CRYPTO 2008

Preliminary Program

All events in Campbell Hall
(unless otherwise noted)

.

Sunday, August 17, 2008

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

Thank you to our sponsors.

Student scholarships were funded by Qualcomm and PGP.

General support was offered by Microsoft Research, HP Secure Advantage, and the D. E. Shaw group.

Student presenter conference registrations were funded by a grant from the Marconi Society.

Monday, August 18, 2008

07:30 - 08:45 **Breakfast** - Ortega Dining Commons

09:00 - 09:10 **Opening Remarks**
Susan Langford, General Chair

Session 1 *Random oracles*
Chair *David Wagner*

09:10 - 09:35 ***The Random Oracle Model and the Ideal Cipher Model are Equivalent***
Best Paper Award
Jean-Sébastien Coron, Jacques Patarin, Yannick Seurin

09:35 - 10:00 ***Programmable Hash Functions and Their Applications***
Dennis Hofheinz and Eike Kiltz

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

Session 2 *Applications*
Chair *Xavier Boyen*

10:30 - 10:55 ***One-Time Programs***
Shafi Goldwasser, Yael Tauman Kalai, and Guy Rothblum

10:55 - 11:20 ***Adaptive One-way Functions and Applications***
Omkant Pandey, Rafael Pass, and Vinod Vaikuntanathan

Session 3 *IACR Distinguished Lecture*
Chair *Bart Preneel*

11:20 - 12:20 ***Vingt-cinq ans après, with apologies to Alexandre Dumas***
Gilles Brassard

12:20 - 13:45 **Lunch** - Ortega Dining Commons

Session 4 *Public-key crypto I*
Chair *Kristin Lauter*

14:00 - 14:25 ***Bit security of the elliptic curve Diffie-Hellman secret keys***
Dimitar Jetchev and Ramarathnam Venkatesan

14:25 - 14:50 ***Improved Bounds on Security Reductions for Discrete Log based Signatures***
Sanjam Garg, Raghav Bhaskar, and Satya Lokam

14:50 - 15:15 ***Circular-Secure Encryption from Decision Diffie-Hellman***
Dan Boneh, Shai Halevi, Mike Hamburg, Rafail Ostrovsky

15:15 - 15:40 ***Public Key Locally Decodable Codes***
Brett Hemenway and Rafail Ostrovsky

15:40 - 16:15 **Afternoon Break**

Session 5 *Hash functions I*
Chair *John Black*

16:15 - 16:40 ***Key-Recovery Attacks on Universal Hash Function based MAC Algorithms***
Helena Handschuh and Bart Preneel

16:40 - 17:05 ***Cryptanalysis of the GOST Hash Function***
Florian Mendel, Norbert Pramstaller, Christian Rechberger, Marcin Kontak, and Janusz Szmidt

17:05 - 17:30 ***Preimages for Reduced SHA-0 and SHA-1***
Christophe De Cannière and Christian Rechberger

17:30 - 18:00 **Evening Break**

Session 6 *Cryptanalysis I*
Chair *Serge Vaudenay*

18:00 - 18:25 ***On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme***
Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalmani

18:25 - 18:50 ***Bug Attacks***
Eli Biham, Yaniv Carmeli, Adi Shamir

19:00 - 21:00 **Dinner** - Anacapa/Santa Cruz Ocean Lawn

Tuesday, August 19, 2008

07:30 - 08:45 **Breakfast** - Ortega Dining Commons

Session 7 *Multiparty computation I*
Chair *Jean-Sébastien Coron*

09:00 - 09:25 ***Scalable Multiparty Computation with Nearly Optimal Work and Resilience***
Ivan Damgård, Yuval Ishai, Mikkel Krøigaard, Jesper Buus Nielsen, and Adam Smith

09:25 - 09:50 ***Cryptographic Complexity of Multi-party Computation Problems: Classifications and Separations***
Manoj Prabhakaran and Mike Rosulek

09:50 - 10:20 **Morning Break**

Session 8 *Cryptanalysis II*
Chair *Matt Robshaw*

10:20 - 10:45 ***Cryptanalysis of MinRank***
Françoise Levy-dit-Vehel, Jean-Charles Faugère, and Ludovic Perret

10:45 - 11:10 ***New State Recovery Attack on RC4***
Alexander Maximov and Dmitry Khovratovich

Session 9 *Invited Talk*
Chair *Matt Robshaw*

11:10 - 12:10 ***How to Solve it: New Techniques in Algebraic Cryptanalysis***
Adi Shamir

12:15 - 13:45 **Lunch** - Ortega Dining Commons

Free Afternoon

14:00 - 17:00 **Tourism** - Santa Barbara
Birds of a Feather Sessions - See Schedule in Anacapa Lobby

17:45 - 19:30 **Dinner** - Ortega Dining Commons

Rump Session

Chair *Dan Bernstein*

18:45 - 23:00 **Snacks and Open Bar** - University Center Courtyard

19:30 - 19:40 **IACR Fellows Induction Ceremony** - University Center Corwin Pavilion

19:45 - Late **Rump Session** - University Center Corwin Pavilion

Wednesday, August 20, 2008

07:30 - 08:45 **Breakfast** - Ortega Dining Commons

Session 10 *Public-key crypto II*
Chair *Brent Waters*

09:00 - 09:25 ***Dynamic Threshold Public-Key Encryption***
Cecile Delerablee and David Pointcheval

09:25 - 09:50 ***On Notions of Security for Deterministic Encryption, and Efficient Constructions Without Random Oracles***
Alexandra Boldyreva, Serge Fehr, and Adam O'Neill

09:50 - 10:15 ***Deterministic Encryption: Definitional Equivalences and Constructions without Random Oracles***
Mihir Bellare, Marc Fischlin, Adam O'Neill, and Thomas Ristenpart

10:15 - 10:40 ***Communication-Complexity Algebraic Lower Bounds For Private Two-Party Protocols***
Rafail Ostrovsky and William E. Skeith III

10:40 - 11:10 **Morning Break**

Session 11 *Invited Talk*
Chair *Hovav Shacham*

11:10 - 12:10 ***The MD6 hash function***
Ronald Rivest

12:15 - 13:45 **Lunch** - Ortega Dining Commons

Session 12 *Hash functions II*
Chair *Yevgeniy Dodis*

14:00 - 14:25 ***Beyond Uniformity: Better Security/Efficiency Tradeoffs for Compression Functions***
Martijn Stam

14:25 - 14:50 ***Compression from collisions, or why CRHF combiners have a long output***
Krzysztof Pietrzak

14:50 - 15:15 ***Constructing Cryptographic Hash Functions from Fixed-Key Blockciphers***
Phillip Rogaway and John Steinberger

15:15 - 15:45 **Afternoon Break**

Session 13 *Privacy*
Chair *Yuval Ishai*

15:45 - 16:10 ***Distributed Private Data Analysis: Simultaneously Solving How and What***
Amos Beimel, Kobbi Nissim, and Eran Omri

16:10 - 16:35 ***New Efficient Attacks on Statistical Disclosure Control Mechanisms***
Cynthia Dwork and Sergey Yekhanin

IACR Membership Meeting
Chair *Bart Preneel, IACR President*

16:40 - 17:40 **IACR Membership Meeting** - Campbell Hall

18:00 - 20:15 **Beach Barbecue** - Goleta Beach

20:00 - 22:30 **Crypto Café** - Anacapa Formal Lounge

Thursday, August 21, 2008

07:30 - 08:45 **Breakfast** - Ortega Dining Commons

Session 14 *Multiparty computation II*
Chair *Susan Hohenberger*

09:00 - 09:25 ***Efficient Secure Linear Algebra in the Presence of Covert or Computationally Unbounded Adversaries***
Payman Mohassel and Enav Weinreb

09:25 - 09:50 ***Collusion-Free Protocols in the Mediated Model***
Joel Alwen, abhi shelat, and Ivan Visconti

09:50 - 10:10 **Morning Break I**

Session 15 *Zero knowledge*
Chair *Manoj Prabhakaran*

10:10 - 10:35 ***Efficient Constructions of Composable Commitments and Zero-Knowledge Proofs***
Yevgeniy Dodis, Victor Shoup, and Shabsi Walfish

10:35 - 11:00 ***Noninteractive Statistical Zero-Knowledge Proofs for Lattice Problems***
Chris Peikert and Vinod Vaikuntanathan

11:00 - 11:20 **Morning Break II**

Session 16 *Oblivious Transfer*
Chair *Craig Gentry*

11:20 - 11:45 ***A Framework for Efficient and Composable Oblivious Transfer***
Chris Peikert, Vinod Vaikuntanathan, and Brent Waters

11:45 - 12:10 ***Founding Cryptography on Oblivious Transfer -- Efficiently***
Yuval Ishai, Manoj Prabhakaran, and Amit Sahai

12:10 ***Conference Adjourns***

12:15 - 13:45 **Lunch** - Ortega Dining Commons