Contemporary Methods in Cryptography

Thursday January 10, 2002

12:00–1:00 *Registration*

1:00–1:50 **Russell Impagliazzo** (University of California at San Diego)
Applications of the Goldreich-Levin Theorem

1:50–2:00 *Break*

2:00–2:50 **Russell Impagliazzo** (University of California at San Diego)
Applications of the Goldreich-Levin Theorem

2:50–3:10 *Break*

3:10–4:00 **Kazue Sako** (NEC)
Electronic Voting

4:00–4:10 *Break*

4:10–5:00 **Kazue Sako** (NEC)
Electronic Voting

Thursday January 10, 2002

8:00–9:00 *Continental Breakfast*

9:00–9:50 **Dan Boneh** (Stanford University)
New Tools in Cryptography from Algebraic Geometry

9:50–10:00 *Break*

10:00–10:50 **Cynthia Dwork** (Microsoft Research)
2-Round Zero Knowledge and Proof Auditors

10:50–11:00 *Break*

11:00–11:50 **Ravi Kumar** (IBM Almaden Research Center)

11:50–2:00 *Lunch (on your own)*

2:00–2:50 **Daniele Micciancio** (University of California at San Diego)
From Ajtai-Dwork to NTRU: the design of practical lattice based cryptosystems

2:50–3:10 *Break*

(Thursday schedule continued on next page)

(Thursday schedule continued from previous page)

3:10–4:00 **Nick Howgrave-Graham** (NTRU Cryptosystems)
Using lattices for Crypto

4:00–4:10 *Break*

4:10–5:00 **Noam Elkies** (Harvard University)
Lattice reduction and approximate Diophantine equations: Further applications and results

5:00–12:00 *Dinner (Hosted by IPAM)*

Friday January 11, 2002

8:00–9:00 *Continental Breakfast*

9:00–9:50 **Neal Koblitz** (University of Washington)
Elliptic Curve Cryptography: which curves to use?

9:50–10:00 *Break*

10:00–10:50 **Joseph Silverman** (Brown University)
The Four Faces of Lifting for the Elliptic Curve Discrete Logarithm Problem

10:50–11:00 *Break*

11:00–11:50 **Edlyn Teske** (University of Waterloo, Canada)
On the Weil descent attack on the elliptic curve discrete logarithm problem

11:50–2:00 *Lunch (on your own)*

2:00–2:50 **Kumar Murty** (University of Toronto)
Elliptic curves and sieve methods

2:50–3:10 *Break*

3:10–4:00 **Antoine Joux** (DCSSI)
The Function Field Sieve in GF(2^n)

4:00–4:10 *Break*

4:10–5:00 **Kristin Lauter** (Microsoft Research)
Attacking the Discrete Log Problem on Elliptic Curves from above

Saturday January 12, 2002

8:00–9:00	*Continental Breakfast*
9:00–9:50	**Dorian Goldfeld** (Columbia University) *A Linear Time Matrix Key Agreement Protocol*
9:50–10:00	*Break*
10:00–10:50	**Luca Trevisan** (UC Berkeley) *Lower Bounds for Linear Locally Decodable Codes and Private Information Retrieval*
10:50–11:00	*Break*
11:00–11:50	**Kobbi Nissim** (Rutgers University) *Private approximation of NP-hard functions*
11:50–2:00	*Lunch (on your own)*
2:00–2:50	**Alice Silverberg** (Ohio State University) *The best and worst of supersingular abelian varieties in cryptography*
2:50–3:10	*Break*
3:10–4:00	**David Wagner** (University of California at Berkeley) *Analysis and design of symmetric ciphers*
4:00–4:10	*Break*
4:10–5:00	**Moni Naor** (Weizmann Institute of Science) *Deniable Ring Authentication*

Sunday January 13, 2002

8:00–9:00	*Continental Breakfast*
9:00–9:50	**Omer Reingold** (AT&T) *Exploring the Worlds Between Minicrypt and Cryptomania, Part I*
9:50–10:00	*Break*
10:00–10:50	**Tal Malkin** (AT&T) *Exploring the Worlds Between Minicrypt and Cryptomania, Part II*
10:50–11:00	*Break*
11:00–11:50	**Steven Rudich** (Carnegie Mellon University) *Formal Program Obfuscation*