西安电子科技大学学报 2008 35 (3): 455-458 ISSN: 1001-2400 CN: 61-1076/TN

用不可能差分法分析17轮SMS4算法

陈杰, 胡予濮, 张跃宇

(西安电子科技大学 计算机网络与信息安全教育部重点实验室，陕西 西安 710071)

收稿日期 修回日期 网络版发布日期 2008-6-4 接受日期

摘要 SMS4是我国在2006年公布的第一个商用分组密码算法. 通过分析SMS4每一轮输入输出对的差分的变化，首次给出一个14轮SMS4的不可能差分特性:如果输入的明文对的差分为(a, a, a, 0)，那么14轮之后的输出差分不可能为(a, a, a, 0). 利用该性质，在14轮不可能差分密码分析的基础上，前面加了两轮，后面加了一轮，提出了一种不可能差分密码分析17轮 SMS4的方法. 该方法分析17轮SMS4需要2¹⁰³的选择明文，2¹²⁴的17轮SMS4加密以及2⁸⁹分组的记忆存储空间，猜测密钥的错误概率仅为2^{-88.7}.

关键词 分组密码 SMS4算法 不可能差分分析

分类号 TN918.1

Impossible differential attack on the 17-round block cipher SMS4

CHEN Jie,HU Yu-pu,ZHANG Yue-yu

(Ministry of Education Key Lab. of Computer Network and Information Security, Xidian Univ., Xi′an 710071， China)

Abstract

The SMS4 is the first commercial block cipher published by our government in 2006. By analyzing the changes of the difference between input and output pairs in each round, this paper first presents an impossible differential property for the 14-round SMS4 if the difference of the input plaintext pair is (a, a, a, 0), it is impossible that the difference of 14-round output pair is (a, a, a, 0). Based on this property, a new method is proposed for cryptanalyzing the 17-round SMS4, which is to add two rounds and one round to each end of the impossible differential cryptanalysis for the 14-round SMS4. This attack on the reduced 17-round SMS4 requires about 2¹⁰³ chosen plaintexts, performs 2¹²⁴ 17-round SMS4 encryptions, and demands 2⁸⁹ words of memory. Furthermore, the probability of its failure to recover the secret key is only 2^{-88.7}.

Key words block cipher SMS4 impossible differential attack

DOI:

通讯作者 陈杰 jchen@mail.xidian.edu.cn