ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

Hardware Implementation of ZUC Stream Cipher

Somnath S.Berad

ME Electronics Engineering, Amrutvahini College of Engineering Sangamner (MS), India

Abstract—This research aims to generate key for network security to long term evolution network/radio network. In this project a hardware implementation of ZUC Stream cipher is designed. ZUC is a stream cipher that forms the heart to the 3GPP confidentiality algorithm 128-EEA3 and the 3GPP integrity algorithm 128-EIA3, offer in reliable security services in Long Term Evolution networks (LTE). A detailed hardware implementation is shown in order to reach satisfactory performance results in LTE systems. The design was coded using VHDL language and for the hardware implementation, a XILINX Spartan-3FPGA was used. Experimental results in terms of performance and hardware resources are shown.

Keywords— Long Term Evolution networks security, Zuc stream cipher, Hardware implementation, FPGA**.**

.

I. INTRODUCTION

Protection and hiding of valuable information has a very old history [1] where cryptology has developed over the centuries from an art, in which only few were ingenious into a science with well established foundations. There are several goals which security professionals desire to achieve through the use of cryptography. These goals include condentiality, data integrity, entity authentication, non-repudiation and data origin authentication [2]. Cryptology encompasses two related fields: cryptography and cryptanalysis. Cryptography can be denied as the study of mathematical techniques to ensure various aspects of information security as those mentioned. On the other hand, cryptanalysis can be defined as the study of techniques to analyze, and break, information security services by targeting, specially, the underlying cryptographic algorithms. Now days there are many stream cipher algorithms proposed in academia and industry. Stream cipher is an important class of symmetric encryption algorithms [3], whats more stream ciphers do not suffer from the error propagation, because each bit is independently encrypted/decrypted from any other. Compared with block cipher, they are generally much faster than block cipher and they have greater software effciency, due to these features stream ciphers have been the choice for several communication protocols, especially wireless ones [4]. Block ciphers are memoryless algorithms that permute N-bit blocks of plain text data under the influence of the secret key and generate N-bit blocks of encrypted data, compared with the block cipher, stream ciphers contain internal states and typically operate serially by generating a stream of pseudo random key bits, the key stream (stream ciphers are also called key stream generators). The key stream is then bit-1wise XORed with the data to encrypt/decrypt .Cipher systems are usually subdivided into block ciphers and stream ciphers. Block ciphers tend to simultaneously encrypt groups of characters, whereas stream ciphers operate on individual characters of a plain text message one at a time [11]. The new stream cipher ZUC is a word-oriented stream cipher [7]. It takes a 128-bit initial key and a 128-bit initial vector as input, and outputs a key stream of 32-bit words.

This key stream can be used to encrypt the plaintext. The execution of ZUC has two stages: key initialization stage and working stage. In the frst stage, a key initialization is performed, i.e. the cipher is clocked without producing output.

The second stage is working stage. In this study, the new architecture is proposed to generate 32-bit key per clock cycle. ZUC has three logical layers. The top layer is a linear feedback shift register (LFSR) of 16 stages, the middle layer is bit-reorganization, and the bottom layer is a nonlinear function F. Long Term Evolution (LTE) is the next-generation network beyond 3G that enable fixed to mobile migrations of Internet applications such as Voice over IP (VoIP), video streaming, music downloading, mobile TV and many others. LTE networks will also provide the capacity to support an explosion in demand for connectivity from a new generation of consumer devices tailored to those new mobile applications. The current radio interface protection algorithms for LTE,128-EEA1 for

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

confidentiality and 128-EIA1 for integrity have been designed by SAGE/ETSI Security Algorithms Group of Experts[4] . 128-EEA1 and 128-EIA1 are based on SNOW3G stream cipher. Also, the 3rd Generation Partnership Project (3GPP), together with the GSM Association specifies a second set of algorithms, 128-EEA2 and 128-EIA2 [3], which are based on AES block cipher [4].

Finally, 3GPP with GSM association specifies a third set of algorithms for confidentiality and integrity the 128-EEA3 and 128-EIA3 respectively. Both ciphers are based on ZUC stream cipher. The most serious reason for these new ciphers is that LTE will be used in many countries worldwide. But Chinese regulation will not allow those algorithms to be used in China, because they were not designed in China. However, ZUC has been designed in China, and thus that it can be used in China. In this paper an efficient FPGA implementation of ZUC stream cipher is presented. Minimize the registers and Look-Up Tables in the design. Our FPGA hardware implementation covers 385 slices and achieves 2.08 Gbps throughput in maximum frequency operation. Comparisons with other stream ciphers implementations are provided. The comparisons prove that the proposed system is efficient in terms of throughput. The aim of the work is to ascertain that the ZUC stream cipher can operate on a recent hardware device for efficient use on LTE networks. Compared with block ciphers, stream ciphers are more efficient when implemented in hardware environment, like Field Programmable Gate Array (FPGA). In this paper, we propose three optimized schemes in the FPGA implementation of a novel and recently proposed stream cipher, ZUC, which is a new cryptographic algorithm proposed for inclusion in the 4G mobile standard called LTE (Long Term Evolution).

Aim

Aim and contribution of this project are summarized as following.

1. The aim of Project is to gives the network security to long term evolution network/radio network.
2. The aim of the work is to ascertain that the ZUC stream cipher can operate on a recent hardware device for efficient use on LTE network.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

II . SYSTEM DESIGN

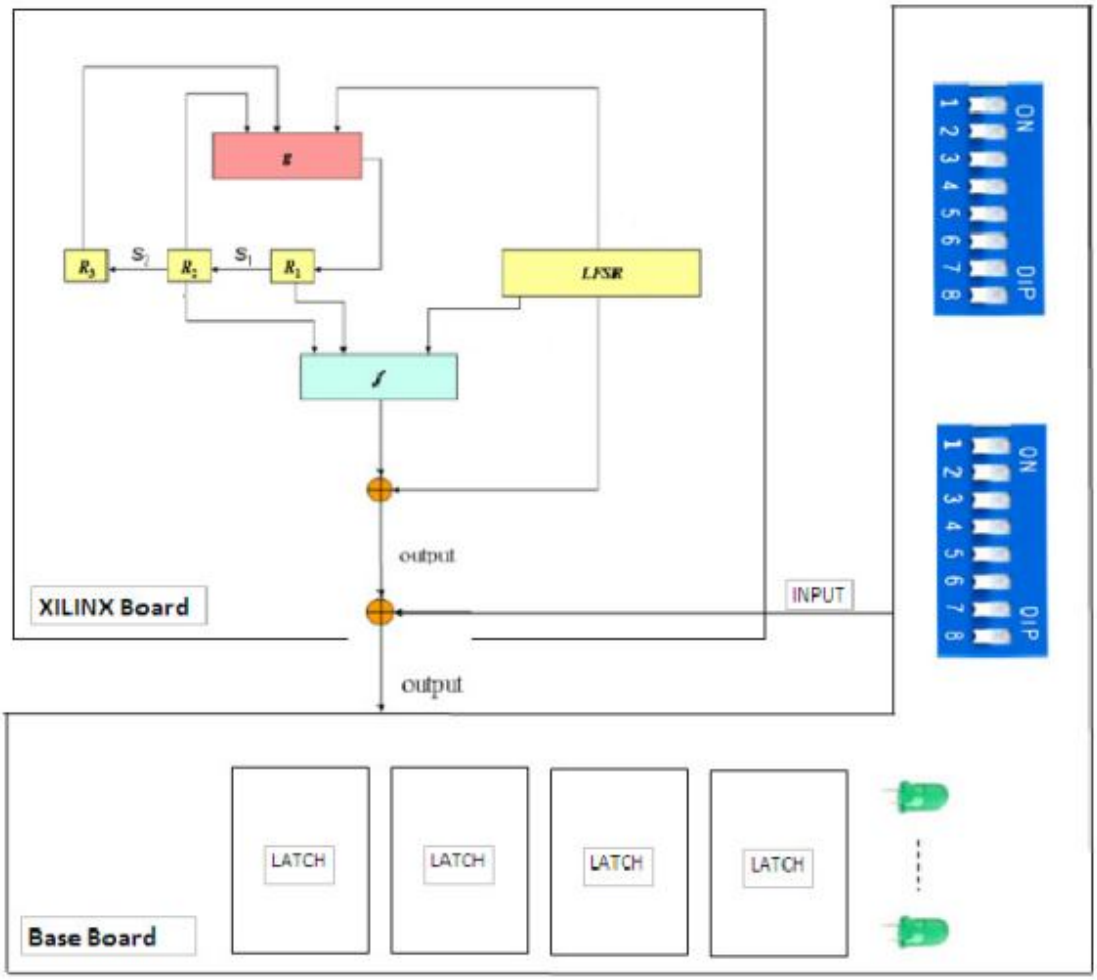

Fig. Block Diagram of System

ZUC is a word-oriented stream cipher [8] that takes a 128-bit Key and a 128-bit Initial Vector (IV) as input, and outputs a key stream of 32-bit words. ZUC has three logical layers. The top layer is a Linear Feedback Shift Register (LFSR) of 16 stages, the middle layer is for bit reorganization (BR), and the bottom layer is a nonlinear function F. The LFSR has 16 of 31-bit cells (s_0 , s_1 , , s_{15}). This LFSR has two stages operations: the initialization stage and the working stage. In the initialization, the LFSR receives a 31-bit input word u, which is obtained by removing the rightmost bit from the 32-bit output W of the nonlinear function F The bit-reorganization [9] layer extracts 128-bit 16 from the cells of the LFSR and forms 4 of 32-bit words, where the first three will be used by the nonlinear function F in the bottom layer, and the last word will be involved in producing the key stream [15]. For the cipher operation firstly the key loading procedure expands the initial key and the initial vector into 16 of 31-bit integers as the initial state of the LFSR and then two stages are executed; initialization stage and working stage. In the first stage, a Key/IV initialization is performed and the cipher is clocked without producing output. The second stage is a working stage in which every clock cycle produces a 32- bit word of output.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

III. ARCHITECTURE OF ZUC STREM CIPHER

The aim of the work is to ascertain that the ZUC stream [10] cipher can operate on a recent hardware device for efficient use on LTE networks. The proposed hardware implementation of the ZUC stream cipher is illustrated in Fig. The proposed system has as main I/O interfaces a 32-bit plaintext/ciphertext input and a 32-bit ciphertext/plaintext output. In addition it has two inputs, a 128-bit secret key, Key, and 128-bit initialization value, IV. Our system supports, the initialization stage, the working stage and the key stream producing stage.
The configuration of the proposed hardware system supports all stages of operation. The main parts of the proposed architecture of ZUC are the Key Loading, the Linear Feedback Shift Register (LFSR)[11].the BR (bit-reorganization) and the configuration according the cipher operation scenario (initialization or working stage). Also, one more adder mod (2^{31} -1) is needed with its result used as first input of the multiplexer. In the Feedback Logic six additions mod (2^{31} -1) are used.

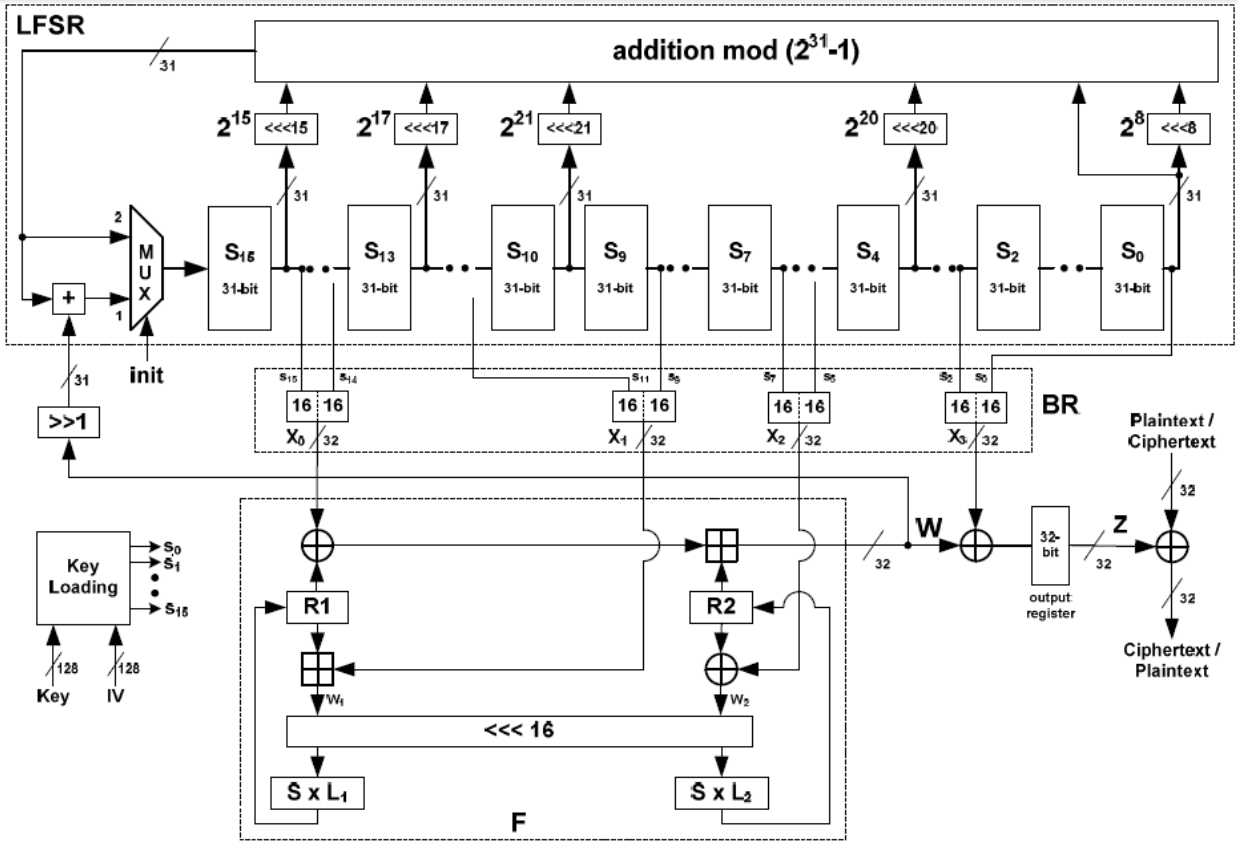

Fig. Proposed architecture of the ZUC stream cipher

IV. SOFTWARE DESIGN

1. The linear feedback shift register (LFSR)

The LFSR has 16 of 31-bit cells (s_0, s_1, …, s_{15}). This LFSR has two stages of operations: the initialization stage and the working stage. In the initialization, the LFSR [12] receives a 31-bit input word u, which is obtained by removing the

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

rightmost bit from the 32-bit output W of the nonlinear function F, (u=W>>1). More specifically, the initialization mode works as follows.

Algorithm 1: LFSRWithInitialisationMode

Input: u

begin
- $v = \{2^{15}S_{15} + 2^{17}S_{13} + 2^{21}S_{10} + 2^{20}S_4 + (1+2^8)S_0\} mod(2^{31}-1)$;
- $S_{16} = v + u \pmod{2^{31}-1}$;
- **if** $S_{16} = 0$ **then**
  - then set $S_{16} = 2^{31} - 1$
- $(S_1, S_2, \ldots, S_{15}, S_{16}) \rightarrow (S_0, S_1, \ldots, S_{14}, S_{15})$;

In the working mode, the LFSR does not receive any input, and it works as Algorithm 2 shown. As Algorithm 2 shown, the LFSR works independently with other part of ZUC. If we can get new S_{16} per clock, the shift registers can shift per clock cycle.

Algorithm 2: LFSRWithWorkMode

begin
- $S_{16} = \{2^{15}S_{15} + 2^{17}S_{13} + 2^{21}S_{10} + 2^{20}S_4 + (1+2^8)S_0\} mod(2^{31}-1)$;
- **if** $S_{16} = 0$ **then**
  - then set $S_{16} = 2^{31} - 1$
- $(S_1, S_2, \ldots, S_{15}, S_{16}) \rightarrow (S_0, S_1, \ldots, S_{14}, S_{15})$;

2. The Bit-reorganization

The middle layer of the algorithm is the Bit-reorganization [13]. It extracts 128 bits from the state of the LFSR and forms 4 of 32-bits words which will be used by the nonlinear function F in the bottom layer. Let S_0; S_2; S_5; S_7; S_9; S_{11}; S_{14}; S_{15} be 8 registers of LFSR. Then the Bit-reorganization forms 4 of 32-bit words X_0;X_1;X_2;X_3 from the above registers as Algorithm 3. Compared with software implementation, the concatenation of signal in hardware is only needed to change the signals order, and it nearly doesn't need extra time to do this work. Therefore the bit reorganization stage can mix with the nonlinear function operation together to save clock cycle.

Algorithm 3: Bitreorganization

begin
- $X_0 = S_{15H} \parallel S_{14L}$;
- $X_1 = S_{11L} \parallel S_{9H}$;
- $X_2 = S_{7L} \parallel S_{5H}$;
- $X_3 = S_{2L} \parallel S_{0H}$;

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

In Algorithm 3, $S15H$ denotes the leftmost 16 bits of integer $S15$, $S14L$ denotes the rightmost 16 bits of integer S_{14}, $S15H \parallel S14L$, denotes the concatenation of strings $S15H$ and $S14L$.

3. The nonlinear function F

The nonlinear function F[14] has 2 of 32-bit memory cells $R1$ and $R2$. The input of the nonlinear function is the $X0;X1;X2$, which are the output of the bit reorganization step, the nonlinear function F outputs a 32-bit word W. The detailed process of F, as shown in Algorithm 4.

Algorithm 4: The nonlinear function

Input: X_0, X_1, X_2

1 **begin**

2 $W = (X_0 \oplus R_1) \boxplus R_2;$

3 $W_1 = R_1 \boxplus R_2;$

4 $R_1 = S(L_1(W_{1L} \parallel W_{2H}));$

5 $R_2 = S(L_2(W_{2L} \parallel W_{1H}));$

V. RESULT

ZUC stream cipher consist of three logical layer, Top layer consist of linear feedback shift register (LFSR), middle layer consist of Bit Reorganisation Unit (BR), Bottom Layer consist Non linear Function (F) forms a 32 bits key and that key encrypted by 32 bits plaintext to produce 32 bits ciphertext.

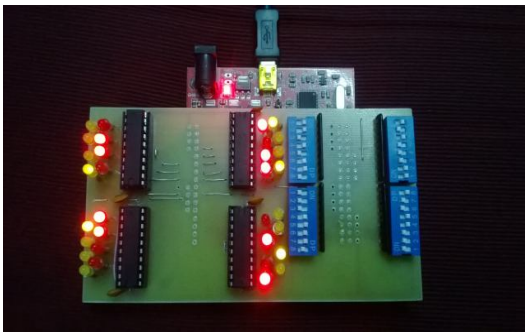

Fig. Practical Results

VI. CONCLUSIONS

1. A ZUC high-speed hardware architecture is described, which has been implemented by means of an FPGA device. Experimental results prove that the ZUC implementation is a flexible solution for LTE applications.
2. The implementation on FPGA achieves a throughput of 2.08 Gbps at a 65 MHz clock frequency.

ACKNOWLEDGEMENTS

I thank god almighty for guiding me through the project. I would like to thank all those who have contributed to the completion of the project report and helped me with valuable suggestion for improvement.

REFERENCES

1. D. Kahn, The Codebreakers: The Story of Secret Writing", Macmillan Pub Co; Reissue edition, 1974.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

2. A.J. Menezes, P.C. Van Oorschot, and S.A. Vanstone,"Handbook of Applied Cryptography", CRC Press, 5th edition, 2001.
3. P. Leglise, F. Standaert, G. Rouvroy, and J. Quisquater, "Ecient implementation of recent stream ciphers on recongurable hardware devices, in 26th Symposium on Information Theory in the Benelux, pp. 261268, 2005.
4. M. Galanis, P. Kitsos, G. Kostopoulos, N. Sklavos, O. Koufopavlou, and C. Goutis, "Comparison of the hardware architectures and FPGA implementations of stream ciphers," in Electronics, Circuits and Systems, 2004. ICECS 2004. Proceedings of the 2004 11th IEEE International Conference on, pp. 571574, IEEE, 2005.
5. 3GPP System Architecture Evolution (SAE): Security Architecture, 3GPP Std. TS 33.401, Rev. 8.2.1, Dec. 2008.
6. Specification for the Advanced Encryption Standard (AES), Federal Information Pro-cessing Standards (FIPS) Publication 197, US Natl Inst. Standards and Technology,2001.
7. Data Encryption Standard, Federal Information Processing Standard (FIPS) 46,National Bureau of Standards, 1977.
8. 3rd Generation Partnership Project. Long Term Evaluation Release 10 and beyond (LTE-Advanced). Proposed to ITU a GPP TSG RAN Meeting, Spain, 2009.
9. D. Wheeler and R. Needham, TEA, a Tiny Encryption Algorithm, In proc. of Fast Software Encryption (FSE) 1994, LNCS 1008, pp. 363-366, Springer-Verlag, 1994.
10. NESSIE, the New European Schemes for Signatures, Integrity and Encryption. Available at https://www.cosic.esat.kuleuven.be/nessie/.
11. ECRYPT, the European Network of Excellence for Cryptology. Available at http://www.ecrypt.eu.org/ecrypt1/
12. eSTREAM, the ECRYPT Stream Cipher Project. Available.
13. H. Wu, The Stream Cipher HC-128, The eSTREAM Finalists, LNCS 4986, pp. 39-47, Springer-Verlag,2008.Also available at http://www.ecrypt.eu.org/stream/hcpf.html
14. D.J. Bernstein, The Salsa20 Family of Stream Ciphers, The eSTREAM Finalists, LNCS 4986, pp.84-97, Springer-Verlag, 2008.Also available at http://www.ecrypt.eu.org/stream/salsa20pf.html.
15. M. Hell, T. Johansson, A. Maximov, and W. Meier, The Grain Family of Stream Ciphers, The eSTREAM Finalists, LNCS 4986, pp. 179-190, Springer-Verlag, 2008, Also available at http://www.ecrypt.eu.org/stream/grain html.