CRYPTO 2005
Rump Session Program

19:30 - 19:35 **Introduction**
Phong Nguyen

Session 1: Cryptanalysis

19:35 - 19:44 **New Collision Search for SHA-1**
Xiaoyun Wang, Andrew Yao and Frances Yao

19:44 - 19:49 **Experiments with DSA**
Daniel Bleichenbacher

19:49 - 19:54 **Discrete Logarithms in GF(p) and GF(2^n)**
Antoine Joux and Reynald Lercier

19:54 - 19:57 **Replication Attack and Cryptographic Research**
John Kelsey, Bruce Schneier, Serge Vaudenay, and David Wagner

Session 2: Side-Channel Cryptanalysis

19:57 - 20:03 **Full AES key extraction in 65 milliseconds using cache attacks**
Dag Arne Osvik, Adi Shamir, Eran Tromer

20:03 - 20:09 **Implementing crypto algorithms to defend against software side channels**
Ernie Brickell, Gary Graunke, Michael Neve, Jean-Pierre Seifert

20:09 - 20:11 **The geobacter attack: when nanotechnology meets chips**
Jean-Jacques Quisquater

Session 3: Announcements

20:11 - 20:15 **A Colossal Problem (revisited)**
Andy Clark

20:15 - 20:16 **EUROCRYPT2006**
Anatoly Lebedev

20:16 - 20:18 **ECC2005, ECC summer school, SHARCS'06 www.sharcs.org**
Tanja Lange

20:18 - 20:19 **PQCrypto 2006 workshop, http://postquantum.cr.yp.to**
Dan Bernstein

20:19 - 20:20 **Southern California Security and Cryptography Workshop**
Stanislaw Jarecki

20:20 - 20:21 **Mycrypt 2005**
Ed Dawson, Serge Vaudenay, Raphael C.-W. Phan

20:21 - 20:22 **Security In Storage Workshop**
James Hughes

20:22 - 20:23 **TCC2006**
Tal Rabin

20:23 - 20:24 **How to experience Italy with Unconditional Security**
Ivan Damgard

20:24 - 20:25 **The IACR fellows program**
Ivan Damgard

20:25 - 20:26 **IEEE P1363 Standards Activity**
William Whyte

20:26 - 20:27 **2005 IEEE Information Theory Workshop**
Yuliang Zheng

20:27 - 20:37 **BREAK**

Session 4: Hash Functions

20:37 - 20:43 **Herding Hash Functions**
John Kelsey and Tadayoshi Kohno

20:43 - 20:47 **Reusable Hash Collisions for Special File Formats**
Max Gebhardt, Georg Illies, Werner Schindler

20:47 - 20:50 **Collisions in Culture**
Hilarie Orman

20:50 - 20:56 **A Simple and Provably Good Code for SHA Message Expansion**
C. S. Jutla and A. C. Patthak

20:56 - 21:02 **VSH, an efficient and provable collision resistant hash function**
Scott Contini, Arjen K. Lenstra, Ron Steinfeld

21:02 - 21:06 **Can we get a Reduction Proof for Truncated Hashes?**
John Kelsey

21:06 - 21:09 **New Hash Function with Chaos**
Chil-Min Kim

21:09 - 21:13 **Paradoxes of the Birthday Paradox**
Iya Mironov

Session 5: Provable Security

21:13 - 21:17 **Perfect NIZK for NP**
Jens Groth and Rafail Ostrovsky and Amit Sahai

21:17 - 21:20 **Cramer-Shoup is Plaintext-Aware in the Standard Model**
Alexander W. Dent

21:20 - 21:24 **Stanford vs. UC: The Big Game**
A Datta, A Derek, J Mitchell, A Ramanathan, A Scedrov

21:24 - 21:28 **Provably Secure Substitution of Cryptographic Tools**
Lea Kissner and David Molnar

21:28 - 21:30 **Security Rituals <> the Pair-wise Union of Two Unbound Variables**
M. Briceno, J. Callas, T. Cannoy, J. Merchant, A. Shostack, N. Van Someren, R. Wagner

Session 6: Signatures

21:30 - 21:33 **NTRUSign Parameters Challenge**
Jeff Hoffstein, Nick Howgrave-Graham, Jill Pipher, Joe Silverman, William Whyte

21:33 - 21:36 **Efficient Designated Confirmer Signatures Without Random Oracles or Generic ZK Proofs**
Craig Gentry, David Molnar, and Zulfikar Ramzan

21:36 - 21:40 **Two Stories of Ring Signatures**
Yoshikazu Hanatani and Kazuo Ohta

Session 7: Symmetric stuff

21:40 - 21:44 **Designing cipher backwards**
Stephen Miller, Ilya Mironov, Venkie

21:44 - 21:48 **On the (im)possibility of blind MACs**
Michel Abdalla, Chanathip Namprempre, Gregory Neven

21:48 - 21:51 **Power Functions Over GF(2^n) for Infinitely Many n**
David Jedlicka

21:51 - 22:01 **BREAK**

Session 8: About Crypto '05

22:01 - 22:06 **Anonymous IBE without Random Oracles**
Dan Boneh and Brent Waters

22:06 - 22:10 **Klein Bottle Onion Routing: An Efficient Alternative to the Onion Routing by Camenisch and Lysyanskaya**
Kun Peng, Juanma González, Yvo Desmedt and Ed Dawson

22:10 - 22:15 **On Parallel and Concurrent Security of the HB and HB+ Protocols**
Jonathan Katz and Ji-Sun Shin

Session 9: Human Crypto

22:15 - 22:19 **Passwords – No Longer Viable**
Arvind Narayanan and Vitaly Shmatikov

22:19 - 22:23 **Visual Secret Sharing Schemes for Plural Secret Images Allowing the Rotation of Shares**
Kazuki Yoneyama, Mitsugu Iwamoto, Lei Wang, Noboru Kunihiro, Kazuo Ohta

22:23 - 22:26 **Ceremonies**
Carl Ellison

22:26 - 22:29 **Human-oriented encryption: from Solitaire to Multitaire**
Jean-Jacques Quisquater

Session 10: The End

22:29 - 22:33 **Secure Triggers**
Ariel Futoransky, Emiliano Kargieman, Carlos Sarruate, Ariel Waissbein

22:33 - 22:37 **Secure Computation with Honest Majority in Expected Constant Rounds**
Jonathan Katz and Chiu-Yuen Koo

22:37 - 22:40 **Password Authenticated Key Exchange Using Hidden Smooth Subgroups**
Craig Gentry, Phil Mackenzie, and Zulfikar Ramzan

22:40 - 22:43 **Digital Cinema System Specification V1.0**
Jean-Jacques Quisquater

GOOD NIGHT!