Cryptology ePrint Archive: Report 2012/715

New Impossible Differential Attack on SAFER_{+} and SAFER_{++}

Jingyuan Zhao and Meiqin Wang and Jiazhe Chen and Yuliang Zheng

Abstract: SAFER\scriptsize + \normalsize was a candidate block cipher for AES with 128-bit block size and a variable key sizes of 128, 192 or 256 bits. Bluetooth uses customized versions of SAFER\scriptsize + \normalsize for security. The numbers of rounds for SAFER\scriptsize + \normalsize with key sizes of 128, 192 and 256 are 8, 12 and 16, respectively. SAFER\scriptsize ++\normalsize, a variant of SAFER\scriptsize +\normalsize, was among the cryptographic primitives selected for the second phase of the NESSIE project. The block size is 128 bits and the key size can take either 128 or 256 bits. The number of rounds are 7 for SAFER\scriptsize ++ \normalsize/128 and 10 for SAFER\scriptsize ++ \normalsize/256. Both ciphers use PHT as their linear transformations. In this paper, we take advantage of properties of PHT and S-boxes to identify 3.75-round impossible differentials for SAFER\scriptsize ++ \normalsize and 2.75-round impossible differentials for SAFER\scriptsize +\normalsize, which result in impossible differential attacks on 4-round SAFER\scriptsize +\normalsize/128 (256), 5-round SAFER\scriptsize ++\normalsize/128 and 5.5-round SAFER\scriptsize ++\normalsize/256. Our attacks significantly improve previously known impossible differential attacks on 3.75-round SAFER\scriptsize +\normalsize/128(256) and SAFER\scriptsize ++\normalsize/128(256). Our attacks on SAFER\scriptsize +\normalsize/128(256) and SAFER\scriptsize ++\normalsize/256 represent the best currently known attack in terms of the number of rounds.

Category / Keywords: SAFER\scriptsize +\normalsize, SAFER\scriptsize ++\normalsize, Impossible Differential, PHT, Bluetooth

Publication Info: ICISC 2012

Date: received 20 Dec 2012, last revised 3 Jan 2013

Contact author: mqwang at sdu edu cn

Available formats: PDF | BibTeX Citation

Version: 20130103:072146 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]