信息安全学报
Journal of Cyber Security

目　　录

公钥可搜索加密体制综述 ······ *1*
秦志光, 徐　骏, 聂旭云, 熊　虎

振荡采样型真随机数发生器的健壮性研究 ······ *13*
陈天宇, 马　原, 荆继武, 朱双怡

云存储完整性验证密码学技术研究进展 ······ *23*
王玉珏, 伍前红

轻量级分组密码 **RECTANGLE** 基于 **FELICS** 的实现与优化 ······ *36*
罗　鹏, 张文涛, 包珍珍

关于无个人公钥的群认证 ······ 48
蒋绍权

BC 加密模式的分析及其改进 ······ *61*
郑凯燕, 王　鹏

期刊基本参数：CN 10-1380/TN＊2016＊q＊16＊78＊zh＊P＊ ￥60＊2000＊6＊2017-03

万方数据

Contents

A Survey of Public-Key Encryption with Keyword Search ········ *1*

QIN Zhiguang, XU Jun, NIE Xuyun, XIONG Hu

On the Robustness of Oscillator-based True Random Number Generators ········ *13*

CHEN Tianyu, MA Yuan, JING Jiwu, ZHU Shuangyi

A Survey on Cryptographic Technologies for Data Integrity Checking in Clouds ········ *23*

WANG Yujue, WU Qianhong

The Implementation and Optimization of Lightweight Block Cipher RECTANGLE based on FELICS ········ 36

LUO Peng, ZHANG Wentao, BAO Zhenzhen

On Group Authentication without Personal Public-Keys ········ *48*

JIANG Shaoquan

The concrete security of BC mode and its improvement ········ *61*

ZHENG Kaiyan, WANG Peng

©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