Eurocrypt 2009

Conference Program 26. - 30. April 2009

April 26, 2009 Sunday	
10:00 – 17:00	Board Meeting (only IACR Board members)
17:00 – 21:00	Welcome Reception and Registration

April 27, 2009 Monday	
08:30	Registration Desk open
09:00 – 09:15	Welcome / Opening Remarks
Session 1 09:15 – 10:55	Security, Proofs and Models I
09:15 – 09:40	Possibility and Impossibility Results for Encryption and Commitment Secure under Selective Opening. *Mihir Bellare, Dennis Hofheinz, Scott Yilek*
09:40 – 10:05	Breaking RSA Generically is Equivalent to Factoring *Divesh Aggarwal, Ueli Maurer*
10:05 – 10:30	Resettably Secure Computation *Vipul Goyal, Amit Sahai*
10:30 – 10:55	On the Security Loss in Cryptographic Reductions *Chi-Jen Lu*
10:55 – 11:25	Coffee Break
Invited Talk 11:25 – 12:25	Practice-Oriented Provable-Security and the Social Construction of Cryptography Phillip Rogaway
12:45 – 13:45	Lunch
Session 2 13:45 – 15:25	Hash Cryptanalysis
13:45 – 14:10	On Randomizing Hash Functions to Strengthen the Security of Digital Signatures *Praveen Gauravaram, Lars R. Knudsen*
14:10 – 14:35	Cryptanalysis of MDC-2 *Lars R. Knudsen, Florian Mendel, Christian Rechberger, Soeren S. Thomsen*

April 29, 2009 Wednesday	
Session 8 15:45 – 16:35	Side Channels
15:45 – 16:10	A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks *Francoix-Xavier Standaert, Tal Malkin, Moti Yung*
16:10 – 16:35	A Leakage-Resilient Mode of Operation *Krzysztof Pietrzak*
16:45 – 18:00	IACR Membership Meeting
19:00 – 23:00	Conference Dinner - Boat Cruise (2h, the boat leaves the pier of K&D at 20:00)

April 30, 2009 Thursday	
Session 9 09:00 – 10:40	Curves
09:00 – 09:25	ECM on Graphics Cards *Daniel Bernstein, Tien-Ren Chen, Chen-Mou Cheng, Tanja Lange, Bo-Yin Yang*
09:25 – 09:50	Double-Base Number System for Multi-Scalar Multiplications *Christophe Doche, David Kohel, Francesco Sica*
09:50 – 10:15	Endomorphisms for Faster Elliptic Curve Cryptography on a Large Class of Curves *Steven Galbraith, Xibin Lin, Michael Scott*
10:15 – 10:40	Generating Genus Two Hyperelliptic Curves over Large Characteristic Finite Fields *Takakazu Satoh*
10:40 – 11:10	Coffee Break + Poster Session Slot
Session 10 11:10 – 12:25	Randomness
11:10 – 11:35	Optimal Randomness Extraction from a Diffie-Hellman Element *Pierre-Alain Fouque, Sebastien Zimmer, David Pointcheval, Celine Chevalier*
11:35 – 12:00	Verifiable Random Functions from Identity-based Key Encapsulation *Michel Abdalla, Dario Catalano, Dario Fiore*
12:00 – 12:25	A New Randomness Extraction Paradigm for Hybrid Encryption *Eike Kiltz, Krzysztof Pietrzak, Martijn Stam, Moti Yung*
12:25 – 12:40	Closing Remarks

14:35 – 15:00	**Cryptanalysis on HMAC/NMAC-MD5 and MD5-MAC** *Xiaoyun Wang, Hongbo Yu, Wei Wang, Haina Zhang, Tao Zhan*
15:00 – 15:25	**Finding Preimages in Full MD5 Faster than Exhaustive Search** *Yu Sasaki, Kazumaro Aoki*
15:25 – 16:25	**Coffee Break + Poster Session Slot**
Session 3 16:25 – 17:40	**Group and Broadcast Encryption**
16:25 – 16:50	**Asymmetric Group Key Agreement** *Qianhong Wu, Yi Mu, Willy Susilo, Bo Qin, Josep Domingo-Ferrer*
16:50 – 17:15	**Adaptive Security in Broadcast Encryption Systems (with Short Ciphertexts)** *Craig Gentry, Brent Waters*
17:15 – 17:40	**Traitors Collaborating in Public: Pirates 2.0** *Olivier Billet, Duong-Hieu Phan*
April 28, 2009 Tuesday	
08:30	**Registration Desk open**
Session 4 09:00 – 10:15	**Cryptosystems I**
09:00 – 09:25	**Key Agreement from Close Secrets over Unsecured Channels** *Bhavana Kanukurthi, Leonid Reyzin*
09:25 – 09:50	**Order-Preserving Symmetric Encryption** *Alexandra Boldyreva, Nathan Chenette, Younho Lee, Adam O'Neill*
09:50 – 10:15	**A Double-Piped Mode of Operation for MACs, PRFs and PROs: Security beyond the Birthday Barrier** *Kan Yasuda*
10:15 – 11:10	**Coffee Break + Poster Session Slot**
Session 5 11:10 – 12:25	**Cryptanalysis**
11:10 – 11:35	**On the Security of Cryptosystems with Quadratic Decryption: The Nicest Cryptanalysis** *Guilhem Castagnos, Fabien Laguillaumie*
11:35 – 12:00	**Cube Attacks on Tweakable Black Box Polynomials** *Itai Dinur, Adi Shamir*
12:00 – 12:25	**Smashing SQUASH-0** *Khaled Ouafi, Serge Vaudenay*
12:25 – 13:30	**Lunch**
14:00 – 18:00	**Social Program - Meeting Point 13:40 in the foyer!** • **City Walking Tour (2,5 h)** • **City Bike Tour (3h)** • **Chocolate Museum (1h)** • **Wallraf-Richartz Museum (1h)** • **Boat Cruise (1h)**
18:00 – 23:00	**Rump Session**
April 29, 2009 Wednesday	
09:00 – 9:15	**Best Paper Award Ceremony**
Session 6 09:15 – 10:30	**Cryptosystems II**
09:15 – 09:40	**Practical Chosen Ciphertext Secure Encryption from Factoring** *Dennis Hofheinz, Eike Kiltz*
09:40 – 10:05	**Realizing Hash-and-Sign Signatures under Standard Assumptions** *Susan Hohenberger, Brent Waters*
10:05 – 10:30	**A Public Key Encryption Scheme Secure against Key Dependent Chosen Plaintext and Adaptive Chosen Ciphertext Attacks** *Jan Camenisch, Nishanth Chandran, Victor Shoup*
10:30 – 11:25	**Coffee Break + Poster Session Slot**
Invited Talk 11:25 – 12:25	**Cryptography without (Hardly any) Secrets ?** ***Shafi Goldwasser***
12:25 – 13:45	**Lunch**
Session 7 13:45 – 15:25	**Security, Proofs and Models II**
13:45 – 14:10	**Salvaging Merkle-Damgard for Practical Applications** *Yevgeniy Dodis, Thomas Ristenpart, Thomas Shrimpton*
14:10 – 14:35	**On the Security of Padding-Based Encryption Schemes (Or: Why we cannot prove OAEP secure in the Standard Model)** *Eike Kiltz, Krzysztof Pietrzak*
14:35 – 15:00	**Simulation without the Artifical Abort: Simplified Proof and Improved Concrete Security for Waters' IBE Scheme** *Mihir Bellare, Thomas Ristenpart*
15:00 – 15:25	**On the Portability of Generalized Schnorr Proofs** *Jan Camenisch, Aggelos Kiayias, Moti Yung*
15:25 – 15:45	**Coffee Break**