Design of a New Cryptosystem Combining a MEMS-Accelerometer and a Chaotic Map

Miguel Garcia-Bosque, Adrián Pérez, Carlos Sánchez-Azqueta, Santiago Celma

Grupo de Diseño Electrónico (GDE)
Instituto de Investigación en Ingeniería de Aragón (I3A)
Universidad de Zaragoza, Mariano Esquillor s/n, 50018, Zaragoza, Spain.
Tel. +34-976762707, e-mail: mgbosque@unizar.es

Abstract

In this work, we have used a new concept of sensor-based seed generator in order to generate the keys for a stream cipher based on Skew Tent Map and a Linear Feedback Shift Register. The cryptosystem has been implemented in a Xilinx Virtex 7 FPGA VC707 Evaluation Kit and has been proven to be fast and secure.

Introduction

Due to the necessity of encrypting high amounts of data in real time, there has been an increasing interest in cryptography in the last years. Usually, stream ciphers are used when a high encryption speed is required. In this ciphers, a seed (key) is used in order to generate a long pseudorandom sequence (keystream). Each digit of the pseudorandom sequence is combined with a bit from the plaintext with an XOR operation in order to give a digit of the ciphertext stream. By using the same key, the receiver is capable of generating the same keystream and, therefore, can decode the message by combining each bit from the key and the keystream with an XOR operation.

Some of the most promising stream ciphers are based on chaotic maps since they are able to provide both high speed and security [1]. However, it has been proved that, in order to be secure, the same key cannot be used several times in these type of cryptosystems. Furthermore, the key should be difficult to guess so it is not advisable that the key is generated by a person or a predictable algorithm. Therefore, it is advisable to have a mechanism capable of generating true random seeds. In our work, we have used the noise generated by the ADXL 335 MEMS accelerometer to generate true random seeds. Our motivation comes from the fact that previous researches have shown that MEMS accelerometers are capable of generating good random numbers [2]. Furthermore, MEMS accelerometers are cheap and are present in many wireless devices (such as cellphones, laptops, vehicles, etc.).

Communication system

In this work, we have used a cryptosystem based on a combination of a Skew Tent Map (STM) and a Linear Feedback Shift Register (LFSR). Due to the ergodic property of the chaotic systems, any chaotic map such as the STM is expected to generate pseudorandom sequences. Furthermore, the STM is one of the simplest systems with a continuous region in which all parameter values retain complete chaocity [3], which makes it a good choice. However, when a chaotic map is digitized, the period length of the generated sequences is usually very small which results in poor randomness. The LFSR guarantees that the period length of the generated sequences is big enough improving considerably the quality of the cryptosystem, which has been shown for the Modified Logistic Map (MLM) [4].

In order to generate the seeds, we have acquired the signal produced by the accelerometer at rest by means of a low-noise real-time digital oscilloscope. Then, we have used this signal to generate the initial parameters of the STM-LFSR system. The block diagram of the chaotic encryption system is shown in Fig. 1.

Conclusions

The stream cipher has been implemented in a Xilinx Virtex 7 FPGA VC707 Evaluation Kit and has achieved a throughput of 200 Mbps using 390 LUTs. In order to test the security of this system, several sequences have been generated and have been subjected to the National Institute of Standard and Technology (NIST) randomness tests. All of them have passed the tests proving that the proposed system is secure. Furthermore, we have tested the randomness of some sequences generated using the STM only in order to check that the inclusion of an

LFSR results in improved randomness. Fig. 2 shows the NIST randomness results for sequences generated by the STM and the STM-LFSR respectively.

In conclusion, a new fast and secure stream cipher with a TRNG seed generator has been proposed and has been implemented in an FPGA platform. The NIST randomness tests have proven that this system is secure.

Acknowledgements

The work has been supported by MINECO FEDER (TEC2014-52840) and FPU fellowship to M. Garcia-Bosque (FPU14/03523).

REFERENCES

[1]. HASIMOTO-BELTRAN, R. High-performance multimedia encryption based on chaos. *Chaos: Interdisciplinary J. Nonlinear Sci.*, vol. 18, no. 2, pp.023110-1 -023110-8, 2008.

[2]. VORIS, J., SAXENA, N. and HALEVI, T. Accelerometers and randomness: Perfect together, *Proc. 4th ACM Conf. Wireless Netw*. Secur, pp. 115-126, 2011.

[3]. ALVAREZ, G. and LI, S. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, *International Journal of Bifurcation and Chaos,* vol. 16, no. 8, pp. 2129-2151, 2006.

[4]. GARCIA-BOSQUE, M., SANCHEZ-AZQUETA, C. and CELMA, S. Secure communication system based on a logistic map and a linear feedback shift register, *Proc. IEEE Int. Symp. Circuits and Systems.* Montreal, pp. 1170-1173, 2016.

[5]. GARCIA-BOSQUE, M., SANCHEZ-AZQUETA, C. and CELMA, S. Application of a MEMS-Based TRNG in a Chaotic Stream Cipher, *Sensors*, Vol. 17, no. 3:646, 2017.

[6]. GARCIA-BOSQUE, M., SANCHEZ-AZQUETA, C. and CELMA, S. MEMS-Based Seed Generator Applied to a Chaotic Stream Cipher, *Proc. SPIE Microtechnologies.* Barcelona, 2016 (accepted)

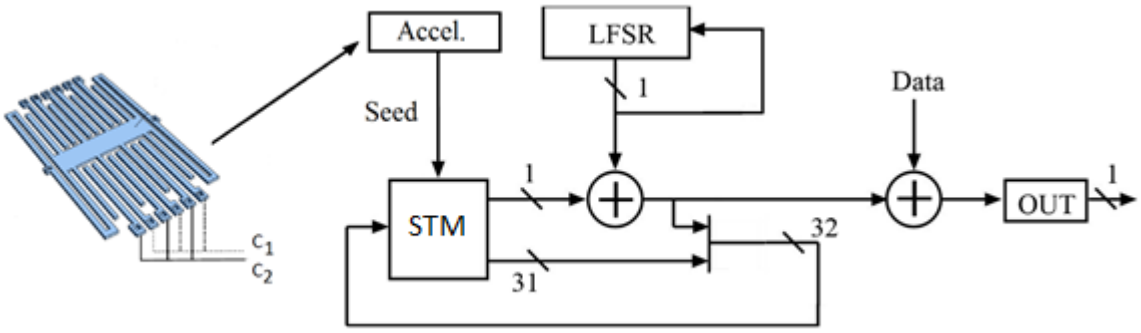
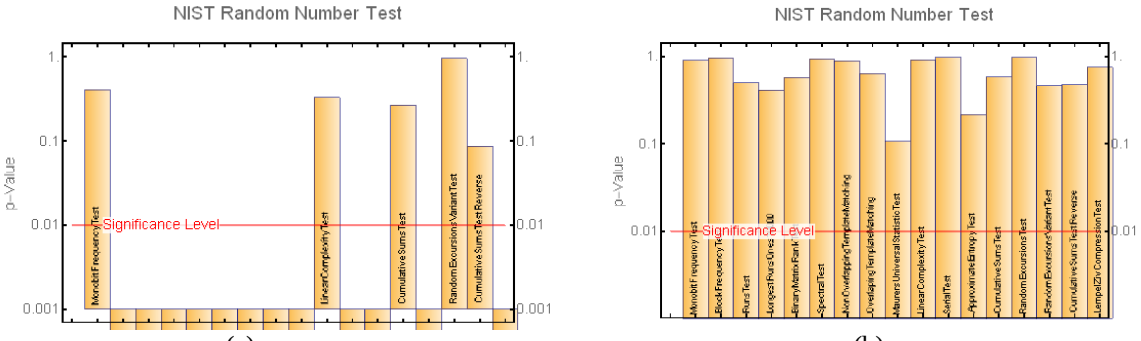


Fig. 1. Block diagram of the chaotic encryption system



(a) (b)

Fig. 2. NIST results for a chaotic sequence generated by (a) STM algorithm (b) STM-LFSR algorithm.