

# Table of Contents

## Invited Talks

Sub-linear Queries Statistical Databases: Privacy with Power .....	1
<i>Cynthia Dwork</i>	
Malicious Cryptography: Kleptographic Aspects .....	7
<i>Adam Young and Moti Yung</i>	

## Cryptanalysis

Resistance of SNOW 2.0 Against Algebraic Attacks .....	19
<i>Olivier Billet and Henri Gilbert</i>	
A Study of the Security of Unbalanced Oil and Vinegar Signature Schemes .....	29
<i>An Braeken, Christopher Wolf, and Bart Preneel</i>	
Hold Your Sessions: An Attack on Java Session-Id Generation .....	44
<i>Zvi Gutterman and Dahlia Malkhi</i>	
Update on SHA-1 .....	58
<i>Vincent Rijmen and Elisabeth Oswald</i>	
A Fast Correlation Attack on the Shrinking Generator .....	72
<i>Bin Zhang, Hongjun Wu, Dengguo Feng, and Feng Bao</i>	

## Public-Key Encryption

Improved Efficiency for CCA-Secure Cryptosystems Built Using Identity-Based Encryption .....	87
<i>Dan Boneh and Jonathan Katz</i>	
A Generic Conversion with Optimal Redundancy .....	104
<i>Yang Cui, Kazukuni Kobara, and Hideki Imai</i>	
Choosing Parameter Sets for NTRUEncrypt with NAEP and SVES-3 .....	118
<i>Nick Howgrave-Graham, Joseph H. Silverman, and William Whyte</i>	

## Signature Schemes

Foundations of Group Signatures: The Case of Dynamic Groups .....	136
<i>Mihir Bellare, Haixia Shi, and Chong Zhang</i>	
Time-Selective Convertible Undeniable Signatures .....	154
<i>Fabien Laguillaumie and Damien Vergnaud</i>	

## Design Principles

On Tolerant Cryptographic Constructions . . . . .	172
<i>Amir Herzberg</i>	

## Password-Based Protocols

Simple Password-Based Encrypted Key Exchange Protocols . . . . .	191
<i>Michel Abdalla and David Pointcheval</i>	
Hard Bits of the Discrete Log with Applications to Password Authentication . . . . .	209
<i>Philip Mackenzie and Sarvar Patel</i>	
Proofs for Two-Server Password Authentication . . . . .	227
<i>Michael Szydlo and Burton Kaliski</i>	
Design and Analysis of Password-Based Key Derivation Functions . . . . .	245
<i>Frances F. Yao and Yiqun Lisa Yin</i>	

## Pairings

A New Two-Party Identity-Based Authenticated Key Agreement . . . . .	262
<i>Noel McCullagh and Paulo S.L.M. Barreto</i>	
Accumulators from Bilinear Pairings and Applications . . . . .	275
<i>Lan Nguyen</i>	
Computing the Tate Pairing . . . . .	293
<i>Michael Scott</i>	
Fast and Proven Secure Blind Identity-Based Signcryption from Pairings . .	305
<i>Tsz Hon Yuen and Victor K. Wei</i>	

## Efficient and Secure Implementation

A Systematic Evaluation of Compact Hardware Implementations for the Rijndael S-Box . . . . .	323
<i>Nele Mentens, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede</i>	
CryptoGraphics: Secret Key Cryptography Using Graphics Cards . . . . .	334
<i>Debra L. Cook, John Ioannidis, Angelos D. Keromytis, and Jake Luck</i>	
Side-Channel Leakage of Masked CMOS Gates . . . . .	351
<i>Stefan Mangard, Thomas Popp, and Berndt M. Gammel</i>	
New Minimal Weight Representations for Left-to-Right Window Methods .	366
<i>James A. Muir and Douglas R. Stinson</i>	

<b>Author Index</b> . . . . .	385
-------------------------------	-----

<http://www.springer.com/978-3-540-24399-1>

Topics in Cryptology -- CT-RSA 2005

The Cryptographers' Track at the RSA Conference

2005, San Francisco, CA, USA, February 14-18, 2005,

Proceedings

Menezes, A.J. (Ed.)

2005, X, 390 p., Softcover

ISBN: 978-3-540-24399-1