

Table of Contents

New Cryptosystems

Faster Generation of NICE-Schnorr-Type Signatures	1
<i>Detlef Hühnlein (secunet Security Networks AG)</i>	
New Key Agreement Protocols in Braid Group Cryptography	13
<i>Iris Anshel (Arithmetica Inc.), Michael Anshel (City College of New York), Benji Fisher (Boston College), Dorian Goldfeld (Columbia University)</i>	

RSA

Improving SSL Handshake Performance via Batching	28
<i>Hovav Shacham (Stanford University), Dan Boneh (Stanford University)</i>	
From Fixed-Length Messages to Arbitrary-Length Messages Practical RSA Signature Padding Schemes	44
<i>Geneviève Arboit (McGill University), Jean-Marc Robert (Gemplus Card International)</i>	
An Advantage of Low-Exponent RSA with Modulus Primes Sharing Least Significant Bits	52
<i>Ron Steinfeld (Monash University), Yuliang Zheng (Monash University)</i>	

Symmetric Cryptography

On the Strength of Simply-Iterated Feistel Ciphers with Whitening Keys ..	63
<i>Paul Onions (Silicon Infusion Ltd.)</i>	
Analysis of SHA-1 in Encryption Mode	70
<i>Helena Handschuh (Gemplus Card International), Lars R. Knudsen (University of Bergen), Matthew J. Robshaw (ISG, Royal Holloway)</i>	
Fast Implementation and Fair Comparison of the Final Candidates for Advanced Encryption Standard Using Field Programmable Gate Arrays ..	84
<i>Kris Gaj (George Mason University), Pawel Chodowicz (George Mason University)</i>	

Gambling and Lotteries

Fair e-Lotteries and e-Casinos	100
<i>Eyal Kushilevitz (Department of Computer Science, Technion), Tal Rabin (IBM T.J. Watson Research Center)</i>	
Secure Mobile Gambling	110
<i>Markus Jakobsson (Bell Laboratories, Lucent Technologies), David Pointcheval (ENS – CNRS), Adam Young (Lockheed Martin)</i>	

Reductions, Constructions and Security Proofs

Formal Security Proofs for a Signature Scheme with Partial Message Recovery	126
<i>Daniel R.L. Brown (Certicom Research), Don B. Johnson (Certicom Research)</i>	
The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES	143
<i>Michel Abdalla (University of California, San Diego), Mihir Bellare (University of California, San Diego), Phillip Rogaway (University of California, Davis)</i>	
REACT: Rapid Enhanced-Security Asymmetric Cryptosystem Transform .	159
<i>Tatsuaki Okamoto (NTT Labs), David Pointcheval (ENS – CNRS)</i>	

Flaws and Attacks

Security Weaknesses in Bluetooth	176
<i>Markus Jakobsson (Bell Laboratories, Lucent Technologies), Susanne Wetzel (Bell Laboratories, Lucent Technologies)</i>	
Distinguishing Exponent Digits by Observing Modular Subtractions	192
<i>Colin D. Walter (Datacard platform⁷ seven, UMIST Manchester), Susan Thompson (Datacard platform⁷ seven)</i>	
On the Power of Misbehaving Adversaries and Security Analysis of the Original EPOC	208
<i>Marc Joye (Gemplus Card International), Jean-Jacques Quisquater (UCL Crypto Group), Moti Yung (CertCo)</i>	

Implementation

Modular Exponentiation on Fine-Grained FPGA	223
<i>Alexander Tiountchik (National Academy of Sciences of Belarus), Elena Trichina (PACT Informationstechnologie)</i>	

Scalable Algorithm for Montgomery Multiplication and Its Implementation on the Coarse-Grain Reconfigurable Chip	235
<i>Elena Trichina (PACT Informationstechnologie), Alexander Tiountchik (National Academy of Sciences of Belarus)</i>	

Software Implementation of the NIST Elliptic Curves Over Prime Fields ..	250
<i>Michael Brown (University of Waterloo), Darrel Hankerson (Auburn University, Certicom Research), Julio López (University of Valle), Alfred Menezes (University of Waterloo, Certicom Research)</i>	

Multivariate Cryptography

The Security of Hidden Field Equations (HFE)	266
<i>Nicolas T. Courtois (Université de Toulon et du Var)</i>	

QUARTZ, 128-Bit Long Digital Signatures	282
<i>Jacques Patarin (Bull CP8), Nicolas Courtois (Bull CP8), Louis Goubin (Bull CP8)</i>	

FLASH, a Fast Multivariate Signature Algorithm	298
<i>Jacques Patarin (Bull CP8), Nicolas Courtois (Bull CP8), Louis Goubin (Bull CP8)</i>	

Number Theoretic Problems

Analysis of the Weil Descent Attack of Gaudry, Hess and Smart	308
<i>Alfred Menezes (University of Waterloo, Certicom Research), Minghua Qu (Certicom Research)</i>	

Using Fewer Qubits in Shor's Factorization Algorithm via Simultaneous Diophantine Approximation	319
<i>Jean-Pierre Seifert (Infineon Technologies)</i>	

Passwords and Credentials

Relying Party Credentials Framework	328
<i>Amir Herzberg (NewGenPay Inc.), Yosi Mass (IBM Haifa Research Lab)</i>	

Password Authentication Using Multiple Servers	344
<i>David P. Jablon (Integrity Sciences, Inc.)</i>	

More Efficient Password-Authenticated Key Exchange	361
<i>Philip MacKenzie (Bell Laboratories, Lucent Technologies)</i>	

Protocols I

Improved Boneh-Shaw Content Fingerprinting	378
<i>Yacov Yacobi (Microsoft Research)</i>	

Efficient Asymmetric Public-Key Traitor Tracing without Trusted Agents . 392
 Yuji Watanabe (IIS, University of Tokyo), Goichiro Hanaoka
 (IIS, University of Tokyo), Hideki Imai (IIS, University of Tokyo)

Targeted Advertising ... And Privacy Too 408
 Ari Juels (RSA Laboratories)

Protocols II

Uncheatable Distributed Computations 425
 Philippe Golle (Stanford University), Ilya Mironov
 (Stanford University)

Forward-Secure Threshold Signature Schemes..... 441
 Michel Abdalla (University of California, San Diego), Sara Miner
 (University of California, San Diego), Chanathip Namprempre
 (University of California, San Diego)

A Cost-Effective Pay-Per-Multiplication Comparison Method for
Millionaires 457
 Marc Fischlin (Johann Wolfgang Goethe-Universität
 Frankfurt am Main)

Author Index 473