15th IACR International Conference on
Practice and Theory in Public Key Cryptography

PKC 2012

Darmstadt, May 21-23, 2012

Conference Program

Day 1 Monday, 21.05.2012

08:20 – 08:45 Registration
08:45 – 09:00 Opening remarks

09:00 – 10:35 ***Session I: Homomorphic Encryption and LWE*** (Chair: Dennis Hofheinz)

- Better Bootstrapping in Fully Homomorphic Encryption
  Craig Gentry, Shai Halevi, and Nigel P. Smart
- Polly Cracker, revisited, revisited
  Gottfried Herold
- Ring-LWE in Polynomial Rings
  Leo Ducas and Alain Durmus
- On Homomorphic Encryption and Chosen-Ciphertext Security
  Brett Hemenway and Rafail Ostrovsky

10:35 – 11:00 Coffee break

11:00 – 12:35 ***Session II: Signature Schemes*** (Chair: Dominique Unruh)

- Waters Signatures with Optimal Security Reduction
  Dennis Hofheinz, Tibor Jager, and Edward Knapp
- Strong Security from Probabilistic Signature Schemes
  Sven Schäge
- Space Efficient Signature Schemes from the RSA Assumption
  Shota Yamada, Goichiro Hanaoka, and Noboru Kunihiro
- The Construction of Ambiguous Optimistic Fair Exchange from Designated Confirmer Signature without Random Oracles
  Qiong Huang, Duncan S. Wong, and Willy Susilo

12:35 – 14:00 Lunch

14:00 – 15:35 ***Session III: Code-Based and Multivariate Crypto*** (Chair: Stanislav Bulygin)

- Efficient implementation of a CCA2-secure variant of McEliece using generalized Srivastava codes
  Pierre-Louis Cayrel, Gerhard Hoffmann, and Edoardo Persichetti
- Solving Underdetermined Systems of Multivariate Quadratic Equations revisited
  Enrico Thomae and Christopher Wolf
- Public-Key Identification Schemes Based on Multivariate Cubic Polynomials
  Koichi Sakumoto
- Public-Key Cryptography from New Multivariate Quadratic Assumptions
  Yun-Ju Huang, Feng-Hao Liu, and Bo-Yin Yang

15:35 – 16:00 Coffee break

16:00 – 17:35 ***Session IV: Public-Key Encryption: Special Properties*** (Chair: Yuliang Zheng)

- Anonymous Broadcast Encryption: Adaptive Security and Efficient Constructions in the Standard Model
  Benoit Libert, Kenneth G. Paterson, and Elizabeth A. Quaglia
- Outsider-Anonymous Broadcast Encryption with Sublinear Ciphertexts
  Nelly Fazio and Irippuge (Milinda) Perera
- Verifiable Functional Encryption and Applications to CCA Security and Anonymous Functional Authentication
  Shota Yamada, Nuttapong Attrapadung, Bagus Santoso, Goichiro Hanaoka, Jacob C.N. Schuldt, and Noboru Kunihiro
- Public Key Encryption Against Related Key Attacks
  Hoeteck Wee

Day 2 Tuesday, 22.05.2012

08:40 – 09:00 Registration

09:00 – 10:35 ***Session V: Identity-Based Encryption*** (Chair: Georg Fuchsbauer)

- Functional Encryption for Threshold Functions (or, Fuzzy IBE) from Lattices
  Shweta Agrawal, Xavier Boyen, Vinod Vaikuntanathan, Panagiotis Voulgaris, and Hoeteck Wee
- Variants of Waters' Dual System Primitives Using Asymmetric Pairings
  Somindu C. Ramanna, Sanjit Chatterjee, and Palash Sarkar
- From Selective to Full Security: Semi-Generic Transformations in the Standard Model
  Michel Abdalla, Dario Fiore, and Vadim Lyubashevsky
- Circular and KDM Security for Identity-Based Encryption
  Jacob Alperin-Sheriff and Chris Peikert

10:35 – 11:00 Coffee break

11:00 – 11:50 ***Session VI: Public-Key Encryption: Constructions*** (Chair: Hoeteck Wee)

- NTRUCCA: How to Strengthen NTRUEncrypt to Chosen-Ciphertext Security in the Standard Model
  Ron Steinfeld, San Ling, Josef Pieprzyk, Christophe Tartary, and Huaxiong Wang

- Generating Provable Primes Efficiently on Embedded Devices
  Christophe Clavier, Benoit Feix, Pascal Paillier, and Loic Thierry

11:50 – 12:50 ***Invited talk*** (Chair: Marc Fischlin)

Password-Based Authenticated Key Exchange
David Pointcheval

12:50 – 14:20 Lunch

14:20 – 15:35 ***Session VII: Secure Two-Party and Multi-Party Computation*** (Ch: Matthew Green)

- Constant-Round Multi-Party Private Set Union using Reversed Laurent Series
  Jae Hong Seo, Jung Hee Cheon, and Jonathan Katz

- Policy-Enhanced Private Set Intersection: Sharing Information While Enforcing Privacy Policies
  Emil Stefanov, Elaine Shi, and Dawn Song

- Efficiently Shuffling in Public
  Kim Ramchen and Vanessa Teague

15:35 – 16:00 Coffee break

16:30 Bus Excursion to Schloss Auerbach and Conference Dinner in Hotel Brandhof
We meet at 16:00 at the main entrance of the conference center Darmstadtium.

Day 3 Wednesday, 23.05.2012

08:40 – 09:00 Registration

09:00 – 10:35 ***Session VIII: Key Exchange and Secure Sessions*** (Chair: Michel Abdalla)

- Efficient Password Authenticated Key Exchange via Oblivious Transfer
  Ran Canetti, Dana Dachman-Soled, Vinod Vaikuntanathan, and Hoeteck Wee

- Strongly Secure Authenticated Key Exchange from Factoring, Codes, and Lattices
  Atsushi Fujioka, Koutarou Suzuki, Keita Xagawa, and Kazuki Yoneyama

- Relatively-Sound NIZKs and Password-Based Key-Exchange
  Charanjit Jutla and Arnab Roy

- Multi-Location Leakage Resilient Cryptography
  Ali Juma, Yevgeniy Vahlis, and Moti Yung

10:35 – 11:00 Coffee break

11:00 – 12:35 ***Session IX: Public-Key Encryption: Relationships*** (Chair: Marc Fischlin)

- On Definitions of Selective Opening Security
  Florian Böhl, Dennis Hofheinz, and Daniel Kraschewski
- New Definitions and Separations for Circular Security
  David Cash, Matthew Green, and Susan Hohenberger
- Correlated Product Security From Any One-Way Function
  Brett Hemenway , Steve Lu, and Rafail Ostrovsky
- Relations between Constrained and Bounded Chosen Ciphertext Security for Key Encapsulation Mechanisms
  Takahiro Matsuda, Goichiro Hanaoka, and Kanta Matsuura

12:35 – 14:00 Lunch

14:00 – 15:35 ***Session X: DL, DDH, and more Number Theory*** (Chair: Dario Fiore)

- Solving a Discrete Logarithm Problem with Auxiliary Input
  Yumi Sakemi, Goichiro Hanaoka, Tetsuya Izu, Masahiko Takenaka, and Masaya Yasuda
- Inferring Sequences Produced by Nonlinear Pseudorandom Number Generators Using Coppersmith's Methods
  Aurelie Bauer, Damien Vergnaud, and Jean-Christophe Zapalowicz
- Extended-DDH and Lossy Trapdoor Functions
  Brett Hemenway and Rafail Ostrovsky
- DDH-like Assumptions Based on Extension Rings
  Ronald Cramer, Ivan Damgård, Eike Kiltz, Sarah Zakarias, and Angela Zottarel

15:35 – 16:00 Coffee break

16:00 – 17:35 ***Session XI: Beyond Ordinary Signature Schemes*** (Chair: Mark Manulis)

- Security of Blind Signatures Revisited
  Dominique Schröder and Dominique Unruh
- Efficient Network Coding Signatures in the Standard Model
  Dario Catalano, Dario Fiore, and Bogdan Warinschi
- Improved Security for Linearly Homomorphic Signatures: A Generic Framework
  David Mandell Freeman
- On the Security of Dynamic Group Signatures: Preventing Signature Hijacking
  Yusuke Sakai, Jacob C. N. Schuldt, Keita Emura, Goichiro Hanaoka, and Kazuo Ohta

17:35 End