

# 《Cryptographic Hardwa》

## 图书基本信息

书名：《Cryptographic Hardware and Embedded Systems - CHES 2005加密硬件与嵌入系统 - CHES 2005 / 会议录》

13位ISBN编号：9783540284741

10位ISBN编号：3540284745

出版时间：2005-9

出版社：北京燕山出版社

作者：Rao, Josyula R.; Sunar, Berk;

页数：458

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.tushu000.com](http://www.tushu000.com)

# 《Cryptographic Hardwa》

## 内容概要

This book constitutes the refereed proceedings of the 7th International Workshop on Cryptographic Hardware and Embedded Systems, CHES 2005, held in Edinburgh, UK in August/September 2005. The 32 revised full papers presented were carefully reviewed and selected from 108 submissions. The papers are organized in topical sections on side channels, arithmetic for cryptanalysis, low resources, special purpose hardware, hardware attacks and countermeasures, arithmetic for cryptography, trusted computing, and efficient hardware.

## 书籍目录

Side Channels Resistance of Randomized Projective Coordinates Against Power Analysis Templates as Master Keys A Stochastic Model for Differential Side Channel Cryptanalysis Arithmetic for Cryptanalysis A New Baby-Step Giant-Step Algorithm and Some Applications to Cryptanalysis Further Hidden Markov Model Cryptanalysis Low Resources Energy-Efficient Software Implementation of Long Integer Modular Arithmetic Short Memory Scalar MultiDlication on Koblitz Curves Hardware/Software Co-design for Hyperelliptic Curve Cryptography(HECC) on the 8051 uP Special Purpose Hardware SHARK: A Realizable Special Hardware Sieving Device for Factoring 1024-Bit Integers Scalable Hardware for Sparse Systems of Linear Equations, with Applications to Integer Factorization Design of Testable Random Bit Generators Hardware Attacks and Countermeasures I Successfully Attacking Masked AES Hardware Implementations Masked Dual-Rail Pre-charge Logic: DPA-Resistance Without Routing Constraints Masking at Gate Level in the Presence of Glitches Arithmetic for Cryptography Bipartite Modular Multiplication Fast Truncated Multiplication for Cryptographic Applications Using an RSA Accelerator for Modular Inversion Comparison of Bit and Word Level Algorithms for Evaluating Unstructured Functions over Finite RingsSide Channel (EM) EM Analysis of Rijndael and ECC on a Wireless Java-Based PDA Security Limits for Compromising Emanations Security Evaluation Against Electromagnetic Analysis at Design TimeSide Channel Trusted Computing Hardware Attacks and Countermeasures Hardware Attacks and Countermeasures Efficient Hardwate Efficient Hardwate Author Index

# 《Cryptographic Hardwa》

## 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.tushu000.com](http://www.tushu000.com)