

第4卷 | 第2期 | Vol.4 | No.2 March 2019

QK1914637  
CN10-1380/TN

# 信息安全学报

## Journal of Cyber Security

ISSN 2096-1146  
03  
9 772096 114190

CSCD核心期刊  
中国科技核心期刊



主办



中国科学院 信息工程研究所  
INSTITUTE OF INFORMATION ENGINEERING, CAS



SKLOIS  
信息安全国家重点实验室



科学出版社  
Science Press

万方数据

# 目 次

## 后量子密码

LWE 问题实际安全性分析综述 ..... 1

毕 蕾, 李帅钢, 刘亚敏, 张 江, 范淑琴

后量子可证明安全研究 ..... 13

江浩东, 刘亚敏

基于编码的后量子公钥密码研究进展 ..... 20

王丽萍, 戚艳红

基于 NTRU 的加密及签名算法研究 ..... 29

贺婧楠, 张振飞

基于 GSPN 的拟态 DNS 构造策略研究 ..... 37

任 权, 邬江兴, 贺 磊

基于数据流深度学习算法的 Android 恶意应用检测方法 ..... 53

朱大立, 金 昊, 吴 荻, 荆鹏飞, 杨 莹

Diskaller: 基于覆盖率制导的操作系统内核漏洞并行挖掘模型 ..... 69

涂序文, 王晓锋, 甘水滔, 陈爱国

事件库构建技术综述 ..... 83

薛 聪, 高 能, 查达仁, 王 雷, 尹芷仪, 曾泽华

# Contents

## Post-quantum cryptography

A Survey on the Analysis of the Concrete Hardness of LWE.....	1
<i>BI Lei, LI Shuaigang, LIU Yamin, ZHANG Jiang, FAN Shuqin</i>	
On Post-Quantum Provable Security.....	13
<i>JIANG Haodong, LIU Yamin</i>	
Recent progress of code-based post-quantum public key cryptography.....	20
<i>WANG Liping, QI Yanhong</i>	
Encryption and Signature Algorithms from NTRU.....	29
<i>HE Jingnan, ZHANG Zhenfei</i>	
Research on Mimic DNS Architectural Strategy Based on Generalized Stochastic Petri Net.....	37
<i>REN Quan, WU Jiangxing, HE Lei</i>	
Android malware detection method based on data-flow deep learning algorithm.....	53
<i>ZHU Dali, JIN Hao, WU Di, JING Pengfei, YANG Ying</i>	
Diskaller: Kernel Vulnerability Parallel Mining Model Based on Coverage Guidance.....	69
<i>TU Xuwen, WANG Xiaofeng, GAN Shuitao, CHEN Aiguo</i>	
Event Database Construction Techniques.....	83
<i>XUE Cong, GAO Neng, ZHA Daren, WANG Lei, YIN Zhiyi, ZENG Zehua</i>	

# 信息安全学报

Xinxi Anquan Xuebao  
(双月刊, 2016年创刊)  
第4卷 第2期 2019年3月

# Journal of Cyber Security

(Bimonthly )  
( Started in 2016)  
Vol.4 No.2 March, 2019

编辑 《信息安全学报》编辑部  
(北京海淀区闵庄路甲89号,  
邮编 100093)  
电话: 010-82546800  
E-mail: jcs@iie.ac.cn

主编 方滨兴

主办单位 中国科学院信息工程研究所  
中国科技出版传媒股份有限公司

主管单位 中国科学院

出版 中国科技出版传媒股份有限公司

印刷装订 北京科信印刷有限公司

总发行 中国科技出版传媒股份有限公司  
地址: 北京东黄城根北街16号  
邮政编码: 100717  
电话: 010-64017032  
E-mail: journal@mail.sciencep.com

Edited by Editorial Board of Journal of Cyber Security  
(89 A Minzhuang Road, Haidian District, Beijing,  
100093, P.R.China)  
E-mail: jcs@iie.ac.cn  
Editor-in-Chief: Binxing Fang

Sponsored by Institute of Information Engineering,  
The Chinese Academy of Sciences(IIECAS);  
China Science Publishing & Media LTD

Published by China Science Publishing & Media LTD  
Printed by Beijing Kexin Printing Limited Company  
Distributed by Science Press  
No.16 Donghuangchenggen North Street  
Beijing 100717,China  
Telephone:010-64017032  
E-mail:journal@mail.sciencep.com

刊号: ISSN 2096-1146  
CN10-1380/TN

©2016 IIECAS (版权所有)  
公开发行

邮发代号: 80-601

定价: 60.00元