International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-4, Issue-6)

Research Article

June 2015

Design and Development of Low Hardware Complexity Stream Cipher on FPGA

[1]Ambili.K, [2]K. S. Lal Mohan, [3]Pradeesh K.P
[1, 3] Department of ECE, KVG College of Engineering, Sullia, India
[2]National Institute of Electronics and Information Theory Calicut, Kerala, India

Abstract—

Stream ciphers based on Quasi Cyclic Low Density Parity Check (QC- LDPC) code is a good option to reduce hardware complexity of the cryptosystem. For encryption of data stream ciphers are preferred to block ciphers because it consumes less power and hardware. As in classical coding theory Quasi Cyclic Low Density Parity Check (LDPC) codes good error correction performance with low decoding complexity. This project proposes to design and implement a hardware efficient stream cipher using QC-LDPC codes. The performance of the resulting system will be compared to the previous stream cipher design using CRC hash.

Keywords— stream cipher; qcldpc; hardware efficiency; periodicity; security

I. INTRODUCTION

Hardware complexity and power consumption are important design criteria for hand held devices, sensor network, smart cards, etc. encryption systems can be built using either block cipher or stream cipher. Stream ciphers include time varying transformation on individual data bits, whereas block cipher are obtained by applying same transformation on a group of data bits. Since the security of the block cipher algorithm directly depends upon the complexity of the algorithm, a good amount of security demands a very complex structure for the encryption system. So when circuit complexity is not a matter of concern, block cipher can be designed to have better security per key bit than stream cipher. Since in stream ciphers security is not directly depended on the circuit complexity, for ciphers of low hardware complexity stream cipher are preferred. Also since the encryption operation is synchronous stream cipher is just an XOR operation, it allows real-time operation of data, which is essential in multimedia communication. Furthermore stream ciphers have different implementation properties that restrict the cryptanalyst from performing side channel analysis.

Linear Feedback Shift Register (LFSR) based stream cipher are the most commonly used stream cipher due to the low hardware complexity and less power consumption. But the main drawback of that is susceptibility to attack due to linearity in the structure. So for better security one-way function based stream cipher are preferred over LFSR stream cipher. Hash function can be used as a part of keystream generators in synchronous stream cipher due to the high security provided by the one wayness of hash functions. Mainly two hash functions were used for stream cipher design, LFSR based Toiplitz hash and CRC hash.

In this work the author suggest some changes in the design of recently proposed stream cipher so that the system becomes cryptographically strong. In this work the CRC hash is completely replaced with QC-LDPC Codes, which ensures low hardware complexity, less power consumption and high security.

II. MATHEMATICAL BAGROUND

A) Introduction to QC-LDPC Codes

A circulant is a square matrix in which each row is the cyclic shift (one place to the right) of the row above it, and the first row is the cyclic shift of the last row.

A QC-LDPC code is given by the null space of an array of sparse circulants of the same size. For two positive integers c and t with $c \leq t$, consider the following c×t array of b×b circulants over GF(2):

$$Hqc = \begin{pmatrix} A_{1,1} & A_{1,2} & \cdots & A_{1,t} \\ A_{2,1} & A_{2,2} & \cdots & A_{2,t} \\ \vdots & \vdots & \ddots & \vdots \\ A_{c,1} & A_{c,2} & \cdots & A_{c,t} \end{pmatrix}$$

which has the following structural properties: 1) the weight of each circulant Aij is small compared with its size b ; and 2)no two rows (or two columns) of Hqc have more than one 1-component in common, called the row-column (RC) constraint.

Let g_{ij} be the generator of G_{ij}. Once we know, g_{ij} 's we can form all the circulants G_{ij}'s of Gqc . The generator matrix Gqc is said to be in SC form. The SC form allows us to encode a QC-LDPC code with simple shift registers. An encoding circuit for Cqc can be devised based on the generators of the circulants in the P matrix of Gqc . Let a=(a_1,a_2,a_3.... $a_{(t-c)b}$) be the information sequence of (t − c)b bits to be encoded , then the code word for the information sequence a is V=(a,p_1,p_2,... p_c)where for $1 \leq j \leq c$, P_j=($p_{j,1}$,$p_{j,2}$... $p_{j,b}$) is a section of p_j parity-check bits. P_j can be formed with a shift-register-adder-accumulator (SRAA) circuit as shown in Figure 1. To form c parity sections, we need c SRAA circuits, one for computing each parity section. A block diagram for the entire encoder is shown in Figure 2.

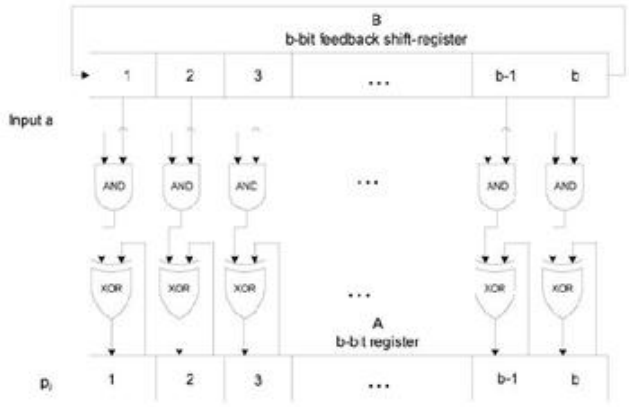

Fig 1. SRAA Encoder

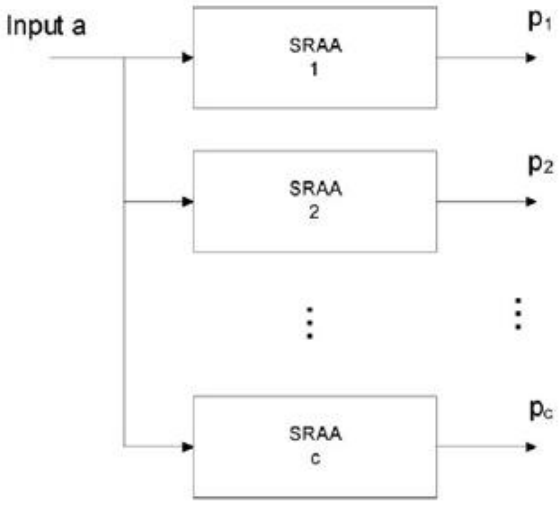

Fig 2. QC-LDPC Encoder

All the c parity sections are formed at the same time in parallel, and they are then shifted into the channel serially. So in this scheme we need parallel to serial circuit.

III. STREAMCIPHER DESIGN BASED ON QC-LDPC CODES

Based on the discussions in section II the structure of the Keystream generator of the proposed stream cipher is shown in figure3.initially the key bits are concatenated with the initial state of $LFSR_s$ and are fed to the first input to the QC-LDPC block. Then this output will be fed back to the QC-LDPC with the next state of LFSRs, which increases the periodicity of the system

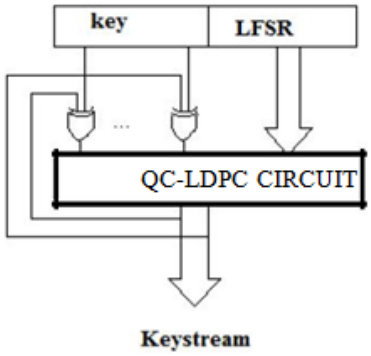

Figure3- proposed Keystream generator using QC-LDPC codes

IV. CONCLUSION

In this paper we propose design of a secure stream cipher of low hardware complexity. The proposed method is introduced as a modification in the design of a recently proposed hardware efficient stream cipher [3]. By introducing qc-ldpc encoder block in place of CRC. In the final proposed design, the security and periodicity is increased by a large margin, with less hardware complexity. Since QC-LDPC block can be implemented in hardware using only flip-flop and logical gates, the hardware complexity is reduced to a great extent. The security of the cipher is increased by combining the input bits through non-linear Boolean function before feeding into modular division circuit. Thus it becomes impossible to retrieve the keys through solution of linear equations. The periodicity of the generated keystream is improved by varying the feedback polynomial of the modular division circuit. The suggested minimum hardware for this purpose is seen to provide large periodicity and throughput with good security.

REFERENCES

[1] Deepthi.P.P, Sathidevi.P.S. Design, implementation and analysis of hardware efficient stream cipher using LFSR based hash functions. Elsevier Computers and security. 28, 229-241(2009).

[2] Panagiotis Rizomiliotis: Misusing universal hash functions: security analysis of a hardware efficient stream

cipher model using LFSR based hash function, Information Theory Workshop(ITW), 2010 IEEE
[3] Nasarathul Nisha.P.K, Deepthi.P.P, Lalmohan.K.S:" Design and Analysis of Stream Cipher of Low Hardware Complexity", 2012 International Conference on Communication Systems and Network Technologies
[4] Angelo P. E. Rosiello, "Design of a Synchronous Stream Cipher from Hash Functions", International Journal of Computer Science and Network Security, Vol.7 No.8, August 2007.
[5] Yong Zhang, Xiamu niu, Juncao Li, Chunming Li, "Research on a Novel Hashing Stream Cipher", International Conference on Computational Intelligence and Security, 3-6 Nov 2006, Guangzho.

