

Table of Contents

Invited Talk

Software Implementation of Elliptic Curve Cryptography over Binary Fields	1
<i>Darrel Hankerson, Julio López Hernandez, and Alfred Menezes</i>	

Implementation of Elliptic Curve Cryptosystems

Implementation of Elliptic Curve Cryptographic Coprocessor over $GF(2^m)$ on an FPGA	25
<i>Souichi Okada, Naoya Torii, Kouichi Itoh, and Masahiko Takenaka</i>	
A High-Performance Reconfigurable Elliptic Curve Processor for $GF(2^m)$	41
<i>Gerardo Orlando and Christof Paar</i>	
Fast Implementation of Elliptic Curve Defined over $GF(p^m)$ on CalmRISC with MAC2424 Coprocessor	57
<i>Jae Wook Chung, Sang Gyoo Sim, and Pil Joong Lee</i>	

Power and Timing Analysis Attacks

Protecting Smart Cards from Passive Power Analysis with Detached Power Supplies	71
<i>Adi Shamir</i>	
Smartly Analyzing the Simplicity and the Power of Simple Power Analysis on Smartcards	78
<i>Rita Mayer-Sommer</i>	
Power Analysis Attacks and Algorithmic Approaches to their Countermeasures for Koblitz Curve Cryptosystems	93
<i>M. Anwar Hasan</i>	
A Timing Attack against RSA with the Chinese Remainder Theorem	109
<i>Werner Schindler</i>	

Hardware Implementation of Block Ciphers

A Comparative Study of Performance of AES Final Candidates Using FPGAs	125
<i>Andreas Dandalis, Viktor K. Prasanna, and Jose D.P. Rolim</i>	
A Dynamic FPGA Implementation of the Serpent Block Cipher	141
<i>Cameron Patterson</i>	

A 12 Gbps DES Encryptor/Decryptor Core in an FPGA	156
<i>Steve Trimberger, Raymond Pang, and Amit Singh</i>	
A 155 Mbps Triple-DES Network Encryptor	164
<i>Herbert Leitold, Wolfgang Mayerwieser, Udo Payer, Karl Christian Posch, Reinhard Posch, and Johannes Wolkerstorfer</i>	

Hardware Architectures

An Energy Efficient Reconfigurable Public-Key Cryptography Processor Architecture	175
<i>James Goodman and Anantha Chandrakasan</i>	
High-Speed RSA Hardware Based on Barret's Modular Reduction Method	191
<i>Johann Großschädl</i>	
Data Integrity in Hardware for Modular Arithmetic	204
<i>Colin D. Walter</i>	
A Design for Modular Exponentiation Coprocessor in Mobile Telecommunication Terminals	216
<i>Takehiko Kato, Satoru Ito, Jun Anzai, and Natsume Matsuzaki</i>	

Invited Talk

How to Explain Side-Channel Leakage to Your Kids	229
<i>David Naccache and Michael Tunstall</i>	

Power Analysis Attacks

On Boolean and Arithmetic Masking against Differential Power Analysis	231
<i>Jean-Sébastien Coron and Louis Goubin</i>	
Using Second-Order Power Analysis to Attack DPA Resistant Software	238
<i>Thomas S. Messerges</i>	
Differential Power Analysis in the Presence of Hardware Countermeasures	252
<i>Christophe Clavier, Jean-Sébastien Coron, and Nora Dabbous</i>	

Arithmetic Architectures

Montgomery Multiplier and Squarer in $GF(2^m)$	264
<i>Huapeng Wu</i>	
A Scalable and Unified Multiplier Architecture for Finite Fields $GF(p)$ and $GF(2^m)$	277
<i>Erkay Savaş, Alexandre F. Tenca, and Çetin K. Koç</i>	

Montgomery Exponentiation with no Final Subtractions: Improved Results	293
<i>Gaël Hachez and Jean-Jacques Quisquater</i>	

Physical Security and Cryptanalysis

Physical Security Devices for Computer Subsystems: A Survey of Attacks and Defenses	302
<i>Steve H. Weingart</i>	
Software-Hardware Trade-Offs: Application to A5/1 Cryptanalysis	318
<i>Thomas Pornin and Jacques Stern</i>	

New Schemes and Algorithms

MiniPASS: Authentication and Digital Signatures in a Constrained Environment	328
<i>Jeffrey Hoffstein and Joseph H. Silverman</i>	
Efficient Generation of Prime Numbers	340
<i>Marc Joye, Pascal Paillier, and Serge Vaudenay</i>	
Author Index	355