电子与信息学报 2006 28 (5): 827-831 ISSN: 1009-5896 CN: 11-4494/TN

论文

# 基于相关攻击的A5/1算法识别

陈 伟①, 胡 云①, 杨义先①, 钮心忻②

①北京邮电大学信息安全中心 北京 100876;②北京邮电大学数字内容研究中心 北京 100876

收稿日期 2004-12-20 修回日期 2005-11-28 网络版发布日期 2007-12-3 接受日期

摘要
利用相关攻击获得畸变的A5/1序列，再用统计工具对其进行处理可以得出A5/1统计特征，从而找到正确区分A5/1算法输出和伪随机序列的方法。实验验证该方法能有效地将A5/1算法输出和伪随机序列区分开来。

关键词 密码分析 算法识别 A5/1算法 相关攻击 正态分布

分类号 TN918

## Application of Correlation Attack in Algorithm Identify

Chen Wei①, Hu Yun①, Yang Yi-xian①, Niu Xin-xin②

①Information Security Center, Beijing University of Posts & Telecommunications, Beijing 100876, China;②Research Center of Digital Contents, Beijing University of Posts & Telecommunications, Beijing 100876, China

Abstract
A correlation attack on A5/1 algorithm can be educed by the linear filling weakness in initiate process of A5/1 algorithm. An aberrant A5/1 sequence can be obtained from it, which have treated by statistic tools to get A5/1 statistic trait, so the distinction of A5/1 output from real random sequence can be found. Test results show that this method can work effectively.

Key words Cryptanalysis Algorithm identify A5/1 algorithm Correlation attack Normal distribution

DOI:



通讯作者

作者个人主页 陈 伟①; 胡 云①; 杨义先①; 钮心忻②