电子与信息学报 1993 15 (2): 208-211 ISSN: 1009-5896 CN: 11-4494/TN

研究简报

用BCH等线性分组码构造McEliece纠错码公钥密码体制

李元兴

北京邮电学院信息工程系 北京 100088

收稿日期 1991-10-19 修回日期 1992-3-6 网络版发布日期 2009-8-25 接受日期

摘要
McEliece公钥密码体制是用线性纠错码中的一种特殊码类Goppa码构造的。本文则表明采用BCH码或RS码等线性分组码也可构造安全的McEliece公钥密码体制。

关键词 Cryptology McEliece s public-key Cryptosystem Error-correcting codes

分类号

扩展功能
本文信息
Supporting info
PDF(772KB)
[HTML全文](0KB)
参考文献[PDF]
参考文献
服务与反馈
把本文推荐给朋友
加入我的书架
加入引用管理器
复制索引
Email Alert
文章反馈
浏览反馈信息
相关信息
本刊中 包含“Cryptology”的 相关文章
本文作者相关文章
· 李元兴

USING BCH OR OTHER LINEAR BLOCK CODES TO CONSTRUCT MCELIECE S PUBLIC KEY CRYPTOSYSTEM

Li Yuanxing

Beijing University of Posts and Telecommunications Beijing 100088

Abstract
McEliece's public-key cryptosystem was constructed with the Goppa codes. This paper shows other linear block codes, i.e., BCH codes or RS codes, can also be used to construct secure McEliece s cryptosystem.

Key words Cryptology McEliece s public-key Cryptosystem Error-correcting codes

DOI:

通讯作者

作者个人主页 李元兴