Cryptology ePrint Archive: Report 2013/190

Power Analysis Attacks against FPGA Implementations of KLEIN

Shaohua Tang and Jianhao Wu and Weijian Li and Zheng Gong

Abstract: KLEIN is a family of block ciphers proposed by Zheng Gong et al. at RFIDSec 2011, and its lightweight features are suitable for resource-constrained devices. However, the original design of KLEIN does not consider the potential attacks by power analysis methods. This paper presents power analysis attacks against a FPGA implementation of KLEIN by the authors of KLEIN. The attacking strategy, attacking point and complexity of our attacks via power analysis against KLEIN are discussed in detail. Besides, the implementation of the attacks is also described, and the experimental data is given. A lot of attacking experiments are launched by this paper, and the experiments confirm that the success probability of our attacks is nearly 100%. Finally, a defensive countermeasure against our attacks is proposed.

Category / Keywords: secret-key cryptography / power analysis attack, KLEIN, FPGA

Date: received 2 Apr 2013, last revised 2 Apr 2013

Contact author: csshtang at gmail com

Available formats: PDF | BibTeX Citation

Version: 20130402:145325 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]