

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

**AES and AES Candidates**

2Gbit/s Hardware Realizations of RIJNDAEL and SERPENT:  
A Comparative Analysis ..... 144  
*A.K. Lutz, J. Treichler, F.K. Gürkaynak, H. Kaeslin, G. Basler,  
A. Erni, S. Reichmuth, P. Rommens, S. Oetiker, W. Fichtner*

Efficient Software Implementation of AES on 32-Bit Platforms ..... 159  
*Guido Bertoni, Luca Breveglieri, Pasqualina Fragneto,  
Marco Macchetti, Stefano Marchesin*

An Optimized S-Box Circuit Architecture for Low Power AES Design ... 172  
*Sumio Morioka, Akashi Satoh*

Simplified Adaptive Multiplicative Masking for AES ..... 187  
*Elena Trichina, Domenico De Seta, Lucia Germani*

Multiplicative Masking and Power Analysis of AES ..... 198  
*Jovan D. Golić, Christophe Tymen*

**Tamper Resistance**

Keeping Secrets in Hardware: The Microsoft Xbox™ Case Study ..... 213  
*Andrew Huang*

**RSA Implementation**

A DPA Attack against the Modular Reduction within a CRT  
Implementation of RSA ..... 228  
*Bert den Boer, Kerstin Lemke, Guntram Wicke*

Further Results and Considerations on Side Channel Attacks on RSA .... 244  
*Vlastimil Klíma, Tomáš Rosa*

Fault Attacks on RSA with CRT: Concrete Results and  
Practical Countermeasures ..... 260  
*Christian Aumüller, Peter Bier, Wieland Fischer, Peter Hofreiter,  
Jean-Pierre Seifert*

**Finite Field and Modular Arithmetic II**

Some Security Aspects of the MIST Randomized  
Exponentiation Algorithm ..... 276  
*Colin D. Walter*

The Montgomery Powering Ladder ..... 291  
*Marc Joye, Sung-Ming Yen*

DPA Countermeasures by Improving the Window Method ..... 303  
*Kouichi Itoh, Jun Yajima, Masahiko Takenaka, Naoya Torii*

|                                                                                  |     |
|----------------------------------------------------------------------------------|-----|
| 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 $\text{GF}(2^n)$ .....                           | 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(2<sup>n</sup>) ..... 484  
    *Adnan Abdul-Aziz Gutub, Alexandre F. Tenca, Erkey Savaş,*  
    *Çetin K. Koç*

Dual-Field Arithmetic Unit for GF(p) and GF(2<sup>m</sup>) ..... 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