Cryptology ePrint Archive: Report 2011/165

Improved Side Channel Cube Attacks on PRESENT

XinJie Zhao and Tao Wang and ShiZe Guo

Abstract: The paper presents several improved side channel cube attacks on PRESENT based on single bit leakage model. Compared with the previous study of Yang et al in CANS 2009 [30], based on the same model of single bit leakage in the 3rd round, we show that: if the PRESENT cipher structure is unknown, for the leakage bit 0, 32-bit key can be recovered within $2^{7.17}$ chosen plaintexts; if the cipher structure is known, for the leakage bit 4,8,12, 48-bit key can be extracted by $2^{11.92}$ chosen plaintexts, which is less than 2^{15} in [30]; then, we extend the single bit leakage model to the 4th round, based on the two level “divide and conquer” analysis strategy, we propose a sliding window side channel cube attack on PRESENT, for the leakage bit 0, about $2^{15.14}$ chosen plaintexts can obtain 60-bit key; in order to obtain more key bits, we propose an iterated side channel cube attack on PRESENT, about $2^{8.15}$ chosen plaintexts can obtain extra 12 equivalent key bits, so overall $2^{15.154}$ chosen plaintexts can reduce the PRESENT-80 key searching space to 2^{8}; finally, we extend the attack to PRESENT-128, about $2^{15.156}$ chosen plaintexts can extract 85 bits key, and reduce the PRESENT-128 key searching space to 2^{43}. Compared with the previous study of Abdul-Latip et al in ASIACCS 2011 [31] based on the Hamming weight leakage model, which can extract 64-bit key of PRESENT-80/128 by 2^{13} chosen plaintexts, our attacks can extract more key bits, and have certain advantages over [31].

Category / Keywords: Side channel attacks, Cube attack, black box attack, divide and conquer, sliding window; iterated attack, PRESENT-80/128

Date: received 1 Apr 2011, last revised 10 Apr 2011

Contact author: zhaoxinjieem at 163 com

Available formats: PDF | BibTeX Citation

Note: Make some corrections of PRESENT-80 attack.

Version: 20110410:161044 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]