CRYPTO '98 Preliminary Program

(Updated Jul 8, 1998 - SUBJECT TO CHANGE)

Sponsored by
The International Association for Cryptologic Research

All sessions are in Campbell Hall, except as noted. All breakfasts and lunches are in De La Guerra Dining Commons. Entry to the dining hall for breakfast is 7:00-8:00; lunch 12:30-1:30.

Sunday, August 23, 1998

2:00-8:00 Registration, Anacapa Lounge

5:30-6:30 Pre-Registration Reception, Anacapa Front Patio

6:30-10:00 Reception, Anacapa Lawn

Monday, August 24, 1998

7:00-8:00 Breakfast, De La Guerra Commons

8:00- 12:00 Registration, outside Campbell Hall

8:30-8:40 Welcome

Session 1: Chosen Ciphertext Security
Chair: Dan Simon (Microsoft Research, USA)

8:40-9:05 Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1
Daniel Bleichenbacher (Bell Labs, USA)

9:05-9:30 A Practical Public Key Cryptosystem Provably Secure Against Adaptive Chosen Ciphertext Attack

Ronald Cramer (ETH Zurich, Switzerland), Victor Shoup (IBM Zurich Research Laboratory, Switzerland)

9:30-9:55 Relations Among Notions of Security for Public-Key Encryption Schemes
Mihir Bellare, Anand Desai (University of California at San Diego, USA), David Pointcheval (Ecole Normale Superieure, France), Phillip Rogaway (University of California at Davis, USA)

9:55-10:20 Break

Session 2: Invited Lecture
Chair: Moti Yung (CertCo, USA)

10:20-11:20 Cryptography and the Internet
Steve Bellovin (AT&T Labs - Research, USA)

Session 3: Cryptanalysis of Hash Functions and Block Ciphers
Chair: Lars Knudsen (University of Bergen, Norway)

11:20-11:45 Differential Collisions in SHA-0
Florent Chabaud, Antoine Joux (Centre d'Electronique de l'Armement, France)

11:45-12:10 From Differential Cryptanalysis to Ciphertext-Only Attacks
Alex Biryukov, Eyal Kushilevitz (Technion, Israel)

12:10-2:00 Lunch, De La Guerra Commons

Session 4: Distributed Cryptography
Chair: Yair Frankel (CertCo, USA)

2:15-2:40 A Simplified Approach to Threshold and Proactive RSA
Tal Rabin (IBM T.J. Watson Research Center, USA)

2:40-3:05 New Efficient and Secure Protocols for Verifiable Signature Sharing and Other Applications
Dario Catalano (Université di Catania, Italy), Rosario Gennaro (IBM T.J. Watson Research Center, USA)

3:05-3:30 Trading Correctness for Privacy in Unconditional Multi-Party Computation
Matthias Fitzi, Martin Hirt, Ueli Maurer (ETH Zurich, Switzerland)

3:30-3:55Break

Session 5: Identification and Certification
Chair: Kazue Sako (NEC, Japan)

3:55-4:20 Fast Digital Identity Revocation
William Aiello (Bellcore, USA), Sachin Lodha (Rutgers University, USA), Rafail Ostrovsky (Bellcore, USA)

4:20-4:45 Self-Delegation with Controlled Propagation -- or -- What If You Lose Your Laptop
Oded Goldreich (Weizmann Institute of Science, Israel), Birgit Pfitzmann (Universität des Saarlandes, Germany), Ronald L. Rivest (MIT Laboratory for Computer Science, USA)

4:45-5:10 Identity Escrow
Joe Kilian (NEC Research Institute, USA), Erez Petrank (IBM Haifa Research Lab, Israel)

7:00-10:00 Reception, De La Guerra Lawn

Tuesday, August 25, 1998

7:00-8:00 Breakfast, De La Guerra Commons

Session 6: Block Cipher Design and Analysis
Chair: Matt Robshaw (RSA Laboratories, USA)

8:30-8:55 Generalized Birthday Attacks on Unbalanced Feistel Networks
Charanjit S. Jutla (IBM T.J. Watson Research Center, USA)

8:55-9:20 Quadratic Relation of S-box and Its Application to the Linear Attack of Full Round DES
Takeshi Shimoyama (TAO, Japan), Toshinobu Kaneko (Science University of Tokyo, Japan)

9:20-9:45 Cryptanalysis of Block Ciphers with Probabilistic Non-Linear Relations of Low Degree
Thomas Jakobsen (Technical University of Denmark, Denmark)

Session 7: AES Special Report
Chair: Rainer Rueppel (R3 Security Engineering AG, Switzerland)

9:45-10:10 Special Report on the AES Conference
Miles Smid (NIST, USA)

10:10-10:35 Break

Session 8: Algebraic Cryptanalysis
Chair: Ueli Maurer (ETH Zurich, Switzerland)

10:35-11:05 Cryptanalysis of the Ajtai-Dwork Cryptosystem
Phong Nguyen, Jacques Stern (Ecole Normale Superieure, France)

11:05-11:35 Cryptanalysis of the Chor-Rivest Cryptosystem
Serge Vaudenay (Ecole Normale Superieure, France)

11:35-12:05 Cryptanalysis of the Oil & Vinegar Signature Scheme
Aviad Kipnis (NDS Technologies, Israel), Adi Shamir (Weizmann Institute of Science, Israel)

12:05-2:00 Lunch, De La Guerra Commons

Free Afternoon

Rump Session
Chair: Stuart Haber (Surety Technologies, USA)

6:00-10:30 Informal presentations to be announced
Corwin Pavilion in the University Center

Wednesday, August 26, 1998

7:00-8:00 Breakfast, De La Guerra Commons

Session 9: Relations Among Cryptographic Primitives
Chair: Rafail Ostrovsky (Bellcore, USA)

8:30-8:55 From Unpredictability to Indistinguishability: A Simple Construction of Pseudo-Random Functions from MACs
Moni Naor, Omer Reingold (Weizmann Institute of Science, Israel)

8:55-9:20 Many-to-one Trapdoor Functions and their Relation to Public-key Cryptosystems
Mihir Bellare (University of California at San Diego, USA), Shai Halevi (IBM T.J. Watson Research Center, USA), Amit Sahai, Salil Vadhan (MIT Laboratory for Computer Science , USA)

Session 10: IACR Distinguished Lecture
Chair: Andrew Odlyzko (AT&T Labs - Research, USA)

9:20-10:20 Authentication
Michael Rabin (Harvard University, USA, and Hebrew University, Israel)

10:20-10:45 Break

Session 11: Algebraic Schemes
Chair: Alfred Menezes (University of Waterloo, Canada)

10:45-11:10 An Efficient Discrete Log Pseudo Random Generator
Sarvar Patel, Ganapathy S. Sundaram (Lucent Technologies, USA)

11:10-11:35 Fast RSA-type Cryptosystem modulo $p^k q$
Tsuyoshi Takagi (NTT Software Laboratories, Japan)

11:35-12:00 An Elliptic Curve Implementation of the Finite Field Digital Signature Algorithm
Neal Koblitz (University of Washington, USA)

12:00-2:00 Lunch, De La Guerra Commons

Session 12: Quantum Cryptography

Chair: Dan Boneh (Stanford University, USA)

2:15-2:40 Quantum Bit Commitment From a Physical Assumption
Louis Salvail (University of Aarhus, Denmark)

Session 13: Signatures, Random Functions and Ideal Ciphers
Chair: Phillip Rogaway (University of California at Davis, USA)

2:40-3:05 On Concrete Security Treatment of Signatures Derived from Identification
Kazuo Ohta, Tatsuaki Okamoto (NTT Laboratories, Japan)

3:05-3:30 Building PRFs from PRPs
Chris Hall (Counterpane Systems, USA), David Wagner (University of California at Berkeley, USA), John Kelsey, Bruce Schneier (Counterpane Systems, USA)

3:30-3:55 Security Amplification by Composition: The Case of Doubly-Iterated, Ideal Ciphers
William Aiello (Bellcore, USA), Mihir Bellare, Giovanni Di Crescenzo (University of California at San Diego, USA), Ramarathnam Venkatesan (Microsoft Research, USA)

4:00-5:00 IACR Business Meeting

6:00-9:00 Beach Barbecue, Goleta Beach

8:00-10:30 Crypto Cafe, Anacapa Lounge

Thursday, August 27, 1998

7:00-8:00 Breakfast, De La Guerra Commons

Session 14: Zero Knowledge
Chair: Tal Rabin (IBM T.J. Watson Research Center, USA)

8:40-9:05 On the Existence of 3-Round Zero-Knowledge Protocols
Satoshi Hada, Toshiaki Tanaka (KDD R&D Laboratories, Japan)

9:05-9:30 Zero-Knowledge Proofs for Finite Field Arithmetic, or: Can Zero-Knowledge be for Free?
Ronald Cramer (ETH Zurich, Switzerland), Ivan Damgaard (Aarhus University, Denmark)

9:30-9:55 Concurrent Zero-Knowledge: Reducing the Need for Timing Constraints
Cynthia Dwork (IBM Almaden Research Center, USA), Amit Sahai (MIT Laboratory for Computer Science, USA)

9:55-10:20 Break

Session 15: Implementation
Chair: Jean-Jacques Quisquater (Universitè de Louvain, Belgium)

10:20-10:45 The Solution of McCurley's Discrete Log Challenge
Damian Weber (Institut fur Techno- und Wirtschaftsmathematik, Germany), Thomas F. Denny (debis IT Security Services, Germany)

10:45-11:10 Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms
Daniel Bailey, Christof Paar (Worcester Polytechnic Institute, USA)

Session 16: Rights Protection
Chair: Matt Franklin (AT&T Labs - Research, USA)

11:10-11:35 Time-Stamping with Binary Linking Schemes
Ahto Buldas, Peeter Laud, Helger Lipmaa, Jan Villemson (Küberneetika AS, Estonia)

11:35-12:00 Threshold Traitor Tracing
Moni Naor, Benny Pinkas (Weizmann Institute of Science, Israel)

12:00-2:00 Lunch, De La Guerra Commons

Adjourn