Table of Contents

Efficient Software Implementation

An Analysis of Affine Coordinates for Pairing Computation 1
Kristin Lauter, Peter L. Montgomery, and Michael Naehrig

High-Speed Software Implementation of the Optimal Ate Pairing over Barreto–Naehrig Curves 21
Jean-Luc Beuchat, Jorge E. González-Díaz, Shigeo Mitsunari, Eiji Okamoto, Francisco Rodríguez-Henríquez, and Tadanori Teruya

Invited Talk 1

Some Security Topics with Possible Applications for Pairing-Based Cryptography (Abstract) 40
Gene Tsudik

Digital Signatures

A New Construction of Designated Confirmer Signature and Its Application to Optimistic Fair Exchange 41
Qiong Huang, Duncan S. Wong, and Willy Susilo

Anonymizable Signature and Its Construction from Pairings 62
Fumitaka Hoshino, Tetsutaro Kobayashi, and Koutarou Suzuki

Identification of Multiple Invalid Pairing-Based Signatures in Constrained Batches 78
Brian J. Matt

Cryptographic Protocols

Oblivious Transfer with Access Control: Realizing Disjunction without Duplication 96
Ye Zhang, Man Ho Au, Duncan S. Wong, Qiong Huang, Nikos Mamoulis, David W. Cheung, and Siu-Ming Yiu

Increased Resilience in Threshold Cryptography: Sharing a Secret with Devices That Cannot Store Shares 116
Koen Simoens, Roel Peeters, and Bart Preneel

Shorter Verifier-Local Revocation Group Signature with Backward Unlinkability 136
Lingbo Wei and Jianwei Liu

Key Agreement

Strongly Secure Two-Pass Attribute-Based Authenticated Key Exchange 147
Kazuki Yoneyama

Constructing Certificateless Encryption and ID-Based Encryption from ID-Based Key Agreement 167
Dario Fiore, Rosario Gennaro, and Nigel P. Smart

Ephemeral Key Leakage Resilient and Efficient ID-AKEs That Can Share Identities, Private and Master Keys 187
Atsushi Fujioka, Koutarou Suzuki, and Berkant Ustaoğlu

Invited Talk 2

Pairing-Based Non-interactive Zero-Knowledge Proofs (Abstract) 206
Jens Groth

Applications: Code Generation, Time-Released Encryption, Cloud Computing

Designing a Code Generator for Pairing Based Cryptographic Functions 207
Luis J. Dominguez Perez and Michael Scott

Efficient Generic Constructions of Timed-Release Encryption with Pre-open Capability 225
Takahiro Matsuda, Yasumasa Nakai, and Kanta Matsuura

Optimal Authenticated Data Structures with Multilinear Forms 246
Charalampos Papamanthou, Roberto Tamassia, and Nikos Triandopoulos

Point Encoding and Pairing-Friendly Curves

Deterministic Encoding and Hashing to Odd Hyperelliptic Curves 265
Pierre-Alain Fouque and Mehdi Tibouchi

Encoding Points on Hyperelliptic Curves over Finite Fields in Deterministic Polynomial Time 278
Jean-Gabriel Kammerer, Reynald Lercier, and Guénaël Renault

A New Method for Constructing Pairing-Friendly Abelian Surfaces 298
Robert Dryło

Generating More Kawazoe-Takahashi Genus 2 Pairing-Friendly Hyperelliptic Curves 312
Ezekiel J. Kachisa

ID-Based Encryption Schemes

New Identity-Based Proxy Re-encryption Schemes to Prevent Collusion Attacks 327
Lihua Wang, Licheng Wang, Masahiro Mambo, and Eiji Okamoto

Fully Secure Anonymous HIBE and Secret-Key Anonymous IBE with Short Ciphertexts 347
Angelo De Caro, Vincenzo Iovino, and Giuseppe Persiano

Chosen-Ciphertext Secure Identity-Based Encryption from Computational Bilinear Diffie-Hellman 367
David Galindo

Invited Talk 3

A Survey of Local and Global Pairings on Elliptic Curves and Abelian Varieties 377
Joseph H. Silverman

Efficient Hardware, FPGAs, and Algorithms

Compact Hardware for Computing the Tate Pairing over 128-Bit-Security Supersingular Curves 397
Nicolas Estibals

A Variant of Miller's Formula and Algorithm 417
John Boxall, Nadia El Mrabet, Fabien Laguillaumie, and Duc-Phong Le

Pairing Computation on Elliptic Curves with Efficiently Computable Endomorphism and Small Embedding Degree 435
Sorina Ionica and Antoine Joux

High Speed Flexible Pairing Cryptoprocessor on FPGA Platform 450
Santosh Ghosh, Debdeep Mukhopadhyay, and Dipanwita Roychowdhury

Author Index 467