吉林大学学报(理学版) 2013, 51(01) 128-131 DOI: ISSN: 0412-1961 CN: 21-1139/TG

电子科学

A5/1的故障分析

左平 [1,2], 申延成 [2], 华宏图 [2,3], 陈守东 [1]

1. 吉林大学 商学院, 长春 130012|2. 空军航空大学 基础部, 长春 130022; 3. 吉林大学 数学学院, 长春 130012

摘要:

结合故障攻击与Guess determine攻击的思想, 提出A5/1在另一种模型下的故障分析. 结果表明: 通过引入故障, 可成功过滤占总猜测数99.9%的错误猜测, 最终可完全恢复A5/1的内部状态, 攻击的复杂度约为2^{40}, 成功的概率大于99%.

关键词: 流密码 GSM A5/1 故障分析

Fault Analysis of A5/1

ZUO Ping [1,2], SHEN Yan cheng [2], HUA Hong tu [2,3], CHEN Shou dong [1]

1. College of Business, Jilin University, Changchun 130012, China;
2. Department of Foundation, Aviation University of Air Force, Changchun 130022, China;
3. College of Mathematics, Jilin University, Changchun 130012, China

Abstract:

A new fault attack was proposed on the basis of combining the idea of fault attack with that of guess determine attack, by which 99.9% of wrong guesses can be discarded successfully, and furthermore the inner state of A5/1 can be recovered in the end. The complexity of this attack is about 2^{40}, and the success probability of this attack is more than 99%.

Keywords: stream cipher; GSM; A5/1; fault analysis

收稿日期 2012-05-04 修回日期 网络版发布日期

DOI:

基金项目:

通讯作者: 陈守东

作者简介:

作者Email: chensd@jlu.edu.cn

参考文献:

本刊中的类似文章

文章评论