Communication services empowered with a classical chaos based cryptosystem

G. Vidal

[1] Institute of Physics
University of Navarra
[2] Enigmedia Co.
gerard@enigmedia.es

Abstract. Enigmedia is an encryption system based on a pseudo-random bit generator (PRBG) which relies on hyperchaotic system, sampled under certain rules in order to avoid any attempt to reconstruct the original trajectory or statistical attacks [1]. The plaintext is XOR'ed with the keystream, obtained from the PRBG. This PRBG is highly efficient, being several orders of magnitude faster than other standards. Furthermore Enigmedia cryptosystem has passed NIST and Diehard statistical test, and it is involved in a validation process.
First application featuring Enigmedia is a plug&play $70 USB-device transforming any TV into encrypted HD-videoconference for e-health purpose. This development is also available for mobile & tablet integration thought App. Further work will include sensor integration for monitoring patients.

References

[1] G. Vidal, M. S. Baptista, H. Mancini, 2012, "Fundamentals of a classical chaos-based cryptosystem with some quantum cryptography features," *Int. J. Bif. Chaos* 22, 1250243 (2012)