



詹英杰,丁 林,关 杰.基于E0算法的猜测决定攻击[J].通信学报,2012,(11):185~190

基于E0算法的猜测决定攻击

DOI:

中文关键词:

英文关键词:

基金项目:

作者

单位

[詹英杰](#)

[丁 林](#)

[关 杰](#)

摘要点击次数: **386**

全文下载次数: **191**

中文摘要:

对短距离无线蓝牙技术中使用的E0序列密码算法进行了猜测决定攻击,攻击中利用线性逼近的方法做出了一个巧妙的攻击假设,降低了候选状态的数量,攻击的计算复杂度为 $O(2^{76})$,需要约988bit密钥流,属于短密钥流攻击。相对于长密钥流攻击,短密钥流攻击所需的密钥流。与目前已有的针对E0的短密钥流攻击相比,所提出猜测决定的攻击结果是最好的。

英文摘要:

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

关闭

版权所有:《通信学报》

地址:北京市丰台区成寿寺路11号邮电出版大厦8层 电话:010-81055478, 81055479
81055480, 81055482 电子邮件: xuebao@ptpress.com.cn

技术支持:北京勤云科技发展有限公司