



• ISSN 0254-4166

• CODEN JIXUD

计算机学报

CHINESE JOURNAL OF COMPUTERS

第35卷 Vol.35

第9期 No.9



2012.9

• 中国计算机学会 中国科学院计算技术研究所 主办

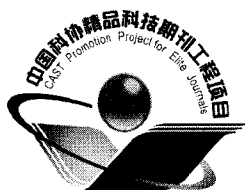
• 科学出版社 出版

CHINESE JOURNAL OF COMPUTERS

Vol.35 No.9 September 2012

CONTENTS

- Graceful Degradation in TSS-BQS Systems WANG Wen-Tao et al. (1793)
- Black-Box Secret Sharing Scheme for Disjunctive Multi-Level Access Structure
..... CHEN Qi et al. (1804)
- A New Space Efficient Secret Sharing Scheme without a Secure Channel ... LIU Yan-Hong et al. (1816)
- An Efficient Gateway-Oriented Password-Based Authenticated Key Exchange Protocol with Strong
User Anonymity WEI Fu-Shan et al. (1823)
- A Framework for Gateway-Oriented Password-Authenticated Key Exchange in the Standard Model
..... WEI Fu-Shan et al. (1833)
- An Attribute-Based Encryption Scheme for Traitor Tracing and Revocation Together
..... MA Hai-Ying et al. (1845)
- Master-Key Leakage-Resilient and Continue Leakage-Resilient Functional Encryption in Dual
Affine Spaces ZHANG Ming-Wu et al. (1856)
- Construct Hash Function from Plaintext to C_{34} Curves YU Wei et al. (1868)
- Identity-Based Ring Signature Scheme with Constant Size Signatures in the Standard Model
..... GE Ai-Jun et al. (1874)
- Certificateless Multi-receiver Signcryption Scheme Based on Multivariate Public Key Cryptography
..... LI Hui-Xian et al. (1881)
- Linear Cryptanalysis of Simplified Trivium SUN Wen-Long et al. (1890)
- Probabilistic Integral Cryptanalysis LI Xiao-Qian et al. (1897)
- Another Look at the Integral Attack by the Higher-Order Differential Attack DONG Le et al. (1906)
- Differential Fault Analysis on Piccolo ZHAO Guang-Yao et al. (1918)
- Password Recovery Attack to Authentication Post Office Protocol LIU Fan-Bao et al. (1927)
- A Security Threats Identification and Analysis Method Based on Attack Graph WU Di et al. (1938)
- Steganalysis Based on Clustering via KFD Index Against Highly Undetectable JPEG Steganography
..... HUANG Wei et al. (1951)
- A Novel Quantization Watermarking Scheme Using Random Normalized Correlation Modulation ...
..... ZHU Xin-Shan et al. (1959)
- Analyzing and Evaluating the Robustness of Natural Language Watermarking HE Lu et al. (1971)



计算机学报

(JISUANJI XUEBAO)

第 35 卷 第 9 期 2012 年 9 月

目 次

《信息安全算法与协议》专辑 前言 冯登国 (i)

秘密共享与认证密钥交换协议

TSS-BQS 系统的 Graceful Degradation 机制 王文韬 林璟铨 荆继武 罗 勃 (1793)
实现分离多级存取结构的黑盒密钥共享体制 陈 祺 裴定一 赵淦森 纪求华 (1804)
不需要安全信道的空间有效秘密分享方案 刘艳红 张福泰 (1816)
具有强匿名性的网关口令认证密钥交换协议 魏福山 马传贵 (1823)
标准模型下网关口令认证密钥交换协议的通用框架 魏福山 张振峰 马传贵 (1833)

密码算法设计与数字签名

可追踪并撤销叛徒的属性基加密方案 马海英 曾国荪 (1845)
抗主密钥泄露和连续泄露的双态仿射函数加密 张明武 杨 波 TAKAGI Tsuyoshi (1856)
构造从字符串到 C_{31} 曲线的散列函数 于 伟 王鲲鹏 李 宝 田 松 (1868)
标准模型下固定长度的基于身份环签名方案 葛爱军 马传贵 张振峰 陈少真 (1874)
基于多变量公钥密码体制的无证书多接收者签密体制 李慧贤 陈绪宝 庞辽军 王育民 (1881)

密码算法分析与安全威胁分析

针对简化版 Trivium 算法的线性分析 孙文龙 关 杰 刘建东 (1890)
概率积分密码分析 李晓千 吴文玲 李 宝 于晓丽 (1897)
高阶差分视角下的积分攻击 董 乐 吴文玲 吴 双 邹 剑 (1906)
Piccolo 算法的差分故障分析 赵光耀 李瑞林 孙 兵 李 超 (1918)
带认证邮局协议的密钥恢复攻击 刘凡保 谢 涛 冯登国 (1927)
一种基于攻击图的安全威胁识别和分析方法 吴 迪 连一峰 陈 恺 刘玉岭 (1938)

信息隐藏与数字水印

基于 KFD 指标聚类的高隐蔽性 JPEG 隐写分析 黄 炜 赵险峰 盛任农 (1951)
一种采用随机归一化相关系数调制的量化水印 朱新山 丁 杰 (1959)
自然语言水印鲁棒性分析与评估 何 路 桂小林 田 丰 武睿峰 房鼎益 (1971)