

Table of Contents

Elliptic and Hyperelliptic Curve Arithmetic

Faster Halvings in Genus 2	1
<i>Peter Birkner and Nicolas Thériault</i>	
Efficient Pairing Computation on Genus 2 Curves in Projective Coordinates	18
<i>Xinxin Fan, Guang Gong, and David Jao</i>	
On Software Parallel Implementation of Cryptographic Pairings	35
<i>Philipp Grabher, Johann Großschädl, and Dan Page</i>	

Block Ciphers I

The Cryptanalysis of Reduced-Round SMS4	51
<i>Jonathan Etrog and Matt J.B. Robshaw</i>	
Building Secure Block Ciphers on Generic Attacks Assumptions	66
<i>Jacques Patarin and Yannick Seurin</i>	

First Invited Talk

Lifting and Elliptic Curve Discrete Logarithms	82
<i>Joseph H. Silverman</i>	

Hash Functions I

Preimage Attacks on One-Block MD4, 63-Step MD5 and More	103
<i>Kazumaro Aoki and Yu Sasaki</i>	
Preimage Attacks on 3-Pass HAVAL and Step-Reduced MD5	120
<i>Jean-Philippe Aumasson, Willi Meier, and Florian Mendel</i>	
Cryptanalysis of Tweaked Versions of SMASH and Reparation	136
<i>Pierre-Alain Fouque, Jacques Stern, and Sébastien Zimmer</i>	

Mathematical Aspects of Applied Cryptography I

Counting Functions for the k -Error Linear Complexity of 2^n -Periodic Binary Sequences	151
<i>Ramakanth Kavuluru and Andrew Klapper</i>	
On the Exact Success Rate of Side Channel Analysis in the Gaussian Model	165
<i>Matthieu Rivain</i>	

Stream Ciphers Cryptanalysis

Algebraic and Correlation Attacks against Linearly Filtered Non Linear Feedback Shift Registers	184
<i>Côme Berbain, Henri Gilbert, and Antoine Joux</i>	
A Cache Timing Analysis of HC-256	199
<i>Erik Zenner</i>	
An Improved Fast Correlation Attack on Stream Ciphers	214
<i>Bin Zhang and Dengguo Feng</i>	

Hash Functions II

A Three-Property-Secure Hash Function	228
<i>Elena Andreeva and Bart Preneel</i>	
Analysis of the Collision Resistance of RadioGatún Using Algebraic Techniques	245
<i>Charles Bouillaguet and Pierre-Alain Fouque</i>	
A Scheme to Base a Hash Function on a Block Cipher	262
<i>Shoichi Hirose and Hidenori Kuwakado</i>	
Collisions and Other Non-random Properties for Step-Reduced SHA-256	276
<i>Sebastian Indesteege, Florian Mendel, Bart Preneel, and Christian Rechberger</i>	

Cryptography with Algebraic Curves

Public Verifiability from Pairings in Secret Sharing Schemes	294
<i>Somayeh Heidarvand and Jorge L. Villar</i>	

The Elliptic Curve Discrete Logarithm Problem and Equivalent Hard Problems for Elliptic Divisibility Sequences	309
<i>Kristin E. Lauter and Katherine E. Stange</i>	

Second Invited Talk – Stafford Tavares Lecture

The “Coefficients H” Technique	328
<i>Jacques Patarin</i>	

Mathematical Aspects of Applied Cryptography II

Distinguishing Multiplications from Squaring Operations	346
<i>Frederic Amiel, Benoit Feix, Michael Tunstall, Claire Whelan, and William P. Marnane</i>	
Subquadratic Polynomial Multiplication over $GF(2^m)$ Using Trinomial Bases and Chinese Remaindering	361
<i>Éric Schost and Arash Hariri</i>	
Bounds on Fixed Input/Output Length Post-processing Functions for Biased Physical Random Number Generators	373
<i>Kyohei Suzuki and Tetsu Iwata</i>	

Curve-Based Primitives in Hardware

HECC Goes Embedded: An Area-Efficient Implementation of HECC . . .	387
<i>Junfeng Fan, Lejla Batina, and Ingrid Verbauwhede</i>	
ECC Is Ready for RFID – A Proof in Silicon	401
<i>Daniel Hein, Johannes Wolkerstorfer, and Norbert Felber</i>	

Block Ciphers II

Cryptanalysis of a Generic Class of White-Box Implementations	414
<i>Wil Michiels, Paul Gorissen, and Henk D.L. Hollmann</i>	
New Linear Cryptanalytic Results of Reduced-Round of CAST-128 and CAST-256	429
<i>Meiqin Wang, Xiaoyun Wang, and Changhui Hu</i>	
Improved Impossible Differential Cryptanalysis of Reduced-Round Camellia	442
<i>Wenling Wu, Lei Zhang, and Wentao Zhang</i>	
Author Index	457