Attila Altay Yavuz, Ph.D.

CONTACT INFORMATION

4202 E Fowler Ave, ENG 117,
Tampa, FL 33620, USA

Voice: +1-813-974-0419
E-mail: attilaayavuz@usf.edu
URL: `https://cse.usf.edu/~attilaayavuz/`

EDUCATION

North Carolina State University (NCSU), Raleigh, North Carolina, USA
Ph.D., Computer Science, (01/01/2007 - 08/01/2011)
Thesis: Compromise Resilient and Compact Cryptographic Constructions for Digital Forensics
Advisor: Prof. Dr. Peng Ning

Bogazici University, Istanbul, Turkey
M.S., Computer Science, (09/01/2004 - 06/01/2006)

Yildiz Technical University, Istanbul, Turkey
B.S., Computer Science and Engineering, (09/01/1999 - 06/01/2004)

PROFESSIONAL EXPERIENCES

- **Associate Professor**, Bellini College of AI, Cybersecurity and Computing, University of South Florida (06/09/2021 - present)
- **Assistant Professor**, The Department of Computer Science and Engineering, University of South Florida (08/31/2018 - 06/08/2021)
- **Assistant Professor**, School of Electrical Engineering and Computer Science, Oregon State University (09/01/2014 - 08/30/2018)
- **Research Scientist**, Bosch Research and Technology Center (09/01/2011 - 08/31/2014)
- **Research/Teaching Assistant**, Department of Computer Science, NC State University, Cyber Defense Laboratory (01/01/2007- 08/31/2011)
- **Research Engineer**, Satellite Networks Research Laboratory, Bogazici University (2004 - 2006)
- **Intern**, Department of Computer Science, NC State University, (06/01/2003 - 08/31/2003)

EXPERTISE

- Cybersecurity; Applied cryptography; Network security

SELECTED AWARDS

- NSF CAREER Award
- Cisco Research Awards (2025, 2022, 2020, and 2019)
- Human-Machine Intelligence for Security Analytics (IEEE S&P 25 Workshop, Best Paper Award)
- USF Excellence in Innovation Award (2022)
- National Academy of Inventors (Member)
- USF Faculty Outstanding Research Achievement Award (2020)
- USF College of Engineering's Outstanding Research Achievement Award (2020)
- Distinguished Research Award, Silicon Valley Cybersecurity Institute (2020).
- USF Nomination for the Excellence in Innovation Award (2020)
- IEEE CNS Best Paper Runner-Up (2020)
- DBSec Best Paper Award (2018)

Funded Research

I have secured $5,868,836 in total with $2,562,555 on my share.

• **Quantum-Resistant Networks and Systems: Primitives, Protocols, and Best Practices**
Cisco Research Award (USF PI)
07/2025 - 07/2026, Total: $50,000

• **NSF-SNSF: A Resilient and Efficient Cyber-security Fabric and Evaluation Framework for Future Integrated Satellite-Terrestrial Networks (SATUQ)**
Attila A. Yavuz (NSF PI), National Science Foundation Award No. ECCS - 2444615
01/2025 - 12/2027, Total: $850,000, my share: $365,000

• **Collaborative Research: SaTC: CORE: Medium: Distributed Computing in Effect: Towards Trustworthy, Resilient and Secure NextG Mobile Networks**
Attila A. Yavuz (PI), National Science Foundation Award No. CNS – 2350213
07/2024 - 07/2028, Total: $1,200,000, my share: $525,000

• **Perceptive and Reactive Autonomous Navigation in Challenging Environments (PRANCE): Additively Manufactured Multidimensional Cryptographic Physically Unclonable Functions for Wireless System Security**
Attila A. Yavuz (Co-PI), Led by Gokhan Mumcu (PI), Army Research Laboratory (ARL)
05/2024 - 05/2027, Total: $917,625, my share: $248,000

• **NSF CAREER: Lightweight and Fast Authentication for Internet of Things**
Attila A. Yavuz (Sole-PI), National Science Foundation Award No. CNS – 1917627
03/2017 - 01/2024, Total: $500,000

• **Trustworthy Digital Forensics for Heterogeneous Internet of Things**
Cisco Research Award (Sole-PI)
01/2022 - present, Total: $98,985.00

• **Trustworthy and Privacy-Preserving Machine Learning Platforms**
Cisco Research Award (Sole-PI)
09/2020 - 01/2025, Total: $99,980

• **Distributed Oblivious Random Access Machine**
Attila A. Yavuz (Sole-PI), Unrestricted Gift, Robert Bosch
12/2019 - present, Total: $50,000

• **Lightweight and Quantum-Safe Authentication for Internet of Things**
Cisco Research Award (Sole-PI)
06/2019 - present, Total: $60,306

• **Low-cost, Scalable and Practical Post-Quantum Key Distribution**
Sole-PI, Department of Energy, Cyber Resilient Energy Delivery Consortium
06/2020 - 05/2022, Total: $100,000

• **The Center for Cryptographic Research (Internal Grant)**

Attila A. Yavuz (Co-PI)

01/2020 - present, Total: $100,000, my share: $25,000

- **Secure Mobile Contact Tracing App - (COVID 19 Response) (Internal Grant)**

  Attila A. Yavuz (Co-PI)

  04/2020 - 09/2020, Total: $25,000, my share: $7,826

- **A Decentralized Digital ID for Pandemics - (COVID 19 Response) (Internal Grant)**

  Attila A. Yavuz (Co-PI)

  08/2020 - 08/2021, Total: $25,000, my share: $3,000

- **Cloud Security Technologies and Oblivious Random Access Machine**

  Attila A. Yavuz (Sole-PI), Unrestricted Gift, Robert Bosch

  12/2018 - present, Total: $50,000

- **Lightweight, Delay-Aware and Scalable Cryptographic Services for Smart-Grids**

  Co-PI, Department of Energy, Cyber Resilient Energy Delivery Consortium

  09/2015 - 07/2018, Total: $1,530,040, my share: $167,558

- **Towards Practical Privacy Enhancing Technologies**

  Attila A. Yavuz (Sole-PI), Unrestricted Gift, Robert Bosch

  09/2014 - 09/2018, Total: $175,000

- **NSF Travel Grant**

  Attila A. Yavuz (Sole-PI), National Science Foundation Award No. CNS - 1821203

  01/11/2018, Total: $18,000

- **NVIDIA Equipment Grant**

  Attila A. Yavuz (Sole-PI), Total: $4,500

- **OSU EECS RIU Initative (Internal Grant)**

  Attila A. Yavuz (PI), 04/2017 - 12/2017, Total: $14,400

Publications

Underlined authors are my current/former advisees (Ph.D./MS) at the time of initial submission/completion of the work. In my field, it is typical for faculty members to appear after their advisees in authorship lists.

Journal Papers [J]

31. Saif E. Nouma and **Attila A. Yavuz**, "Lightweight and High-Throughput Secure Logging for Internet of Things and Cold Cloud Continuum", in *ACM Transactions on Internet of Things (ACM TIoT)*, January 2026.
30. Kiarash Sedghighadikolaei and **Attila A. Yavuz** ,"A Survey of Threshold Signatures: NIST Standards, Post-Quantum Cryptography, Exotic Techniques, and Real-World Applications", in *ACM Computing Surveys*, Volume 58, Issue 6, Article No.: 143, Pages 1 - 39, 9 December 2025.

29. Gurkan Gur and **Attila A. Yavuz**, "Post-Quantum Cryptography for Integrated Space-Aerial-Terrestrial Networks: Current State, Challenges and Trends", *Book Chapter in Cybersecurity in Space: Technologies, Threats, and Solutions by Armasuisse Science and Technology, Federal Administration, Department of Defense of Swiss Confederation.* Springer Cham, to be appear, June 2026.

28. Saif E. Nouma and **Attila A. Yavuz**, "Lightweight and Resilient Signatures for Cloud-Assisted Embedded IoT Systems", in *Security and Privacy, Wiley*, December 2025, DOI: 10.1002/spy2.70173.

27. S. Aghapour, K. Sedghighadikolaei, **Attila A. Yavuz**, B. Hamdaoui and M. Mozaffari-Kermani, "Efficient Fault-Detection Architectures for Barrett Reduction and Multiplication in Classical and Post-Quantum Cryptographic Systems," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 33, no. 12, pp. 3465-3477, Dec. 2025.

26. **Attila A. Yavuz**, Saleh Darzi and Saif E. Nouma, "LiteQSign: Lightweight and Quantum-Safe Signatures for Heterogeneous IoT Applications", in *IEEE Access*, vol. 13, pp. 171442-171456, 7 October, 2025.

25. A. Pendino, Nghia Nguyen, Saif E. Nouma, Jing Wang, **Attila A. Yavuz**, Yasin Yilmaz and Gokhan Mumcu, "Additively Manufactured RF Electronics With Structurally Integrated Physically Unclonable Functions for Wireless System Security", in *IEEE Access*, vol. 13, pp. 145042-145059, August 2025.

24. Kiarash Sedghighadikolaei, **Attila A. Yavuz**, and Saif E. Nouma, "Signer-optimal multiple-time post-quantum hash-based signature for heterogeneous IoT Systems", *Internet of Things*, Volume 33, July 2025, 101694, ISSN 2542-6605.

23. Yiwei Zhang, Rouzbeh Behnia, **Attila A. Yavuz**, Reza Ibrahimi, and Elisa Bertino, "Efficient Full-Stack Private Federated Deep Learning with Post-Quantum Security", *IEEE Transactions on Dependable and Secure Computing (IEEE TDSC)*, pages 1-19, May 2025.

22. Saif E Nouma and **Attila A. Yavuz**, "Trustworthy and efficient digital twins in post-quantum era with hybrid hardware-assisted signatures", *ACM Transactions on Multimedia Computing, Communications and Applications*, Vol. 20, Issue 6, No: 156, Pages 1-30, March 2024.

21. Mohamed Grissa, **Attila A. Yavuz** , Bechir Hamdaoui and Chittibabu Tirupathi, "Anonymous Dynamic Spectrum Access and Sharing Mechanisms for the CBRS Band", *IEEE Access*, February 2021.

20. Thang Hoang, **Attila A. Yavuz** and Jorge Guajardo, "A Multi-server ORAM Framework with Constant Client Bandwidth Blowup", *ACM Transactions on Privacy and Security (TOPS)*, Vol. 23, Issue 1, pp. 1-35, February 2020.

19. **Attila A. Yavuz** and Muslum O. Ozmen, "Ultra Lightweight Multiple-time Digital Signature for the Internet of Things Devices", *IEEE Transactions on Services Computing*, July 2019.

18. Thang Hoang, **Attila A. Yavuz**, Fatma B. Durak, and Jorge Guajardo, "A Multi-server Oblivious Dynamic Searchable Encryption Framework", *Journal of Computer Security*, Vol 27, Issue 6, pp. 649-676, May 2019.

17. Mohamed Grissa, **Attila A. Yavuz** and Bechir Hamdaoui, "Location Privacy in Cognitive Radios with Multi-Server Private Information Retrieval", *IEEE Transactions on Cognitive Communications and Networking*, June 2019.

16. Thang Hoang, **Attila A. Yavuz**, and Jorge Guajardo, "A Secure Searchable Encryption Framework for Privacy-Critical Cloud Storage Services", *IEEE Transactions on Services Computing*, February 2019.

15. Mohamed Grissa, Bechir Hamdaoui and **Attila A. Yavuz**, "Unleashing the Power of Multi-Server PIR for Enabling Private Access to Spectrum Databases", *IEEE Communications Mag-*

azine, vol. 56, no. 12, pp. 171-177, December 2018.

14. Thang Hoang, Ceyhun D. Ozkaptan, Gabriel Hackebeil, and **Attila A. Yavuz**, "Efficient Oblivious Data Structures for Database Services on the Cloud", *IEEE Transactions on Cloud Computing*, November 2018.

13. Rouzbeh Behnia, Muslum O. Ozmen, and **Attila A. Yavuz**, "Lattice-Based Public Key Searchable Encryption from Experimental Perspectives", *IEEE Transactions on Dependable and Secure Computing (TDSC)*, August 2018.

12. **Attila A. Yavuz**, "Immutable Authentication and Integrity Schemes for Outsourced Databases" *IEEE Transactions on Dependable and Secure Computing (TDSC)*, vol. 15, no.1, pp.69-82, February 2018.

11. **Attila A. Yavuz**, Anand Mudgerikar, Ankush Singla, Ioannis Papapanagiotou and Elisa Bertino, "Real-Time Digital Signatures for Time-Critical Networks", in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 11, pp. 2627-2639, July 2017.

10. Mohamed Grissa, **Attila A. Yavuz** and Bechir Hamdaoui, "Location Privacy Preservation in Database-Driven Wireless Cognitive Networks Through Encrypted Probabilistic Data Structures", in *IEEE Transactions on Cognitive Communications and Networking*, vol. 3, no. 2, pp. 255-266, June 2017.

9. Mohamed Grissa, Bechir Hamdaoui and **Attila A. Yavuz**, "Location privacy in cognitive radio networks: a survey", in *IEEE Communications Surveys and Tutorials*, vol. 19, no. 3, pp. 1726-1760, thirdquarter 2017.

8. Mohamed Grissa, **Attila A. Yavuz** and Bechir Hamdaoui, "Preserving the Location Privacy of Secondary Users in Cooperative Spectrum Sensing", in *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 2, pp. 418-431, February 2017.

7. Nadia Adem, Bechir Hamdaoui and **Attila A. Yavuz**, "Mitigating Jamming Attacks in Mobile Cognitive Networks Through Time Hopping", *Wireless Communications and Mobile Computing*, Wiley, vol. 16, issue 17, Pages 3004-3014, December 2016.

6. Velin Kounev, David Tipper, **Attila A. Yavuz**, Brandon M. Grainger and Gregory F. Reed, "A Secure Communication Architecture for Distributed Microgrid Control", in *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2484-2492, Sept. 2015.

5. Panos Kampanakis, **Attila A. Yavuz**, "BAFi: A Practical Cryptographic Secure Audit Logging Scheme for Digital Forensics", in *Wiley Security and Communication Networks*, vol. 8, no. 17, pp. 3180-3190, November 2015.

4. **Attila A. Yavuz**, "An Efficient Real-Time Broadcast Authentication Scheme for Command and Control Messages", *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1733-1742, October 2014.

3. **Attila A. Yavuz**, Peng Ning and Michael K. Reiter, "BAF and FI-BAF: Efficient and Publicly Verifiable Cryptographic Schemes for Secure Logging in Resource-Constrained Systems", *ACM Transaction of Information Systems Security*, vol. 15, issue 2, Article 9, 28 pages, July 2012.

2. **Attila A. Yavuz** and Peng Ning, "Self-sustaining, efficient and forward-secure cryptographic constructions for Unattended Wireless Sensor Networks", *Journal of Ad Hoc Networks*, vol. 10, issue 7, pp. 1204-1220, September 2012.

1. **Attila A. Yavuz**, Fatih Alagoz, and Emin Anarim,"A new multi-tier adaptive military MANET security protocol using hybrid cryptography and signcryption", *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 18, issue 1, January 2010.

International Conference Papers [C]

62. Saif E. Nouma and **Attila A. Yavuz**, "Lightweight and Breach-Resilient Authenticated Encryption Framework for Internet of Things", in *43rd IEEE Military Communications Conference 2025*, 6–10 October 2025 , Los Angeles, CA, USA.

61. Nora Basha, Bechir Hamdaoui, **Attila A. Yavuz**, Thang Hoang, and Mehran M. Kermani, "Secret-Key Agreement Through Hidden Markov Modeling of Wavelet Scattering Embeddings", *13th IEEE Conference on Communications and Network Security (CNS)*, Avignon, France, September 2025.

60. Yiwei Zhang, Rouzbeh Behnia, Imtiaz Karim, **Attila A. Yavuz**, and Elisa Bertino,"Standing Firm in 5G: A Single-Round, Dropout-Resilient Secure Aggregation for Federated Learning", The 18th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2025), July 2025, Arlington, Virginia, USA.

59. Saleh Darzi and **Attila A. Yavuz**, "SLAP: Secure Location-proof and Anonymous Privacy-preserving Spectrum Access", The IEEE Silicon Valley Cybersecurity Conference (SVCC), June 2025, San Francisco, CA, USA.

58. Gurkan Gur and **Attila A. Yavuz**, "Getting Ready for the Future (or Now): Towards a Cybersecurity Fabric for Future Integrated Satellite-Terrestrial Networks", IEEE 101st Vehicular Technology Conference: VTC2025-Spring, 17 - 20 June 2025, Oslo, Norway.

57. Kasra Ahmadi, Rouzbeh Behnia, Reza Ebrahimi, Mehran Mozaffari Kermani, Jeremiah Birrell, Jason Pacheco, **Attila A. Yavuz**, "An Interactive Framework for Implementing Privacy-Preserving Federated Learning: Experiments on Large Language Models", IEEE S&P 25 Workshops, the 1st Human-Machine Intelligence for Security Analytics (HMI-SA), (Co-located with IEEE S&P 2025), May 2025, San Francisco, USA **(Best Paper Award!)**.

56. Yiwei Zhang, Rouzbeh Behnia, **Attila A. Yavuz**, Reza Ebrahimi and Elisa Bertino, " Uncovering Attacks and Defenses in Secure Aggregation for Federated Deep Learning", *IEEE International Conference on Data Mining (IEEE ICDM)*, December 2024, Abu Dhabi, UAE.

55. Saleh Darzi and **Attila A. Yavuz**, "Privacy-Preserving and Post-Quantum Counter Denial of Service Framework for Wireless Networks", *IEEE Military Communications Conference (IEEE Milcom)*, October 2024, Washington, DC.

54. Saleh Darzi and **Attila A. Yavuz**, "Counter Denial of Service for Next-Generation Networks within the Artificial Intelligence and Post-Quantum Era", *The Sixth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS)*, October 2024, Washington, DC.

53. Kiarash Sedghighadikolaei and **Attila A. Yavuz**, "Fast and Post-Quantum Authentication for Real-time Next Generation Networks with Bloom Filter", *The Sixth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS)*, October 2024, Washington, DC.

52. Gurkan Gur, Pawani Porambage, Diana Moya Osorio, **Attila A. Yavuz**, and Madhusanka Liyanage, "6G Security Vision - A Concise Update", *IEEE Future Networks World Forum (FNWF)*, November 2023, Baltimore, MD.

51. **Attila A. Yavuz**, Kiarash Sedghighadikolaei, Saleh Darzi and Saif E. Nouma, "Beyond Basic Trust: Envisioning the Future of NextGen Networked Systems and Digital Signatures", *The Fifth IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS)*, November 1-3, 2023. Atlanta, GA.

50. Saif E. Nouma and **Attila A. Yavuz**, "Lightweight Digital Signatures for Internet of Things: Current and Post-Quantum Trends and Visions", *The 6th IEEE Conference on Dependable and Secure Computing (IEEE DSC)*, October 2023, Tampa, FL.

49. Saif E. Nouma and **Attila A. Yavuz**, "Practical Cryptographic Audit Tools for Lightweight

Internet of Things and Cold Storage Systems", *8th ACM/IEEE Conference on Internet of Things Design and Implementation*, May 9-12, 2023, San Antonio, Texas.

48. Saif E. Nouma and **Attila A. Yavuz**, "Post-Quantum Forward-Secure Signatures with Hardware-Support for Internet of Things", *IEEE International Conference on Communications (ICC)*, May 28 - June 1, 2023, Rome, Italy.

47. Tung Le, Pengzhi Huang, **Attila A. Yavuz**, Elaine Shi, and Thang Hoang, "Efficient Dynamic Proof of Retrievability for Cold Storage", in *the Annual Network and Distributed System Security Symposium (NDSS)*, February 2023, San Diego, CA, USA.

46. **Attila A. Yavuz**, Saif E. Nouma , Thang Hoang, Duncan Earl, and Scott Packard, "Distributed Cyber-infrastructures and Artificial Intelligence in Hybrid Post-Quantum Era", *4th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (IEEE TPS)*, December 2022.

45. **Attila A. Yavuz**, Duncan Earl, Scott Packard and Saif E. Nouma, "Hybrid Low-Cost Quantum-Safe Key Distribution", Quantum 2.0, Boston, MA, June 2022.

44. Weikeng Chen, Thang Hoang, Jorge Guajardo and **Attila A. Yavuz**, "Titanium: A Metadata-Hiding File-Sharing System with Malicious Security", in *The Network and Distributed System Security Symposium – (NDSS)*, The Internet Society, February 2022, San Diego, CA, USA.

43. Rouzbeh Behnia and **Attila A. Yavuz**, "Towards Practical Post-quantum Signatures for Resource-Limited Internet of Things", *37th Annual Computer Security Applications Conference (ACSAC 2021)*, December 2021.

42. Rouzbeh Behnia, Eamonn W. Postlethwaite, Muslum Ozgur Ozmen and **Attila A. Yavuz**, "Lattice-Based Proof-of-Work for Post-Quantum Blockchains", *5th International Workshop on Cryptocurrencies and Blockchain Technology - CBT 2021 (with ESORICS 2021)*, October 2021.

41. Efe Seyitoglu, **Attila A. Yavuz** and Thang Hoang, "Proof-of-Useful-Randomness: Mitigating the Energy Waste in Blockchain Proof-of-Work", *The 18th International Conference on Security and Cryptography (SECRYPT 2021)*, July 2021.

40. Ankush Singla, Rouzbeh Behnia, Syed Rafiul Hussain, **Attila A. Yavuz** and Elisa Bertino, "Look Before You Leap: Secure Connection Bootstrapping for 5G Networks to Defend Against Fake Base-Stations", *16th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2021)*, June 2021.

39. Rouzbeh Behnia, **Attila A. Yavuz**, Ozgur O. Ozmen and Tsz Hon Yuen, "Compatible Certificateless and Identity-Based Cryptosystems for Heterogeneous IoT", *the 23rd Information Security Conference (ISC) 2020*, December 2020.

38. Efe Seyitoglu, **Attila A. Yavuz** and Ozgur O. Ozmen, "Compact and Resilient Cryptographic Tools for Digital Forensics", *8th IEEE Conference on Communications and Network Security (CNS 2020)*, June 2020 (listed among the best paper award candidates).

37. Thang Hoang, Rouzbeh Behnia, Yeongjin Jang, and **Attila A. Yavuz**, "MOSE: Practical Multi-User Oblivious Storage via Secure Enclaves", *10th ACM Conference on Data and Application Security and Privacy (CODASPY)*, April 2020.

36. Thang Hoang, Jorge Guajardo and **Attila A. Yavuz**, "MACAO: A Maliciously-Secure and Client-Efficient Active ORAM Framework", in *The Network and Distributed System Security Symposium – (NDSS) 2020*, The Internet Society, February 2020, San Diego, CA, USA.

35. Muslum O. Ozmen, Rouzbeh Behnia, and **Attila A. Yavuz**, "Energy-Aware Digital Signatures for Embedded Medical Devices", *7th IEEE Conference on Communications and Network Security (CNS)*, Washington, D.C., USA, June 2019.

34. Rouzbeh Behnia, Muslum O. Ozmen, and **Attila A. Yavuz**, "ARIS: Authentication for Real-Time IoT Systems", *IEEE International Conference on Communications (ICC 2019)*, Shanghai, China, May 2019.

33. Thang Hoang, Muslum O. Ozmen, Yeongjin Jang and **Attila A. Yavuz**, "Hardware-Supported ORAM in Effect: Practical Oblivious Search and Update on Very Large Dataset", *19th Privacy Enhancing Technologies Symposium (PETS 2019)*, July 2019, Stockholm, Sweden.

32. Mohamed Grissa, **Attila A. Yavuz**, and Bechir Hamdaoui, "TrustSAS: A Trustworthy Spectrum Access System for the 3.5 GHz CBRS Band", *IEEE International Conference on Computer Communications (IEEE INFOCOM 2019)*, April 2019, Paris, France.

31. Muslum O. Ozmen, Rouzbeh Behnia, and **Attila A. Yavuz**, "Fast Authentication from Aggregate Signatures with Improved Security". *International Conference on Financial Cryptography and Data Security (FC 2019)*, St. Kitts, February 2019.

30. Rouzbeh Behnia, Muslum O. Ozmen, **Attila A. Yavuz**, and Mike Rosulek, "TACHYON: Fast Signatures from Compact Knapsack", *The 25th ACM Conference on Computer and Communications Security (CCS)*, Toronto, Canada, October 2018.

29. Muslum O. Ozmen and **Attila A. Yavuz**, "Dronecrypt - An Ultra-Low Energy Cryptographic Framework for Small Aerial Drones", *The 37th IEEE International Conference for Military Communications (MILCOM)*, Los Angeles, CA, USA, October 2018.

28. Thang Hoang, **Attila A. Yavuz**, F. Betul Durak, and Jorge Guajardo, "Oblivious Dynamic Searchable Encryption on Distributed Cloud Systems", *The 32nd International conference on Data and Applications Security and Privacy (DBSec 2018)*, Bergamo, Italy, July 16-18, 2018. **(Best Paper Award)**

27. Muslum O. Ozmen, Rouzbeh Behnia and **Attila A. Yavuz**, "Compact Energy and Delay-aware Authentication", *6th IEEE Conference on Communications and Network Security (CNS)*, Beijing, China, May 30 June 1, 2018.

26. Muslum O. Ozmen, Thang Hoang and **Attila A. Yavuz**, "Forward-private Dynamic Searchable Symmetric Encryption with Efficient Search", *IEEE International Conference on Communications (ICC)*, Kansas City, MO, May 2018.

25. Thang Hoang, Ceyhun D. Ozkaptan, **Attila A. Yavuz**, Jorge Guajardo and Tam Nguyen, "S3ORAM: A Computation-Efficient and Constant Client Bandwidth Blowup ORAM with Shamir Secret Sharing", in *Proceedings of* ACM SIGSAC Conference on Computer and Communications Security (CCS), pp. 491-505, Dallas, TX, USA, October 30-November 03, 2017.

24. Muslum O. Ozmen and **Attila A. Yavuz**, "Low Cost Standard Public Key Cryptography Services for Wireless IoT Systems", *The first ACM CCS Workshop on Internet of Things Security and Privacy (IoT S&P)*, Dallas, TX, USA, November 2017.

23. Mohamed Grissa, **Attila A. Yavuz** and Bechir Hamdaoui, "When the Hammer Meets the Nail: Multi-Server PIR for Database-Driven CRN with Location Privacy Assurance", *5th IEEE Conference on Communications and Network Security (CNS)*, Las Vegas, USA, October, 2017.

22. Rouzbeh Behnia, **Attila A. Yavuz** and Muslum O. Ozmen, "High-Speed High-Security Public Key Encryption with Keyword Search", *31th International conference on Data and Applications Security and Privacy (DBSec'17)*, pp. 365-385, Philadelphia, USA, July 2017.

21. Yousef Qassim, Mario E. Magana, and **Attila A. Yavuz**, "Post-Quantum Hybrid Security Mechanism for MIMO Systems", *International Workshop on Computing, Networking and Communications (CNC) - with International Conference on Computing, Networking and Communication (ICNC)*, Silicon Valley, California, USA, January 2017.

20. Thang Hoang, **Attila A. Yavuz** and Jorge Guajardo,"Practical and Secure Dynamic Searchable Encryption via Oblivious Access on Distributed Data Structure", in Proceedings of the

32nd Annual Computer Security Applications Conference (ACSAC 16), pp. 302-313, Los Angeles, California, USA, December 5-9, 2016.

19. Mohamed Grissa, **Attila A. Yavuz** and Bechir Hamdaoui, "An Efficient Technique for Protecting Location Privacy of Cooperative Spectrum Sensing Users", *IEEE Infocom Green and Sustainable Networking and Computing (GSNC 2016) Workshop*, pp. 915-920, San Francisco, April 2016.

18. Nadia Adem, Bechir Hamdaoui and **Attila A. Yavuz**, "Pseudorandom Time-Hopping Anti-Jamming Technique for Mobile Cognitive Users", *IEEE International Workshop on Advances in Software Defined Radio Access Networks and Context-aware Cognitive Networks (SDRAN-CAN 2015)*, San Diego, CA, USA, December 2015.

17. Mohamed Grissa, **Attila A. Yavuz** and Bechir Hamdaoui, "Cuckoo Filter-Based Location-Privacy Preservation in Database-Driven Cognitive Radio Networks", *IEEE 2nd World Symposium on Computer Networks and Information Security*, Tunusia, September 2015.

16. Ankush Singla, Anand A. Mudgerikar, Ioannis Papapanagiotou and **Attila A. Yavuz**, "HAA: Hardware-Accelerated Authentication for Internet of Things in Mission Critical Vehicular Networks", *International Conference for Military Communications (MILCOM)*, pp. 1298–1304, Tampa, FL, USA, October 2015.

15. Mohamed Grissa, **Attila A. Yavuz** and Bechir Hamdaoui, "LPOS: Location Privacy for Optimal Sensing in Cognitive Radio Networks", *IEEE Global Communications Conference (IEEE Globecom 2015)*, pp. 1-6, San Diego, USA, December 2015.

14. **Attila A. Yavuz** and Jorge Guajardo, "Dynamic Searchable Symmetric Encryption with Minimal Leakage and Efficient Updates on Commodity Hardware", *Selected Areas in Cryptography (SAC) 2015*, pp. 241-259, Sackville, New Brunswick, Canada, August 2015.

13. **Attila A. Yavuz**, "Practical immutable signature bouquets (PISB) for authentication and integrity in outsourced databases", In Proceedings of the *27th international conference on Data and Applications Security and Privacy XXVII (DBSec'13)*, Springer-Verlag, Berlin, Heidelberg, pp. 179-194, Newark, USA, July 2013.

12. **Attila A. Yavuz**, "ETA: efficient and tiny and authentication for heterogeneous wireless systems". In Proceedings of the *sixth ACM conference on Security and privacy in wireless and mobile networks (WiSec '13)*, pp. 67-72, Hungary, Budapest, April 2013.

11. Benjamin Glas, Jorge Guajardo, Hamit Hacioglu, Markus Ihle, Karsten Wehefritz and **Attila A. Yavuz**, "Signal-based Automotive Communication Security and Its Interplay with Safety Requirements", *ESCAR, Embedded Security in Cars Conference*, Germany, November 2012.

10. **Attila A. Yavuz**, Peng Ning and Michael K. Reiter, "Efficient, Forward-secure and Append-only Cryptographic Constructions for Publicly Verifiable Audit Logging", *Financial Cryptography and Data Security (FC 2012)*, Lecture Notes in Computer Science (LNCS), vol. 7397, pp. 148-163, Bonaire, March 2012.

9. **Attila A. Yavuz** and Peng Ning, "BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems", in *Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC '09)*, pp. 219-228, December 2009, Honolulu, Hawaii, USA.

8. **Attila A. Yavuz** and Peng Ning, "Hash-Based Sequential Aggregate and Forward Secure Signature for Unattended Wireless Sensor Networks", Annual International *Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous*, pp. 13-16, Toronto, Canada, July 2009.

7. **Attila A. Yavuz**, Fatih Alagoz and Emin Anarim, "NAMEPS: N-Tier Satellite Multicast Security Protocol Based on Signcryption Schemes", *IEEE GLOBECOM Conference, San Francisco*, November 2006.

6. **Attila A. Yavuz**, Fatih Alagoz and Emin Anarim, "Three-Tier Satellite Security Multicast

Security Protocol Based on ECMQV and IMC Methods", *Computer-Aided Modeling, Analysis and Design of Communication Links and Networks, (IEEE CAMAD'06)*, Italy, April 2006.

5. **Attila A. Yavuz**, Fatih Alagoz and Emin Anarim, "A New Satellite Multicast Security Protocol Based on Elliptic Curve Signatures," *2nd Information and Communication Technologies (ICTTA '06)*, 2006.

4. **Attila A. Yavuz**, Fatih Alagoz, Emin Anarim, "A New Multicast Security Protocol", *GAP, International V. Engineering Congress*, 2006.

3. **Attila A. Yavuz**, Fatih Alagoz and Emin Anarim, "HIMUTSIS: Hierarchical Multi-Tier Adaptive Ad-hoc Network Security Protocol Based on Signcryption Type Key Exchange Schemes", *ISCIS 2006 vol. 4263, Lecture Notes in Computer Science (LNCS)*, page 434-445, Springer-Verlag, November 2006.

2. **Attila A. Yavuz**, Emin Anarim and Fatih Alagoz, "Improved Merkle Cryptosystem", *ISCIS 2006 vol. 4263, Lecture Notes in Computer Science (LNCS)*, page 924-934, Springer-Verlag, Nov. 2006.

1. Goksel Biricik, **Attila A. Yavuz**, Omur Kartal, Oya Kalipsiz, "Developing Information System with N-Tier Architecture: Hospital Management Information System", *Biltek International Informatik Congress*, 2005.

Patents [P]

30. **Attila A. Yavuz** and Saleh Darzi, "System and Method for Secure Location-Proof and Anonymous Privacy-Preserving Spectrum Access", Attorney Docket No. 11001-226US1, USF TTO Ref. 24T238US2, Provisional Filed: June 16, 2025.

29. **Attila A. Yavuz** and Saleh Darzi, "Resilient Authentication for Next-Generation Wireless Networks with Lawful Interception and Quantum-Safe Forgery Detection", Attorney Docket No. 173738-3055, USF TTO Ref. 25T059US, Provisional Filed: June 2025.

28. **Attila A. Yavuz** and Kiarash Sedghi, "A Lightweight Multiple-Time Post-quantum Signature for Heterogeneous Internet of Things", TTO Ref. 25T013PR-CS, Submitted: August 20, 2024, Status: Provisional Patent Filed.

27. **Attila A. Yavuz** and Kiarash Sedghi, "Efficient, Scalable and Post-Quantum Authentication for Real-time Next Generation Networks with Probabilistic Data Structures", TTO Ref. 24T240PR-CS, Submitted: June 28, 2024, Status: Provisional Patent Filed.

26. **Attila A. Yavuz** and Saleh Darzi, "A System and Method for Privacy-preserving and Post-quantum Secure Counter Denial of Service for Spectrum Management in Next-Generation Wireless Networks", TTO ref. 24T238PR-CS , Submitted: June 21, 2024, Status: Provisional Patent Filed.

25. Bechir Hamdaoui and **Attila A. Yavuz**, "System and Method for Increased Resiliency of Mobile Wireless Networks via Disributed Public Key (PKI) Alliances", U.S. Patent Application No. US18/676435, Published: November 11, 2024, Status: Utility Application Filed.

24. **Attila A. Yavuz** and Saif E. Nouma, "System and Method for Cryptographic Forensic Audits on Ligthweight IoT and Digital Archives", Patent US20240007300A1, U.S. Patent Application No. US18/341,901, Published: January 01, 2024, Status: Utility Application Filed.

23. **Attila A. Yavuz**, "Lightweight, Resilient and Aggregate Symmetric Cryptographic tools for Internet of Things and Forensics", International Patent Application No. PCT/US23/75133, Submitted: 09/26/2023, Status: Utility-Filed.

22. **Attila A. Yavuz**, "Publicly Verifiable and Resilient Symmetric Authentication and Privacy

Systems and Related Methods", Patent US20230283481A1, Application US18/178,286, Submitted: 09/07/2023, Status: Utility-Filed.

21. **Attila A. Yavuz** and Saif Nouma, "Hardware Supported Authentication and Signatures for Wireless, Distributed and Blockchain Systems", Patent US20230308289A1, Application US18/188,749, Submitted: 09/28/2022, Status: Utility-Filed.

20. Rouzbeh Behnia and **Attila A. Yavuz**, "Lightweight Post-quantum Authentication", Patent US20220385484A1, Submitted: 12/01/2022, Status: Utility-Filed.

19. Jean-François Biasse, Sriram Chelleppan, Sherzod Kariev, Noyem Khan Lynette Menezes, Efe U. A. Seyitoglu, Charurut Somboonwit and **Attila A. Yavuz**, "Anonymity Preserving Contact-Tracing App.", USF-20A073, Submitted: 07/19/2020, Status: Under revision.

18. Efe U. A. Seyitoglu and **Attila A. Yavuz**, "System and Method for Energy Efficient and Useful Blockchain Proof of Work", Patent WO 2022/104132 A1, Issue Date: 05/19/2022, Status: Granted.

17. **Attila A. Yavuz**, "Sender Optimal, Breach-Resilient, and Post-Quantum Secure Cryptographic Methods and Systems for Digital Auditing", Patent US10630478B1, Submitted: October 23, 2018, Issue Date: 04/21/2020, Status: Granted.

16. Muslum O. Ozmen, Rouzbeh Behnia and **Attila A. Yavuz**, "Algebraic proof-of-work algorithm for blockchains", Patent US20210314158A1, File Date: 04/07/2020, Publication Date: 10/07/2021, Status: Granted.

15. **Attila A. Yavuz**, Muslum O. Ozmen and Rouzbeh Behnia, "Energy-Aware Digitial Signatures", USF-19A001, Serial No: 16/273,828, Patent No: 10,547,455, File Date: 02/12/2019, Issue Date: 01/20/2020, Status: Granted.

14. **Attila A. Yavuz**, "System and Methods for Compromise Resilient and Compact Authentication for Digital Forensics", USF-19A107US, Serial No: 62/896,705, File Date: 09/04/2020, Status: Utility Patent Filed.

13. Rouzbeh Behnia, Muslum Ozmen and **Attila A. Yavuz**, "Efficient Identity-based and Certificateless Cryptosystems", USF- 19A051, Patent No: US10,673,625, Serial No: 16/442,467, File Date: 06/16/2019, Patent WO 2022/104132 A1, Status: Granted.

12. **Attila A. Yavuz**, "System and Method of Audit Log Protection", USF-18B164, Serial No: 16/389,519, Patent No: 10,554,416, File Date: 04/19/2019, Issue Date: 05/12/2020, Status: Granted.

11. **Attila A. Yavuz**, "Communication Efficient Key Exchange Methods for Internet of Things and Systems", USF-18B160PR, Provisional Patent Application No:62/750,337, 09/18/2018.

10. Muslum O. Ozmen, Thang Hoang, and **Attila A. Yavuz** "Forward-Private Dynamic Searchable Symmetric Encryption with Efficient Search", Patent US10922273B1, Issue Date: 02/18/2021, Status: Granted.

9. Mohamed Grissa, **Attila A. Yavuz**, and Bechir Hamdaoui, "Apparatus and method for protecting location privacy of cooperative spectrum sensing users", Patent US10575331B2, Issued: February 25, 2020, Status: Granted.

8. **Attila A. Yavuz**, Jorge Guajardo, and Thang Hoang, "Method and System for Search Pattern Oblivious Dynamic Symmetric Searchable Encryption", Patent US11144663B2, Filed: 12/28/2017, Issued: 10/12/2021, Status: Granted.

7. Jorge Guajardo, Paul Duplys, and **Attila A. Yavuz**, "System and method for shared key agreement over untrusted communication channels", Patent US9438417B2, Issued: 09/06/2016,

Status: Granted.

6. Anand A. Mudgerikar, Ankush Singla, Ioannis Papapanagiotou and **Attila A. Yavuz**. "Hardware Accelerated Priority based Message Authentication for Vehicular Networks", USPTO: 62/201096 , Submitted: August 3, 2015.

5. **Attila A. Yavuz**, Jorge Guajardo and Anvesh Ragi, "System and method for dynamic, non-interactive, and parallelizable searchable symmetric encryption", Patent WO2015055762 A1, Priority Date: October 18, 2013, Filing Date: October 16, 2014, Issued: April 23, 2015.

4. Jorge Guajardo, **Attila A. Yavuz**, Benjamin Glas, Markus Ihle, Hamit Hacioglu, and Karsten Wehefrit, "System and method for counter mode encrypted communication with reduced bandwidth", Patent US 20140270163 A1, Filed: March 14, 2013, Issued: September 18, 2014.

3. **Attila A. Yavuz**. "System and Method for Secure Review of Audit Logs", International Publication Number: WO 2015/187640 A3, Filed: June 2, 2014, Issued: 10 December, 2015.

2. **Attila A. Yavuz**, Jorge Guajardo, and Shalabh Jain, "System and method for mitigation of denial of service attacks in networked computing systems", Patent WO2014144555 A1, Filed: March 15, 2013, Issued: September 18, 2014.

1. **Attila A. Yavuz**, "System and method for message verification in broadcast and multicast networks", Patent US8667288 B2, Filed: May 29, 2012, Issued: March 4, 2014.

E-Prints [E]

11. Saif Eddine Nouma, Gokhan Mumcu, and **Attila A. Yavuz**, "Diamond: Design and Implementation of Breach-Resilient Authenticated Encryption Framework For Internet of Things", ePrint Archive, arXiv:2601.00353v1, January 2026.

10. Saleh Darzi, Saif Eddine Nouma, Kiarash Sedghighadikolaei, **Attila A. Yavuz**, "QPADL: Post-Quantum Private Spectrum Access with Verified Location and DoS Resilience", October 4, 2025, arXiv preprint, arXiv:2510.03631.

9. Saleh Darzi, Mirza Masfiqur Rahman, Imtiaz Karim, Rouzbeh Behnia, **Attila A Yavuz**, and Elisa Bertino, "Future-Proofing Authentication Against Insecure Bootstrapping for 5G Networks: Feasibility, Resiliency, and Accountability", ePrint Archive, arXiv:2510.23457v2, December 2025.

8. Yilu Dong, Rouzbeh Behnia, **Attila A. Yavuz** and Syed Rafiul Hussain, "Securing 5G Bootstrapping: A Two-Layer IBS Authentication Protocol", ePrint Archive, arXiv:2502.04915v1, Feb 2025.

7. Kiarash Sedghighadikolaei and **Attila A. Yavuz**, "Privacy-Preserving and Trustworthy Deep Learning for Medical Imaging", June 29, 2024, arXiv preprint arXiv:2407.00538.

6. Saleh Darzi, Kasra Ahmadi, Saeed Aghapour, **Attila A. Yavuz** and Mehran M. Kermani, "A Comprehensive Survey of Threshold Digital Signatures: NIST Standards, Post-Quantum Cryptography, Exotic Techniques, and Real-World Applications", October 18, 2023, arXiv preprint arXiv:2310.12037.

5. Saleh Darzi and **Attila A. Yavuz**, "PQC meets ML or AI: Exploring the Synergy of Machine Learning and Post-quantum Cryptography", February 13, 2024, TechRxiv.

4. Opeyemi Ajibuwa, Bechir Hamdaoui and **Attila A. Yavuz**, "A Survey on AI/ML-Driven Intrusion and Misbehavior Detection in Networked Autonomous Systems: Techniques, Challenges and Opportunities", May 2023, ePrint Archive, arXiv:2305.05040.

3. **Attila A. Yavuz** and Rouzbeh Behnia, "FROG: Forward-Secure Post-Quantum Signature",

May 2022, CoRR abs/2205.07112.

2. Muslum O. Ozmen, Rouzbeh Behnia, and **Attila A. Yavuz**, "IoD-Crypt: A Lightweight Cryptographic Framework for Internet of Drones." 2019, arXiv 1904.06829.

1. Jean-François Biasse, Sriram Chelleppan, Sherzod Kariev, Noyem Khan, Lynette Menezes, Efe U. A. Seyitoglu, Charurut Somboonwit and **Attila A. Yavuz**, "Trace-Σ: a privacy-preserving contact tracing app", Cryptology ePrint Archive, Report 2020/792.

Edited Books Computer Simulation Techniques - The Definitive Intro with Prof. Dr. Harry Perros

Teaching

I introduced three new courses to the USF curriculum and re-designed a core-course. The USF follows the semester system.

- CIS 4212/6214: Privacy-Preserving and Trustworthy Cyber-Infrastructures (Spring 2019-2026)
- CIS 4930/6930 Cryptography: Theory and Practice (Fall 2022, Fall 2025)
- COP 4538 IT Data Structures (Fall 2019-2024)
- COP 4931: Information Privacy and Trustworthy Systems (Fall 2018)

I introduced four new courses to the OSU curriculum, and also taught others. OSU follows the quarter system.

- CS 519/ECE 599: Applied Cryptography (Winter 2015-2018)
- CS 478/ECE 478: Introduction to Network Security (Spring 2015-2018)
- CS 372/ECE 372: Introduction to Computer Networks (Spring 2017)
- CS/ECE 578: Cyber-security (Fall 2017)
- CS 519/ECE 559: Advanced Network Security (Fall 2014-2016)
- CS 505 Cyber-security Reading Seminar (Fall 2015)

Mentoring

I am privileged to work with the following talented students:

- **Current Ph.D. Students**
  - Saleh Darzi (Spring 2022 - present)
  - Kiarash Sedghi (Spring 2023 - present)
  - Reeshav Acharya (Fall 2025 - present)
  - Lazar Lazarevic (Spring 2026 - present)
  - Sean Hernandez (Fall 2026 - present)
- **Graduated**
  - Saif Nouma (Ph.D., Spring 2026)
  - Rouzbeh Behnia (Ph.D., Spring 2021)
    - Assistant Professor (tenure-track) at the Muma College of Business at USF in Tampa (starting Summer 2021)
  - Thang Hoang (Ph.D., Spring 2020)
    - Assistant Professor (tenure-track) at The Department of Computer Science, Virgina Tech, VA (December 2020)
  - Mohamed Grissa (Ph.D., Fall 2018, Co-advised (equal share) with Dr. Bechir Hamdaoui)
    - Cryptographic engineer at Gradient (MIT-Berkeley-NSA founded), Boston, MA
  - Efe U. A. Seyitoglu (MS, Spring 2020)

    - Software Engineer, Yelp, England.
  - Muslum Ozgur Ozmen (MS, Spring 2018, continued as a Ph.D. at USF in 2019)
    - Assistant Professor (tenure-track), Computer Science, Arizona State University, AZ.
  - Gungor Basa, "Image Based Cryptography", (MS, Spring 2016)
    - Software engineer at DeliveryHero, Berlin, Germany
  - Gabriel Hackebeil, "Efficient Oblivious Access to Trees", (MS, Fall 2016)
    - Software engineer at Deepfield, Ann Arbor, MI

- **Current and Past Undergraduate Students**
  - Sheng Rao (REU, NSF 2350213, USF 2025)
  - Lazar Lazarevic (REU, NSF S-STEM (by Dr. Sanjukta Bhanja), USF 2025)
  - Sean Hernandez (USF 2025)
  - Matthew Signore (2023)
  - Patricia Tran (WICSE Program - NSF CAREER, USF 2022)
  - Francis Hahn (NSF CAREER, USF 2022)
  - Brandt Stevenson (DoE, USF 2022)
  - Bianca Dehaan (DoE, USF 2022)
  - Henry Cardenas (DoE , USF 2021)
  - Sydney Seelen (WICSE Program - NSF CAREER, USF 2021)
  - Lokambika Muthu (WICSE Program - NSF CAREER, USF 2020)
  - Kelsy Ecclesiastre (BullsEYE - NSF CAREER, USF 2019)
  - Aaya Watson (BullsEYE - NSF CAREER, USF 2019)
  - Keanno Carter (NSF LSAMP, USF 2019)
  - Morgan Hausmann (WICSE Program - NSF CAREER, USF 2019)
  - Garrett Christophe Haley (EECS Capstone, OSU 2018)
  - Andrew Ekstedt (EECS Capstone, OSU 2018)
  - Scott Merrill (EECS Capstone, OSU 2018)
  - Scott Russell (EECS Capstone, OSU 2018)
  - Joshua Webb (NSF-FUND STEM Leaders Program, OSU 2017)
  - Nathan Burnett (EECS RIU Initiative, OSU 2017)
  - Matt Baker (EECS RIU Initiative, OSU 2017)
  - Erich Hansje Kramer (EECS RIU Initiative, OSU 2017)

Past Mentoring Experience: During my work at Robert Bosch Research and Technology Center and University of Pittsburgh, I found opportunity to work with the following students: Shalabh Jain, Velin Kounev, Alana Libonati, Shauna Michelle Policicchio and Anvesh Ragi. I also advised Ceyhun Ozkaptan (2015) at OSU.

Outreach Activities

I have been organizing/participating several outreach activities targeting underrepresented groups.

- The CodeBreakHERS: I am the co-organizer of a cybersecurity camp, in which we train more than 50 K-12 female students via hands-on cryptography activities every summer.
- Contributing to the preparation of educational videos on advanced cryptographic primitives, Center for Cryptographic Research at USF.
- Women in Computer Science and Engineering (WICSE): We recruit underrepresented female undergraduates at CSE USF every year (participation).
- Bulls Engineering Youth Experience (Bulls - EYE). We support underrepresented USF undergraduates to mentor middle school youth from the Tampa Bay community (participation).
- Louis Stokes Alliance for Minority Participation (LSAMP). I have been recruiting underrepresented undergraduate students both at OSU and USF via (FG)LSAMP program.
- EECS at OSU Research in Undergraduate Activities. We supported undergraduate research at junior-level via an internal grant.

Professional Services

Associate Editor:

- IEEE Transactions on Dependable and Secure Computing (2023-)

Program Committee (PC), Chair, and Panel Member:

- NSF Panelist (2020-2024, 2026)
- Usenix Symposium (2024-2026)
- IEEE Silicon Valley Cybersecurity Conference (SVCC), 2020-2026
- NDSS Student Support Committee (2025)
- Program Co-Chair - ACM CCS Workshop on Quantum-Resistant Cryptography and Security (QRSEC 2025)
- Program Co-Chair - IEEE TPS 2025
- IEEE TPS (2024-2025)
- IEEE MLC Workshop (2025)
- Privacy Enhancing Technologies Symposium (PETS), 2020-2024
- The ACM Conference on Computer and Communications Security (CCS), Doctoral Symposium Committee (2024)
- ACM Workshop on Privacy in the Electronic Society WPES - Co-located with CCS (2024)
- IEEE Global Blockchain Conference (IEEE GBC) (2024)
- Annual Computer Security Applications Conference (ACSAC), 2017-2022
- Security and Privacy Track Chair, IEEE International Conference on Mobile Ad-Hoc and Smart Systems (MASS 2022)
- IEEE Conference on Communications and Network Security (CNS), 2022
- IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) (2020-2021)
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2020
- Conference on Data and Applications Security and Privacy (DBSec), 2018-2020
- Annual Web Conference (WWW), 2019-2020
- Military Communications (Milcom), 2019
- International Workshop on Security and Privacy for the Internet-of-Things (IoTSec), 2019
- IEEE SmartGridComm, 2018
- IEEE IEMCON, 2018

- IEEE International Workshop on Big Data Security and Services, 2018
- ACM International Workshop on Trustworthy Embedded Devices (TrustED), 2014-2016
- Advanced Intrusion Detection and Prevention Workshop (AIDP), 2014
- International Workshop on Collaborative Cloud (CollabCloud), 2014
- ASE International Conference on Cyber Security, 2014

Reviewer in Journals:

- IEEE Transactions on Information Forensics and Security (2014-2025)
- IEEE Transactions on Dependable and Secure Computing (2014-2025)
- IEEE Transactions on Services Computing (2024-2025)
- IEEE Transactions on Mobile Computing (2024)
- IEEE Transactions on Network and Service Management (2024)
- ACM Transactions on Embedded Computing Systems (2024)
- ACM Transactions on Privacy and Security (TOPS) (2017-2024)
- ACM Transactions on Internet Technologies (TOIT) (2022-2023)
- Future Generation of Computer Systems, Elsevier (2016,2021)
- IEEE Transactions on Computers (2012-2014, 2020)
- IEEE Communications Surveys and Tutorials (2014-2015, 2020)
- Journal of Information Security and Applications (2020)
- Journal of Computer Security (2013-2014, 2020)
- IEEE Transactions on Cloud Computing (2017)
- IEEE Transactions on Parallel and Distributed Systems (2014-2016)
- IEEE Transactions on Smart Grid (2014-2016)
- International Journal of Distributed Sensor Networks (2016)
- IEEE Transactions on Internet of Things (2015)
- IEEE Transactions on Education (2015)
- International Journal of Parallel, Emergent and Distributed Systems (2015)
- Journal of Sensors, Open Access Journal by MPDI (2015)
- International Journal of Communication Systems by Wiley (2013-2014)
- Concurrency and Computation: Practice and Experience (2011)
- Journal of System and Software (2007-2011)
- IEEE Transactions on Information Technology in Biomedicine (2007)

Services:

- Scouting Commitee, BCAICC at USF, (2025-2026)
- Recruitment Commitee at BCAICC USF, (2025-2026)
- Tenure and Promotion Committee at BCAICC USF, (2024-2026)
- Graduate Committee at BCAICC USF, (2018-2026)
- Ad-hoc committee for career prep modules, BCAICC at USF, (2025)
- Broadening Participating in Computing (BPC) Committee at CSE USF (2022-2024)
- IEEE Senior Membership Elevation Committee (2020-2021)

- EECS Graduate Curriculum and Admission Committees at OSU (2014-2018)
- Ph.D. Thesis Committee
  - Thushari Hapuarachchi, Ph.D., University of South Florida, (Defense 2026)
  - Saeed Aghapour, Ph.D., University of South Florida, (Major Area 2025)
  - Saleh Darzi, Ph.D., University of South Florida, (Major Area 2025)
  - Wenwei Zhao, Ph.D., University of South Florida, (Major Area 2025)
  - Xiaowen Li, Ph.D., University of South Florida, (Major Area 2025)
  - Yuwen Cui, Ph.D., University of South Florida, (Defense 2025)
  - Thomas Ran, Ph.D., University of South Florida, (Major Area 2025)
  - Rabiah Othman Alnashwan, Ph.D., University of Sheffield, (Viva 2024)
  - Daniel A. Ramirez, Ph.D., University of South Florida, (Defense 2024)
  - Tanvir Bhuiyan, Ph.D., University of South Florida, (Defense 2023)
  - Zhe Qu, Ph.D., University of South Florida, (Defense 2022)
  - Xiao Han, Ph.D., University of South Florida, (Major Area 2022)
  - Tao Hou, Ph.D., University of South Florida, (Defense 2022)
  - Jing Ling, Ph.D., University of South Florida, (Defense 2022)
  - Di Zhuang, Ph.D., University of South Florida, (Defense 2021)
  - Abed Alanazi, Ph.D., University of South Florida, (Defense 2021)
  - Chengbin Hu, Ph.D., University of South Florida, (Major Area 2020)
  - Tao Hou, Ph.D., University of South Florida, (Defense 2020)
  - Longfei Wang, Ph.D., University of South Florida, (Defended 2018)
  - Brent Carmer, Ph.D., Oregon State University (Defended 2017)
  - Peter Byerley Rindal, Ph.D., Oregon State University (Defended 2017)
  - Sherif Abdelwahab, Ph.D., Oregon State University (Defended 2017)
  - Abdelkader Aljerme, Ph.D., Oregon State University (Defended 2016)
  - Bassem Khalfi, Ph.D., Oregon State University (Defended 2018)
  - Mehiar Dabbagh, Ph.D., Oregon State University (Defended 2016)
  - Nadia Adem , Ph.D., Oregon State University (Defended 2016)
  - Velin Kounev, Ph.D., University of Pittsburgh, (Defended 2015)
- MS Thesis Committee
  - Zhangxiang Hu, MS, (Defended 2015)
  - Shajith Ravi, MEng, (Defended 2016)

Memberships: IEEE Senior Member and ACM Member.