EUROCRYPT 2006 Program

Sunday, May 28

17.00-21.00: Registration is open

18.00-21.00: Welcome Reception: Drinks and snacks in the conference foyer

Monday, May 29

8.00: Registration is open

9.15-9.25: Opening Remarks

9.25-10.40: Cryptanalysis (chair: Stefan Lucks)

Security Analysis of the Strong Diffie-Hellman Problem
Jung Hee Cheon (Seoul National University)

Cryptography in Theory and Practice: The Case of Encryption in IPsec
Kenneth G. Paterson and **Arnold K.L. Yau** (Royal Holloway, University of London)

Polynomial Equivalence Problems: Algorithmic and Theoretical Aspects
Jean-Charles Faugère (University of Paris) and **Ludovic Perret** (University of Louvain-La-Neuve)

10.40-11.15: Coffee break

11.15-12.15: Invited Talk I (chair: Serge Vaudenay)

Alien vs. Quine, the Vanishing Circuit and Other Tales from the Industry's Crypt

David Naccache (Ecole Normale Supérieure)

12.15-14.00: Lunch

14.00-15.15: Cryptography Meets Humans (chair: Alexandra Boldyreva)

Hiding Secret Points amidst Chaff
Ee-Chien Chang and **Qiming Li** (National University of Singapore)

Parallel and Concurrent Security of the HB and HB+ Protocols
Jonathan Katz and **Ji Sun Shin** (University of Maryland)

Polling with Physical Envelopes: A Rigorous Analysis of a Human-Centric Protocol
Tal Moran and **Moni Naor** (Weizmann Institute)

15.15-15.45: Coffee break

15.45-17.00: Stream Ciphers (chair: Greg Rose)

QUAD: a Practical Stream Cipher with Provable Security
Côme Berbain and **Henri Gilbert** (France Telecom) and **Jacques Patarin** (University of Versailles)

How to Strengthen Pseudo-Random Generators by Using Compression
Aline Gouget and **Hervé Sibert** (France Telecom)

Efficient Computation of Algebraic Immunity for Algebraic and Fast Algebraic Attacks
Frederik Armknecht (University of Mannheim) and **Claude Carlet** (INRIA) and **Philippe Gaborit** (University of Limoges) and

Simon Kűnzli and **Willi Meier** (FH Nordwestschweiz) and **Olivier Ruatta** (University of Limoges)

Tuesday, May 30

9.00-9.50: Hash Functions (chair: Berry Schoenmakers)

VSH, an Efficient and Provable Collision-Resistant Hash Function
Scott Contini (Macquarie University) and **Arjen K. Lenstra** (EPFL) and **Ron Steinfeld** (Macquarie University)

Herding Hash Functions and the Nostradamus Attack
John Kelsey (NIST) and **Tadayoshi Kohno** (UC San Diego)

9.50-10.40: Oblivious Transfer (chair: Helger Lipmaa)

Optimal Reductions between Oblivious Transfers using Interactive Hashing
Claude Crépeau and **George Savvides** (McGill University)

Oblivious Transfer is Symmetric
Stefan Wolf and **Jűrg Wullschleger** (ETH Zűrich)

10.40-11.15: Coffee break

11.15-12.30: Numbers and Lattices (chair: Jonathan Katz)

Symplectic Lattice Reduction and NTRU
Nicolas Gama (Ecole Normale Supérieure) and **Nick Howgrave-Graham** (NTRU Cryptosystems) and **Phong Q. Nguyen** (Ecole Normale Supérieure)

The Function Field Sieve in the Medium Prime Case
Antoine Joux (University of Versailles) and **Reynald Lercier** (CELAR)

Learning a Parallelepiped: Cryptanalysis of GGH and NTRU Signatures
Phong Q. Nguyen (Ecole Normale Supérieure) and **Oded Regev** (University of Tel-Aviv)

12.30- 14.00: Lunch

Free afternoon. Conference Excursion to Petergoff Grand Palace and Park.

19.00: Rump session (chair: Kenny Paterson)

Wednesday, May 31

9.00-10.40: Foundations (chair: Eiichiro Fujisaki)

The Cramer-Shoup Encryption Scheme is Plaintext Aware in the Standard Model
Alexander W. Dent (Royal Holloway, University of London)

Private Circuits II: Keeping Secrets in Tamperable Circuits
Yuval Ishai (Technion) and **Manoj Prabhakaran** (UI Urbana-Champaign) and **Amit Sahai** (UCLA) and **David Wagner** (UC Berkeley)

Composition Implies Adaptive Security in Minicrypt
Krzysztof Pietrzak (Ecole Normale Supérieure)

Perfect Non-Interactive Zero Knowledge for NP
Jens Groth and **Rafail Ostrovsky** and **Amit Sahai** (UCLA)

10.40-11.15: Coffee break

11.15-12.15: Invited Talk II (chair: Arjen Lenstra)

Language Modeling and Encryption on Packet Switched Networks
Kevin S. McCurley (Google)

12.15-14.00: Lunch

14.00-15.15: Block Ciphers (chair: Mitsuru Matsui)

A Provable-Security Treatment of the Key-Wrap Problem
Phillip Rogaway (UC Davis) and **Thomas Shrimpton** (Portland State University)

Luby-Rackoff Ciphers from Weak Round Functions?
Ueli Maurer and **Yvonne Anne Oswald** (ETH Zűrich) and **Krzysztof Pietrzak** (Ecole Normale Supérieure) and **Johan Sjödin** (ETH Zűrich)

The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs
Mihir Bellare (UC San Diego) and **Phillip Rogaway** (UC Davis)

15.15-15.45: Coffee break

15.45-17.00: Cryptography Without Random Oracles (chair: Jean-Sébastien Coron)

Compact Group Signatures Without Random Oracles
Xavier Boyen (Voltage Inc) and **Brent Waters** (SRI International)

Practical Identity-Based Encryption Without Random Oracles
Craig Gentry (Stanford University)

Sequential Aggregate Signatures and Multisignatures Without Random Oracles

Steve Lu and **Rafail Ostrovsky** and **Amit Sahai** (UCLA) and **Hovav Shacham** (Weizmann Institute) and **Brent Waters** (SRI International)

17.00-17.50: IACR Business Meeting

19.00: Conference Dinner

Thursday, June 1

9.00-10.40: Multiparty Computation (chair: Juan Garay)

Our Data, Ourselves: Privacy via Distributed Noise Generation
Cynthia Dwork (Microsoft Research) and **Krishnaram Kenthapadi** (Stanford University) and **Frank McSherry** and **Ilya Mironov** (Microsoft Research) and **Moni Naor** (Weizmann Institute)

On the (Im-)Possibility of Extending Coin Toss
Dennis Hofheinz (CWI) and **Jörn Műller-Quade** and **Dominique Unruh** (University of Karlsruhe)

Efficient Binary Conversion for Paillier Encrypted Values
Berry Schoenmakers (TU Eindhoven) and **Pim Tuyls** (Philips Research Labs)

Information-Theoretic Conditions for Two-Party Secure Function Evaluation
Claude Crépeau and **Georges Savvides** (McGill University) and **Christian Schaffner** (University of Aarhus) and **Jűrg Wullschleger** (ETH Zűrich)

10.40-11.15: Coffee break

11.15-12.30: Cryptography for Groups (chair: Robert Zuccherato)

Unclonable Group Identification
Ivan Damgård and **Kasper Dupont** and **Michael Østergård Pedersen** (University of Aarhus)

Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and Private Keys
Dan Boneh (Stanford University) and **Amit Sahai** (UCLA) and **Brent Waters** (SRI International)

Simplified Threshold RSA with Adaptive and Proactive Security
Jesús F. Almansa and **Ivan Damgård** and **Jesper Buus Nielsen** (University of Aarhus)

12.30-12.45 Closing Remarks

12.45-14.00: Lunch