Lightweight Block Cipher on VHDL

Mohd Saufy Rohmad, Azilah Saparon, Harith Amaran, Nazmin Arif, Habibah Hashim
Information Security and Trusted Infrastructure
Laboratory (InsTiL)
Faculty of Electrical Engineering, Universiti Teknologi MARA Shah Alam Selangor MALAYSIA
saufy@salam.uitm.edu.my

***Abstract*— Internet of Things (IoT) will change how we interact with our physical world. It will enable total sensing and controlling of most of the things around us. However, the practical acceptance of IoT from the market determine by the level of confidence perceived by the user. This is why IoT security is the main issues or concern of real IoT deployment. IoT security need light encryption engine that makes the encryption process very fast and efficient. Here we simulate the implementation of lightweight block cipher on VHDL that can be further realized on real hardware in the form of ASIC or FPGA chips. The results are compared from three points of views, security, physical size on hardware. Achieving the balance between these 3 areas is the key success of efficient cryptography implementation for IoT systems.**

Keywords—Internet of Things, Hardware Implementation, VHDL, FPGA, ASIC, Lightweight block cipher

I. INTERNET OF THINGS IS CHANGING THE WORLD

Internet of Things is changing our world. From 'big' into really tiny things, the world will be connected through internet. Since electronics is moving crazily into very tiny and smaller, it directly contributes to the birth of new sensing and actuating technologies. Everything will collide into a very small devices. Sensing, actuating, processing, encrypting and communicating. This is what the future era of IoT promise us. And the parts that interest us is the encryption part, where the level of user acceptance is really determined, whether data being communicate securely.

II. LIGHTWEIGHT CRYPTOGRAPHY

Lightweight Cryptography [1] is actually divided into lightweight asymmetric and lightweight block ciphers. We only focus on the lightweight block cipher in this research due to the fact that the asymmetric cipher that required for key exchange part is done before hand and the keys is hardwired on the sensor. Literature defines lightweight block ciphers as the ciphers that required less than 3000 physical gate counts. Basic architecture of lightweight block ciphers is inherit from the architecture of AES that based on substitution permutation network (SPN) and DES that based on Fiestal network. There are also other structure of lightweight block ciphers such as stream based and Lai-massey (combination between SPN and fiestal).

In this paper we choose 4 lightweight block ciphers which is Present, DESXL, TEA and simon.

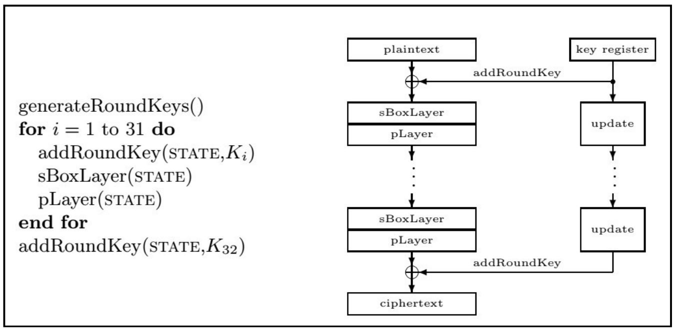
TABLE I. STRUCTURE OF SELECTED CIPHERS

	Key Size	Block Size	Round	Structure
Present	80	64	31	SPN
Simon	92	64	42	Fiestal
DESXL	184	64	16	Fiestal
TEA	128	64	64	Fiestal

Table I show the basic structure of selected ciphers. All ciphers are 64 bit block with the round number and key size that varied. Detail description of each cipher is in the original papers from the authors that with the detail of cryptanalysis for each ciphers.

Present [2] is lightweight block cipher created by group of researchers from Embedded security group, Ruhr university of bochum, Germany. It is based on the AES style that use substitution and permutation network (SPN) structure. Compared to AES that consist of 4 complex operations, Present only contain 2 simple operation that very light on hardware. The main focus of Present is to make it very compact in hardware and its being classified as ultra-lightweight block cipher.

Fig. 1. Internal operation of present



DESXL [3] is the lightweight version of DES. It inherits all DES structure with a few design simplification. Firstly the subtitution box is being reduce to single box and the whitening keys is applied to the cipher. It yield DESXL from its original DES.

TEA [4] is from Cambridge computer laboratory that defined very simple operations to be known as tiny encryption engine (TEA). It is a fiestal structure cipher that consist of two operation which is XOR and left shift.

Simon[5] is the most recent lightweight block cipher from NSA – national security agency, US. It is a fiestal based block cipher with variable size block cipher, with varied number of round for each encryption size. Fig. 2 shows the internal operation of single round SIMON which consist of XOR, AND and left bitwise rotation operation.

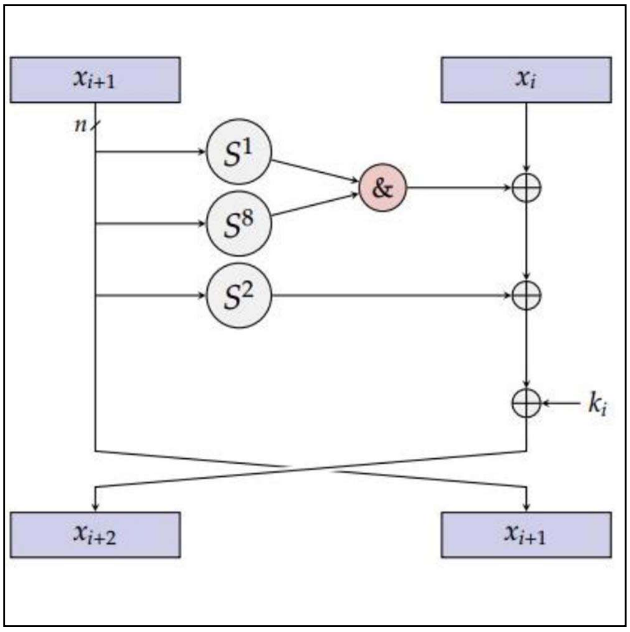


Fig. 2. Round Operation of SIMON

III. IMPLEMENTATION OF LIGHTWEIGHT CRYPTOGRAPHY

Theory and implementation can be very far different. Same goes in cipher implementation, the secure claim on theory can't guarantee secure in implementations. Practically, figure 3 below depict the reality of juggling between security, performance and cost of lightweight cipher implementations [6]. Security is the main part and objectives. However, it must be just adequate for the system requirement. Don't use cipher with too big key size because it will cost the performance and size. All of this factor need to be juggle smartly based on the requirement of the power, area, speed and security.

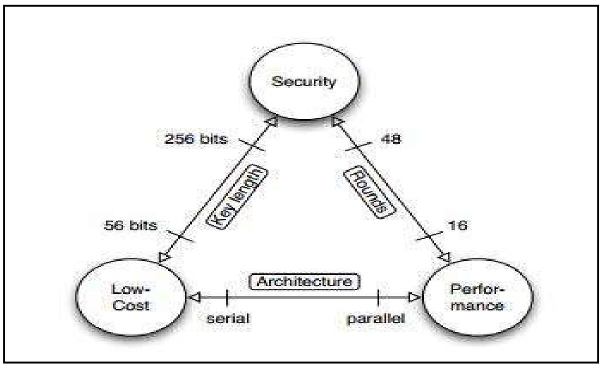


Fig. 3. Balance Triangle between Security, Performance and Cost.

IV. CIPHER ON HARDWARE

Computer system is a very complex machine. Determining the best implementation on a computer system is also a hard decision. On hardware itself there are a few implementation options. Firstly, it can be implemented as hardware block like we did in this paper. Secondly, it can be implemented with cipher processor as an instruction set. Thirdly, it can be integrated with existing soft microprocessor in the form of extension instruction set. Entire of this implementation options have its own advantages and disadvantages. In this paper, we choose the first type of implementation, hardware block of lightweight block cipher dedicated for each algorithm.

V. HARDWARE BLOCK FOR EACH CIPHER

The work is implemented using VHDL on Xilinx ISE tools. Each cipher is tested separately with its own test benches to ensure the results is correct and following the test vectors data specify by the cipher author. Each individual hardware block depict the implementation on VHDL including data and key lines, enable and clock lines.

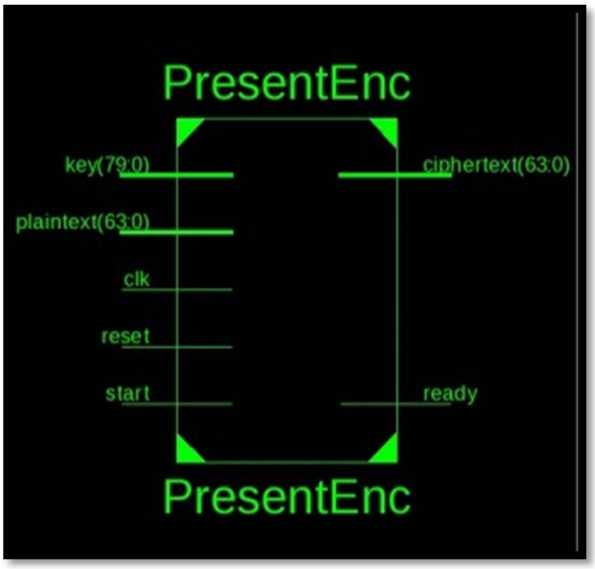


Fig. 4. Present Block with its I/O

Present hardware block that implemented is only consist of encryption operation. The relational is in IoT environment that have tight resource constrain, the sensor only need to encrypt data and the decryption process is performed on the server side.

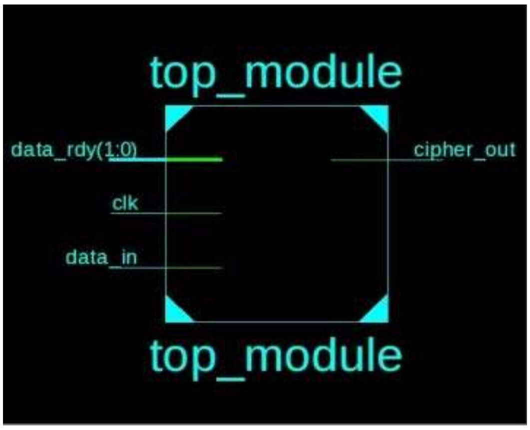


Fig. 5. Simon Block with I/O Pins

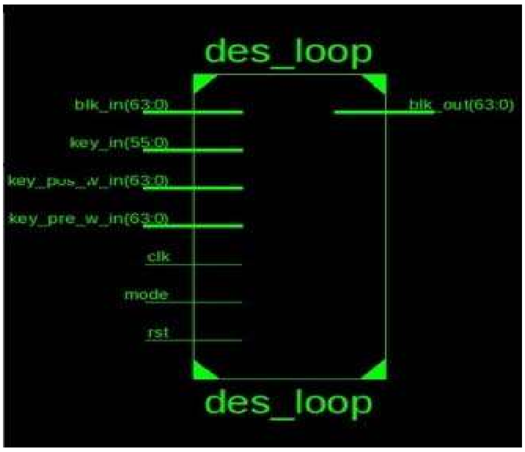


Fig. 6. Desxl Block with I/O Pins

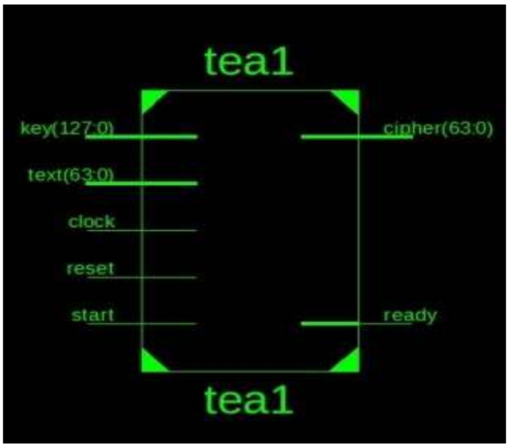


Fig. 7. TEA block with I/O Pins

Figure 5,6, and 7 show the I/O port of simon,desxl and TEA. It shows the port for inputting the plaintext, key and output port for ciphertext. Implementation on VHDL required this port to be defined as entity and the implementation detail of the entity is describe in architectural part.

VI. RESULTS AND DISCUSSION

We run the VHDL codes on Xilinx ISE and various results is produced by the systems. Comparing Xilinx and Altera FPGA tools, Xilinx tools seems to be more verbose in producing detail result of the hardware created.

Table 1 shows the result obtained from the experiment. Simon is the most recent cipher (2014) release by NSA (national security agency) that have very flexible internal characteristics. The key size and round is varied depend on the block size. It only consist of only three operations, shift left, bitwise and and xor and in the balance fiestal network, the heavy operation only performed on the half of that state (plaintext). Second smallest is present, followed by tea and DESXL. Why simon only need 30 slices? Because the structure is very simple and the strenght of the cipher depend on the number of round that use in simon. Maximum number of round needed by simon is 72 rounds.

TABLE II. PHYSICAL SIZE OF EACH CIPHERS

Size	Present	Simon	DESXL	TEA
Slice register	151	30	462	231
Slice LUT	218	52	602	232
LUT-FF	27	27	230	103
IO Block	5	5	315	260
Clock buffer	1	1	1	1

From the performance point, present score the fastest frequency with lowest period of each cycle. TEA with other side scores the slowest performance despite its simple architecture and implementation in both software and hardware.

TABLE III. PERFORMANCE OF EACH CIPHERS

	Present	Simon	DESXL	TEA
Min period (ns)	1.506	1.905	1.652	2.760
Max freq(MHz)	664.082	505.045	605.290	362.260
XST Synthesis Time (sec)	13	9.17	13	9

Its shows that the minimum period is directly inline with the maximum frequency that can be use on the circuit. Back to triangle in figure 3, the performance and size results can be relate to the cipher characteristics in table I so that we can see the balance between security strengths (which is for now we defined directly as a number of key bits), size on hardware (the number of slice register and LUT on FPGA), and the speed of the hardware.

For security parameters, we can extent the figure 1 with other detail attributes of the cipher.

TABLE IV. DETAIL EXPLANATION OF CIPHER ANALYZED

	Internal Op	Weakest Weakness	Round	Structure
Present	4 bit s-box Bit permutation	Key schedule attack[2]	31	SPN
Simon	Bitwise XOR Bitwise AND Left Rotation	Still unconcluded [7]	42	Fiestal
DESXL	xor with whitening keys single s-box 8x	Linear Cryptanalysis[3]	16	Fiestal
TEA	Left shift xor	Equivalent key attack[4]	64	Fiestal

Table IV shows detail explanation of each cipher that we used in this work. The weakest cipher is TEA that produce the weakest cryptanalysis result (from literature). Hence the most strong cipher is present due to the stringent cryptanalysis on it presented in the paper produce by its author.

This is one of the main objectives of the research, to find a balance between the security parameters (which is not directly proportional to key size actually), size or resources that being used and the performance of the cipher. This work will become a foundation on the future investigation of lightweight block cipher and be our basis for future experiment and implementation enhancement.

VII. CONCLUSION

This work presents our initial result on the implementation of lightweight block cipher on FPGA using VHDL. This is the basic implementation of such cipher. Other implementation method such as serial and parallel implementation is considered in future papers.

ACKNOWLEDGEMENT

Thanks to Ministry of Higher Education Malaysia for the NRGS – Niche Research Grant Scheme 600-RMI/NRGS 5/3 (5/2013) and Universiti Teknologi MARA (UiTM) for supporting this research. Thanks also for all lab members for the supports that motivates be in this research work.

REFERENCE

[1] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann and L. Uhsadel, "A Survey of Lightweight-Cryptography Implementations," in *IEEE Design & Test of Computers*, vol. 24, no. 6, pp. 522-533, Nov.-Dec. 2007.
[2] A. Bogdanov *et al.*, "PRESENT: An ultra-lightweight block cipher," in *Cryptographic Hardware and Embedded Systems - CHES 2007*. Springer Science + Business Media, pp. 450–466.
[3] G. Leander, C. Paar, A. Poschmann, and K. Schramm, "New lightweight DES variants," in *Lecture Notes in Computer Science*. Springer Nature, pp. 196–210.
[4] Tiny Encryption Algorithms[Online] https://en.wikipedia.org/wiki/Tiny_Encryption_Algorithm
[5] R.Beaulieu, D.Shors, J.Smith, S.Treatman-Clark, B.Weeks, L.Wingers, "SIMONand Speck: Blocks Ciphers for Internet of Things" *NIST Lightweight Cryptography Workshop* 20 July 2015.
[6]Axel York Poschmann (2009) Lightweight Cryptography: Cryptographic Engineering for a Pervasive World (Doctoral Dissertation). Retrieved from https://www.emsec.rub.de/research/theses/
[7] Hoda A. Alkharizmi, Martin M.Lauridsen (2013) Cryptanalysis of the SIMON Family of Block Ciphers : Presented in PhD summer school titled 'Theoretical and Practical Topics in resources-efficient Cryptography'.