
Technical Program of Asiacrypt 2007

December 3rd (Monday)

[Session 1. Number Theory and Elliptic Curve]
9:00-10:15

A Kilobit Special Number Field Sieve Factorization,
Kazumaro Aoki (NTT)
Jens Franke (University of Bonn, Department of Mathematics)
Thorsten Kleinjung (University of Bonn, Department of Mathematics)
Arjen K. Lenstra (EPFL and Bell Laboratories)
Dag Arne Osvik (EPFL)

When e-th Roots Become Easier Than Factoring,
Antoine Joux (DGA and Université de Versailles)
David Naccache (Ecole normale supérieure)
Emmanuel Thomé (INRIA Lorraine, LORIA)

Faster Addition and Doubling on Elliptic Curves,
Daniel J. Bernstein (University of Illinois at Chicago, USA)
Tanja Lange (Technische Universiteit Eindhoven, Netherlands)

[Session 2. Protocol]
10:40-11:30

A Non-Interactive Shuffle with Pairing Based Verifiability,
Jens Groth (University College London)
Steve Lu (UCLA, Math Department)

On Privacy Models for RFID,
Serge Vaudenay (EPFL)

[Invited Talk I]
11:30-12:30

Treading the Impossible: A Tour of Set-Up Assumptions
for Obtaining Universally Composable Security,
Ran Canetti (IBM T.J. Watson Research Center)

[Session 3. Hash Function Design]
14:00-15:15

A Simple Variant of the Merkle-Damgård Scheme with a Permutation,
Shoichi Hirose (University of Fukui, Japan),
Je Hong Park (ETRI Network & Communication Security Division, Korea),
Aaram Yun (ETRI Network & Communication Security Division, Korea)

Seven-Property-Preserving Iterated Hashing: ROX,
Elena Andreeva (Katholieke Universiteit Leuven)
Gregory Neven (Katholieke Universiteit Leuven)
Thomas Shrimpton (Portland State University and University of Lugano)
Bart Preneel (Katholieke Universiteit Leuven)

How to Build a Hash Function from Any Collision-resistant Function,

Thomas Ristenpart (University of California, San Diego)
Thomas Shrimpton (Portland State University and University of Lugano)

[Session 4. Group/Broadcast Cryptography]
15:40-16:55

Fully Anonymous Group Signatures without Random Oracles,
Jens Groth (University College London)

Group Encryption,
Aggelos Kiayias (University of Connecticut, USA)
Yiannis Tsiounis (BestQuotes, USA)
Moti Yung (Columbia University, USA)

Identity-Based Broadcast Encryption with Constant Size Ciphertexts and Private
Keys,
Cécile Delerablée (Orange Labs)

December 4th (Tuesday)

[Session 5. MAC and Implementation]
14:00-15:15

Boosting Merkle-Damgård Hashing for Message Authentication,
Kan Yasuda (NTT, Japan)

On Efficient Message Authentication Via Block Cipher Design Techniques,
G. Jakimoski and K. P. Subbalakshmi (Stevens Institute of Technology)

Symmetric Key Cryptography on Modern Graphics Hardware,
James Goodman and Jason Yang (Advanced Micro Devices, Inc.)

[Session 6. Multiparty Computation I]
15:40-16:55

Blind Identity-Based Encryption and Simulatable Oblivious Transfer,
Matthew Green and Susan Hohenberger (The Johns Hopkins University)

Multi-Party Indirect Indexing and Applications,
Matthew Franklin, Mark Gondree and Payman Mohassel
(Dept. of Computer Science, University of California, Davis)

Two-Party Computing with Encrypted Data,
Seung Geol Choi (Computer Science Department, Columbia University)
Ariel Elbaz (Computer Science Department, Columbia University)
Ari Juels (RSA Laboratories)
Tal Malkin (Computer Science Department, Columbia University)
Moti Yung (Computer Science Department, Columbia University)

December 5th (Wednesday)

[Session 7. Block Cipher]
9:00-10:15

Known-Key Distinguishers for Some Block Ciphers,
Lars R. Knudsen (Technical University of Denmark)
Vincent Rijmen (Graz University of Technology, Austria)

Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions,
Jacques Patarin (University of Versailles)
Valerie Nachev (University of Cergy-Pontoise)
Come Berbain (France Télécom Research and Développement)

On Tweaking Luby-Rackoff Ciphers,
David Goldenberg (College of William and Mary)
Susan Hohenberger (Johns Hopkins University)
Moses Liskov (College of William and Mary)
Elizabeth Crump Schwartz (College of William and Mary)
Hakan Seyalioglu (College of William and Mary)

[Session 8. Multiparty Computation II]
10:40-12:20

Secure Protocols with Asymmetric Trust,
Ivan Damgård (Aarhus University)
Yvo Desmedt (University College London)
Matthias Fitzi (ETH Zürich)
Jesper Buus Nielsen (Aarhus University)

Simple and Efficient Perfectly-Secure Asynchronous MPC,
Zuzana Beerliová-Trubíniová and Martin Hirt
(ETH Zürich)

Efficient Byzantine Agreement with Faulty Minority,
Zuzana Beerliová-Trubíniová,
Martin Hirt and Micha Riser
(ETH Zürich)

Information-theoretic Security without an Honest Majority,
Anne Broadbent and Alain Tapp (Université de Montréal)

[Session 9. Foundation]
14:00-15:15

Black-Box Extension Fields and the Inexistence of Field-Homomorphic One-Way
Permutations,
Ueli Maurer and Dominik Raub (ETH Zürich)

Concurrent Statistical Zero-Knowledge Arguments for NP from One Way Functions,
Vipul Goyal, Ryan Moriarty, Rafail Ostrovsky and Amit Sahai
(UCLA)

Anonymous Quantum Communication,
Gilles Brassard (Université de Montréal)
Anne Broadbent (Université de Montréal),
Joseph Fitzsimons (University of Oxford)
Sébastien Gambs (Université de Montréal),

Alain Tapp (Université de Montréal)

[Invited Talk II]

15:40-16:40

Authenticated Key Exchange and Key Encapsulation in the Standard Model,
Tatsuaki Okamoto (NTT, Japan)

December 6th (Thursday)

[Session 10. Public Key Encryption]

9:00-10:15

Miniature CCA2 PK Encryption : Tight Security Without Redundancy,
Xavier Boyen (Voltage Inc.)

Bounded CCA2-Secure Encryption,
Ronald Cramer (CWI & Leiden University)
Goichiro Hanaoka (AIST, Japan)
Dennis Hofheinz (CWI)
Hideki Imai (AIST, Japan)
Eike Kiltz (CWI)
Rafael Pass (Cornell University)
abhi shelat (U. Virginia)
Vinod Vaikuntanathan (MIT)

Relations Among Notions of Non-Malleability for Encryption,
Rafael Pass (Cornell University)
abhi shelat (U. Virginia)
Vinod Vaikuntanathan (MIT)

[Session 11. Cryptanalysis]

10:40-11:55

Cryptanalysis of the Tiger Hash Function,
Florian Mendel (Institute for Applied Information Processing and Communications
(IAIK))
Vincent Rijmen (Graz University of Technology, Austria)

Cryptanalysis of Grindahl,
Thomas Peyrin (France Télécom R&D, AIST, University of Versailles)

A Key Recovery Attack on Edon80,
Martin Hell and Thomas Johansson (Lund University, Sweden)
