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: `http://www.csee.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 - 06/01/2004)

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

Professional Experiences

- **Associate Professor**, The Department of Computer Science and Engineering, 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)
- **Adjunct Faculty**, School of Computing and Information, University of Pittsburgh, (2014-present)
- **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

Awards

- NSF CAREER Award
- Cisco Research Award (2022)
- USF Excellence in Innovation Award (2022)
- Cisco Research Award (2020)
- 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)
- Cisco Research Award (2019)
- DBSec Best Paper Award (2018)

Funded Research

I have secured $2,851,211 in total with $1,374,555 on my share.

- **NSF CAREER: Lightweight and Fast Authentication for Internet of Things**
  Attila A. Yavuz (Sole PI), National Science Foundation Award No. CNS – 1917627
  03/2017 - 02/2022, 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 - present, 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]

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 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*, 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]

45. **Attila A. Yavuz**, Duncan Earl, Scott Packard and Saif Eddine 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 (SDRANCAN 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]

23. **Attila A. Yavuz**, "Lightweight, Resilient and Aggregate Symmetric Cryptographic tools for Internet of Things and Forensics", USF21B144PR, Submitted: 04/21/2022, Status: Under

Revision.

22. **Attila A. Yavuz** and Saif Nouma, "Hardware Supported Authentication and Signatures for Wireless, Distributed and Blockchain Systems", USF 22A009PR, US Serial No. 63/269,779, Submitted: 03/23/2022, Status: Under revision.

21. **Attila A. Yavuz**, " Efficient Privacy, Authentication and Resiliency Technologies on Wireless Systems for Forensic and Sensitive Data", USF 21B144PR, Submitted: 03/01/2022, Status: Under revision.

20. Rouzbeh Behnia and **Attila A. Yavuz**, "Lightweight Post-quantum Authentication", USF-20B156PR, Submitted: 02/16/2022, Status: Provisional-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", USF-20A088WO, nternational Patent Application No. PCT/US2021/059233, Submitted: 10/15/2021, Status: International Patent Pending.

17. **Attila A. Yavuz**, "Sender Optimal, Breach-Resilient, and Post-Quantum Secure Cryptographic Methods and Systems for Digital Auditing", USF-18B167, Patent No: US106,304,78 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.

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: 9/6/2019, Status: Patent Pending.

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, Status: Issued.

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: Issued.

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", USF-18B151, OSU-17-55, Provisional Application No: 62/572,339, Submitted: October 10, 2017, Revised: 08/15/2018.

9. Mohamed Grissa, **Attila A. Yavuz**, and Bechir Hamdaoui, "Apparatus and method for protecting location privacy of cooperative spectrum sensing users", Patent US10575331B2, Filed: February 22, 2018, Issued: February 25, 2020.

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.

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

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.

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

E-Prints [E]

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.

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 2019-2022)
- CIS 4930/6930 Cryptography: Theory and Practice (Fall 2022)
- COP 4538 IT Data Structures (Fall 2019-2022)
- 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**
  - Mohamed Bouzayene (Spring 2021 - present)
  - Saif Nouma (Fall 2021 - present)
  - Saleh Darzi (Spring 2022 - present)
  - Kiarash Sedghi (starting Fall 2022)
- **Graduated**
  - 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)
    - Ph.D. student at Purdue University
  - 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**
  - 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

Program Committee (PC) Member:

- NSF Panel Review (2020-2022)
- Privacy Enhancing Technologies Symposium (PETS), 2020-2022
- Annual Computer Security Applications Conference (ACSAC), 2017-2022
- Silicon Valley Cybersecurity Conference (SVCC), 2020-2022
- IEEE International Conference on Mobile Ad-Hoc and Smart Systems (MASS 2022), Security and Privacy Track Chair
- 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:

- ACM Transactions on Privacy and Security (TOPS) (2017-2022)
- IEEE Transactions on Information Forensics and Security (2014-2022)
- IEEE Transactions on Dependable and Secure Computing (2014-2022)
- ACM Transactions on Internet Technologies (TOIT) (2022)
- 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:

- IEEE Senior Membership Elevation Committee (2020-2021)
- CSE Graduate Committee at USF, (2018-present).
- EECS Graduate Curriculum and Admission Committees at OSU, 2014-2018.
- Ph.D. Thesis Committee
  - 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 Kouven, 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.