EFFECT OF THE NUMBER OF TAPPING BITS OF THE A5/1 STREAM CIPHER TOWARDS HARDWARE PERFORMANCE

S.Y.A.M. Fauzi[1,*],M. Othman[2],F.M.M. Shuib[2], K. Seman[2]

[1]*Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai Negeri Sembilan. Malaysia*

[2]*Faculty of Engineering and Built Environment, Universiti Sains Islam Malaysia, 71800 Nilai Negeri Sembilan. Malaysia*

[*]For correspondence; E-mail: sy,akmal91@gmail.com

ABSTRACT: *A5/1 stream cipher is a type of cryptographic algorithm which is widely used for encryption of the GSM communication. While numerous work on the modification of the conventional design of the A5/1 stream have been carried out, to the best of author's knowledge, they are mainly tested in terms of the randomness (and hence security) level, whereas the practicality of the algorithm's design in hardware is typically overlooked. Objective: In this paper, two modified designs proposed by the author are implemented into hardware and the resulting rate of power consumption is compared with that of the conventional design of the A5/1 stream cipher. Results: The results obtained shows that the rate of power consumption of the hardware is inversely proportional to that of the number of tapping bits used in the design. Conclusion: While the tapping bits are known to play a minor role when it comes to generating random binary sequence (and following it, the strength of the security of the design), it actually plays a positive role when it comes to increasing the efficiency of the performance of the hardware.*

Keywords: A5/1 stream cipher, FPGA, hardware performance

1. INTRODUCTION

Field Programmable Gate Array or FPGA is a type of VLSI (Very Large Scale) integrated circuit technology. It is very useful for prototyping due to its programmable feature. This feature helps to eliminate the non-recurring engineering (NRE) cost and reduces time-to-market [1]. Compared side-by-side with ASIC (Application Specific Integrated Circuit), FPGA is the more notable choice for prototyping [1–3], as despite the lower cost of the former, its non-programmable feature of the IC (integrated circuit) makes it less flexible, where the need to remodel the production line will spike up the production cost.

Work on various cryptographic algorithm [4–11] tend to take advantage of the programmable feature of the FPGA to test their design at hardware level implementation.

One of the widely used cryptographic algorithm is the A5/1 stream cipher which acts as the encryption for GSM (Global System for Mobile) communication. Although the design has been weakened since the covert design was leaked, leading to several attacks [12–17], the fact that it was widely deployed meant that the A5/1 is still highly relevant, and is still growing, hence the numerous work still being carried out on the original design to help improve its security strength [18–26]. Nevertheless, none of these modified designs, to the best of author's knowledge, has been realized and tested at the hardware level, which will allow a proper study of the performance versus security trade-off, looking at how the modified characteristics affects the hardware performance compared to that of the conventional design of the A5/1 stream cipher.

In this study, two modified designs are proposed in which the number of tapping bits is changed. This paper is structured as follows: A brief detail on the structural design of the conventional A5/1 stream cipher is explained, which is then followed by the details on the hardware implementation of the cryptographic algorithm. The results obtained on the hardware performance are then discussed, and concluded upon.

2. STRUCTURAL DESIGN OF THE A5/1 STREAM CIPHER

The implementation of the A5/1 stream cipher follows the basic process of a stream cipher that involves an initialization vector (IV) or seed, along with a secret key Ki to generate a sequence of bit streams which is the cipher. The cipher will then be XOR-ed with plaintext to produce the ciphertext. For the A5/1 stream cipher, the secret key produced will eventually XOR-ed with 228-bit frames of GSM conversation which are transmitted every 4.6 milliseconds [27,28].

The conventional design of the A5/1 stream cipher consists of four main characteristics that make up the system, and these are the linear feedback shift register (LFSR), the feedback polynomials, the clocking mechanism, and the combinational function. Figure (1) illustrates the design.

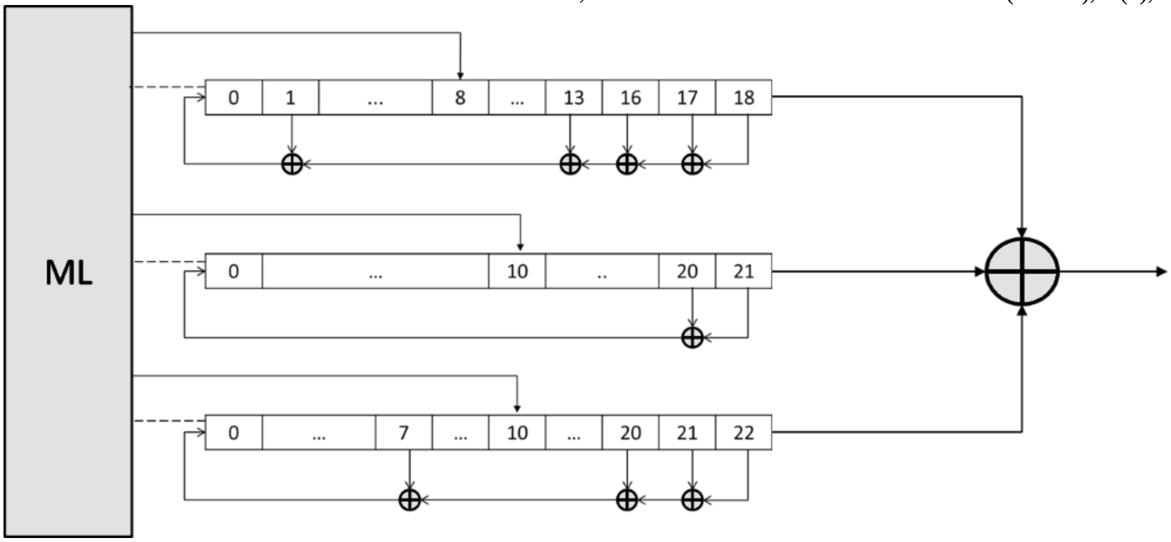
The conventional A5/1 stream cipher design consists of three sets of LFSRs, namely LFSR1, LFSR2 and LFSR3, with bit sizes of 19, 22 and 23 respectively that sums up to 64 bits altogether.

The polynomials, shown in Equations (1)-(3), represent the tapping bits within each of the LFSRs, where for example, the tapping bits in LFSR1, as can be seen in Equation (1) are bit registers 19, 18, 17, and 14.

$$f(x) = x^{19} + x^{18} + x^{17} + x^{14} + 1 \quad (1)$$

$$f(x) = x^{22} + x^{21} + 1 \quad (2)$$

$$f(x) = x^{23} + x^{22} + x^{21} + x^{8} + 1 \quad (3)$$



Fig(1) Design of conventional A5/1 stream cipher

The LFSRs are controlled by a function known as the majority logic (ML) function which controls the shifting of the register. The combinational function used in the conventional A5/1 stream cipher makes use of the XOR, whereby the most significant bit (MSB) from each LFSR will be XOR-ed to produce the secret key.

The secret key is generated through two phases namely as the initialization phase and the secret key generation phase, the details of which are as follows:

Phase I: Initialization Phase

First, all the bit registers of the LFSRs are set to zero. Next, 64-bits key session (KC) is fed into the three LFSRs in parallel, bit by bit. Once finished, the 22-bits frame number (FN) are then fed in the same fashion. During initialization phase, the LFSR is shifted by ignoring the majority logic function and the least significant bit (LSB) is replaced with the tapped bits of the LFSR.

Phase II: Secret Key Generation Phase

LFSRs will then be shifted according to the majority logic rule for 100 cycles. This blank cycle does not generate any output until the 100th cycle is completed. While the LFSRs are shifted, the MSB of each LFSR is XOR-ed to produce the 228-bit secret key.

In a session, the maximum amount of secret key that can be generated is 228 bits per frame which means that if more bits are needed for the secret key, the process will be repeated several times over until the session is ended.

3. PROPOSED A5/1 STREAM CIPHER DESIGNS

As previously mentioned, the feedback polynomials represent the tapping bits which are used to feed the least significant bit (LSB) of the LFSR. In the conventional A5/1 stream cipher design, the number of tapping bits of each of the LFSRs is 4, 2 and 4 for LFSR1, LFSR2 and LFSR3 respectively.

In this paper, two modified design with differing number of tapping bits are proposed. Details of the design are shown in Table (1).

Table (1) Details of the proposed modified designs

	Polynomial	Number of Tapping bits	Clockin g Bit
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:** $f(x) = x^{23} + x^{22} + x^{21} + x^{8} + 1$	4, 2, 4	R[8], R10], R[10]
Design 1	**LFSR 1:** $f(x) = x^{19} + x^{18} + x^{16} + x^{13} + x^{12} + x^{6} + 1$ **LFSR 2:** $f(x) = x^{22} + x^{21} + x^{14} + x^{9} + x^{4} + x^{2} + 1$ **LFSR 3:** $f(x) = x^{23} + x^{17} + x^{13} + x^{12} + x^{11} + x^{5} + 1$	6, 6, 6	R[8], R10], R[10]
Design 2	**LFSR 1:** $f(x) = x^{19} + x^{18} + x^{17} + x^{14} + 1$ **LFSR 2:** $f(x) = x^{22} + x^{12} + x^{7} + x^{3} + 1$ **LFSR 3:** $f(x) = x^{23} + x^{22} + x^{21} + x^{8} + 1$	4, 4, 4	R[8], R10], R[10]

4. HARDWARE IMPLEMENTATION

All the proposed designs including the conventional designs are implemented into hardware by means of FPGA. The implementation helps to analyze the cryptographic algorithm performance on software level.

There are quite a few aspects to be looked upon for hardware implementation performance to gauge the feasibility and the efficiency of the system including throughput, area utilization, power consumption, throughput-to-area ratio, etc. [4], [5], [29]. All these aspects can be a key factor to the feasibility of the implemented cryptographic algorithm.

To the best of author's knowledge, there has been no published works on hardware implementation of modified A5/1 stream cipher based on the designs proposed by previous works. However, there are hardware performance result for conventional design published which shows the throughput, throughput-to-area ratio and the area utilization [5], [29].

In this study, Spartan 3AN Starter Kit board is used. The designs are programmed using the Verilog hardware description language (HDL) and synthesized using Xilinx ISE Simulation software. Upon successful synthesis process, the resistor-transistor-logic (RTL) schematic can be generated as well as the timing simulation.

RTL schematic helps in validating the system design. The example of the RTL design of Design 1 is shown in Figure 2.

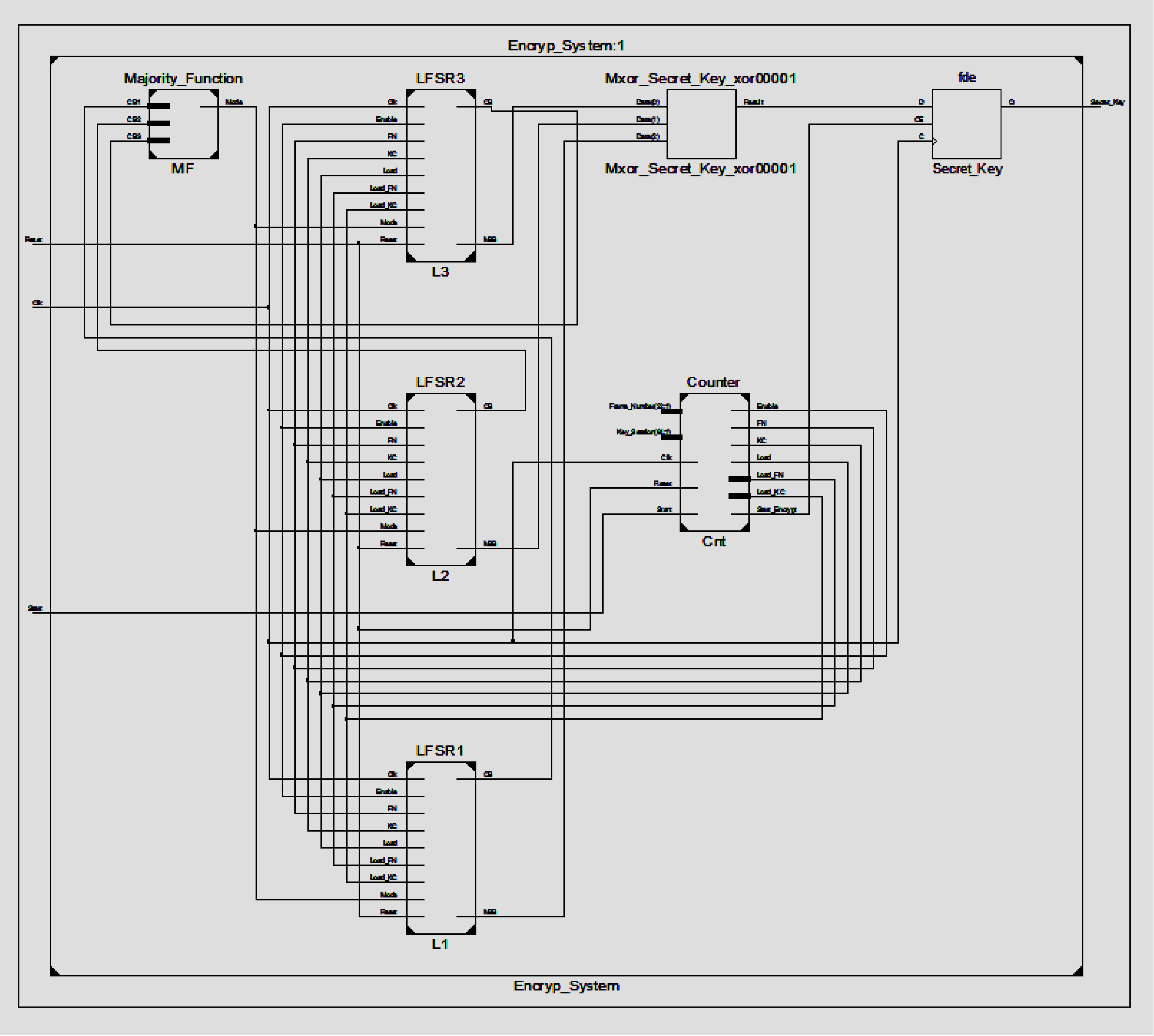


Figure (2) RTL schematic for Design 2

The design in Figure (2) can be compared with Figure (1) and both have three sets of LFSR with majority logic function. the RTL schematic has an addition of Counter submodule which is used to keep track on the number of cycles that has passed.

For the timing simulation, the ISE Simulation (ISim) tool available with the software is used. The timing simulation helps to validate the design by comparing the timing simulation with the design process. Example of the ISim result is shown in Figure 3. The timing simulation shows the two phases that produces the secret key which are the initialization phase and the secret key generation phase.

Once the timing simulation has been successfully run and validated, the hardware performance analysis of the design will be generated and updated in the design summary report.

Ultimately, the power consumption of the hardware is studied, as this parameter directly determines the performance of the algorithm when implemented into hardware.

Before the design can be implemented into hardware, the design coding must be successfully synthesized.

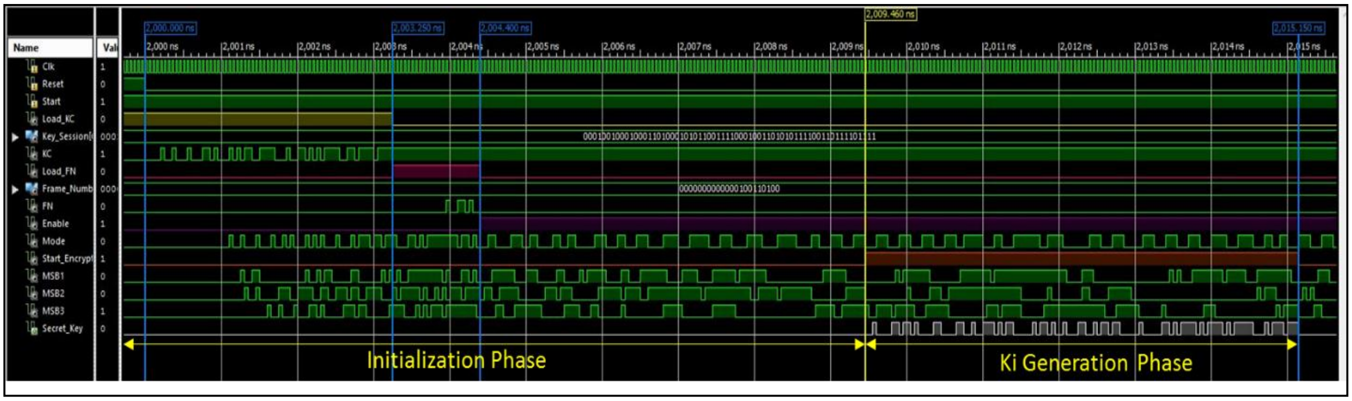


Figure (3) Timing simulation for conventional A5/1 stream cipher

5. RESULTS AND ANALYSIS

Once the design has been implemented, the summary table of device utilization will be updated. The result on power consumption for both conventional and proposed designs are tabulated as shown in Table (2).

Table (2) Result on hardware performance

Design	Conventional	Design 1	Design 2
Power (mW)	39.86	39.35	39.42

Table (2) shows the total power consumption for the three designs tested. All the above makes use of the XOR as the combinational function. The only parameter that has been changed is that of the number of tapping bits. The author has made use of the same LFSR size for all the designs, such that the clocking bits remains the same, allowing for a proper comparison to be made, as only one parameter is being changed at any one time. In design 1, the number of tapping bits has been increased compared to the conventional design, with a uniform number (six here), being used, while in design 2, only LFSR2 sees an increase in terms of the number of tapping bits, from the original two, to four. It is observed that when the value of an individual tapping bit is increased, the amount of power consumed is decreased, but this consumption rate reduces even further when this parameter is increased for the other LFSRs. 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 number of tapping bits along with the use of an XOR as the combinational function gives the best performance overall. This is the first time that this type of study and observation have been carried out. This finding is interesting and useful, because it is known that between both the tapping bits and the combinational function, the former would contribute less in generating random binary sequence (and following it, the strength of the security of the design). However, while in terms of the security level, the tapping bits might not seem to be a major player, it plays a positive role when it comes to increasing the efficiency of the performance of the hardware.

6. CONCLUSIONS

Stream ciphers are known to be very area efficient when it comes to hardware implementation, but their sequential nature gives rise to the probability of the design consuming a lot of power. The results obtained shows that the rate of power consumption of the hardware is inversely proportional to the number of tapping bits used in the design. This finding is hoped to help to act as a guideline for better the achievement of better power efficiency in the design of future algorithms.

7. ACKNOWLEDGEMENT

This research 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.

8. REFERANCE

[1] N. Grover and M. K.Soni, "Reduction of Power Consumption in FPGAs - An Overview," *International Journal of Information Engineering and Electronic Business*, vol. 4, no. 5, pp. 50–69, 2012.

[2] M. G. Arnold, "Verilog Hardware Description," in *Verilog Digital Computer Design: Algorithms Into Hardware*, Prentice Hall PTR, 1999, pp. 64–133.

[3] M. Knezevic, *Efficient Hardware Implementations of Cryptographic Primitives*, no. March. Leuven-Heverlee: Katholieke Universiteit Leuven – Faculty of Engineering, 2011.

[4] L. Batina, S. Kumar, J. Lano, K. Lemke, N. Mentens, C. Paar, B. Preneel, K. Sakiyama, and I. Verbauwhede, "Testing Framework for eSTREAM Profile II Candidates," *Advances*, 2015.

[5] K. Gaj, G. Southern, and R. Bachimanchi, "Comparison of Hardware Performance of Selected Phase II eSTREAM Candidates," 2007.

[6] G. Kostopoulos, N. Sklavos, M. D. Galanis, and O. Koufopavlou, "VLSI Implementation of GSM Security : A5/1 and W7 Ciphers," in *IEEE Workshop on Wireless Circuits and Systems*, 2004, pp. 4–5.

[7] P. Ghosal, M. Biswa, and M. Biswas, "Hardware Implementation of TDES Crypto System with On Chip Verification in FPGA," *Journal of Telecommunications*, vol. 1, no. 1, pp. 113–117, 2010.

[8] F. K. Gürkaynak and P. Luethi, "Recommendations for Hardware Evaluation of Cryptographic Algorithms."

[9] B. Hakhamaneshi, "A Hardaware Implementation of The Advanced Encryption Standard (AES) Algorithm Using System Verilog," Islamic Azad University, Iran, 2009.

[10] P. Kitsos and O. Koufopavlou, "An FPGA-Based Implementation of the Pomaranch Stream Cipher," *Proceedings of the 3rd International ICST Conference on Mobile Multimedia Communications*, 2007.

[11] F. Islam and M. A. M. Ali, "FPGA Implementation of An LFSR Based Pseudorandom Pattern Generator for MEMS Testing," *International Journal of Computer Applications*, vol. 75, no. 11, pp. 30–34, 2013.

[12] A. AlHamdan, B. Harry, E. Dawson, L. Simpson, and K. K.-H. Wong, "Weak key-IV Pairs in the A5/1 Stream Cipher," in *Twelfth Australasian Information Security Conference (AISC 2014)*, 2014, vol. 149, pp. 23–36.

[13] E. Barkan, E. Biham, and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," *Journal of Cryptology*, vol. 21, pp. 392–429, 2008.

[14] T. Gendrullis, M. Novotný, and A. Rupp, "A Real-World Attack Breaking A5/1 Within Hours," *Cryptographic Hardware and Embedded Systems – CHES 2008*, vol. 5154, pp. 266–282, 2008.

[15] S. Meyer, "Breaking GSM With Rainbow Tables," no. Cryptography and Security (cs.CR), 2010.

[16] A. Mahalanobis and J. Shah, "An Improved Guess-and-Determine Attack on the A5/1 Stream Cipher," *Computer and Information Science*, vol. 7, no. 1, pp. 115–124, 2014.

[17] H. Wu, *Cryptanalysis and Design of Stream Ciphers*, no. July. 2008.

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

[19] R. Kaur and N. Bajaj, "Enhancement in Feedback Polynomials of LFSR used in A5/1 Stream Cipher," *International Journal of Computer Applications*, vol. 57, no. 19, pp. 32–35, 2012.

[20] 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.

[21] 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.

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

[23] S. B. Sadkhan and N. H. Jawad, "Improvement of A5/1 Encryption Algorithm Based on Using Unit Delay," *Iraqi Academic Scientific Journal*, vol. 22, no. 2, pp. 622–633, 2014.

[24] S. B. Sadkhan and N. H. Jawad, "Simulink Based Implementation of Developed A5/1 Stream Cipher Cryptosystems," *Procedia Computer Science*, vol. 65, pp. 350–357, 2015.

[25] D. Upadhyay, P. Sharma, and S. Valiveti, "Randomness Analysis of A5/1 Stream Cipher for Secure Mobile Communication," *International Journal on Soft Computing (IJSC)*, vol. 5, no. March-September, pp. 95–100, 2014.

[26] N. H. L. @ A. Zawawi, K. Seman, and N. J. M. Zaizi, "A New Proposed Design of a Stream Cipher Algorithm : Modified Grain - 128," vol. 3, no. 5, pp. 902–908, 2014.

[27] M. D. Galanis, P. Kitsos, G. Kostopoulos, N. Sklavos, O. Koufopavlou, and C. E. Goutis, "Comparison of the Hardware Architectures and FPGA Implementations of Stream Ciphers," *Proceedings of the 2004 11th IEEE International Conference on Electronics, Circuits and Systems, 2004. ICECS 2004.*, pp. 2–5, 2004.

[28] L. Chen and G. Gong, "Appendix B . Design of Stream Ciphers," *Communication Systems Security*, pp. 1–17, 2008.

[29] M. Galanis, P. Kitsos, G. Kostopoulus, N. Sklavos, and C. Goutis, "Comparison of The Hardware Implementation of Stream Cipher," *The International Arab Journal of Information Technology*, vol. 2, no. 4, pp. 267–274, 2005.