《Cryptology and Netwo》

图书基本信息

书名：《Cryptology and Network Security密码术与网络安全》

13位ISBN编号：9783540308492

10位ISBN编号：3540308490

出版时间：2006-1

出版社：Springer

作者：Yvo G. Desmedt

页数：348

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

《Cryptology and Netwo》

内容概要

This book constitutes the refereed proceedings of the 4th International Conference on Cryptology and Network Security, CANS 2005, held in Xiamen, China in December 2005. The 28 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 118 submissions. The papers are organized in topical sections on cryptanalysis, intrusion detection and viruses, authentication and signature, signcryption, e-mail security, cryptosystems, privacy and tracing, information hiding, firewalls, denial of service and DNS security, and trust management.

《Cryptology and Netwo》

书籍目录

Cryptanalysis　The Second-Preimage Attack on MD4　On the Security of Certificateless Signature Schemes from Asiacrypt 2003　On the Security of a Group Signcryption Scheme from Distributed Signcryption Scheme　Cryptanalysis of Two Group Key Management Protocols for Secure Multicast　Security Analysis of Password-Authenticated Key Agreement ProtocolsIntrusion Detection and Viruses　An Immune-Based Model for Computer Virus Detection　A New Model for Dynamic Intrusion Detection　Self Debugging Mode for Patch-Independent Nullification of Unknown Remote Process Infection　A New Unsupervised Anomaly Detection Framework for Detecting Network Attacks in Real-TimeAuthentication and Signature　ID-Based Aggregate Signatures from Bilinear Pairings　Efficient Identity-Based Signatures and Blind Signatures　How to Authenticate Real Time Streams Using Improved Online/Of[line Signatures　New Authentication Scheme Based on a One-Way Hash Function and　Diffie-Hellman Key ExchangeSigncryption　Two Proxy Signcryption Schemes from Bilinear Pairings　Constructing Secure Warrant-Based Proxy Signcryption SchemesE-mail Security　Design and Implementation of an Inline Certified E-mail Service　Efficient Identity-Based Protocol for Fair Certified E-mail Delivery Cryptosystems　Similar Keys of Multivariate Quadratic Public Key Cryptosystems　A Note on Signed Binary Window Algorithm for Elliptic Curve Cryptosystems　Constructions of Almost Resilient FunctionsPrivacy and TracingInformation HidingFirewalls,Denial of Service and DNS SecurityTrust ManagementAuthor Index

《Cryptology and Netwo》

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