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

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 8, August 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.569

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

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008170 |

Spartan-6 FPGA Implementation of SIMON Light Weight Block Cipher Algorithm on 45 nm and 90 nm Technology

Anil Gopal Sawant [1], Akhilesh Kumar Mishra [2], Vilas N. Nitnaware [3]

Research Scholar, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan, India[1]

Professor, Department of ECE, Shri Jagdishprasad Jhabarmal Tibrewala University, Rajasthan, India[2]

Professor, D. Y. Patil School of Engineering Academy, Pune, India[3]

ABSTRACT: In the era of twenty first century, there are new technologies like internet of things, artificial intelligence, block chain technology, cyber security, data Science, cryptography, mobile technology (5G /6G), augmented reality and virtual reality. These technologies are emerging, developing, and enhancing their operational as well as research use in various engineering fields. These technologies provides services and related applications in many areas which was not explored in last decade. These technologies expands to new horizon in many fields in such a way that it explores new possibilities in every stage in order to serve better world and whole mankind. Security requirement of these technologies are depending upon their use in different field, different services, different applications and to provide such security, Cryptography plays important or critical role. Proposed SIMON Block Cipher algorithm implemented in Verilog HDL and Simulated and Synthesized in Integrated Environment synthesis Xilinx 14.6 version software. Actual result of SIMON Operation is validated on hardware in the form of Spartan 6 FPGA and also used Arduino software for communication between Spartan 6 FPGA and PC. Proposed design of 64/128 bit Simon Cipher also synthesized in Synopsys Design vision and Cadence RC compiler with a 45 nm and 90 nm technology. On 100 Mhz frequency received 0.86 mw total power consumption for 45 nm technology and 0.0638 mw total power consumption for 90 nm technology which is far better than previously implemented designs. In this Paper, Proposed approach demonstrating experimental results for Simon block cipher algorithm puts this algorithm in the category of light weight block cipher which outperformed in resource constraint, less hardware and low power embedded environment where IOT devices are extensively used.

KEYWORDS: Cryptography, Block Cipher, FPGA, Internet of things, Artificial Intelligence, Mobile Technology

I. INTRODUCTION

Now Technologies are improving in all areas of research and use of technology whole populations of the globe connected together in different ways. Many Countries investing billions and billions dollars and taking so much efforts to develop advanced technologies such as 5G/6G mobile technologies by launching to many satellites in the space to verify the advanced communication technologies which works on Terahertz (Thz) or few hundred GHz. 5G /6G mobile technologies are under developments at various stages of Planning, Testing and Implementations in many countries around the globe. Many countries like China, united states, South Korea and Japan like almost 60 countries started launching these technologies where as India planning to launch these technologies. The use of these technologies can be use separately and also simultaneously or synchronously with each other because technologies are designed, developed, tested and implemented on small, medium, large or ultra large services, applications, platforms, functionalities[1]. Also these technologies are extensively used in different fields like Military and Defence, Power sector (grid management), Oil and Gas, Transportation and logistics, Engineering Fields, Medicine, Pharmacy, health care, Space Technology, Automotive industry, Banking Sector and so on. Whole world is connected and interacted with each other by means of electronics medium and also billions and billions electronics devices are interacted with themselves continuously by means of human intelligence or through Artificial Intelligence[1-3]. Speed at which these electronics devices establishes connections and interacted among themselves in microseconds which is very fast and continuously increasing[4]. These electronic devices whenever interacted or communicated, lots of data either generated or shared among themselves so interaction or communications between devices must be needs to be secured and the data/Information which electronic devices generated or shared also needs to be secured[4]. That means to provide secured communication and secured data[5], There is needs to be different layers of security to each stages are

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008170 |

required[2]. Cryptography basically used to provide security to data or information depending upon their requirements by applying some cryptographic algorithms[6]. These cryptographic algorithms are works on Encryption and Decryption process in two different types such as block cipher and stream cipher[1]. These block cipher and stream cipher can be implemented in three different ways like Symmetric, Asymmetric and Hash types. Nowadays symmetric block cipher algorithms used to secure electronic devices connections[2] and their data and it became a critical need in today's electronic world[3].

Proposed Cryptographic algorithm discussed is 64/128 bit simon block cipher algorithms. In Real Time applications generally are having restricted resources, Less Computation time, smaller area and less power consumptions apart from these constraints, needs to be focused on enhanced security[2-3] . Proposed Simon Block cipher works more efficiently than other block cipher algorithms in FPGA based advanced embedded system on Internet of things applications[6].

II. SIMON BLOCK CIPHER STRUCTURE

SIMON light weight Block Cipher which is designed to meet the requirement of future IOT devices in Resource or power constraint environment[6]. The Simon Cipher is a one bit-based cipher that uses a balanced Feistel network consisting of left shifts, logical XOR (⊕) and logical AND (∧) functions. The cipher employs a complex key schedule that is used against the data for a number of rounds[5]. This key schedule includes a sequence of constant bits to further strengthen the key. In order to balance security requirements with energy consumption, power, and physical space, the Simon Cipher supports a large number of key and data block configurations. Here Fig. 1 demonstrated one round function[1]. Block size 2n in two parts leftmost part represents Xi+1 and rightmost part represents Xi. Key which utilized in each round that indicated by Ki where i indicates round number. Round function carried out shifting operation , anding operation and Xoring Operation. In this research work the current block xi which is used to create logic for next block xi+1 and after completion of all rounds these blocks are swapped[1].

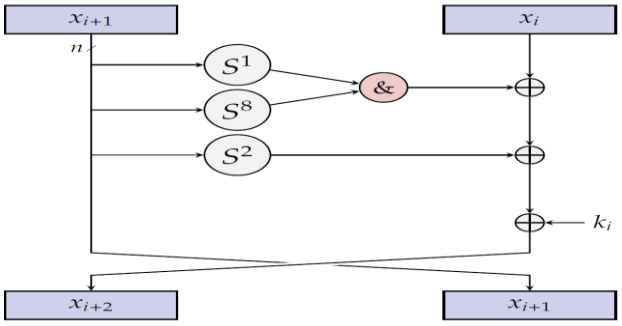

Fig. 1. SIMON one round Feistel Structure

SIMON Cipher is described in Table 1. Shows various parameters like the block size 2n, key size mn, word size n, key word m. block size and the key size which ultimately decides the number of rounds. Security of the cipher that depends upon rounds with given more attention to increasing the properties of confusion and diffusion. More the rounds, the stronger the security.

Table 1 SIMON Parameters and Rounds

Block Size 2n	Key Size mn	Word size n	Key Word m	Rounds
32	64	16	4	32
48	72	24	3	36
48	96	24	4	36
64	96	32	3	42
64	128	32	4	44
96	96	48	2	52
96	144	48	3	54
128	128	64	2	68
128	256	64	4	72

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008170 |

Key Schedule is designed to generate the key in each round. Key schedule techniques in Fig 2 which is focused on operations like shift right, XORing with a constant which is generally very simple and lighter than round function. Key word which decides the structure of key schedule expansion[1].

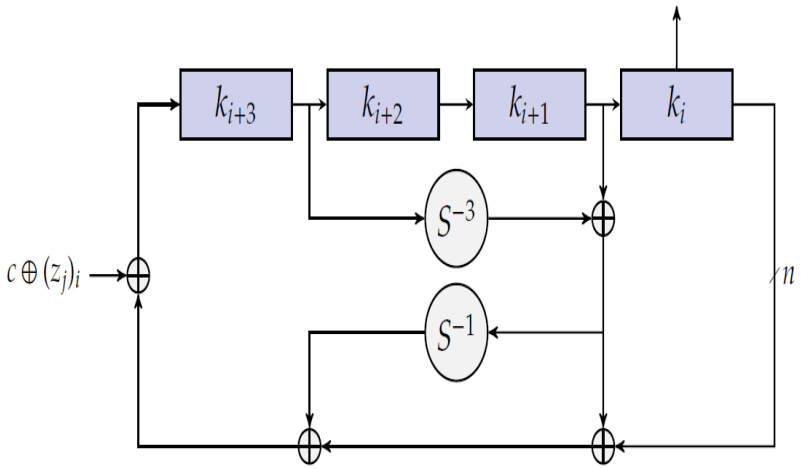

Fig 2. Simon Four word Key Expansion

III. RESULT AND DISCUSSION

Proposed design of 64/128 bit Simon cipher algorithms simulated and synthesized using Xilinx ISE 14.6 Environment in Verilog code. Proposed Design also validated on hardware in the form of Spartan 6 FPGA board and actual output of simon cipher which accessed from Spartan 6 FPGA on communication port of the PC using Arduino software. Hardware optimization successfully performed as Realized hardware or utilized hardware on Spartan 6 FPGA which is very less as compared to previous designs. Proposed design of 64/128 bit Simon Cipher synthesized in Cadence RC compiler and Synopsys Design vision with 45 nm and 90 nm technology. Total power consumption obtained on 100 Mhz frequency for 45nm technology is 0.86 mw and for 90 nm technology is 0.0638mw which is again very less than previous designs.

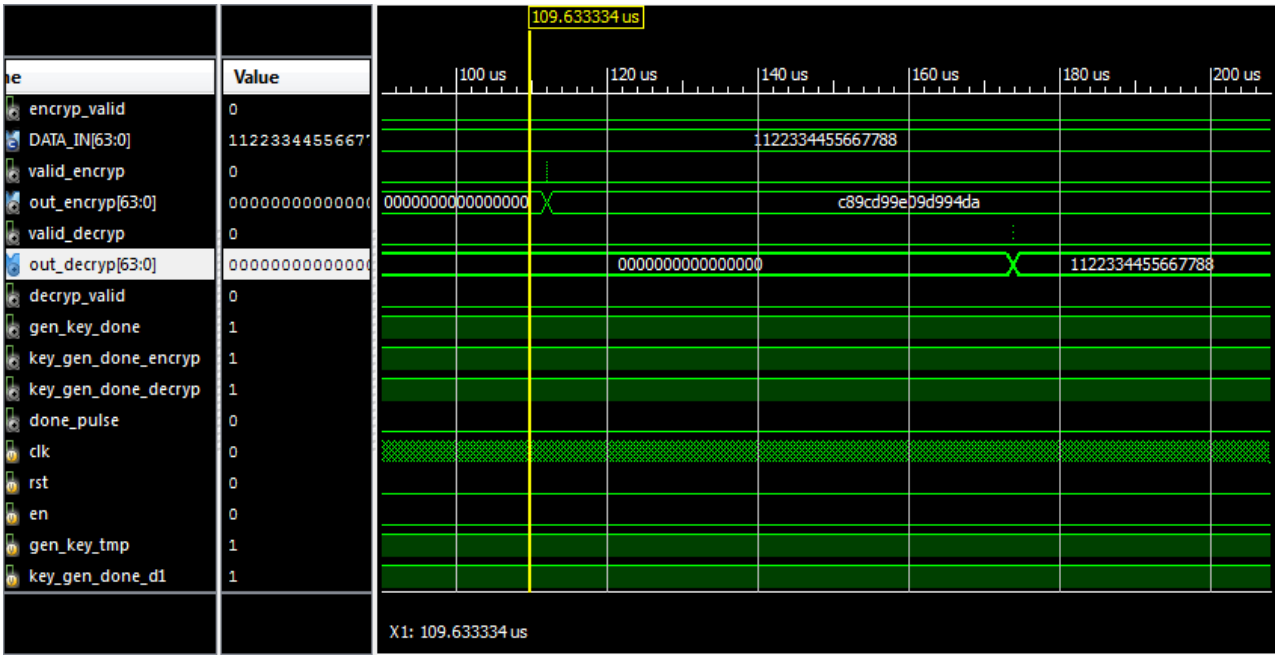

Fig. 3 Simon Simulation Result on Xilinx 14.6

| e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 7.569|

|| Volume 10, Issue 8, August 2021 ||

| DOI:10.15680/IJIRSET.2021.1008170 |

Table 2 Spartan 6 FPGA Hardware Utilization Report

Sr. No	Parameters	[3] Previous Simon Utilization	Proposed Simon Utilization	[4] AES Utilization	Speck Utilization
1	Block Size	64	64	128	64
2	Key size	128	128	128	128
3	Rounds	44	44	10	27
4	Number of Slice Registers	8222	2395	70	2283
5	Number of Slice LUTs:	9509	3817	151	4213
6	occupied Slices	4000	3816	46	2283

Table 3 Power Utilization Report

Sr. No	Parameters	[5] Previously implemented Simon cipher power consumption (65 nm)	Proposed Simon cipher power consumption (45 nm)	Proposed Simon cipher power consumption (90 nm)
01	Total Power Consumption	1.9 mw	0.86 mw	0.0638mw (63.82 uW)

IV. CONCLUSION

The Proposed design presented a ultra low power micro-architecture for the FPGA implementation of SIMON block cipher algorithm. This implementation shows that total power consumption on 100 Mhz frequency for 45 nm technology is 0.86mw which is half of the previously implemented designs and total power consumption on 100 Mhz frequency for 90 nm technology is 0.0638 mw which sets new record when compared with previously implemented designs. The proposed approach of Simon Cipher algorithm outperformed in hardware realization for FPGA that demonstrating FPGA hardware utilization is very less and ultra low power consumption with enhanced security architecture.

REFERENCES

[1] R. Beaulieu, et al,“ The SIMON and SPECK families of lightweight block ciphers”, 2013.
[2] Duc-Phong Le, et al, “Algebraic Differential Fault Analysis on SIMON Block Cipher”,IEEETransactions on Computers, Volume: 68, Issue: 11, Nov. 2019 Journal Article DOI:10.1109/TC.2019.2926081.
[3] Arkan Alkamil, et al,“ Efficient FPGA-Based Reconfigurable Accelerators for SIMON Cryptographic Algorithm on Embedded Platforms”, International Conference on ReConFigurable Computing and FPGAs (ReConFig), February 2020 DOI: 10.1109/ReConFig48160.2019.8994803
[4] Anil Gopal Sawant, Vilas N. Nitnaware, Anupama A. Deshpande, “Spartan-6 FPGA Implementation of AES Algorithm”,Springer Nature, Lecture Notes in Electrical Engineering 570, DOI:10.1007/978-981-13-8715-9_26, 2020
[5] Jaya Dofe, et al,“Strengthening SIMON Implementation against Intelligent Fault Attacks”, IEEE Embedded Systems Letters, Volume: 7, Issue: 4, Dec. 2015 DOI:10.1109/LES.2015.2477273
Ray Beaulieu, et al,“ Simon and Speck: Block Ciphers for the Internet of Things”, 52nd ACM /EDAC /IEEE Design Automation Conference (DAC) 2015 DOI: 10.1145/2744769.2747946

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.569

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details