IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555
Vol. 2, No.2, April 2012

A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers

Anjali Arora, Priyanka,
Information Technology Department,
Banasthali Vidyapith, Rajasthan.

Saibal Kumar Pal,
Scientific Analysis Group,
Defence Research and Development Organization,
Delhi.

Abstract— **Lightweight block ciphers are used in applications where low power consumption is a requirement along with hardware area constraints regarding their implementation. Design of these ciphers demands an optimal tradeoff between computational efficiency and security. These ciphers being supportive in fast and secure transmission of data from one location to another are prone to several attacks that need to be identified and analyzed before deployment. This paper focuses on describing and categorizing all recent attacks in accordance to various lightweight block ciphers available to us. We present recently published lightweight block ciphers, their comparison trade-offs between security, cost and performance and cryptanalytic attacks launched on some of these ciphers.**

Keywords: Block Ciphers, Lightweight encryption, Resource Constraints, Attacks, Cryptanalysis.

I. INTRODUCTION

Development of wireless communication has led to the applications which inculcate pervasive computing such as, smart cards, RFID tags, and sensor nodes. These applications are helpful in public transport, pay TV systems, smart electricity anti-counterfeiting, etc. Wireless networks have gathered attention due to their increasing usage in the areas of environmental monitoring, military scouting and healthcare. Some of these applications require secure storage and transmission of data over unprotected communication links.

Lightweight cryptography [1] is used to provide secure transmission of data on extremely constrained devices. These constraints depend upon the cost and limited computing power supply. In addition to providing benefits in data transmission on constrained devices, lightweight ciphers are also prone to several attacks.

In particular, wireless sensor networks (WSNs) have attracted more and more attention since they promise practical solutions for many real-time applications. Resource-constrained nodes/devices on these networks always have an urge on the selection of security algorithms on the basis of implementation costs. Lightweight block ciphers use a secret key shared between the sender and receiver [2] and are quite suitable for some of these applications.

Substitution and permutation network, Fiestel, iterative (special type of Fiestel), Misty are various structural forms which are used in the design of symmetric encryption systems. The popular DES block cipher follows the Fiestel network structure in which the encryption algorithm function start splitting the plaintext into two halves of equal bits each. It used to be a very strong cipher, but due to present improvement in hardware and computational resources it was possible to crack in practical time. CLEFIA, Sony's Cipher also follows the Fiestel structure and is used under the Digital Rights Management (DRM) framework. It is difficult to comment regarding the security and computational efficiency of the Fiestel cipher unless considering its particular round function F [3].

Iterative block ciphers apply another significant design principle. In iterative block cipher, several permutations are applied to build the round transformation in order to give efficient implementations such as IDEA. IDEA is a symmetric block cipher which operates on 64 bit block and uses 128 bit key. It contains 8.5 similar rounds having a similar process of encryption and decryption. It uses 52 round keys and each round uses six 16 bit sub keys. IDEA derives much of the security from bitwise exclusive-OR, addition modulo 2^{16} and multiplication modulo $2^{16}+1$ operations. The security of IDEA depends on these primitives whereas the Misty block cipher also include Fiestel network in recursive fashion [3].

Trade-off between key length and security finds out the security aspect of the cryptographic system. Larger the key length higher the resistance to brute force attack. In providing security to embedded systems, block cipher plays a vital role. The lightweight block cipher can be used not only for encryption but also for authentication on devices having highly constrained resources. For security and performance concerns, some types of sensors are equipped with hardware implementation of AES-128 [4] and other lightweight block ciphers.

Lightweight ciphers can be applied not only for encryption but also for hashing and authentication under environment that are highly constrained. For such an environment, normal block encryption algorithms like AES could prove to be expensive and hence unsuitable for use, despite the various approaches proposed to optimize AES hardware and software implementations.

Skipjack is a lightweight block cipher designed by U.S. National Security Agency (NSA) [3] for embedded applications. It has an 80-bit key with a 64-bit block length based on an unbalanced Fiestel network.

NOEKEON is a hardware-efficient block cipher by Daemen *et al.* [5]. HIGHT was designed by Hong *et al*. [6] as a generalized Fiestel-like cipher suitable for low-resource

devices. mCrypton is designed by redesigning Crypton by compact implementation of both hardware and software. Leander *et al.* [7] proposed a family of new lightweight variants of DES. Instead of using eight S-boxes, new variants of DES use just one S-box.

Bogdanov *et al.* [8] proposed an ultra-lightweight block cipher called PRESENT. Its design is extremely hardware efficient as it uses diffusion layer without any algebraic unit.

De Canni`ere *et al.* [9] proposed a new family of ultra lightweight block ciphers called KATAN and KTANTAN. Both of them uses an 80-bit key length with 32, 48, or 64-bit block size, while KTANTAN is more compact in hardware since its key is unchangeably burnt on devices.

Engels *et al.* [10] proposed a novel ultra-lightweight cipher called Hummingbird with 256-bit key length and 16-bit block size. It is used for resource-constrained devices.

Tomoyasu *et al.* [11] proposed a lightweight cipher called TWINE which is based on a Generalized Feistel Structure (GFS), a classical approach to block cipher. In hardware, it can be implemented with 1.5 KGates and low-end micro-controllers due to its small memory consumption. This lightweight cipher finds applications and is suitable for secure encryption and authentication for cars, RFIDs and sensor nets, etc.

As far as GFS is concerned, it is helpful in enabling small implementations for both software and hardware. However, it generally requires several iterations to make the resulting cipher sufficiently secure. To recover this drawback, TWINE employs an improved variant of GFS which results in making it to be ultra lightweight while keeping sufficient speed.

Biham *et al.* have discovered an impossible differential attack on 31 of the 32 rounds [12] of Skipjack. Knudsen *et al.* [13] published a truncated differential attack against 28 rounds of Skipjack [12]. Similar to these attacks, this paper will try to highlight all possible attacks on the available lightweight ciphers.

The remaining of this paper is organized as follows. Section II will discuss generic design criteria of lightweight block ciphers. Lightweight block ciphers, their hardware & software specifications and different cryptanalytic attacks are described in section III.

II. DESIGN CRITERIA OF LIGHTWEIGHT BLOCK CIPHER

Conventional algorithms such as Advanced Encryption Standard (AES) were expensive in context of implementation and hence were unsuitable for applications where there was presence of strict power constructs and limited resources. In order to solve this deficiency of existing algorithms, new family of cryptographic algorithms were proposed under Lightweight Cryptography.

Before designing the lightweight cryptographic system, some principles need to be kept in mind such as,

- it should be computationally efficient and hardware optimized
- it should have low implementation cost
- it should be secure

Lightweight cryptography deals with designing ciphers for extremely resource constrained environments. These applications include RFID tags and sensor networks.

Designers of lightweight cryptographic schemes cope with the trade-off between security, costs, and performance. In case of block ciphers, the key length provides a security-cost trade-off, while the number of rounds provides a security-performance trade-off and the hardware architecture a cost-performance trade-off. Any two of the three design goals, security and low costs, security and performance, low costs and performance can be easily optimized, whereas it is very difficult to optimize all three design goals at the same time.

Modern block ciphers were primarily designed with good software implementation properties and not necessarily with hardware-friendly characteristics. If the goal is to provide extremely low-cost security on devices where both of those assumptions do not hold, it turns out that many modern block ciphers do not perform well for these scenarios.

Hence it became necessary to develop ciphers that were lightweight in nature and fulfilled desired requirements. Succeeding section will discuss several attacks that have been proposed on existing lightweight block ciphers.

III ATTACKS ON LIGHTWEIGHT BLOCK CIPHERS

Cryptanalysis aims at finding weaknesses of the algorithm, and developing a method of decryption. This analysis is based on the algorithm of algebraic structures falling into three main categories: differential attack, linear attack, and integral analysis. Analysis which is based on algorithm realization is called side channel attack uses the leakage of confidential information that may exist. Various types of cryptanalytic attacks are mentioned in fig 1.

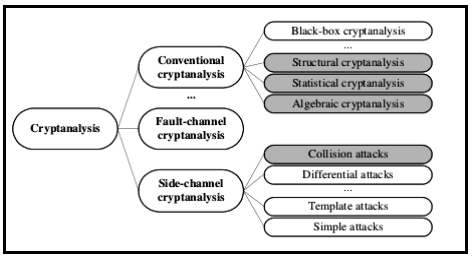

Figure 1: Showing types of Cryptanalysis

Black-box cryptanalysis uses the generic representation of algorithms to perform attacks which are based on the size of the internal state, if any, as well as on the lengths of inputs and outputs such as time-memory trade-off attacks, time-memory-data trade-off attacks, etc. Structural cryptanalysis includes attacks that are based on internal structure of algorithms signifying the properties of the high-level building blocks of the algorithms. In statistical cryptanalysis, the individual properties of the low-level building blocks of the algorithm, depicts the properties of the Boolean mappings describing the algorithm transformation such as linear cryptanalysis is based

on how well the algorithm transformation can be approximated by a linear mapping; differential cryptanalysis is based on how well differences in the input propagate to output differences. Algebraic cryptanalysis solves linear and nonlinear equations on input, output and key variables using algebraic representations of the algorithm transformation. Attack efficiency can be defined as a complex notion that can be interpreted in terms of time needed for the attack to succeed, financial costs of the attack, etc. Hardware-assisted attacks reduce both the time complexity and the financial effort required for the attack. The side-channel cryptanalysis additionally allows the adversary to observe physical parameters of the implementation during algorithm execution. Fault-channel cryptanalysis additionally allows the adversary to induce errors to the execution of a cryptographic algorithm.

This section describes various aspects of lightweight block ciphers. Along with this, their hardware specifications are also described. Several attacks which have been reported till date are specified along with the extent to which they are capable of resisting such attacks.

A. *PRINTcipher:*

The new block cipher PRINTcipher was presented as a light-weight encryption solution for printable circuits was proposed in 2011. It implements Sub space attack which breaks the full cipher for a significant fraction of its keys. This attack can be considered as a weak-key variant of a statistical saturation attack. For such weak keys, a chosen plaintext distinguishing attack can be mounted in unit time [14].

B. *HIGHT:*

HIGHT (high security and light weight) was proposed by *Hong et al*. in 2006. It possesses 64-bit block length and 128-bit key length is suitable for low-cost, low-power, and ultra-light implementation. It undergoes 32-round iterative structure which is a variant of generalized Feistel network. The operations included in it are its salient feature. It consists of simple operations such as XOR, addition mod 28, and left bitwise rotation. Hence, it can be thought of being hardware-oriented rather than software-oriented. Its other hardware specification is summarized in Table 3.

HIGHT can be implemented with 3048 gates on 0.25 μ m technology. Its circuit processes one round encryption per one clock cycle, thus its data throughput is about 150.6 Mbps at an 80 MHz clock rate. This performance is much faster than those of recently proposed low-resource hardware implementations of AES [15]. Comparison chart of HIGHT with AES is given in Table 1.

One of the attacks known as saturation attack [16, 17] uses a saturated multi-set of plaintexts. For an adversary, the property of XOR sum should be known that XOR sum of particular parts of the corresponding cipher texts is zero. This is known as saturation characteristic. These characteristics are useful for the attack and are often found in block ciphers in which small portions of the bits are interleaved by a strong nonlinear function while the main interleaving stage is linear.

Another attack called as the Boomerang attack [18] uses two short differential characteristics having relatively high probabilities instead of one long differential with low probability. Rest possible attacks of HIGHT are mentioned in Table 2.

Table 1: Comparison of the hardware implementation of HIGHT with AES's [15].

Algorithm	Technology (µm)	Area (GEs)	Throughput (Mbps)	Max frequency (MHz)
AES	0.35	3400	9.9	80
HIGHT	0.25	3048	150.6	80

Table 2: Showing various possible attacks on HIGHT [15]

ATTACKS	EXTENT TO WHICH THESE ATTACKS ARE POSSIBLE
Differential Cryptanalysis	➢ If applied on 13-round HIGHT without the final transformation, recovers the subkeys of the 12th and 13th rounds with 2^{62} plaintexts. ➢ It is impossible to find all of the corresponding differential characteristics of HIGHT for given 2^{64} possible input values.
Linear Cryptanalysis	➢ If applied on 13-round of HIGHT without the final transformation recovers 36 bits of the subkeys of the 1st, 12th, and 13th rounds. ➢ It requires 2^{57} plaintexts with the success rate 96.7%.
Truncated Differential Cryptanalysis	➢ It can be used to recover 96 bits of the subkeys used from the 11th round to the 16th round in 16-round HIGHT. ➢ The attack requires 214.1 plaintexts and $2^{108.69}$ encryptions of 16-round HIGHT.
Impossible Differential Cryptanalysis	➢ This attack requires $2^{46.8}$chosen-plaintexts and $2^{109.2}$ encryptions of 18-round HIGHT.
Saturation Attack	➢ Applies on 16-round of HIGHT. ➢ It requires 2^{42} plaintexts and 2^{51} encryptions of 16-round HIGHT.
Boomerang Attack	➢ Applicable on 11-round ➢ recovers the subkeys of the 13th round with 2^{62} plaintexts.
Interpolation and Higher Order Differential Attack	➢ Interpolation [13] and higher order differential [15] attacks are aimed against block ciphers which have low algebraic degree. ➢ Since the degree of a round function of HIGHT is 8, the full-round HIGHT has a high degree as a vector Boolean function.
Algebraic Attack	➢ A round function of HIGHT is the degree 8 as a vector Boolean function, it may be impossible to convert any equation system in HIGHT into an over-defined system.

Slide and Related-Key Attacks	➢ HIGHT uses different constant for each round, ➢ It is secure against slide attack. ➢ 8-round related-key boomerang distinguisher is composed of two short related-key differential characteristics with relatively high probability; ➢ This is useful to attack on 19 rounds HIGHT but can be used to attack on full-round HIGHT.
Weak Keys	➢ it is very difficult to find such kind of weak keys in HIGHT.

Table 3: Gate count for hardware implementation of HIGHT [15]

C. PRESENT:

COMPONENT	GATE COUNT
Round Function	838
Key Schedule	1648
Control Logic	562
Total	***3048***

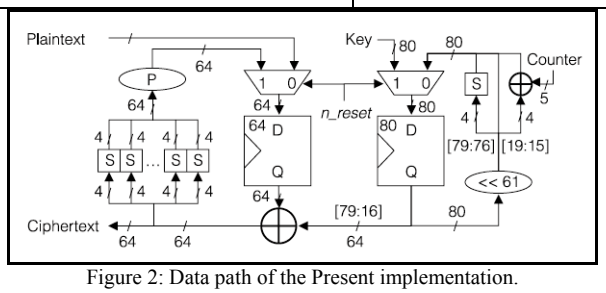

Figure 2: Data path of the Present implementation.
(S: substitution layer; P: permutation layer.)
(Source: Bogdanov et al. [13])

PRESENT is an example of an SP-network [13] and consists of 31 rounds. Its block length is 64 bits and two key lengths of 80 and 128 bits are supported. In order to fulfill the current requirements, 80 bit PRESENT cipher is recommended [19].

This much amount of performance is considered to be more than adequate for low security applications required in tag-based deployments and is given in table 5 [19]. The most effective attacks are related-key attacks [2] and slide attacks [19], and both rely on the build-up of identifiable relationships between different sets of subkeys. Remaining attacks are as given in Table 4.

ATTACKS	EXTENT TO WHICH THESE ATTACKS ARE POSSIBLE
Differential and linear cryptanalysis	➢ maximum differential probability of a present S-box is 2^{-2} ➢ hence probability of a single 2^5-round differential characteristic is bounded by 2^{100}. ➢ data required to exploit the remaining 2^5-round differential characteristic exceeds the amount available ➢ linear cryptanalysis of the cipher would require the order of 2^{84} known plaintext/ciphertexts.
Structural attacks	➢ design of present is almost exclusively bitwise and permutation operation is somewhat regular, ➢ the development and propagation of word-wise structures are disrupted by the bitwise operations used in the cipher.
Algebraic attacks	➢ increase in block size, addition of s-boxes, and an appropriate version of linear diffusion layer yields in large system. ➢ Taking into consideration a system, which consists of seven S-boxes, i.e. a block size of 2^8 bits, its difficult to get a solution in a reasonable time to a two-round version of the reduced cipher ➢ algebraic attacks are unlikely to pose a threat to present.
Key schedule attacks	➢ all bits in the key register are a non-linear function of the 80-bit user-supplied key by round 21, ➢ each bit in the key register after round 21 depends on at least four of the user-supplied key bits ➢ when arriving at derivation of K^{32}, six bits are degree two expressions of the 80 user-supplied key bits, 24 bits are of degree three, while the remaining bits are degree six or degree nine function of the user-supplied key bits ➢ these properties are sufficient to resist key schedule-based attacks.

Table 4: Showing various possible attacks PRESENT [13]

Module	**GE**	**%**
Data state	384.39	24.48
s-layer	448.45	28.57
p-layer	0	0
Counter: state	28.36	1.81
Counter: combinatorial	12.35	0.79
Other	3.67	0.23
KS: key state	480.49	30.61
KS:S-box	28.03	1.79
KS: Rotation	0	0
KS: counter-XOR	13.35	0.85
sum	***1569.93***	***100***

Table 5: Showing Hardware performance of Present [13]

Table 6: Showing comparision of lightweight cipher implementation [13]

Cipher	Key size	Block Size	Cycles per Block	Throughput at 100KHz (Kbps)	Logic Process(μm)	Area	
						GE	Rel.
Block Ciphers							
PRESENT-80	80	64	32	200	0.18	1570	1
AES-128	128	128	1032	12.4	0.35	3400	2.17
HIGHT	128	64	34	188.2	0.25	3048	1.65
mCrypton	96	64	13	492.3	0.13	2681	1.71
Camellia	128	128	20	640	0.35	11350	7.23
DES	56	64	144	44.4	0.18	2309	1.47
DESXL	184	64	144	44.4	0.18	2168	1.38
Stream Ciphers							
Trivium	80	1	1	100	0.13	2599	1.66
Grain	80	1	1	100	0.13	1294	0.82

D. EPCBC:

EPCBC is a lightweight cipher that has 96-bit key size and 48/96-bit block size. This cipher is suitable for Electronic Product Code (EPC) encryption, which uses low-cost passive RFID-tags. EPCBC is based on a generalized PRESENT having block size 48 and 96 bits for the main cipher structure and customized key schedule design which provides strong protection against related-key differential attacks [20].

E. LBLOCK:

In the lightweight block cipher LBlock, the block size of is 64-bit and the key size is 80-bit. It came into existence in 2011. Its hardware implementation requires about 1320 GE on 0.18 μm Technology with a throughput of 200 Kbps at 100 KHz. The software implementation of LBlock on 8-bit microcontroller requires about 3955 clock cycles to encrypt a plaintext block [21].

Table 7: Showing various possible attacks on LBlock [21]

ATTACKS	EXTENT TO WHICH THESE ATTACKS ARE POSSIBLE
Linear	➢ Complexity estimation of linear cryptanalysis concludes that it is difficult to find useful 15-round linear-hulls which can be used to distinguish LBlock from a random permutation. ➢ Hence it is less prone to linear attacks.
Impossible Differential Cryptanalysis	➢ The time complexity of the attack is about $2\times2\times2^{78} \times 1/8 \times 20 \approx 2^{72.7}$ 20-round encryptions. ➢ Complexities of impossible differential attack on 20-round LBlock imply that the full 32-round LBlock has enough security margins against this attack.
Integral Attack	➢ An integral attack on 20-round LBlock based on the 15-round integral distinguisher can be done. ➢ The attack procedure is similar with the attack on 18-round LBlock.
Related-Key Attacks	➢ The best related-key differential obtained so far is a 13-round distinguisher with 26 active S-boxes, and its probability is $(2^{-2})25 \cdot (2^{-3}) = 2^{-53}$. ➢ For the 14-round related-key differential obtained, there are 32 active S-boxes and its probability is less than $(2^{-2})31 \cdot (2^{-3}) = 2^{-65}$.

Differential Cryptanalysis is one of the possible attacks of Lblock. Considering that there are at least 32 active S-boxes for 15-round LBlock and the best differential probabilities of si are all equal to 2^{-2}, then the maximum probability of differ rental characteristics for 15-round LBlock satisfies DCPmax ≤ $2^{32}\times (-2) = 2^{-64}$.This means there is no useful 15-round differential characteristic for LBlock, since the block length of LBlock is only 64-bit. Therefore, we believe that the full 32-round LBlock is secure against differential cryptanalysis. Possible attacks that can be mounted on Lblock are given in Table 7.

Software implementations of Lblock on 8-bit microcontroller only require about 3955 clock cycles to encrypt a plaintext block [21]. Hardware based performance is mentioned in table 8. Hence, LBlock can achieve competitive hardware and software performances compared with other known lightweight block ciphers.

Table 8: Showing Hardware Performance of lblock [21]

F. KLEIN:

Algorithm	Block size	Key size	Area #GE	Speed kbps@100 KHz	Logic process (in μm)
XTEA	64	128	3490	57.1	0.13
HIGHT	64	128	3048	188.2	0.25
mCrypton	64	128	2500	492.3	0.13
DES	64	56	2300	44.4	0.18
DESXL	64	184	2168	44.4	0.18
KATAN	64	80	1054	25.1	0.13
KTANTAN	64	80	688	25.1	0.13
PRESENT	64	80	1570	200	0.18
LBlock	64	80	1320	200	0.18

KLIEN implies a family of block ciphers having fixed 64-bit block size and variable key length of 64/80/96-bits. Depending upon different key length, the nomenclature of ciphers is done as KLEIN-64/80/96, respectively [22]. Differential characteristic of PRESENT has only 10 active S-boxes after 5 rounds. An integral attack will investigate the propagation of sums of many values, whilst a differential attack will consider the propagation of differences between pairs. In a byte-oriented cipher, the sum of a group differences might be a predictable value after certain rounds. Cryptanalysis attacks of KLIEN are described in Table 9.

Table 9: Showing various possible attacks of KLIEN [22]

ATTACKS	EXTENT TO WHICH THESE ATTACKS ARE POSSIBLE
Linear and Differential Attacks	➢ By combining the RotateNibbles and MixNibbles steps, KLEIN can achieve a balance between the minimum number of active S-boxes and the software performance for resource-constrained devices. ➢ Any four-round differential characteristic of KLEIN has a minimum of 15 active S-boxes.
Key Schedule Attacks	➢ For KLEIN-64/80/96, each bit in the key register depends on at least 4 user-supplied bits after 4/5/6 rounds. ➢ For KLEIN-64/80/96, all the bits in the key register are a non-linear function of the 64/80/96-bit user-supplied key by 8/10/12 rounds.
Integral Attack	➢ Based on the 15-round integral distinguisher, we can mount a key recovery attack up to 20-round LBlock ➢ Time complexities will increase to about $13 \times 2^{60} \approx 2^{63.7}$
Related-Key Attacks	➢ For related-key differential characteristic with high probability, controlling the number of active S-boxes is obtained ➢ For example: 14-round related-key differential obtained, there are 32 active S-boxes and its probability is less than $(2^{-2})^{31} \cdot (2^{-3}) = 2^{-65}$

G. HUMMINGBIRD:

Hummingbird possesses a small block size and is therefore expected to meet the stringent response time and power consumption requirements described in the ISO protocol without any modification of the current standard. It owns 16-bit block size, 256-bit key size, and 80-bit internal state [23]. Comparisons of Hummingbird with PRESENT are given in table 11.

The cube attack is applicable on Hummingbird with high probability if the degree of the internal state transition function in a stream cipher is low. Attacks that can be performed on Hummingbird are discussed in Table 10.

Table 10: Showing various possible attacks on Hummingbird [23]

ATTACKS	EXTENT TO WHICH THESE ATTACKS ARE POSSIBLE
Differential Cryptanalysis.	➢ The standard differential cryptanalysis method is not applicable to Hummingbird with practical time complexity.
Linear Cryptanalysis.	➢ Hummingbird encryption function could be bounded by the square root of 2^{16} multiplying by a constant. ➢ Resistant to linear cryptanalysis attack with practical time complexity.
Algebraic Attack.	➢ The internal state transition involves modulo 2^{16} operations. ➢ It is hard to apply efficient linearization techniques for algebraic attacks to Hummingbird.
Cube Attack	➢ The degree of the internal state transition function is very high. no linear equations of key bits can be used.
Slide and Related-Key Attack.	➢ The subkeys used in four small block ciphers are independent. ➢ The four rotors affect the output of each small block cipher in a nonlinear way. ➢ Slide attacks [9] and related-key attacks cannot be applied to the Hummingbird.
Interpolation and Higher Order Differential Attack.	➢ The algebraic degree of the Hummingbird encryption is high. ➢ It is difficult to apply interpolation and higher order differential attacks to the Hummingbird.

Table 11: Showing Memory consumption and Cycle Count Comparison [23]

Cipher	Key Size (bit)	Block Size (bit)	8-bit/16-bit Microcontroller	Flash Size (bytes)	Hex Code (bytes)	SRAM Size (bytes)	Init. (Cycles)	Enc. (cycles/block)	Dec. (cycles/block)
Hummingbird	256	16	ATmega128L	1,308	3.68	0	14,735	3,664	3,868
			MSP430F1611	1,064	2.95	0	9,667	2,414	2,650
PRESENT	80	64	ATmega163	1,474	-	32	-	646,166	634,614
			C167CR	-	9.67	-	-	1,442,556	1,332,062

H. DESL:

DESL (DES Lightweight) is based on the classical DES (Data Encryption Standard) design, but unlike DES it uses a single S-box repeated eight times [24].

The designers' goal was to minimize the probability of collisions at the output of the S-boxes and thus at the output of the f-function. As a matter of fact, it is only possible to cause a collision, i.e. two different inputs are mapped to the same output, in three adjacent S-boxes, but not in a single S-box or a pair of S-boxes due to the diffusion caused by the expansion permutation. The possibility to have a collision in three adjacent S-boxes leads to the most successful differential attack based on a 2-round iterative characteristic with probability $1/2^{34}$ [24]. Possible attacks of DESL are given in table 12.

- Use of a serial hardware architecture which reduces the gate complexity.
- Optionally apply key-whitening in order to render brute-force attacks impossible.
- Optionally replace the 8 original S-Boxes by a single one which further reduces the gate complexity.

Table 12: Showing various possible attacks on DESL [24]

ATTACKS	EXTENT TO WHICH THESE ATTACKS ARE POSSIBLE

Differential Cryptanalysis and Davis Murphy Attack	➢ Secure against certain types of linear and differential Cryptanalysis and the Davies-Murphy attack, ➢ More size-optimized, and more power efficient than DES.

Table 13:Showing Comaprision of Efficient ciphers based on Gate Count, Clock Cycles, and Current Consumption [24]

Ciphers	Gate equivalent		Cycles/block	μA at 100 kHz	Process μm
	Total	Rel.			
DESL	1848	1	144	0.89	0.18
DES	2309	1.25	144	1.19	0.18
DESX	2629	1.42	144	-	0.18
DESXL	2168	1.17	144	-	0.18
AES-128	3400	1.84	1032	3.0	0.35
HIGHT	3048	1.65	34	-	0.25
Trivium	2599	1.41	-	-	0.13
Grain-80	1294	0.70	-	-	0.13

I. KATAN:

KATAN is composed of three block ciphers, with 32, 48, or 64-bit block size and is denoted by KATAN32, KATAN48 and KATAN64. These three types of ciphers accept 80-bit keys, and have a different block size (n-bit for KATANn). These three block ciphers are highly compact and achieve the minimal size. The largest and most flexible candidate, KATAN64 of the family, uses 1054 GE and has a throughput of 25.1 Kbit/sec (at 100 KHz) [25].

- *KATAN32:*
  26-round differential characteristic have probability $(2^{-11})3 = 2^{-33}$[25].
- *KATAN48:*
  43-round differential characteristic has probability of at most 2^{-18}. This implies that any 129-round differential characteristic has probability of at most $(2^{-18})3 = 2^{-54}$[25].
- *KATAN64:*
  37-round differential characteristic has probability 2^{-20}. Hence, any 111-round differential characteristic has probability of at most 2^{-60} [25].

The linear bounds are 2^{-11} for 37 rounds and 2^{-31} for 111 rounds. The probability of any differential characteristic of 128 rounds can be bounded by 2^{-n} for KATANn 42-round KATAN32 has probability at most 2^{-11}.

KATAN undergoes impossible differential attack which is based on finding a differential which has probability zero of as many rounds as possible. The most common way to construct such a differential is in a miss-in-the-middle manner, which is based on finding two (truncated) differentials with probability 1 which cannot co-exist. Due to the quick diffusion, changing even one bit would necessarily affect all bits after at most 42 rounds. Slide Attacks is also possible on it which is based on finding two messages such that they share most of the encryption process given the fact that there is a difference between the deployed round functions. This is possible only for a very small number of rounds. Another attack known as related-key attack searches for two intermediate encryption values as well as keys which develop in the same manner for as many rounds as possible. Related-key differential attack is the only attack where there is a difference between the two families of ciphers according to their key schedule algorithm.

J. KTANTAN:

KTANTAN also consists of same block sizes. It is more compact in hardware as the key is burnt into the device. Comparison of this cipher with respect to other ciphers is given in table 15. KTANTAN32, the smallest cipher of the entire family, can be implemented in 462 GE achieving encryption speed of 12.5 Kbit/sec (at 100 KHz). KTANTAN48 is the version we recommend for RFID tags uses 588 GE [25]. Various attacks of KTATAN are discussed in Table 14.

Table 14: Showing various possible attacks on KATANTAN [25]

ATTACKS	EXTENT TO WHICH THESE ATTACKS ARE POSSIBLE
Differential and Linear Cryptanalysis	➢ Secure against differential and linear attacks.
Boomerang attack.	➢ The probability of a boomerang quartet in 128-round KATAN32 is at most 2^{-44} .
the impossible differential	➢ There is no impossible differential of more than 168 rounds.
Slide and Related-Key Attacks	➢ Considering KATAN32, there is no slide property with probability 2^{-32} starting from the first round of the cipher. ➢ If an attacker achieves the same intermediate encryption value after round 19 and round 118, he may find a "slid" pair which maintains the equality with probability 2^{-31} until the end of the cipher. ➢ Implies there are no good slid properties in the cipher family by changing even one singly bit of the key causes a difference after at most 80 rounds of similar encryption process.
related-key differential attack	➢ No related-key differential characteristic for more than 150 rounds of KTANTAN32 with probability greater than 2^{-32} .
Cube Attacks and Algebraic Attacks	➢ The low algebraic degree of the combining function, are susceptible to algebraic attacks or cube attack after 160 rounds.

Table 15: Showing comparison of Ciphers Designed for Low-End Environments (optimized for size) [25].

Cipher	Block (bits)	Key (bits)	Size (GE)	Gates per Memory	Throughput*	Logic Process

				Bit	(kb/s)	(μm)
AES-128	128	128	3400	7.97	12.4	0.35
AES-128	128	128	3100	5.8	0.08	0.13
HIGHT	64	128	3048	N/A	188.25	0.25
mCrypton	64	64	2420	5	492.3	0.13
DES	64	56		12.19	44.4	0.18
DESL	64	56		12.19	44.4	0.18
PRESENT-80	64	80	1570	6	200	0.18
PRESENT-80	64	80	1000	N/A	11.4	0.35
Grain	1	80	1294	7.25	100	0.13
Trivium	1	80	749	2^*		0.35
KATAN32	32	80	802	6.25	12.5	0.13
KATAN48	48	80	927	6.25	18.8	0.13
KATAN64	64	80	1054	6.25	25.1	0.13
KTANTAN32	32	80	462	6.25	12.5	0.13
KTANTAN48	48	80	588	6.25	18.8	0.13
KTANTAN64	64	80	688	6.25	25.1	0.13

*----A throughput is estimated for frequency of 100 KHz
---Fully serialized implementation (the rest are only synthesized)
---This throughput is projected, as the chip requires higher frequencies
---This is a full-custom design using C^2MOS dynamic logic

K. TEA:

It uses a large number of iterations rather than a complicated program. It was proposed in 1994 but its cryptanalysis attacks were reported during the period of 2002-2010. It can replace DES algorithm. It has 32 rounds and is faster than DES with 16 rounds.

All modes of DES are applicable with it. The cycle count can readily be varied, or even made part of the key. It is expected that security can be enhanced by increasing the number of iterations.

This cipher is vulnerable to attacks such as equivalent keys, related-key and slide attacks [26]. In equivalent keys attack, each key is equivalent to three others, implying that the effective key size is only 126 bits [26]. This leads to providing a method for hacking Microsoft's Xbox game console. When used in Xbox, it was used as a hash function [26].

Due to these attacks, a number of revised versions of TEA have been designed, including XTEA [26]. In 1997, Needham and Wheeler came out with it. TEA, extended tiny encryption algorithm, is a block cipher designed to correct weaknesses of TEA. Similar to TEA, XTEA is a 64-bit block Feistel network with a 128-bit key and consists of 64 rounds. In 2006, the best attack reported on XTEA was related-key differential attack on 26 out of 64 rounds of XTEA [26].

L. LED:

LED is a 64-bit lightweight block cipher that can handle key sizes from 64 bits up to 128 bits [27]. *Guo et al*. proposed it in 2007.

The keyed permutation present in LED is inspired from the Advanced Encryption Cipher (AES) structure. LED is capable of providing strong security arguments against all state-of-the-art attacks, even in the related-key model. In particular in case of differential and linear cryptanalysis, it can be shown that any 4-round differential path for any of the LED versions contains at least 25 active S-boxes (which are having a non-zero difference) in the single-key model. Even in the more pessimistic related-key model, any 16-round differential path for any of the LED versions contains at least 50 active S-boxes [27].

M. KEELOQ:

KeeLoq is a lightweight block cipher with a 32-bit block size and a 64-bit key proposed by *Bogdanov* in 2007. Despite its short key size, it is widely used in remote key less entry systems and other wireless authentication applications. Key recovery attack against KeeLoq that requires 2^{16} known plaintexts and has a time complexity of $2^{44.5}$ KeeLoq encryptions. Software simulations show that, given the data, the key can be found in 7.8 days of calculations on 64 CPU cores [28]. Complexity chart of keeloq on the basis of data, time and memory is described in table 16.

Attack Type	Complexity		
	Data	Time	Memory
Time-Memory Trade-Off	2 CP	$2^{42.7}$	≈ 100 TB
Slide/Algebraic	2^{16} KP	$2^{65.4}$	?
Slide/Algebraic	2^{16} KP	$2^{51.4}$	?
Slide/Guess-and-Determine	2^{32} KP	2^{52}	16 GB
Slide/Guess-and-Determine	2^{32} KP	$2^{50.6}$	16 GB
Slide/Cycle Structure	2^{32} KP	$2^{39.4}$	16.5 GB
Slide/Cycle/Guess-and-Determine	2^{32} KP	2^{37}	16.5 GB
Slide/Points	2^{32} KP	2^{27}	>16 GB
Slide-Channel Analysis	10-1000 traces	-	-
Slide/Meet-in-the-Middle	2^{16} KP	$2^{45.0}$	≈ 2 MB
Slide/Meet-in-the-Middle	2^{16} KP	$2^{44.5}$	≈ 3 MB
Slide/Meet-in-the-Middle	2^{16} CP	$2^{44.5}$	≈ 2 MB
Time-Memory-Data Trade-Off	68 CP,34 RK	$2^{39.3}$	≈ 10 TB
Related-Key	66 CP, 34 $RK^{\ggg}$	Negligible	Negligible
Related-Key	512 CP, 2 $RK^{\ggg}$	2^{32}	Negligible
Related-Key/Slide/MitM	$2^{17.6}$ CP, 2 $RK^{\ominus}$	$2^{41.9}$	≈ 16MB

Time complexities are expressed in full Keeloq encryptions (528 rounds).
KP: Known Plaintext; CP: Chosen Plaintext
$RK^{\ggg}$: Related Keys(by rotation); $RK^{\ggg}$:Related Keys(by LSB)

Table 16: Showing complexity comparison chart of KEELOQ [28]

N. NOEKEON:

The block size and the key size are both 128 bits. It produces a ciphertext after iterating a round function 16 times,

followed by a final output function. The specification of NOEKEON [29], provides a key schedule which converts the 128-bit "Cipher Key" (i.e. the original key) into a 128-bit "Working Key", which is used in the round function. However, the use of the key schedule is optional. If related-key attack scenarios [29] are not of a concern, then the key schedule is not applied this side channel attack model, it is possible to extract 60 independent linear equations over 99 (out of 128) key variables. To recover the whole 128-bit key, the attack requires only about 2^{10} chosen plaintext and $O(2^{68})$ time complexity.

O. MIBS:

MIBS operates on 64-bit blocks, uses keys of 64 or 80 bits and iterates 32 rounds [30]. Linear attacks are possible on MIBS up to 18-round, and the first ciphertext-only attacks are possible on 13-round MIBS. Differential analysis reaches 14 rounds, and impossible-differential attack reaches 12 rounds. These attacks do not threaten the full 32-round MIBS, but significantly reduce its margin of security by more than 50% [30].

IV CONCLUSION

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

ACKNOWLEDGMENT

The authors would like to acknowledge the support received from Scientific Analysis Group, Defence Research & Development Organization, Delhi.

REFERENCES

[1] Thomas Eisenbarth, Christof Paar and Axel Poschmann, Sandeep Kumar, Leif Uhsadel, "A Survey of light weight cryptography implementation", Design and Test of ICs for secure Embedded Computing.

[2] Zheng Gong, Svetla Nikova, and Yee-Wei Law, "KLEIN: A New Family of Lightweight Block Ciphers".

[3] Anjali Arora, Aditi and S.K. Pal, "Design and Analysis of Tweakable Block Ciphers", National Workshop on Cryptology, 2011.

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

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

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

[7] G. Leander, C. Paar, A. Poschmann, and K. Schramm. New lighweight DES variants. In A. Biryukov, editor, *Fast Software Encryption 2007 - FSE 2007*, Volume LNCS 4593, pages 196–210. Springer, Berlin, 2007.

[8] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. 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*, Volume LNCS 4727, pages 450–466. Springer Heidelberg, 2007.

[9] C. De Canni`ere, O. Dunkelman, and M. Kneˇzevi´c. Katan and Ktantan - a family of small and efficient hardware-oriented block ciphers. In C. Clavier and K. Gaj, editors, *Cryptographic Hardware and Embedded Systems - CHES 2009*, volume LNCS 5747, pages 272–288. Springer, 2009.

[10] D. Engels, X. Fan, G. Gong, H. Hu and E.M. Smith. Hummingbird: Ultra-Lightweight Cryptography for Resource-Constrained Devices. In R. Sion et al editors, *FC 2010 Workshops*, volume LNCS 6054, pages 3–18. Springer, 2010.

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

[12] E. Biham, A. Shamir, and A. Biryukov. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In J. Stern, editor, *Advances in Cryptology - EUROCRYPT 1999*, volume LNCS 1592, pages 12–23. Springer, 1999.

[13] L.R. Knudsen, M.J.B. Robshaw, and D. Wagner. Truncated differentials and skipjack. In M. Wiener, editor, *Advances in Cryptology - CRYPTO 1999*, volume LNCS 1666, pages 165–180. Springer, 1999.

[14] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, Erik Zenner, "A Cryptanalysis of PRINTcipher: The Invariant Subspace Attack".

[15] Deukjo Hong, Jaechul Sung, "HIGHT: A New Block Cipher Suitable for Low-Resource Device" 2006.

[16] A. Moradi and A. Poschmann. Lightweight cryptography and DPA countermeasures: A survey Workshop on Lightweight Cryptography for Resource-Constrained Devices - WLC'2010, 2010.

[17] J. Daemen, L. Knudsen and V. Rijmen, "The Block Cipher SQUARE", FSE'97, LNCS 1267, Springer-Verlag, pp. 137-151, 1997.

[18] S. Lucks, "The Saturation Attack - A Bait for Twofish," FSE 2001, LNCS 1039, Springer-Verlag, pp. 189-203, 2001.

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

[20] Huihui Ya, Khoongming Khoo, Axel Poschmann and Matt Henricksen, "EPCBC - A Block Cipher Suitable for Electronic Product Code Encryption", Singapore National Research Foundation under Research Grant, 2007.

[21] Wenling Wu and Lei Zhang. "LBlock: A Lightweight Block Cipher", ACNS 2011, LNCS 6715, pp. 327-344.

[22] Zheng Gong, Svetla Nikova and Yee-Wei Law, "KLEIN: A New Family of Lightweight Block Ciphers".

[23] Daniel Engels, Xinxin Fan, Guang Gong, Honggang Hu, and Eric M. Smith, "Ultra-Lightweight Cryptography for Low-Cost RFID Tags: Hummingbird Algorithm and Protocol".

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

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

[26] David J.Wheeler, Roger Needham, "A Tiny Encryption Algorithm ".

[27] Jian Guo, Thomas Peyrin, Axel Poschmann and Matt Robshaw, "The LED Block Cipher", CHES 2011, LNCS 6917, pp 326-341, Springer 2011.

[28] Wim Aerts, Eli Biham, Dieter De Moiti´e, Elke De Mulder, Orr Dunkelman, Sebastiaan Indesteege, Nathan Keller, Bart Prenee, Guy Vandenbosch, and Ingrid Verbauwhede, "A Practical Attack on Keeloq".

[29] Shekh Faisal Abdul-Latip, Mohammad Reza Reyhanitabar, Willy Susilo, and Jennifer Seberry, "On the Security of NOEKEON against Side-Attack".

[30] Asl Bay, Jorge Nakahara Jr , and Serge Vaudenay, "Cryptanalysis of reduced-round MIBS Block Cipher".

AUTHORS PROFILE

Anjali Arora. This author became a graduate degree holder in Information Technology from Maharishi Dayanand University, Rohtak in 2010. Currently, she is pursuing post-graduation in Information Technology from Banasthali Vidyapith. At present, she is undergoing her industrial training at Scientific Analysis Group, Defence Research and Development Organization, Delhi. She has presented and published a number of research papers in leading conferences of national and international levels. Her areas of interest lie in the field of Cryptography and Network Security.

Priyanka. This author became a graduate degree holder in Information Technology from Guru Gobind Singh Indraprastha University, Delhi in 2010. Currently, she is pursuing post-graduation in Information Technology from Banasthali Vidyapith. At present, she is undergoing her industrial training at Scientific Analysis Group, Defence Research and Development Organization, Delhi. She has presented and published a number of research papers in leading conferences of national and international levels. Her areas of interest lie in the field of Cryptography, Network Security and Multimedia Information Security.

Saibal Kumar Pal is currently working as Scientist 'F' at Defence Research and Development Organization, SAG, Delhi. He holds a PhD in the area of Information Security. His areas of interest are in cryptography, multimedia & network security, computational intelligence & data mining. He is in the editorial board & review / program committee of a number of journals & international conferences. He has over 100 publications in science, technology & management studies.