Workshop I: Number Theory and Cryptography - Open Problems

Monday October 9, 2006

8:00–8:45 *Check-In/Light Breakfast (Hosted by IPAM)*

8:45–9:00 *Welcome and Opening Remarks*

9:00–10:00 **Antoine Joux** (Université Versailles/Saint Quentin-en-Yvelines)
Discrete Logarithm in all finite fields Short

10:00–10:30 *Break*

10:30–11:30 **Ronald Rivest** (Massachusetts Institute of Technology)
Controlled Algebras and GII's

11:30–1:30 *Lunch (on your own)*

1:30–2:30 **Pascal Paillier** (Gemplus)
Can RSA keys be instance-malleable?

2:30–2:45 *Break*

2:45–3:45 **Peter Montgomery** (Microsoft Research)
Searching for Higher-Degree Polynomials for the General Number Field Sieve

3:45–4:15 *Break*

4:15–5:15 **Johannes Buchmann** (Technishche Universtitat Darmstadt)
CMSS - An efficient version of the Merkle signature scheme

5:15–7:00 *Wine/Cheese Reception (Hosted by IPAM)*

Tuesday October 10, 2006

8:00–9:00 *Continental Breakfast*

9:00–10:00
TBA

10:00–10:30 *Break*

(Tuesday schedule continued on next page)

(Tuesday schedule continued from previous page)

10:30–11:30 **Denis Charles** (Microsoft Research)
Computing isogenies on elliptic curves

11:30–1:30 *Lunch (on your own)*

1:30–2:30 **Tanja Lange** (Technische Universiteit Eindhoven)
Open Problems in Pairings

2:30–2:45 *Break*

2:45–3:45 **Igor Shparlinski** (Macquarie University)
Group structure of elliptic curves over finite fields

3:45–4:15 *Break*

4:15–5:15 **Neal Koblitz** (University of Washington)
Generic Groups

5:30–7:00 *Dinner (Hosted by IPAM)*

Wednesday October 11, 2006

8:00–9:00 *Continental Breakfast*

9:00–10:00 **Renate Scheidler** (University of Calgary)
Real Hyperelliptic Curves

10:00–10:15 *Break*

10:15–11:15 **Kristin Lauter** (Microsoft Research)
Algorithms for computing genus 2 curves for use in cryptography

11:15–11:45 *Break*

11:45–12:45 **Phong Nguyen** (École Normale Supérieure)
Hermite's Constant and Lattice Reduction

12:45–2:00 *Lunch (on your own)*

2:00–3:00 **Yvo Desmedt** (University College London)
Trapdoor-Free RSA Like Assumption

4:00–5:00 *Igor Shparlinski, Macquarie University "Inversions " (* talk located in Math Science (MS) Bldg. 6943)*

5:15–6:15 *Joseph Silverman, Brown University "Dynamical Systems from an Arithmetical Viewpoint "(* talk located in Math Science (MS) Bldg. 6943)*

Thursday October 12, 2006

8:00–9:00 *Continental Breakfast*

9:00–10:00 **Gerhard Frey** (Universität Duisburg-Essen)
Duality in Arithmetic Geometry and Applications to Discrete Logarithms

10:00–10:30 *Break*

10:30–11:30 **Wayne Raskind** (University of Southern California)
Global duality and the discrete logarithm problem in abelian algebraic groups over finite fields (joint work with Ming-Deh Huang).

11:30–1:30 *Lunch (on your own)*

1:30–2:30 **Everett Howe** (Center for Communications Research)
Low-genus curves over finite fields

2:30–2:45 *Break*

2:45–3:45 **Jean-Marc Couveignes** (Université de Toulouse II (Le Mirail))
Linearizing torsion classes in the Picard group of algebraic curves over finite fields

3:45–4:15 *Break*

4:15–5:15 **Kiran Kedlaya** (Massachusetts Institute of Technology)
Recent results on p-adic computation of zeta functions

Friday October 13, 2006

8:00–9:00 *Continental Breakfast*

9:00–10:00 **Joseph Silverman** (Brown University)
Independence of Heegner Points

10:00–10:15 *Break*

10:15–11:15 **Kirsten Eisentraeger** (University of Michigan)
On the computation of the Cassels pairing and applications to cryptography

11:15–11:30 *Break*

11:30–12:30 **Daniele Micciancio** (University of California, San Diego)
Cyclic lattices: cryptographic applications and open problems

12:30–1:30 *Lunch (on your own)*

1:30–2:30 **Alexander May** (Technishche Universtitat Darmstadt)
On Solving Number Theoretic Problems with Lattice Reduction

2:45–3:45 **Ming-Deh Huang** (University of Southern California)
The height function and the elliptic curve discrete logarithm problem