信息安全学报

信息安全学报

Journal of Cyber Security

中国计算机学会 CCF

ISSN 2096-1146
9 772096 114206 11>

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

一种检测 C&W 对抗样本图像的盲取证算法 ········ *1*

邓　康, 罗盛海, 彭安杰, 曾　辉, 黄晓芳

基于信息增益的无线通信信号指纹构建及识别机制研究 ········ *11*

黄伟庆, 杨召阳, 魏　冬, 张　萌, 王　文, 叶　彬

隐私数据验证场景下的隐私保护研究 ········ *27*

石　侃, 陈　洁

多源融合信息泄漏检测方法 ········ *40*

曹雨晨, 周永彬

基于参数转换的语音深度伪造及其对声纹认证的威胁评估 ········ *53*

苗晓孔, 孙　蒙, 张雄伟, 李嘉康, 张星昱

基于 GPU 的 X25519/448 密钥协商算法的高速实现 ········ *60*

董建阔, 郑昉昱, 林璟锵

一种基于二维码对抗样本的物理补丁攻击 ········ *75*

钱亚冠, 刘新伟, 顾钊铨, 王　滨, 潘　俊, 张锡敏

基于后量子假设的高效范围证明方案 ········ *87*

滕瑜莹, 谢　翔, 邓　燚

期刊基本参数：CN 10-1380/TN＊2016＊b＊16＊102＊zh＊P＊ ￥60＊2000＊10＊2020-11

万方数据

信息安全学报
Journal of Cyber Security

Contents

Blind forensics of adversarial images generated by C&W algorithm ········ 1

DENG Kang, LUO Shenghai, PENG Anjie, ZENG Hui, HUANG Xiaofang

Fingerprint construction and identity recognition of Wireless signal based on information gain ········ 11

HUANG Weiqing, YANG Zhaoyang, WEI Dong, ZHANG Meng, WANG Wen, YE Bin

Research on privacy protection in privacy data verification scenarios ········ 27

SHI Kan, CHEN Jie

Multi-Channel Fusion Leakage Detection ········ 40

CAO Yuchen, ZHOU Yongbin

Deep Speech Forgery Based on Parameter Transformation and Threat Assessment to Voiceprint Authentication ···· 53

MIAO Xiaokong, SUN Meng, ZHANG Xiongwei, LI Jiakang, ZHANG Xingyu

Implementing High-performance X25519/448 Key Agreement Scheme in General Purpose GPUs ········ 60

DONG Jiankuo, ZHENG Fangyu, LIN Jingqiang

QR Code Based Patch Attacks in Physical World ········ 75

QIAN Yaguan, LIU Xinwei, GU Zhaoquan, WANG Bin, PAN Jun, ZHANG Ximin

Efficient Range Proofs from Post-Quantum Assumptions ········ 87

TENG Yuying, XIE Xiang, DENG Yi

©Copyright 2016, Institute of Information Engineering, the Chinese Academy of Sciences. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form without the prior written permission of the Institute of Information Engineering, the Chinese Academy of Sciences.

万方数据