# 计 算 机 研 究 与 发 展

（Jisuanji Yanjiu Yu Fazhan）

第 53 卷 第 10 期 2016 年 10 月


## 目 次


**网络空间共享安全研究进展专题**

前 言 …… 曹珍富 徐秋亮 张玉清 董晓蕾 (2133)

**综 述**

大数据安全与隐私保护研究进展 …… 曹珍富 董晓蕾 周 俊 沈佳辰 宁建廷 巩俊卿 (2137)

基于云计算服务的安全多方计算 …… 蒋 瀚 徐秋亮 (2152)

HTML5 新特性安全研究综述 …… 张玉清 贾 岩 雷柯楠 吕少卿 乐洪舟 (2163)

口令安全研究进展 …… 王 平 汪 定 黄欣沂 (2173)

僵尸网络发展研究 …… 李 可 方滨兴 崔 翔 刘奇旭 (2189)

**密码安全**

去中心化且固定密文长度的基于属性加密方案 …… 肖思煜 葛爱军 马传贵 (2207)

一个 LWE 上的短公钥多位全同态加密方案 …… 陈智罡 宋新霞 赵秀凤 (2216)

针对 SM4 密码算法的多点联合能量分析攻击 …… 杜之波 吴 震 王 敏 饶金涛 (2224)

基于验证元的三方口令认证密钥交换协议 …… 杨晓燕 侯孟波 魏晓超 (2230)

具备强表达能力的选择密文安全高效属性基加密方案 …… 张 凯 魏立斐 李祥学 陈 洁 钱海峰 (2239)

**系统安全**

Android Settings 机制应用安全性分析与评估 …… 路晔绵 应凌云 苏璞睿 冯登国 靖二霞 谷雅聪 (2248)

基于敏感字符的 SQL 注入攻击防御方法 …… 张慧琳 丁 羽 张利华 段 镭 张 超 韦 韬 李冠成 韩心慧 (2262)

基于代码防泄漏的代码复用攻击防御技术 …… 王 烨 李清宝 曾光裕 陈志锋 (2277)

VDNS：一种跨平台的固件漏洞关联算法 …… 常 青 刘中金 王猛涛 陈 昱 石志强 孙利民 (2288)

Maldetect：基于 Dalvik 指令抽象的 Android 恶意代码检测系统 …… 陈铁明 杨益敏 陈 波 (2299)

**隐私保护**

基于 R-LWE 的密文域多比特可逆信息隐藏算法 …… 柯 彦 张敏情 苏婷婷 (2307)

面向车联网的多服务器架构的匿名双向认证与密钥协商协议 …… 谢 永 吴黎兵 张宇波 叶璐瑶 (2323)

基于层次树的动态群组隐私保护公开审计方案 …… 黄龙霞 张功萱 付安民 (2334)

基于加权贝叶斯网络的隐私数据发布方法 …… 王 良 王伟平 孟 丹 (2343)

一种遗传算法实现的图聚类匿名隐私保护方法 …… 姜火文 曾国荪 胡克坤 (2354)

**应用安全**

在线/离线密文策略属性基可搜索加密 …… 陈冬冬 曹珍富 董晓蕾 (2365)

TSNP：空间信息网中 PCL 安全高效的群组认证协议 …… 李学峰 张俊伟 马建峰 刘 海 (2376)

适合云存储的访问策略可更新多中心 CP-ABE 方案 …… 吴光强 (2393)

一种新的基于指纹与移动端协助的口令认证方法 …… 安 迪 杨 超 姜 奇 马建峰 (2400)

基于 DAA-A 的改进可授权电子现金系统 …… 柳 欣 张 波 (2412)

编者专栏 2014 年《计算机研究与发展》高被引论文 TOP10 …… (2430)

读者专栏 《计算机研究与发展》征订启事 …… (2162)

《信息安全研究》期刊简介 …… (2429)

《计算机研究与发展》编委会 …… (封底)



责任编辑：万数据荐