通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

郑雅菲,卫宏儒.分组密码TWIS的三子集中间相遇攻击[J].通信学报,2014,(6):180~184

分组密码TWIS的三子集中间相遇攻击

3-subset meet-in-the-middle attack on block cipher TWIS

投稿时间： 2013-03-05

DOI：10.3969/j.issn.1000-436x.2014.6.023

中文关键词：分组密码 TWIS 中间相遇攻击 复杂度

英文关键词:block cipher TWIS meet-in-the-middle attack complexity

基金项目:国家自然科学基金资助项目（61272476）；内蒙古自治区科技创新引导奖励资金基金资助项目（2012）

作者	单位
郑雅菲，卫宏儒	北京科技大学 数理学院，北京 100083

中文摘要:

对轻量级分组密码TWIS的安全性做进一步分析，将三子集中间相遇攻击应用于忽略后期白化过程的10轮TWIS。基于TWIS密钥生成策略中存在的缺陷，即其实际密钥长度仅为62 bit且初始密钥混淆速度慢，攻击恢复10轮TWIS全部62 bit密钥的计算复杂度为245，数据复杂度达到最低，仅为一个已知明密文对。分析结果表明TWIS在三子集中间相遇攻击下是不安全的。

英文摘要:

To do further analysis of the security of lightweight block cipher TWIS, 3-subset meet-in-the-middle attack was applied to 10-round TWIS without the final whitening. Based on the weakness in the key schedule of TWIS，its actual key size was only 62-bit and the confusion speed of the initial key was rather slow, the time complexity to recover the whole 62-bit key of 10-round TWIS was 245, and the data complexity was low enough with only one known plaintext-ciphertext pair. The result shows that block cipher TWIS is not secure under 3-subset meet-in-the-middle attack.

查看全文 查看/发表评论 下载PDF阅读器

关闭