Journal of Engineering and Applied Sciences 13 (20): 8439-8447, 2018
ISSN: 1816-949X

Analysis of Security Attacks on Lightweight Block Ciphers and their Countermeasures

Deepti Sehrawat and Nasib Singh Gill
Department of Computer Science and Applications, Maharshi Dayanand University,
Rohtak, Haryana, India

Abstract: Internet of Things is a global network based architecture utilizing sensor networks for communication between objects. Security and privacy are primary and essential requirements for network based application. Lightweight cryptography works for smart IoT environment by providing lightweight ciphers as a security solution. Cryptanalysis is another related field with the aim to explore cipher designs by revealing hidden factors like key, state of cipher and plain/cipher text. For this an attacker applies different attacks on a cipher. A cipher providing enough resistance against feasible attacks is considered as a good cipher. In lightweight cryptography, a cipher has to be lightweight in terms of resources and simultaneously it must provide good immunity against feasible attacks. This study summarizes various cryptographic attacks on lightweight block ciphers. Analysis of the effects of various attacks in such a smart environment is also presented in this study along with some countermeasures, so as to prevent from such attacks. This in turn, provides a sound foundation for new researchers wishing to gain an insight into IoT security.

Key words: IoT architecture, attacks, security, RFID, IoT layers, key technologies, threats, security solutions

INTRODUCTION

A world-wide sensor network of interconnected objects is referred to as Internet of Things (IoT). Many of the objects in IoT are the objects that surround us. Objects in IoT can be living or non-living such as person, things, places, etc., communicating their private secret information over sensor networks. These objects are distinctively addressable. The vital idea for smart application of IoT is to attach sensors to self-configuring things/objects that work together without human intervention in dynamic and global network infrastructure (Botta *et al*., 2014). Small sensors attached to these IoT enabled devices communicate their personnel information over internet for utilizing smart services provided by IoT. As computing grow to be omnipresent, embedded systems are developed in a wide range of domains such as industrial systems, critical infrastructures, handy and wearable applications (Manifavas *et al*., 2014).

Enormous amount of objects are taking part in IoT, resulting in huge data over network which communicates among objects. Cloud can benefit IoT through virtual unlimited cloud's resources like storage, processing, management and communication. Major concerns in cloud IoT paradigm is security and privacy because of lack of trust in service providers and involvement of private data in sensor devices (Botta *et al*., 2016). This smart environment model of ever-present computing presents a big challenge in the form of security maintenance, i.e., confidentiality, integrity and authenticity of data as most of the devices run on limited resources (Ranea *et al*., 2017).

Wireless technologies fueled this relatively new concept of smart environment in IoT. Smart sensor network, communication technologies, internet protocols and Radio Frequency Identification (RFID) are main technologies that give rise to meet this new challenge (Gubbi *et al*., 2013). IoT is described by real world and small things with low storage, low arithmetic processing, low power consumption, security and privacy. Due to constrained devices involved in IoT, numerous significant obstacles like privacy and security remains to fulfill IoT vision. Main issue is who manages the security and privacy. Cryptographic algorithms and protocols are main mechanisms to provide protection to data along with some others (John and Shpantzer, 2014).

Currently available data security solutions to IoT are not straight-forward applicable because of several constraints in the form of limited memory, limited arithmetic computation, enormous participating devices, heterogeneous environment, insecure, dynamic and continuously changing environment different protocols

Corresponding Author: Deepti Sehrawat, Department of Computer Science and Applications, Maharshi Dayanand University, Rohtak, Haryana, India

and large-scale implementations. Even widely used encryption standards like AES, DES and RSA have proven to be very expensive and inefficient on IoT devices which have limited computational capabilities and limited memory size. This proves to be more challenging in case of networked vehicles and small drones especially, when concurrently multiple operations are carried out. Because of above mentioned limitations, common cryptographic algorithms leads to waste of power, energy and time and proves to be inefficient (Hosseinzadeh and Hosseinzadeh, 2016).

A new field in the form of lightweight cryptography comes into existence to support this security demand in IoT. The challenge is to provide sufficient security models to make IoT a success. However, lacking strong security foundations, threats in the IoT will outweigh its benefits (John and Shpantzer, 2014). Meeting this challenge requires understanding the security solutions and threats/attacks on IoT security solutions.

The analysis of cryptographic algorithms aiming to reveal hidden factors such as key, cipher's state and cipher/plain text is called cryptanalysis. For the cipher designers, it is required to carefully consider the various attacks that may be applied to a cipher. Cryptographic attacks mainly focus on key retrieval. Once, a key is retrieved it is possible to break the cipher.

This study examines various attacks that have so far been applied on cryptographic solutions in the context of IoT environment. Effects of various attacks on IoT cryptography and different countermeasures to protect ciphers from such attacks are also presented.

MATERIALS AND METHODS

Security in IoT: Encryption process converts plaintext into cipher text by using a secret key and then cipher text is again converted to plaintext with the same/another secret key. Earlier encryption/decryption are considered important to achieve confidentiality. During last several years, other parameters like Integrity, authentication and Digital signature are also, included in cryptography along with confidentiality (Zissis and Lekkas, 2012). A number of data encryption algorithms are present nowadays but using these security techniques in IoT based applications is not possible because of some IoT constraints like, memory requirement in IoT based devices is less due to which RAM size and ROM size of ciphers must be low, IoT devices run on different environment and power consumption must be low for IoT based ciphers. So, for IoT enabled environment, lightweight cryptography came into existence. Lightweight encryption schemes are generally based on either block cipher, stream cipher or hash functions. Block ciphers are playing a major role in providing security of the smart objects (Nandhini and Vanitha, 2017). For applications that require high-level security, multiple rounds of operations on ciphers are required. This increase in the number of rounds in ciphers increases the security of ciphers but it also increases time consumption.

Classification of lightweight algorithms is based upon either implementation mode, i.e., hardware and software or the architecture, i.e., symmetric algorithms and asymmetric algorithms (Okello *et al*., 2017).

Software implementation based: Software implementations offer lower cost and more flexibility over hardware implementations of a cipher. Also, it requires regular updation as a result consuming more power (Okello *et al*., 2017). Speck, Pride, LEA, RoadRunner, Hummingbird, PICO and Chaskey are few software optimized ciphers.

Hardware implementation based: Targeted to optimize hardware resources and are relatively easier to build than software implementations by using logic gates (Okello *et al*., 2017). Some examples of hardware-based ciphers are: Present, MIDORI, Print, Klein, etc.

Symmetric algorithms: Uses a single common key for both encryption and decryption processes. These are simple and faster and requires secure sharing of the key over network. These may be classified as: block ciphers, stream ciphers or hash functions. Block ciphers are considered over the other two because it is possible to implement hash and stream ciphers from block ciphers (Okello *et al*., 2017). These algorithms are more open source and generally preferred over asymmetric algorithms

Asymmetric algorithms: Two keys, one public and other private are used in these types of ciphers. Asymmetric algorithms are slower, more complex and the keys in it are more secure. These algorithms prove to be costly for constrained devices and are not suitable for lightweight cryptography, so, mostly ciphers aimed for IoT are symmetric (Okello *et al*., 2017).

Cryptanalysis: Analyzing cryptanalysis systems to reveal cipher's internal state, private key and cipher text or plain text is referred to as cryptanalysis (Okello *et al*., 2017). Attacks in cryptanalysis are categorized into two main categories, generic and non-generic.

Generic attacks: Generic attacks aim to extract a key or plain-text/cipher-text combination and are independent

of cipher's internal state. These attacks make use of pre-known key sizes and block sizes. To thwart these attacks there is a strong need of carefully choosing a key size, block size or internal-state size of a cipher. Key sizes of greater than 128 bits are ideally unbreakable in current scenario (Okello *et al*., 2017).

Non-generic attacks: Attacks manipulating internal state of a cipher through some mathematical models, so as to discover the key, internal state or plain text/cipher text combination are called non-generic attacks. Providing resistance to these attacks is relatively a more difficult task than protecting a cipher against generic attacks. Linear approximation, differential cryptanalysis and algebraic attacks are some of the non-generic attacks (Okello *et al*., 2017).

Understanding lightweight ciphers in terms of their weaknesses and strengths through cryptanalysis provides a strong base for the design of new ciphers. This section covers various attacks to lightweight block ciphers in IoT enabled smart environment.

RESULTS AND DISCUSSION

Evolution from closed or limited-access networks to open ones increased the need for security alarms to protect interconnected devices from intrusions (Sicari *et al*., 2015). Many attacks can occur in lightweight ciphers in IoT, few of these are described below. Alongwith the attacks, countermeasures to protect from these attacks are also, specified.

Linear approximation: In linear approximation, a linear approximate expression of a cipher is determined. A statistical linear path is first discovered between the input bits and output bits of each S-box. Then this discovered path is extended to the entire algorithm to find linear approximate expression without intermediate values. A linear expression is then used to determine the key. To find the linear approximation, a condition is that sufficiently many plaintexts are available. This is also, known as a known-plaintext attack (Matsui, 1993). To provide protection against linear approximation good diffusion layer must be provided (Standaert *et al*., 2003).

Differential cryptanalysis: In this method, the effect of differences in plaintext pairs is analyzed on the differences in ciphertext pairs. These differences are then used to find the most appropriate key. Differential cryptanalysis is also, known as a chosen-plaintext attack (Biham and Shamir, 1990). In these attacks, nonlinear operations in cipher algorithm are modeled as linear operations. The probability of replacements made and the effect of these cryptanalysis techniques are strongly correlated. Using high number of active S-boxes and non-linear elements provides resistance against these two attacks (Standaert *et al*., 2003). To find the effect of differential cryptanalysis over RoadRunneR lightweight cipher, (Qianqian *et al*., 2016) computed the minimum number of active S-boxes and it gives a precise measurement for resistance against the linear and differential attack.

Truncated differential: This technique includes differential trails sets having identical S-boxes. This attack is somehow similar to differential attack like complexity analysis and rate evaluation of the two adopts the same method. To find the truncated differential for block ciphers, MITM technique is adopted (Qianqian *et al*., 2016). Truncated differentials exist when it is possible to predict only part of the difference in the cipher-text (Knudsen, 1994).

Impossible differential cryptanalysis: This attack can be successfully applied to GFN based block ciphers because of its slow diffusion property. Finding input difference propagating to particular output difference with a zero probability results to an impossible differential distinguisher. The longest possible impossible differential is applied in a key recovery attack by prepending and/or appending a small number of extra rounds known as analysis rounds. Pairs having specific input/output differences are collected, followed by guessing of some key-bits of analysis round. Any pair satisfying input/output differences of impossible differential for some sub-key gives a wrong key. The procedure discards the wrong keys and proceeds further search with the remaining key (Abdelkhalek *et al*., 2017). Block ciphers having slow diffusion allows to trace few impossible differential properties. This impossible differential property is because of bit contradiction as in case of Tea and XTEA ciphers which allows this attack to be feasible on these ciphers (Chen *et al*., 2012). An impossible differential attack is likely to be applied to GFN-based ciphers but Piccolo utilizing the same GFN variant is free from this attack because it uses round permutation for faster diffusion (Shibutani *et al*., 2011).

Related-key rectangle attack: This attack is an extension to differential cryptanalysis. It uses one or two S-box

operations in every iteration. This attack is applicable on ciphers having slow diffusion rate or slow mixing in key scheduling (Ozen *et al*., 2009). Fast diffusion rate by providing strong permutation layer gives resistance against this attack.

Slide attacks: If an iterative process in round function exhibits self-similarity to some degree then Slide attacks are applicable. It is independent of the number of rounds and round function properties. Slide attacks can exploit weaknesses of key scheduling part and even general structural properties of a cipher. It all depends upon the design of a cipher that to what extent this attack exploits the cipher. Iterative block ciphers in which there is a repeating sub-key for all rounds or having a periodic key schedule are more vulnerable to such attacks. Auto-key ciphers which have a data-dependent choice of round sub-keys are easily affected by slide attacks (Biryukov and Wagner, 1999). To prevent from slide attacks, cipher designers have to avoid self-similarity in the rounds of the cipher. This could be accomplished by adding some round counters or random constants in each round (Biryukov and Wagner, 1999). Not using periodic key scheduling is another countermeasure (Standaert *et al*., 2003). Zhang *et al.* (2015) added different round constants in the key schedule and this provides resistance against slide key as a result, the proposed cipher Rectangle prevents from slide attacks. A similar study by Suzaki *et al.* (2011) presents a lightweight block cipher, Twine, providing resistance against slide attacks by applying different constants in the key schedule in each round. Present cipher uses round dependent counter which provides resistance to the cipher against slide attacks (Ozen *et al*., 2009).

Advanced sliding techniques: Complementation slide and sliding with a twist are two advanced sliding techniques. In complementation slide, a self-similarity is amplified in Feistel block ciphers with two-round self-similarity. This is done by utilizing complementation properties which results in better attacks (Biryukov and Wagner, 2000). Sliding with a twist is a new technique on a Feistel cipher with two-round self-similarity.

Interpolation attack: It is useful for attacking ciphers using simple algebraic functions as S-boxes. In interpolation attack polynomials are constructed using pairs of plaintexts and cipher-texts. It is assumed that time needed in polynomial construction is less than the time it takes to convert plaintext to cipher text by encryption (Jakobsen and Knudsen, 1997). To make this attack infeasible, complex and higher degree algebraic expressions as S-boxes in Galois Field, GF (2^8) can be used with good diffusion property (Barreto and Rijmen, 2000).

Boomerang attack: The boomerang attack is considered as an intermediate between differential attack and higher-order differential attack. It is also called a differential-differential attack and is well suited for the security analysis of ciphers which are using asymmetric round functions. In this attack an attempt is made to create a quartet structure at an intermediate value halfway through the cipher (Wagner, 1999). To protect against these attacks good differentials must not be there especially for the first half or the last half of the cipher (Wagner, 1999). Good differentials can be implemented throughout the entire cipher to weaken the effect of boomerang attack. It is required to have complete diffusion along with probable differentials in fewer rounds (Standaert *et al*., 2003).

Integral cryptanalysis: It is dual to differential cryptanalysis and is mainly appropriate to those block ciphers in which only bijective components are used. In integral cryptanalysis, propagation of sums of several values is considered (Knudsen and Wagner, 2002). It is also known as a square attack and it propagates the sums of many values (Zhang *et al*., 2015). Do not use only bijective components for providing security to the block ciphers.

Meet in the middle attack: In this attack, a checkpoint is found at the middle by dividing the cipher into two parts. In the two parts, the effect of key bits is separated. A suitable plaintext is chosen for encryption. Then key bytes are found by applying partial decryption on the cipher text. The obtained values of decryption are then compared with the values of the pre-computed set. A match gives the probable right key value (Demirci and Selcuk, 2008). Feistel block ciphers having a simple key schedule and slow diffusion rate are more prone to such types of attacks. Multidimensional MITM is a variant of MITM which is applicable to those ciphers in which key length is greater than the block length (Bogdanov *et al*., 2011). Larger number of rounds are required in Feistel ciphers so as to prevent ciphers from this particular attack. For initial 3 rounds, Twine cipher contains all the key bits and it is free from MITM attack. So, good key scheduling and fast diffusion is also a possible solution for providing resistance against this attack.

Three subset meet in the middle attack: It is a modification of the basic MITM (Meet-in-the-Middle)

attack by removing the restrictions that were made on the choice of key bits. Three subsets of key bits are considered in this modified attack rather than two subsets of key bits as in basic MITM approach. In this approach there are two stages: First is MITM stage, to filter the wrong key candidates in order to reduce the key space, the second stage is testing, to find the right key in the reduced key space. m' bits out of 'b' bits are used for matching and remaining (b-m) bits are used in the key testing stage (Bogdanov and Rechberger, 2010). Weaknesses in bitwise key schedule is responsible for the success of this attack and works without any related keys. Ciphers with little key dependency (large parts of cipher depend on only a subset of key bits) are more vulnerable to this type of attack. For SPN, it is often difficult to mount MITM attack because each round of SPN uses sub-keys of the block length (Bogdanov and Rechberger, 2010).

Zero correlation linear cryptanalysis: Zero correlation linear cryptanalysis rely on linear approximations with ½ probability. It results in stronger attacks than its equivalent impossible differential cryptanalysis. Some of the block ciphers have multiple linear approximations for every key over a significant number of rounds with a zero correlation (Bogdanov and Meiqin, 2012). Identifying a linear approximation with zero correlation for all keys implies a rule to an entire class of similar types. Key recovery is possible by linear approximations of correlation zero (Sadeghi *et al*., 2016).

Leakage attacks: In leakage attacks, the attacker after each round of encryption find one bit of information about intermediate state via. physical probing, power measurement, calculating encryption time or by any other side channel type. This attack is usually applicable to the hardware implementation of block ciphers which are iterative in nature and uses the same hardware to execute rounds sequentially. It assumes that same side information is provided at the end of each round of encryption (Dinur and Shamir, 2009). Software implementations of ciphers are not vulnerable to leakage attacks.

Cube attack: Cube attacks are another type of attacks which are general key derivation attacks. It is also known as Leakage attack. If in a cryptography system even a single bit of information can be given by low degree multivariate polynomial then it is vulnerable to cube attacks (Dinur and Shamir, 2009). Hardware implementations of block ciphers are on the darker side of this type of attack (Dinur and Shamir, 2009).

Key-Recovery attack: Its basis is on a family of differential characteristics. Key recovery attack utilizes some round function properties and tweakey schedule of the lightweight cipher (Dobraunig *et al*., 2017). Do not allow repetition exploitation of properties of the ciphers so that retrieving the characteristics of the cipher would be difficult for an attacker. The same is the case with the Mantis cipher which makes its security margin too optimistic. Lightweight tweakey schedule of some ciphers also makes this attack successful (Dobraunig *et al*., 2017).

Invariant attacks: Lightweight block ciphers using very light and simple key schedules like the case where round keys differ only by using round constant are more vulnerable to invariant attack. Ciphers like Prince, Skinny-64 and $Mantis_7$ are free from this attack (Beierle *et al*., 2017). Invariant factors of the linear layer have a huge impact on this attack, if it is small then it is easy to find the round constants. It is free from the choice of S-box (Beierle *et al*., 2017). Linear layer and round constants play a major role in the success of this attack. Avoid using fixed constants in rounds and if every instance of a cipher has a variant function for both linear and substitution layer, it can resist invariant attack (Beierle *et al*., 2017).

Related key attacks: An attacker obtains input-output examples under different keys which is not the original key. This is applicable to block ciphers and finding the correct input-output combination of cipher for a specifically related key is known as a related key attack because here the key that gives correct input-output combination is not the original one, it is related to original key (Mihir and Kohno, 2003). Different key schedule in all rounds provides resistance to such attacks. One can use non-linear key schedules, round constants, strong diffusion layer and maximizing avalanche effect (Standaert *et al*., 2003).

Related key differential attack: Related keys and key differentials are used by a distinguisher to stop differentials in data processing part (Shibutani *et al*., 2011). In order to provide resistance against related-key differential attack, higher numbers of differentially active F-functions in the related-key setting are required. AKF, Feistel lightweight block cipher uses the concept of alternating keys which can make a cipher vulnerable to related-key differential attack. But AKF is resistant to this attack because of not having 10 round differential which makes it infeasible for this attack as having differential is desirable in a related key differential attack (Karakoç *et al*., 2015). A similar study of

(Shibutani *et al*., 2011) proves that Piccolo provides sufficient number of differentially active F-functions in related-key setting. Strong key scheduling proving non-linearity is another way to make related-key differential attacks inapplicable to a cipher (Ozen *et al*., 2009).

Related key impossible differential attack: This attack takes the benefits of the weak key schedule which creates low weight differential paths for an initial difference (Minier and Naya-Plasencia, 2012).

Self-similarity attacks: This attack uses a self-similarity that exists between round functions in a cipher. To prevent from such attacks, using round constants or random numbers is a possible solution (Biryukov and Wagner, 2000).

Rotational cryptanalysis: If a round function has rotated variant of some input words then it is exposed to Rotational cryptanalysis. This type of attack is more successfully implemented to ARX-based block ciphers (Khovratovich and Nikolic, 2010). A variant of this attack known as Rotational-XOR cryptanalysis is given by Leuven (2017). This attack is a statistical technique to attack the ARX-based block ciphers. This attack considers the ARX primitives in those cases where constants are used in the state. Researchers in this study presented a computer tool based on Python implementation of ARX cipher to automatically find best possible rotational-XOR characteristics. Using round constants and n-bit security having at least 0.7n operations provides good resistance against rotational cryptanalysis (Dmitry *et al*., 2012).

Algebraic attack: In this attack, a secret key is recovered by finding a solution for the over-defined system of multivariate algebraic equations. Multivariate relations which involve key bits/state bits are used by an algebraic attack and it outputs bits of function. The effect of these attacks is much higher if low degree relation is found in the key/state bits (Meier *et al*., 2004). Expressions of higher degree complicate algebraic attack on ciphers (Canniere *et al*., 2009). High algebraic-degree and branch number of S-boxes provides prevention from algebraic attacks (Engels *et al*., 2011).

Biclique attack: To recover the secret key, Biclique attacks do not use related-keys. It is a kind of MITM attack. Bicliques are constructed on the target sub-cipher from independent related key (Jeong *et al*., 2015). In this attack, using some structural trails, full structure of states can be developed. These structures are termed as bicliques in graph theory and have two sets of internal states where there exists a relation among each state in a set with all states in another set (Khovratovich and Nikolic, 2010). It is described by dimension (cardinality of biclique elements) and length (number of rounds covered). Constructing high dimensional bicliques for primitives having fast dimension is a difficult task. This approach depends on the high probability related-key differentials on cipher (Bogdanov *et al*., 2011). This attack provides a base for the key-recovery attack by reducing the effort required on block ciphers for key-recovery attacks (Jeong *et al*., 2015). Slow and limited diffusion results in long bicliques (Jeong *et al*., 2015). So to prevent the secret-keys from this attack, good diffusion layer with fast permutations is essential.

Weak keys: Encryption and decryption procedures having same keys are known as weak keys. If encryption using key K0 and decryption using key K1 are same then the keys K0 and K1 are known as semi-weak keys. Normal behavior of a block cipher is retrieved from weak or sub-weak keys.

Statistical saturation attack: Due to weak diffusion/ permutation layer of present, this attack came into existence and it is successfully applied to other ciphers also, like, rectangle. Saturation attack proves to be strong against Generalized Feistel Networks based Block ciphers (Wentao *et al*., 2015). Providing good diffusion layer to the cipher design provides immunity against this attack.

Chosen message attack: It attempts to extract the full secret key and relies on differentials in the high bits of words. Chosen message attack does not depend on permutation layer and is successfully implemented on Hummingbird-1 due to its weak initialization function. State size of Hummingbird-1 is very small due to which its internal state bits are affected by a chosen input. This type of cipher attack is based on differential divide-and-conquer method (Saarinen, 2011). Increasing the states bits which execute regardless of input data provides a guard against chosen message attack (Saarinen, 2011).

Attack analysis: Through analysis of various attacks on lightweight ciphers, it is revealed that all attacks are not relevant to a cipher, some ciphers are free from some attacks like only hardware implementation of ciphers are prone to leakage/cube attacks and SPN ciphers are less exposed to MITM attack. Prevention from attacks is also possible by adopting some designing measures such as

Table 1: Types of various attacks and their prevention

Attacks	Types	Prevention
Linear approximation	Non-generic	Strong diffusion layer
Differential analysis	Non-generic	Strong diffusion layer
Impossible differential cryptanalysis	Non-generic	Fast diffusion
Related-key rectangle attack	Non-generic	Fast diffusion
Slide attacks	Non-generic	Avoid self-similarity in the rounds using round-counters or random-constants
Interpolation attack	Non-generic	Using higher-degree algebraic expressions as S-boxes
Boomerang attack	Non-generic	Good differentials throughout the entire cipher
Integral cryptanalysis	Non-generic	Do not use only bijective components
Meet-in-the-middle attack	Generic	Strong key scheduling, fast diffusion
Three subset meet-in-the-middle attack	Generic	Strong key schedule with high key dependency
Leakage attacks	Non-generic	Software Implementations
Cube attack	Generic	Software implementation using high degree multivariate polynomial
Key-recovery attack	Non-generic	Avoid repeating structure
Invariant attacks	Non-generic	Using variant functions and round constants
Related key attacks	Generic	Using non-linear key schedules, round constants, and strong diffusion layer
Related key differential attack	Non-generic	Using higher numbers of differentially active f-functions in the related-key setting and strong key.scheduling proving non-linearity
Self-similarity attacks	Generic	Using round constants or random numbers
Rotational cryptanalysis	Generic	Using round constants
Algebraic attack	Non-generic	Using higher degree functions
Biclique kttack	Generic	Strong and fast diffusion
Statistical saturation attack	Non-generic	Strong diffusion
Chosen message attack	Non-generic	Increasing the states bits

using round constants or random numbers helps in prevention from self-similarity attack. To prevent from integral effect, do not use only bijective functions. Boomerang attack is avoided by not allowing good differential on either half. Table 1 summarizes different types of attacks discussed in this study and some preventive measures that can provide strong basis for the design of a new lightweight cipher. Some of available lightweight ciphers are not fully optimized and have some kind of weaknesses like:

- Weak substitution box
- Weak permutation layer
- Weak key scheduling
- Susceptibility to some kind of attacks
- Computationally complex and expensive
- Low resource utilization

Due to these weaknesses the ciphers are vulnerable to different attacks. The efforts are being made by researchers aiming to design a lightweight cipher which should fulfill the requirements of a good lightweight cipher as well as providing good resistance against feasible attacks. This motivates the researchers of this study to attempt to design a lightweight cipher for security in IoT based smart applications.

CONCLUSION

Emergence of IoT is finding its way into the modern digital world to improve the quality of life by proving smart environment. Available security solutions are not enough for IoT applications and smart environment because for several constraints such as dynamic environment, limited memory, different technologies, protocols, etc. Lightweight cryptography as a security solution provides confidentiality, integrity, authentication and digital signature. Designing a robust lightweight cipher requires enough analysis to be done and it is not so easy as the cipher should consume fewer resources for being lightweight and simultaneously it should be able to resist all feasible attacks. This study presents an overview of the premise of various attacks on lightweight block ciphers and also specified some preventive measures to avoid these attacks. This in turn, provides a sound foundation for further new research in security of IoT enabled smart environment.

REFERENCES

Abdelkhalek, A., M. Tolba and A.M. Youssef, 2017. Impossible Differential Attack on Reduced Round SPARX-64/128. In: Cryptology in Africa, Joye M. and A. Nitaj (Eds.) Springer, Cham, Switzerland, ISBN:978-3-319-57338-0, pp: 135-146.

Beierle, C., A. Canteaut, G. Leander and Y. Rotella, 2017. Proving resistance against invariant attacks: Properties of the linear layer. Proceedings of the Conference on Early Symmetric Crypto (ESC'17), January 16-20, 2017, Mercure Kikuoka Golf Club Hotel, Canach, Luxembourg, pp: 1-5.

Biham, E. and A. Shamir, 1991. Differential cryptanalysis of DES-like cryptosystems. J. Cryptol., 4: 3-72.

Biryukov, A. and D. Wagner, 1999. Slide Attacks. In: Fast Software Encryption, Knudsen, L. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-66226-6, pp: 245-259.

Biryukov, A. and D. Wagner, 2000. Advanced Slide Attacks. In: Theory and Applications of Cryptographic Techniques, Preneel, B. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-67517-4, pp: 589-606.

Bogdanov, A. and C. Rechberger, 2010. A 3-Subset Meet-in-the-Middle Attack: Cryptanalysis of the Lightweight Block Cipher KTANTAN. In: Selected Areas in Cryptography, Biryukov, A., G. Gong and D.R. Stinson (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-19573-0, pp: 229-240.

Bogdanov, A. and M. Wang, 2012. Zero Correlation Linear Cryptanalysis with Reduced Data Complexity. In: Fast Software Encryption, Canteaut, A. (Ed.). Springer, Berlin, Germany, ISBN:978-3-642-34046-8, pp: 29-48.

Bogdanov, A., D. Khovratovich and C. Rechberger, 2011. Biclique Cryptanalysis of the Full AES. In: Theory and Application of Cryptology and Information Security, Lee, D.H. and X. Wang (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-25384-3, pp: 344-371.

Botta, A., W.D. Donato, V. Persico and A. Pescape, 2014. On the integration of cloud computing and internet of things. Proceedings of the 2014 International Conference on Future Internet of Things and Cloud (FiCloud'14), August 27-29, 2014, IEEE, Barcelona, Spain, ISBN:978-1-4799-4357-9, pp: 23-30.

Botta, A., W.D. Donato, V. Persico and A. Pescape, 2016. Integration of cloud computing and internet of things: A survey. Future Generation Comput. Syst., 56: 684-700.

Canniere, D.C., O. Dunkelman and M. Knezevic, 2009. KATAN and KTANTAN: A Family of Small and Efficient Hardware-Oriented Block Ciphers. In: Cryptographic Hardware and Embedded Systems-CHES, Clavier, C. and ?K. Gaj (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-04137-2, pp: 272-288.

Chen, J., M. Wang and B. Preneel, 2012. Impossible Differential Cryptanalysis of the Lightweight Block Ciphers TEA, XTEA and HIGHT. In: Cryptology in Africa, Mitrokotsa, A. and S. Vaudenay (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-31409-4, pp: 117-137.

Demirci, H. and A.A. Selcuk, 2008. A meet-in-the-middle attack on 8-round AES. In: Fast Software Encryption, Nyberg, K. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-71038-7, pp: 116-126.

Dinur, I. and A. Shamir, 2009. Cube Attacks on Tweakable Black Box Polynomials. In: Advances in Cryptology-EUROCRYPT, Joux, A. (Ed.). Springer, Berlin, Germany, ISBN:978-3-642-01000-2, pp: 278-299.

Dmitry, K., C. Rechberger and A. Savelieva, 2012. Bicliques for preimages: Attacks on skein-512 and the SHA-2 family. Proceedings of the 19th FSE International Workshop on Fast Software Encryption, March 19-21 2012, Springer, Washington, DC, USA., ISBN:978-3-642-34046-8, pp: 244-263.

Dobraunig, C., M. Eichlseder, D. Kales and F. Mendel, 2017. Practical key-recovery attack on MANTIS5. IACR. Trans. Symmetric Cryptology, 2016: 248-260.

Engels, D., M.J.O. Saarinen, P. Schweitzer and E.M. Smith, 2011. The Hummingbird-2 Lightweight Authenticated Encryption Algorithm. In: Radio Frequency Identification: Security and Privacy Issues, Juels, A. and C. Paar (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-25285-3, pp: 19-31.

Gubbi, J., R. Buyya, S. Marusic and M. Palaniswami, 2013. Internet of Things (IoT): A vision, architectural elements and future directions. Future Generation Comput. Syst., 29: 1645-1660.

Hosseinzadeh, J. and M. Hosseinzadeh, 2016. A comprehensive survey on evaluation of lightweight symmetric ciphers: Hardware and software implementation. Adv. Comput. Sci. Intl. J., 5: 31-41.

Jakobsen, T. and L.R. Knudsen, 1997. The Interpolation Attack on Block Ciphers. In: Fast Software Encryption, Biham, E. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-63247-4, pp: 28-40.

Jeong, K., H. Kang, C. Lee, J. Sung and S. Hong *et al*., 2015. Weakness of lightweight block ciphers mCrypton and LED against biclique cryptanalysis. Peer Networking Appl., 8: 716-732.

John, P. and G. Shpantzer, 2014. Securing the internet of things survey. SANS Institute, North Bethesda, Maryland. http://cybersec.orglearn. com/wp-content/uploads/2014/02/Securing the Internet of Things Survey.pdf

Karakoc, F., H. Demirci and A.E. Harmanci, 2015. AKF: A key alternating Feistel scheme for lightweight cipher designs. Inf. Process. Lett., 115: 359-367.

Khovratovich, D. and I. Nikolic, 2010. Rotational Cryptanalysis of ARX. In: Fast Software Encryption, Hong, S. and T. Iwata (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-13857-7, pp: 333-346.

Knudsen, L. and D. Wagner, 2002. Integral cryptanalysis. Proceedings of the 9th FSE International Workshop on Fast Software Encryption, February 4-6, 2002, Springer, Leuven, Belgium, ISBN:978-3-540-44009-3, pp: 112-127.

Knudsen, L.R., 1994. Truncated and higher order differentials. Proceedings of the Second FSE International Workshop on Fast Software Encryption, December 14-16, 1994, Springer, Washington, DC, USA., ISBNl:978-3-540-60590-4, pp: 196-211.

Manifavas, C., G. Hatzivasilis, K. Fysarakis and K. Rantos, 2014. Lightweight Cryptography for Embedded Systems: A Comparative Analysis. In: Data Privacy Management and Autonomous Spontaneous Security, Garcia-Alfaro, J., G. Lioudakis, N. Cuppens-Boulahia, S. Foley and W. Fitzgerald (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-54567-2, pp: 333-349.

Matsui, M., 1993. Linear Cryptanalysis Method for DES Cipher. In: Theory and Application of Cryptographic Techniques, Helleseth, T. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-57600-6, pp: 386-397.

Meier, W., E. Pasalic and C. Carlet, 2004. Algebraic attacks and decomposition of Boolean functions. Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, May 2-6, 2004, Interlaken, pp: 474-491.

Mihir, B. and T. Kohno, 2003. A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs and Applications. In: Theory and Applications of Cryptographic Techniques, Biham, E. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-14039-9, pp: 491-506.

Minier, M. and M. Naya-Plasencia, 2012. A related key impossible differential attack against 22 rounds of the lightweight block cipher LBlock. Inf. Process. Lett., 112: 624-629.

Nandhini, P. and D.V. Vanitha, 2017. A study of lightweight cryptographic algorithms for IoT. Intl. J. Innov. Adv. Comput. Sci., 6: 26-35.

Okello, W.J., Q. Liu, F.A. Siddiqui and C. Zhang, 2017. A survey of the current state of lightweight cryptography for the internet of things. Proceedings of the 2017 International Conference on Computer, Information and Telecommunication Systems (CITS'17), July 21-23, 2017, IEEE, Dalian, China, ISBN:978-1-5090-5958-4, pp: 292-296.

Ozen, O., K. Varici, C. Tezcan and C. Kocair, 2009. Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT. In: Information Security and Privacy, Boyd, C. and J.G. Nieto (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-02619-5, pp: 90-107.

Qianqian, Y., L. Hu, S. Sun and L. Song, 2016. Truncated differential analysis of round-reduced roadrunner block cipher. IACR. Cryptology ePrint Arch., 1: 1-11.

Ranea, A., Y. Liu and T. Ashur, 2017. An easy-to-use tool for rotational-XOR cryptanalysis of ARX block ciphers. Proc. Romanian Acad. Ser. A ., 18: 307-316.

Saarinen, M.J.O., 2011. Cryptanalysis of Hummingbird-1. In: Fast Software Encryption, Joux, A. (Ed.). Springer, Berlin, Germany, ISBN:978-3-642-21701-2, pp: 328-341.

Sadegh, S., T. Mohammadi and N. Bagheri, 2016. Cryptanalysis of reduced round SKINNY block cipher. IACR. Cryptology ePrint Arch., 1: 1-11.

Shibutani, K., T. Isobe, H. Hiwatari, A. Mitsuda and T. Akishita *et al*., 2011. Piccolo: An Ultra-Lightweight Block Cipher. In: Cryptographic Hardware and Embedded Systems, Preneel, B. and T. Takagi (Eds.). Springer, Berlin, Germany, ISBN:978-3-642-23950-2, pp: 342-357.

Sicari, S., A. Rizzardi, L.A. Grieco and P.A. Coen, 2015. Security, privacy and trust in internet of things: The road ahead. Comput. Networks, 76: 146-164.

Standaert, F.X., G. Piret and J.J. Quisquater, 2003. Cryptanalysis of block ciphers: A survey. Master Thesis, Universite Catholique de Louvain, Ottignies-Louvain-la-Neuve, Belgium.

Wagner, D., 1999. The Boomerang Attack. In: Fast Software Encryption, Knudsen, L. (Ed.). Springer, Berlin, Germany, ISBN:978-3-540-66226-6, pp: 156-170.

Zhang, W., Z. Bao, D. Lin, V. Rijmen and B. Yang *et al*., 2015. RECTANGLE: A bit-slice lightweight block cipher suitable for multiple platforms. China Inf. Sci., 58: 1-15.

Zissis, D. and D. Lekkas, 2012. Addressing cloud computing security issues. Future Gener. Comput. Syst., 28: 583-592.