CRYPTO 2006

Final Program

All events in Campbell Hall
(unless otherwise noted)

Sunday, August 20, 2006

17:00 - 20:00 **Registration**, Anacapa Formal Lounge
(registration continues outside Campbell Hall starting Monday morning)

17:30 - 21:30 **Dinner Reception**, Anacapa/Santa Cruz Ocean Lawn

Monday, August 21, 2006

07:30 - 08:45	**Breakfast** - De La Guerra Commons

09:00 - 09:10	**Opening Remarks** Josh Benaloh, General Chair

Session 1

Chair *Moni Naor*

09:10 - 09:35	***Rigorous Bounds on Cryptanalytic Time/Memory Tradeoffs*** Elad Barkan, Eli Biham, and Adi Shamir
09:35 - 10:00	***On the Power of the Randomized Iterate*** ***Best Paper Award*** Iftach Haitner, Danny Harnik, and Omer Reingold

10:00 - 10:30	**Morning Break**

Session 2

Chair *Yiqun Lisa Yin*

10:30 - 10:55	***Strengthening Digital Signatures via Randomized Hashing*** Shai Halevi and Hugo Krawczyk
10:55 - 11:20	***Round-Optimal Composable Blind Signatures in the Common Reference String Model*** Marc Fischlin

Session 3

Chair *Yiqun Lisa Lin*

11:20 - 11:45	***On Signatures of Knowledge*** Melissa Chase and Anna Lysyanskaya
11:45 - 12:10	***Non-interactive Zaps and New Techniques for NIZK*** Jens Groth, Rafail Ostrovsky, and Amit Sahai

12:15 - 13:45	**Lunch** - De La Guerra Commons

Session 4	
Chair	*Cynthia Dwork*
14:00 - 14:25	***Rankin's Constant and Blockwise Lattice Reduction*** Nicolas Gama, Nick Howgrave-Graham, Henrik Koy, and Phong Q. Nguyen
Session 5	***Invited Talk***
Chair	*Cynthia Dwork*
14:25 - 15:25	***Lattice-Based Cryptography*** Oded Regev
15:25 - 15:55	**Afternoon Break**
Session 6	
Chair	*Arjen Lenstra*
15:55 - 16:20	***A Method for Making Password-Based Key Exchange Resilient to Server Compromise*** Craig Gentry, Philip MacKenzie, and Zulfikar Ramzan
16:20 - 16:45	***Mitigating Dictionary Attacks on Password-Protected Local Storage*** Ran Canetti, Shai Halevi, and Michael Steiner
Session 7	
Chair	*Arjen Lenstra*
16:45 - 17:10	***Rationality and Adversarial Behavior in Multi-Party Computation*** Anna Lysyanskaya and Nikos Triandopoulos
17:10 - 17:35	***When Random Sampling Preserves Privacy*** Kamalika Chaudhuri and Nina Mishra
17:45 - 19:30	**Dinner** - De La Guerra Commons
19:30 - 21:30	**Dessert Reception**, Anacapa/Santa Cruz Ocean Lawn

Tuesday, August 22, 2006

07:30 - 08:45	**Breakfast** - De La Guerra Commons

Session 8
Chair *Yehuda Lindell*

09:00 - 09:25	***Tight Bounds for Unconditional Authentication Protocols in the Manual Channel and Shared Key Models*** Moni Naor, Gil Segev, and Adam Smith
09:25 - 09:50	***Robust Fuzzy Extractors and Authenticated Key Agreement from Close Secrets*** Yevgeniy Dodis, Jonathan Katz, Leonid Reyzin, and Adam Smith
09:50 - 10:15	***On Forward-Secure Storage*** Stefan Dziembowski

10:15 - 10:45	**Morning Break**

Session 9
Chair *Jonathan Katz*

10:45 - 11:10	***Construction of a Non-Malleable Encryption Scheme from Any Semantically Secure One*** Rafael Pass, abhi shelat, and Vinod Vaikuntanathan
11:10 - 11:35	***Anonymous Hierarchical Identity-Based Encryption (Without Random Oracles)*** Xavier Boyen and Brent Waters
11:35 - 12:00	***Fast Algorithms for the Free Riders Problem in Broadcast Encryption*** Zulfikar Ramzan and David Woodruff

12:15 - 13:45	**Lunch** - De La Guerra Commons

	Free Afternoon
14:00 - 17:00	**Tourism** - Santa Barbara **Birds of a Feather Sessions** - See Schedule in Anacapa Lobby **Soccer** - Lawn
17:45 - 19:30	**Dinner** - De La Guerra Commons
	Rump Session
18:45 - 23:00	**Snacks and Open Bar** - University Center Courtyard
19:30 - 19:40	**New IACR Fellows Induction Ceremony** - University Center Corwin Pavilion
19:40 - 19:45	**Crypto 2006 T-shirt Solution and Prize Drawing** - University Center Corwin Pavilion
19:45 - Late	**Rump Session** - University Center Corwin Pavilion

Wednesday, August 23, 2006

07:30-08:45	**Breakfast** - De La Guerra Commons
Session 10	
Chair	*Phong Nguyen*
09:00-09:25	***The Number Field Sieve in the Medium Prime Case*** Antoine Joux, Reynald Lercier, Nigel Smart, and Frederik Vercauteren
09:25-09:50	***Inverting HFE is Quasipolynomial*** Louis Granboulan, Antoine Joux, and Jacques Stern
09:50-10:15	***Cryptanalysis of 2R$^-$ Schemes*** Jean-Charles Faugère, and Ludovic Perret
10:15-10:45	**Morning Break**
Session 11	
Chair	*Ivan Damgård*
10:45-11:10	***Receipt-Free Universally-Verifiable Voting With Everlasting Privacy*** Tal Moran and Moni Naor
Session 12	***Invited Talk***
Chair	*Ivan Damgård*
11:10-12:10	***Cryptographic Protocols for Electronic Voting*** David Wagner
12:15-13:45	**Lunch** - De La Guerra Commons

Session 13	
Chair	*Yuval Ishai*
14:00 - 14:25	***Asymptotically Optimal Two-Round Perfectly Secure Message Transmission*** Saurabh Agarwal, Ronald Cramer, and Robbert de Haan
14:25 - 14:50	***Random Selection with an Adversarial Majority*** Ronen Gradwohl, Salil Vadhan, and David Zuckerman
14:50 - 15:15	***Oblivious Transfer and Linear Functions*** Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner
15:15 - 15:45	**Afternoon Break**
Session 14	
Chair	*Moni Naor*
15:45 - 16:10	***On Expected Constant-Round Protocols for Byzantine Agreement*** Jonathan Katz and Chiu-Yuen Koo
16:10 - 16:35	***Robust Multiparty Computation with Linear Communication Complexity*** Martin Hirt, Jesper Buus Nielsen
16:35 - 17:00	***On Combining Privacy with Guaranteed Output Delivery in Secure Multiparty Computation*** Yuval Ishai, Eyal Kushilevitz, Yehuda Lindell, and Erez Petrank
	IACR Membership Meeting
Chair	*Bart Preneel, IACR Vice-President*
17:05 - 17:50	**IACR Membership Meeting** - Campbell Hall
18:00 - 20:15	**Beach Barbecue** - Goleta Beach
20:00 - 22:30	**Crypto Café** - Anacapa Formal Lounge

Thursday, August 24, 2006

07:30 - 08:45	**Breakfast** - De La Guerra Commons

Session 15
Chair *Hovav Shacham*

09:00 - 09:25	***Scalable Secure Multiparty Computation*** Ivan Damgård and Yuval Ishai
09:25 - 09:50	***Algebraic Geometric Secret Sharing Schemes and Secure Multi-Party Computations over Small Fields*** Hao Chen, Ronald Cramer
09:50 - 10:15	***Automated Security Proofs with Sequences of Games*** Bruno Blanchet and David Pointcheval

10:15 - 10:45	**Morning Break**

Session 16
Chair *Bart Preneel*

10:45 - 11:10	***On Robust Combiners for Private Information Retrieval and Other Primitives*** Remo Meier and Bartosz Przydatek
11:10 - 11:35	***On the Impossibility of Efficiently Combining Collision Resistant Hash Functions*** Dan Boneh and Xavier Boyen
11:35 - 12:00	***On the Higher Order Nonlinearities of Algebraic Immune Functions*** Claude Carlet
12:00 - 12:25	***New Proofs for NMAC and HMAC: Security without Collision-Resistance*** Mihir Bellare
12:25	***Conference Adjourns***

12:15 - 13:45	**Lunch** - De La Guerra Commons