

Table of Contents

	Page
<u>Invited Talk</u>	
Protecting Embedded Systems – The Next Ten Years 1 <i>R. Anderson</i>	
<u>Side Channel Attacks I</u>	
A Sound Method for Switching between Boolean and Arithmetic Masking ...3 <i>L. Goubin</i>	
Fast Primitives for Internal Data Scrambling in Tamper Resistant Hardware16 <i>E. Brier, H. Handschuh, and C. Tymen</i>	
Random Register Renaming to Foil DPA28 <i>D. May, H.L. Muller, and N.P. Smart</i>	
Randomized Addition-Subtraction Chains as a Countermeasure against Power Attacks39 <i>E. Oswald and M. Aigner</i>	
<u>Rijndael Hardware Implementations</u>	
Architectural Optimization for a 1.82Gbits/sec VLSI Implementation of the AES Rijndael Algorithm 51 <i>H. Kuo and I. Verbauwhede</i>	
High Performance Single-Chip FPGA Rijndael Algorithm65 <i>M. McLoone and J.V. McCanny</i>	
Two Methods of Rijndael Implementation in Reconfigurable Hardware77 <i>V. Fischer and M. Drutarovský</i>	
<u>Random Number Generators</u>	
Pseudo-random Number Generation on the IBM 4758 Secure Crypto Coprocessor93 <i>N. Howgrave-Graham, J. Dyer, and R. Gennaro</i>	
Efficient Online Tests for True Random Number Generators 103 <i>W. Schindler</i>	

Elliptic Curve Algorithms

The Hessian Form of an Elliptic Curve	118
<i>N.P. Smart</i>	
Efficient Elliptic Curve Cryptosystems from a Scalar Multiplication Algorithm with Recovery of the y-Coordinate on a Montgomery-Form Elliptic Curve	126
<i>K. Okeya and K. Sakurai</i>	
Generating Elliptic Curves of Prime Order	142
<i>E. Savaş, T.A. Schmidt, and Ç. K. Koç</i>	

Invited Talk

New Directions in Cryptography	159
<i>A. Shamir</i>	

Arithmetic Architectures

A New Low Complexity Parallel Multiplier for a Class of Finite Fields	160
<i>M. Leone</i>	
Efficient Rijndael Encryption Implementation with Composite Field Arithmetic	171
<i>A. Rudra, P.K. Dubey, C.S. Jutla, V. Kumar, J.R. Rao, and P. Rohatgi</i>	
High-Radix Design of a Scalable Modular Multiplier	185
<i>A.F. Tenca, G. Todorov, and Ç.K. Koç</i>	
A Bit-Serial Unified Multiplier Architecture for Finite Fields $GF(p)$ and $GF(2^m)$	202
<i>J. Großschädl</i>	

Cryptanalysis

Attacks on Cryptoprocessor Transaction Sets	220
<i>M. Bond</i>	
Bandwidth-Optimal Kleptographic Attacks	235
<i>A. Young and M. Yung</i>	
Electromagnetic Analysis: Concrete Results	251
<i>K. Gandolfi, C. Mourtel, and F. Olivier</i>	

Embedded Implementations and New Ciphers

NTRU in Constrained Devices	262
<i>D.V. Bailey, D. Coffin, A. Elbirt, J.H. Silverman,</i> <i>and A.D. Woodbury</i>	
Transparent Harddisk Encryption	273
<i>T. Pornin</i>	

Side Channel Attacks II

Sliding Windows Succumbs to Big Mac Attack	286
<i>C.D. Walter</i>	
Universal Exponentiation Algorithm: A First Step towards <i>Provable</i> SPA-Resistance	300
<i>C. Clavier and M. Joye</i>	
An Implementation of DES and AES, Secure against Some Attacks	309
<i>M. Akkar and C. Giraud</i>	

Hardware Implementations of Ciphers

Efficient Implementation of “Large” Stream Cipher Systems	319
<i>P. Sarkar and S. Maitra</i>	
Tradeoffs in Parallel and Serial Implementations of the International Data Encryption Algorithm IDEA	333
<i>O.Y.H. Cheung, K.H. Tsoi, P.H.W. Leong, and M.P. Leong</i>	
A Scalable $GF(p)$ Elliptic Curve Processor Architecture for Programmable Hardware	348
<i>G. Orlando and C. Paar</i>	
Implementation of RSA Algorithm Based on RNS Montgomery Multiplication	364
<i>H. Nozaki, M. Motoyama, A. Shimbo, and S. Kawamura</i>	

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. Liardet and N.P. Smart

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

Author Index 411

<http://www.springer.com/978-3-540-42521-2>

Cryptographic Hardware and Embedded Systems -
CHES 2001

Third International Workshop, Paris, France, May 14-16,
2001 Proceedings

Koc, C.K.; Nacchae, D.; Paar, C. (Eds.)

2001, XIV, 418 p., Softcover

ISBN: 978-3-540-42521-2