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

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

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：