

AFOSR Cyber Security Program Review

Agenda Day 1 - Monday, 21 May 2018

Time	Topic*	Speaker
8:00-8:20	Registration And Speaker Setup	
8:20-8:30	Introduction	Tristan Nguyen, Lt. Col. Mario Serna, Lt. Col. Ryan Thomas International Office
8:30-9:00	Foundations of Nanoelectronic Physically Unclonable Computing Systems	Garrett Rose University of Tennessee, Knoxville
9:00-9:30	Policy Enforcement by Using Security Labels	Fred Schneider Cornell University
9:30-10:00	Break & Discussion	
10:00-10:30	Provably Secure Cyber-Physical Systems	Andre Platzer CMU
10:30-11:00	Cloud ARMS (Allocation, Replication, Monitoring, and Sharing)	Laurent Njila AFRL/RI
11:00-12:30	LUNCH	
12:30-1:00	Models and Protocols for Quantum Distributed Computation	Jason Morton Penn State
1:00-1:30	Meta-models of Machine Learning for Adversarial Machine Learning	Maria Jose Ramirez Valencia Polytechnic
1:30-2:30	Break & Discussion	
2:30-3:00		

*Titles subject to change

3:00-3:30		
3:30-4:00	Break & Discussion	
4:00	ADJOURN FOR THE DAY	

*Titles subject to change

AFOSR Cyber Security Program Review

Agenda Day 2 - Tuesday, 22 May 2018

Time	Topic*	Speaker
8:00-8:20	Registration And Speaker Setup	
8:20-8:30	Introduction	Tristan Nguyen, Lt. Col. Mario Serna, Lt. Col. Ryan Thomas AFOSR, AOARD, EOARD
8:30-9:00	Entrapping Machine	Elham Kashefi University of Edinburgh
9:00-9:30	Feasible Quantum Technology for Secure Classical Computing	Philip Walther University of Vienna
9:30-10:00	Break & Discussion	
10:00-10:30	Quantum primitives for secure computing	Joseph Fitzsimons Singapore University of Technology and Design
10:30-11:00	Quantum Networking	Rod van Meter Keio University
11:00-12:30	LUNCH	
12:30-1:00	Writing and Securing Peer-to-Peer Computation	Stephen Chong Harvard University
1:00-1:30	Verification of quantum cryptography	Dominique Unruh University of Tartu
1:30-2:30	Break & Discussion	
2:30-3:00	Monitoring at Any Cost	Srdjan Kristic and Joshua Schneider ETH Zurich

*Titles subject to change

3:00-3:30		
3:30-4:00	Break & Discussion	
4:00	ADJOURN FOR THE DAY	

*Titles subject to change

AFOSR Cyber Security Program Review

Agenda Day 3 - Wednesday, 23 May 2018

Time	Topic*	Speaker
8:00-8:20	Registration And Speaker Setup	
8:20-8:30	Introduction	Tristan Nguyen, Lt. Col. Mario Serna, Lt. Col. Ryan Thomas AFOSR, AOARD, EOARD
8:30-9:00	Foundations and Applications of Program Obfuscation	Rafael Pass Cornell University
9:00-9:30	New Directions in Secure Computation via Function Secret Sharing	Elette Boyle Interdisciplinary Center (IDC) Herzliya
9:30-10:00	Break & Discussion	
10:00-10:30	Feasible device-independent quantum cryptography	Renato Renner ETH Zurich
10:30-11:00		
11:00-12:30	LUNCH	
12:30-1:00	Making Cryptography at the Edges Reliable	Sanjam Garg University of California, Berkeley
1:00-1:30	Realizing the promise of proof-based verifiable computation	Mike Walfish New York University
1:30-2:30	Break & Discussion	
2:30-3:00	Advanced symbolic methods for the cryptographic protocol analyzer Maude-NPA	Santiago Escobar Valencia Polytechnic

*Titles subject to change

3:00-3:30		
3:30-4:00	Break & Discussion	
4:00	ADJOURN FOR THE DAY	

*Titles subject to change

AFOSR Cyber Security Program Review

Agenda Day 4 - Thursday, 24 May 2018

Time	Topic*	Speaker
8:00-8:20	Registration And Speaker Setup	
8:20-8:30	Introduction	Tristan Nguyen, Lt. Col. Mario Serna, Lt. Col. Ryan Thomas AFOSR, AOARD, EOARD
8:30-9:00	Monoidal Computers, Networks and Strategic Learning: Methods for Adaptive Defense in Cyber Security	Dusko Pavlovic University of Hawaii
9:00-9:30	Accountable Predictive Systems	Anupam Datta Carnegie Mellon University
9:30-10:00	Break & Discussion	
10:00-10:30	Foundations of Type Theory for Computation and Mathematics	Andrej Bauer University of Ljubljana
10:30-11:00	Verification of Quantum Computations	Anne Broadbent University of Ottawa
11:00-12:30	LUNCH	
12:30-1:00	Sheaves as models for cybersecurity	Sanjeevi Krishnan Ohio State University
1:00-1:30	Atomically Unique Physically Uncloneable Functions	Robert Young Lancaster University
1:30-2:30	Break & Discussion	
2:30-3:00	Foundations of Language-Based Provenance Security	Wilmer Ricciotti University of Edinburgh

*Titles subject to change

3:00-3:30	Statespace Enhancements for Network Security Protocol Model Checkers	Cas Cremers Oxford University (tentative)
3:30-4:00	Break & Discussion	
4:00	ADJOURN FOR THE DAY	

*Titles subject to change

AFOSR Cyber Security Program Review

Agenda Day 5 - Friday, 25 May 2018

Time	Topic*	Speaker
8:00-8:20	Registration And Speaker Setup	
8:20-8:30	Introduction	Tristan Nguyen, Lt. Col. Mario Serna, Lt. Col. Ryan Thomas AFOSR, AOARD, EOARD
8:30-9:15	Efficient Characterization of High-Dimensional Quantum Systems	Paul Alsing AFRL/RI
9:15-10:00	Gravitational Effects on the Free Space Quantum Key Distribution for Satellite Communication	Warner Miller & Doysol Ahn Florida Atlantic University & University of Seoul
10:00-10:30	Break & Discussion	
10:30-11:15	Integrated approaches of physically unclonable cryptographic primitives using random lasers and optoelectronics	Young Kim & Young Min Song Purdue University & Gwangju Institute of Science and Technology
11:15-12:00	Towards Provable-secure Multi-party Authenticated Key Exchange Protocol based on Lattices in a Quantum World	Jintai Ding & Kwangjo Kim University of Cincinnati & KAIST
12:00-1:30	LUNCH	
1:30-2:15	Single Quantum Emitters based on Strained Quantum Dots in Two-dimensional Semiconductors	SungWoo Nam & Hong-Gyu Park University of Illinois, Urbana-Champaign & Korea University
2:15-3:00	Rule Specification-based Misbehavior Detection for IoT-Embedded Cyber Physical Systems	Ing-Ray Chen Chen & Il-sun You Virginia Tech & Soonchunhyang University

*Titles subject to change

3:00-3:45	Biological Primitives to Analyze Complexity for Telecom	Nicola Marchetti, Irene MacAluso Trinity College Dublin
3:45	ADJOURN FOR THE DAY	

*Titles subject to change