

Table of Contents

Invited Talk

The First 30 Years of Cryptographic Hash Functions and the NIST SHA-3 Competition	1
<i>Bart Preneel</i>	

Public-Key Cryptography

Errors Matter: Breaking RSA-Based PIN Encryption with Thirty Ciphertext Validity Queries	15
<i>Nigel P. Smart</i>	
Efficient CRT-RSA Decryption for Small Encryption Exponents	26
<i>Subhamoy Maitra and Santanu Sarkar</i>	
Resettable Public-Key Encryption: How to Encrypt on a Virtual Machine	41
<i>Scott Yilek</i>	
Plaintext-Awareness of Hybrid Encryption	57
<i>Shaoquan Jiang and Huaxiong Wang</i>	
Speed Records for NTRU	73
<i>Jens Hermans, Frederik Vercauteren, and Bart Preneel</i>	
High-Speed Parallel Software Implementation of the η_T Pairing	89
<i>Diego F. Aranha, Julio López, and Darrel Hankerson</i>	
Refinement of Miller's Algorithm Over Edwards Curves	106
<i>Lei Xu and Dongdai Lin</i>	
Probabilistic Public Key Encryption with Equality Test	119
<i>Guomin Yang, Chik How Tan, Qiong Huang, and Duncan S. Wong</i>	
Efficient CCA-Secure PKE from Identity-Based Techniques	132
<i>Junzuo Lai, Robert H. Deng, Shengli Liu, and Weidong Kou</i>	
Anonymity from Asymmetry: New Constructions for Anonymous HIBE	148
<i>Léo Ducas</i>	
Making the Diffie-Hellman Protocol Identity-Based	165
<i>Dario Fiore and Rosario Gennaro</i>	

On Extended Sanitizable Signature Schemes	179
<i>Sébastien Canard and Amandine Jambert</i>	

Side-Channel Attacks

Unrolling Cryptographic Circuits: A Simple Countermeasure Against Side-Channel Attacks	195
<i>Shivam Bhasin, Sylvain Guilley, Laurent Sauvage, and Jean-Luc Danger</i>	
Fault Attacks Against EMV Signatures	208
<i>Jean-Sébastien Coron, David Naccache, and Mehdi Tibouchi</i>	
Revisiting Higher-Order DPA Attacks: Multivariate Mutual Information Analysis	221
<i>Benedikt Gierlichs, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede</i>	
Differential Cache-Collision Timing Attacks on AES with Applications to Embedded CPUs	235
<i>Andrey Bogdanov, Thomas Eisenbarth, Christof Paar, and Malte Wienecke</i>	

Cryptographic Protocols

Usable Optimistic Fair Exchange	252
<i>Alptekin Küpçü and Anna Lysyanskaya</i>	
Hash Function Combiners in TLS and SSL	268
<i>Marc Fischlin, Anja Lehmann, and Daniel Wagner</i>	
Improving Efficiency of an ‘On the Fly’ Identification Scheme by Perfecting Zero-Knowledgeness	284
<i>Bagus Santoso, Kazuo Ohta, Kazuo Sakiyama, and Goichiro Hanaoka</i>	

Cryptanalysis

Linear Cryptanalysis of Reduced-Round PRESENT	302
<i>Joo Yeon Cho</i>	
Dependent Linear Approximations: The Algorithm of Biryukov and Others Revisited	318
<i>Mia Hermelin and Kaisa Nyberg</i>	
Practical Key Recovery Attack against Secret-IV Edon- <i>R</i>	334
<i>Gaëtan Leurent</i>	

Rebound Attacks on the Reduced Grøstl Hash Function 350
*Florian Mendel, Christian Rechberger, Martin Schläffer, and
Søren S. Thomsen*

Symmetric Cryptography

The Sum of CBC MACs Is a Secure PRF 366
Kan Yasuda

On Fast Verification of Hash Chains 382
Dae Hyun Yum, Jin Seok Kim, Pil Joong Lee, and Sung Je Hong

Author Index 397