

《信息安全与密码学》

图书基本信息

书名：《信息安全与密码学》

13位ISBN编号：9787030311948

10位ISBN编号：7030311949

出版时间：2011-6

出版社：来学嘉 科学出版社 (2011-06出版)

作者：来学嘉

页数：195

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《信息安全与密码学》

内容概要

由来学嘉编著的《信息安全与密码学（英文版）》是2010年10月在上海召开的第六届中国密码学与信息安全国际会议（The 6th china International Conference on Information Security and cryptology-Inscrypt 2010）的短论文文集。Inscrypt系列国际会议是由信息安全国家重点实验室发起，与中国密码学会联合举办的高水平国际会议，每年在中国举办一次，该会议论文集由Springer出版社出版。本书收录了这次会议的短文13篇。主要内容包括公钥和椭圆曲线密码学、密码系统构造、系统安全等

。《信息安全与密码学（英文版）》可供从事密码学、信息安全、通信与信息系统、计算机应用技术等专业的科技人员和高等院校师生参考。

书籍目录

Public Key and Elliptic Curve Cryptography
Attacking Code/Lattice-based Cryptosystems Using Partial Knowledge Robert Niebuhr, Pierre-Louis Cayrel, Stanislav Bulygin, Johannes Bachmann
Multivariate Quadratic Quasigroups (MQGs): Construction, Bounds and Complexity Yanling Chen, Svein Johan Knapskog, Danilo Gligoroski
How to Hash into Twisted Edwards Form Elliptic Curves Wei Yu, KunPeng Wang
Fast Algorithm Converting Integer to Double Base Chain Wei Yu, KunPeng Wang, Bao Li
Cryptographic Construction
Visualizing Key Authenticity: Turning Your Face into Your Public Key..Joan Arnedo-Moreno, Agata Lapedriza
Practical Multi-signature Scheme in the Plain Public Key Model with Tight Security Changshe Ma
Security Improvement of a Pixel Bit Based Image Scrambling Encryption Scheme Through the Self-correlation Method Liang Zhao, Avishek Adhikari, Di Xiao, Kouichi Sakurai
Hierarchical Attributes: Practical Extension for Attribute-based Encryption Song Luo, Jianbin Hu, Zhong Chen
A Modular Proof Technique for Password-based Authenticated Key Exchange Protocols Libin Wang, Jiabin Pan, Changshe Ma
Cryptographic Hash Functions: Recent Design Trends and Security Notions Sail Al-Kuwari, James H. Davenport, Russell J. Bradford
System Security
Three-party Password Authenticated Key Exchange in the Standard Model Xuexian Hu, Zhenfeng Zhang, Wenfen Liu
Ticket Based Pre-authentication Method for Trusted Nodes in Proxy Mobile IPv6 Domain Ling Tie, Di He
Software Protection Combined with Hardware Kazuhide Fukushima, Kiyomoto Shinsaku, Toshiaki Tanaka
Author Index

《信息安全与密码学》

编辑推荐

由来学嘉编著的《信息安全与密码学（英文版）》是2010年10月在上海召开的第六届中国密码学与信息安全国际会议（The 6th china International Conference on Information Security and cryptology-Inscrypt 2010）的短论文文集。本书主要内容包括公钥和椭圆曲线密码学、密码系统构造、系统安全等。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:www.tushu111.com