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

赵永哲,赵 博,裴士辉,姜占华.HFEM公钥密码方案的设计与实现[J].通信学报,2011,(6):24~31

HFEM公钥密码方案的设计与实现

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
赵永哲	
赵 博	
裴士辉	
姜占华	

中文摘要：

基于BMQ问题的困难性，以及有限域上的矩阵与向量之间的关系，提出了一种新的公钥密码方案，即隐藏域上遍历矩阵的公钥密码。给出了有关矩阵集合的约束条件以及利用遍历矩阵来构造满足条件之矩阵集合的方法。与已有MPKC方案相比，HFEM具有陷门设计新颖、算法简单、不涉及任何乘幂及复杂运算、加/解密算法效率相当、中心映射难以抽象、密钥/明文/密文空间大等特点。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭