Abstracts of MMA2016, June 1–4, 2016, Tartu, Estonia

CHAOS BASED CRYPTOGRAPHY

BENSON K. MUITE and GELO N. TABIA

Institute of Computer Science, University of Tartu

J. Liivi 2, 50409 Tartu, Estonia

E-mail: benson.muite@ut.ee, gelo.tabia@ut.ee

Reversible chaotic dynamical systems have been used to generate cryptographic schemes by many experts from the dynamical systems community. Unfortunately, few cryptographers have examined this work closely since security analysis of such schemes is usually difficult and implementations are typically slow compared to other cryptographic schemes. In this paper, an approach that allows the use of dynamical systems to produce a family of efficient encryption schemes that are easy to encode is introduced. Many of the prescriptions suggested in [1] are followed. To ensure good mixing properties, the scheme also uses a discretized partial differential equation. Additional suggestions applied mathematicians should follow to ensure greater uptake of use of chaotic inspired ciphers by cryptographers are introduced.

REFERENCES

[1] M. Henricksen. A critique of some Chaotic-Map and Cellular Automata-Based Stream Ciphers. In: *Proc. 13th Asian Computing Science Conference, Seoul, Korea, December 14-16, 2009*, Advances in Computer Science - ASIAN 2009. Information Security and Privacy Volume 5913 of the series Lecture Notes in Computer Science, 69-78.