

国家信息中心主办

第5卷 第1期 2019年1月

Vol.5 No.1 Jan. 2019



QK1868335

信息安全研究

Journal of Information Security Research

特别策划：网络强国系列

2018 全国网民网络安全感满意度调查

密码应用安全技术体系

公钥密码的实际安全性发展研究

基于 GPU 的高性能密码计算

本期专题：密码应用安全

ISSN 2096-1057



9 772096 105198 0 1 >
邮发代号：2-41 定价：20.00 元

Xinxi Anquan Yanjiu

信息安全研究

(月刊 2015年创刊)

第5卷第1期(总第40期)2019年1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

02 2018 全国网民网络安全感满意度调查

..... 崔传桢 黄丽玲 叶科 王晖

» 密码应用安全专题

14 密码应用安全的技术体系探讨

..... 林璟铨 荆继武

23 分组密码工作模式的应用安全问题

..... 王鹏 郭婷婷

29 公钥密码的实际安全性发展研究

..... 刘亚敏 薛海洋 张道德

39 随机数发生器的设计与检测

..... 马原 陈天宇 吴鑫莹 杨静 林璟铨 荆继武

50 PKI 证书服务的安全增强技术

..... 王琼霄 王聪丽 林璟铨 宋利

59 单点登录协议实现的安全分析

..... 郭丞乾 蔡权伟 林璟铨 刘丽敏

68 密钥安全研究进展

..... 林璟铨 郑昉昱 王跃武

75 侧信道分析技术概览与实例

..... 葛景全 屠晨阳 高能

88 基于 GPU 的高性能密码计算

..... 郑昉昱 董建阔 林璟铨 高莉莉

CONTENTS 目次

Special Report

Survey on the Satisfaction of Internet Security of Chinese

Netizens in 2018 Cui Chuanzhen, et al (02)

Issue of Cryptography Application Security

The Taxonomy Towards the Security Application of Cryptography

..... Lin Jingqiang, et al (14)

Application Security of Block Cipher Mode of Operation

..... Wang Peng, et al (23)

On the Development of the Practical Security of Public Key

Cryptosystems Liu Yamin, et al (29)

Design, Implementation and Testing of Random Number

Generators Ma Yuan, et al (39)

Security Enhancement of Certificate Services in Public Key

Infrastructures Wang Qiongqiao, et al (50)

Security Analysis on the Implementations of Single-Sign-On

Protocols.....Guo Chengqian, et al (59)

Advances in Cryptographic Key Protection

..... Lin Jingqiang, et al (68)

Technology Overview of Side Channel Analysis

..... Ge Jingquan, et al (75)

High-Performance Cryptographic Computations in GPUs

..... Zheng Fangyu, et al (88)

Journal of Information Security Research

Vol.5 No.1 Jan. 2019

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 王小云

编委会委员

方滨兴 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

蔡涛先生油画作品选



油画：繁忙的渔港

油画的写实创作

蔡涛，男，中国美术家协会会员，八零油画学社成员。1988年生于山东泰安，2010年毕业于山东大学（威海）艺术学院油画专业。2010年进修于北京画院，2013年进修于中国油画院，现为徐州书画院专职画家。

这幅《繁忙的渔港》是完全基于写实的创作。福建冬季的海边比北方暖和很多，作为北方来的画家，作者在这里感觉气候柔软舒适。静静的渔港，忙碌的渔民，画面自然和谐。渔民说着外地人一句也听不懂的闽南话，微笑、夸赞，虽然听不懂，但能感觉到他们的善意和淳朴，这幅画就记录了当时渔民忙碌的场面。作品用色丰富、生动、朴实，笔法厚重，人物与海景融合处理浑然一体，达到了非常好的整体感，具有浓烈的生活气息。