

# Table of Contents

## Tutorial 1

Tor and the Censorship Arms Race: Lessons Learned (Abstract) .....	1
<i>Roger Dingledine</i>	

## Tutorial 2

Elliptic Curves for Applications (Abstract) .....	2
<i>Tanja Lange</i>	

## Side-Channel Attacks

PKDPA: An Enhanced Probabilistic Differential Power Attack Methodology .....	3
<i>Dhiman Saha, Debdeep Mukhopadhyay, and Dipanwita RoyChowdhury</i>	

Formal Analysis of the Entropy / Security Trade-off in First-Order Masking Countermeasures against Side-Channel Attacks .....	22
<i>Maxime Nassar, Sylvain Guilley, and Jean-Luc Danger</i>	

Square Always Exponentiation .....	40
<i>Christophe Clavier, Benoit Feix, Georges Gagnerot, Mylène Roussellet, and Vincent Verneuil</i>	

An Enhanced Differential Cache Attack on CLEFIA for Large Cache Lines .....	58
<i>Chester Rebeiro, Rishabh Poddar, Amit Datta, and Debdeep Mukhopadhyay</i>	

Partial Key Exposure: Generalized Framework to Attack RSA .....	76
<i>Santanu Sarkar</i>	

## Invited Talk 1

The Yin and Yang Sides of Embedded Security (Abstract) .....	93
<i>Christof Paar</i>	

# Secret-Key Cryptography, Part 1

Mars Attacks! Revisited: Differential Attack on 12 Rounds of the MARS Core and Defeating the Complex MARS Key-Schedule . . . . .	94
<i>Michael Gorski, Thomas Knapke, Eik List, Stefan Lucks, and Jakob Wenzel</i>	
Linear Cryptanalysis of PRINTCIPHER–Trails and Samples Everywhere . . . . .	114
<i>Martin Ågren and Thomas Johansson</i>	
Practical Attack on 8 Rounds of the Lightweight Block Cipher KLEIN . . . . .	134
<i>Jean-Philippe Aumasson, María Naya-Plasencia, and Markku-Juhani O. Saarinen</i>	
On Related-Key Attacks and KASUMI: The Case of A5/3 . . . . .	146
<i>Phuong Ha Nguyen, Matthew J.B. Robshaw, and Huaxiong Wang</i>	

# Invited Talk 2

Cryptology: Where Is the New Frontier? (Abstract) . . . . .	160
<i>Ross Anderson</i>	

# Secret-Key Cryptography, Part 2

Analysis of the Parallel Distinguished Point Tradeoff . . . . .	161
<i>Jin Hong, Ga Won Lee, and Daegun Ma</i>	
On the Evolution of GGHN Cipher . . . . .	181
<i>Subhadeep Banik, Subhamoy Maitra, and Santanu Sarkar</i>	
HiPAcc-LTE: An Integrated High Performance Accelerator for 3GPP LTE Stream Ciphers . . . . .	196
<i>Sourav Sen Gupta, Anupam Chattopadhyay, and Ayesha Khalid</i>	
Addressing Flaws in RFID Authentication Protocols . . . . .	216
<i>Mohammad Hassan Habibi, Mohammad Reza Aref, and Di Ma</i>	

# Hash Functions

Practical Analysis of Reduced-Round KECCAK . . . . .	236
<i>María Naya-Plasencia, Andrea Röck, and Willi Meier</i>	
Boomerang Distinguisher for the SIMD-512 Compression Function . . . . .	255
<i>Florian Mendel and Tomislav Nad</i>	

Lightweight Implementations of SHA-3 Candidates on FPGAs . . . . .	270
<i>Jens-Peter Kaps, Panasayya Yalla, Kishore Kumar Surapathi, Bilal Habib, Susheel Vadlamudi, Smriti Gurung, and John Pham</i>	

## Pairings

Publicly Verifiable Secret Sharing for Cloud-Based Key Management . . .	290
<i>Roy D'Souza, David Jao, Ilya Mironov, and Omkant Pandey</i>	
On Constructing Families of Pairing-Friendly Elliptic Curves with Variable Discriminant . . . . .	310
<i>Robert Drylo</i>	
Attractive Subfamilies of BLS Curves for Implementing High-Security Pairings . . . . .	320
<i>Craig Costello, Kristin Lauter, and Michael Naehrig</i>	

## Invited Talk 3

Stone Knives and Bear Skins: Why Does the Internet Run on Pre-historic Cryptography? (Abstract) . . . . .	343
<i>Eric Rescorla</i>	

## Protocols

The Limits of Common Coins: Further Results . . . . .	344
<i>Hemanta K. Maji and Manoj Prabhakaran</i>	
Secure Message Transmission in Asynchronous Directed Graphs . . . . .	359
<i>Shashank Agrawal, Abhinav Mehta, and Kannan Srinathan</i>	
Towards a Provably Secure DoS-Resilient Key Exchange Protocol with Perfect Forward Secrecy . . . . .	379
<i>Lakshmi Kuppusamy, Jothi Rangasamy, Douglas Stebila, Colin Boyd, and Juan Gonzalez Nieto</i>	

## Tutorial 3

Software Optimizations for Cryptographic Primitives on General Purpose x86_64 Platforms . . . . .	399
<i>Shay Gueron</i>	

Author Index . . . . .	401
------------------------	-----