通信学报
Journal on Communications
主管单位：中国科学技
主办单位：中国通信学

乔帅庭1,2,李益发1,韩文报1,2.新扩展多变量公钥密码方案[J].通信学报,2014,(4):148~154

新扩展多变量公钥密码方案

Novel extended multivariate public key cryptosystem

投稿时间： 2012-12-29

DOI：10.3969/j.issn.1000-436x.2014.4.017

中文关键词：温顺变换 新的扩展方案 线性攻击 差分攻击 代数攻击

英文关键词:tame transformation the novel extended cryptosystem linearization attack differential attack algebraic attack

基金项目:国家高技术研究发展计划(“863”计划)基金资助项目(2009AA012201)；数学工程与先进计算国家重点实验开放课题基金资助项目(2013A03, 2013A10)

作者	单位
乔帅庭1,2，李益发1，韩文报1,2	1.信息工程大学 四院，河南 郑州 450002；2. 数学工程与先进计算国家重点实验室，江苏 无锡 214125

中文摘要:

为了有效地抵抗线性攻击和差分攻击，基于“温顺变换”思想构造了一种非线性可逆变换，将此变换与Matsumoto-Imai (MI)方案结合，提出了一种新的扩展多变量公钥密码方案着，在扩展方案的基础上，设计出了新的多变量公钥加密方案和签名方案。分析结果表明：该方案继承了MI方案计算高效的优点，并且能够抵抗线性攻击、差分攻击和代数攻击。

英文摘要:

To resist linearization attack and differential attack effectively, a nonlinear invertible transformation based on “tame transformation” was constructed. Incorporated with the Matsumoto-Ima scheme, a novel extended multivariate public key cryptosystem was proposed. Then, according to the proposed scheme, two practical applications including an encryption scheme and a signature scheme were designed respectively. Analysis results demonstrate that the extended cryptosystem inherits the merit of MI, i.e. efficient computation. Meanwhile, the novel extended scheme can al resist linearization attack, differential attack and algebraic attack.