De Cannière, Christophe; **Preneel, Bart**

Trivium. (English) Zbl 1285.94054

Robshaw, Matthew (ed.) et al., New stream cipher designs. The eSTREAM finalists. Berlin: Springer (ISBN 978-3-540-68350-6/pbk). Lecture Notes in Computer Science 4986, 244-266 (2008).

Summary: In this chapter, we propose a new stream cipher construction based on block cipher design principles. The main idea is to replace the building blocks used in block ciphers by equivalent stream cipher components. In order to illustrate this approach, we construct a very simple synchronous stream cipher which provides a lot of flexibility for hardware implementations, and seems to have a number of desirable cryptographic properties.

For the entire collection see [Zbl 1259.94006].

MSC:

94A60 Cryptography
68P25 Data encryption (aspects in computer science)

Software:

Trivium

Full Text: DOI