Table of Contents

Selected Areas in Cryptography 2011

Cryptanalysis of Hash Functions

Boomerang Distinguishers on MD4-Family — First Practical Results on Full 5-Pass HAVAL 1
Yu Sasaki

Improved Analysis of ECHO-256 19
Jérémy Jean, María Naya-Plasencia, and Martin Schläffer

Provable Chosen-Target-Forced-Midfix Preimage Resistance 37
Elena Andreeva and Bart Mennink

Security in Clouds

On CCA-Secure Somewhat Homomorphic Encryption 55
Jake Loftus, Alexander May, Nigel P. Smart, and Frederik Vercauteren

Efficient Schemes for Anonymous Yet Authorized and Bounded Use of Cloud Resources 73
Daniel Slamanig

Invited Paper I

Group Law Computations on Jacobians of Hyperelliptic Curves 92
Craig Costello and Kristin Lauter

Bits and Randomness

Cryptographic Analysis of All 4×4-Bit S-Boxes 118
Markku-Juhani O. Saarinen

The Cryptographic Power of Random Selection 134
Matthias Krause and Matthias Hamann

Proof of Empirical RC4 Biases and New Key Correlations 151
Sourav Sen Gupta, Subhamoy Maitra, Goutam Paul, and Santanu Sarkar

Cryptanalysis of Ciphers I

Combined Differential and Linear Cryptanalysis of Reduced-Round PRINTCIPHER 169
Ferhat Karakoç, Hüseyin Demirci, and A. Emre Harmancı

Practical Attack on the Full MMB Block Cipher 185
Keting Jia, Jiazhe Chen, Meiqin Wang, and Xiaoyun Wang

Conditional Differential Cryptanalysis of Trivium and KATAN 200
Simon Knellwolf, Willi Meier, and María Naya-Plasencia

Cryptanalysis of Ciphers II

Some Instant- and Practical-Time Related-Key Attacks on KTANTAN32/48/64 213
Martin Ågren

Analysis of the Initial and Modified Versions of the Candidate 3GPP Integrity Algorithm 128-EIA3 230
Thomas Fuhr, Henri Gilbert, Jean-René Reinhard, and Marion Videau

New Insights on Impossible Differential Cryptanalysis 243
Charles Bouillaguet, Orr Dunkelman, Pierre-Alain Fouque, and Gaëtan Leurent

Cryptanalysis of Public-Key Cryptography

A Unified Framework for Small Secret Exponent Attack on RSA 260
Noboru Kunihiro, Naoyuki Shinohara, and Tetsuya Izu

Cipher Implementation

Very Compact Hardware Implementations of the Blockcipher CLEFIA 278
Toru Akishita and Harunaga Hiwatari

Invited Paper II

Another Look at Tightness 293
Sanjit Chatterjee, Alfred Menezes, and Palash Sarkar

New Designs

Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications 320
Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche

Blockcipher-Based Double-Length Hash Functions for Pseudorandom Oracles 338
Yusuke Naito

ASC-1: An Authenticated Encryption Stream Cipher 356
Goce Jakimoski and Samant Khajuria

Mathematical Aspects of Applied Cryptography

On Various Families of Twisted Jacobi Quartics 373
Jérôme Plût

Improved Three-Way Split Formulas for Binary Polynomial Multiplication 384
Murat Cenk, Christophe Negre, and M. Anwar Hasan

Sublinear Scalar Multiplication on Hyperelliptic Koblitz Curves 399
Hugo Labrande and Michael J. Jacobson Jr.

Faster Hashing to $\mathbb{G}_2$ 412
Laura Fuentes-Castañeda, Edward Knapp, and Francisco Rodríguez-Henríquez

Author Index 431