

Table of Contents

Invited Talks

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

Cryptanalysis

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

Public-Key Encryption

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

Signature Schemes

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

Design Principles

On Tolerant Cryptographic Constructions 172
Amir Herzberg

Password-Based Protocols

Simple Password-Based Encrypted Key Exchange Protocols 191
Michel Abdalla and David Pointcheval

Hard Bits of the Discrete Log with Applications
to Password Authentication 209
Philip Mackenzie and Sarvar Patel

Proofs for Two-Server Password Authentication 227
Michael Szydlo and Burton Kaliski

Design and Analysis of Password-Based Key Derivation Functions 245
Frances F. Yao and Yiqun Lisa Yin

Pairings

A New Two-Party Identity-Based Authenticated Key Agreement 262
Noel McCullagh and Paulo S.L.M. Barreto

Accumulators from Bilinear Pairings and Applications 275
Lan Nguyen

Computing the Tate Pairing 293
Michael Scott

Fast and Proven Secure Blind Identity-Based Signcryption from Pairings . . 305
Tsz Hon Yuen and Victor K. Wei

Efficient and Secure Implementation

A Systematic Evaluation of Compact Hardware Implementations
for the Rijndael S-Box 323
Nele Mentens, Lejla Batina, Bart Preneel, and Ingrid Verbauwhede

CryptoGraphics: Secret Key Cryptography Using Graphics Cards 334
Debra L. Cook, John Ioannidis, Angelos D. Keromytis, and Jake Luck

Side-Channel Leakage of Masked CMOS Gates 351
Stefan Mangard, Thomas Popp, and Berndt M. Gammel

New Minimal Weight Representations for Left-to-Right Window Methods . 366
James A. Muir and Douglas R. Stinson

Author Index 385