2006 Vol.45 No.3 pp.477-482 DOI:

A Cryptographic Scheme Based on Spatiotemporal Chaos of Coupled Map Lattices

MA Hui,[1] ZHU Kai-En,[1] and CHEN Tian-Lun[1,2]

[1] Institute of Physics, Nankai University, Tianjin 300071, China
[2] CCAST (World Laboratory), P.O. Box 8730, Beijing 100080, China

(Received: 2004-11-9; Revised: 2005-9-8)

Abstract: We propose a cryptographic scheme based on spatiotemporal chaos of coupled map lattices (CML) ,which is based on one-time pad. The structure of the cryptosystem determines that the progress in decryption implies the progress in exploring the dynamical behavior of spatiotemporal chaos in CML. A part of the initial condition of CML is used as a secret key, and the recovery of the secret key by exhaustive search is impossible due to the sensitivity to the initial condition in spatiotemporal chaos system. Specially the software implementation of the scheme is easy.

PACS: 05.45.Ra, 05.45.Vx

Key words: spatiotemporal chaos, coupled map lattices, cryptography

[Full text: PDF]

Close