Workshop on Formal and Computational Cryptography

THURSDAY JUNE 26	FCC Workshop Steinberg Auditorium, Baker Hall A53
8:30-8:55	**Registration**
8:55-9:00	**Welcome**
9:00-10:00	**Invited Talk** Gilles Barthe (joint work with Benjamin Gregoire, Roman Janvier, Federico Olmedo, Santiago Zanella Beguelin) *Formal Verification of Code-based Cryptographic Proofs*
10:00-10:30	Hubert Comon-Lundh, Veronique Cortier *Computational Soundness of Observational Equivalence*
10:30-11:00	**Break**
11:00-11:30	Cedric Fournet, Gurvan Le Guernic, Tamara Rezk *A Cryptographic Compiler for Information-Flow Security*
11:30-12:00	Pedro Adao, Cedric Fournet, Nataliya Guts, Francesco Zappa Nardelli *High-Level Programming for E-Cash (work in progress)*
12:00-12:30	Michael Backes, Matthias Berg, Dominique Unruh *A Formal Language for Cryptographic Pseudocode*
12:30-2:00	**Lunch**
2:00-2:30	Christian Ene, Judicael Courant, Yassine Lakhnech, Marion Daubignard, Pascal Lafourcade *Automated Proofs for Asymmetric Encryption*
2:30-3:00	Karthikeyan Bhargavan, Ricardo Corin, Cedric Fournet, Eugen Zalinescu *Cryptographically Verified Implementations for TLS*
3:00-3:30	Aaron D. Jaggard, Catherine Meadows, Michael Mislove *Task Probabilistic Input/Output Automata as Domains*
3:30-4:00	Anupam Datta, Joseph Halpern, John Mitchell, Riccardo Pucella, Arnab Roy *Reasoning about Conditional Probability and Concrete Security in Protocol Proofs (work in progress)*
4:00-4:30	**Break** End of workshop