最大跳跃数及基于数学理论的密码体制

关 键 词：跳跃数 密码体制 数学理论 签名算法 密钥 指纹

所属年份：2004	成果类型：基础理论
所处阶段：	成果体现形式：
知识产权形式：	项目合作方式：
成果完成单位：海南师范大学	

成果摘要：

完全否定了SCI核心期刊“Linear Algebra and its Appl.”主编Brualdi等人提出的关于跳跃数的一个重要猜想；研究了一类多重采样序列的极小多项式；指出了国际电子学核心期刊“Elec. Lett.”上的一篇论文中提出的一种签名加密体制的错误，并提出了三种改进的签名加密算法；提出了若干基于椭圆曲线的(盲)数字签名新算法及签名算法的一般方程；提出了两种比二元法及Müller算法快得多的有理点标量乘的新算法；提出了一种比二元法要快近四倍的除子标量乘新算法；借助Riemann-Roch 定理， 证明了任何一个度数为零的除子唯一等价于一个约化除子，并得到了任何一对多项式唯一确定一个除子的判定条件；研究了用DNA计算来攻击AES算法的可能性；首次提出了用指纹来产生密钥的椭圆曲线签名算法。

成果完成人：游林;王天明

完整信息

推荐成果

· 空间飞行器SPACEWIRE高速数据... 04-23
· Adhoc网络中的QoS保证(Wirel... 04-23
· 基于正交多载波传输的高速无... 04-23
· 光因特网体系结构与管理技术 04-23
· 一种光因特网中不同网络结构... 04-23
· 40Gbit/s DWDM软件仿真系统 04-23
· 移动互联网服务质量控制工程... 04-23
· 数字图像处理系统研究 04-23
· IPv6核心路由器 04-23

行业资讯

QH3792S腔式双工器
数字微波传输关键设备研制
2.4G无线接入系统设备
VSAT卫星通信系统
码分多址卫星数据通信地球站
WSD-1卫星数据通信单收站
1560点对多点微波通信系统
M2000 6GHz 155Mb/s SDH微波...
2×155Mbit/s SDH微波通信系统
M1000型2×34Mb/s数字微波接...

成果交流