

Table of Contents

Invited Talk

CHES: Past, Present, and Future	1
<i>Jean-Jacques Quisquater</i>	

Attack Strategies

Optical Fault Induction Attacks	2
<i>Sergei P. Skorobogatov, Ross J. Anderson</i>	
Template Attacks	13
<i>Suresh Chari, Josyula R. Rao, Pankaj Rohatgi</i>	
The EM Side-Channel(s)	29
<i>Dakshi Agrawal, Bruce Archambeault, Josyula R. Rao, Pankaj Rohatgi</i>	

Finite Field and Modular Arithmetic I

Enhanced Montgomery Multiplication	46
<i>Shay Gueron</i>	
New Algorithm for Classical Modular Inverse	57
<i>Róbert Lórencz</i>	
Increasing the Bitlength of a Crypto-Coprocessor	71
<i>Wieland Fischer, Jean-Pierre Seifert</i>	

Elliptic Curve Cryptography I

Enhancing Simple Power-Analysis Attacks on Elliptic Curve Cryptosystems	82
<i>Elisabeth Oswald</i>	
Implementation of Elliptic Curve Cryptography with Built-In Counter Measures against Side Channel Attacks	98
<i>Elena Trichina, Antonio Bellezza</i>	
Secure Elliptic Curve Implementations: An Analysis of Resistance to Power-Attacks in a DSP Processor	114
<i>Catherine H. Gebotys, Robert J. Gebotys</i>	
Address-Bit Differential Power Analysis of Cryptographic Schemes OK-ECDH and OK-ECDSA	129
<i>Kouichi Itoh, Tetsuya Izu, Masahiko Takenaka</i>	

AES and AES Candidates

2Gbit/s Hardware Realizations of RIJNDAEL and SERPENT: A Comparative Analysis	144
<i>A.K. Lutz, J. Treichler, F.K. Gürkaynak, H. Kaeslin, G. Basler, A. Erni, S. Reichmuth, P. Rommens, S. Oetiker, W. Fichtner</i>	
Efficient Software Implementation of AES on 32-Bit Platforms	159
<i>Guido Bertoni, Luca Breveglieri, Pasqualina Fragneto, Marco Macchetti, Stefano Marchesin</i>	
An Optimized S-Box Circuit Architecture for Low Power AES Design ...	172
<i>Sumio Morioka, Akashi Satoh</i>	
Simplified Adaptive Multiplicative Masking for AES	187
<i>Elena Trichina, Domenico De Seta, Lucia Germani</i>	
Multiplicative Masking and Power Analysis of AES.....	198
<i>Jovan D. Golić, Christophe Tymen</i>	

Tamper Resistance

Keeping Secrets in Hardware: The Microsoft Xbox™ Case Study	213
<i>Andrew Huang</i>	

RSA Implementation

A DPA Attack against the Modular Reduction within a CRT Implementation of RSA	228
<i>Bert den Boer, Kerstin Lemke, Guntram Wicke</i>	
Further Results and Considerations on Side Channel Attacks on RSA....	244
<i>Vlastimil Klíma, Tomáš Rosa</i>	
Fault Attacks on RSA with CRT: Concrete Results and Practical Countermeasures	260
<i>Christian Aumüller, Peter Bier, Wieland Fischer, Peter Hofreiter, Jean-Pierre Seifert</i>	

Finite Field and Modular Arithmetic II

Some Security Aspects of the MIST Randomized Exponentiation Algorithm	276
<i>Colin D. Walter</i>	
The Montgomery Powering Ladder	291
<i>Marc Joye, Sung-Ming Yen</i>	
DPA Countermeasures by Improving the Window Method	303
<i>Kouichi Itoh, Jun Yajima, Masahiko Takenaka, Naoya Torii</i>	

Efficient Subgroup Exponentiation in Quadratic and Sixth Degree Extensions	318
<i>Martijn Stam, Arjen K. Lenstra</i>	

Elliptic Curve Cryptography II

On the Efficient Generation of Elliptic Curves over Prime Fields	333
<i>Elisavet Konstantinou, Yiannis C. Stamatiou, Christos Zaroliagis</i>	
An End-to-End Systems Approach to Elliptic Curve Cryptography	349
<i>Nils Gura, Sheueling Chang Shantz, Hans Eberle, Sumit Gupta, Vipul Gupta, Daniel Finchelstein, Edouard Goupy, Douglas Stebila</i>	
A Low-Power Design for an Elliptic Curve Digital Signature Chip	366
<i>Richard Schroepel, Cheryl Beaver, Rita Gonzales, Russell Miller, Timothy Draelos</i>	
A Reconfigurable System on Chip Implementation for Elliptic Curve Cryptography over $\mathbb{GF}(2^n)$	381
<i>M. Ernst, M. Jung, F. Madlener, S. Huss, R. Blümel</i>	
Genus Two Hyperelliptic Curve Coprocessor	400
<i>N. Boston, T. Clancy, Y. Liow, J. Webster</i>	

Random Number Generation

True Random Number Generator Embedded in Reconfigurable Hardware	415
<i>Viktor Fischer, Miloš Drutarovský</i>	
Evaluation Criteria for True (Physical) Random Number Generators Used in Cryptographic Applications	431
<i>Werner Schindler, Wolfgang Killmann</i>	
A Hardware Random Number Generator	450
<i>Thomas E. Tkacik</i>	

Invited Talk

RFID Systems and Security and Privacy Implications	454
<i>Sanjay E. Sarma, Stephen A. Weis, Daniel W. Engels</i>	

New Primitives

A New Class of Invertible Mappings	470
<i>Alexander Klimov, Adi Shamir</i>	

Finite Field and Modular Arithmetic II

Scalable and Unified Hardware to Compute Montgomery Inverse in
GF(p) and GF(2ⁿ) 484
*Adnan Abdul-Aziz Gutub, Alexandre F. Tenca, ErKay Savaş,
Çetin K. Koç*

Dual-Field Arithmetic Unit for GF(p) and GF(2^m) 500
Johannes Wolkerstorfer

Error Detection in Polynomial Basis Multipliers over Binary
Extension Fields 515
Arash Reyhani-Masoleh, M.A. Hasan

Hardware Implementation of Finite Fields of Characteristic Three 529
D. Page, N.P. Smart

Elliptic Curve Cryptography III

Preventing Differential Analysis in GLV Elliptic Curve
Scalar Multiplication 540
Mathieu Ciet, Jean-Jacques Quisquater, Francesco Sica

Randomized Signed-Scalar Multiplication of ECC to
Resist Power Attacks 551
Jae Cheol Ha, Sang Jae Moon

Fast Multi-scalar Multiplication Methods on Elliptic Curves with
Precomputation Strategy Using Montgomery Trick 564
Katsuyuki Okeya, Kouichi Sakurai

Hardware for Cryptanalysis

Experience Using a Low-Cost FPGA Design to Crack DES Keys 579
Richard Clayton, Mike Bond

A Time-Memory Tradeoff Using Distinguished Points: New Analysis
& FPGA Results 593
*Francois-Xavier Standaert, Gael Rouvroy, Jean-Jacques Quisquater,
Jean-Didier Legat*

Author Index 611

Template Attacks

Suresh Chari, Josyula R. Rao, and Pankaj Rohatgi

No Institute Given

Cryptographic Hardware and Embedded Systems -
CHES 2002

4th International Workshop, Redwood Shores, CA, USA,
August 13-15, 2002, Revised Papers

Kaliski, B.S.J.; Koc, C.K.; Paar, C. (Eds.)

2003, XIV, 618 p., Softcover

ISBN: 978-3-540-00409-7