# Table of Contents

## Invited Talk I

Bilinear Groups of Composite Order .................................................. 1  
_Dan Boneh_

## Applications

Public Key Encryption with Conjunctive Keyword Search and Its  
Extension to a Multi-user System .................................................... 2  
_Yong Ho Hwang and Pil Joong Lee_

Practical Time Capsule Signatures in the Standard Model from Bilinear  
Maps ...................................................................................................... 23  
_Benoît Libert and Jean-Jacques Quisquater_

Fully Collusion Secure Dynamic Broadcast Encryption with  
Constant-Size Ciphertexts or Decryption Keys ..................................... 39  
_Cécile Delerablee, Pascal Paillier, and David Pointcheval_

## Certificateless Public Key Encryption

Certificateless Public Key Encryption in the Selective-ID Security  
Model ...................................................................................................... 60  
_Jong Hwan Park, Kyu Young Choi, Jung Yeon Hwang, and  
Dong Hoon Lee_

General and Efficient Certificateless Public Key Encryption  
Constructions .......................................................................................... 83  
_Zhaohui Cheng, Liqun Chen, Li Ling, and Richard Comley_

## Invited Talk II

Hyperelliptic Pairings ................................................................. 108  
_Steven D. Galbraith, Florian Hess, and Frederik Vercauteren_

## Hyperelliptic Curves

Zeta Function and Cryptographic Exponent of Supersingular Curves of  
Genus 2 .................................................................................................. 132  
_Gabriel Cardona and Enric Nart_
Constructing Pairing-Friendly Genus 2 Curves with Ordinary Jacobians .................................................. 152

David Freeman

Invited Talk III

Implementing Cryptographic Pairings ................................. 177

Michael Scott

Implementation

Implementing Cryptographic Pairings over Barreto-Naehrig Curves .... 197

Augusto Jun Devegili, Michael Scott, and Ricardo Dahab

Instruction Set Extensions for Pairing-Based Cryptography .......... 208

Tobias Vejda, Dan Page, and Johann Großschädl

The Importance of the Final Exponentiation in Pairings When Considering Fault Attacks ............................. 225

Claire Whelan and Michael Scott

Protocol I

Proxy Re-encryption Systems for Identity-Based Encryption ......... 247

Toshihiko Matsuo

Fair Blind Signatures Revisited .......................................... 268

Emeline Hufschmitt and Jacques Traoré

Invited Talk IV

Supersingular Elliptic Curves in Cryptography .......................... 293

Alfred Menezes

Analysis

On the Minimal Embedding Field ....................................... 294

Laura Hitt

Remarks on Cheon’s Algorithms for Pairing-Related Problems ....... 302

Shunji Kozaki, Taketeru Kutsuna, and Kazuto Matsuo

Invited Talk V

On Pairing Inversion Problems ........................................... 317

Takakazu Satoh
Algorithms

The Tate Pairing Via Elliptic Nets .......................... 329
Katherine E. Stange

Eta Pairing Computation on General Divisors over Hyperelliptic Curves $y^2 = x^7 - x \pm 1$ .......................................................... 349
Eunjeong Lee, Hyang-Sook Lee, and Yoonjin Lee

Protocol II

Provably Secure Pairing-Based Convertible Undeniable Signature with Short Signature Length ......................................................... 367
Xinyi Huang, Yi Mu, Willy Susilo, and Wei Wu

Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key ........................................... 392
Fuchun Guo, Yi Mu, and Zhide Chen

Author Index ........................................................................... 407