ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization Vol. 5, Special Issue 4, March 2016

National Conference on Signal Processing, Instrumentation and Communication Engineering (SPICE' 16)

Organized by

Dept. of ECE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India

AES Is For the Present Era, Whereas SIMON Could Be For the Future

Nithya R[1], Deepa S.Kumar[2]

PG Scholar [VLSI and Embedded Systems], Dept. of ECE, College of Engineering Munnar, Munnar, Kerala, India[1]

HOD, Dept. of CSE, College of Engineering Munnar, Munnar, Kerala, India [2]

ABSTRACT: The upcoming era, the so called Internet Of Things / IoT involves the interconnection of millions and trillions of sensors and other devices wirelessly. Though the IoT was born sometime between the year 2008 and 2009,it has an immense impact on various areas of our life which include business, science, education, humanity, medical fields, government sectors and many others. Interconnection of devices asks for proper security and hence block ciphers came into existence. Existing block ciphers such as AES are mostly designed specifically for desktop computing systems but the upcoming era cannot make use of these existing block ciphers as they involve resource constrained devices constrained on power , area utilised, memory , throughput and other aspects. This led to the requirement of lightweight block ciphers. Intense research has been done on these lightweight block ciphers. One among the recent proposal of lightweight block cipher is, by NSA in June 2013, is SIMON which is designed to be flexible, secure, simple and efficient and which acts as a very strong alternative to the existing AES. This paper concentrates on a comparison of the two block ciphers in terms of implementation aspects in hardware.

KEYWORDS: AES, Internet Of Things, Pervasive Computing, Lightweight block cipher SIMON.

I. INTRODUCTION

Internet Of Things(IOT)/Internet Of Objects is the upcoming era, wherein several objects can get interconnected with each other wirelessly. This upcoming era of IoT [3] and Pervasive Computing [2] causes immense changes in our lives. The evolution from the Internet from the initial days, to the upcoming era so called Internet Of Things is quite unimaginable. The invention of internet leads to the first phase of transformation in this world. That is the invention of internet has bought in changes in several phases of our life which includes education, communication science, business, humanity, in government sectors, in medical fields and various other sectors. It has been thus inferred that Internet has been one of the best, profound and wonderful inventions of man kind.

The second phase of Internet occurred from the evolution from Internet to Internet Of Things(IoT). This new era evolved in Massachusetts Institute of Technology (MIT), at the Auto-ID Center in the year 1999. The group had been working in the field of the emerging sensing technologies and networked radio frequency identification (RFID). In other words Internet of Things is the instant when more than people being interconnected to the internet, more “Things” are being connected to the internet. Several Studies revealed that IoT was born sometime in the year 2008 and 2009.It was also inferred that Internet is found doubling every 5.32 years which is an analogy to the Moore's Law in VLSI systems. The IoT era is the instant where millions and trillions of sensors being embedded onto the earth so that each and every action and event could be tracked, thus enabling us to closely watch the earthly activities in various angles and circumstances.

And security is important aspect for many of these devices when millions of devices are being brought together: a hacker should not be taking control of the insulin pump or overriding the brakes in a car. The security issues are addressed by the cryptographic concepts. And that we are moving into the Internet Of Things era, it is the lightweight cryptography and the lightweight platforms that comes into existence. The obvious question is, Why lightweight platforms do not accomodate AES?, Inspite that AES has been suggested for even lightweight use. However, for the constrained environments, AES is not the right choice specially in hardware, for example, the emerging statistics asks for area not exceeding 2000 gate equivalents in resource constrained devices, meanwhile the smallest implementation of AES itself requires 2400 hence AES cannot be used for resource constrained devices as it would result in unwanted waste of chip area.

Existing cryptographic algorithms were designed keeping in mind the desktop computing systems. Now that we are moving on into IoT era ,there is necessity that the block ciphers ought to be used on the resource constrained platforms and software based devices which are intended to communicate wirelessly and thus it is there is a consequent shift to the world of Lightweight cryptography .The block ciphers designed specifically for the Light weight Cryptography are the Lightweight block ciphers. A lot of research work has already been going in this area.

II. AES

Advanced Encryption Standard(AES), [1] which is a specification of National Institute Of Standards and Technology, it’s applications are in many and most reliably used and much of the work is going on in making AES lightweight. ASIC implementations of AES 128 utilizes about 2400 gate equivalents. It is found that it is quite difficult to make AES to accommodate the future resource constrained devices. For example a recent statistics commands the RFID tags to make use of only 2000 GE which is the chip area allocated for it’s security which is quite out of reach for AES on ASIC implementations. AES provides a high level of security, but not every application would ask for a high security. If 96 bits of security would be enough, then there would be no point in using an algorithm that provides 128 or 192 or 256 bits of security. Even in implementations where it requires only 64 bits, an algorithm demanding 128 bits would result in unwanted waste of chip area. This led to the work on the upcoming Lightweight block ciphers satisfying flexibility, efficiency security, and simplicity of the algorithm design**.**

III. INTRODUCTION TO LIGHTWEIGHT BLOCK CIPHERS - SIMON AND SPECK

It was not until the year 2011that, after the prompting by the U.S. Government with regard to the requirements of more lightweight block ciphers, work on SIMON and SPECK [4], [5], [8] began accompanied by the Research Directorate of U.S. National Security Agency (NSA). These lightweight block ciphers namely SIMON and SPECK were designed in such a way that they were to be flexible, efficient, simple and secure in order to be implemented for resource constrained devices. The proposal of these lightweight block ciphers ensured increased security benchmark for future Internet Of Things (IoT) devices. Henceforth the lightweight block ciphers were released in June 2013 by the NSA(National Security Agency).For the past two years intense work has been going on by the NSA cryptanalysts to ensure the cipher’s security and scrutinizing has been going on by various international cryptographic community around the globe. SIMON and SPECK are designed in such a way that these are flexible, as these are not meant for a single platform rather can be implemented on any resource constrained. An algorithm is at its best in hardware when it has small hardware implementations and when it results in minimal flash and SRAM usage it is known to be at it’s best in software implementations. These light weight block ciphers is known to work well on both hardware and software platforms though SIMON is tuned for hardware and SPECK is tuned for software.

Considering a different aspect of flexibility, it is not that an algorithm should work well on many platforms, it must as well have varying implementations on a single platform. For hardware applications , the algorithm must utilize the available resources in terms of area i.e only less area is to be utilized if an extremely constrained environment is the and must take the advantage if the constraints are not so tight and result in higher throughput and higher area applications. For software implementations, very small flash and SRAM usage should be the main concern, but low-energy and high-throughput implementations should be attainable as well. Thus the lightweight algorithms designed in such a way to be flexible to be able to accommodate on any platform and have varying implementations and therefore SIMON and SPECK were to be designed to be flexible in all aspects.

Flexibility can also be considered in another direction as well, as devices, platforms and it’s applications vary, it asks for the flexibility in block and key sizes of block ciphers as well, that is desktop computing accommodates 64 and 128 bits whereas, electronic product code (EPC) applications utilises typical block sizes of 48 or 96 bits. Key sizes used are designed to provide desired level of security, that is a low cost device uses key size of 64 bits to achieve adequate security and a sensitive device can require 256 bits of key. Thus with the varying applications SIMON and SPECK lightweight block ciphers are designed with flexible block and key sizes. SIMON and SPECK block ciphers, supports block sizes 32, 48, 64, 96, and 128 bits, and up to three key sizes. Thus each family of SIMON and SPECK accommodates ten algorithms in all.. Table 1 below lists the SIMON’s and SPECK.’s different block and key sizes, in bits.

TABLE 1: PARAMETERS OF SIMON AND SPECK

Block Size	Key Size
32	64
48	72,96
64	96,128
96	96,144
128	128,192,256

IV. THE SIMON FAMILY OF LIGHTWEIGHT BLOCK CIPHER

The SIMON [4] , [5] block cipher is known to be as SIMON2n, with an n-bit word, where n can be 16, 24, 32, 48, or 64. SIMON2n can have m-word key (mn-bit) and thus referred as SIMON2n/mn. For example, SIMON 128/192 refers to the instance of SIMON with 128-bit plaintext blocks and a 192-bit key. SIMON is specifically based on the Feistel mapping structure. The algorithm was designed in such a way to be extremely small and efficient in hardware and easy to serialize at distinct levels, without sacrificing for the software performance.

Round Functions of SIMON Block Cipher

SIMON2n encryption and decryptions involve the following operations on n-bit words:

- bitwise XOR, $\oplus$
- bitwise AND, &, and
- left circular shift, S^j, by j bits.

The key-dependent SIMON2n round function is nothing but the two-stage Feistel map as shown below , for k belongs to $GF(2)^n$

$R_k : GF(2)^n \times GF(2)^n \longrightarrow GF(2)^n \times GF(2)^n$ defined by

$R_k(x, y) = (y \oplus f(x) \oplus k, x)$

where $f(x) = (Sx \,\&\, S^8x) \oplus S^2x$ and k denotes the round key. The inverse of the round function, which is used for decryption, is

$R^{-1}_k (x, y) = (y, \oplus x \oplus f(y) \oplus k).$

The SIMON round function is as shown in the following Figure 1

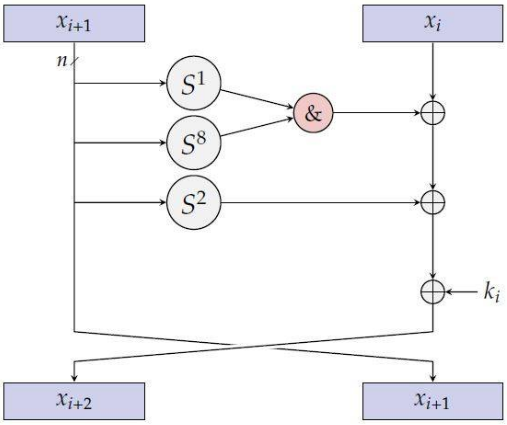


Fig. 1: Feistel Mapping Structure of SIMON round function

The SIMON parameters shown in the following Table 2. which makes SIMON flexible to be used in numerous applications.

TABLE 2: SIMON PARAMETERS

Block Size *2n*	Key Size *mn*	Word Size *n*	Key words *m*	Constant Sequence	Rounds *T*
32	64	16	4	Z_0	32
48	72	24	3	Z_0	36
	96				
			4	Z_1	36
64	96	32	3	Z_2	42
	128				
			4	Z_3	44
96	96	48	2	Z_2	52
	144				
			3	Z_3	54
128	128	64	2	Z_2	68
	192				
	256		3	Z_3	69
			4	Z_4	72

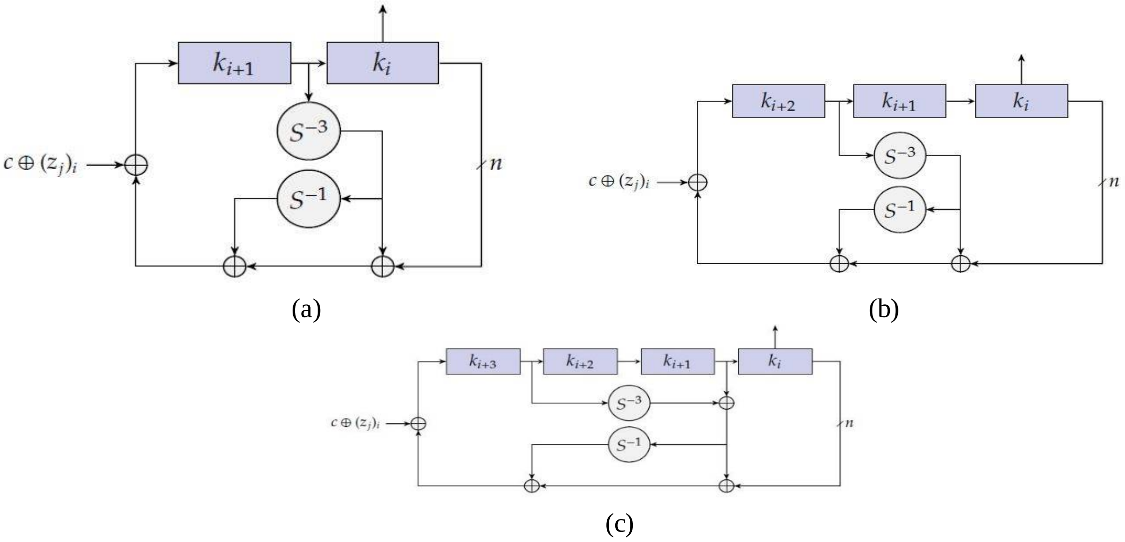
Key Schedule of SIMON Block Cipher

Except for the use of distinct round key in each round ,all rounds of SIMON are quite same and the round key is what makes each of the round distinct. Use of a sequence of 1-bit round constants eliminates slide properties and circular shift symmetries..The c used in key schedules is c = $2^n - 4$ = 0xff · · · fc.

Cryptographic separation is provided between different versions of SIMON having the same block size by actually incorporating five sequences: z0,…., z4. Each of these sequences is defined as follows:

z_0= 11111010001001010110000111001100 . . . ,
z_1= 10001110111110010011000010110100 . . . ,
z_2= 10101111011100000011010010011000101000010001111110010110110011 . . . ,
z_3= 11011011101011000110010111100000010010001010011100110100001111 . . . ,
z_4= 11010001111001101011011000100000010111000011001010010011101111 . . . ,

The SIMON two, three, and four-word key expansions are as shown in the following figures.



(a)
(b)
(c)

Fig. 2:The SIMON (a) two, (b) three, and (c) four-word key expansions

Though SIMON could be implemented on both hardware and software platforms, SIMON is tuned for hardware applications. Thus making SIMON more flexible and dedicated for future devices.

V. PERFORMANCE ANALYSIS OF SIMON AND AES ON RECONFIGURABLE HARDWARES(ASIC AND FPGAs) – A SURVEY

Many of the block ciphers designed so far were to be used only on a single platform such as ASIC ie dedicated to be used in a single platform only and not on others [6] and the criteria of flexibility is lost.This makes them less flexible and not liable to be used in the future devices as we are not sure about the devices yet to come. Thus the lightweight block ciphers are to be designed in such a way that it is to be flexible to be used on any hardware platform. The following tables 3,4, and 5 shows the survey of SIMON and AES performance analysis on ASIC and FPGA platforms [8].

TABLE 3: Performance analysis of SIMON and AES on ASIC platform
(clock speeds are 100 khz)

Size	Name	Area (GE)	Throughput (kbps)
48/96	SIMON	763	15.0
64/96	SIMON	838	17.8
64/128	SIMON	1000	16.7
96/96	SIMON	984	14.8
128/128	SIMON	1317	22.9
	AES	2400	56.6

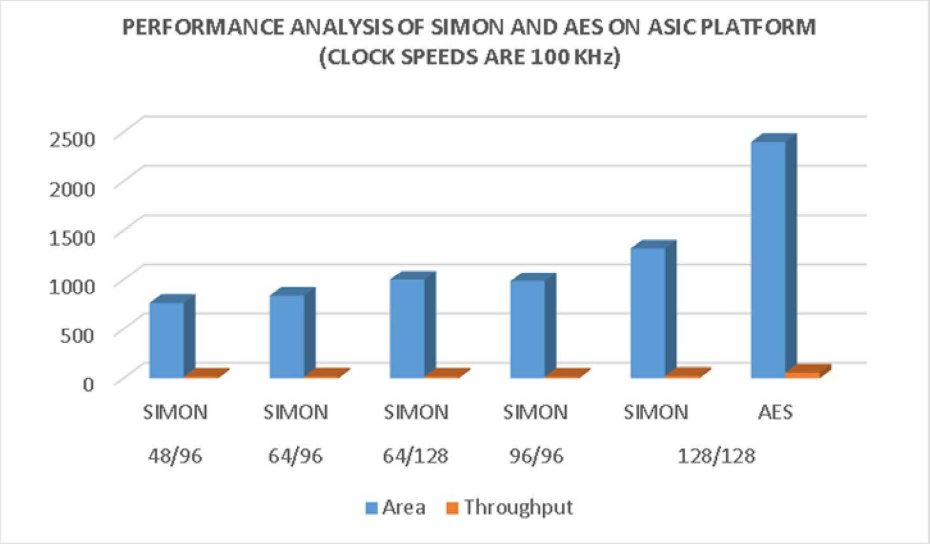


TABLE 4: PERFORMANCE ANALYSIS OF SIMON AND AES ON SPARTAN 3 FPGA

Size	Name	Area (slices)	Throughput (kbps)
64/128	SIMON	24	9.6
128/128	SIMON	28	5.7
	AES	184	36.5

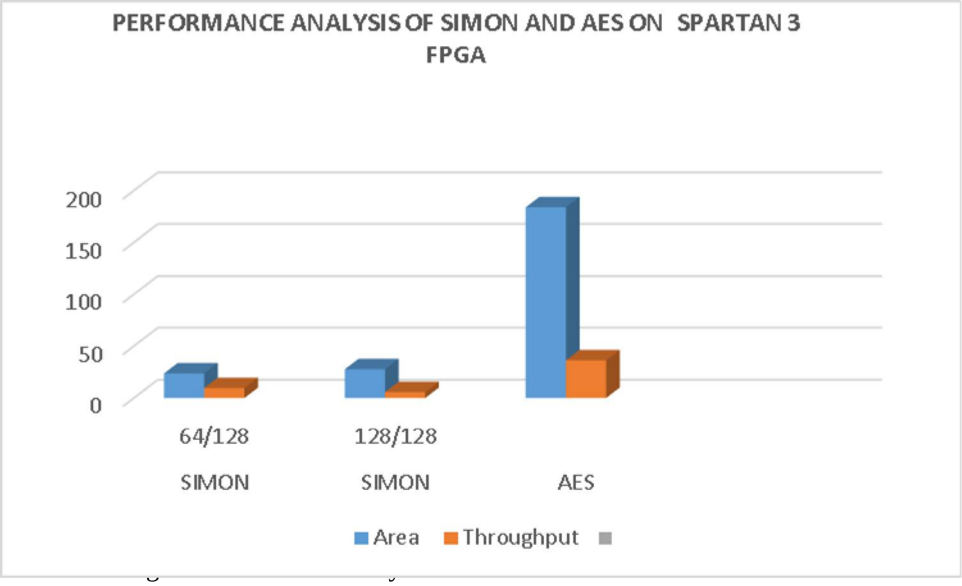


TABLE 5: PERFORMANCE ANALYSIS OF SIMON ON SPARTAN 6 FPGA

Size	Name	Area (slices)	Throughput (kbps)
64/128	SIMON(iterative-Integrated Ram routing)[9]	105	206.524
128/128	SIMON (bit serialized)[7]	36	3.6

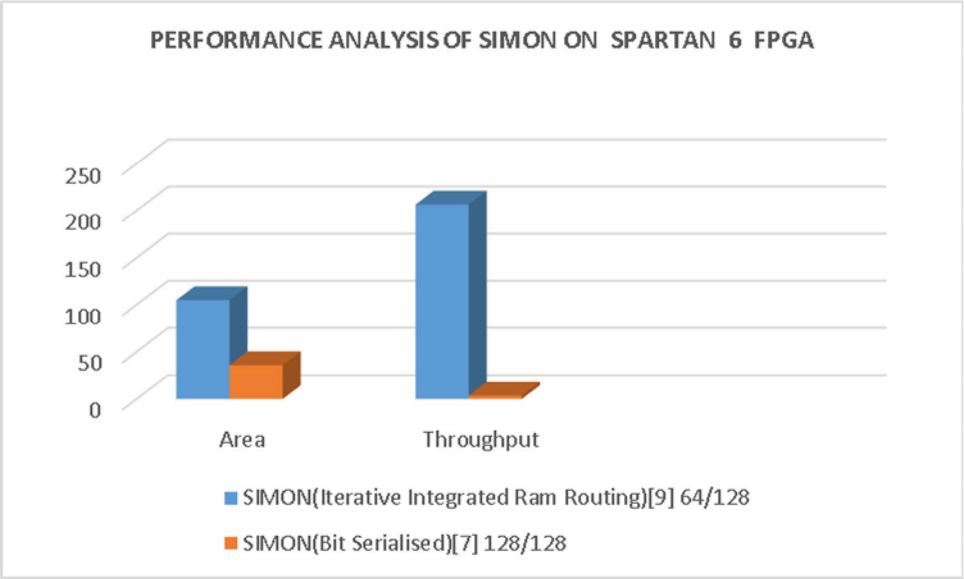


Fig. 5: Performance Analysis of SIMON and AES on SPARTAN 3

From the Tables 3,4 and 5 and the charts in figures 3,4 and 5,it is possible to infer that SIMON has the least area utilisation when compared to AES. The main objective of IoT is that it must make use of resource constrained devices constrained in area ,power, throughput and memory. Hence SIMON works better in reconfigurable platforms such as ASICs and FPGAs when compared with the AES in terms of area which is to be considered important for resource constrained platforms. The throughput of SIMON is found to be less when compared with AES as we notice from Table 3 and 4.Hence SIMON configurations could be implemented in lower technology boards such as Zedboard and the performance can be evaluated. Though SIMON is yet to be standardised ,the immense reduction in area can make it to be used in the Internet Of Things era.

VI. CONCLUSION

Internet Of Things being the upcoming era requires making use of resource constrained devices. Hence to provide security one of the lightweight block cipher recently proposed by NSA namely SIMON could be used indeed for the IoT era.The lightweight block cipher SIMON acts as a very strong alternative to the existing AES in terms of area and thus can be used efficiently and thus SIMON is most reliable that it can be used for resource constrained devices in the Internet of Things era. Hence the lightweight block cipher SIMON is designed in such a way that it must be flexible to be implemented on any hardware even the future devices yet to come, and it is simple, efficient and secure.

REFERENCES

.
[1] .J. Daemen and V. Rijmen," Aes proposal": Rijndael, 1999.
[2] M. Satyanarayanan, ,"Pervasive computing: Vision and challenges" ,Personal Communications, IEEE, vol. 8, no. 4, pp. 10–17, 2001
[3] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey", Computer networks, vol. 54, no. 15, pp. 2787–2805, 2010.
[4] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers," The simon and speck families of lightweight block ciphers".,IACR Cryptology ePrint Archive, vol. 2013, p. 404, 2013
[5] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The simon and speck lightweight block ciphers", in Proceedings of the 52nd Annual Design Automation Conference, p. 175, ACM, 2015.
[6] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "Performance of the simon and speck families of lightweight block ciphers", Agency NS
[7] A.Aysu,E.Gulcan,and P.Schaumont,"Simonsays:Break area records of block ciphers on fpgas",Embedded Systems Letters,IEEE,vol.6,no.2,pp.37-40,2014
[8] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "Simon and speck: Block ciphers for the internet of things", in NIST Lightweight Cryptography Workshop, vol. 2015, 2015. J. Wetzels and W. Bokslag ,"Simple simon: Fpga implementations of the simon 64/128 block cipher", arXiv preprintar Xiv:1507.06368,2015.