Ron 60  Fest!

May 11, 2007

Scientific Program (Patil/Kiva)

10am Prof. **Adi Shamir** (Weizmann Institute): *Cryptanalysis of Multivariate Schemes*

Newsflash: SFLASH —an obfuscated variant of the RSA— Gets Flushed
(Joint work with Dubois, Fouque, and Stern)

11am Prof. **Benny Chor** (The Technion): *Two Issues in Public Key Cryptography*

Crypto Wear & Tear: How Public-Key Issues Fare (Two Issues Two Decades Later)

2pm Prof. **Robert Schapire** (Princeton University): *The Story of Boosting*

From Big Bang to Date: The Tortuous Development of a Main Learning Technique

3pm Prof. **Anna Lysyanskaya** (Brown University): *Compact Ecash and Applications*

Big, Secret, and Quick: Anonymous Withdrawal of Huge Amounts of Cash in Tiny Time and Space
(Joint work with Camenisch, Hohenberger, Kohlweiss, and Meyerovich)

4pm Prof. **Susan Hohenberger** (John Hopkins University): *Authentication for Pervasive Communications*

A World of Words: How to Talk Fast to Everyone and Prove It's You!

Edible Program (4th Floor Common Area)

5:00-6:00 Pizza!

Attack Program (32-141)

MEMORY ATTACKS

6:00-6:20 Adi Shamir: *The R, the S, and the A in the RSA*

6:20-6:26 Shafi Goldwasser: *Can't Possibly Thank Ron in 5 Minutes*

ART ATTACK

6:26-6:30 Erik and Martin Demaine: *Ron on a Pedestal: Modern Monuments for Modern Men*

MIND ATTACK

6:30-8:00 Dr. Marc Salem (www.marcsalem.com): *Cryptography or Not, I'll Read Your Thought*