Andreas Veneris

Curriculum Vitæ

Edward S. Rogers Sr.
Department of Electrical
and Computer Engineering
University of Toronto
10 King's College Road
Toronto, Ontario, M5S 3G4, Canada
Canada M5S 3G4
tel: (416) 946-3062
veneris@eecg.toronto.edu

120 Homewood Ave., #614
Toronto, Ontario
Canada M4Y 2J3
(416) 801-8407

Research Interests

Game-theoretical incentives for crypto-economics; Mechanism/system & cybersecurity for distributed ledge (blockchain) systems; Formal methods and CAD; Central Bank Digital Currencies; Techno-legal questions for blockchain/payment systems and AML/CFT; Data analytics for fintech

Academic History

2011–today	Connaught Scholar and Professor, Edward S. Rogers Sr. Department of Electrical and Computer Engineering, Department of Computer Science, and Munk School of Global Affairs & Public Policy at the University of Toronto.
1999–2011	Associate and Assistant Professor, Edward S. Rogers Sr. Department of Electrical and Computer Engineering and Department of Computer Science, University of Toronto

Past and Other Appointments:

2017–today	Alumni of Japanese Society for the Promotion of Science
2006–2016	Visiting Professor, Athens University of Economics and Business, Department of Informatics
2010–2011	Visiting Professor, University of Tokyo, Department of Electrical and Computer Engineering, as Fellow of the Japanese Society for the Promotion of Science (JSPS)
1998–1999	Visiting Assistant Professor, Department of Computer Science, University of Illinois, Urbana-Champaign

Education

1993–1998	University of Illinois, Urbana–Champaign Ph.D. in Computer Science, October 1998
1991–1992	University of Southern California, Los Angeles M.Sc. in Computer Science, December 1992
1986–1991	University of Patras, Department of Computer Engineering and Informatics Diploma in Computer Science and Engineering, July 1991

Professional Affiliations

AAAS (1998), *ACM* (1998), *AMS* (2012), *IEEE* (1997), *Japanese Society for the Promotion of Science* (2010), *Professionals Engineers of Ontario* (2008), *Technical Chamber of Greece* (1991), and the *Planetary Society* (1997).

Activities and Awards

Research:

- *Hoover Institution & Stanford University (2021-22):* Acknowledged for contributions to the classified report by the Hoover Institution, edited by Darrell Duffie and Elizabeth Economy, prefaced by former US Secretary of the State Condoleezza Rice, and co-authored by an extensive list of prominent world-thinkers. This embargoed report was eventually released on March 1, 2022 titled "Digital Currencies: The US, China, And The World At A Crossroads." A week later, on March 8, 2022, US President Joe Biden signed an Executive Order implementing key recommendations of this report.
- *Bank of Canada, Model X Competition (2020-21)* for work to provide a technical, economic and regulatory design for Canada's digital currency, also coined as the "digital loonie," a term that it is widely used today in mainstram media
- *Connaught Global Challenge Award* for work in distributed ledger technology (2018)
- *IBM Faculty Award* for work in verification and distributed ledger rechnology (2018)
- *10 Year Retrospective Most Influential Paper* Award by IEEE/ACM Asian-South Pacific Design Automation Conference 2014
- *Best Paper Awards*: ACM/IEEE International Conference on Software Engineering 2024 (ACM SIGSOFT flagship Distinguished Paper Award), IEEE International Conference on Blockchain and Cryptocurrency 2024 & 2022, IEEE International Workshop on Cryptocurrency and Exchanges 2023, IEEE Conference on Blockchain Research & Applications for Innovative Networks and Services 2020, and IEEE/ACM Asian-South Pacific Design Automation Conference, 2001
- Nominated for the Bower Award and Prize in Science (Franklin Institute, 2013) by Turing Award recipient Prof. Stephen Cook
- Contributions to white papers by the International Monetary Fund, the Bank of International Settlements, Bank of Canada and Hong Kong Monetary Authority, among others

University of Toronto:

- Fields Institute of Mathematics (2017–present): Blockchain Research Series. Founder of research seminar series to promote GTA research in blockchain fintech. Funded by Fields, NSERC and private sector.
- Blockchain@UofT (2016–present): inter-departmental meetup drawing more than 250 people
- Student-evaluated teaching honors (2001, 2002, 2004, 2008).
- Coordinator for ECE's *Distinguished Lecture Series* (2002–2004). Search committee for new Chair at *Mechanical and Industrial Engineering* at University of Toronto (2002–2003). Member of *Computer Engineering Group* and *Electronics Group* ECE's Curriculum update committee at University of Toronto (2001). University of Toronto undergraduate scholarship program committee (2004–2007).

Entrepreneurial:

- IIAC (2023–present): Advisory Board Member for the Investment Industry Association of Canada.
- Vennsa Technologies (2006–present): Founder/CEO/President. Commercializing research from the University of Toronto. Raised Series A funding from private and government sources with customers from Tier 1 global semiconductor industry.
- OnRamp, New York (1994-1998): Technical consultant and fields journalist, internet multimedia services. Member of the team that performed the first audio/video Internet broadcasting ever (37th Annual Grammy Awards, 1995), as also acknowledged by the American Congress. OnRamp went public (NASDAQ) in 1996 as Think New Ideas.

Publications

Refereed Journal Papers (published or accepted)

[1] P. Michalopoulos, O. Olowookere, N. Pocher, J. Sedlmeir, A. Veneris, and P. Puri, "Privacy and Compliance Design Options in Offline Central Bank Digital Currencies," in IEEE Transactions on Network and Service Management 2025.

[2] J. Chen, J. Hull, Z. Poulos, H. Rasul, A. Veneris, and Y. Wu, "Variational Autoencoder Approach to Conditional Generation of Possible Future Volatility Surfaces," in The Journal of Financial Data Science(JFDS), July 2025.

[3] S. F. Singh, V. Nekriach, P. Michalopoulos, A. Veneris and J. Klinck, "Options Contracts in the DeFi Ecosystem: Opportunities, Solutions, & Technical Challenges" in ACM International Journal on Network Management (Wiley), 2025.

[4] S. F. Singh, P. Michalopoulos, and A. Veneris, "DEEPER: A shared liquidity decentralized exchange design for low trading volume tokens to enhance average liquidity," in ACM International Journal on Network Management (Wiley), 2024.

[5] J. A. Choi, S. M. Beillahi, S. F. Singh, P. Michalopoulos, P. Li, A. Veneris, and F. Long, "LMPT: A Novel Authenticated Data Structure to Eliminate Storage Bottlenecks for High Performance Blockchains," in IEEE Transactions on Network and Service Management, 2023.

[6] K. Nelaturu, A. Mavridou, E. Stachitari, A. Veneris, and A. Laszka, "Correct-by-design interacting smart contracts and a systematic approach for verifying ERC20 and ERC721 contracts with VeriSolid," in IEEE Transactions on Dependable and Secure Computing, 2022.

[7] J. Meijers, P. Michalopoulos, S. Motepalli, G. Zhang, S. Zhang, A. Veneris, and H. A. Jacobsen, "Blockchain for V2X: Applications and Architectures," in IEEE Open Journal of Vehicular Technology, 2022.

[8] S. K. Kanhere, A. Veneris, S. Yoshihama, S. Chakraborty, O. Rottenstreich, M. B. Pardo, and B. Rodriguez, "Guest Editorial: Special Issue on Recent Advances on Blockchain for Network and Service Management," in IEEE Transactions on Network and Service Management, 2022.

[9] N. Pocher and A. Veneris, "Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme," in IEEE Transactions on Network and Service Management, 2022.

[10] Z. Zhao, S. M. Beillahi, R. Song, Y. Cai, A. Veneris, and F. Long, "SigVM: enabling event-driven execution for truly decentralized smart contracts," in Proceedings of the ACM on Programming Languages, 2022.

[11] M. Bergeron, N. Fung, J. Hull, Z. Poulos and A. Veneris, "Variational Autoencoders: A Hands-Off Approach to Volatility," in Journal of Financial Data Science (JFDS), 2022.

[12] N. Pocher and A. Veneris, "Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme," in IEEE Transactions on Network and Service Management, 2021 (invited paper)

[13] Y. Cai, N. Irtija, E.E. Tsiropoulou and A. Veneris, "Truthful Decentralized Blockchain Oracles," in International Journal of Network Management (Wiley), 2021

[14] K. Nelaturu, J. Adler, M. Merlini, R. Berryhill, N. Veira, Z. Poulos and A. Veneris, "On Public Crowdsource-based Mechanisms for a Decentralized Blockchain Oracle," in IEEE Trans. on Technology and Engineering Management, 2020

[15] N. Veira, Z. Poulos and A. Veneris, "Searching for Bugs using Probabilistic Suspect Implications," in IEEE Trans. in Computer-Aided Design, 2020

[16] Z. Poulos and A. Veneris, "Failure Triage in RTL Regression Verification," in IEEE Trans. in Computer-Aided Design, Sep. 2018

[17] R. Berryhill and A. Veneris, "Efficient Suspect Selection in Unreachable State Diagnosis," in Annals of Mathematics and Artificial Intelligence, Springer, Nov. 2018

[18] R. Berryhill and A. Veneris, "Methodologies for Diagnosis of Unreachable States via Property Directed Reachability," *IEEE Trans. on Computer-Aided Design*, vol. 37, no. 6, pp. 1298–1311, June 2018

[19] R. Berryhill and A. Veneris, "Efficient Suspect Selection in Unreachable State Diagnosis," *Annals of Mathematics and Artificial Intelligence*, vol. 82, no. 4, pp. 261–277, April 2018

[20] Z. Poulos and A. Veneris, "Failure Triage in RTL Regression Verification," *IEEE Trans. on Computer-Aided Design*, accepted December 2017

[21] J. Adler and A. Veneris, "Leveraging Software Configuration Management in Automated RTL Design Debug," *IEEE Trans. on Computer-Aided Design*, vol. 34, no. 5, pp. 47–53, October 2017

[22] Z. Poulos and A. Veneris, "Exemplar-based Failure Triage for Regression Design Debugging," *Journal of Electronic Testing, Theory and Applications (JETTA)*, vol. 32, no. 2, pp. 125–136, April 2016

[23] H. Mangassarian, B. Le, and A. Veneris, "Debugging RTL using Structural Dominance," in *IEEE Trans. on Computer-Aided Design*, vol. 33, no. 1, pp. 153–166, Jan. 2014

[24] B. Keng and A. Veneris, "Path Directed Abstraction and Refinement for SAT-Based Design Debugging," *IEEE Trans. on Computer-Aided Design*, vol. 32, no. 10, pp. 1609–1622, Oct. 2013

[25] H. Mangassarian, A. Veneris, and F. N. Najm, "Maximum Circuit Activity Estimation Using Pseudo-Boolean Satisfiability," *IEEE Trans. on Computer-Aided Design*, vol. 31, no. 2, pp. 271–284, Feb. 2012

[26] Y. S. Yang, A. Veneris and N. Nicolici, "Automating Data Analysis and Acquisition Setup in a Silicon Debug Environment," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, vol. 20, no. 6, pp. 1118–1131, June 2012

[27] E. Safi, A. Moshovos, and A. Veneris, "Two-stage Pipelined Register Renaming," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, vol. 19, no. 10, pp. 1926–1931, Oct 2011

[28] Y. S. Yang, S. Sinha, A. Veneris, and R. Brayton, "Automating Re-synthesis with Approximate SPFDs," *IEEE Trans. on Computer-Aided Design*, vol. 30, no. 5, pp. 651–664, May 2011

[29] B. Keng, S. Safarpour, and A. Veneris, "Bounded Model Debugging," *IEEE Trans. on Computer-Aided Design*, vol. 29, no. 11, pp. 1790–1803, Nov 2010

[30] H. Mangassarian, A. Veneris, and M. Benedetti, "Robust QBF Encodings for Sequential Circuits with Applications to Verification, Debug and Test," *IEEE Trans. on Computers*, vol. 25, no. 7, pp. 981–994, July 2010

[31] Y. Chen, S. Safarpour, J. M. Silva, and A. Veneris, "Automated Design Debugging with Maximum Satisfiability," *IEEE Trans. on Computer-Aided Design*, vol. 29, no. 11, pp. 1804–1817, Nov 2010

[32] E. Safi, A. Moshovos, and A. Veneris, "On the Latency and Energy of Checkpointed, Superscalar Register Alias Tables," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, vol. 18, no. 3, pp. 379–382, Mar 2010

[33] S. Safarpour and A. Veneris, "Automated Design Debugging with Abstraction and Refinement," *IEEE Trans. on Computer-Aided Design*, vol. 28, no. 10, pp. 1597–1608, Oct 2009

[34] S. Safarpour, A. Veneris, and R. Drechsler, "Improved SAT-based Reachability Analysis with Observability Don't Cares," *Journal on Satisfiability (JSAT)*, vol. 5, pp. 1–25, 2008

[35] E. Safi, A. Moshovos, and A. Veneris, "L-CBF: A Low-Power Fast Counting Bloom Filter Architecture," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, vol.16, no. 6, pp. 628–638, May 2007

[36] Y. S. Yang, A. Veneris, P. Thadikaran, and S. Venkataraman, "Extraction Error Modeling and Debugging in High-Performance Custom-Made Designs," in *IEEE Trans. on Computer-Aided Design*, vol. 14, no. 7, pp. 763–776, July 2006

[37] A. Smith, A. Veneris, M. Fahim Ali, and A. Viglas, "Design Diagnosis using Boolean Satisfiability," *IEEE Trans. on Computer-Aided Design*, vol. 24, no. 10, pp. 1606–1622, Oct 2005

[38] B. J. Liu, and A. Veneris, "Incremental Diagnosis of Multiple Faults and Errors," *IEEE Trans. on Computer-Aided Design*, vol. 24, no. 2, pp. 240–251, Feb 2005

[39] A. Veneris and B. J. Liu, "Incremental Logic Debugging," *Kluwer Journal of Electronic Testing: Theory and Applications*, vol. 21, no. 5, pp. 485–494, Oct 2005

[40] A. Veneris, "Logic Rewiring for Delay and Power Minimization," *Journal of Information Science and Engineering*, vol. 20, no. 6, pp. 1231–1238, Nov 2004

[41] A. Veneris, R. Chang, M. S. Abadir, and S. Seyedi, "Functional Fault Equivalence and Diagnostic Test Generation in Combinational Logic Circuits Using Conventional ATPG," *Kluwer Journal of Electronic Testing: Theory and Applications*, vol. 21, no. 5, pp. 495–502, Oct 2005

[42] A. Veneris and M. S. Abadir "Design Rewiring Using ATPG," *IEEE Trans. on Computer-Aided Design*, vol. 21, no. 12, pp. 1469–1479, Dec 2002

[43] A. Veneris and I. N. Hajj, "Design Error Diagnosis and Correction Via Test Vector Simulation," in *IEEE Trans. on Computer-Aided Design*, vol. 18, no. 12, pp. 1803–1816, Dec 1999

[44] L. M. Kirousis and A. Veneris, "Efficient Algorithms for Checking the Atomicity of a Run of Read and Write Operations," in *Acta Informatica (Springer-Verlag)*, vol. 32, pp. 155–170, 1995

Refereed Conference Papers (published or accepted)

[1] V. Nekriach, S. Beillahi, A.Veneris and F. Long, "HEMVM: a Heterogeneous Blockchain Framework for Interoperable Virtual Machines", to ACM Object-Oriented Programming, Systems, Languages & Applications (OOPSLA), 2025

[2] S. F. Singh, P. Michalopoulos and A. Veneris, "Option Contracts in the DeFi Ecosystem: Motivation, Solutions, & Technical Challenges," in IEEE 2nd Workshop on Cryptocurrency and Exchanges (CRYPTOEX'24), 2024 **(recipient of Best Paper Award)**.

[3] R. K. X. Li, S. F. Singh, A. Park, and A. Veneris, "On Tokenizing Securities in Contemporary Decentralized Finance Ecosystems," in IEEE Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2024 **(Best Paper Finalist)**.

[4] X. Deng, S. M. Beillahi, H. Du, C. Minwalla, A. Veneris, and F. Long, "Analysis of DeFi Oracles," in Bank of Canada Staff Discussion Paper, 2024.

[5] X. Deng, S. M. Beillahi, H. Du, C. Minwalla, A. Veneris, and F. Long, "Safeguarding DeFi Smart Contracts against Oracle Deviations," in ACM/IEEE Proceedings of the 46th International Conference on Software Engineering (ICSE), 2024. **(ACM SIGSOFT Distinguished Paper Award)**

[6] P. Michalopoulos, O. Olowookere, N. Pocher, J. Sedlmeir, A. Veneris, and P. Puri, "Compliance Design Options for Offline CBDCs: Balancing Privacy and AML/CFT," in IEEE International Conference on Blockchain and Cryptocurrency 2024, 2024. **(recipient of Best Paper Award)**

[7] S. F. Singh, P. Michalopoulos, and A. Veneris, "BAKUP: Automated, Flexible, and Capital-Efficient Insurance Protocol for Decentralized Finance," in IEEE International Conference on Blockchain and Cryptocurrency 2024, 2024.

[8] K. Nelaturu, E. Kelity, and A. Veneris, "Natural Language-based Model-Checking Framework for Move Smart Contracts," in the 10th IEEE Conference on Software Defined Systems (SDS), 2023.

[9] J. Chen, J. Hull, Z. Poulos, H. Rasul, A. Veneris, and Y. Wu, "A Variational Autoencoder Approach to Conditional Generation of Possible Future Volatility Surfaces," in SSRN, 2023.

[10] E. Kelity, K. Nelaturu, A. Kastania, and A. Veneris, "Gas Optimization Patterns in Move Smart Contracts on the Aptos Blockchain," in IEEE Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2023.

[11] S. F. Singh, P. Michalopoulos, S. M. Beillahi, A. Veneris, and F. Long, "Mobius: an Atomic State Sharding Design for Account-Based Blockchains," in IEEE International Conference on Blockchain and Cryptocurrency 2023, 2023.

[12] X. Deng, X. Zhao, S. M. Beillahi, H. Du, C. Minwalla, K. Nelaturu, A. Veneris, and F. Long, "A Robust Front-Running Methodology for Malicious Flash-Loan DeFi Attacks," in IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), 2023.

[13] P. Michalopoulos, S. F. Singh, and A. Veneris, "Inducing Trust in Blockchain-enabled IoT Marketplaces Through Reputation and Dispute Resolution," in IEEE International Conference on Metaverse Computing, Networking and Applications (METACOM), 2023.

[14] S. F. Singh, P. Michalopoulos, and A. Veneris, "DEEPER: Enhancing Liquidity in Concentrated Liquidity AMM DEX via Sharing," in 1st IEEE International Workshop on Cryptocurrency and Exchanges (CRYPTOEX), 2023 **(recipient of Best Paper Award)**.

[15] P. Michalopoulos, J. Meijers, S. F. Singh, and A. Veneris, "A V2X Reputation System with Privacy Considerations," in 2022 IEEE 13th International Conference on Software Engineering and Service Science (ICSESS), 2022.

[16] S. M. Beillahi, E. Kelity, K. Nelaturu, A. Veneris, and F. Long, "Automated Auditing of Price Gouging TOD Vulnerabilities in Smart Contracts," in 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2022.

[17] E. Kelity, K. Nelaturu, B. Wu, and A. Veneris, "A Model-Checking Framework for the Verification of Move Smart Contracts," in 2022 IEEE 13th International Conference on Software Engineering and Service Science (ICSESS), 2022.

[18] E. Kelity, K. Nelaturu, B. Wu, and A. Veneris, "WIP: A Model-Checking Framework for the Verification of Move Smart Contracts," in Crypto Economics Security Conference (CESC), 2022.

[19] J.A. Choi, S.M. Beillahi, P. Li, A. Veneris and F. Long, "LMPTs: Eliminating Storage Bottlenecks for Processing Blockchain Transactions," in IEEE Int'l Conference on Blockchain and Cryptocurrency (ICBC), 2022 **(recipient of Best Paper Award)**.

[20] S.M. Beillahi, E. Keilty, K. Nelaturu, A. Veneris and F. Long, "Automated Auditing of Price Gouging TOD Vulnerabilities in Smart Contracts," in IEEE Int'l Conference on Blockchain and Cryptocurrency (ICBC), 2022

[21] K. Nelaturu, S.M. Beillahi, F. Long and A. Veneris, "Smart Contracts Refinement for Gas Optimization," in IEEE Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS), 2021

[22] J. Meijers, E. Au, Y. Cai, H-A. Jacobsen, S. Motepalli, R. Sun, A. Veneris, G. Zhang and S. Zhang, "Blockchain for V2X: A Taxonomy of Design Use Cases and System Requirements," in IEEE Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS), 2021

[23] N. Pocher, and A. Veneris, "Privacy and Transparency in CBDCs: A Regulation-by-Design AML/CFT Scheme," in IEEE Int'l Conference on Blockchain and Cryptocurrency (ICBC), 2021

[24] J. Meijers, G.D. Putra, G. Kotsialou, S. Kanhere, and A. Veneris "Cost-Effective Blockchain-based IoT Data Marketplaces with a Credit Invariant," in IEEE Int'l Conference on Blockchain and Cryptocurrency (ICBC), 2021

[25] Y. Cai, G. Fragkos, E. E. Tsiropoulou, and A. Veneris, "A Truth-Inducing Sybil Resistant Decentralized Blockchain Oracle," in IEEE Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS), 2020 **(recipient of Best Paper Award)**.

[26] Y. Cai, F. Long, A. Park and A. Veneris, "Engineering Ecoomics in the Conflux Network," in IEEE Conference on Blockchain Research and Applications for Innovative Networks and Services (BRAINS), 2020

[27] K. Nelaturu, A. Mavridou, A. Veneris and A. Laszka, "Verified Development and Deployment of Multiple Interacting Smart Contracts with VeriSolid," in IEEE Int'l Conference on Blockchain and Cryptocurrency (ICBC), 2020

[28] R. Berryhill, and A. Veneris, "Chasing Minimal Inductive Validity Cores in Hardware Model Checking," in Formal Methods in CAD (FMCAD), 2019

[29] N. Veira, B. Keng, K. Padmanabhan and A. Veneris, "Unsupervised Emdedding Enhancements of Knowledge Graphs using Textual Associations," in International Joint Conference on Artificial Intelligence, 2019

[30] R. Berryhill and A.Veneris, "Finding Minimal Inductive Validity Cores of Circuits," in Formal Methods in CAD (FMCAD), 2019

[31] M. Merlini, N. Veira, R. Berryhill and A. Veneris, "On Public Decentralized Ledger Oracles via a Paired-Question Protocol," in IEEE Int'l Conference on Blockchain and Cryptocurrency (ICBC), 2019

[32] N. Veira, B. Keng, and A. Veneris, "Unsupervised Embedding Enhancements of Knowledge Graphs using Textual Associations", in International Joint Conference on Artificial Intelligence", 2019

[33] N. Veira, Z. Poulos and A. Veneris, "Suspect2vec: A Suspect Prediction Model for Directed RTL Debugging," in IEEE/ACM Asian-South Pacific Design Automation Conference (ASP-DAC), 2019

[34] J. Adler, R. Berryhill, and A. Veneris, Z. Poulos, N. Veira, and A. Kastania "Astraea: A Decentralized Blockchain Oracle," in *IEEE Int'l Conference on Blockchain*, 2018

[35] N. Veira, Z. Poulos, and A. Veneris, "Suspect Set Prediction in RTL Bug Hunting," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2018

[36] R. Berryhill, A. Ivrii, N. Veira, and A. Veneris, "Learning Support Sets in IC3 and Quip: The Good, the Bad, and the Ugly," in *Formal Methods in CAD (FMCAD)*, 2017

[37] R. Berryhill, N. Veira, A. Veneris, and Z. Poulos, "Learning Lemma Support Graphs in Quip and IC3," in *IEEE Int'l Workshop on Verification and Security*, 2017

[38] J. Adler, R. Berryhill, and A. Veneris, "An Extensible Perceptron Framework for Revision RTL Debug Automation," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2017

[39] Z. Poulos, R. Berryhill, J. Adler, and A. Veneris, "On Simulation-based Metrics that Characterize Behavior of RTL Errors," in *Summer Simulation Multi Conference*, 2016

[40] J. Adler, R. Berryhill, and A. Veneris, "Revision Debug with Non-Linear Version History in Regression Verification," in *IEEE Int'l Workshop on Verification and Security*, 2016

[41] R. Berryhill and A. Veneris, "Efficient Selection of Suspect Sets in Unreachable State Diagnosis," in *Int'l Symposium on Artificial Intelligence and Mathematics (ISAIM)*, 2016

[42] J. Adler, D. Maksimovic, and A. Veneris, "Root-Cause Analysis for Memory-Locked Errors," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2016

[43] R. Berryhill and A. Veneris, "A Complete Approach to Unreachable State Diagnosability via Property Directed Reachability," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2016

[44] L. V. Nguyen, D. Maksimovic, T. T. Johnson, and A. Veneris, "Quantified Bounded Model Checking for Rectangular Hybrid Automata," in *IEEE Constraints in Formal Verification (CFV) Workshop*, 2015

[45] R. Berryhill and A. Veneris, "Diagnosing Unreachable States Using Property Directed Reachability," in *IEEE Constraints in Formal Verification (CFV) Workshop*, 2015

[46] D. Maksimovic, A. Veneris, and Z. Poulos, "Clustering-based Revision Debug in Regression Verification," in *IEEE Int'l Conference on Computer Design (ICCD)*, 2015

[47] Z. Poulos and A. Veneris, "Mining Simulation Metrics for Failure Triage in Regression Testing," in *IEEE Int'l On-Line Test Symposium (IOLTS)*, 2015

[48] B. Le, D. Maksimovic, D. Sengupta, E. Ergin, R. Berryhill, and A. Veneris, "Constructing Stability-based Clock Gating with Hierarchical Clustering," in *IEEE Int'l Workshop on Power and Timing Modeling, Optimization and Simulation*, 2015

[49] Z. Poulos and A. Veneris, "Exemplar-based Failure Triage for Regression Design Debugging," in *IEEE Latin-American Test Symposium (LATS)*, 2015

[50] R. Berryhill and A. Veneris, "Automated Rectification Methodologies to Functional State-Space Unreachability," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2015

[51] D. Maksimovic, B. Le, and A. Veneris, "Multiple Clock Domain Synchronization in a QBF-based Verification Environment," in *IEEE/ACM Int'l Conference on Computer-Aided Design (ICCAD)*, 2014

[52] Z. Poulos and A. Veneris, "Clustering-based Failure Triage for RTL Regression Debugging," in *IEEE Int'l Test Conference (ITC)*, 2014

[53] Z. Poulos, Y.-S. Yang, A. Veneris, and B. Le, "Simulation and atisfiability Guided Counter-example Triage for RTL Design Debugging," in *IEEE Int'l Symposium on Quality of Electronic Design (ISQED)*, 2014

[54] B. Keng, E. Qin, A. Veneris, and B. Le, "Automated Debugging of Missing Assumptions," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2014

[55] D. Sengupta, E. Elgin, and A. Veneris, "Early Detection of Current HotSpots in Power Gated Designs," in *IEEE Int'l Symposium on Low Power Electronic Devices (ISLPED)*, 2013

[56] B. Le, D. Sengupta, and A. Veneris, "Reviving Erroneous Stability-based Clock Gating using Partial Max-SAT,", in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2013

[57] Z. Poulos, Y.S.Yang, and A. Veneris, "A Failure Triage Engine Based On Error Trace Signature Extraction," in *IEEE Int'l On-Line Test Symposium (IOLTS)*, 2013

[58] B. Le, D. Sengupta, A. Veneris, and Z. Poulos, "Accelerating Post Silicon Debug of Deep Electrical Faults," in *IEEE Int'l On-Line Test Symposium (IOLTS)*, 2013

[59] B. Keng and A. Veneris, "Automated Debugging of Missing Input Constraints in a Formal Verification Environment," in *Formal Methods in CAD (FMCAD)*, pp. 101–105, 2012

[60] B. Keng and A. Veneris, "Path Directed Abstraction and Refinement in SAT-based Design Debugging," in *IEEE/ACM Design Automation Conference (DAC)*, 2012

[61] D. Sengupta, F. M. de Paula, A. Hu, A. Ivanov, and A. Veneris, "Lazy Suspect-Set Computation: Fault Diagnosis for Deep Electrical Bugs," in *IEEE Great Lakes VSLI Symposium (GLVLSI)*, 2012

[62] B. Le, H. Mangassarian, B. Keng, and A. Veneris, "Non-Solution Implications using Reverse Domination in a Modern SAT-based Debugging Environment," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, pp. 629–634, 2012

[63] Z. Poulos, Y. S. Yang, J. Anderson, and A. Veneris, "Leveraging Reconfigurability to Raise Productivity in FPGA Functional Debug", in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2012

[64] H.Mangassarian, H.Yoshida, A.Veneris, S.Yamashita, and M.Fujita, "On Error Tolerance and Engineering Change with Partially Programmable Circuits," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2012

[65] Y. S. Yang, A. Veneris, N. Nicolici, and M. Fujita, "Automated Data Analysis Techniques for a Modern Silicon Debug Environment," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2012 (invited paper)

[66] B. Keng, D. E. Smith, and A. Veneris, "Efficient Debugging of Multiple Design Errors," in *IEEE Microprocessor Test and Verification Workshop*, 2011

[67] H. Mangassarian, A. Veneris, D. E. Smith, and S. Safarpour "Debugging with Dominance: On-the-fly Debug Solution Implications," in *IEEE/ACM Int'l Conference on Computer-Aided Design (ICCAD)*, 2011

[68] D. Sengupta, A. Veneris, S. Wilton, A. Ivanov, and R. Saleh, "Sequence Pair Based Voltage Island Floorplanning," in *IEEE International Green Computing Conference*, 2011

[69] B. Keng, S. Safarpour, and A. Veneris, "Automated Debugging of SystemVerilog Assertions," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2011

[70] A. Veneris and S. Safarpour, "From RTL to Silicon: The Case for Debug Automation," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2011 (invited paper)

[71] B. Keng and A. Veneris, "Managing Complexity in Design Debugging with Sequential Abstraction and Refinement," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2011

[72] H. Mangassarian, B. Le, A. Goultiaeva, A. Veneris, and F. Bacchus, "Leveraging Dominators for Preprocessing QBF," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2010

[73] S. Safarpour, B. Keng and A. Veneris, "An Automated Framework for Correcting and Debugging PSL Assertions," in *IEEE Microprocessor Test and Verification Workshop*, 2010.

[74] Y. S. Yang, B. Keng, A. Veneris, N. Nicolici, and H. Mangassarian, "Software Solutions to Automating Data Analysis and Acquisition Setup in Silicon Debug," in *IEEE Silicon Debug and Diagnosis Workshop (SDD)*, 2010

[75] S. Safarpour, A. Veneris, and F. Najm, "Managing Verification Error Traces with Bounded Model Debugging," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2010

[76] Y. S. Yang, B. Keng, N. Nicolici, and A. Veneris, "Automated Silicon Debug Data Analysis Techniques for a Hardware Data Collection Environment," in *IEEE Int'l Symposium on Quality of Electronic Design (ISQED)*, 2009.

[77] S. Safarpour and A. Veneris, "Automated Debugging with High Level Abstraction and Refinement," in *IEEE High Level Design Validation and Test Workshop*, 2009

[78] B. Keng and A. Veneris, "Scaling VLSI Design Debugging with Interpolation," in *Formal Methods in CAD (FMCAD)*, November 2009

[79] Y. Chen, S. Safarpour, and A. Veneris, "Optimal Trace Compaction with Property Preservation," in *IEEE Midwest Symposium on Circuits and Systems*, July 2009

[80] A. Veneris and S. Safarpour, "The Day Sherlock Holmes Decided to do EDA," in *IEEE/ACM Design Automation Conference (DAC)*, July 2009 (invited paper)

[81] E. Safi, A. Moshovos, and A. Veneris, "A Physical-Level Study of the Compacted Matrix Instruction Scheduler for Dynamically Scheduled Superscalar Processors," in *IEEE Int'l Symposium on Systems, Architectures, Modeling and Simulation (SAMOS)*, October 2009

[82] Y. Chen, S. Safarpour, A. Veneris, and J. M. Silva, "Spatial and Temporal Design Debug using Partial MaxSAT," in *IEEE Great Lakes VSLI Symposium (GLVLSI)*, May 2009

[83] T. Yang, A. Veneris, and N. Nicolici, "Automated Software Data Analysis Solutions to Silicon Debug,"in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, April 2009

[84] T. Yang, S. Sinha, A. Veneris, and R. Brayton, "Sequential Logic Rectification Techniques using Approximate SPFDs," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, April 2009

[85] B. Keng, H. Mangassarian, and A. Veneris, "A Succinct Memory Model for Automated Design Debugging," in *IEEE/ACM Int'l Conference on Computer-Aided Design (ICCAD)*, 2008

[86] S. Almukhaizim, Y. Makris, Y. S. Yang, and A. Veneris, "On the Minimization of Potential Transient Errors and SET in Logic Circuits using SPFD," in *IEEE Int'l On-Line Test Symposium (IOLTS)*, 2008

[87] S. Safarpour, M. Liffton, H. Mangassarian, A. Veneris, and K. A. Sakallah, "Improved Design Debugging Using Maximum Satisfiability," in *Formal Methods in CAD (FMCAD)*, 2007

[88] H. Mangassarian, A. Veneris, S. Safarpour, M. Benedetti, and D. Smith, "A Performance-Driven QBF-Based Iterative Logic Array Representation with Applications to Verification, Debug and Test," in *IEEE/ACM Int'l Conference on Computer-Aided Design (ICCAD)*, 2007

[89] E. Safi, P. Akl, A. Moshovos, A. Veneris, and A. Arapoyianni, "On the Latency, Energy and Area of Checkpointed, Supescalar Register Alias Tables," in *IEEE Int'l Symposium on Low Power Electronic Devices (ISLPED)*, 2007

[90] H. Mangassarian, A. Veneris, and M. Benedetti, "Fault Diagnosis Using Quantified Boolean Formulas," in *IEEE Silicon Debug and Diagnosis Workshop (SDD)*, 2007

[91] H. Mangassarian, A. Veneris, S. Safarpour, F. N. Najm, and M. S. Abadir, "Maximum Circuit Activity Estimation Using Pseudo-Boolean Satisfiability," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2007

[92] S. Safarpour and A. Veneris, "Abstraction and Refinement Techniques for Automated Design Debugging," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2007

[93] Y. S. Yang, S. Sinha, A. Veneris, and R. K. Brayton, "Automating Rectification by Approximate SPFDs," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2007

[94] S. Safarpour, A. Veneris, and H. Mangassarian, "Trace Compaction using SAT-based Reachability Analysis," in *IEEE Int'l Symposium on Low Power Electronic Devices (ISLPED)*, 2006

[95] S. Safarpour, M. Hutton, and A. Veneris, "Efficient SAT-based Boolean Matching for FPGA Technology Mapping," in *IEEE/ACM Design Automation Conference (DAC)*, 2006

[96] E. Safi, A. Moshovos, and A. Veneris, "L-CBF: A Low-Power, Fast Counting Bloom Filter Architecture," in *IEEE Int'l Symposium on Low Power Electronic Devices (ISLPED)*, 2006

[97] G. Fey, S. Safarpour, A. Veneris, and R. Drechsler, "On the Relation Between Simulation-based and SAT-based Diagnosis," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2006

[98] M. F. Ali, S. Safarpour, A. Veneris, M. S. Abadir, and R. Drechsler, "Post-Verification Debugging of Hierarchical Designs," in *IEEE/ACM Int'l Conference on Computer-Aided Design (ICCAD)*, 2005

[99] J. B. Liu, M. S. Abadir, A. Veneris, and S. Safarpour,"Diagnosing Multiple Transition Faults in the Absense of Timing Information," in *IEEE Great Lakes VSLI Symposium (GLVLSI)*, 2005

[100] S. Safarpour, G. Fey, A. Veneris, and R. Drechsler, "Utilizing Don't Care States in SAT-based Bounded Sequential Problems," in *IEEE Great Lakes VSLI Symposium (GLVLSI)*, 2005

[101] Y. S. Yang, A. Veneris, P. Thadikaran, R. Chang, and S. Venkataraman, "Extraction Error Modeling and Automated Model Debugging in High-Performance Custom Designs," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2005

[102] M. F. Ali, A. Veneris, S. Safarpour, R. Drechsler, A. Smith, and M. S. Abadir, "Debugging Sequential Circuits Using Boolean Satisfiability," in *IEEE/ACM Int'l Conference on Computer-Aided Design (ICCAD)*, 2004

[103] J. B.Liu, M. S. Abadir, R. Chang, and A. Veneris, "MONARCH: A Platform for Logic Optimization using ATPG/Diagnosis-based Design Rewiring," in *IEEE Latin-American Test Workshop (LATW)*, 2004

[104] A. Smith, A. Veneris, and A. Viglas, "Design Diagnosis Using Boolean Satisfiability," *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2004 **Recipient of 10-Year Retrospective Best Paper Award)**.

[105] A. Veneris, R. Chang, M. S. Abadir, and M. Amiri, "Fault Equivalence and Diagnostic Test Generation Using ATPG," in *IEEE Int'l Symposium on Systems and Circuits*, 2004

[106] S. Safarpour, A. Veneris, R. Dreschler, and J. Lee, "Managing Logic Don't Cares in Boolean Satisfiability," *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2004

[107] Y. Yang, B. Liu, P. Thadikaran and A. Veneris, "Extraction Error Diagnosis and Correction in High-Performance Designs," in *IEEE Int'l Test Conference (ITC)*, 2003.

[108] R. Chang, S. Seyedi, A. Veneris, and M. S. Abadir, "Exact Functional Fault Collapsing in Combinational Logic Circuits," in *IEEE Latin-American Test Workshop (LATW)*, 2003

[109] Y.-S. Yang, J. B. Liu, P. Thadikaran, and A. Veneris, "Extraction Error Analysis, Diagnosis and Correction in Custom-Made High-Performance Designs," in *IEEE Microprocessor Test and Verification Workshop*, 2003.

[110] A. Veneris, A. Smith, and M. S. Abadir, "Logic Verification Using Diagnosis Techniques," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2003.

[111] B. J. Liu, A. Veneris and H. Takahashi, "Incremental Diagnosis of Multiple Open Interconnects," in *IEEE Int'l Test Conference (ITC)*, 2002.

[112] A. Veneris, M. S. Abadir, and M. Amiri, "Design Rewiring Using ATPG," in *IEEE Int'l Test Conference (ITC)*, 2002.

[113] A. Veneris, M. Amiri, and I. Ting, "Design Rewiring for Power Minimization," in *IEEE Int'l Symposium on Circuits and Systems*, 2002.

[114] J. B. Liu, A. Veneris, and H. Takahashi, "A Diagnoser for Multiple Open-Interconnect Faults," in *IEEE Microprocessor Test and Verification Workshop*, 2002.

[115] B. Liu, A. Veneris and M. S. Abadir, "Efficient and Exact Diagnosis of Multiple Stuck-at faults," in *IEEE Latin-American Test Workshop (LATW)*, 2002.

[116] A. Veneris, B. J. Liu, M. Amiri and M. S. Abadir "Incremental Diagnosis and Debugging of Multiple Faults and Errors," in *IEEE/ACM Design, Automation and Test in Europe (DATE)*, 2002.

[117] I. Ting, A. Veneris, and M. S. Abadir "Design Optimization for Delay and Power Minimization," in *IEEE Latin-American Test Workshop (LATW)*2001.

[118] A. Veneris, M. S. Abadir, and I. Ting, "Design Rewiring based on Diagnosis Techniques," in *IEEE/ACM Asia and South Pacific Design Automation Conference (ASP-DAC)*, pp. 479–484, 2001 **(Recipient of ASP-DAC 2001's best paper award)**.

[119] A. Veneris, M. S. Abadir, and I. N. Hajj, "Design Optimization based on Diagnosis Techniques," in *IEEE Latin-American Test Workshop (LATW)*, 2000.

[120] A. Veneris, S. Venkataraman, I. N. Hajj, and W. K. Fuchs, "Multiple Design Error Diagnosis and Correction in Digital VLSI Circuits," in *IEEE VLSI Test Symposium*, pp. 58–63, 1999.

[121] A. Veneris, and I. N. Hajj, "A Hybrid Approach to Design Error Detection and Correction," in *Proceedings of International Conference on Electronics, Circuits and Systems*, 1999.

[122] A. Veneris and I. N. Hajj, "Correcting Multiple Design Errors in Digital VLSI Circuits," in *IEEE International Symposium on Circuits and Systems*, 1999.

[123] A. Veneris and I. N. Hajj, "A Fast Algorithm for Locating and Correcting Simple Design Errors," in *IEEE Great Lakes VSLI Symposium (GLVLSI)*, pp. 45–50, 1997.

[124] A. Veneris and I. N. Hajj, "Error Diagnosis and Correction in VLSI Digital Circuits," in *IEEE Midwest Symposium on Circuits and Systems*, pp. 1005–1008, 1997.

[125] L. M. Kirousis and A. Veneris, "Efficient Algorithms for Checking the Atomicity of a Run of Read and Write Operations," in *7th International Workshop of Distributed Algorithms, Lecture Notes in Computer Science 725, Springer-Verlag*, pp. 54–68, 1993.

[126] L. M. Kirousis, P. Tsigas, and A. Veneris, "An Atomicity Criterion for Composite Registers," in *Proceedings of IMACS/IFAC International Symposium on Parallel and Distributed Computing in Engineering Systems (North-Holland)*, pp. 31–34, 1992.

Submitted Conference and Journal papers

[1] Z. Chen, S. Beillahi, A. Veneris and F. Long, "Enforcing Control Flow Integrity on DeFi Smart Contracts", submitted to IEEE/ACM International Conference on Software Engineering, 2026

[2] R. Li, S. F. Singh, A. Park and A. Veneris, "Blockchain Meets Securities: A Scalable Tokenization Framework", submitted to ACM Journal of Distributed Ledger Technologies: Research and Practice (invited paper)

[3] P. Michalopoulos, C. Clark, A. Mack, L. Chen, J. Sedlmeir, A. Veneris, "A prototype for private and compliant offline CBDC transactions", submitted to 32nd ACM Conference on Computer and Communications Security (CCS)

Policy White Papers

[1] A. Veneris, "Decentralization, Anonymity and Privacy in the 21st Digital Century", in Centre for International Governance Innovation (CIGI), to appear

[2] Y. S. Ming, A. M. Ho, Y. T. Hon, L. Y. Wang, Q. Xianrui, A. Veneris and N. Pocher, "Privacy on CBDC: A Technical Overview", Bank of International Settlements and Hong Kong Monetary Authority, to appear

[3] D. Duffie, O. Olowookere, and A. Veneris, "A Note on Privacy and Compliance for Stablecoins", SSRN, to appear

Patents

[1] S. Safarpour and A. Veneris, "Method, System and Computer Program for Hardware Design Debugging," US Patent 8,881,077

[2] S. Safarpour and A. Veneris, "Method, System and Computer Program for Hardware Design Debugging," US Patent 8,751,984

[3] A. Veneris and M. S. Abadir "ATPG-based Design Rewiring", US Patent 7,003,743

Books and Book Chapters

[1] N. Pocher and A. Veneris, "Central Bank Digital Currencies", Springer Handbook on Blockchain, 2022

[2] Y. S. Yang, S. Sinha, A. Veneris and R. K. Brayton, "Advanced Techniques in Logic Synthesis, Optimizations and Applications," *Springer 2010* (Ed: Sunil P. Khatri and Kanupriya Gulati)

[3] A. Veneris, and D. Kalles, "Fortran 77: A Comprehensive Introduction" (in Greek), *Voulgaris Editions,* 1987 (1st ed.), 1989 (2nd ed.), 1991 (3rd ed.)

Invited Talks (partial)

[1] University of Illinois: January 2001
[2] Motorola, Austin, TX: July 2001, June 2003
[3] Southern Illinois University: August 2001
[4] McGill University: July 2002
[5] Intel Corporation, Hillsboro, OR: August 2002, August 2003
[6] Purdue University: August 2002
[7] University of Crete, Heraklion: January 2004
[8] Infineon Corporation, Munich, Germany: June 2004
[9] Altera Corporation, San Jose, CA: October 2004
[10] University of British Columbia, Vancouver: February 2005
[11] University of California, Berkeley, CA: February 2005
[12] University of California, Santa Cruz, CA: February 2005
[13] Bremen University, Bremen: February 2005
[14] Athens University of Economics and Business, Athens: June 2005
[15] Carnegie Mellon University, Pittsburgh: January 2006
[16] University of Michigan, Ann Arbor: January 2006
[17] Intel Corporation, Oregon: July 2006
[18] Cadence Berkeley Laboratories: October 2006
[19] University of Tokyo: February 2007
[20] University of Tokyo, grand opening VLSI Design and Education Center: January 2008 (*keynote talk*)
[21] The University of Western Australia, Perth: February 2009
[22] Cadence Berkeley Labs: February 2009
[23] IEEE/ACM Design Automation Conference: July 2009
[24] National Taiwan University: April 2010
[25] IEEE/ACM Asia and South Pacific Design Automation Conference: January 2011 (*invited talk*)
[26] Tokyo University, Tokyo: January 2011
[27] Osaka University, Osaka: January 2011
[28] Kyoto University, Kyoto: January 2011
[29] Ehime University, Ehime: January 2011
[30] Hitachi, Tokyo: February 2012
[31] University of Illinois, Urbana-Champaign: August 2012
[32] AMD, Markham: April 2013
[33] University of Western Australia, Perth: February 2014
[34] IBM Haifa Verification Conference, 2016 (keynote)
[35] Canada Blockchain Fintech, 2017
[36] Canadian Pension Plan Investment Board, 2018

[37] Blockchain and Security Workshop, 2019
[38] Canada Revenue Agency, 2020
[39] Boston University, Distinguished Lecture Series, 2021
[40] Bennet Jones LLP, 2021

Student Supervision

All graduate students are financially supported by research grants. Of importance is also the balanced diversity in my group. Further, numerous undergraduates have been supported by NSERC USRA and other means in the past decades, not noted here.

Current Graduate Students and Post-Doctoral

- Panos Michalopoulos (Ph.D., 2025 expected)
- Odun Olowookere (Ph.D., 2027 expected) (co-supervision with Osgoode Law School)
- Srisht Fateh Singh (Ph.D., 2027 expected)
- Xun Deng (Ph.D., 2028 expected)
- Yuntao (Winston) Wu (Ph.D., 2028 expected)
- Reina Li (M.A.Sc., 2025 expected, admitted to Ph.D. 2029 expected)
- Vladyslav Nekriach (M.A.Sc., 2025 expected)
- Yuntao Cai (M.A.Sc., 2025 expected)
- Mahmoud Khaled (M.A.Sc., 2027 expected)
- Justin Shi (M.A.Sc, 2027 expected)
- Sayyed Muhammad Jaffry (M.A.Sc., 2027 expected)

Ph.D. Students, and Post-Doctoral (graduated)

- Sidi Mohamed Beillahi (post-doctoral, 2021-2024)
- Keerthi Nelaturu (Ph.D., 2024)
- Ryan Berryhill (Ph.D., 2020)
- Zisis Poulos (Ph.D., 2018)
- Dipanjan Sengupta (post-doctoral, 2010–2013)
- Brian Keng (Ph.D., 2013)
- Hratch Mangassarian (Ph.D., 2012)
- Yu Shen (Terry) Yang (Ph.D., 2010)
- Elham Safi (Ph.D., 2009)
- Sean Safarpour (Ph.D., 2009)

M.A.Sc. and M.Eng. (with thesis) (graduated)

- Bowen Wu (M.A.Sc., 2024)
- Xun Deng (M.A.Sc, 2024)
- Yuntao (Winston) Wu (M.A.Sc, 2024)
- Srisht Fateh Singh (M.A.Sc., 2023)
- Eric Keilty (M.A.Sc., 2023)
- Armita Jalooli (M.A.Sc., 2022)
- James Meijers (M.A.Sc., 2022)
- Yuxi Cai (M.A.Sc., 2021)
- Nick Fung (M.A.Sc., 2021)
- Neil Veira (M.A.Sc., 2019)
- John Adler (M.A.Sc., 2017)
- Kazi Arif (M.Eng., 2018)
- Ryan Berryhill (M.A.Sc., 2016)
- Bao Le (M.A.Sc., 2015)
- Djordje Maksimovic (M.A.Sc., 2015)
- Zisis Poulos (M.A.Sc., 2013)
- Bao Le (M.A.Sc., 2012)
- Brian Keng (M.A.Sc., 2009)
- Yibin Chen (M.A.Sc., 2009)
- Jackey Wong (M.Eng., August 2008)
- Hratch Mangassarian (M.A.Sc., 2006)
- Moayad Fahim Ali (M.A.Sc., 2005)
- Sean Safarpour (M.A.Sc., 2005).
- Terry Yang (M.A.Sc., 2004)
- Karen Ha (M.Eng., 2004)
- Joanna Lee (M.Eng., 2004)
- Robert Chang (M.Eng., 2004)

- Alexander Smith (M.A.Sc., 2004)
- Brandon Jiang Liu (M.A.Sc., 2002)
- Mandana Amiri (M.Eng., 2001)
- Ivor Ting (M.Eng., 2000)

Research Support (committed)

Funds in Canadian dollars. All amounts below are matched with equivalent amounts by UofT Open, OGS and NSERC/Bell, etc scholarships (not shown here).

Individual projects:

- *NSERC Discovery*, $355,000, Interoperability, Security and Decentralized ID In Modern DeFi Blockchain Payment Networks (2025–2031)
- *MITACS and Bank of Canada*, $35,000, Enhancing the Security of DeFi Ecosystem via Smart Contract Analysis (2024-25)
- *Ripple Foundation*, $660,000, Donation (2023)
- *MITACS and Bank of Canada*, $108,000, Enhancing the Security of DeFi Ecosystem via Smart Contract Analysis (2023-24)
- *MITACS and Bank of Canada*, $105,000, Verification and Security of Blockchain Oracle Network Effects on Smart Contracts (2022-23)
- *Bank of Canada, Model X Competition*, $65,000, Design of Digital Loonie (leading-PI in grant with Andreas Park (Rotman), Fan Long (DCS), Poonam Puri (Osgoode Law School)) (2020)
- *Huawei Canada*, $395,000, Blockchain architecture for V2X IoT (co-PI with Arno Jacobsen, 50% split) (2020-23)
- *MITACS* with support from *Riskfuel*, $15,000, Geometric Deep Learning of Volatility Surfaces
- *Connaught Global Challenge*, $250,000, Technology of Cryptoeconomics, Regulation and Decentralized Finance
- *IBM Faculty Award*, $40,000, Formal verification of chaincode
- *NSERC Discovery*, $140,000, Automated Smart Contract Synthesis and Verification for Distributed Blockchain Technology, (2019–2024)
- *NSERC Engage* with *Rubikloud*, $25,000, Multimodal representation learning for retail product ontology (2017)
- *OCE Talent Edge* supported by *Sysomos*, $30,000, Multimodal Representation with Deep Learning for Joint Image and Text Reasoning (2016–2017)
- *NSERC Discovery*, $167,500, Theory and Methodology for Performance-Driven Automation in RTL and Testbench Debugging (2014–2018)
- *MITACS* supported by *Sysomos*, $ 30,000, Time-aware Network Diffusion for Social Network Analytics (2015)
- *OCE* supported by *AMD*, $ 50,000, Power Grid Verification (2013)

- *NSERC CRD* supported by *AMD*, $ 150,000, Low-Power Design using Power Gating (2012–2014)
- *NSERC Engage* with *Altera Corporation*, $ 25,000, Debugging Emulation Failures (2012)
- *NSERC Engage* with *AMD*, $ 25,000, Verification for Low Power Design (2011)
- *TGAP* $ 30,000 (Debugging with Abstraction and Refinement, 2010)
- *MITACS Cluster Accelerate Ontario,* $ 120,000 (SVA-based verification and debug, 2009–2010)
- *NSERC Post-Doctoral grant*, $ 70,000 for Dr. Dipanjan Sengputa (2010)
- *NSERC Discovery Grant*, $ 230,000 (QBF and SAT Encodings for Verification, Debug and Test, 2009–2013). *Nominated for an NSERC Discovery Accelerate Supplement for this application.*
- *MITACS Accelerate Ontario*, $ 30,000 (Silicon Debug, 2008)
- *CITO Tech Readiness*, $ 50,000 (Prototype for Logic Debugging, 2006–2007)
- *Infineon, Munich* $ 15,000 (unrestricted)
- *NSERC Operational Grant*, $ 73,500 (SAT-based debugging, 2006–2008)
- *NSERC Collaborative Research Program*, $ 18,000 (2003-2004)
- *CITO* with industrial matching from *Motorola (Austin, TX)*, $ 150,000 (ATPG- and SAT-based techniques for Logic Verification, 2004–2005)
- *Intel (Portland, OR)* $ 17,000 (Transistor level diagnosis for high-performance custom made designs, unrestricted)
- *CITO* with industrial matching from *Motorola (Austin, TX)*, $ 80,000 (Incremental Logic Diagnosis and Repair Techniques, 2001–2002)
- *Micronet Grant*, $ 20,000 (Design for Low Power, 2000)
- *NSERC Operational Grant*, $ 88,000 (Design Optimization, 2002–2005)
- *NSERC Operational Grant*, $35,000 (Design Optimization, 2000–2001)
- *Connaught New Faculty*, $ 20,000 (Design Optimization, 2 years)
- *Start up Connaught Fund*, $ 10,000 (unrestricted)
- *Start up Departmental Fund*, $ 60,000 (unrestricted)

Joint projects:

- *CFI New Opportunities Equipment Grant*, $ 54,000 (2000–2004). This amount is part of a larger project funded by CFI for a total of approximately $ 550,000 towards five new faculty at U-Toronto/ECE. The proposal was supervised by Prof. F. Najm.
- *NSERC*, $ 96,000 for a computing server. Proposal supervised by Prof. P. Chow for 15 faculty members at U-Toronto/ECE.

Professional Services

Services (partial list)

- Steering Committee of IEEE Int'l Conference on Blockchain and Cryptocurrency (ICBC), General co-Chair of IEEE ICBC in 2022, General co-Chair for IEEE Blockchain and Research Applications for Innovative Networks and Services (BRAINS) 2021, Associate Editor for IEEE Transactions on Network and Service Management (2020-present)
- Program Committee Member (present and past): IEEE Int'l Conference on Blockchain and Cryptocurrency, IEEE Int'l Blockchain Conference, IEEE AI Block, ACM Blockchain and IoT Conference, International Conference on. Mathematical Research for Blockchain Economy (MARBLE), IEEE Blockchain and IoT Conference (BIOTC), Int'l Conference on Mathematical Research of Blockchain Economy (MARBLE), IEEE/ACM Design and Test in Europe Conference, IEEE International Test Conference, IEEE VLSI Design Conference, IEEE International Conference on Embedded Systems, IEEE North American Test Workshop, IEEE Microprocessor Test and Verification Workshop, IEEE On Line Test Symposium, IEEE Latin-American Test Workshop, IEEE Workshop on Constraints in Formal Verification, IEEE Asian Test Symposium, and IEEE International Conference on Very Large Scale of Integration.
- Student Activities Chair Technical Test Technology Council (TTTC, 2002-07), PC for ACM Student Research Competition at ICCAD (2007-10)

Reviewer (partial list)

- Reviewer for NSERC, NSF, OCE, California Micro, SRC.
- Reviewer for IEEE Int'l Conference on Blockchain, IEEE Trans. On Computer-Aided Design, IEEE Trans. On Computers, IEEE Trans. On VLSI, IEEE Design and Test, IEEE/ACM International Conference on Computer-Aided Design (ICCAD), IEEE/ACM Design Automation Conference (DAC), IEEE/ACM Design and Test in Europe (DATE), IEEE International Test Conference (ITC), IEEE VLSI Test Symposium (VTS), IEEE Asia and South Pacific Design Automation Conference (ASP-DAC), IEEE Great Lakes VLSI Symposium (GVLSI), IEEE Latin American Test Workshop (LATW), IEEE/ACM International Symposium on Circuits and Systems (ISCAS), Kluwer Journal on Electronic Testing: Theory and Applications (JETTA), ACM Transactions on Design Automation of Electronic Systems, ACM Formal Methods in CAD, Journal of Satisfiability (JSAT), IEE Trans. On Computers and Digital Techniques, VLSI Journal: Integration