University of Windsor

SAC2022

SAC2022 Summer School Program

(All tutorials/breaks/lunches will take place in the CEI Building)

Monday, 22 August 2022 (Room 3000, CEI)

08:30-09:00	Registration
09:00-10:30	*Tutorial 1: From modern elliptic-curve cryptography to post-quantum isogeny-based cryptography* Benjamin Smith
10:30-11:00	Coffee break
11:00-11:15	Self-introductions/mini-presentations by audience
11:15-12:15	*Tutorial 1 continued*
12:15-13:45	Lunch break
13:45-15:15	*Tutorial 2: Integrating post-quantum cryptography in real-world protocols* Douglas Stebila
15:15-15:45	Coffee break
15:45-16:00	Self-introductions/mini-presentations by audience
16:00-17:00	*Tutorial 2 continued*
17:00-17:30	Skillshare slot

Tuesday, 23 August 2022 (Room 2101, CEI)

09:00-10:30	*Tutorial 3: Quantum computing and isogeny-based cryptography* Javad Doliskani
10:30-11:00	Coffee break
11:00-11:15	Self-introductions/mini-presentations by audience
11:15-12:15	*Tutorial 3 continued*
12:15-13:45	Lunch break
13:45-15:15	*Tutorial 4: Foundations for the Castryck-Decru and Maino-Martindale attacks on SIDH and SIKE* Benjamin Smith
15:15-15:45	Coffee break
15:45-16:00	Self-introductions/mini-presentations by audience
16:00-17:00	*Tutorial 4 continued*
17:00-17:30	Skillshare slot