

<<(加密硬件与嵌入式系统CHES 20)>>

图书基本信息

书名：<<(加密硬件与嵌入式系统CHES 2001)Cryptographic hardware and embedded systems>>

13位ISBN编号：9783540425212

10位ISBN编号：3540425217

出版时间：2001-12

出版时间：1 edition (2001年9月1日)

作者：Cetin K. Koc

页数：410

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>

<<(加密硬件与嵌入式系统CHES 20)>>

内容概要

This book constitutes the thoroughly refereed post-proceedings of the Third International Workshop on Cryptanalysis Hardware and Embedded Systems, CHES 2001, held in Paris, France in Mai 2001. The 31 revised full papers presented were carefully reviewed and selected from 66 submissions. The papers are organized in topical sections on side channel attacks, Rijndael hardware implementation, random number generators, elliptic curve algorithms, arithmetic architectures, cryptanalysis, embedded implementations of ciphers, and side channel attacks on elliptic curve cryptosystems.

书籍目录

Invited Talk Protecting Embedded Systems - The Next Ten Years
Side Channel Attacks I A Sound Method for Switching between Boolean and Arithmetic Masking
Fast Primitives for Internal Data Scrambling in Tamper Resistant Hardware
Random Register Renaming to Foil DPA
Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks
Rijndael Hardware Implementations Architectural Optimization for a 1.82Gbits/sec VLSI Implementation of the AES
Rijndael Algorithm High Performance Single-Chip FPGA Rijndael Algorithm
Two Methods of Rijndael Implementation in Reconfigurable Hardware
Random Number Generators Pseudo-random Number Generation on the IBM 4758 Secure Crypto Coprocessor
Efficient Online Tests for True Random Number Generators
Elliptic Curve Algorithms The Hessian Form of an Elliptic Curve
Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication Algorithm with Recovery of the y -Coordinate on a Montgomery-Form Elliptic Curve
Generating Elliptic Curves of Prime Order
Invited Talk New Directions in Cryptography
Arithmetic Architectures A New Low Complexity Parallel Multiplier for a Class of Finite Fields .
Efficient Rijndael Encryption Implementation with Composite Field Arithmetic
High-Radix Design of a Scalable Modular Multiplier
A Bit-Serial Unified Multiplier Architecture for Finite Fields $GF(p)$ and $GF(2^m)$
Cryptanalysis Attacks on Cryptoprocessor Transaction Sets
Bandwidth-Optimal Kleptographic Attacks
Electromagnetic Analysis: Concrete Results
Embedded Implementations and New Ciphers
Hardware Implementations of Ciphers
Author Index

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>