# Table of Contents

**Invited Talk**

Protecting Embedded Systems – The Next Ten Years .......................... 1
  
  *R. Anderson*

**Side Channel Attacks I**

A Sound Method for Switching between Boolean and Arithmetic Masking ... 3
  
  *L. Goubin*

Fast Primitives for Internal Data Scrambling in Tamper Resistant Hardware ................................................................. 16
  
  *E. Brier, H. Handschuh, and C. Tymen*

Random Register Renaming to Foil DPA ........................................... 28
  
  *D. May, H.L. Muller, and N.P. Smart*

Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks ......................................................... 39
  
  *E. Oswald and M. Aigner*

**Rijndael Hardware Implementations**

Architectural Optimization for a 1.82Gbits/sec VLSI Implementation of the AES Rijndael Algorithm ................................................. 51
  
  *H. Kuo and I. Verbauwhede*

High Performance Single-Chip FPGA Rijndael Algorithm ....................... 65
  
  *M. McLoone and J.V. McCanny*

Two Methods of Rijndael Implementation in Reconfigurable Hardware .......... 77
  
  *V. Fischer and M. Drutarovsky*

**Random Number Generators**

Pseudo-random Number Generation on the IBM 4758 Secure Crypto Coprocessor ................................................................. 93
  
  *N. Howgrave-Graham, J. Dyer, and R. Gennaro*

Efficient Online Tests for True Random Number Generators .................. 103
  
  *W. Schindler*
Elliptic Curve Algorithms

The Hessian Form of an Elliptic Curve ........................................... 118
  N.P. Smart

Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication
Algorithm with Recovery of the y-Coordinate
on a Montgomery-Form Elliptic Curve ........................................ 126
  K. Okeya and K. Sakurai

Generating Elliptic Curves of Prime Order .................................... 142
  E. Savaş, T.A. Schmidt, and Ç. K. Koç

Invited Talk

New Directions in Cryptography .............................................. 159
  A. Shamir

Arithmetic Architectures

A New Low Complexity Parallel Multiplier for a Class of Finite Fields .... 160
  M. Leone

Efficient Rijndael Encryption Implementation
with Composite Field Arithmetic .............................................. 171
  A. Rudra, P.K. Dubey, C.S. Jutla, V. Kumar,
  J.R. Rao, and P. Rohatgi

High-Radix Design of a Scalable Modular Multiplier ....................... 185
  A.F. Tenca, G. Todorov, and Ç.K. Koç

A Bit-Serial Unified Multiplier Architecture
for Finite Fields GF(p) and GF(2^m) .................................... 202
  J. Großschädl

Cryptanalysis

Attacks on Cryptoprocessor Transaction Sets ................................ 220
  M. Bond

Bandwidth-Optimal Kleptographic Attacks .................................... 235
  A. Young and M. Yung

Electromagnetic Analysis: Concrete Results ................................ 251
  K. Gandolfi, C. Mourtel, and F. Olivier
Embedded Implementations and New Ciphers

NTRU in Constrained Devices ............................................262
   D.V. Bailey, D. Coffin, A. Elbirt, J.H. Silverman, and A.D. Woodbury

Transparent Harddisk Encryption .........................................273
   T. Pornin

Side Channel Attacks II

Sliding Windows Succumbs to Big Mac Attack .........................286
   C.D. Walter

Universal Exponentiation Algorithm:
   A First Step towards Provable SPA-Resistance ......................300
   C. Clavier and M. Joye

An Implementation of DES and AES, Secure against Some Attacks ....309
   M. Akkar and C. Giraud

Hardware Implementations of Ciphers

Efficient Implementation of “Large” Stream Cipher Systems .............319
   P. Sarkar and S. Maitra

Tradeoffs in Parallel and Serial Implementations
   of the International Data Encryption Algorithm IDEA ...............333

A Scalable $GF(p)$ Elliptic Curve Processor Architecture
   for Programmable Hardware ..........................................348
   G. Orlando and C. Paar

Implementation of RSA Algorithm
   Based on RNS Montgomery Multiplication ............................364
   H. Nozaki, M. Motoyama, A. Shinbo, and S. Kawamura
Side Channel Attacks on Elliptic Curve Cryptosystems

Protections against Differential Analysis for Elliptic Curve Cryptography: An Algebraic Approach ........................................... 377
   M. Joye and C. Tymen

Preventing SPA/DPA in ECC Systems Using the Jacobi Form .......... 391
   P.-Y. Lariidet and N.P. Smart

Hessian Elliptic Curves and Side-Channel Attacks ..................... 402
   M. Joye and J.-J. Quisquater

Author Index ........................................................................ 411
Cryptographic Hardware and Embedded Systems - CHES 2001
Koc, C.K.; Nauchae, D.; Paar, C. (Eds.)
2001, XIV, 418 p., Softcover
ISBN: 978-3-540-42521-2