

# 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	<b>ADJOURN FOR THE DAY</b>	

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

\*Titles subject to change

3:00-3:30		
3:30-4:00	Break & Discussion	
4:00	<b>ADJOURN FOR THE DAY</b>	

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

\*Titles subject to change

3:00-3:30		
3:30-4:00	Break & Discussion	
4:00	<b>ADJOURN FOR THE DAY</b>	

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

\*Titles subject to change

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

\*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 & Ilsun You Virginia Tech & Soonchunhyang University

\*Titles subject to change

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

\*Titles subject to change