

<<密码术故障诊断与容错>>

图书基本信息

书名：<<密码术故障诊断与容错>>

13位ISBN编号：9783540462507

10位ISBN编号：3540462503

出版时间：2006-11-13

出版时间：Springer

作者：Breveglieri, Luca; Koren, Israel; Naccache, David

页数：250

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：<http://www.tushu007.com>

<<密码术故障诊断与容错>>

内容概要

This book constitutes the refereed proceedings of the Third International Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2006, held in Yokohama, Japan in October 2006. The 12 revised papers of FDTC 2006 are presented together with 9 papers from FDTC 2004 and FDTC 2005 that passed a second round of reviewing. They all provide a comprehensive introduction to the issues faced by designers of robust cryptographic devices and to the currently available methodologies and techniques for protecting these devices against fault injection attacks. The papers are organized in topical sections on attacks on public key systems, protection of public key systems, attacks on and protection of symmetric key systems, models for fault attacks on cryptographic devices, fault-resistant arithmetic for cryptography, as well as fault attacks and other security threats.

<<密码术故障诊断与容错>>

书籍目录

Attacks on Public Key Systems Is It Wise to Publish Your Public RSA Keys? (2006) Wagner's Attack on a Secure CRT-RSA Algorithm Reconsidered (2006) Attacking Right-to-Left Modular Exponentiation with Timely Random Faults (2006) Sign Change Fault Attacks on Elliptic Curve Cryptosystems (2004-05) Cryptanalysis of Two Protocols for RSA with CRT Based on Fault Infection (2004-05) Protection of Public Key Systems Blinded Fault Resistant Exponentiation (2006) Incorporating Error Detection in an RSA Architecture (2004-05) Data and Computational Fault Detection Mechanism for Devices That Perform Modular Exponentiation (2004-05) Attacks on and Protection of Symmetric Key Systems Case Study of a Fault Attack on Asynchronous DES Crypto-Processors (2006) A Fault Attack Against the FOX Cipher Family (2006) Fault Based Collision Attacks on AES (2006) An Easily Testable and Reconfigurable Pipeline for Symmetric Block Ciphers (2006) Models for Fault Attacks on Cryptographic Devices An Adversarial Model for Fault Analysis Against Low-Cost Cryptographic Devices (2004-05) Cryptographic Key Reliable Lifetimes: Bounding the Risk of Key Exposure in the Presence of Faults (2004-05) A Comparative Cost/Security Analysis of Fault Attack Countermeasures (2004-05) Fault-Resistant Arithmetic for Cryptography Non-linear Residue Codes for Robust Public-Key Arithmetic (2006) Fault Attack Resistant Cryptographic Hardware with Uniform Error Detection (2004-05) Robust Finite Field Arithmetic for Fault-Tolerant Public-Key Cryptography (2004-05) Fault Attacks and Other Security Threats DPA on Faulty Cryptographic Hardware and Countermeasures (2006) Fault Analysis of DPA-Resistant Algorithms (2006).....Author Index

<<密码术故障诊断与容错>>

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:<http://www.tushu007.com>