北京大学学报

（自然科学版）

第 46 卷 第 5 期　　总 第 241 期

目　次

研究论文

用有效可计算自同态来计算 Tate 配对（英文） …… 胡志　周正华　徐茂智 (685)

关于 Trivium 算法设计的研究（英文） …… 田芸　陈恭亮　李建华 (691)

含 3 阶点椭圆曲线的同构类 …… 吴宏锋　冯荣权　王子龙 (699)

具有最大代数免疫阶的布尔函数的新构造 …… 曹浩　魏仕民　卓泽鹏 等 (704)

基于齐次线性递归的可验证多秘密共享方案 …… 陈恭奎　于佳　程相国 等 (709)

l-序列的采样元素分布及 k-错线性复杂度 …… 谭林　戚文峰 (715)

一种抗 DoS 攻击的密钥交换协议 …… 程庆丰　魏福山　马传贵 (720)

具有最大代数免疫度的偶数元布尔函数的计数 …… 熊晓雯　付绍静　屈龙江 (725)

对 5 轮 IDEA 算法的两种攻击 …… 鲁林真　陈少真 (731)

二元域上 Edwards 型椭圆曲线的配对计算 …… 徐茂智　喻洪辉　唐春明 等 (736)

实现 $k=18$ 的 Brezing-Weng 曲线的最优配对 …… 唐春明　亓延峰　徐茂智 (743)

η_T 配对的配对域 F_{36m} 上的最优乘法算法 …… 亓延峰　贾大江　唐春明 等 (749)

轻量级分组密码 KeeLoq 的故障攻击 …… 游建雄　李瑞林　李超 (756)

基于细粒度新鲜性的密码协议分析 …… 程正杰　陈克非　来学嘉 (763)

XTrim：一种基于 XML Schema 和微型数据块优化的 XML 压缩方法 …… 仇睿恒　汤帜　胡薇 等 (771)

铝-金属玻璃-铝复合板的抗破甲性能研究 …… 刘伟东　冯荣欣　刘凯欣 等 (779)

2008 年广东及周边海域暴雨期间强对流活动时空分布特征 …… 朱兴明　郑永光　郭丽娜 等 (784)

我国副热带地区夏季深对流活动气候分布特征 …… 郑永光　王颖　寿绍文 (793)

乌拉特中旗二叠纪 I 型花岗岩类地球化学特征及构造意义 …… 罗红玲　吴泰然　赵磊 (805)

环境减灾卫星高光谱数据大气校正模型及验证 …… 杨贵军　黄文江　刘三超 等 (821)

珠江三角洲可吸入颗粒物污染急性健康效应的经济损失评价 …… 刘晓云　谢鹏　刘兆荣 等 (829)

基于 MODIS 数据的东北亚森林时序变化分析 …… 付安民　孙国清　迟志峰 等 (835)

科技论坛

我国应对大震巨灾应急救援装备的技术需求研究 …… 胡卫建　尚红　司洪波　等 (844)

北京大学科研国际合作的成效与发展对策 …… 郑如青　张琰 (851)

研究简报

含有非理想完整约束的非完整系统的打击问题 …… 姚文莉 (855)

孔雀羽毛的纳米结构生色机理及其仿生结构器件的应用初探 …… 龚爽　卢永凯　王红凤　等 (859)

2010 年 9 月 20 日出版　　本期责任编辑　尉立肖　李亚文　张树宇

ACTA SCIENTIARUM NATURALIUM UNIVERSITATIS PEKINENSIS

Vol. 46 No. 5 Total No. 241

CONTENTS

Articles

A Note on Computing the Tate Pairing with Effciently Computable Endomorphisms ..... HU Zhi, ZHOU Zhenghua, XU Maozhi (685)
On the Design of Trivium ..... TIAN Yun, CHEN Gongliang, LI Jianhua (691)
Isomorphism Classes of Elliptic Curves with 3-Torsion Point ..... WU Hongfeng, FENG Rongquan, WANG Zilong (699)
New Construction of Boolean Function with Maximum Algebraic Immunity ..... CAO Hao, WEI Shimin, ZHUO Zepeng, et al (704)
Verifiable Multi-secret Sharing Scheme Based on Homogeneous Linear Recursion ..... CHEN Yangkui, YU Jia, CHENG Xiangguo, et al (709)
Element Distribution of Decimations and k-Error Linear Complxity of l-Sequences ..... TAN Lin, QI Wenfeng (715)
A New Authenticated Key Exchange Protocol with DoS Resilience ..... CHENG Qingfeng, WEI Fushan, MA Chuangui (720)
On the Number of Even-Variable Boolean Functions with Maximum Algebraic Immunity ..... XIONG Xiaowen, FU Shaojing, QU Longjiang (725)
Two Attacks on 5-Round IDEA ..... LU Linzhen, CHEN Shaozhen (731)
The Pairing Computation on Binary Edwards Curves ..... XU Maozhi, YU Honghui, TANG Chunming, et al (736)
Implementing Optimal Pairings over Brezing-Weng Elliptic Curves with $k=18$ ..... TANG Chunming, QI Yanfeng, XU Maozhi (743)
Optimal Multiplication Algorithm for the η_T Pairing over $F_{3^{6m}}$ ..... QI Yanfeng, JIA Dajiang, TANG Chunming, et al (749)
Fault Attack on Lightweight Block Cipher KeeLoq ..... YOU Jianxiong, LI Ruilin, LI Chao (756)
Security Analysis of Cryptographic Protocols Based on Fine-Grained Freshness ..... CHENG Zhengjie, CHEN Kefei, LAI Xuejia (763)
XTrim: An XML Compressor Based on XML Schema and Tiny Data Block Optimization ..... QIU Ruiheng, TANG Zhi, HU Wei, et al (771)
Research on the Property of Aluminum-Metallic Glass-Aluminum Sandwich Panelagainst Shaped Charge Jet Penetration ..... LIU Weidong, FENG Rongxin, LIU Kaixin, et al (779)
Distribution and Spatiotemporal Variations of Deep Convection over Guangdong and Adjacent Areas during Heavy Rainfall Period of 2008 ..... ZHU Xingming, ZHENG Yongguang, GUO Lina, et al (784)
Climatology of Deep Convection over the Subtropics of China during Summer ..... ZHENG Yongguang, WANG Ying, SHOU Shaowen (793)
Geochemistry and Tectonic Implications of the Permian I-Type Granitoids from Urad Zhongqi, Inner Monglia ..... LUO Hongling, WU Tairan, ZHAO Lei (805)
Research on Modeling and Validating of Atmospheric Correction for HJ-1A Hyperspectral Imager Data ..... YANG Guijun, HUANG Wenjiang, LIU Sanchao, et al (821)
Economic Assessment of Acute Health Impact Due to Inhalable Particulate Air Pollution in the Pearl River Delta ..... LIU Xiaoyun, XIE peng, LIU Zhaorong, et al (829)
Forest Changes Detection in the Northeastern Asia Using MODIS Imagery ..... FU Anmin, SUN Guoqing, GUO Zhifeng, et al (835)

Forum

The Demand Study of the Technological Equipments for Disposal to the Emergency Rescue of a Great Earthquake in China ..... HU Weijian, SHANG Hong, SI Hongbo, et al (844)
Effects and Strategy of the International Scientific Research at Peking University ..... ZHENG Ruqing, ZHANG Yan (851)

Reports

Impact on Non-holonomic Systems with Nonideal Holonomic Constraints ..... YAO Wenli (855)
Study on the Relationship between Nanostructure and Color of Peacock Feather and Its Biomimetic Application ..... GONG Yan, LU Yongkai, WANG Hongfeng, et al (859)

Published on Sept. 20, 2010