计算机工程与应用 2008 44 (27): 31-32 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

基于ECC和HFE的纠错密码构造

杨 敏[1], 孟庆树[2], 张焕国[2]

1.武汉大学 国际软件学院，武汉 430079
2.武汉大学 计算机学院，武汉 430079

收稿日期 2008-6-12 修回日期 2008-7-30 网络版发布日期 2008-9-18 接受日期

摘要 纠错密码是一种利用纠错码体制来实现纠错和加密双重功能的一种密码体制。大部分已知的纠错密码从变换的角度看是一种对明文的线性变换。从密码分析的角度看，由于不具有非线性变换，密码的混淆能力不强，容易被攻击。利用纠错码 （Error-Correction Code，ECC） 改造基本HFE （Hidden Field Equations） 密码算法，所得的新密码算法具有纠错和加密功能，而且因其具有概率密码特性以及建立在MQ困难问题之上，具有很高的安全强度。

关键词 纠错码 HFE密码 纠错密码

分类号

Construction of error-correction cryptosystem based on ECC and HFE

YANG Min[1],MENG Qing-shu[2],ZHANG Huan-guo[2]

1.International School of Software，Wuhan University，Wuhan 430079，China
2.School of Computer，Wuhan University，Wuhan 430079，China

Abstract

Error-correction cryptosystem can be used to correct transmission errors and encrypt messages.Most of the proposed such systems are based on linear transformation.They are weak in resisting cryptanalysis because of the lack of nonlinear transformation in systems.The authors modify the basic Hidden Field Equations（HFE） into a new error-correction cryptosystem by substituting the generate matrix of an Error-Correction Code（ECC） for the last linear transformation of the basic HFE.The new cryptosystem can be used to correct transmission errors and encrypt messages with high security.

Key words Error-Correction Code（ECC） Hidden Field Equations（HFE） cipher error-correction cryptosystem

DOI: 10.3778/j.issn.1002-8331.2008.27.010

通讯作者 杨 敏 yangm75@hotmail.com