THANG HOANG, PhD

Last update: December 19, 2025

Contact Information

Gilbert Place, Room 4304
220 Gilbert Street
Blacksburg, VA, 24060

Email: thanghoang@vt.edu
Phone: (+1) 540-231-0908
Webpage: http://thanghoang.github.io/

Research Interests

Security and Privacy
Applied Cryptography
Biometrics

Education

University of South Florida, Tampa, Florida, United States 2019 – 2020
Doctor of Philosophy, Computer Science
- Dissertation: *Privacy-Preserving and Functional Information Systems*
- Advisor: Dr. Attila Altay Yavuz

Oregon State University, Corvallis, Oregon, United States 2015 – 2018
PhD student, Computer Science
- Advisor: Dr. Attila Altay Yavuz

Phi Kappa Phi Honor Society (OSU Chapter)

Chonnam National University, Gwangju, South Korea 2012 – 2014
Master of Science, Computer Science
- Thesis: *Gait Authentication on Mobile Phone Using Pattern Recognition and Biometric Cryptosystem*
- Advisor: Dr. Deokjai Choi

University of Science VNU-HCMC, Ho Chi Minh city, Vietnam 2006 – 2010
Bachelor of Science, Computer Science
- Thesis: *Integrating Camera Based Supervision System to Access Control Devices and Applications*
- Advisor: Dr. Thuc D. Nguyen

Professional Experiences

Assistant Professor, Department of Computer Science, Virginia Tech, Blacksburg, VA Jan 2021 – current

Postdoctoral Fellow, Computer Science, Carnegie Mellon University, Pittsburgh, PA Aug 2020 – Dec 2020
- Host: Prof. Elaine Shi

Research Associate, CSE, University of South Florida, Tampa, FL Aug 2020 – Dec 2020

Research Intern, Robert Bosch Research & Technology Center, Pittsburgh, PA, USA 2016, 2018

Lecturer, Saigon Technology University, Ho Chi Minh city, Vietnam 2014 – 2015

Research Scientist, RedOne Technologies Co., Ltd., Gwangju, South Korea 2014 – 2015

Grants

Collaborative Research: SaTC: CORE: Medium: Distributed Computing in Effect: Towards Trustworthy, Resilient and Secure NextG Mobile Networks July 2024 – June 2028
PI(s): Attila A. Yavuz (Lead PI, University of South Florida), Mehran Mozaffari Kermani (Co-PI, University of South Florida), Bechir Hamdaoui (PI, Oregon State University), Thang Hoang (PI, Virginia Tech)
Sponsor: National Science Foundation (NSF)
Total: $1,200,000 (*Personal share:* $320,799)

Student Travel Grant for 2024 IEEE Symposium on Security and Privacy July 2024 – June 2025
PI(s): Thang Hoang (Sole PI, Virginia Tech)
Sponsor: Army Research Laboratory (ARL)

Total: $10,000

Travel: NSF Student Travel Grant for 2024 IEEE Symposium on Security and Privacy May 2024 – April 2025
PI(s): Thang Hoang (Sole PI, Virginia Tech)
Sponsor: National Science Foundation (NSF)
Total: $25,000

Privacy-Aware Federated Learning in Heterogeneous IoT July 2023 – June 2024
PI(s): Thang Hoang (Lead PI, Virginia Tech), Tran Phuong (PI, Old Dominion University)
Sponsor: Commonwealth Cyber Initiative Southwest Virginia (CCI SWVA), FY24 Cybersecurity Research
Total: $75,000 (*Personal share:* $45,000)

Trustworthy Services for Autonomous Mission Computing Systems Jun 2023 – May 2024
PI(s): Jin-Hee Cho (Lead PI, Virginia Tech), Bo Ji (Co-PI, Virginia Tech), and Thang Hoang (Co-PI, Virginia Tech)
Sponsor: Commonwealth Cyber Initiative Southwest Virginia (CCI SWVA), Research Engagement Program
Total: $20,000 (*Personal share:* $6,667)

Privacy-Preserving and Trustworthy AI for Smart Transportation Mar 2023 – Jun 2024
PI(s): Thang Hoang (Sole PI, Virginia Tech)
Sponsor: 4-VA, Pre-Tenure Faculty & Collaborative Research Grants
Total: $45,000

New Cryptographic Audit Tools for Effective Data Integrity Attestation in Large-scale Storage-as-a-service Infrastructure July 2022 – Jun 2023
PI(s): Thang Hoang (Sole PI, Virginia Tech)
Sponsor: Commonwealth Cyber Initiative Southwest Virginia (CCI SWVA), Seeding Funding Program
Total: $20,000

Verifiable and Privacy-Preserving Machine Learning as a Service Jun 2022 – Aug 2022
PI(s): Thang Hoang (Sole PI, Virginia Tech)
Sponsor: Commonwealth Cyber Initiative Southwest Virginia (CCI SWVA), Research Engagement Program
Total: $15,000

Towards Privacy-Enhancing Technologies Dec 2020 – current
PI(s): Thang Hoang (Sole PI, Virginia Tech)
Sponsor: Robert Bosch, unrestricted gift
Total: $100,000

ACSAC Student Conferenceship Travel Grant 2016
Total: $1,000

Publications

Underlined indicates my current/former advisees at the time of initial/completion.

Journals

[1] Haodi Wang, Rongfang Bie, and **Thang Hoang**, "An Efficient and Zero-Knowledge Classical Machine Learning Inference Pipeline". *IEEE Transactions on Dependable and Secure Computing* (IEEE TDSC), Volume 22, Issue 2, pp. 1347–1364, 2025.
doi:10.1109/TDSC.2024.3435010

[2] Thao M. Dang, Thuc D. Nguyen, **Thang Hoang**, Hyunseok Kim, Andrew Beng Jin Teoh, and Deokjai Choi, "AVET: A Novel Transform Function to Improve Cancellable Biometrics Security". *IEEE Transactions on Information Forensics and Security* (IEEE TIFS), 2022.
doi:10.1109/TIFS.2022.3230212

[3] Lam Tran, **Thang Hoang**, Thuc Nguyen, Hyunil Kim, and Deokjai Choi, "Multi-Model Long Short-Term Memory Network for Gait Recognition Using Window-Based Data Segment". *IEEE Access*, Volume 9, pp. 23826–23839, February 2021.
doi:10.1109/ACCESS.2021.3056880

[4] **Thang Hoang**, Attila A. Yavuz, and Jorge Guajardo, "A Multi-server ORAM Framework with Constant Client Bandwidth Blowup". *ACM Transactions on Privacy and Security* (ACM TOPS), Volume 23, Issue 1, pp. 1–35, February 2020.
doi:10.1145/3369108

[5] **Thang Hoang**, Attila A. Yavuz, and Jorge Guajardo, "A Secure Searchable Encryption Framework for Privacy-Critical Cloud Storage Services". *IEEE Transactions on Services Computing* (IEEE TSC), Volume 14, Issue 6, pp. 1675–1689, November 2021.
doi:10.1109/TSC.2019.2897096

[6] **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* (IEEE TCC), Volume 9, Issue 2, pp. 598–609, April 2021.
doi:10.1109/TCC.2018.2879104

[7] **Thang Hoang**, Attila A. Yavuz, F. Betül Durak, and Jorge Guajardo, "A Multi-Server Oblivious Dynamic Searchable Encryption Framework". *Journal of Computer Security* (JCS), IOS Press, Volume 27, Issue 6, pp. 649–676, 2019.
doi:10.3233/JCS-191300

[8] **Thang Hoang**, Thuc Nguyen, and Deokjai Choi, "Gait Authentication on Mobile Phone Using Biometric Cryptosystem and Fuzzy Commitment Scheme". *International Journal of Information Security* (IJIS), Volume 14, Issue 6, pp. 549–560, November 2015.
doi:10.1007/s10207-015-0273-1

[9] **Thang Hoang** and Deokjai Choi, "Secure and Privacy Enhanced Gait Authentication on Smart Phone". *The Scientific World Journal* (TSWJ), Volume 2014, May 2014.
doi:10.1155/2014/438254

[10] **Thang Hoang**, Thuc D. Nguyen, Chuyen Luong, Son Do, and Deokjai Choi, "Adaptive Cross-Device Gait Recognition Using Mobile Accelerometer". *Journal of Information Processing System* (JIPS), Volume 9, Issue 2, pp. 333–348, June 2013.
doi:10.3745/JIPS.2013.9.2.333

[11] Viet Q. Vo, **Thang Hoang**, and Deokjai Choi, "Personalization in Mobile Activity Recognition System using K-Medoids Clustering Algorithm". *International Journal of Distributed Sensor Networks* (IJDSN), Volume 2013, June 2013.
doi:10.1155/2013/315841

Conferences

[12] Rouzbeh Behnia, Jeremiah Birrell, Arman Riasi, Reza Ebrahimi, Kaushik Dutta, and **Thang Hoang**, "Trustworthy Federated Learning with Local Differential Privacy", in *35th Workshop on Information Technologies and Systems* (WITS), December 2025, Nashville, TN, USA. ***Best Paper Award***
doi:10.1145/3719027.3765056

[13] Arman Riasi, Haodi Wang, Rouzbeh Behnia, Viet Vo, and **Thang Hoang**, "Zero-Knowledge AI Inference with High Precision", in *32nd ACM Conference on Computer and Communications Security* (CCS), October 2025, Taipei, Taiwan. (*Acceptance rate: 14.5%*)
doi:10.1145/3719027.3765056

[14] Nora Basha, Bechir Hamdaoui, Attila A. Yavuz, **Thang Hoang**, and Mehran Mozaffari Kermani, "Secret-Key Agreement Through Hidden Markov Modeling of Wavelet Scattering Embeddings", in *13th IEEE Conference on Communications and Network Security* (CNS), September 2025, Avignon, France. (*Acceptance rate: 27.9%*)
doi:10.1109/CNS66487.2025.11194987

[15] Hoang-Dung Nguyen, Jorge Guajardo, and **Thang Hoang**, "Client-Efficient Online-Offline Private Information Retrieval", in *25th Privacy Enhancing Technologies Symposium* (PETS), July 2025, Washington DC, USA. (*Acceptance rate: 26%*)
doi:10.56553/popets-2025-0095

[16] Munshi Rejwan Ala Muid, Taejoong Chung, and **Thang Hoang**, "AccuRevoke: Enhancing Certificate Revocation with Distributed Cryptographic Accumulators", in *46th IEEE Symposium on Security and Privacy* (S&P), May 2025, San Francisco, CA, USA. (*Acceptance rate: 14.8%*)
doi:10.1109/SP61157.2025.00129

[17] Tung Le and **Thang Hoang**, "Hermes: Efficient and Secure Multi-Writer Encrypted Database", in *46th IEEE Symposium on Security and Privacy* (S&P), May 2025, San Francisco, CA, USA. (*Acceptance rate: 14.8%*)
doi:https://doi.org/10.1109/SP61157.2025.00184

[18] Arman Riasi, Jorge Guajardo, and **Thang Hoang**, "Privacy-Preserving Verifiable Neural Network Inference Service", in *40th Annual Computer Security Applications Conference* (ACSAC), December 2024, Waikiki, HI, USA. (*Acceptance rate: 19.7%*)
doi:10.1109/ACSAC63791.2024.00063

[19] Rouzbeh Behnia, Arman Riasi, Mohammadreza Ebrahimi, Sherman S. M. Chow, Balaji Padmanabhan, and **Thang Hoang**, "Efficient Secure Aggregation for Privacy-Preserving Federated Machine Learning", in *40th Annual Computer Security Applications Conference* (ACSAC), December 2024, Waikiki, HI, USA. (*Acceptance rate: 19.7%*)

[20] Atharva Haldankar, Arman Riasi, Hoang-Dung Nguyen, Tran Phuong, and **Thang Hoang**, "Breaking Privacy in Model-Heterogeneous Federated Learning", in *27th International Symposium on Research in Attacks, Intrusions and Defenses* (RAID), September 2024, Padua, Italy. (*Acceptance rate: 25%*)
doi:10.1145/3678890.3678905

[21] Tung Le, Rouzbeh Behnia, Jorge Guajardo, and **Thang Hoang**, "MUSES: Efficient Multi-User Searchable Encrypted Database", in *33rd USENIX Security Symposium* (USENIX Security), August 2024, Philadelphia, PA, USA. (*Acceptance rate: 19.1%*)

[22] Pengzhi Huang, **Thang Hoang**, Yueying Li, Elaine Shi, and G. Edward Suh, "Efficient Privacy-Preserving Machine Learning with Lightweight Trusted Hardware", in *24th Privacy Enhancing Technologies Symposium* (PETS), July 2024, Bristol, United Kingdom. (*Acceptance rate: 20.9%*)
doi:10.56553/POPETS-2024-0119

[23] Jacob Haltiwanger and **Thang Hoang**, "Exploiting Update Leakage in Searchable Symmetric Encryption", in *14thACM Conference on Data and Application Security and Privacy* (CODASPY), June 2024, Porto, Portugal. (*Acceptance rate: 21.3%*)
doi:10.1145/3626232.3653260

[24] Trevor Miller, Bobby Alvarez, and **Thang Hoang**, "VTBC: Privatizing the Volume and Timing of Transactions for Blockchain Applications", in *32nd International Conference on Computer Communications and Networks* (ICCCN), July 2023, Honolulu, HI, USA. (*Acceptance rate: 30.3%*)
doi:10.1109/ICCCN58024.2023.10230098

[25] Tung Le and **Thang Hoang**, "MAPLE: A Metadata-Hiding Policy-Controllable Encrypted Search Platform with Minimal Trust", in *23rd Privacy Enhancing Technologies Symposium* (PETS), July 2023, Lausanne, Switzerland. (*Acceptance rate: 23.5%*)
doi:10.56553/POPETS-2023-0105

[26] Haodi Wang and **Thang Hoang**, "ezDPS: An Efficient and Zero-Knowledge Machine Learning Inference Pipeline", in *23rd Privacy Enhancing Technologies Symposium* (PETS), July 2023, Lausanne, Switzerland. (*Acceptance rate: 23.5%*)
doi:10.56553/POPETS-2023-0061

[27] 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. (*Acceptance rate: 15.2%*)
doi:10.14722/NDSS.2023.23307

[28] Mohit Bhasi Thazhath, Jan Michalak, and **Thang Hoang**, "Harpocrates: Privacy-Preserving and Immutable Audit Log for Sensitive Data Operations", in*4th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications* (TPS-ISA), December 2022, Virtual Event.
doi:10.1109/TPS-ISA56441.2022.00036

[29] Hai-Van Dang, Tran Phuong, Thuc Nguyen, and **Thang Hoang**, "ZAC: Efficient Zero-Knowledge Dynamic Universal Accumulator and Application to Zero-Knowledge Elementary Database", in *4th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications* (TPS-ISA), December 2022, Virtual Event.
doi:10.1109/TPS-ISA56441.2022.00038

[30] Attila A Yavuz, Saif Nouma, **Thang Hoang**, Duncan Earl, and Scott Packard, "Distributed Cyber-infrastructures and Artificial Intelligence in Hybrid Post-Quantum Era", in *4th IEEE International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications* (TPS-ISA), December 2022, Virtual Event. (**Invited Paper**) doi:10.1109/TPS-ISA56441.2022.00014

[31] Jiaheng Zhang, Tiancheng Xie, **Thang Hoang**, Elaine Shi, and Yupeng Zhang, "Polynomial Commitment with a One-to-Many Prover and Applications", in *31st USENIX Security Symposium* (USENIX Security), August 2022, Boston, MA, USA. (*Acceptance rate: 18.1%*)

[32] Weikeng Chen, **Thang Hoang**, Jorge Guajardo, and Attila A. Yavuz, "Titanium: A Metadata-Hiding File-Sharing System with Malicious Security", in *the Annual Network and Distributed System Security Symposium* (NDSS), February 2022, San Diego, CA, USA. (*Acceptance rate: 16.2%*) doi:10.14722/NDSS.2022.24161

[33] Efe Ulas Akay Seyitoglu, Attila A. Yavuz, and **Thang Hoang**, "Proof-of-Useful-Randomness: Mitigating the Energy Waste in Blockchain Proof-of-Work", in *18th International Conference on Security and Cryptography* (SECRYPT), July 2021 (virtual). (*Acceptance rate: 18.4%*) doi:10.5220/0010519204120419

[34] **Thang Hoang**, Rouzbeh Behnia, Yeongjin Jang, and Attila A. Yavuz, "MOSE: Practical Multi-User Oblivious Storage via Secure Enclaves", in *10th ACM Conference on Data and Application Security and Privacy* (CODASPY), March 2020, New Orleans, LA, USA. (*Acceptance rate: 19.4%*) doi:10.1145/3374664.3375749

[35] **Thang Hoang**, Jorge Guajardo, and Attila A. Yavuz, "MACAO: A Maliciously-Secure and Client-Efficient Active ORAM Framework", in *the Annual Network and Distributed System Security Symposium* (NDSS), February 2020, San Diego, CA, USA. doi:10.14722/NDSS.2020.24313 (*Acceptance rate: 17.4%*)

[36] **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", in *19th Privacy Enhancing Technologies Symposium* (PETS), July 2019, Stockholm, Sweden. (*Acceptance rate: 22.1%*) doi:10.2478/POPETS-2019-0010

[37] **Thang Hoang**, Attila A. Yavuz, F. Betül Durak, and Jorge Guajardo, "Oblivious Dynamic Searchable Encryption on Distributed Cloud Systems", in *32nd Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy* (DBSec), July 2018, Bergamo, Italy. (*Acceptance rate: 32%*) ***Best Paper Award*** doi:10.1007/978-3-319-95729-6_8

[38] Muslum O. Ozmen, **Thang Hoang**, and Attila A. Yavuz, "Forward-Private Dynamic Searchable Symmetric Encryption with Efficient Search", in *IEEE International Conference on Communications* (ICC), May 2018, Kansas City, MO, USA. (*Acceptance rate: 39.9%*) doi:10.1109/ICC.2018.8422480

[39] Lam Tran, **Thang Hoang**, Thuc Nguyen, and Deokjai Choi, "Improving Gait Cryptosystem Security Using Gray Code Quantization and Linear Discriminant Analysis", in *International Conference on Information Security* (ISC), November 2017, Ho Chi Minh, Vietnam. (*Acceptance rate: 25.7%*) doi:10.1007/978-3-319-69659-1_12

[40] **Thang Hoang**, Ceyhun D. Ozkaptan, Attila A. Yavuz, Jorge Guajardo, and Tam Nguyen, "S^3ORAM: A Computation-Efficient and Constant Client Bandwidth Blowup ORAM with Shamir Secret Sharing", in *24th ACM Conference on Computer and Communications Security* (CCS), October 2017, Dallas, TX, USA. (*Acceptance rate: 17.9%*) doi:10.1145/3133956.3134090

[41] **Thang Hoang**, Attila A. Yavuz, and Jorge Guajardo, "Practical and Secure Dynamic Searchable Encryption via Oblivious Access on Distributed Data Structure", in *32nd Annual Computer Security Applications Conference* (ACSAC), December 2016, Los Angeles, CA, USA. (*Acceptance rate: 22.8%*) doi:10.1145/2991079.2991088

[42] **Thang Hoang**, Deokjai Choi, and Thuc Nguyen, "On the Instability of Sensor Orientation in Gait Verification on Mobile Phone", in *12th International Conference on Security and Cryptography* (SECRYPT), July 2015, Colmar, France. (*Acceptance rate: 10.4%*)
doi:10.5220/0005572001480159

[43] **Thang Hoang** and Deokjai Choi, "A Biometric Cryptosystem Using Gait Captured from Mobile Accelerometer", in *FTRA International Symposium on Ubiquitous Computing and Embedded Systems*, December 2013, Danang, Vietnam. ***Best Paper Award*** (extended version published in [9])

[44] **Thang Hoang**, Deokjai Choi, Viet Vo, Anh Nguyen, and Thuc Nguyen, "A Lightweight Gait Authentication on Mobile Phone Regardless of Installation Error", in *28th International Information Security and Privacy Conference* (IFIP SEC), July 2013, Auckland, New Zealand. (*Acceptance rate: 37.3%*)
doi:10.1007/978-3-642-39218-4_7

[45] Chuyen Luong, Son Do, **Thang Hoang**, and Deokjai Choi, "A Mobility Prediction Algorithm for The Seamless Handoff", in *5th International Conference Ubiquitous and Future Networks* (ICUFN), July 2013, Danang, Vietnam.
doi:10.1109/ICUFN.2013.6614854

[46] Viet Q. Vo, **Thang Hoang**, and Deokjai Choi, "Adaptive Energy-Saving Strategy for Activity Recognition on Mobile Phone", in *IEEE International Symposium on Signal Processing and Information Technology* (ISSPIT), December 2012, Ho Chi Minh city, Vietnam.
doi:10.1109/ISSPIT.2012.6621267

[47] **Thang Hoang**, Viet Q. Vo, Thuc D. Nguyen, and Deokjai Choi, "Gait Identification Using Accelerometer on Mobile Phone", in *1st International Conference on Control, Automation and Information Sciences* (ICCAIS), November 2012, Ho Chi Minh, Vietnam. ***Best Paper Award***
doi:10.1109/ICCAIS.2012.6466615

Patents

[1] Rouzbeh Behnia, Mohammadreza Ebrahimi, **Thang Hoang**, and Balaji Padmanabhan, , "FESA: Fast and Efficient Secure Aggregation for Privacy-Preserving Federated Learning", Application # 63/490814, Filed: Mar 17, 2023.

[2] **Thang Hoang** and Jorge Guajardo, "Secure and Efficient Multi-server Oblivious Random Access Machine in a Malicious Execution Environment", US Patent US20210135850A1, Filed: Nov 06, 2019, Issued: May 06, 2021.

[3] Attila A. Yavuz, Jorge Guajardo, and **Thang Hoang**, "Method and System for Search Pattern Oblivious Dynamic Symmetric Searchable Encryption", US Patent US11144663B2, Filed: Dec 28, 2017, Issued: Oct 21, 2021.

[4] **Thang Hoang**, Muslum O. Ozmen, and Attila A. Yavuz, "Forward-Private Dynamic Searchable Symmetric Encryption with Efficient Search", US Patent US10922273B1, Filed: Oct 10, 2017, Issued: Feb 16, 2021.

[5] Deokjai Choi, **Thang Hoang**, Thuc D. Nguyen, and Thu D. Tran, "Device and Method for Authentication System using Prime Number", Korea Patent 10-1754796, Filed: September 17, 2014, Issued: June 30, 2017.

[6] Deokjai Choi and **Thang Hoang**, "Secure Authentication System, and its Device and Method for Biometric Information, Derived Information from User Characteristic Information", Korea Patent 10-1622253, Filed: July 09, 2014, Issued: May 12, 2016.

[7] **Thang Hoang**, Deokjai Choi, and Chilwoo Lee, "Gait Authentication System and its Device and Method", Korea Patent 10-1622252, Filed: December 11, 2013, Issued: May 12, 2016.

Awards and Honors

- Best Paper Award in WITS 2025, Nashville, TN 2025
- Best Paper Award in IFIP DBSec 2018, Bergamo, Italy 2018
- Best Paper Award in UCES 2013 symposium, Da Nang, Vietnam 2013
- Best Paper Award for the most innovative application in ICCAIS 2012, Ho Chi Minh city, Vietnam 2012

Teaching

I have been teaching the following courses at undergraduate (4XXX) and graduate (5XXX/6XXX) levels at Virginia Tech

- CS 6204: Advanced Topics in Systems — Spring 2025
- CS 5594: Blockchain Technologies — Spring 2021, Spring 2023, Spring 2024
- CS 4104: Data and Algorithm Analysis — Fall 2022, Fall 2023, Fall 2024, Fall 2025
- CS 4274: Secure Computing Capstone — Spring 2022

Mentoring

I am fortunate to work with the following talented students:

Current PhD Students

- Tung Le — Fall 2021 – present
- Arman Riasi — Fall 2022 – present
- Hoang-Dung Nguyen — Spring 2023 – present
- Changqi Sun — Fall 2023 – present
- Munshi Ala Muid (co-advise w/ Prof. Tijay Chung) — Fall 2023 – present

Visiting Students

- Haodi Wang, PhD student, Beijing Normal University — Jan 2021 – Dec 2023

Graduated

- Atharva Haldankar, MS — Spring 2024
  - *Thesis*: Breaking Privacy in Model-Heterogeneous Federated Learning
  - *First Job*: Software Engineer at Capital One
- Jacob Haltiwanger, MS — Spring 2024
  - *Thesis*: Exploiting Update Leakage in Searchable Symmetric Encryption
  - *First Job*: Federal (Nondisclosure position)
- Trevor Miller, MS — Spring 2023
  - *Thesis*: Privatizing the Volume and Timing of Transactions for Blockchain Applications
- Mohit Bhasi, MS — Spring 2022
  - *Thesis*: Privacy-Preserving and Immutable Audit Log for Sensitive Data Operations
  - *First Job*: Software Engineer at Robinhood

Current and Past Undergraduate Students

- Jan Michalak
- Bobby Alvarez
- Atharva Haldankar

Professional Services

Proposal Panelist

- 2025 NSF Review Panelist (3 panels)
- 2024 NSF Review Panelist (2 panels)

Organizing Committee

- IEEE S&P, Student Travel Grants Chair (2024)
- IEEE S&P, Short Talks Chair (2022, 2023)
- Vietnam Conference on Blockchain Computing (CBC), Program Chair (2022)

Program Committee

- ACM CCS (2026), ACISP (2026), IEEE S&P (2026), ACSAC (2021-2025), SafeThings, IEEE/ACM Workshop (2025), IEEE MASS (2022-2023, 2025), PETS (2023-2025), VRICS (2024, 2025), Inscrypt (2023), WWW (2022), IEEE ICCCN (2021), CosDEO (PerCom Workshop) (2018, 2020)

Journal Reviewer

- IEEE Transactions on Dependable and Secure Computing (2017-2025), IEEE Transactions on Cloud Computing (2019, 2021, 2023, 2025), IEEE Transactions on Information Forensics and Security (2018-2023, 2025), Elsevier Computers & Security (2020, 2025), ACM Transactions on Privacy and Security (2017, 2020, 2022, 2024), IEEE Transactions

on Services Computing (2022), ACM Digital Threats: Research and Practice (2020, 2021), IEEE Transactions on Cybernetics (2019), Elsevier Information Sciences (2017), Elsevier Journal of Information Security and Applications (2019)

Conference Reviewer

- ACM CCS (2021), IEEE S&P (2021), PETS (2020-2022), ACSAC (2017-2019), ASIACRYPT (2018), EUROCRYPT (2018), IEEE CSF (2021), IEEE CNS (2019), IFIP DBSec (2018, 2019), WiSec (2020), WWW (2019)

Graduate Thesis Committee

- Atul Bharadwaj, MS, Computer Science, Virginia Tech (Defended Spring 2025)
- Akash Mittal, MS, Computer Science, Virginia Tech (Defended Fall 2024)
- Fatemeh Sharifi, Ph.D, Electrical and Computer Engineering, (Preliminary Exam, Fall 2024)
- Benjamin Asad Akhtar, MS, Electrical and Computer Engineering, Virginia Tech (Defended Summer 2024)
- Akhilesh Marathe, MS, Electrical and Computer Engineering, Virginia Tech (Defended Spring 2024)
- Rishi Ranjan, MS, Computer Science, Virginia Tech (Defended Spring 2024)
- Ashrith Reddy Thukkaraju, MS,Computer Science, Virginia Tech (Defended Fall 2023)
- Protick Bhowmick, MS, Computer Science, Virginia Tech (Defended Fall 2023)
- Leo Stone, MS, Computer Science, Virginia Tech (Defended Spring 2023)

Other Services

- PhD Qualifier Exam Chair, Department of Computer Science, Virginia Tech 2024
- PhD Qualifier Exam Committee, Department of Computer Science, Virginia Tech 2023
- Graduate Admission Committee, Department of Computer Science, Virginia Tech 2021 – 2023

Talks

Towards Robust and Privacy-Preserving Federated Machine Learning

- Invited talk at Math Colloquium Series, University of Louisiana at Lafayette Remote, Oct 2025

Zero-Knowledge AI Inference with High Precision

- Invited talk at Bosch RTC in Pittsburgh Remote, Oct 2025
- Presented at ACM CCS 2025 Taipei, Taiwan, Oct 2025

Privacy-Preserving and Trustworthy AI: from Theory to Practice

- Invited lecture at FIT@HCMUS Summer School on Generative AI and Multi-Agent System Saigon, VN, Aug 2025

Zero-Knowledge Machine Learning Inference Pipeline

- Invited keynote talk at 4th ICDM Workshop on Machine Learning for Cybersecurity (MLC) 2024 Remote, Dec 2024
- Invited keynote talk at BK FinTech Conference 2024 Remote, Jun 2024

Privacy-Preserving and Trustworthy Storage-as-a-service

- Invited talk at Bosch RTC Pittsburgh, PA, May 2024
- Invited talk at Secure and Data Technology Workshop Blacksburg, VA, Apr 2024

Towards Practical Dynamic Proof of Retrievability

- Invited talk at SIAM Southeastern Atlantic Section Annual Meeting Blacksburg, VA, Mar 2023

Harpocrates: Privacy-Preserving and Immutable Audit Log for Sensitive Data Operations

- Presented at Vietnam Conference on Blockchain Computing (CBC) Remote, Dec 2022

Privacy-Preserving Collaborative Information Processing

- Research Seminar at Robert Bosch RTC Remote, Feb 2022

Privacy-Preserving and Functional Information Systems

- Research Seminar at Robert Bosch RTC Remote, Jan 2021
- Seminar at Binghamton University Binghamton, NY, Mar 2020
- Seminar at Virginia Tech Remote, Mar 2020
- Seminar at University of Iowa Remote, Apr 2020
- Seminar at University of South Florida Tampa, FL, Apr 2020

MACAO: A Maliciously-Secure and Client-Efficient Active ORAM Framework

- Presented at ISOC NDSS 2020 San Diego, CA, USA, Feb 2020

Distributed ORAM for Data Outsourcing

- Seminar at Cornell University — Ithaca, NY, USA, Nov 2019

S^3ORAM: A Computation-Efficient and Constant Client Bandwidth Blowup ORAM with Shamir Secret Sharing

- Presented at ACM CCS 2017 — Dallas, TX, USA, Oct 2017

Practical and Secure Dynamic Searchable Encryption via Oblivious Access on Distributed Data Structure

- Presented at ACSAC 2016 — Los Angeles, CA, USA, Dec 2016

Wireless Network Security

- Seminar at Eduroam Workshop, University of Indonesia — Depok, Indonesia, Aug 2015

On the Instability of Sensor Orientation in Gait Verification on Mobile Phone

- Presented at SECRYPT 2015 — Colmar, France, Jul 2015

A Lightweight Gait Authentication on Mobile Phone Regardless of Installation Error

- Presented at IFIP SEC 2013 — Auckland, New Zealand, Jul 2013

Gait Identification Using Accelerometer on Mobile Phone

- Presented at IEEE ICCAIS 2012 — Ho Chi Minh city, Vietnam, Nov 2012