ISSN 2395-1621

Reconfigurable Architecture for SNOW 3G Stream Cipher

[#1]Apeksha Kailas Mule, [#2]Mrunal Deepak Pawar, [#3]Ashwini Kareppa Yaragudri

[1]muleapeksha2014@gmail.com
[2]pawarmrunal3@gmail.com
[3]ashwiniy106@gmail.com

[#123]Department of Electronics and Telecommunication

JSPM's BSIOTR, Pune, India.

ABSTRACT

SNOW 3G is a stream cipher algorithm that had been conceived and chosen in 2006 as the heart of the second set of UMTS confidentiality and integrity algorithms. This stream cipher is a two components with an internal state of 608 bits initialized by a 128-bit key and a 128-bit initialization vector IV. We are interested in SNOW 3G algorithm structure, its components and then its two different operation modes. We will focus on its efficiency by studying its time and space complexity. The SNOW 3G will be implemented by the FPGA using the verilog HDL software platform. We propose the merger of SNOW 3G stream ciphers, which constitute a part of the 3GPP LTE-Advanced security suite. We propose a high performance integrated design that generates ciphers in hardware, based on their structure. The integrated architecture reduces the area overhead significantly compared to distinct cores, and also provides almost higher throughput in terms of key stream generation. The SNOW 3G address issues of higher security and platform-specific implementation.

Keywords: SNOW 3G, stream cipher, LFSR, Encryption, Time complexity, Space complexity, LTE, 3GPP.

ARTICLE INFO

Article History

Received: 20th April 2017

Received in revised form :

20th April 2017

Accepted: 24th April 2017

Published online :

24th April 2017

I. INTRODUCTION

The current radio interface protection algorithms for Universal Mobile Telecommunication System (UMTS), UEA1 for confidentiality, and UIA1 for integrity of signaling messages were designed by SAGE/ETSI Security Algorithms Group of Experts. No weakness has been discovered in these algorithms, and there is no indication that a weakness is likely to be found. However, if one ever were found, it would be much better to have a replacement. So the 3rd Generation Partnership Project (3GPP), together with the GSM Association, called SAGE wishes to specify a second set of algorithms, UEA2 and UIA2. Apart from the obvious requirements on speed and implementation complexity, the main design criterion for these new algorithms was that they should be fundamentally different in nature from UEA1 and UIA1, for cryptanalytic reasons. SAGE delivered the UEA2 and UIA2 specifications in January 2006. At the heart of these algorithms is the SNOW 3G stream cipher. The two basic issues in mobile communications security are Data Confidentiality and Data Integrity. The term of Data Confidentiality is referred to keeping information secret from all but those who are authorized to see it while the term of Data Integrity is referred to ensuring information has not been altered by unauthorized or unknown means. Additionally, in mobile systems the constrains in power consumption and chip covered area are very strict while the performance requirements are essential. Therefore, the existence of supplementary hardware is essential, if the designer's goal is to construct efficient systems in limited area resources, like in mobile systems. In this paper an efficient implementation of the SNOW 3G cipher is presented. The proposed hardware system has been implemented using only the main functionality of the algorithm. It uses the feedback logic in order to support the basic operation scenarios. Also, we improve and accelerate the complex internal operations of the system in order to have a performance efficient system and compatible with the current wireless-cellular communication standards. Our ASIC hardware implementation covers 25016 nand (2:1) equivalent gates and it achieves 7.97 Gbps throughput in maximum frequency operation. Comparisons with other stream ciphers implementations are provided. The comparisons prove that the proposed system outperforms in terms of throughput efficiency. Stream ciphers hold a major share in the world of

© 2017, IERJ All Rights Reserved

symmetric key cryptography, primarily due to their blazing speed of operation and simplicity of design suitable for implementation in both software and hardware. During the last decade, an array of stream ciphers has been developed to cater to the needs of modern day digital communication, both in public and private sectors. After implementing the LTE cryptographic algorithms in FPGA (Field Programmable Gate Array) hardware platform which is more suitable for 4G era to ensure security of wireless communication, SNOW 3G performs higher throughput than ZUC.

II. SNOW 3G ARCHITECTURE

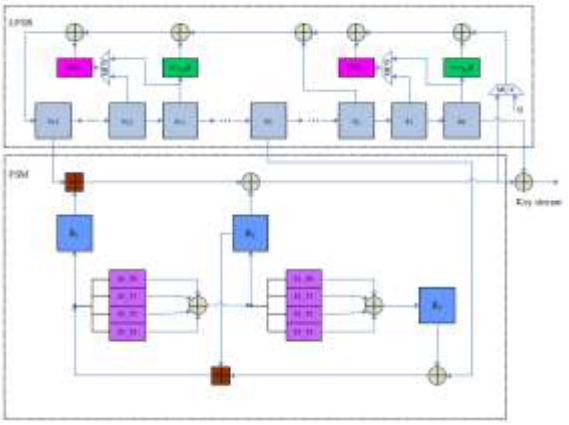

Fig No1: Block Diagram

The structure of ZUC, is similar to that of SNOW 3G. SNOW 3G is composed of two parts, the **LFSR** (Linear Feedback Shift Registers) and the **FSM** (Finite State Machine).

Linear Feedback Shift Registers (LFSR):

In SNOW 3G, the LFSR consists of 16 registers, s0, s1, ・ ・ , s15, and each of them holds 32 bits. In each cycle, a new state *v* of *s*15 is computed, while the new state of registers remains the old state of si+1, i ∈ {0, 1, ・ ・ ・ , 14}. The clocking of the LFSR has two modes of operations, the Initialization Mode and the Key stream Mode. The difference between them is the way the new state *v* is calculated. In the Initialization Mode, the output of the FSM, which is denoted by *F*, is used to calculate *v* while it is not in the Key stream Mode. The main operations of the computation of *v* are XORs. The proposed system has as main I/O interfaces a 32-bit plaintext/cipher text input and a 32-bit cipher text/plaintext output. In addition it has two input parameters values, a secret key and initialization value IV. The IV value is considered as a four word value IV = (IV3, IV2, IV1, IV0), where IV0 is the least significant one. The secret key K also, is considered as a four word value K = (K3, K2, K1, K0), where K0 is the least significant one. Our proposed hardware system supports both key-initialization and key generation processes. The main parts of the proposed architecture of SNOW 3G are the Initial Operations, the Linear Feedback Shift Register (LFSR), the Finite State Machine (FSM) and the Feedback Logic Unit. The LSFR consists of sixteen register stages named s0, s1, s2…, s15 each holding 32 bits. In the initialization mode the LFSR receives a 32-bit input word F.

FSM (Finite State Machine)

The Finite State Machine (FSM) constitute the nonlinear combiner of SNOW3G.It has three 32-bit registers R1, R2,R3.During its operation, the FSM involves two input data from the LFSR, s5 ands15 stages contents . The introduction of two inputs to the FSM part makes a guess and-determine attack more difficult. The FSM uses two S-boxes S1 and S2 to update the registers R2 and R3 and that provides stronger diffusion since each output bit depends on each input bit thanks to the use of the S-Box component. The combining functions used are the bitwise exclusive-OR operation and the addition modulo 232.

S-Box S2 32x32-bit:

In order to increase the resistance against algebraic attacks, the third memory element which is the 32-bit register R3 and the second ensemble of S-boxes S2were introduced in the FSM-component of SNOW 3G.The new S-box S2 consists of four new 8-bit to 8-bit substitutions followed by the mix Column operation of Rijndael . The S-Box S2 maps a 32-bit input to a 32-bit output.

Key Initialization mode

First the key initialization mode occurs, which is presented in Fig 3.2. During key initialization process the LFSR and the internal FSM registers fetch their initial values. Firstly, the Key and the IV vectors are been transformed. The initial values are stored at LFSR stages through OR gates. Additionally, the R1, R2 and R3 FSM registers are set to zero. SNOW 3G is initialized with a 128-bit key consisting of four 32-bit words k0, k1, k2, k3 and an 128-bit initialization variable consisting of four 32-bit words IV0, IV1, IV2, IV3 .

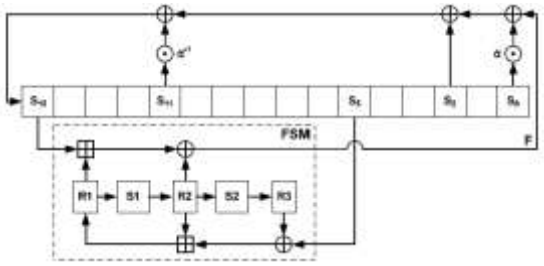

Fig No 2 : Key initialization

In the Initialization Mode, the LFSR receives a 32-bit input word F, which is the input of the FSM.
Let s0 = s0, 0 || s0, 1 ||s0, 2 ||s0,3.
Let s11 = s11,0 ||s11,1 || s11,2 || s11,3.

An intermediate value v is calculated as follow:

v = (s0,1 || s0,2 || s0,3 || 0x00) ⊕MUL α(s0,0) ⊕s2 ⊕(0x00 || s11,0 ||s11,1 || s11,2) ⊕DIV α(s11,3) ⊕F

Then, the different stages of the LFSR are synchronized as presented below:
s0 = s1, s1 = s2, s2 = s3, s3 = s4, s4 = s5, s5 = s6, s6 = s7, s7 = s8, s8 = s9, s9 = s10, s10 = s11, s11 = s12, s12 = s13, s13 = s14, s14 = s15,s15 = v.

© 2017, IERJ All Rights Reserved

Key generation mode

First, the FSM is clocked once and the FSM output word is discarded. Then, the LFSR is clocked in Key stream mode. After that, n 32-bit words of key stream are produced. In Fig 3.3 the key stream-generation operation of SNOW 3G is presented. After the key generation process the system is up to process the data in order to encrypt or decrypt. First, the cipher is clocked once and the output is discarded. Finally, the produced output sequence, called running key, is added bitwise to the plaintext sequence. The result is the cipher text sequence.

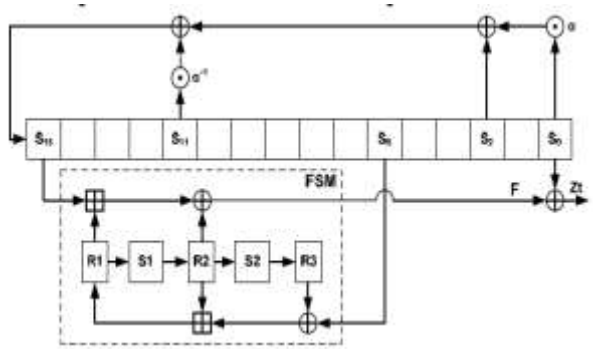

Fig No 3. Key Generation

For t = 1 to n
{
Step1: The FSM is clocked and produces a 32-bit output word F.
Step2: The next key stream word is calculated as follow: z*t* =F ⊕s0.
Step3: Then, the LFSR is clocked in Keystream mode
}

III. CONCLUSION

We have found that SNOW 3G has a linear time complexity, which guarantee efficiency and rapidity during the encryption/decryption process. Furthermore, SNOW 3G has a constant space complexity. SNOW 3G consume a constant and already known amount of temporary memory which is very useful for systems with small working memory such as mobile equipments.

From the study of the time and space complexity of SNOW 3G, we can conclude that this stream cipher was well chosen to be the heart of the confidentiality and integrity algorithms (UEA2/UIA2) of the 3rd generation of mobile Telecommunications Experimental results prove that the SNOW 3G is a very good solution not only for 3G mobile devices however also for applications with high speed demands.

Idea for unified cryptographic hardware accelerator design based on the algorithmic and structural similarities between the ciphers to be implemented. As practical case studies of our proposal, we present LTE, an integrated high performance hardware accelerator for 3GPP LTE stream ciphers SNOW 3G.

	Paper	Algorithm	Throughput
1	High Performance ASCI Implementation of the SNOW 3GStream Cipher	SNOW 3G	7968
2	Comparative Study on4G/LTE Cryptographic Algorithms Based on Different Factors	SNOW 3G	11712
3	Reconfigurable Architecture for SNOW 3G Stream Cipher	SNOW 3G	In our proposed system we are going to increase the throughput from the previous one.

REFERENCE

1) 3GPP TS 33.401 v11.0.1. 3rd Generation Partnership Project, Technical Specification Group Services and Systems Aspects.3GPP System Architecture Evolution(SAE): Security Architecture. Release 11, June 2011.

2) 3rd Generation Partnership Project. Long Term Evaluation Release 10 a beyond (LTE-Advanced). Proposed to ITU at 3GPP TSG RAN Meeting, Spain, 2009.

3) B. Debraize and I.M. Corbella. Fault Analysis of the Stream Cipher Snow 3G. In Fault Diagnosis and Tolerance in Cryptography (FDTC'09), September, 2009.

4) P. Ekdahl and T. Johansson. A New Version of the Stream Cipher SNOW. In Selected Areas in Cryptography (SAC'02), LNCS, Springer, Vol. 2595, pp. 47–61, 2003.

5) Elliptic Technologies Inc. CLP-41: SNOW 3G Flow Through Core. Products-clp- 41. Php. Retrieved on 5 August 2011.

6) Elliptic Technologies Inc. CLP-400: SNOW 3G Key Stream Generator.

7) Elliptic Technologies Inc. CLP-403: SNOW 3G Look Aside Core. products-clp- 403. php. Retrieved on 5 August 2011.

8) Oded Goldreich, "Computational Complexity: A Conceptual Perspective", Cambridge University Press, 2008.

9) ETSI/SAGE Specification: Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2, Document 2: SNOW 3G Specification, September 2006.

10) ETSI/SAGE Technical report: Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 &

© 2017, IERJ All Rights Reserved

UIA2. Document 5: Design and Evaluation Report, Version 1.1, September 2006.

11) K. Alexander, R. Karri, I. Minkin, K. Wu, P. Mishra, X. Li, "Towards 10-100 gbps Cryptographic Architectures", in proc. Of CATT/WICAT Annual Research Review, 2003.

12) Analysis and Implementation of the SNOW 3G Generator Used in 4G/LTE Systems J. Molina-Gil , P. Caballero-Gil C. Caballero-Gil ,Amparo Fuster-Sabater

© 2017, IERJ All Rights Reserved