

原书缺封面

通 信 学 报

第 35 卷第 7 期 2014 年 7 月

目 次

论文 I：密码算法与安全协议

基于高阶差分的 type-1 广义 Feistel-SP 结构与 Feistel-SPSP 结构比较研究	董 乐, 杜 蛟, 吴文玲 (1)
基于信誉的快速无可信第三方匿名撤销方案	奚 璩, 冯登国 (10)
指定测试者的基于身份可搜索加密方案	王少辉, 韩志杰, 肖 甫, 王汝传 (22)
可证安全的高效可托管公钥加密方案	刘文浩, 王圣宝, 曹珍富, 韩立东 (33)
前向安全的密文策略基于属性加密方案	魏江宏, 刘文芬, 胡学先 (38)

论文 II

面向 XML 关键字查询的高效 RKN 求解策略	陈子阳, 王 璿, 汤 显 (46)
递归 SOQPSK-TG 信号的两状态判决反馈解调算法	孙锦华, 韩会梅 (56)
动态时变衰落信道下的频谱感知算法	孙梦巍, 赵 龙, 许巧春, 李 斌, 赵成林 (63)
有损网络下的高性能传输控制协议研究	潘 凯, 李 挥 (70)
图像分块压缩感知中的自适应测量率设定方法	李 然, 干宗良, 崔子冠, 武明虎, 朱秀昌 (77)
基于对数谱射频指纹识别的 RFID 系统信息监控方法	袁红林, 包志华, 严 燕 (86)
可信计算环境下的 WLAN Mesh 安全关联方案	肖跃雷, 王育民, 庞辽军, 谭示崇 (94)
高效可证明安全的基于属性的在线/离线加密机制	马海英, 曾国荪, 王占君, 王 伟 (104)
干扰对消系统的非零带宽性能与延时匹配	蒋云昊, 陈炜峰, 钟水明, 贾红云, 曹永娟, 毛 鹏 (113)
基于节点识别的慢任务调度算法	崔云飞, 李新明, 李 艺, 刘 东 (122)
基于布尔集线器的线速多播自路由交换结构	尘福兴, 李 挥, 崔 凯, 张 博 (129)
面向云计算环境的动态公平性度量方法	卢 笛, 马建峰, 王一川, 习 宁, 孟宪佳 (140)
基于叠加训练的非合作多用户/MIMO 信道估计	何纯全, 窦高奇, 高 俊, 黄高明 (151)
MIBS 算法的积分攻击	潘志舒, 郭建胜, 曹进克, 罗 伟 (157)
未知网络应用流量的自动提取方法	王变琴, 余顺争 (164)
引入梯度导引似 p 范数约束的稀疏信道估计算法	伍飞云, 周跃海, 童 峰 (172)

综 述

主动网络流水印技术研究进展	郭晓军, 程 光, 朱琛刚, TRUONG Dinh-Tu, 周爱平 (178)
---------------	--

学 术 通 信

抗特洛伊木马攻击的量子密钥多播通信协议	马鸿洋, 范兴奎 (193)
基于融合策略的单幅图像去雾算法	郭 璠, 唐 璘, 蔡自兴 (199)
高速铁路无线通信中基于正交空时码的格型正交重构算法	罗万团, 方旭明, 程 梦 (208)
捕获效应下 RFID 标签的 CATPE 防冲突协议	杨 茜, 吴海锋, 曾 玉 (215)

Contents

Papers

- Higher-order differences based research on comparison between type-1 generalized Feistel-SP network and Feistel-SPSP network *DONG Le, DU Jiao, WU Wen-ling* (1)
- Efficient anonymous reputation-based revocation without TTP *XI Li, FENG Deng-guo* (10)
- Identity-based searchable encryption scheme with a designated tester *WANG Shao-hui, HAN Zhi-jie, XIAO Fu, WANG Ru-chuan* (22)
- Provably secure and efficient escrowable public key encryption schemes *LIU Wen-hao, WANG Sheng-bao, CAO Zhen-fu, HAN Li-dong* (33)
- Forward-secure ciphertext-policy attribute-based encryption scheme *WEI Jiang-hong, LIU Wen-fen, HU Xue-xian* (38)
- Efficiently computing RKN for keyword queries on XML data *CHEN Zi-yang, WANG Xuan, TANG Xian* (46)
- Decision feedback demodulation algorithm for recursive SOQPSK-TG signal *SUN Jin-hua, HAN Hui-mei* (56)
- New spectrum sensing method under time-variant flat fading channels *SUN Meng-wei, ZHAO Long, XU Qiao-chun, LI Bin, ZHAO Cheng-lin* (63)
- Research on the high-performance transmission control protocol under lossy networks *PAN Kai, LI Hui* (70)
- Adaptive measurement rate setting method in block compressed sensing of images *LI Ran, GAN Zhong-liang, CUI Zi-guan, WU Ming-hu, ZHU Xiu-chang* (77)
- Information monitor method of RFID system based on logarithm spectrum RF fingerprint identification *YUAN Hong-lin, BAO Zhi-hua, YAN Yan* (86)
- WLAN Mesh security association scheme in trusted computing environment *XIAO Yue-lei, WANG Yu-min, PANG Liao-jun, TAN Shi-chong* (94)
- Efficient and provably secure attribute-based online/offline encryption schemes *MA Hai-ying, ZENG Guo-sun, WANG Zhan-jun, WANG Wei* (104)
- Nonzero bandwidth performance and time delay matching of interference cancellation system *JIANG Yun-hao, CHEN Wei-feng, ZHONG Shui-ming, JIA Hong-yun, CAO Yong-juan, MAO Peng* (113)
- Slow task scheduling algorithm based on node identification *CUI Yun-fei, LI Xin-ming, LI Yi, LIU Dong* (122)
- Novel wire-speed multicast self-routing switch fabric based on Boolean concentrator *CHEN Fu-xing, LI Hui, CUI Kai, ZHANG Bo* (129)
- Dynamic fairness evaluation framework for cloud computing *LU Di, MA Jian-feng, WANG Yi-chuan, XI Ning, MENG Xian-jia* (140)
- Uncoordinated multiuser/MIMO channel estimation using superimposed training *HE Chun-quan, DOU Gao-qi, GAO Jun, HUANG Gao-ming* (151)
- Integral attack on MIBS block cipher *PAN Zhi-shu, GUO Jian-sheng, CAO Jin-ke, LUO Wei* (157)
- Automatic extraction for the traffic of unknown network applications *WANG Bian-qin, YU Shun-zheng* (164)
- Estimation algorithm for sparse channels with gradient guided p -norm like constraints *WU Fei-yun, ZHOU Yue-hai, TONG Feng* (172)

Comprehensive Reviser

- Progress in research on active network flow watermark *GUO Xiao-jun, CHENG Guang, ZHU Chen-gang, TRUONG Dinh-Tu, ZHOU Ai-ping* (178)

Correspondences

- Multicast communication protocol based on quantum key distribution against trojan horse attacking *MA Hong-yang, FAN Xing-kui* (193)
- Single image defogging based on fusion strategy *GUO Fan, TANG Jin, CAI Zi-xing* (199)
- Trellis orthogonal reconstruction algorithm based on orthogonal space-time block code for wireless communication system in high-speed railway *LUO Wan-tuan, FANG Xu-ming, CHENG Meng* (208)
- CATPE protocol with capture effect for RFID tag anti-collision *YANG Xi, WU Hai-feng, ZENG Yu* (215)

原书缺封底