Hardware Implementation of Modified A5/1 Stream Cipher

Siti Yohana Akmal Mohd Fauzi, Marinah Othman, Farrah Masyitah Mohd Shuib, and Kamaruzzaman Seman

***Abstract*— This paper describes the implementation of the modified cryptographic algorithm namely A5/1 stream cipher which is widely used in *Global System for Mobile* (GSM) communication. While there are numerous published work on the A5/1 stream, very few have implemented the modified design into hardware and none of them, to the best of the author's knowledge, has clearly analyzed as to how the different characteristics of the conventional A5/1 stream cipher would affect performance at hardware level implementation. Two modified designs with different total bits and combinational functions are implemented into hardware by means of an Field Programmable Gate Array (FPGA) board and the throughput, area consumption, power consumption as well as the throughput-to-area ratio performance of the hardware are analysed and compared with that of the conventional design of the A5/1 stream cipher. While the algorithms in use have the same level of randomness, and hence strength in terms of security, at the hardware level, when total bits in use is increased, the total power consumed actually reduces. It is also observed that the use of the XOR logic has the better power consumption rate, compared to when a multiplexer is implemented as the combinational function.**

***Index Terms*—A5/1 stream cipher, field programmable gate array, FPGA, throughput, cryptographic algorithm.**

I. Introduction

A5/1 stream cipher is a type of cryptographic algorithm that operates by generating streams of secret key which is used in GSM communication. The design was initially being kept secret from public as the developer believed in security through obscurity. However, the A5/1 stream cipher design was eventually leaked and led to several attacks that weaken the system. Though there are efforts to enhance the system design, not many had tested it to hardware level and to the best of author's knowledge, none of them had clearly defined how the modified characteristics affects the hardware performance [1]–[5].

In this paper, two designs with new combinational function; each with total bits of 64-bits and 128-bits respectively is proposed and implemented into hardware. The rest of the paper is organized as follow: Section II will look into the details of characteristics of conventional A5/1 stream cipher along with the proposed designs. Section III describes the methodology for hardware implementation by means of FPGA followed by a discussion on the analysis of the data obtained in Section IV. Finally, Section V will conclude the work.

Manuscript received February 26, 2017; revised April 23, 2017. This work was supported by the RAGS grant, under the Ministry of Higher Education Malaysia. (USIM/RAGS/FST/36/50813). SYAMF acknowledges a graduate fellowship through the MyBrain15 programme.

S. Y. A. M. Fauzi is with Faculty of Science and Technology, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai N. Sembilan, Malaysia (e-mail: sy.akmal91@ gmail.com).

M. Othman, F. M. M. Shuib, and K. Seman are with the Faculty of Engineering and Built Environment, Universiti Sains Islam Malaysia, Bandar Baru Nilai, 71800 Nilai N. Sembilan, Malaysia (e-mail: marinah@usim.edu.my, farrah@usim.edu.my, drkzaman@usim.edu.my).

II. Research Background

A. Structure of A5/1 Stream Cipher

The basis of the modified design of A5/1 stream cipher is the characteristics that made up the cryptographic system which are linear feedback shift register (LFSR), polynomials, clocking mechanism, and combinational function.

LFSR can be considered as the main characteristics that made up the system. Conventional A5/1 stream cipher design consists of three sets of LFSR, namely LFSR1, LFSR2 and LFSR3, with bit size of 19, 22 and 23 which sums up to 64 bits altogether.

The polynomials represent the tapping bits within the LFSR which are as in Equation (1), (2) and (3).

$$f(x) = x19 + x18 + x17 + x14 + 1 \quad (1)$$

$$f(x) = x22 + x21 + 1 \quad (2)$$

$$f(x) = x23 + x22 + x21 + x8 + 1 \quad (3)$$

The clocking mechanism used in the A5/1 stream cipher system is called the majority logic function. From each LFSR, one of the middle bit register (R[x]) is assigned as the clocking bit which is then compared with the clocking bits from the other LFSR. If the clocking bit is the same as the majority, then the LFSR will be shifted, else, it will remain as it is.

The combinational function is the final stage before a bit of the secret key is produced. The most significant bit (MSB) from each LFSR is XOR-ed to produce the secret key. The design structure for the conventional A5/1 stream cipher is shown in Fig. 1.

B. Bit Stream Generation Process

The bit stream produced from the A5/1 stream cipher is called the secret key (Ki) which is generated from the 64-bits session key (KC) and the 22-bit frame number (FN) that will be used in GSM communication [1]. The generation process can be broken down into two phases, the first being the initialisation phase, and the second, the Ki generation phase.

DOI: 10.7763/IJCTE.2017.V9.1171

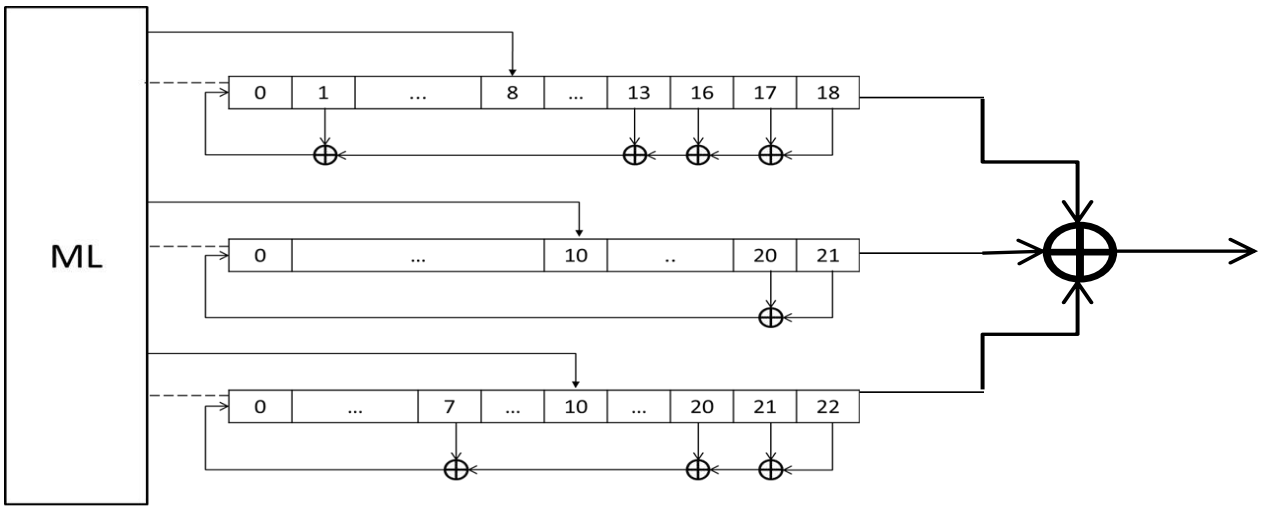

Fig. 1. Design structure of conventional A5/1 stream cipher.

The initialisation phase starts with all of the LFSRs being set to zero. Then, the 64-bits session key is shifted from the least significant bit (LSB) of each of the LFSRs, bit-by-bit by ignoring the majority logic function. This is then followed by the 22-bits frame number being shifted in the same fashion.

For the second phase, the LFSRs are clocked by abiding the majority logic function. However, the K_i is first produced only after 100 cycles. Then, 114 bits of K_i is produced which represent one frame. The next process will then increase the frame number by 1. The session key remains the same until the ongoing conversation is ended and a new conversation begins.

C. Proposed Design

Based on previous works [1], [2], the linearity of the combinational function is said to be one of the key factor that weakens the A5/1 stream cipher. Therefore, the proposed design uses a 4-to-1 multiplexer (Mux) as the combinational function. The detail of the design is as in Table I. Compared to the conventional A5/1, design 1 has a higher total bit, while in design 2, the combinational function is that of a Mux.

TABLE I: DESCRIPTION OF PROPOSED DESIGN COMPARED TO CONVENTIONAL DESIGN

	Polynomial	Total Bits	Clocking Bit	Combinational Function
Conventional	LFSR 1: $f(x)=x^{19}+x^{18}+x^{17}+x^{14}+1$ LFSR 2: $f(x)=x^{22}+x^{21}+1$ LFSR 3: $f(x)=x^{23}+x^{22}+x^{21}+x^{8}+1$	64	R[8], R10], R[10]	XOR
Design 1	LFSR 1: $f(x)=x^{19}+x^{18}+x^{17}+x^{14}+1$ LFSR 2: $f(x)+x^{22}+x^{21}+1$ LFSR 3: $f(x)=x^{23}+x^{22}+x^{21}+x^{8}+1$	64	R[8], R10], R[10]	MUX
Design 2	LFSR 1: $f(x)=x^{19}+x^{18}+x^{17}+x^{14}+1$ LFSR 2: $f(x)=x^{22}+x^{21}+1$ LFSR 3: $f(x)=x^{87}+x^{56}+x^{53}+x^{21}+1$	128	R[8], R10], R[10]	MUX

III. HARDWARE IMPLEMENTATION

In this study, the FPGA board used is the Spartan 3AN Starter Kit, programmed using Verilog and simulated using the Xilinx ISE Simulation software. The process for hardware implementation is illustrated by the flow chart in Fig. 2.

The first step for hardware implementation is to sketch the architecture design of the system. The design should specify the main system or top module along with all the subsystems or submodules and the interconnection wire.

(Clk) and left hand side and one output;

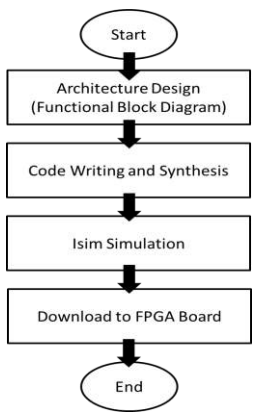

Fig. 2. Hardware implementation process.

As shown in the Fig. 3, there are three inputs, Start, Clock (Clk) and Reset located on the left hand side and one output; the Secret Key. The small boxes within is considered as submodules and the dotted line represent the interconnecting wires that connects one submodules to another.

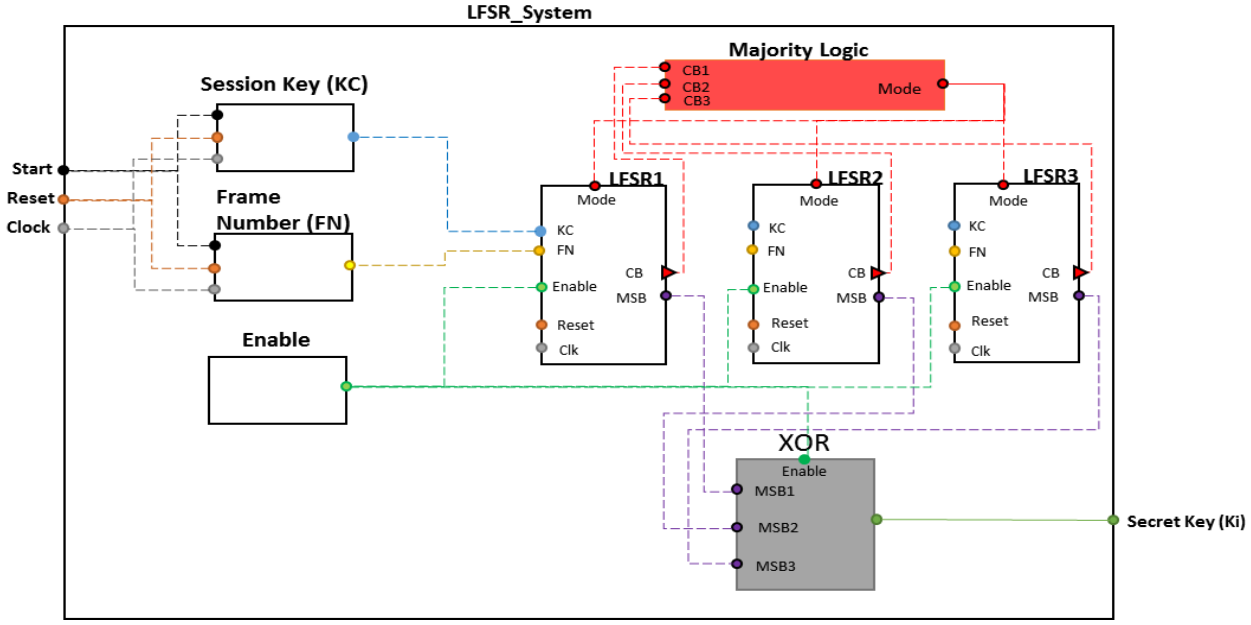

Fig. 3. Sketch design for conventional A5/1 stream cipher.

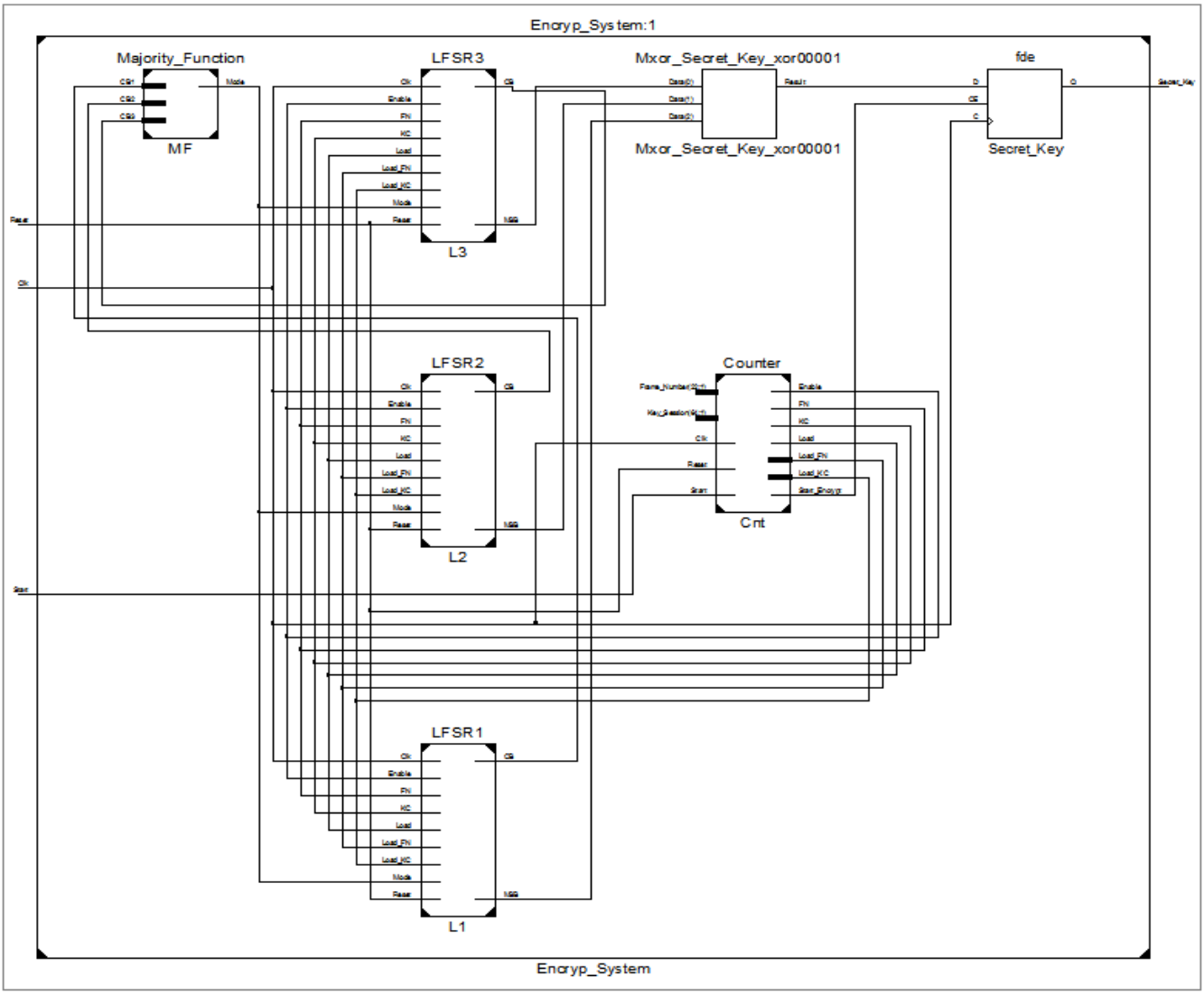

Fig. 4. RTL Schematic for conventional A5/1 stream cipher.

A. Hardware Programming

There are two well-known hardware description languages (HDL), which are the VHDL and the Verilog respectively. VHDL is short for VHSIC (Very High Speed Integrated Circuit) hardware description language. Between the two, the Verilog programming style is closer to both the C and the C++ languages. The difference between VHDL and Verilog lies on how the library is defined as well as how the system architecture is elaborated. In this study, Verilog HDL is opted.

The coding is written by referring to the architecture design; beginning from the submodules and finally the top module that links up all of the submodules. Once the coding is finished, it will be synthesized and if it returns an error, the coding must be fixed and 2re-synthesized. This process continues until no error is returned.

IV. Result And Analysis

A. RTL (Resistor-Transistor Logic) Schematic

Once the code synthesis returns zero error, the RTL schematic can be generated in order to validate the design. Fig. 4 shows the RTL schematic for the conventional A5/1 stream cipher design.

As shown in Fig. 4, there are no submodules KC, FN and Enable as it has been simplified and declared as port instead. This helps to save the total memory used. The Counter submodule is created to keep track of the cycles passed which is useful to trigger the start of the secret key generation.

B. ISE (Integrated Synthesis Environment) Simulation

ISE simulation or ISim is a tool developed by Xilinx to run timing simulations of a system design in order to observe and validate the functionality of the system designed [6]. The timing simulation for the conventional design of the A5/1 stream cipher is shown in Fig. 5, where it can be seen that the timing is broken into two phases: the initialization phase and the secret key generation phase.

The initialization phase starts with Reset being set to zero and the Load_KC is equal to one which marks the start of the key session feeding phase until it reaches the 64th cycle. Then the frame number feeding phase kicks in and continue for 22 cycles. During the initialization phase, no secret key is generated until the secret key generation phase begins.

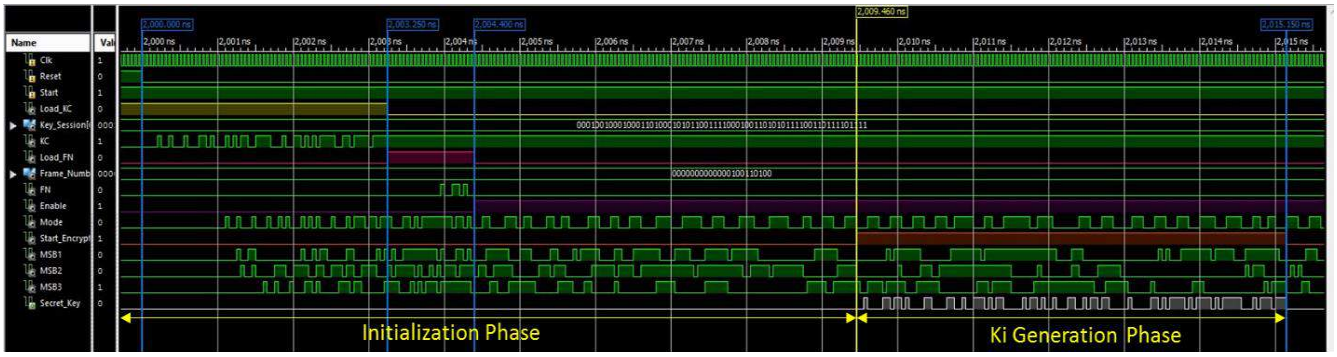

Fig. 5. Timing simulation for conventional A5/1 stream cipher.

C. Hardware Performance Result

Once the design has been implemented, the summary table of device utilization will be updated. In this work, the power consumption of the hardware is studied, as this parameter directly determines the performance of the algorithm when implemented into hardware.

TABLE II: Hardware Performance Result for Conventional and Proposed Designs

Design	Conventional	Design 1	Design 2
Power	39.86	40.18	40.17

Table II shows the total power consumption for the three designs tested. When the XOR is maintained as the combinational function, in design 1, an increase in the number of total bits shows the better power consumption rate. However, for the same polynomials and hence the same number of total bits, a change in the combinational function, whereby a mux is used in place of the XOR, sees a relatively large jump in terms of the power consumed. This result was tested for several configurations although not presented here, and the same trend has been observed. This indicates that when aiming to move on to hardware implementation, the combination of a higher total bits along with the use of an XOR as the combinational function gives the best performance overall.

It is to be noted that while the conventional A5/1 shows a slightly lower need of power compared to that of design 2, this design has already been compromised, and is therefore no longer considered relevant. This is the first time that this type of study and observation have been carried out. This finding is interesting and useful, as a higher total bit is expected to also increase the randomness level (and hence the security) of the algorithm [1], [4]. Nevertheless, between XOR and MUX, MUX is proven to produce a much better randomness property of bit stream [7].

V. Conclusion

It can be concluded that the use of multiplexer as a substitute or the XOR function affects the area utilization, efficiency and power in hardware level implementation. Although Design 2 has more area consumption, it has lower power consumption compared to Design 1.

REFERENCES

[1] N. Bajaj, "Effects of parameters of enhanced A5/1," *International Journal of Computer Applications*, vol. 2, no. 2, pp. 7–13, 2011.

[2] A. S. Bhal and Z. Dhillon, "LFSR based stream cipher (enhanced A5/1)," *International Journal of Computer Applications*, vol. 57, no. 19, pp. 32–35, 2014.

[3] M. Madani and S. Chitroub, "Enhancement of A5 / 1 Stream Cipher Overcoming Its Weaknesses," in *Proc. The Tenth International Conference on Wireless and Mobile Communications (ICWMC)*, 2014, pp. 154–159.

[4] N. H. Zakaria, K. Seman, and I. Abdullah, "Modified A5/1 based stream cipher for secured GSM communication," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 11, no. 2, pp. 223–226, 2011.

[5] F. Masoodi, S. Alam, and M. U. Bokhari, "Article: An analysis of linear feedback shift registers in stream ciphers," *International Journal of Computer Applications*, vol. 46, no. 17, pp. 46–49, 2012.

[6] U. Guide, "Xilinx UG029 chipscope pro 11.4 software and cores user guide," vol. 29, 2009.

[7] S. Y. A. M. Fauzi, M. Othman, F. M. M. Shuib, and K. Seman, "Modified A5/1 stream cipher for secured global system for mobile (GSM) communication," in *Proc. the 3rd International Conference on Artificial Intelligence and Computer Science (AICS2015)*, 2015, pp. 12–13.

S. Y. A. M. Fauzi was born in Segamat, Johor on December 15, 2015. She had successfully completed her bachelor degree in Universiti Sains Islam Malaysia in applied physics majoring in microelectronic in 2014, and currently pursuing her master degree in computer science field specifically cryptography.