

目 次

可信计算

无线环境下的可信网络连接协议	马 卓, 马建峰, 杨 超, 杨 力(577)
一种混合交叉认证的平台兼容性方案	马朝斌, 黄宁玉, 张 兴(582)
可信计算中的可信度量机制	张立强, 张焕国, 张 帆(586)
基于管道的 TCB 扩展模型	廖建华, 赵 勇, 沈昌祥(592)
可信网络匿名连接方案	庄俊玺, 公 备(597)
基于 I-MOMSDH 假设的短群签名 DAA 方案	周雁舟, 张焕国, 李立新, 宋 扬(601)
虚拟可信平台层次化安全体系结构设计	沈晴霓, 杜 虹, 卿斯汉(605)
基于角色的软件可信评估技术	袁 霖, 王怀民, 尹 刚, 史殿刁, 米海波(611)
基于参数依赖关系检查的测试用例空间约简方法	陈亚莎, 叶 清, 廖建华(616)
电子数据取证的可信固定方法	孙国梓, 耿伟明, 陈丹伟, 林清秀(621)

密码学

多变量代数理论及其在密码学中的应用	王后珍, 张焕国, 管海明, 伍前红(627)
三次单项布尔函数的二阶非线性度下界	李雪莲, 胡予濮, 高军涛, 方益奇(635)
基于 GPU 的 MD6 算法快速实现	李立新, 叶 剑, 余 洋(640)
广义圆锥曲线的多方签名的安全分析与设计	丁 丽, 周 渊, 钱海峰(646)
serpent 加密算法的差分代数攻击	胡志华(651)
标准模型下基于身份的具有部分消息恢复功能的签名方案	刘振华, 张襄松, 田绪安, 胡予濮(654)
时间和功耗双随机化的 AES 抗差分能量攻击设计	严迎建, 刘 凯, 任 方, 朱巍巍(659)

网络安全

基于项重写的安全电子交易形式化模型	陈 晨, 刘 楠, 陈卫红, 祝跃飞(664)
-------------------------	-------------------------

基于字符串相似性聚类的网络短文本舆情热点发现技术 杨 震, 段立娟, 赖英旭(669)

基于兴趣分类、信任和安全等级的 P2P 访问控制 刘益和(674)

基于选择机制的实体间最信任路径发现方法 周国强, 曾庆凯(679)

基于身份的无密钥托管的变色龙 hash 函数和签名 詹 阳, 田海博, 陈晓峰, 王育民(685)

基于 Fisher 信息的最优隐写方法 孙怡峰, 刘粉林, 王 飞, 曾 颖(689)

系统安全

用于公文流转的强制访问控制模型 范艳芳, 韩 臻, 赵 勇, 耿秀华(694)

全程一致访问控制体系研究 韩培胜, 赵 勇, 李 瑜(698)

可保护隐私的外包数据库查询验证技术 王晓明, 袁多宝(703)

一种基于 PEPA 流近似方法的动态自省模型 吕宏武, 王慧强, 马春光, 林相君, 赵 倩(710)

基于关键分支的不可行路径确定方法 潘丽丽, 邹北骥, 王天镔, 陈 浩(716)

责任编辑: 苗艳玲 张士瑛 刘 潇 张 蕾 终审、终校: 杨小玲

本期基本参数: CN11-2286/T * 1974 * m * A4 * 144 * zh + en * P * ¥20.00 * 1 000 * 28 * 2010-05

**JOURNAL OF BEIJING
UNIVERSITY OF TECHNOLOGY**

Vol. 36

May 2010

No. 5

CONTENTS

Trusted Computing

- Trusted Network Connect Protocol for Wireless Environment
..... MA Zhuo, MA Jian-feng, YANG Chao, YANG Li(577)
- A Mixed Cross-authentication Scheme for Trusted Platform Compatibility
..... MA Chao-bin, HUANG Ning-yu, ZHANG Xing(582)
- The Trust Measurement Scheme in Trusted Computing
..... ZHANG Li-qiang, ZHANG Huan-guo, ZHANG Fan(586)
- Channel-Based TCB Extension Model
..... LIAO Jian-hua, ZHAO Yong, SHEN Chang-xiang(592)
- The Connection Anonymous Scheme of Trusted Network ZHUANG Jun-xi, GONG Bei(597)
- A Short Group Signature DAA Scheme Based on l-Modified One More Strong Diffie-Hellman Problem Assumption
..... ZHOU Yan-zhou, ZHANG Huan-guo, LI Li-xin, SONG Yang(601)
- Hierarchal Security Architecture of Virtualized Trusted Platform
..... SHEN Qing-ni, DU Hong, QING Si-han(605)
- Trustworthy Evaluation Technology of Software Based on Roles
..... YUAN Lin, WANG Huai-min, YIN Gang, SHI Dian-xi, MI Hai-bo(611)
- Dynamic Arguments Dependence Analysis Technique for Test-suite Deduction
..... CHEN Ya-sha, YE Qing, LIAO Jian-hua(616)
- One Trusted Fix Method of Digital Data Forensics
..... SUN Guo-zi, GENG Wei-ming, CHEN Dan-wei, LIN Qing-xiu(621)

Cryptography

- Multivariable Algebra Theory and Its Application in Cryptography
..... WANG Hou-zhen, ZHANG Huan-guo, GUAN Hai-ming, WU Qian-hong(627)
- The Nonlinearity Lower Bounds on the Second Order of Cubic Monomial Boolean Functions
..... LI Xue-lian, HU Yu-pu, GAO Jun-tao, FANG Yi-qi(635)
- The Fast Implementation of MD6 on GPU LI Li-xin, YE Jian, YU Yang(640)
- Security Analysis and Improvement of Digital Multi-signature on the Generalized Conic Curve
..... DING Li, ZHOU Yuan, QIAN Hai-feng(646)
- Differential Algebraic Attack of Serpent HU Zhi-hua(651)
- Identity-based Signature Scheme with Partial Message Recovery in the Standard Model
..... LIU Zhen-hua, ZHANG Xiang-song, TIAN Xu-an, HU Yu-pu(654)

Design of AES on Time Randomization and Power Randomization Based Differential Power

Analysis Resist Countermeasure YAN Ying-jian, LIU Kai, REN Fang, ZHU Wei-wei(659)

Network Security

A Formal Model of Secure Electronic Transaction Based on Term Rewriting

..... CHEN Chen, LIU Nan, CHEN Wei-hong, ZHU Yue-fei(664)

Online Public Opinion Hotspot Detection and Analysis Based on Short Text Clustering Using

String Distance YANG Zhen, DUAN Li-juan, LAI Ying-xu(669)

P2P Access Control Research Based on Interest Classification, Trust and Security Grade

..... LIU Yi-he(674)

An Algorithm for Finding the Most Trusted Path Between Entities Based on Selected Mechanism

..... ZHOU Guo-qiang, ZENG Qing-kai(679)

ID-based Chameleon Hash Scheme and Signature Without Key Escrow

..... ZHAN Yang, TIAN Hai-bo, CHEN Xiao-feng, WANG Yu-min(685)

Optimal Steganography Based on Fisher Information

..... SUN Yi-feng, LIU Fen-lin, WANG Fei, ZENG Ying(689)

System Security

The Mandatory Access Control Model for Document Flow

..... FAN Yan-fang, HAN Zhen, ZHAO Yong, GENG Xiu-hua(694)

Process-Consistent Access Control System HAN Pei-sheng, ZHAO Yong, LI Yu(698)

Query Verification Technique Preserving Privacy for Outsourced Databases

..... WANG Xiao-ming, YUAN Duo-bao(703)

A Dynamic Self-reflection Model Based on Fluid Flow Approximation of PEPA

..... LÚ Hong-wu, WANG Hui-qiang, MA Chun-guang, LIN Xiang-jun, ZHAO Qian(710)

Analysis of the Infeasible Path Based on Key Branch

..... PAN Li-li, ZOU Bei-ji, WANG Tian-e, CHEN Hao(716)

Responsible Editors: MIAO Yan-ling, ZHANG Shi-ying, LIU Xiao, ZHANG Lei

Final Reviewer and Final Reviser: YANG Xiao-ling