potential cyberthreats.“Small devices have limited

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

resources, and they need security that has a compact implementation. These algorithms should cover most devices that have these sorts of resource constraints," said Kerry McKay, a computer scientist at NIST.[8]

Ascon was determined as the most efficient set of lightweight algorithms for small devices after the NIST Lightweight Cryptography Team concluded a selection and evaluation process that started in 2018. Ten finalists were selected from 57 algorithm candidates through a multi-round public review process.Ascon was developed by a cryptography team from Graz University of Technology, Infineon Technologies, Lamarr Security Research and Radboud University.The algorithms will support authenticated encryption with associated data and hashing to ensure the security of small platforms.[9]The generalization of connected objects raises security and privacy issues. Lightweight cryptography aims to deal with these issues by building algorithms that are optimized for these devices of limited resources, without compromising on their level of protection.In 2016, researchers from the Weizmann Institute of Science in Tel-Aviv, Israel, managed to take control of some Philips smart bulbs and demonstrate the catastrophic consequences of such a hack. They describe a chain reaction implicating devices connected to the ZigBee network having reached a critical mass in a city such as Paris; an attack that starts with one lightbulb, then spreads throughout the city in a few minutes, making it possible to turn all the city lights on or off, or to exploit them to launch a massive distributed denial-of-service (DDoS) attack… [10]"We cannot afford to have connected objects, no matter how trivial they are, that are not secure", states Léo Perrin, a research fellow in symmetric cryptography within the COSMIQ team at Inria (the French National Institute for Research in Digital Science and Technology), and co-author of several lightweight cryptography algorithms. This field of research is committed to building low-cost cryptographic systems that are optimized (in particular) for the small devices of the Internet of Things (IoT).[11]

It raises the double issue of privacy and security. Firstly, a connected object collects personal data that can be sent to the manufacturer's servers. This can, by design, infringe on personal privacy. Secondly, even if the object has been designed to protect confidentiality, the data are still collected and stored. They flow through an internal network, within a house for example, where various objects can communicate together. These objects must be secure in order to avoid being hacked and the data getting out in the open. This is not immediately striking when thinking of a connected hairbrush, but securing these types of devices is crucial because they can become gateways into the network to which they are connected and be used to carry out more elaborate attacks, as demonstrated by the Israeli research team. Current cryptographic standards were written for computers. The algorithms are optimized for the resources available on a PC, or even a smartphone. But connected objects have limited resources, energy and power in particular, and the implementation of traditional algorithms can hinder their performance, meaning their production and running costs, because it requires additional resources and electricity consumption.However, performance constraints are essential in cryptography; it is not enough to build algorithms that secure communications, it is also necessary to ensure they are used in practice, and therefore reduce their costs as much as possible. For an RFID tag, for example, this means reducing the cost of the electronic circuit by reducing the number of logic gates. For a microcontroller, it will mean a reduction in the number of instructions needed for an encryption or authentication operation.[12]

But a microcontroller is different from a processor in a computer. Many operations that seem obvious (including essential operations in cryptography) are not present, or they cost more on a microcontroller. Therefore, not only are the performance constraints stronger on Internet of Things devices, but also, the actual operation costs model is different.In addition, these objects are more likely to be subjected to physical attacks. [13]To hack a badge equipped with an RFID chip, the attacker may attempt to read the cryptographic key directly in the electronic circuit or, for example, analyze the variations in power consumption. This is what is called a "side channel attack". Ideally, lightweight cryptography will aim to develop algorithms that are less vulnerable to this kind of attack, or at least, that enable more secure physical implementation. This is one of the great difficulties of this field (including for NIST): cryptography constantly seeks "lightness", that is to say providing maximum security for minimum cost. During my thesis, I suggested to define lightweight cryptography as a cryptography that is explicitly dedicated to particular niches. For me, what ultimately defines it is the lightness of the platforms on which it must be implemented. For example, an RFID tag has a "lighter"

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

computing power. What's more, lightweight cryptography allows compromises that could not be allowed in "normal" cryptography. One can, for example, consider that attackers have access to less encrypted data (a quantity crucial to their attack) when they target an RFID tag rather than a PC because it can encrypt much less text in a given time[14]. Lightweight cryptography does not offer a lower level of security, but it takes these limits into account when building the algorithms. For this to be possible, I am convinced that we must concentrate on certain niches and develop specialized algorithms that can meet the specific constraints of these niches. The idea behind this notion of niches it to say that it is not possible to have a single algorithm that is excellent everywhere. Yet, that is what is being researched in lightweight cryptography, to lower the barriers to the adoption of encryption in constrained devices. I therefore think it is necessary to identify use cases where we cannot use AES for performance reasons and build efficient algorithms in these cases, which implies having several. The exact specification of these niches has not yet been decided, but RFID tags and microcontrollers each represent one.[15]

III. RESULTS

NIST "officially" launched a reflection process on the standardization of lightweight cryptographic algorithms in 2015 and attempted to obtain profiles (a description of the different niches) from industry. This did not work out, industrials were reluctant to share encrypted data (relating to their product's needs in terms of electricity consumption or the expected level of security, for example) for trade secrecy reasons. NIST then initiated a standardization process in 2018, with a call for submissions including two specifications corresponding to two profiles: material platforms (electronic circuits such as RFID tags) and microcontroller type software platforms. They received over fifty submissions. [16]Today there are only ten candidates left, these include both generalist algorithms (Ascon, for example) and specialist algorithms (like Grain-128AEAD). Sparkle, the algorithm I co-wrote and that is based on another algorithm, SPARX, conceived during my thesis in Luxembourg, is optimized for microcontrollers, meaning the operations used are ones that microcontrollers can perform very well.The choice between a generalist algorithm and specialist algorithms is a very difficult one as both approaches have good arguments. The risk, in opting for a single algorithm, would be that of having a second AES, that is to say an algorithm that is good all round (sometimes even very good) but that will not be excellent in the most constrained cases. The final decision will be given by NIST at the end of the year. Large volumes of sensitive data are being transferred among devices as the Internet of Things (IoT) grows in popularity. As a result, security measures must be implemented to ensure that unauthorized parties do not obtain access to the data. It is well acknowledged that IoT devices have restricted resources, such as limited battery life, memory, and hence reaction time. Classical encryption approaches and methods become inefficient for IoT devices due to memory limits. Large volumes of sensitive data are being transferred between devices as the Internet of Things (IoT) grows in popularity. [17]This involves the implementation of security safeguards to ensure that unauthorized parties do not obtain access to the data. IoT devices are notorious for having limited resources, such as battery life, memory, and hence response time. Classical encryption approaches and methods become inefficient for IoT devices due to memory limits. As a result, a Lightweight cryptosystem that fits the needs of Lightweight devices and ubiquitous computing systems has emerged. The goal of this study is to present a Lightweight cryptosystem (LWC) that may be used as a plugin to secure data transfers in IoT devices and pervasive computing. To that goal, the researchers employ several simple measuring techniques. The suggested system was then implemented on a field-programmable gate array (FPGA) board using the Verilog programming language to demonstrate its appropriateness for actual security applications. FPGA is also utilized in hardware applications to assess the system's resource usage and performance. Finally, a comparison of the proposed system with previous lightweight cryptography systems is performed to reinforce the major goal of this work, which is to present a new lightweight cryptosystem. With the incredible growth of technology over the previous century, computers, machines, and gadgets have been able to perform some functions without the need for human participation.[18] IoT refers to these devices linked as a network of equipment, gadgets, and computers that may communicate with one another. IoT also enables data transport and sharing via a network without the need for direct human engagement. IoT may be utilized in a variety of sectors in our daily lives, including healthcare and industry. The relevance of IoT is growing fast, and it is managing many aspects of our lives; thus, it is critical to preserve and secure the information and data utilized in IoT.[19]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

To preserve and protect sensitive material, one must encrypt it. Encrypting data increases security by prohibiting unauthorized parties from accessing or modifying it (integrity constraints). Encryption is a method of hiding original data by using a specific key; this process turns the original data into another shape that hides the original data's essence. In this process, the original data is referred to as plaintext, while the encrypted data is referred to as ciphertext. The encryption process should be reversible, allowing the plaintext to be recovered from the ciphertext with the help of a key. [20]If the same key is used for encryption and decryption, the encryption is symmetric. If, on the other hand, the key used in decryption is different from the key used in encryption, the encryption is asymmetric. In asymmetric encryption, one key is private while the other is made public. The public key of the receiver is used for encryption, whereas the private key of the receiver is utilized for decryption.Internet of Things (IoT) devices include wearable devices, monitors, sensors, and any other computer-capable item. These gadgets often feature a small memory capacity, a short battery life, and a quick response time . Because of the resource restrictions of IoT devices, they necessitate a specialized encryption algorithm that saves energy usage, accounts for limited accessible memory, and maintains a quicker response time. [21]Lightweight cryptosystems are the name given to these specific cryptosystems.The suggested system extends the previous stream cipher chaos-based encryption method created by Abutaha et al. This chaos-based encryption technique is extended to create a LWC. This chaos-based encryption technique is extended to create a LWC. This chaos-based encryption method is expanded to produce a LWC. This study's key contribution is the development of a LWC system that may be employed in embedded systems, IoT devices, or any other device with limited resources.[22]

In our new work we present an effective LWC with software and hardware implementation on a field-programmable gate array (FPGA) board using the Verilog programming language to show its suitability for practical security applications. In addition, FPGA is used in hardware applications to evaluate the system's resource utilization and performance. In addition, in our new work, we apply the RAPL and POWERTOP to calculate power usage. In addition, we included memory consumption, resource performance, and utilization in our comprehensive research.The "Background and literature review" section explains the key principles and reviews past work on this topic. Measurement instruments for power and memory are mentioned in the "Design and methodology" section. The "Software and hardware implementation" section describes the system's software and hardware implementation. Under the meanwhile, the findings are displayed in the "Results" section. [23]

IV. CONCLUSIONS

To safeguard the original data (plaintext), the ciphertext does not reveal anything about it. As a result, only the sender and recipient have access to the original data. Cryptography is the study of encryption and decryption8. To maintain data security, most apps, computers, and devices (through IoT) employ encryption in their communication. The data is encrypted using a secret key to create the ciphertext, which is then sent to the recipient. The key is known to the recipient, who uses it to decrypt the ciphertext and obtain the original data. If the key used to encrypt and decode the data is the same, the encryption is symmetric, however in asymmetric encryption, we can encrypt the entire data set at once, which is known as stream cipher. Otherwise, we can partition the data into blocks, encrypt each one, and then transmit them as blocks to be decrypted. Block cipher is the process of dividing data into blocks to be encrypted.[22]

As previously stated, block cipher encryption is a symmetric encryption that encrypts n-bits of data at a time to generate n-bits of ciphertext; each n-bit is referred to as a block. If the data size is greater than n bits, it can be partitioned into blocks that generate a block of ciphertext for each block of data. After partitioning the entire data into blocks based on block size, if some remaining bits do not match the block size, padding techniques are used to finish the block so that the remaining bits may be encrypted as a block. 64 bit, 128 bit, and 256 bit are the most frequent block sizes. There are numerous block cipher algorithms available, including Digital Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), and others. Stream cipher is another sort of Symmetric encryption in which we

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

encrypt 1 bit or byte of plaintext at a time. There are several stream cipher algorithms, such as RC4 , salsa20 and Rabbit. The stream cipher generates a series of random integers using mathematical algorithms. This sequence is the produced key value. The numbers in the series almost have the qualities of random numbers, making them difficult to predict. The pseudorandom generator must be unexpected, which implies there should be no effective technique that can predict the next key from the preceding one with a probability greater than 0.5.The machine-to-machine (M2M) concept was created in the late 1970s to explain wired or wireless communication between devices. This notion was then used to a variety of applications, including data collection via sensors. With the growth of the internet in the 2000s, the M2M idea brought the "IoT," which stands for "Internet of Things." In this environment, "Things," which may be apps, machines, sensors, cars, and so on, can communicate with one another without the need for user intervention, and they can freely transmit data17. It's a given that "Things" use a computer to communicate with one another. This idea gave rise to the phrase "ubiquitous computing".[24]

Ubiquitous computing indicates that computers are everywhere, and they may be any device, in any place, and in any format at any time. Pervasive computing, wearable computing, and tangible computers are examples of ubiquitous computing.

REFERENCES

[1] https://www.iotforall.com/5-worst-iot-hacking-vulnerabilities/
[2] Sattar B. Sadkhan, Akbal O. Salman. "A Survey on LightweightCryptography" 2018 International Conference on Advances in Sustainable Engineering and Applications (ICASEA). pp. 105–108. 2018.
[3] Shamsher Ullah, Xiang-Yang Li, Lan Zhang. "A Review of Signcryption Schemes Based on HyperElliptic Curve" 2017 3rd International Conference on Big Data Computing and Communications (BIGCOM). pp. 51–58. 2017.
[4] Biryukov, Alex and Leo Perrin. "State of the Art in Lightweight Symmetric Cryptography." IACR Cryptology ePrint Archive P. 511. 2017.
[5] Guo J, Peyrin T, Poschmann A. "The PHOTON family of lightweight hash functions Springer, vol 6841. pp. 222–239. 2011
[6] Bogdanov A, Knezevic M, Leander G, et al. "{SPONGENT}: the design space of lightweight cryptographic hashing" IACR Cryptology ePrint Archive, 2011.
[7] Hirose S, Ideguchi K, Kuwakado H, et al. A lightweight 256-bit hash function for hardware and low end devices Lesamnta-LW. Berlin, Heidelberg. pp. 151–168. Springer 2011.
[8] Buchanan WJ, "Chaskey Cipher." [Internet]. Available from: http://asec uritysite.com/encryption/chas.
[9] Buchanan WJ, "Mickey V2 lightweight stream cipher." [Internet]. Available from: http://asecuritysite.com/encryption/mickey.
[10] Buchanan WJ, "Trivium lightweight stream cipher." [Internet]. Available from: http://asecuritysite.com/encryption/trivium.
[11] 9WJ, "Grain lightweight stream cipher." [Internet]. Available from: http://asecuritysite.com/encryption/grain.
[12] Bogdanov A, Knudsen LR, Leander G, et al. "PRESENT: An ultralightweight block cipher" vol 4727. pp. 450–466. 2007.
[13] A. Moradi et al., "Pushing the Limits: A Very Compact and a Threshold Implementation of AES," in Advances in Cryptology – EUROCRYPT 2011 Lecture Notes in Computer Science, vol. 6632, pp. 69–88. Springer, 2011.
[14] A. Bogdanov et al., "PRESENT: An Ultra-Lightweight Block Cipher, in Cryptographic Hardware and Embedded Systems - CHES 2007 Lecture Notes in Computer Science, pp. 450–466. Springer, 2007.
[15] W. Zhang et al., RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms," in Science China Information Sciences, vol. 58(12), pp. 1–15. 2015.
[16] D. Hong et al., "HIGHT: A New Block Cipher Suitable for LowResource Device," in Cryptographic Hardware and Embedded Systems – CHES 2006 Lecture Notes in Computer Science, pp. 46–59. 2006.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 1, January 2019

[17] A. Satoh and S. Morioka, "Hardware Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES," in Lecture Notes in Computer Science Information Security, pp. 252–266. Springer, 2003.
[18] T. Suzaki et al., "TWINE: A Lightweight Block Cipher for Multiple Platforms," in Selected Areas in Cryptography Lecture Notes in Computer Science, vol. 7707, pp. 339–354. Springer, 2013.
[19] R. Beaulieu et al., "The SIMON and SPECK lightweight block ciphers, in Proceedings of the 52nd Annual Design Automation Conference, pp. 1–6. 2015.
[20] R. M. Needham and D. J. Wheeler. Tea extensions. Technical report, Cambridge University, Cambridge, UK, October 1997.
[21] Christophe De Cannière, Orr Dunkelman, and Miroslav Kneževic.´ KATAN and KTANTAN – a family of small and efficient hardwareoriented block ciphers. In Christophe Clavier and Kris Gaj, editors, Cryptographic Hardware and Embedded Systems – CHES 2009, volume 5747 of Lecture Notes in Computer Science, pp. 272–288. Springer, Heidelberg, September 2009.
[22] Gideon Yuval. Reinventing the Travois: Encryption/MAC in 30 ROM bytes. In Biham [Bih97], pp. 205–209, 1997.
[23] Thierry Pierre Berger, Julien Francq, Marine Minier, and Gaël Thomas. Extended generalized Feistel networks using matrix representation to propose a new lightweight block cipher: Lilliput. IEEE Transactions on Computers, pp. 99, August 2015.
[24] Julia Borghoff, Anne Canteaut, Tim Güneysu, Elif Bilge Kavun, Miroslav Knezecic, Lars R. Knudsen, Gregor Leander, Ventzislav Nikov, Christof Paar, Christian Rechberger, Peter Rombouts, Søren S. Thomsen, and Tolga Yalçin. "PRINCE – A low-latency block cipher for pervasive computing applications" vol 7658, pp. 208–225. 2012.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details