# Cryptology ePrint Archive: Report 2011/345

### LBlock: A Lightweight Block Cipher *

*Wenling Wu and Lei Zhang*

**Abstract:** In this paper, we propose a new lightweight block cipher called LBlock. Similar to many other lightweight block ciphers, the block size of LBlock is 64-bit and the key size is 80-bit. Our security evaluation shows that LBlock can achieve enough security margin against known attacks, such as differential cryptanalysis, linear cryptanalysis, impossible differential cryptanalysis and related-key attacks etc. Furthermore, LBlock can be implemented efficiently not only in hardware environments but also in software platforms such as 8-bit microcontroller. Our hardware implementation of LBlock requires about 1320 GE on 0.18 $\mu m$ technology with a throughput of 200 Kbps at 100 KHz. The software implementation of LBlock on 8-bit microcontroller requires about 3955 clock cycles to encrypt a plaintext block.

**Category / Keywords:** secret-key cryptography /

**Publication Info:** corrected version of the paper published at ACNS 2011, LNCS 6715

**Date:** received 26 Jun 2011, last revised 29 Jun 2011

**Contact author:** zhanglei1015 at is iscas ac cn

**Available formats:** PDF | BibTeX Citation

**Note:** This paper was first published at ACNS 2011, LNCS 6715, pp. 327-344. Unfortunately, there are some errors in the contents of S-box table in page 332, and here we provide a revision of this paper. There are some errors in the contents of $s_8$ and $s_9$ in the original paper, and we have corrected them here. Note that the other parts of this paper remain unchanged (including test vectors in Appendix I). The errors are only introduced in our typos. PS. Thanks very much for the reminder by Nese Oztop, and apologized for our carelessness.

**Version:** 20110629:063440 (All versions of this report)

**Discussion forum:** Show discussion | Start new discussion

---

[ Cryptology ePrint archive ]