**Caballero-Gil, P.**; **Fúster-Sabater, A.**

**A cellular automata based method for predicting binary sequences.** (English) Zbl 1157.68392

Gammerman, A. (ed.), Artificial intelligence and applications. Machine learning. As part of the 26th IASTED international multi-conference on applied informatics. Calgary: International Association of Science and Technology for Development (IASTED); Anaheim, CA: Acta Press (ISBN 978-0-88986-710-9/CD-ROM). 164-168 (2008).

Summary: The paper studies the application of linear hybrid cellular automata (CA) to generate some binary sequences with application in cryptography. In this sense, we propose a novel CA-based linear model that behaves exactly the same as the reproduced cryptographic keystream generators. Due to the simplicity of the transition rules that govern these linear automata, the implementation of such models is quite easy. Some illustrative examples showing the potential usefulness of the proposed tool for cryptanalysts complete the work.

For the entire collection see [Zbl 1154.68012].

**MSC:**

68Q80 Cellular automata (computational aspects)
68P25 Data encryption (aspects in computer science)

**Keywords:**

applications of cellular automata; cryptographic sequences