Karim Eldefrawy

karim.eldefrawy@sri.com
Personal Home Page
LinkedIn Home Page

Work Address
Office EL-256, 333 Ravenswood Avenue
Menlo Park, CA 94025
Work Phone: (650) 859-5388

Profiles
Google Scholar
Research Gate
DBLP

EDUCATION

Ph.D. and M.Sc. August 2010 and May 2008
Donald Bren School of Information and Computer Science
University of California, Irvine (UCI)
Adviser - Gene Tsudik

M.Sc. and B.Sc. August 2005 and July 2003
Department of Electrical Engineering
Cairo University, Egypt

HONORS AND AWARDS

Awards and Nominations

Nominated for"Living the Mission (Individual Contributor)" Award at SRI	2019
Distinguished Inventor Award at HRL Laboratories	2015
New Inventor Award at HRL Laboratories	2013
Winner of the Computer Science HiTEC Product Development Competition at UCI	2008
3rd Place in the Merage Business Plan Competition at UCI	2008

Fellowships

Department of Education Graduate Assistant in Areas of National Need (GAANN) Fellowship	2007-2010
AT&T Virtual University Research Initiative (VURI) Program	2007-2008
UCI Calit2 Emulex Graduate Fellowship	2006-2007
UCI Center for Pervasive Communication and Computing (CPCC) Graduate Fellowship	2006-2007
UCI Information and Computer Science Graduate Fellowship	2005-2006

RESEARCH AND INDUSTRY EXPERIENCE

SRI International (formerly Stanford Research Institute), Menlo Park, CA
Principal Computer Scientist at the SRI Computer Science Lab (CSL) January 2017 – Present

HRL Laboratories (formerly Hughes Research Laboratories), Malibu, CA
Research Staff Scientist, Research Staff Member, Postdoctoral Researcher October 2010 – December 2016

System Security Group at ETH Zurich, Zurich, Switzerland
Visiting Academic Researcher (Hosted by Prof. Srdjan Capkun) February 2009 – August 2009

AT&T Research Labs, Florham Park, NJ
Research Summer Internship (Hosted by Dr. Balachander Krishnamurthy) May 2007 – August 2007

Donald Bren School of Information and Computer Science, Irvine, CA
Graduate Student Researcher (Advised by Prof. Gene Tsudik) September 2005 – August 2010

SySDSoft (acquired by Intel in 2011), Cairo, Egypt
M.Sc. Thesis on "OFDMA Subcarrier Allocation" as a Systems Engineer — October 2003 – August 2005

Cisco Systems, San Jose, CA
Summer Internship — June 2002 – September 2002

Bell Labs Lucent Technologies, Naperville, IL
Summer Internship — June 2001 – September 2001

TEACHING EXPERIENCE

As Instructor

1. *2019 Fall Semester (11 students):* "Security and Privacy" graduate course (CS683) at the Department of Computer Science at the University of San Francisco.
2. *2018 Spring Semester (12 students):* "Security and Privacy" graduate course (CS683) at the Department of Computer Science at the University of San Francisco.
3. *2016 Fall Quarter (106 students):* "Elements of Cryptography and Computer and Network Security" undergraduate course (CS134) at the Donald Bren School of Information and Computer Science at the University of California, Irvine.
4. *2014 Winter Quarter (34 students):* "Advanced Networking Lab" graduate course (CS233/NETSYS202) at the Donald Bren School of Information and Computer Science at the University of California, Irvine.
5. *2013 Spring Quarter (120 students):* "Computer Networking" undergraduate course (CS132/EECS148) at the Donald Bren School of Information and Computer Science at the University of California, Irvine.
6. *2013 Winter Quarter (33 students):* "Advanced Networking Lab" graduate course (CS233/NETSYS202) at the Donald Bren School of Information and Computer Science at the University of California, Irvine.

As Teaching Assistant

1. *2006 Spring Quarter:* "Computer Networking" undergraduate course (CS132/EECS148) at the Donald Bren School of Information and Computer Science at the University of California, Irvine.
2. *2006 Winter Quarter:* "Advanced Networking Lab" undergraduate course (CS133) at the Donald Bren School of Information and Computer Science at the University of California, Irvine.

FUNDING

Extramurally Funded at SRI (over $11 million)

- *2020 - 2022: SRI's Principal Investigator of:* "LOQI: Leveraging Optimization using Quantum-devices for Internet-security" member of a team led by QC Ware (PI Prof. Wim van Dam) funded by the Air Force Quantum Collider program.
- *2020 - 2024: Co-Principal Investigator of:* "EMPHASIZE: End-to-end Machinery for Proving Highly sensitive Application-oriented Statements In ZEro-knowledge," funded by the U.S. Defense Advanced Research Project Agency (DARPA) under theSecuring Information for Encrypted Verification and Evaluation (SIEVE) program.
- *2019 - 2023: Principal Investigator of:* "PRISM: PRivacy-preserving Intrusion-resilient Secure Multi-party-computation (for anonymous messaging)," funded by the U.S. Defense Advanced Research Project Agency (DARPA) under the Resilient Anonymous Communication for Everyone (RACE) program.
- *2018: Principal Investigator of:* "ALICE: Automated Late-stage Instrumentation of Cryptographic Executables," funded as a seedling by the U.S. Department of Homeland Security (DHS).

- *2017: Principal Investigator of:* "SRI-AB: Secure and Resilient Identification and Access-control using Biometrics," funded as a seedling by the U.S. Department of Homeland Security (DHS).

Intramurally Funded at SRI

- Principal Investigator of a 2020 project on computer-aided verification of secure multi-party computation protocols and consensus and Byzantine agreement protocols.
- Principal Investigator of a 2019 project on computer-aided verification of secure multi-party computation protocols.
- Principal Investigator of a 2018 project on designing efficient secure multi-party computation protocols for blockchains and other applications.
- Principal Investigator of a 2018 project on analyzing public blockchain-based cryptocurrencies.

Extramurally Funded at HRL (over $3.5 million)

- *2016 - 2017: Principal Investigator of* "ABC: Acquiring Biometrics with Cryptography," funded by the U.S. Intelligence Advanced Research Project Activity (IARPA).
- *2015 - 2017: Task Lead for Secure Remote Attestation and Software Updates on* "Side-channel Security Analysis and Secure Software Updates for Cyber-Physical Systems," funded from by the U.S. Department of Homeland Security (DHS).
- *2013 - 2017: Co-Principal Investigator of* "Cloud-COP: A Secure Cloud Control and Operation Plane," funded from 2013 to 2016 by the U.S. Department of Homeland Security (DHS).

Intramurally Funded at HRL

- 2011 - 2014: Principal Investigator leading projects designing and implementing: (i) efficient secure multi-party computation (MPC) protocols for distributed computations on networks of untrusted hosts and clouds, and (ii) cryptographic protocols for secure and privacy-preserving search of text and images.
- 2015 - 2016: Principal Investigator for projects funded by Boeing for developing algorithms and automated tools for mapping network service dependencies and generating network traffic filtering rules for airplanes.

PUBLICATIONS

Refereed Journals and Magazine Articles

1. Ivan De Olivera Nunes, Karim Eldefrawy, Tancrede Lepoint, "Non-interactive User Re-enrollment in Cryptographically Secured Biometrics-based Identification and Authentication Systems," Elsevier Journal on Future Generation Computer Systems (FGCS), Volume 98, September 2019, Pages 259-273.
2. Karim Eldefrawy and Vincent Sritapan, "Security Threats, Defenses, and Recommended Practices for Enterprise Mobility," Information Systems Security Association (ISSA) Journal, Vol. 16 No. 5, May 2018.
3. Joshua Baron, Karim Eldefrawy, Kirill Minkovich, Rafail Ostrovsky, Eric Tressler, "5PM: Secure Pattern Matching", Journal of Computer Security (JCS), Vol. 21 No. 5, September 2013.
4. Karim Eldefrawy, Sky Faber, "Blindfolded Searching of Data via Secure Pattern Matching", in IEEE Computer Magazine, Vol. 46 No.12 , December 2013.
5. Mishari Al Mishari, Emiliano De Cristofaro, Karim Eldefrawy, Gene Tsudik, "Harvesting SSL Certificate Data to Mitigate Web-Fraud", International Journal of Network Security (IJNS), Vol. 14 No. 6, November 2012.
6. Karim Eldefrawy, Gene Tsudik,"Privacy-Preserving Location-Based On-Demand Routing in MANETs", IEEE Journal of Selected Areas of Communication (IEEE JSAC), Vol. 29 No. 10, December 2011.
7. Karim Eldefrawy, Gene Tsudik,"Anonymous Location Aided Routing in Suspicious MANETs", IEEE Transactions on Mobile Computing (IEEE TMC), Vol. 10 No. 9, September 2011.

Book Chapters and Books

1. Karim Eldefrawy, Rafail Ostrovsky, Moti Yung, "Theoretical Foundations of Moving Target Defense: Proactive Secret Sharing and Secure Multi-party Computation," From Database to Cyber Security, Springer International Publishing, 2018.

Refereed Conferences and Workshops

1. Karim Eldefrawy, Seoyeon Hwang, Moti Yung, Rafail Ostrovsky, "Communication-Efficient (Proactive) Secure Computation for Dynamic General Adversary Structures and Dynamic Groups", in proceedings of the12th Conference Security and Cryptography in Networks (SCN), 2020.
2. Ivan De Olivera Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, Gene Tsudik "APEX: Architecture for Provable EXecution", in proceedings of the 29th Usenix Security Symposium, 2020.
3. Karim Eldefrawy, Michael Locasto, Norrathep Rattanavipanon, Hassen Saidi, "ALICE: Automated-augmentation of Legacy and Insecure Cryptographic Executables", in proceedings of the 18th International Conference on Applied Cryptography and Network Security (ACNS), 2020.
4. Karim Eldefrawy, Tancrede Lepoint, Antonin Leroux "Communication Efficient Proactive Secret Sharing for Dynamic Groups with Dishonest Majorities", in proceedings of the 18th International Conference on Applied Cryptography and Network Security (ACNS), 2020.
5. Karim Eldefrawy, Vitor Pereira, "A High-Assurance Evaluator for Machine-Checked Secure Multi-Party Computation", in proceedings of the ACM Conference on Computer and Communications Security (CCS), 2019.
6. Ivan De Olivera Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, Michael Steiner, Gene Tsudik, "VRASED: A Verified Hardware/Software Co-Design for Remote Attestation," in proceedings of the Usenix Security Symposium, 2019.
7. Karim Eldefrawy, Ashish Gehani, Alexandre Matton, "Longitudinal Study of Misuse of Bitcoin," in proceedings of the International Conference on Applied Cryptography and Network Security (ACNS'19), 2019.
8. Karim Eldefrawy, Gene Tsudik, "Opinion: Advancing Remote Attestation via Computer-aided Formal Verification," in proceedings of the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (Wisec), 2019.
9. Ivan De Oliveira Nunes, Karim Eldefrawy, Norrathep Rattanavipanon, Gene Tsudik, "PURE: Using Verified Remote Attestation to Obtain Proofs of Update, Reset and Erasure in Low-End Embedded Systems," in proceedings of the IEEE/ACM International Conference On Computer Aided Design (ICCAD), 2019.
10. Karim Eldefrawy, Rafail Ostrovsky, Sunoo Park, Moti Yung, "Proactive Secure Computation with a Dishonest Majority," in proceedings of the 11th Conference Security and Cryptography in Networks (SCN), 2018.
11. Ivan De Olivera Nunes, Karim Eldefrawy, Tancrede Lepoint, "Non-interactive User Re-enrollment in Cryptographically Secured Biometrics-based Identification and Authentication Systems," in proceedings of the 2018 International Symposium on Cyber Security Cryptography and Machine Learning (CSCML), 2018.
12. Xavier Carpent, Karim Eldefrawy, Norrathep Rattanavipanon, Ahmad-Reza Sadeghi, Gene Tsudik, "Invited Paper: Reconciling Remote Attestation and Safety-Critical Operation on Simple IoT Devices," in proceedings of the Design Automation Conference (DAC), 2018.
13. Xavier Carpent, Karim Eldefrawy, Norrathep Rattanavipanon, Gene Tsudik, "Temporal Consistency of Integrity-Ensuring Computations and Applications to Embedded Systems Security," in proceedings of ACM Asia Conference on Computer and Communications Security (AsiaCCS), 2018.
14. Gabriela Ciocarlie, Karim Eldefrawy, Tancrede Lepoint, "BlockCIS - A Blockchain-based Cyber Insurance System," 1st IEEE Workshop on Blockchain Applications and Technologies (BAT), 2018.

15. Karim Eldefrawy, Norrathep Rattanavipanon, Gene Tsudik, "Fusing Hybrid Remote Attestation with a Formally Verified Microkernel: Lessons Learned," 47th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2017.
16. Karim Eldefrawy, Norrathep Rattanavipanon, Gene Tsudik, "HYDRA: HYbrid Design for Remote Attestation (Using a Formally Verified Microkernel)," in proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (Wisec), 2017.
17. Shlomi Dolev, Karim Eldefrawy, Juan Garay, Rafail Ostrovsky, Moti Yung, "Brief Announcement: Secure Self-stabilizing Computation," in proceedings of the ACM Symposium on Principles of Distributed Computing (PODC), 2017.
18. Daniel Apon, Chongwon Cho, Karim Eldefrawy, Jonathan Katz, "Efficient, Reusable Fuzzy Extractors from LWE," in proceedings of the 2017 International Symposium on Cyber Security Cryptography and Machine Learning (CSCML), 2017.
19. Karim Eldefrawy, Sky Faber, Tyler Kazcmarek, "Proactively Secure Cloud-enabled Storage," in proceedings of the 37th IEEE International Conference on Distributed Computing Systems (ICDCS), 2017.
20. Xavier Carpent, Karim Eldefrawy, Norrathep Rattanavipanon, Gene Tsudik, "LIghtweight Swarm Attestation: a Tale of Two LISA-s," in proceedings of ACM Asia Conference on Computer and Communications Security (ASIACCS), 2017.
21. Shlomi Dolev, Karim Eldefrawy, Joshua Lampkins, Rafail Ostrovsky, Moti Yung, "Proactive Secret Sharing with a Dishonest Majority," in proceedings of the10th Conference Security and Cryptography in Networks (SCN), 2016.
22. Shlomi Dolev, Karim Eldefrawy, Joshua Lampkins, Rafail Ostrovsky, Moti Yung, "Brief Announcement: Proactive Secret Sharing with a Dishonest Majority," in proceedings of the ACM Symposium on Principles of Distributed Computing (PODC), 2016.
23. Karim Eldefrawy, Tiffany Kim, Pape Sylla, "Automated Identification of Network Service Dependencies via Transfer Entropy," in proceedings of the 40th IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC'16), ADMNET: The 4th IEEE International Workshop on Architecture, Design, Deployment and Management of Networks and Applications, 2016.
24. Karim Eldefrawy, Tyler Kazcmarek, "Byzantine Fault Tolerant Software-Defined Network (SDN) Controllers," in proceedings of the 40th IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC'16), MidCCI: The 2nd IEEE International Workshop on Middleware for Cyber Security, Cloud Computing and Internetworking, 2016.
25. Joshua Baron, Karim Eldefrawy, Joshua Lampkins, Rafail Ostrovsky, "Communication-Optimal Mobile Proactive Secret Sharing" in proceedings of the International Conference on Applied Cryptography and Network Security (ACNS'15), 2015.
26. Karim Eldefrawy, Gavin Holland, Gene Tsudik, "(Extended Abstract) Remote Attestation of Heterogeneous Cyber-Physical Systems: The Automotive Use Case" presented at the Embedded Security in Cars USA (escar USA) Workshop, 2015.
27. Karim Eldefrawy, Joshua Lampkins, "Founding Digital Currency on Secure Computation", in proceedings of the ACM Conference on Computer and Communications Security (CCS), 2014.
28. Joshua Baron, Karim Eldefrawy, Joshua Lampkins, Rafail Ostrovsky, "How to Withstand Mobile Virus Attacks, Revisited", in proceedings of the ACM Symposium on Principles of Distributed Computing (PODC), 2014.
29. Karim Eldefrawy, Joshua Lampkins, "Disincentivizing/Incentivizing Malicious/Honest Behavior on the Internet Via Privacy-preserving AppCoins" in proceedings of the Ninth Workshop on Secure Network Protocols (NPSec), 2014.
30. Joshua Baron, Karim Eldefrawy, Aleksey Nogin, Rafail Ostrovsky, "An Architecture for Resilient Cloud Operations" in proceedings of the IEEE International Conference on Technologies for Homeland Security (HST), 2013.

31. Martin Strohmeier, Ivan Martinovic, Utz Roedig, Karim Eldefrawy, Jens Schmitt "Neighborhood Watch: On Network Coding Throughput and Key Sharing", in proceedings of the IEEE Global Communications Conference (GLOBECOM), 2013.
32. Joshua Baron, Karim Eldefrawy, Kirill Minkovich, Rafail Ostrovsky, Eric Tressler, "5PM: Secure Pattern Matching", in proceedings of the 8th conference on Security and Cryptography for Networks (SCN), 2012.
33. Karim Eldefrawy, Gavin Holland, "Secure and Privcay-preserving Querying of Content in MANETs", in proceedings of the IEEE International Conference on Technologies for Homeland Security (HST), 2012.
34. Karim Eldefrawy, Aurelien Francillon, Daniele Perito, Gene Tsudik, "SMART: Secure and Minimal Architecture for (Establishing Dynamic) Root of Trust", in proceedings of Network & Distributed System Security Symposium (NDSS), 2012.
35. Srdjan Capkun, Karim Eldefrawy, Gene Tsudik, "Group Distance Bounding Protocols", in proceedings of the 4th International Conference on Trust and Trustworthy Computing (TRUST), 2011.
36. Boris Danev, Heinrich Luecken, Srdjan Capkun, Karim Eldefrawy, "Attacks on Physical-layer Identification", in proceedings of the ACM Conference on Wireless Network Security (WiSec), 2010.
37. Claude Catellucia, Karim Eldefrawy, Gene Tsudik, "Link-Layer Encryption Effect on the Capacity of Network Coding in Wireless Networks", in proceedings of IEEE INFOCOM Work in Progress, 2010.
38. Karim Eldefrawy, John Solis, Gene Tsudik, "Leveraging Social Contacts for Message Confidentiality in Delay Tolerant Networks", in proceedings of the IEEE International Computer Software and Applications Conference (COMPSAC), 2009.
39. Karim Eldefrawy, Gene Tsudik, "PRISM: Privacy-friendly Routing In Suspicious MANETs (and VANETs)", in proceedings of the IEEE International Conference of Network Protocols (ICNP), 2008
40. Fabio Soldo, Karim Eldefrawy, Athina Markopoulou, Bala Krishnamurthy, Kobus van der Merwe, "Filtering Sources of Unwanted Traffic Based on Blacklists", in proceedings of the Information Theory and Applications Workshop (ITA), 2008.
41. Karim Eldefrawy, Gene Tsudik, "ALARM: Anonymous Location Aided Routing in Suspicious MANETS", in proceedings of the IEEE International Conference of Network Protocols (ICNP), 2007.
42. Karim Eldefrawy, Athina Markopoulou, Katerina Argyraki, "Optimal Filter Allocation Against Distributed Denial-of-Service Attacks", in proceedings of the Information Theory and Applications Workshop (ITA), 2007.
43. Karim Eldefrawy, Minas Gjoka, Athina Markopoulou, "BotTorrent: Misusing BitTorrent to Launch DDoS Attacks", in proceedings of USENIX Steps Towards Reducing Unwanted Traffic on the Internet (SRUTI), 2007.
44. Karim Eldefrawy, Magda El Zarki, Gene Tsudik, "Incentive-Based Cooperative and Secure Inter-Personal Networking", in proceedings of ACM MobiOpp, 2007.
45. Karim Eldefrawy, Claudio Soriente, "PEUC-WiN: Privacy Enhancement by User Cooperation in Wireless Networks", in proceedings of Second Workshop on Secure Network Protocols (NPSEC), 2006.
46. Karim Eldefrawy, Magda El Zarki , Mohamed Khairy, "Proposal for a cross-layer coordination framework for next generation wireless systems", in proceedings of the International Conference on Communications and Mobile Computing (IWCMC), 2006.
47. Karim Eldefrawy, Mohamed Khairy, Amin Nassar, "Sub-Carrier Allocation using Channel Prediction for OFDMA systems based on IEEE 802.16 Standard", in proceedings International Conference on Computer Engineering and Systems (ICCES), 2006.

Ongoing Work and Preprints

1. Aysajan Abidin, Karim Eldefrawy, Dave Singlee, "Entanglement-based (Mutual) Quantum Distance Bounding", under review at CANS 2020.

2. Karim Eldefrawy, Julian Loss, Ben Terner, "Byzantine Agreement for Hybrid Network Settings with Optimal Tolerance to Byzantine and Crash Faults", in preparation.

PATENTS

Granted Patents

1. "STAGS: secure, tunable, and accountable generic search in databases" United States Patent Number US Patent 10691754
2. "Generic pattern matching system" United States Patent Number US Patent 10621364
3. "System and method to integrate secure and privacy-preserving biometrics with identification, authentication, and online credential systems" United States Patent Number US10523654
4. "One-time obfuscation for polynomial-size ordered binary decision diagrams (POBDDs)" United States Patent Number US10509918.
5. "System and method for operating a proactive digital currency ledger" United States Patent Number US10423961.
6. "System and method for cloud control operations plane based on proactive security algorithms" United States Patent Number US9846596.
7. "Information secure protocol for mobile proactive secret sharing with near-optimal resilience" United States Patent Number US9787472.
8. "System and method for cloud control operations plane based on proactive security algorithms" United States Patent Number US9846596.
9. "Secure Multi-dimensional Pattern Matching for Secure Search and Recognition" United States Patent Number US9613292.
10. "Cryptographically-secure Packed Proactive Secret Sharing Protocol" United States Patent Number US9614676.
11. "Information Theoretically Secure Protocol for Mobile Proactive Secret Sharing with Near-optimal Resilience " United States Patent Number US9558359.
12. "Secure Mobile Proactive Multi-party Computation Protocol" United States Patent Number US9536114.
13. "Method for Secure and Resilient Distributed Generation of Elliptic Curve Digital Signature Algorithm (ECDSA) Based Digital Signatures with Proactive Security" United States Patent Number US9489522.
14. "Generic Proactively Secure Secret Sharing Protocol from any Suitable Honest-Majority Secret Sharing Protocol" United States Patent Number US9467451.
15. "General Protocol for Proactively Secure Computation" United States Patent Number US9449177.
16. "System and Method for Mobile Proactive Secret Sharing" United States Patent Number US9443089.
17. "System and Method for Deep Packet Inspection and Intrusion Detection" United States Patent Number US9336239.
18. "Wireless Network Security" United States Patent Number US9119077.
19. "Secure Pattern Matching" United States Patent Number US9009089.
20. "Ensuring Promises are Kept in an Anonymous System" United States Patent Number US9026786.
21. "Wireless Network Security" United States Patent Number US8612743.
22. "Filtering Unwanted Data Traffic via a Per-Customer Blacklist" United States Patent Number US8161155.
23. "System and Method for Filtering Unwanted Internet Protocol Traffic based on Blacklists" United States Patent Number US8539576.

15+ Applications Pending.

SELECTED INVITED COLLOQIA AND TALKS

Invited Talks

- October 2019: "Longitudinal Study of Misuse of Cryptocurrencies," invited talk at the National University of Colombia, Bogota.
- August 2019: "A High-Assurance Evaluator for Machine-Checked Secure Multi-Party Computation," invited talk at the 2019 CRYPTO associated workshop on "Standardization of Advanced Cryptography."
- April 2019: "Recent Development in Secure Remote Attestation of Embedded and Internet-of-Things Devices," at the Open Graduate Seminar at the Texas A&M University. Hosted by Prof. Juan Garay.
- April 2019: "Secure and Privacy-preserving Computation," a short tutorial at the DevPulseCon development conference by the CodeChix organization which aims to retain women engineers and technologists in industry and academia.
- February 2019: "Surfacing Hidden-centralities in Overlay Consensus-powered Systems (SHOCS)," at the DARPA workshop on Applications and Barriers to Consensus (ABC).
- August 2018: "Secure and Privacy-preserving Computation: Recent Progress and Applications," at the Harvard Project for Asian and International Relations (HPAIR), Kuala Lampur, Malaysia.
- July 2017: "Recent Progress in Secure Remote Attestation," at the Institute for Information Infrastructure Protection (I3P) monthly webinar series at George Washington University (GWU).
- June 2017: "Composing Secure Computation" at the IARPA workshop on Homomorphic Encryption Computing Techniques with Overhead Reduction (HECTOR).
- July 2016: "Proactively Secure Cryptography: High Resilience and Long-Term Confidentiality," at SRI International's Computer Science Laboratory Seminar (CSL), California, USA. Hosted by Patrick Lincoln, CSL Director.
- February 2016: "Proactive Secret Sharing and Multi-party Computation," at "Computation Algebra" (CS290T) Class at the University of California Santa Barbara (UCSB), California, USA. Hosted by Prof. Cetin Kaya Koc.
- January 2016: "Proactively Secure Cryptographic Protocols: High Resilience and Long-Term Confidentiality for Distributed Computation and Storage," at the Colloquium of the Department of Computer Science and Engineering, University of California, Riverside (UCR), California, USA. Hosted by Prof. Jiasi Chen.
- May 2015: "Proactive Secret Sharing and Secure Multi-party Computation: Long-Term Confidentiality and Increased Resilience," at Stanford Research Institute (SRI International) Computer Science Laboratory Seminar (CSL), California, USA. Hosted by Patrick Lincoln, CSL Director.
- April 2013: "Secure Pattern Matching," at the "Introduction to Cryptography" (CS178) Class at the University of California Santa Barbara (UCSB), California, USA. Hosted by Prof. Cetin Kaya Koc.
- September 2012: "Secure Remote Attestation in Embedded Systems," Indian Institute of Technology (IIT), Mumbai, India. Hosted by Prof. Magda ElZarki.
- July 2009: "Privacy and Security in Location Centric Communication," at Telefonica Research, Barcelona, Spain. Hosted by Prof. Michael Sirivianos.
- June 2009: "Privacy and Security in Location Centric Communication," at the Laboratory for Communications and Applications (LCA) Seminar at EPFL, Lausanne, Switzerland. Hosted by Prof. Jean-Pierre Hubaux.
- June 2009: "Security and Privacy in Location-based Mobile Ad-Hoc Networks," at Eurocom Institute, Sophia Antipoliss, France. Hosted by Prof. Refik Molva.
- May 2009: "Security and Privacy in Location-based Mobile Ad-Hoc Networks," at INRIA Research, Grenoble, France. Hosted by Prof. Claude Castelluccia.
- June 2009: "Security and Privacy in Location-based Mobile Ad-Hoc Networks," at the Systems Security Group Seminar at ETH Zurich, Zurich, Switzerland. Hosted by Prof. Srdjan Capkun.

- July 2008: "Denial-of-Service Attacks Using BitTorrent," at the American University in Cairo (AUC), Cairo, Egypt. Hosted by Prof. Sherif Elkassas.

Invited Colloquia and Workshops

- June 2017: "Composing Secure Computation" at the IARPA workshop on Homomorphic Encryption Computing Techniques with Overhead Reduction (HECTOR).
- *October 2015:* "Government Vehicle Cybersecurity Steering Group Kickoff" organized by SRI International and sponsored by U.S. Department of Homeland Security (DHS).
- May 2014: "Workshop on Security and Privacy Assurance Research - Multi-party Computation (SPAR-MPC)" organized by MIT Lincoln Laboratory and sponsored by IARPA.
- November 2011: "DARPA Colloquium on Future Directions in Cyber Security" sponsored by the DARPA Information Innovation Office (I2O).

SELECTED PROFESSIONAL ACTIVITIES

- (2011-2015) Information Director of ACM Transactions on Information and System Security (TISSEC).
- Program Committees: ACM CCS'20, ACM WiSec'20, ACM WiSec'19, CSCML'19, Inscrypt'18, ESCAR'18, ACM WiSec'18, BAT'18, IEEE CNS'18, CSCML'18, CCNC'18, IEEE CNS'17, Inscrypt'17, ESCAR'17, CSCML'17, Inscrypt'16, CCNC'17, SCN'16, ESCAR'16, CRYPTO'15, CCNC'15, ACM WISEC'12, ACM WISEC'11, ACNS'11.
- Journal Reviews: ACM Transactions on Privacy and Security (TOPS) (formerly known as TISSEC), Elsevier Theoretical Computer Science (TCS), IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transactions of Mobile Computing (TMC), IEEE Transactions on Information Forensics and Security (TIFS), IEEE Journal of Selected Areas of Communication (JSAC), IEEE Transactions on Wireless Communications (TWC), IEEE Transactions on Networking (ToN), IEEE Pervasive Computing, Elsevier Comcom.
- Conference Reviews: Usenix Security'19, ACM CCS'19, Eurocrypt'17, ACM AsiaCCS'17.