

Preliminary Program

Thursday June 23th

Session 1 B. Blanchet	9 :00 - 9 :15	Welcome and organizational information	M. ABADI R. KÜSTERS
	9 :15 - 9 :25	Introduction	
	9 :25 - 10 :05	On the Relationships Between Notions of Simulation-Based Security	
break			
Session 2 A. Scedrov	10 :35 - 11 :05	Universally Composable Symbolic Analysis of Cryptographic Protocols	R. CANETTI
	11 :05 - 11 :45	Justifying Formal Methods and Cryptography under Active Attacks, and Limitations Thereof	M. BACKES
	11 :45 - 12 :00	Simulatable Security and Concurrent Composability	D. HOFHEINZ
lunch			
Session 3 M. Backes	14 :00 - 14 :45	Soundness of Formal Encryption in the Presence of Key-Cycles	G. BANA
	14 :45 - 15 :30	Computationally Sound Implementations of Equational Theories against Passive Adversaries	M. BAUDET
break			
Session 4 C. Fournet	16 :00 - 16 :45	Computationally sound verification of cryptographic protocols with more cryptographic primitives	L. MAZARE
	16 :45 - 17 :00	Computationally sound security proofs using formal models	V. CORTIER
	17 :00 - 17 :15	Towards a notion of Quantitative Security Analysis	I. CERVESATO
	17 :15 - 18 :00	Combining intruder theories	Y. CHEVALIER

Friday June 24th

Session 5 J. Guttman	9 :00 - 9 :45	Probabilistic and nondeterministic aspects of Anonymity	C. PALAMIDESSI
	9 :45 - 10 :00	Probable innocence revisited	K. CHATZIKOKOLAKIS
	10 :00 - 10 :15	The Computer Ate My Vote	P. RYAN
break			
Session 6 P. Ryan	10 :45 - 11 :30	Cryptographic Protocol Logic : A Synthetic Approach	S. KRAMER
	11 :30 - 11 :45	PS-LTL for constraint-based security protocol analysis	A. SAPTAWIJAYA
	11 :45 - 12 :00	Skeletons and the Shapes of Bundles	J. GUTTMAN
lunch			
Session 7 R. Canetti	14 :00 - 14 :45	Cryptographic Protocols and Abstract Algorithms	D. RUNJE
	14 :45 - 15 :00	A machine-checker formalization of the generic model and the random oracle model	S. TARENTO
	15 :00 - 15 :30	A Computationally Sound Automatic Prover for Cryptographic Protocols	B. BLANCHET
break			
Session 8 Y. Lakhnech	16 :00 - 16 :20	Probabilistic polynomial-time semantics for a protocol security logic	M. TURUANI
	16 :20 - 16 :40	Guessing Attacks in the pi-calculus with a Computational Justification	T. CHOTHIA