Graduate Summer School on Post-quantum and Quantum Cryptography

Monday July 25, 2022

8:00–8:50	*Check-In/Breakfast (Hosted by IPAM)*
8:50–9:00	*Welcome & Opening Remarks: Dean Miguel García-Garibay (Dean of Physical Sciences, UCLA) and Dima Shlyakhtenko (Director, IPAM)*
9:00–10:30	**Jonathan Katz** (University of Maryland) *Introduction to Cryptography I*
10:30–11:00	*Break*
11:00–12:00	**Jonathan Katz** (University of Maryland) *Introduction to Cryptography II*
12:00–1:45	*Lunch (on your own)*
1:45–2:45	**Jonathan Katz** (University of Maryland) *Introduction to Cryptography III*
2:45–3:15	*Break*
3:15–4:15	*TA Session I*
4:15–5:45	*Poster Session & Reception (Hosted by IPAM)*

Tuesday July 26, 2022

8:00–9:00	*Check-In/Breakfast (Hosted by IPAM)*
9:00–10:30	**Fang Song** (Portland State University) *Introduction to quantum computing I*
10:30–11:00	*Break*
11:00–12:00	**Fang Song** (Portland State University) *Introduction to quantum computing II*
12:00–1:45	*Lunch (on your own)*
1:45–2:45	**Fang Song** (Portland State University) *Introduction to quantum computing III*
2:45–3:15	*Break*

(Tuesday schedule continued on next page)

(Tuesday schedule continued from previous page)

3:15–4:15 *TA Session II*

4:15–5:45 **Craig Costello** (Microsoft Research)
Post-quantum key exchange from supersingular isogenies

Wednesday July 27, 2022

8:00–9:00 *Check-In/Breakfast (Hosted by IPAM)*

9:00–10:30 **Anne Broadbent** (University of Ottawa)
Information-Theoretic Quantum Cryptography

10:30–11:00 *Break*

11:00–12:30 **Anne Broadbent** (University of Ottawa)
Information-Theoretic Quantum Cryptography

12:30–2:15 *Lunch (on your own)*

2:15–3:45 **Chris Peikert** (University of Michigan)
Post Quantum assumptions II

3:45–4:15 *Break*

4:15–5:45 *Mentoring Session*

Thursday July 28, 2022

8:00–9:00 *Check-In/Breakfast (Hosted by IPAM)*

9:00–10:30 **Dominique Unruh** (Tartu State University)
The quantum random oracle model I

10:30–11:00 *Break*

11:00–12:30 **Dominique Unruh** (Tartu State University)
The quantum random oracle model II

12:30–2:15 *Lunch (on your own)*

2:15–3:45 **Fermi Ma** (University of California, Berkeley (UC Berkeley))
Post-Quantum Proof Techniques, Part 1: Introduction to Quantum Rewinding

3:45–4:15 *Break*

4:15–5:45 **Fermi Ma** (University of California, Berkeley (UC Berkeley))
Post-Quantum Proof Techniques, Part 2: How to Rewind a Quantum Attacker Many Times

Friday July 29, 2022

8:00–9:00 *Check-In/Breakfast (Hosted by IPAM)*

9:00–10:30 **Dakshita Khurana** (University of Illinois at Urbana-Champaign)
Weakening Assumptions in Quantum Cryptography IV. a

10:30–11:00 *Break*

11:00–12:30 **Dakshita Khurana** (University of Illinois at Urbana-Champaign)
Weakening Assumptions in Quantum Cryptography IV.b