

国家信息中心主办

第4卷 第6期 2018年6月

Vol.4 No.6 June 2018

信息安全研究

Journal of Information Security Research



QK1823990

特别策划：网络强国系列

网络强国建设中的信息系统审计机制研究

区块链与量子计算

论虚拟货币金融犯罪的监管

密钥泄露下 Even-Mansour 密码的滑动攻击

ISSN 2096-1057



9 772096 105181
邮发代号：2-41 定价：20.00 元

万方数据

信息安全研究

(月刊 2015年创刊)

第4卷第6期(总第33期)2018年6月

本刊全文已被《CNKI中国期刊全文数据库》、《中国核心期刊(遴选)数据库》、《中文科技期刊数据库》、《超星期刊域出版平台》、《博看网》收录。

主管单位 国家发展和改革委员会
主办单位 国家信息中心

出版单位 《信息安全研究》杂志社
地址 北京市西城区三里河路58号
邮编 100045
电话 +86(10)68557385
网址 <http://ris.sic.gov.cn>
电子信箱 ris@cei.gov.cn

主编 李新友
社长 欧阳鹏
执行主编 崔传桢
副主编 吕欣 马修军 田霞
出版日期 每月5日

中国标准刊号 ISSN 2096-1057
CN 10-1345/TP

广告经营许可证 京西工商广登字20170054号
印刷单位 北京博海升彩色印刷有限公司
国内发行 北京市报刊发行局
订购处 全国各地邮电局(所)
邮发代号 2-41
定价 20.00元

战略合作单位 北京龙象之本投资管理有限公司
协办单位 亚信网络安全产业技术研究院

稿件授权声明: 凡向本刊投稿并被录用,由本刊支付稿酬的稿件,均视为稿件作者同意以下条款:

1. 文责自负。作者保证其拥有该作品的完全著作权(版权),该作品不侵犯任何他人的著作权。
2. 全权许可。本刊有权以任何形式(包括但不限于媒体、网络、光盘等介质)使用、编辑、修改该作品,无须另行征得作者同意,无须另行支付稿酬。
3. 独家使用。未经本刊书面许可,作者不同意任何单位和个人以任何形式使用(包括但不限于通过媒体、网络、光盘等介质转载、张贴、集结、出版)该作品,著作权法另有规定的除外。

版权声明: 未经本刊书面许可,任何单位和个人不得以任何形式使用(包括但不限于通过媒体、网络、光盘等介质转载、张贴、集结、出版)该作品,著作权法另有规定的除外。

» 特别策划

490 网络强国建设中的信息系统审计机制研究
..... 裴晓宁 王新杰

» 学术论文

496 区块链与量子计算 郭炜立 杨宇光

505 论虚拟货币金融犯罪的监管 朱振洁 朱翠景

511 一种基于本地代码特征的 Android 恶意代码检测方法
..... 何平 胡勇

518 密钥泄露下 Even-Mansour 密码的滑动攻击
..... 杨光 张平 胡红钢

526 一种改进的多用户多副本数据完整性验证方案
..... 潘洪志 方群 何昕

533 基于节点特征的不确定图社交网络隐私保护方法
..... 颜军 胡静 温阁 田靖攀

539 基于压缩感知的视觉有意义图像加密算法
..... 曹圣楠 杨宇光

548 基于数据生命周期的金融数据安全风险管理研究
..... 丁丽媛

555 基于 M 序列的轻量级 RFID 认证协议
..... 徐鹏翔 滕济凯 马鸿洋

» 技术应用

559 区块链技术及应用
..... 郭学沛 杨宇光

570 基于人工智能的信用卡安全营销及应用
..... 陈任峰

575 区块链技术基础及应用
..... 张舒 杨宇光

CONTENTS 目次

Special Report

Research on Information System Auditing Mechanism
for the Cyberpower Development Pei Xiaoning, et al (490)

Research Papers

Blockchain and Quantum Computing
..... Guo Weili, et al (496)

On the Supervision of Virtual Currency Financial Crimes
..... Zhu Zhenjie, et al (505)

An Android Malicious Code Detection Method Based on Native Code Features
..... He Ping, et al (511)

Slide Attacks on the Even-Mansour Scheme with Key Leakage
..... Yang Guang, et al (518)

An Improved Multi-Replica Data Integrity Verification Scheme in
Cloud Storage Environment Pan Hongzhi, et al (526)

A Method of Uncertain Graphs Based on Node Characteristics for
Preserving Privacy in Social Networks Yan Jun, et al (533)

A Visually Meaningful Image Encryption Algorithm Based on
Compressed Sensing Cao Shengnan, et al (539)

Research on Financial Data Security Management Based on Data Life Cycle
..... Ding Liyuan (548)

A Light-Weight RFID Authentication Protocol Based on M-Sequence
..... Xu Pengao, et al (555)

Technical Applications

Blockchain Technology and Application
..... Guo Xuepei, et al (559)

The Application of Credit Card Security Marketing Based on
Artificial Intelligence Chen Renfeng (570)

The Foundation and Application of Blockchain Technology
..... Zhang Shu, et al (575)

Journal of Information Security Research

Vol.4 No.6 June 2018

Publishing Period: Monthly

Date of Publication: 5th day of each month

International Standard Serial Number:
ISSN 2096-1057

Issues of Domestic Unit: CN 10-1345/TP

Editor-in-Chief: Li Xinyou

Directed by: National Development and Reform
Commission

Sponsored by: The State Information Center

Published by: Journal of Information Security
Research

Address: No.58 Sanlihe Road, Xicheng District,
Beijing

Zip Code: 100045

Website: <http://ris.sic.gov.cn>

E-mail: ris@cei.gov.cn

AD Permit: BAIC XBB Ad. No.0410

Distributor: Beijing Press and Publication Bureau

Domestic Issue Code: 2-41

Price: 20.00RMB

编委会顾问

蔡吉人 崔书昆 杜虹 顾建国 何德全
吕述望 倪光南 卿斯汉 沈昌祥 严明
杨学山 赵战生

编委会主任 杜平

编委会委员

方滨兴 王小云 安德智 陈钟 陈嘉兴
陈尚义 陈晓桦 陈兴蜀 程学旗 丁珂
丁丽萍 杜彦辉 杜跃进 段海新 方勇
封化民 冯登国 谷大武 顾健 郭莉
郭艳卿 何政 胡爱群 胡昌振 胡红钢
胡红升 贾焰 荆继武 康海燕 孔祥维
李晖 李剑 李涛 李建彬 李建华
李京春 李守鹏 李小勇 李欲晓 李舟军
林鹏 林东岱 林家骏 刘云 刘宝旭
刘吉强 罗森林 马智 马民虎 孟丹
孟小峰 闵京华 潘泉 潘柱廷 秦玉海
任卫红 孙伟 孙德刚 谭晓生 田俊峰
王标 王军 王楠 王智 王宝生
王丽娜 温巧燕 翁健 吴文玲 吴志军
肖新光 徐立臻 许光全 杨庚 杨义先
叶红 俞能海 云晓春 张健 张力
张兴 张功萱 张宏莉 张焕国 张建标
张建军 张仕斌 张玉清 赵波 赵粮
赵淦森 赵有健 钟力 周民 周文
周琳娜 周世杰 朱岩 朱建明 祝烈煌
邹维 邹德清



油画：圣母玛利亚

经典油画的再创作

李枚先生，现任爱德万斯国际集团董事长。中央美院油画系本科毕业，天津美术学院油画硕士，清华、北大EMBA。

这幅写实油画原是19世纪法国画家威廉阿道夫·布格罗的作品《百合花与圣母玛利亚》，是西方经典油画作品之一。1986年，李枚参考作品画册重新完成。作品在再现古典美的同时，赋予了时代、时尚新气息，并展现了作者细腻深厚的写实功底及个性化思考。