A new key generator based on an auto-switched hybrid chaotic system and its FPGA implementation

Sid Hichem[*], Azzaz Mohamed Salah[*] and Sadoudi Saïd[**]
[*] *Laboratoire Systèmes Electroniques et Numériques, EMP, Algiers, Algeria*
[**] *Laboratoire Télécommunications, EMP, Algiers, Algeria*

Abstract. In this paper a new key generator is presented, it is constructed by an auto-switched numerical resolution of multiple three dimensional continuous chaotic systems (Lorenz, Rôssler, Chen) how excite a discreet chaotic system (Henon Map). The designed chaotic system provides complex chaotic attractors and can change its behaviors automatically via a chaotic switching-rule. The originality of the proposed architecture is that allows to solve the problem of the finite precision due to the digital implementation while provides a good compromise between high security, performance and hardware resources (low power and cost). Hardware digital implementation and FPGA circuit experimental results of this generator demonstrate that this promising technique can be applied in efficient embedded ciphering communication systems.

Introduction

Currently, several chaotic generators have been studied (Lorenz, Chen, Chua and Lü, etc) [1]. However, these main chaotic generators are easily identifiable by a simple visualization of their attractors that can be used in cryptosystems [2]. When chaotic systems are implemented or implanted in digital form, a dynamic degradation of the response occurs. More precisely, the dynamic properties of digital chaotic systems can become non-ideal. The most well-known problem is the existence of many chaotic short-length orbits, which can weaken the desired statistical properties of chaotic evolving digital data, resulting in degradation of the security of the encryption process [3]. In this context, it becomes important to mask or to develop mechanisms associated with these generators in order to increase the complexity of a cryptanalysis from an identification of the chaotic signals on one side and to solve the problem of precision during a digital implementation, on the other hand. In this work we will use the principle of chaos in order to propose, design and implement a new generator based chaos that better responds to the requirement of modern cryptography. The interest of our solution is to propose a complex chaotic system allowing an unidentifiable cipher key generator by an analysis of its attractors, while proposing optimized architecture and hardware implementation giving a very useful and attractive compromise between high speed, low area cost and secure data communications for embedded applications. Our proposed logic Register Transfer Level (RTL) architecture is based on pipelined numerical method to resolve several 3D chaotic differential equations characterizing some chaotic systems. In this work, we'll present, the modeling of the presented auto-switched system and its hardware architecture, the simulations results on Xsim of Vivado, the discussion of the hardware implementation results on Genesys 2 Kintex-7 Xilinx FPGA technology, performance evaluations, real-time measurements and the evaluation of the random dynamical behaviors of our new scheme through statistical tests in order to prove that the proposed hybrid generator exhibits truly random sequences suitable as cipher keys for the data encryption.

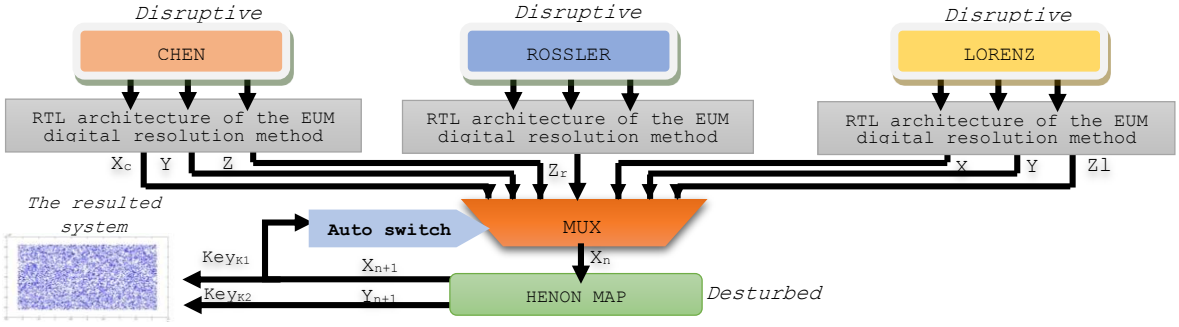

Figure 1: The perturbation technique adopted for the modeling of the proposed generator.

Results and discussion

The synthesis results after place, route and real time implementation show a low power consumption, a very low latency and low use of the resources of our FPGA card, all this is due to our working approach and the optimization of the codes developed. After visualization of the different signals of our generator, we observed the similarity between the simulation results and the real-time implementation results, which validates our hardware implementation approach. To quantify the random criterion of the keys generated, we performed a statistical analysis using the statistical test batteries of NIST, DIEHARD and ENT. We noticed that our results passed all the tests successfully. Consequently, we can say that the generated keys have a random character, so they are robust, and they are ready to be used in cryptosystems.

References

[1] E. N. Lorenz (1963) Deterministic nonperiodic flow. *J. Atmos. Sci.* **130**:141-20.
[2] M. S. Azzaz (2012) Implantation paramétrable d'un nouvel algorithme de cryptage symétrique basée Chaos par inclusion au sein d'une architecture reconfigurable de type FPGA. PhD thesis, Cotutelle de thèse EMPA. & U A. F.
[3] G. Alvarez and S. Li (2006) Some basic cryptographic requirements for chaos-based cryptosystems. *Int. J. Bifurct. Chaos* **16**:2129-2151