

古春生. 破解HFEM公钥密码方案[J]. 通信学报, 2013, (3): 85~89

破解HFEM公钥密码方案

DOI:

中文关键词:

英文关键词:

基金项目:

作者

单位

[古春生](#)

摘要点击次数: 627

全文下载次数: 389

中文摘要:

为设计后量子公钥密码, 赵永哲等人提出了一种基于BMQ问题新的公钥方案。利用有限域上遍历矩阵的性质, 从该方案公钥能够直接求出其等价私钥, 从而破解了该HFEM公钥密码方案。

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