KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express ▮ (▮▮▮▮) ▮▮▮–▮▮▮

www.elsevier.com/locate/icte

Performance evaluation of Grain family and Espresso ciphers for applications on resource constrained devices

Subhrajyoti Deb*, Bubu Bhuyan

Department of Information Technology, North-Eastern Hill University, Shillong, India

Received 1 December 2017; received in revised form 21 January 2018; accepted 22 January 2018
Available online xxxx

Abstract

A secure stream cipher is an effective security solution for applications running on resource-constrained devices. The Grain family of stream ciphers (Grain v1, Grain-128, and Grain-128a) is a family of stream ciphers designed for low-end devices. Similarly, Espresso is a lightweight stream cipher that was developed recently for 5G wireless mobile communication. The randomness of the keystream produced by a stream cipher is a good indicator of its security strength. In this study, we have analyzed the randomness properties of the keystreams produced by both the Grain Family and Espresso ciphers using the statistical packages DieHarder and NIST STS. We also analyzed their performances in two constrained devices (ATmega328P and ESP8266) based on three attainable parameters, namely computation time, memory, and power consumption.
© 2018 The Korean Institute of Communications Information Sciences. Publishing Services by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Keywords: Stream cipher; Randomness; Dieharder; NIST STS

1. Introduction

Due to the interconnection of a huge number of heterogeneous devices, security assurance has become an important issue, which needs to be addressed in order to make the vision of IoT a reality. To address this issue, a new route of investigation known as Lightweight Cryptography (LWC) was introduced. In March 2017, the National Bureau of Standards, which is now known as National Institute of Standards and Technology (NIST), of the United States started a lightweight cryptography project to examine the limitations and to design a scheme for the standardization of cryptographic algorithms [1].

Over the last few years, numerous LWC primitives, including block ciphers, hash functions, and stream ciphers have been proposed. In this direction, Linear Feedback Shift Register (LFSR) based stream cipher has a very good prospect, because it can generate a large number of pseudo-random binary strings with good cryptographic properties and is easy to implement using hardware. Linear recurrences are used in LFSR, whereas nonlinear recurrence functions are used in Nonlinear Feedback Shift Registers (NFSR). In the context of stream cipher, the same key will always produce the same sequence. To solve this problem, stream cipher uses a fixed-size, one-time Initialization Vector (IV) which may be made public. Examples of LFSR based stream ciphers include A5/1 used in GSM security, E0 used in Bluetooth, etc. The current lightweight stream-cipher design paradigm is very interesting; however, the success of a cipher design depends on its ability to resist cryptanalytic attacks. This motivates us to study stream ciphers that may run on constrained devices.

The main contributions of the paper are as follows:

- We have implemented Grain family and Espresso cipher (in C language) and generated 10^6 keystream bits (with 100 independent files using different keys and IV) for each cipher. The randomness of the generated 10^6 bits was tested using DieHarder and NIST STS.
- We have optimized our C code to achieve faster execution. Further, our optimized codes are ported into two constrained

* Corresponding author.
E-mail addresses: subhrajyotideb1@gmail.com (S. Deb), b.bhuyan@gmail.com (B. Bhuyan).
Peer review under responsibility of The Korean Institute of Communications Information Sciences.

https://doi.org/10.1016/j.icte.2018.01.005
2405-9595/© 2018 The Korean Institute of Communications Information Sciences. Publishing Services by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Please cite this article in press as: S. Deb, B. Bhuyan, Performance evaluation of Grain family and Espresso ciphers for applications on resource constrained devices, ICT Express (2018), https://doi.org/10.1016/j.icte.2018.01.005.

devices, namely Arduino Uno (ATmega328P) and ESP8266 (NodeMcu). The performance of the stream ciphers in the above mentioned constrained devices are measured in terms of time, memory, and power dissipation. Finally, our improved results are compared with those of several existing works.

The remainder of this paper is organized as follows. Section 2 presents the basic specifications of the Grain family and Espresso. Section 3 describes different statistical randomness tests and provides their performance analysis and comparison. Finally, Section 4 concludes the paper.

2. Grain family and Espresso

Grain family: Since last few years, the Grain family of stream ciphers has received considerable attention, because of its lightweight properties. Grain v1 is one of the hardware (Profile 2) candidates of the eStream project [2], and it is the lightest cipher in the portfolio of eSTREAM. The Grain family of ciphers were proposed by Ågren, Hell, Johansson, Maximov, and Meier [3]. In Grain, the filtering function is considered as a type of NFSR, and it introduces nonlinearity to the cipher. The output of the LFSR is masked with the input of this NFSR to balance its state. Grain adopts a bit-oriented architecture, which is appropriate for constrained hardware implementations. Table 1 presents the overall description of the Grain family [3].

Espresso: In 2015, a new type of stream cipher emerged with the publication of Espresso by Elena Dubrova and Martin Hell for 5th generation (5G) mobile communication systems [4]. The key size of the cipher is 128-bit and its IV size is 96-bit. The exact structure of the cipher consists of two building blocks, namely the 256-bit Galois structure NLFSR G and the 20-variable nonlinear output function. The feedback functions of the NLFSR G are specified as follows:

$$\begin{cases} g_{255}(x) = x_0 \oplus x_{41}x_{70} \\ g_{251}(x) = x_{252} \oplus x_{42}x_{83} \oplus x_8 \\ g_{247}(x) = x_{248} \oplus x_{44}x_{102} \oplus x_{40} \\ g_{243}(x) = x_{244} \oplus x_{43}x_{118} \oplus x_{103} \\ g_{239}(x) = x_{240} \oplus x_{46}x_{41} \oplus x_{117} \\ g_{235}(x) = x_{236} \oplus x_{67}x_{90}x_{110}x_{137} \\ g_{231}(x) = x_{232} \oplus x_{50}x_{159} \oplus x_{189} \\ g_{217}(x) = x_{218} \oplus x_3x_{32} \\ g_{213}(x) = x_{214} \oplus x_4x_{45} \\ g_{209}(x) = x_{210} \oplus x_6x_{64} \\ g_{205}(x) = x_{206} \oplus x_5x_{80} \\ g_{201}(x) = x_{202} \oplus x_8x_{103} \\ g_{197}(x) = x_{198} \oplus x_{29}x_{52}x_{72}x_{99} \\ g_{193}(x) = x_{194} \oplus x_{12}x_{21}. \end{cases}$$

However, the remaining feedback functions of G are of the type $g_i(x) = x_{i+1}$. The output keystream $z(x)$ is produced by

$$\begin{aligned} z(x) = {} & x_{80} \oplus x_{99} \oplus x_{137} \oplus x_{227} \oplus x_{222} \oplus x_{187} \\ & \oplus x_{243}x_{217} \oplus x_{247}x_{231} \oplus x_{213}x_{235} \\ & \oplus x_{255}x_{251} \oplus x_{181}x_{239} \oplus x_{174}x_{44} \\ & \oplus x_{164}x_{29} \oplus x_{255}x_{247}x_{243}x_{213}x_{181}x_{174}. \end{aligned} \tag{1}$$

Stream ciphers with a minimal internal state are the best option for low-end devices. Recently, many lightweight stream ciphers such as Sprout, Fruit, and Lizard, which maintain the basic structure of Grain v1, were proposed by various researchers. Thus, the main expectations from a cipher are good statistical properties and a large period.

Here, we present a short background of statistical randomness tests. In the last few years, several researches related to randomness checking in lightweight ciphers have been conducted. Marton et al. highlighted the importance of randomness in modern cryptographic primitives [5]. Meltem Sonmez Turan et al. showed that stream cipher can be used as a random number generator and that the quality of the keystream depends upon different statistical randomness test results [6]. Although different randomness testing mechanisms have their own procedures and advantages, different test strategies lead to blindness in the process. Concurrently, multiple researches are being carried out on randomness issues related to computer science, mathematics, computational complexity, communications etc.

3. Experiment and result analysis

3.1. Methodology

Firstly, we implement the Grain family and Espresso stream ciphers with 10^6 keystream bits. In this work, we have fixed 128-bit key length for Espresso and 80-bit, 128-bit, and 128-bit key lengths for Grain v1, Grain 128, and Grain 128a stream ciphers, respectively. The investigations resulted in several interesting hypotheses; however, keystreams from these ciphers are good in terms of their randomness property. Apart from these findings, we study all the randomness test properties that are used in DieHarder and NIST STS. Here, we tested 100 independent keystream files for each cipher using different keys and IV. In the DieHarder and NIST test suites, all the test case randomness parameters or functions take the finite length of input bits and generate a real number between 0 and 1 known as the p-value. In our experiments, we preferred the significance level of $\alpha = 0.01$, which is the default value for both DieHarder and NIST. Further, we optimized our C codes, and it was ported to ATmega328P and ESP8266. The configuration of the system used for the experiment was as follows: Version: Intel(R) Xeon(R) CPU E31230 3.20 GHz, slot: XU1 PROCESSOR, size: 1794 MHz, capacity: 3800 MHz, width: 64 bits, and clock: 100 MHz.

3.2. Randomness test analysis

Producing high quality random numbers from the deterministic system is a live research problem. The output sequences of the Pseudorandom Number Generator (PRNG) act like independent random variables following uniform distribution over (0,1). Currently, DieHarder and NIST STS are the two extensive statistical tools popularly used for randomness checking. The DieHarder package was developed by Robert G. Brown [7]. The DieHarder test suit consists of 31 fully independent statistical tests. As evident from the statistical randomness literature, very few detailed analyses are available to achieve good randomness results. Most of the generator performances are based on clever

Please cite this article in press as: S. Deb, B. Bhuyan, Performance evaluation of Grain family and Espresso ciphers for applications on resource constrained devices, ICT Express (2018), https://doi.org/10.1016/j.icte.2018.01.005.

Download English Version:

https://daneshyari.com/en/article/6925863

Download Persian Version:

https://daneshyari.com/article/6925863

Daneshyari.com