De Cannière, Christophe; **Dunkelman, Orr**; **Knežević, Miroslav**

KATAN and KTANTAN – a family of small and efficient hardware-oriented block ciphers.

(English) Zbl 1290.94060

Clavier, Christophe (ed.) et al., Cryptographic hardware and embedded systems – CHES 2009. 11th international workshop Lausanne, Switzerland, September 6–9, 2009. Proceedings. Berlin: Springer (ISBN 978-3-642-04137-2/pbk). Lecture Notes in Computer Science 5747, 272-288 (2009).

Summary: In this paper we propose a new family of very efficient hardware oriented block ciphers. The family contains six block ciphers divided into two flavors. All block ciphers share the 80-bit key size and security level. The first flavor, KATAN, is composed of three block ciphers, with 32, 48, or 64-bit block size. The second flavor, KTANTAN, contains the other three ciphers with the same block sizes, and is more compact in hardware, as the key is burnt into the device (and cannot be changed).

The smallest cipher of the entire family, KTANTAN32, can be implemented in 462 GE while achieving encryption speed of 12.5 KBit/sec (at 100 KHz). KTANTAN48, which is the version we recommend for RFID tags uses 588 GE, whereas KATAN64, the largest and most flexible candidate of the family, uses 1054 GE and has a throughput of 25.1 Kbit/sec (at 100 KHz).

For the entire collection see [Zbl 1172.68301].

MSC:

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

Software:

KATAN; KTANTAN

Full Text: DOI