Dr. Attila Altay Yavuz

CONTACT INFORMATION

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

E-mail: attilaayavuz@usf.edu
URL: https://cse.usf.edu/~attilaayavuz/

EXECUTIVE SUMMARY

Dr. Attila A. Yavuz is an internationally recognized scholar in applied cryptography and cybersecurity whose work bridges rigorous cryptographic design and deployable systems for post-quantum security, privacy, and mission-critical networks. As Director of the Applied Cryptography Research Laboratory and Co-Director of the Cryptologic Center at the University of South Florida, he leads a research program spanning lightweight and post-quantum authentication, privacy-enhancing technologies, and security protocols for IoT, 5G/NextG, and critical systems. His record includes 123 publications/patents, $5.86M in competitively awarded funding ($2.25M personal share), technology-transfer activity involving Bosch and DOE-affiliated initiatives, and mentorship of graduates who have gone on to tenure-track positions. His service as Associate Editor of IEEE TDSC, NSF panelist, Program Co-Chair, and invited speaker at national venues and internationally attended forums reflects sustained external recognition and leadership in applied cryptography and cybersecurity.

Funding	Secured $5,864,336 in competitively awarded funding ($2,254,377 personal share), including an NSF CAREER award, two NSF Medium projects as lead PI, and seven industry awards from Cisco and Bosch.
Scholarly Impact	Authored 123 publications and patents (excluding 12 e-prints and 4 manuscripts under revision), with work appearing in premier venues such as IEEE S&P, NDSS, ACM CCS, PETS, and IEEE TIFS/TDSC. This body of work has been recognized with best paper, outstanding research, and innovation awards. Thirty-seven publications/patents are accompanied by open-source software for public use, and multiple projects have informed real-world evaluation efforts, including DOE-affiliated initiatives and Bosch-tested DSSE platforms. Google Scholar metrics (May 2026): h-index 32, i10-index 74, 2,965+ citations; full metrics: https://scholar.google.com/citations?user=vx6BwmwAAAAJ&hl=en.
Mentorship	Graduated 8 students (4 Ph.D., 4 M.S.). Two Ph.D. graduates now hold tenure-track faculty positions at Virginia Tech and USF, and one M.S. graduate holds a tenure-track faculty position at Arizona State University. Mentored 25+ undergraduate researchers and industry interns.
Leadership	Associate Editor (IEEE TDSC); Program Co-Chair (ACM QRSec 2025, IEEE TPS 2025); Steering Committee Member (ACM PQQS 2026); service on 25 program committees; reviewer for 16 IEEE/ACM journals; and panelist on 8 NSF review panels. Served on internal committees at USF and OSU, led research initiatives at Bosch, and delivered invited talks at NSF and cybersecurity forums.
Educational	Developed 7 cybersecurity electives across USF and OSU and taught large-enrollment core courses such as data structures and computer networks. His teaching evaluations are at or above the college average, and his courses are recognized for strong research orientation and innovation. He has also led outreach through (FG)LSAMP, Bulls-EYE, WICSE, and CodeBreakHERS.
Post-Tenure (2021–present)	Since 2021, secured $3.1M in funding ($983,307 personal share), including two active NSF projects as lead PI, two industry awards, and one federal grant as Co-PI. Produced 47 papers and patents (9 journal articles, 25 conference papers, 13 patents), including work appearing in IEEE S&P 2026, IEEE S&P workshops, NDSS 2022/2023, and several IEEE/ACM transactions. Graduated one Ph.D. student, advanced another to candidacy, and currently advises 5 Ph.D. students. Many of his most visible external leadership roles, including Associate Editorship and Program Co-Chair appointments, have also been undertaken post-tenure.

Education

North Carolina State University, Ph.D., Computer Science, Raleigh, NC (2007–2011)
Thesis: Compromise Resilient and Compact Cryptographic Constructions for Digital Forensics
Advisor: Prof. Dr. Peng Ning

Bogazici University, M.S., Computer Science, Istanbul, Turkey (2004–2006)

Yıldız Technical University, B.S., Computer Science, Istanbul, Turkey (1999–2004)

Professional Experiences

- **Associate Professor**, the Bellini College of AI, Cybersecurity, and Computing (BCAICC), University of South Florida (USF) (2021–present)
- **Assistant Professor**, the Department of Computer Science and Engineering, USF (2018–2021)
- **Assistant Professor**, the School of Electrical Engineering and Computer Science, Oregon State University (2014–2018)
- **Research Scientist**, Bosch Research and Technology Center (2011–2014)
- **Research/Teaching Assistant**, the Department of Computer Science, NC State University, Cyber Defense Laboratory (2007–2011)
- **Research Engineer**, Satellite Networks Research Laboratory, Bogazici University (2004–2006)

Expertise

- **Applied Cryptography**: Digital signatures (lightweight, post-quantum, aggregate, forward-secure, threshold), secure audit logging, public-key infrastructure, authenticated encryption.
- **Network & System Security**: IoT, 5G/NextG, vehicular, satellite-terrestrial, and smart-grid security protocols; hardware-assisted cryptographic implementations, broadcast authentication.
- **Privacy-Enhancing Technologies**: Searchable encryption (dynamic symmetric and public-key based), applications of secure multi-party computation, Oblivious RAM (ORAM), private ML.
- **Post-Quantum Cryptography**: Hash-based and lattice-based signature and authentication schemes; hybrid classical/post-quantum protocol design for networked systems.

Selected Awards

- NSF CAREER Award (2017)
- Cisco Research Awards (2025, 2022, 2020, and 2019)
- Human-Machine Intelligence for Security Analytics (IEEE S&P 25 Workshop, Best Paper Award) (2025)
- USF Excellence in Innovation Award (2022)
- Member of National Academy of Inventors (2021)
- 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

Dr. Yavuz secured a total of $5,864,336, including $2,254,377 as his 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, his 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, his share: $282,324

• **Perceptive and Reactive Autonomous Navigation in Challenging Environments: 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, his share: $186,998

• **NSF CAREER: Lightweight and Fast Authentication for Internet of Things**

Attila A. Yavuz (Sole-PI), National Science Foundation Award No. CNS–1917627

03/2017–01/2023, Total: $500,000

• **Trustworthy Digital Forensics for Heterogeneous Internet of Things**

Cisco Research Award (Sole-PI)

01/2022–01/2025, Total: $98,985

• **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

12/2019–12/2022, Total: $50,000

• **Lightweight and Quantum-Safe Authentication for Internet of Things**

Cisco Research Award (Sole-PI)

06/2019–01/2025, 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)

01/2020–01/2022, Total: $100,000, his 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, his 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, his share: $3,000

- **Cloud Security Technologies and Oblivious Random Access Machine**
  Attila A. Yavuz (Sole-PI), Unrestricted Gift, Robert Bosch
  12/2018–12/2022, 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, his 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
  11/2018–12/2018, Total: $18,000

- **OSU EECS RIU Initiative (Internal Grant)**
  Attila A. Yavuz (PI), 04/2017–12/2017, Total: $14,400

Publications

Underlined authors are Dr. Yavuz's current or former Ph.D./MS advisees at the time of the work's initial submission. In his field, it is typical for faculty members to appear after their advisees in authorship.

Journal Papers [J]

30. 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)*, Vol. 7, No. 2, Article 14, 33 pages, May 2026.
29. Saif E. Nouma and **Attila A. Yavuz**, "Lightweight and Resilient Signatures for Cloud-Assisted Embedded IoT Systems", in *Security and Privacy, Wiley*, Vol. 9, No. 1, January 2026.
28. 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*, Vol. 58, Issue 6, No. 143, pp. 1–39, December 2025.
27. S. Aghapour, Kiarash Sedghighadikolaei, **Attila A. Yavuz**, B. Hamdaoui and Mehran M. 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, December 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, October 2025.
25. Yiwei Zhang, Rouzbeh Behnia, **Attila A. Yavuz**, Reza Ebrahimi, and Elisa Bertino, "Efficient Full-Stack Private Federated Deep Learning with Post-Quantum Security", *IEEE Transactions*

on Dependable and Secure Computing (IEEE TDSC), Vol. 22, pp. 5567–5583, October 2025.

24. 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.

23. 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*, Vol. 33, September 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, pp. 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*, Vol. 9, pp. 33860–33879, 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. 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*, Vol. 5, No. 4, pp. 949–962, December 2019.

18. **Attila A. Yavuz** and Muslum O. Ozmen, "Ultra Lightweight Multiple-time Digital Signature for the Internet of Things Devices", *IEEE Transactions on Services Computing*, Vol. 15, Issue 1, pp. 215–227, July 2019.

17. 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.

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*, Vol. 14, Issue 6, pp. 1675–1689, 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 Magazine*, 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*, Vol. 9, No. 2, pp. 598–609, 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)*, Vol. 17, Issue 5, pp. 1269–1282, 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, 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, July 2017.

9. 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.

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, pp. 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, September 2015.

5. Panos Kampanakis, **Attila A. Yavuz**, "BAFi: A Practical Cryptographic Secure Audit Logging Scheme for Digital Forensics", in *Security and Communication Networks* (Wiley), 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** 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.

2. **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 Transactions on Information and System Security*, Vol. 15, Issue 2, Article 9, 28 pages, July 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]

64. Gurkan Gur and **Attila A. Yavuz**, "SATUQ: Quantum-Ready Cybersecurity for Integrated Space–Aerial–Terrestrial Networks", in *23rd ACM International Conference on Computing Frontiers (CF'26)*, Invited Paper, to appear, May 19–20, 2026, Catania, Sicily, Italy.

63. Kiarash Sedghighadikolaei, Changqi Sun, Thang Hoang, Bechir Hamdaoui, and **Attila A. Yavuz**, "A Full Threshold NIST PQC-Compliant Framework for Distributed Trust in Federal Public Key Infrastructure", in *47th IEEE Symposium on Security and Privacy (IEEE S&P 26)*, to appear, 18–21, May 2026, San Francisco, CA, USA.

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 (IEEE MILCOM)*, 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)*, pp. 1–9, September 2025, Avignon, France.

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), pp. 280–285, 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 M. Kermani, Jeremiah Birrell, Jason Pacheco, and **Attila A. Yavuz**, "An Interactive Framework for Implementing Privacy-Preserving Federated Learning: Experiments on Large Language Models", IEEE S&P 25 Workshops, 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", in Quantum 2.0 Conference and Exhibition, Technical Digest Series (Optica Publishing Group), 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 O. 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 U. A. 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**, Muslum 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 U. A. Seyitoglu, **Attila A. Yavuz** and Muslum 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)*, Vol. 1., pp. 172–191, Stockholm, Sweden, July 2019.

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)*, Paris, France, April 2019.

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**, Fatma B. 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 3, 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", *31st 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*, Tunisia, 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 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, Budapest, Hungary, 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 Multicast Security Protocol Based on ECMQV and IMC Methods", *Computer-Aided Modeling, Analysis and Design of Communication Links and Networks, (IEEE CAMAD'06)*, Trento, Italy, April 2006, pp. 129–136.

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)*, pp. 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)*, pp. 924–934, Springer-Verlag, Nov. 2006.

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

Patents [P]

28. **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.

27. **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.

26. Muslum O. Ozmen, Rouzbeh Behnia and **Attila A. Yavuz**, "Algebraic Proof-of-Work Algorithm for Blockchains", Patent US20210314158A1, File Date: April 7, 2020, Publication Date: October 7, 2021, Issue Date: February 18, 2025, Status: Granted.

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

24. **Attila A. Yavuz** and Kiarash Sedghighadikolaei, "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.

23. **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.

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

21. **Attila A. Yavuz** and Saif E. Nouma, "System and Method for Cryptographic Forensic Audits on Lightweight IoT and Digital Archives", Patent US20240007300A1, U.S. Patent Application No. US18/341,901, Published: January 1, 2024, Status: Utility Application Filed.

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

19. **Attila A. Yavuz**, "Publicly Verifiable and Resilient Symmetric Authentication and Privacy Systems and Related Methods", Patent US20230283481A1, Application US18/178,286, Submitted: September 7, 2023, Status: Utility-Filed.

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

17. Rouzbeh Behnia and **Attila A. Yavuz**, "Lightweight Post-Quantum Authentication", Patent US20220385484A1, Submitted: December 1, 2022, Status: Utility-Filed.

16. 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: May 19, 2022, Status: Granted.

15. **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: April 21, 2020, Status: Granted.

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

13. **Attila A. Yavuz**, "System and Methods for Compromise Resilient and Compact Authentication for Digital Forensics", USF-19A107US, Serial No. 62/896,705, File Date: September 4, 2020, Status: Utility Patent Filed.

12. Rouzbeh Behnia, Muslum O. Ozmen and **Attila A. Yavuz**, "Efficient Identity-based and Certificateless Cryptosystems", Patent No. US12231568B2, Issue Date: June 2, 2020, Status: Granted.

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

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

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

8. 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.

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

6. Jorge Guajardo, Paul Duplys, and **Attila A. Yavuz**, "System and Method for Shared Key Agreement over Untrusted Communication Channels", Patent US9438417B2, Issued: September 6, 2016, Status: Granted.

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 Wehefritz, "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: December 10, 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.

Book Chapters [B]

1. Gurkan Gur and **Attila A. Yavuz**, "Post-Quantum Cryptography for Integrated Space-Aerial-Terrestrial Networks: Current State, Challenges and Trends", in *Cybersecurity in Space: Technologies, Threats, and Solutions*, Springer Cham, Armasuisse Science and Technology, to appear, June 2026.

E-Prints [E]

12. Elisa Bertino, Ramana Kompella, Ashish Kundu, Cristina Nita-Rotaru, Jaideep Vaidya and **Attila A. Yavuz**, "Quantum-Resistant Networks: A Review of Primitives, Protocols and Best Practices", ePrint Archive, arXiv:2605.04129, May 2026.

11. Saif E. 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 (under revision at ACM Transactions on Embedded Computing Systems).

10. Saleh Darzi, Saif E. Nouma, Kiarash Sedghighadikolaei, and **Attila A. Yavuz**, "QPADL: Post-Quantum Private Spectrum Access with Verified Location and DoS Resilience", October 4, 2025, arXiv preprint, arXiv:2510.03631 (under revision at Journal of Computer Networks, Elsevier).

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 (under revision at Journal of Computer Networks, Elsevier).

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, February 2025 (under revision at IEEE TDSC).

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. 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, August 2020, Report 2020/792.

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

TEACHING

In total, Dr. Yavuz introduced seven new courses (three at USF, four at OSU) and redesigned two core courses. USF follows the semester system.

- CIS 4212/6214: 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)

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

It is a privilege to have worked with the following talented students, both current and graduated.

Current Ph.D. Students

Name	**Since**	**Research Focus**
Saleh Darzi	Sp. 2022, Candidacy	Post-Quantum and Privacy-Preserving Spectrum Access for NextG Networks
Kiarash Sedghighadikolaei	Sp. 2023	Threshold Cryptography
Reeshav Acharya	Fa. 2025	Trustworthy AI
Lazar Lazarevic	Sp. 2026	Post-Quantum Cryptographic Protocols
Sean Hernandez	Fa. 2026 (Admitted)	Cybersecurity and Applied Cryptography

Graduated Ph.D. and M.S. Students

Name	**Degree**	**Year**	**Current Position**
Saif E. Nouma	Ph.D.	Sp. 2026	Recently Defended
Rouzbeh Behnia	Ph.D.	Sp. 2021	Asst. Prof. (tenure-track), Information Systems and Decision Sciences, Muma College of Business, USF
Thang Hoang	Ph.D.	Sp. 2020	Asst. Prof. (tenure-track), Department of Computer Science, Virginia Tech
Mohamed Grissa	Ph.D.	Fa. 2018	Senior Cryptographic Engineer, Gradient, Boston, MA (co-advised with Dr. Hamdaoui)
Muslum O. Ozmen	M.S.	Sp. 2018	Asst. Prof. (tenure-track), Department of Computer Science, Arizona State University
Efe U. A. Seyitoglu	M.S.	Sp. 2020	Software Engineer, Yelp, UK
Gabriel Hackebeil	M.S.	Fa. 2016	Software Engineer, Deepfield, Ann Arbor, MI
Gungor Basa	M.S.	Sp. 2016	Software Engineer, EggYolk AI, Ankara, Turkiye

Current and Past Undergraduate Students

- Sheng Rao, REU, NSF 2350213, USF, 2025
- Lazar Lazarevic, REU funded with Dr. Bhanja, USF, 2025; Ph.D. student since 2026
- Sean Hernandez, USF, 2025; Ph.D. student since 2026
- 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, Bulls-EYE – NSF CAREER, USF, 2019
- Aaya Watson, Bulls-EYE – 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-Funded 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 Industry/Visiting Mentees

- Shalabh Jain, Bosch, 2014
- Anvesh Ragi, Bosch, 2013
- Alana Libonati, Bosch, 2013
- Velin Kounev, University of Pittsburgh, 2013
- Shauna Michelle Policicchio, University of Pittsburgh, 2013

OUTREACH ACTIVITIES

Dr. Yavuz has organized and contributed to several outreach activities:

- CodeBreakHERS: He is a co-organizer of a cybersecurity camp, where he contributes to the training of more than 50 K-12 female students via hands-on cryptography activities every summer.
- He contributed to the preparation of educational videos on advanced cryptographic primitives for the Center for Cryptographic Research at USF.
- Bulls Engineering Youth Experience (Bulls-EYE). He supported underrepresented USF undergraduates in mentoring middle school youth from the Tampa Bay community.
- Louis Stokes Alliance for Minority Participation (LSAMP). He has been recruiting underrepresented undergraduate students both at OSU and USF via the (FG)LSAMP program.
- EECS at OSU Research in Undergraduate Activities. He supported undergraduate research at the junior level via an internal grant.

Memberships

IEEE Senior Member, ACM Member, Member of the National Academy of Inventors (NAI).

Selected Research and Invited Talks

Dr. Yavuz has delivered numerous research and invited talks at conferences and professional forums. Selected highlights:

- "Deployable, Breach-Resilient and Quantum-Safe Critical National Infrastructures", Cisco Research Quantum Security and PQC Virtual Summit, April 2026.
- "Trustworthy AI Systems Through Lenses of Post-Quantum Security and Privacy-Enhancing Techniques", CyberBay 2025, Tampa, Florida, October 2025.
- "Unleashing and Advancing Secure Computation for NextG Networks in the Post-Quantum and Artificial Intelligence Era", US-Taiwan NSF Cybersecurity Workshop, Invited Presentation, Arlington, VA, US, March 2025.
- "Envisioning the Future of NextGen Networked Systems and Digital Signatures", TSG Tech Seminar, June 2024.
- "Energy-Aware Digital Signatures for Embedded Devices", Distinguished Research Forum, Silicon Valley Cyber Security Conference (Distinguished Research Award), December 2020.
- "CAREER: Lightweight and Fast Authentication for Internet of Things", the 4th NSF SaTC Meeting, Alexandria, VA, October 2019.
- "Low-cost, Scalable and Practical Post-Quantum Key Distribution (CQKD)", CREDC-DoE Symposium, Q-Center, St. Charles, IL, June 25, 2019.

Professional Services

Associate Editor:

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

Panels, Chairing, and Leadership Roles:

- NSF Panelist (2020–2024, 2026)
- Steering Committee - ACM Conference on Post-Quantum and Quantum-based Security (ACM PQQS) (2026)
- Program Co-Chair - ACM CCS Workshop on Quantum-Resistant Cryptography and Security (QRSEC 2025)
- Program Co-Chair - IEEE TPS (2025)
- Security and Privacy Track Chair, IEEE International Conference on Mobile Ad-Hoc and Smart Systems (MASS 2022)
- IEEE Senior Membership Elevation Committee (2020–2021)

Program Committee (PC):

- USENIX Security Symposium (2024–2026)
- NextG Networks Cryptography and Security (NextG-Sec) (2026)
- IEEE Silicon Valley Cybersecurity Conference (SVCC) (2020–2026)
- NDSS Student Support Committee (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)
- 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 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)
- 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)

Internal Service:
- Scouting Committee at BCAICC USF (2025–2026)
- Recruitment Committee 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 Participation in Computing (BPC) Committee at CSE USF (2022–2024)
- EECS Graduate Curriculum and Admission Committees at OSU (2014–2018)

Ph.D. Thesis Committee:
- Jiahao Xue, Ph.D., University of South Florida, (Defense 2026)
- Thushari Hapuarachchi, Ph.D., University of South Florida, (Defense 2026)
- Wenwei Zhao, Ph.D., University of South Florida, (Defense 2026)
- Joshua Ranstrom,, Ph.D., University of South Florida, (Defense 2025)
- Saeed Aghapour, 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)
- 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)
- Longfei Wang, Ph.D., University of South Florida, (Defense 2018)
- Brent Carmer, Ph.D., Oregon State University (Defense 2017)
- Peter Byerley Rindal, Ph.D., Oregon State University (Defense 2017)
- Sherif Abdelwahab, Ph.D., Oregon State University (Defense 2017)
- Abdelkader Aljerme, Ph.D., Oregon State University (Defense 2016)
- Bassem Khalfi, Ph.D., Oregon State University (Defense 2018)
- Mehiar Dabbagh, Ph.D., Oregon State University (Defense 2016)
- Nadia Adem, Ph.D., Oregon State University (Defense 2016)
- Velin Kounev, Ph.D., University of Pittsburgh, (Defense 2015)

MS Thesis Committee:
- Zhangxiang Hu, Oregon State University, MS, (Defense 2015)
- Shajith Ravi, Oregon State University, MEng, (Defense 2016)