View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Repositorio Universidad de Zaragoza

Available online at www.sciencedirect.com

ScienceDirect

Procedia Engineering 168 (2016) 1663 – 1666

Procedia Engineering

www.elsevier.com/locate/procedia

30th Eurosensors Conference, EUROSENSORS 2016

Sensor-Based Seeds for a Chaotic Stream Cipher

M. Garcia-Bosque[a],*, C. Sánchez-Azqueta[a], S. Celma[a]

Group of Electronic Design, Aragón Institute of Engineering Research, Universidad de Zaragoza
C/Pedro Cerbuna 12, Zaragoza, 50009, Spain.

Abstract

In this paper we have used a surface micromachined capacitive accelerometer in order to generate seeds that are suitable for secure communications between wireless smart sensors for IoT networks. These seeds have then been used in a chaotic stream cipher based on a Modified Logistic Map and a Linear Feedback Shift Register. The sequences generated by the chaotic stream cipher have been subjected to the randomness NIST tests. All the tests have been passed, proving that the proposed approach could be used for secure communications.

© 2016 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).

Peer-review under responsibility of the organizing committee of the 30th Eurosensors Conference

Keywords: Security; Encryption; Logistic Map.

1. Introduction

In the last years, cryptography has become an important field of study due to the necessity of encrypting high amounts of data in real time. Typically, stream ciphers are used in applications where high speed is needed.

A stream cipher consists in a symmetric key cipher where each bit of the plaintext is combined with the bit of a pseudorandom sequence (keystream). Usually, the keystream is generated from a seed that serves as the cryptographic key. The receiver, using the same seed, is able to generate an identical keystream as the transmitter and, by doing the inverse combining operation, can recover the original plaintext. Stream ciphers have the advantage over other ciphers of being usually faster and having lower hardware complexity.

Some of the most promising stream ciphers are based on chaotic maps, since they are able to provide both speed and high security [1]. In our work, we have used a cipher that consists on a combination of a Modified Logistic Map (MLM) and a Linear Feedback Shift Register (LFSR). The chaotic nature of the MLM is capable of generating random-

* Corresponding author. Tel.: +34-876-553539
E-mail address: mgbosque@unizar.es

1877-7058 © 2016 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY-NC-ND license
(http://creativecommons.org/licenses/by-nc-nd/4.0/).

Peer-review under responsibility of the organizing committee of the 30th Eurosensors Conference
doi:10.1016/j.proeng.2016.11.485

like sequences while the LFSR manages to increase the period of the cycles, avoiding the periodic windows that can appear due to the digitalization of a chaotic system.

However, in order to be secure, it is necessary that the same key is not used several times. Furthermore, the seed should be difficult to guess, so making a person or a predictable algorithm choose the key should be avoided. For these reasons, the best solution is to have a mechanism capable of generating true random seeds.

In our work, we have used a surface micromachined capacitive accelerometer in order to generate true random seeds. Our motivation comes from the fact that previous works have shown that accelerometers are capable of generating good random numbers [2]. Furthermore, inertial MEMS such as accelerometers are cheap, are present in many wireless devices (e.g. cellphones, cameras, bikes, vehicles, laptops, etc.) and can be added easily to other devices that typically do not have them (e.g. security systems, hifi equipment, home appliances, etc.).

Once the seeds have been generated, they have been used as the initial parameters of the MLM-LFSR system that is capable of generating long sequences at high speed. These sequences have been subjected to the NIST randomness test, proving that our system is secure.

2. Modified Logistic Map

The classic logistic map is given by:

$$x_{i+1} = \gamma x_i(1 - x_i) \tag{1}$$

where x_i is a parameter between zero and one, and γ is a parameter that determines the behavior of the system. Typically, when $3.57 < \gamma \leq 4$ the system presents chaos and, therefore, small variations in the initial value of x_0 yield to very different sequences. When $\gamma > 4$ most initial values leave the interval $[0,1]$ and diverge while, for $\gamma < 3.57$ the system generates non-chaotic sequences.

Due to its simplicity, many of the proposed cryptosystems are based on the logistic map. This map, however, cannot be implemented directly in a real cryptosystem for two reasons. First, even in the chaotic region, there is an open and dense set of parameters γ that yield to periodic (non-chaotic) sequences. In order to encrypt a message properly, one must avoid choosing one of those parameters. Unfortunately, the parameters that generate these periodic sequences are not fully known.

Second, the images in this map are not uniformly distributed in the interval $[0,1]$ but, instead, in the interval $[0, \gamma/4]$. Therefore, an attacker could measure the length of the attractor and, therefore, estimate the value of γ. This can be a problem since the value of γ is usually part of the key.

In our work, we have used a Modified Logistic Map that is capable of solving this problems:

$$f(x_i) = x_{i+1} = \begin{cases} \gamma x_i(1 - x_i) \ (\mathrm{mod}\ 1), & x \in I_{ext} \\ \dfrac{\gamma x_i(1 - x_i) \ (\mathrm{mod}\ 1)}{\frac{\gamma}{4} \ (\mathrm{mod}\ 1)}, & x \in I_{int} \end{cases} \tag{2}$$

where $I_{ext} \in \ (0,1) \backslash I_{int}$, $I_{int} = [\eta_1, \eta_2]$, $\eta_1 = (1/2) - \sqrt{(1/4) - [\gamma/4]/\gamma}$ and $\eta_2 = (1/2) + \sqrt{(1/4) - [\gamma/4]/\gamma}$ and $[\gamma/4]$ is the integer part of $\gamma/4$.

When $\gamma > 4$, this system has been proven of being capable of generating chaotic sequences with the values of x_i uniformly distributed in the interval $[0,1]$ for any value of γ [3].

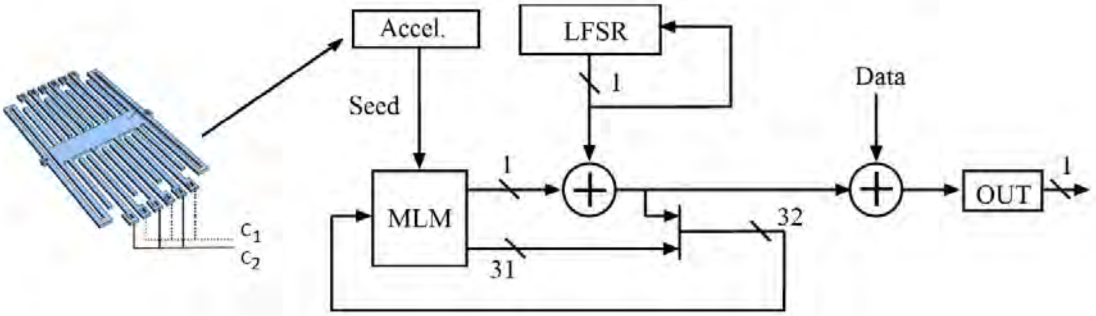

Fig. 1. Block diagram of the communication system.

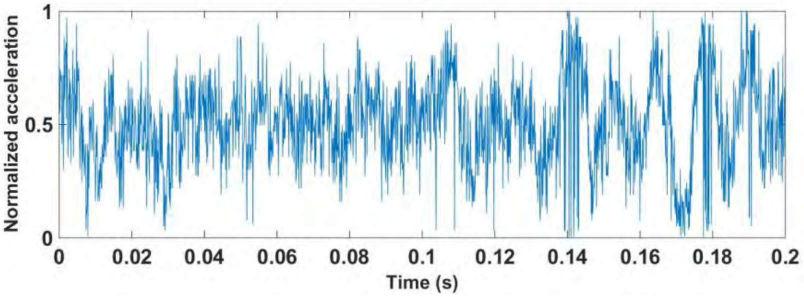

Fig. 2. Random noise generated by an accelerometer

3. Encryption algorithm

Although the MLM is theoretically capable of generating good random sequences, when it is digitalized a new problem arises. Since there is a finite number of different possible values of x_i and, for a fixed value of γ, given a value of x_i the value of x_{i+1} is unambiguously determined, the generated sequences will always be periodic. For an n bit implementation, the maximum possible period of the sequences is 2^n but, typically, the sequences obtained have a much shorter period. In order to solve this problem, our algorithm introduces small pseudorandom perturbations in the values of x_i.

The operation of our communication system is summarized in Fig. 1. The Least Significant Bit (LSB) of each x_i generated by the MLM is XORed with a pseudorandom bit generated by a Linear Feedback Shift Register (LFSR). This bit, which should have good randomness properties, is then XORed with the bit of data that we want to encrypt. This bit is also recombined with the other bits of x_i in order to generate the next value of the sequence (x_{i+1}). It has been proven in [4] that, if the period of the LFSR is a prime number, the period of the generated sequences will be bigger or equal than this number. Some possible orders of the LFSR that can be used since they generate sequences with prime periods are 19, 31, 61 and 89.

Finally, in order to generate the initial parameters of the system (i.e. x_0, γ and the initial state of the LFSR) we have used the noise generated by an ADXL 335 accelerometer. This way, we assure that the seed is generated by a true number generator instead of a predictable algorithm. For that purpose, we have measured with an oscilloscope the signal produced by the accelerometer motionless. In order to remove the electric hum, we have subtracted the x-acceleration and the y-acceleration signals. The results obtained are shown in Fig. 2.

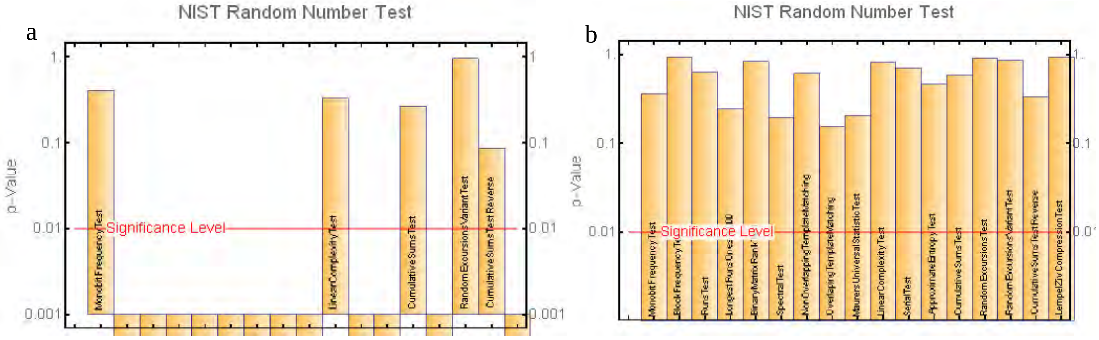

Figure 3. NIST results for a chaotic sequence generated by (a) the MLM algorithm (b) the MLM-LFSR algorithm.

4. Results

This communication system has been simulated in a Simulink environment using a 32-bit fixed-point arithmetic. We have used the blocks provided by Xilinx System Generator in order to be able to translate the code into an FPGA easily in the future. In order to test the security of this system, several sequences have been generated and have been subjected to the National Institute of Standards and Technology (NIST) randomness test [5]. Furthermore, we have tested some sequences generated using only the MLM in order to check that our algorithm is indeed an improvement.

We have seen that the sequences generated using exclusively the MLM have only passed some of the randomness test while the sequences generated by our algorithm have passed all the tests (Fig. 3).

5. Conclusions

A secure encryption system with an MLM-LFSR architecture and a sensor based seed generator has been proposed. This communication system have been proven to be capable of generating good random sequences proving that could be suitable to applications that require high security

This algorithm is currently being implemented in a Zedboard that includes a Zynq-7000 system on chip. The implementation results will be presented in the conference.

Acknowledgements

This work has been supported by MINECO-FEDER (TEC2011-23211 and TEC2014-52840-R) and FPU fellowship (FPU14/03523).

References

[1] M. Garcia-Bosque, C. Sánchez-Azqueta, S. Celma, 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.

[2] J. Voris, N. Saxena, T. Halevi, Accelerometers and randomness: Perfect together, Proc. 4th ACM Conf. Wireless Netw. Secur, pp. 115-126, 2011.

[3] S. L. Chen, S. M. Chang, W. W. Lin, T. Hwang, Digital secure-communication using robust hyper-chaotic systems, Int. J. Bif. Chaos, vol. 18, no.11, pp. 3325-3339, 2008.

[4] L. Kocarev, S, Lian, Chaos-based cryptography, Springer, 2009.

[5] NIST Special Publication 800-22 Rev.1a: A statistical test suit for random and pseudorandom number generators for cryptographioc applications, 2010.

[6] J. Van der Geer, J.A.J. Hanraads, R.A. Lupton, The art of writing a scientific article, J. Sci. Commun. 163 (2000) 51–59.