

Table of Contents

Side Channels I

Towards Efficient Second-Order Power Analysis	1
<i>Jason Waddle, David Wagner</i>	
Correlation Power Analysis with a Leakage Model	16
<i>Eric Brier, Christophe Clavier, Francis Olivier</i>	
Power Analysis of an FPGA (Implementation of Rijndael: Is Pipelining a DPA Countermeasure?)	30
<i>François-Xavier Standaert, Siddika Berna Örs, Bart Preneel</i>	

Modular Multiplication

Long Modular Multiplication for Cryptographic Applications	45
<i>Laszlo Hars</i>	
Leak Resistant Arithmetic	62
<i>Jean-Claude Bajard, Laurent Imbert, Pierre-Yvan Liardet, Yannick Tégia</i>	
Efficient Linear Array for Multiplication in $GF(2^m)$ Using a Normal Basis for Elliptic Curve Cryptography	76
<i>Soonhak Kwon, Kris Gaj, Chang Hoon Kim, Chun Pyo Hong</i>	

Low Resources I

Low-Power Elliptic Curve Cryptography Using Scaled Modular Arithmetic	92
<i>E. Öztürk, B. Sunar, E. Savaş</i>	
A Low-Cost ECC Coprocessor for Smartcards	107
<i>Harald Aigner, Holger Bock, Markus Hütter, Johannes Wolkerstorfer</i>	
Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs	119
<i>Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, Sheueling Chang Shantz</i>	

Implementation Aspects

Instruction Set Extensions for Fast Arithmetic in Finite Fields $GF(p)$ and $GF(2^m)$	133
<i>Johann Großschädl, Erkan Savaş</i>	

Aspects of Hyperelliptic Curves over Large Prime Fields in Software Implementations	148
<i>Roberto Maria Avanzi</i>	

Collision Attacks

A Collision-Attack on AES (Combining Side Channel- and Differential-Attack)	163
<i>Kai Schramm, Gregor Leander, Patrick Felke, Christof Paar</i>	
Enhancing Collision Attacks	176
<i>Hervé Ledig, Frédéric Muller, Frédéric Valette</i>	

Side Channels II

Simple Power Analysis of Unified Code for ECC Double and Add	191
<i>Colin D. Walter</i>	
DPA on n -Bit Sized Boolean and Arithmetic Operations and Its Application to IDEA, RC6, and the HMAC-Construction	205
<i>Kerstin Lemke, Kai Schramm, Christof Paar</i>	
Side-Channel Attacks in ECC: A General Technique for Varying the Parametrization of the Elliptic Curve	220
<i>Loren D. Olson</i>	
Switching Blindings with a View Towards IDEA	230
<i>Olaf Neiß, Jürgen Pulkus</i>	

Fault Attacks

Fault Analysis of Stream Ciphers	240
<i>Jonathan J. Hoch, Adi Shamir</i>	
A Differential Fault Attack Against Early Rounds of (Triple-)DES	254
<i>Ludger Hemme</i>	

Hardware Implementation I

An Offset-Compensated Oscillator-Based Random Bit Source for Security Applications	268
<i>Holger Bock, Marco Bucci, Raimondo Luzzi</i>	
Improving the Security of Dual-Rail Circuits	282
<i>Danil Sokolov, Julian Murphy, Alex Bystrov, Alex Yakovlev</i>	

Side Channels III

A New Attack with Side Channel Leakage During Exponent Recoding Computations	298
<i>Yasuyuki Sakai, Kouichi Sakurai</i>	
Defeating Countermeasures Based on Randomized BSD Representations	312
<i>Pierre-Alain Fouque, Frédéric Muller, Guillaume Poupard, Frédéric Valette</i>	
Pipelined Computation of Scalar Multiplication in Elliptic Curve Cryptosystems	328
<i>Pradeep Kumar Mishra</i>	
Efficient Countermeasures Against RPA, DPA, and SPA	343
<i>Hideyo Mamiya, Atsuko Miyaji, Hiroaki Morimoto</i>	

Low Resources II

Strong Authentication for RFID Systems Using the AES Algorithm	357
<i>Martin Feldhofer, Sandra Dominikus, Johannes Wolkerstorfer</i>	
TTS: High-Speed Signatures on a Low-Cost Smart Card	371
<i>Bo-Yin Yang, Jiun-Ming Chen, Yen-Hung Chen</i>	

Hardware Implementation II

XTR Implementation on Reconfigurable Hardware	386
<i>Eric Peeters, Michael Neve, Mathieu Ciet</i>	
Concurrent Error Detection Schemes for Involution Ciphers	400
<i>Nikhil Joshi, Kaijie Wu, Ramesh Karri</i>	

Authentication and Signatures

Public Key Authentication with One (Online) Single Addition	413
<i>Marc Girault, David Lefranc</i>	
Attacking DSA Under a Repeated Bits Assumption	428
<i>P.J. Leadbitter, D. Page, N.P. Smart</i>	
How to Disembed a Program?	441
<i>Benoît Chevallier-Mames, David Naccache, Pascal Paillier, David Pointcheval</i>	

Author Index	455
--------------------	-----