

Curriculum Vitae

Sidi Mohamed Beillahi

Postdoctoral Researcher

University of Toronto

sm.beillahi@utoronto.ca

<https://beillahi.github.io>

Google Scholar

Linkedin

❖ Research Interests

Software engineering; Software security; Software verification; Distributed systems; Blockchain; Formal verification; Algorithmic verification; Programming languages; Program synthesis.

❖ Education

Ph.D. — Computer Science

Dec 2017 – Mar 2021

Thesis: **Automated Verification of Programs Running on top of Distributed Systems**

Paris Diderot University, France

Advisors: Ahmed Bouajjani and Constantin Enea

Master of Applied Science — Computer Engineering

Sep 2014 – Nov 2016

Thesis: **Towards the Design Automation of Quantum Circuits**

Concordia University, Canada

Advisor: Sofiène Tahar

Engineer's Degree — Polytechnicien

Sep 2011 – Jun 2014

Thesis Title: **Formalization of Signal-Flow Graphs in HOL**

Tunisia Polytechnic School, Tunisia

Advisor: Sofiène Tahar

DEUPC — Mathematics and Physics

Sep 2009 – Jun 2011

Sfax Preparatory Engineering Institute

University of Sfax, Tunisia

❖ Experience

NSERC Postdoctoral Research Fellow, University of Toronto

Jun 2021 – present

Advisors: Fan Long and Andreas Veneris

Toronto, Canada

Mitacs Accelerate Postdoctoral Fellow, University of Toronto and Bank of Canada

Sep 2022 – present

Course Instructor, York University

Jan 2024 – present

Toronto, Canada

Research Consultant, Conflux Network

Dec 2021 – present

Course Instructor, University of Toronto

Sep 2022 – Apr 2023

Research Assistant, Institut de Recherche en Informatique Fondamentale

Dec 2017 – May 2021

Advisors: Ahmed Bouajjani and Constantin Enea

Paris, France

Teaching Assistant, Paris Diderot University

Sep 2018 – Jan 2021

Research Intern, SRI International

Apr 2019 – Aug 2019

Advisor: Michael Emmi

New York City, USA

Software Programmer, TRU Simulation + Training

May 2017 – Dec 2017

Montréal, Canada

Research Assistant, Concordia University

Mar 2014 – Nov 2016

Advisor: Sofiène Tahar

Montréal, Canada

Teaching Assistant, Concordia University

Sep 2015 – May 2016

Research Engineer, Marinvent inc.

Mar 2016 – Nov 2016

Advisor: Sofiène Tahar

Montréal, Canada

Intern, STMicroelectronics

Jul 2013 – Aug 2013

Advisor: Mohamed Ben Ahmed

Tunis, Tunisia

❖ Awards and Recognitions

- ACM SIGSOFT Distinguished Paper Award, ICSE 2024.
- Invited to a Journal Special Issue for Selected OSDI 2023 papers, 2023.
- IEEE ICBC Distinguished Paper Award, 2022.
- Invited to a Journal Special Issue for Selected CONCUR 2019 Papers, 2019.
- Best Undergraduate Thesis, Tunisia Polytechnic School, 2014.
- Ranked 31st in the National Grandes Ecoles Exam, Tunisia, 2011.
- Olympian in the International Mathematical Olympiad, Germany, 2009.
- Ranked 3rd in the National Mathematical Olympiad, Mauritania, 2009.
- Ranked 1st in the National Bac Exam in Mathematics, Mauritania, 2009.

❖ Grants and Scholarships

- PI in a MITACS Mitacs Business Strategy Grant, 2024, CAD 31,000.
- PI in two MITACS Accelerate Partnership Grants, 2022 – 2024, CAD 205,500.
- NSERC Postdoctoral Fellowship, 2022 – 2024, CAD 90,000.
- Smart Contract Research Forum Grant, 2022, USD 1,000.
- VMW Scholarship Award for CAV 2016, USD 650.
- Concordia Graduate Student Association Conference Funding for CAV 2016, CAD 100.
- Concordia University Conference and Exposition Award for NFM 2016, CAD 1,000.
- Graduate Student Support Program, Concordia University, 2014 – 2016, CAD 20,000.
- National Scholarship, Mauritania, 2009 – 2014, EUR 13,500.
- Scholarship Award to Participate in the International Mathematical Olympiad, Mauritania, 2009, EUR 1,000.

❖ Service

- Co-organizer, Institut de Recherche en Informatique Fondamentale Verification Seminar, Mar 2020 – July 2020.
- Artificat Evaluation Committees: POPL 2021-2022, CAV 2021, CAV 2024, OOPSLA 2021-2022.
- Extended Review Committees: OOPSLA 2022.
- Sub-Reviewer: FTSCS 2016, VMCAI 2020, CAV 2020, Blockchain 2021, ICDCS 2022, ICBC 2022-2023, TACAS 2024.
- Journal Invited Reviewer: IEEE Transactions on Network and Service Management
- Student Volunteer: CAV 2016.

❖ Journal Publications

LVMT: An Efficient Authenticated Storage for Blockchain

Chenxing Li, **Sidi Mohamed Beillahi**, Guang Yang, Ming Wu, Wei Xu, Fan Long

Accepted to the ACM Transactions on Storage

Invited special issue for best storage papers from OSDI 2023

2024

LMPT: A Novel Authenticated Data Structure to Eliminate Storage Bottlenecks for High Performance Blockchains

Jemin Andrew Choi, **Sidi Mohamed Beillahi**, Srisht Fateh Singh, Panagiotis Michalopoulos, Peilun Li, Andreas Veneris, Fan Long

IEEE Transactions on Network and Service Management, 21(2), 1333 – 1343

Invited special issue for best papers from ICBC 2022

Apr 2024

J5

J4

- J3 **SigVM: Enabling Event-Driven Execution for Truly Decentralized Smart Contracts** Oct 2022
Zihan Zhao, **Sidi Mohamed Beillahi**, Ryan Song, Yuxi Cai, Andreas Veneris, Fan Long
Proceedings of the ACM on Programming Languages, 6(OOPSLA2), 149:673 – 149:698
- J2 **Robustness Against Transactional Causal Consistency** Feb 2021
Sidi Mohamed Beillahi, Ahmed Bouajjani, Constantin Enea
Logical Methods in Computer Science, 17(1): 12:1 – 12:42
Invited special issue for selected papers from CONCUR 2019
- J1 **A Modeling and Verification Framework for Optical Quantum Circuit** Mar 2019
Sidi Mohamed Beillahi, Mohamed Yousri Mahmoud, Sofiène Tahar
Formal Aspects of Computing, 31(3): 321 – 351

❖ Conference Publications

- C22 **Enforcing Control Flow Integrity on DeFi Smart Contracts** 2024
Zhiyang Chen, **Sidi Mohamed Beillahi**, Pasha Barahimi, Cyrus Minwalla, Han Du, Andreas Veneris, Fan Long
under submission
- C21 **OpenTracer: A Dynamic Transaction Trace Analyzer for Smart Contract Invariant Generation and Beyond** 2024
Zhiyang Chen, Ye Liu, **Sidi Mohamed Beillahi**, Yi Li, Fan Long
In Proc. The 39th IEEE/ACM International Conference on Automated Software Engineering, Tool Demonstrations Track (ASE 2024 Demo)
- C20 **Assessing Code Generation with Intermediate Languages** 2024
Xun Deng, Sicheng Zhong, Honghua Dong, Jingyu Hu, **Sidi Mohamed Beillahi**, Xujie Si, Fan Long
under submission
- C19 **HEMVM: a Heterogeneous Blockchain Framework for Interoperable Virtual Machines** 2024
Vladyslav Nekriach, **Sidi Mohamed Beillahi**, Chenxing Li, Peilun Li, Ming Wu, Andreas Veneris, Fan Long
under submission
- C18 **Infernomic: A Decentralized System for Economic LLM Inference** 2024
Haohui Mai, **Sidi Mohamed Beillahi**, Yiyang Zhao, Guanqun Yang, Qianqi Sun, Jingbo Shang, Jiacheng Zhao, Xueqing Liu, Mingyu Gao, Christos Kozyrakis
under submission
- C17 **Demystifying Invariant Effectiveness for Securing Smart Contracts** Jul 2024
Zhiyang Chen, Ye Liu, **Sidi Mohamed Beillahi**, Yi Li, Fan Long
In Proc. The ACM International Conference on the Foundations of Software Engineering (FSE 2024)
- C16 **FlashSyn: Flash Loan Attack Synthesis via Counterexample-Driven Approximation** Apr 2024
Zhiyang Chen, **Sidi Mohamed Beillahi**, Fan Long
In Proc. 46th IEEE/ACM International Conference on Software Engineering (ICSE 2024)
- C15 **Safeguarding DeFi Smart Contracts against Oracle Deviations** Apr 2024
Xun Deng, **Sidi Mohamed Beillahi**, Cyrus Minwalla, Han Du, Andreas Veneris, Fan Long
In Proc. 46th IEEE/ACM International Conference on Software Engineering (ICSE 2024)
ACM SIGSOFT Distinguished Paper Award.
- C14 **IVMT: An Efficient Authenticated Storage for Blockchain** Jul 2023
Chenxing Li, **Sidi Mohamed Beillahi**, Guang Yang, Ming Wu, Wei Xu, Fan Long
In Proc. 17th USENIX Symposium on Operating Systems Design and Implementation (OSDI), 2023
Invited to a Special Issue of the ACM Transactions on Storage Journal for Selected OSDI 2023 Papers.
- C13 **A Robust Front-Running Methodology for Malicious Flash-Loan DeFi Attacks** Jul 2023
Xun Deng, Zihan Zhao, **Sidi Mohamed Beillahi**, Han Du, Cyrus Minwalla, Keerthi Nelaturu, Andreas Veneris, Fan Long
In Proc. IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), 2023

- C12 Möbius: an Atomic State Sharding Design for Account-Based Blockchains** May 2023
Srisht Fateh Singh, Panagiotis Michalopoulos, **Sidi Mohamed Beillahi**, Andreas Veneris, Fan Long
In Proc. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2023
- C11 Comparing Causal Convergence Consistency Models** May 2023
Sidi Mohamed Beillahi, Ahmed Bouajjani, Constantin Enea
In Proc. 11th International Conference on Networked Systems (NETYS), 2023
- C10 Automated Synthesis of Asynchronizations** Dec 2022
Sidi Mohamed Beillahi, Ahmed Bouajjani, Constantin Enea, Shuvendu Lahiri
In Proc. 29th Static Analysis Symposium (SAS), 2022
- C9 Automated Auditing of Price Gouging TOD Vulnerabilities in Smart Contracts** May 2022
Sidi Mohamed Beillahi, Eric Keilty, Keerthi Nelaturu, Andreas Veneris, Fan Long
In Proc. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2022
- C8 LMPTs: Eliminating Storage Bottlenecks for Processing Blockchain Transactions** May 2022
Jemin Andrew Choi, **Sidi Mohamed Beillahi**, Peilun Li, Andreas Veneris, Fan Long
In Proc. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2022
IEEE ICBC Distinguished Paper Award.
- C7 Smart Contracts Refinement for Gas Optimization** Sep 2021
Keerthi Nelaturu, **Sidi Mohamed Beillahi**, Fan Long, Andreas Veneris
In Proc. 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2021
- C6 Checking Robustness Between Weak Transactional Consistency Models** Mar 2021
Sidi Mohamed Beillahi, Ahmed Bouajjani, Constantin Enea
In Proc. 30th European Symposium on Programming (ESOP), 2021
- C5 Behavioral Simulation for Smart Contracts** Jun 2020
Sidi Mohamed Beillahi, Gabriela Ciocarlie, Michael Emmi, Constantin Enea
In Proc. 41st annual ACM SIGPLAN conference on Programming Language Design and Implementation (PLDI), 2020
- C4 Robustness Against Transactional Causal Consistency** Sep 2019
Sidi Mohamed Beillahi, Ahmed Bouajjani, Constantin Enea
In Proc. 30th International Conference on Concurrency Theory (CONCUR), 2019
Invited to a Special Issue of the Logical Methods in Computer Science Journal for Selected CONCUR 2019 Papers.
- C3 Checking Robustness Against Snapshot Isolation** Jul 2019
Sidi Mohamed Beillahi, Ahmed Bouajjani, Constantin Enea
In Proc. 31st International Conference on Computer Aided Verification (CAV), 2019
- C2 Hierarchical Verification of Quantum Circuits** Jun 2016
Sidi Mohamed Beillahi, Mohamed Yousri Mahmoud, Sofiène Tahar
In Proc. 8th International Symposium NASA Formal Methods (NFM), 2016
- C1 Formal Analysis of Power Electronic Systems** Nov 2015
Sidi Mohamed Beillahi, Umair Siddique, Sofiène Tahar
In Proc. 17th International Conference on Formal Engineering Methods (ICFEM), 2015

❖ Workshop Publications

- W3 Formal Analysis of Engineering Systems Based on Signal-Flow-Graph Theory** Jul 2016
Sidi Mohamed Beillahi, Umair Siddique, Sofiène Tahar
In Proc. 9th International Workshop Numerical Software Verification (NSV-CAV), 2016
- W2 On the Formal Analysis of Photonic Signal Processing Systems** Jun 2015
Umair Siddique, **Sidi Mohamed Beillahi**, Sofiène Tahar
In Proc. 20th International Workshop Formal Methods for Industrial Critical Systems (FMICS), 2015

A Tool for the Formal Verification of Quantum Optical Computing Systems

Apr 2015

Sidi Mohamed Beillahi, Mohamed Yousri Mahmoud, Sofiène Tahar

*In Proc. Automated Reasoning Workshop (ARW), 2015***❖ Teaching**

- Course Instructor at York University
 - EECS3342Z: System Specification and Refinement for 3rd Year Software Engineering Students, Jan 2024 – present.
- Course Co-Instructor at University of Toronto
 - CSC323H1S: Principles of Programming Languages for 3rd Year Computer Science Students, Jan 2023 – Apr 2023.
 - ECE345H1F: Algorithms & Data Structures for 3rd Year Computer Engineering Students, Sep 2022 – Dec 2022.
- Teaching Assistantships at Paris Diderot University
 - Automata and Lexical Analysis for 2nd Year Computer Science Students, Sep 2020 – Dec 2020.
 - Principles of Binary Machines for 1st Year Computer Science Students, Sep 2020 – Dec 2020.
 - Java Programming for 1st Year Computer Science Students, Sep 2019 – Dec 2019.
 - Principles of Object-Oriented Programming in Java for 2nd Year Computer Science Students, Sep 2019 – Dec 2019.
 - Python Programming for 1st Year Social Science Students, Sep 2018 – Dec 2018.
 - Relational Databases and SQL for 2nd Year Computer Science Students, Sep 2018 – Dec 2018.
- Teaching Assistantships at Concordia University
 - Hardware Functional Verification for Graduate and Senior Undergraduate Students, Jan 2016 – Apr 2016.
 - Computer Architecture and Design for Graduate Students, Jan 2016 – Apr 2016.
 - Digital Design for Undergraduate Students, Jan 2016 – Apr 2016.
 - Microprocessors and their Applications for Graduate Students, Sep 2015 – Dec 2015.

❖ Professional Affiliations

ACM (2020); IEEE (2022).

❖ Supervision

- Keerthi Nelaturu, Ph.D. student, University of Toronto
- Zihan Zhao, MASc student, University of Toronto - graduated in 2022
- Zhiyang Chen, Ph.D. student, University of Toronto
- Eric Keilty, MASc student, University of Toronto - graduated in 2023
- Srisht Fateh Singh, MASc student, University of Toronto - graduated in 2023
- Hossein Ghotbaddini, MASc student, University of Toronto - graduated in 2023
- Xun Deng, MASc student, University of Toronto
- Vladyslav Nekriach, MASc student, University of Toronto
- Jacky Zhou, MASc student, University of Toronto

❖ Talks**Improving the Reliability and Performance of Distributed Software Systems**

Département d'Informatique, Université du Québec à Montréal (UQAM)

Jul 2024

School of Information Technology, York University (virtual)

Apr 2024

Synthesis of Multi-Threaded (& Asynchronous) Programs

13th Workshop on Synthesis (SYNT 2024) at CAV 2024, Montréal, Canada

Jul 2024

Securing Smart Contracts Through Program Synthesis IRIF Verification Seminar, Université Paris Cité (virtual)	<i>Apr 2024</i>
Automated Synthesis of Asynchronizations 29th Static Analysis Symposium (SAS 2022) at SPLASH 2022, Auckland, New Zealand Workshop on Verification of Distributed Systems (VDS) 2024 at NETYS 2024, Rabat, Morocco	<i>Dec 2022</i> <i>May 2024</i>
SigVM: Enabling Event-Driven Execution for Truly Decentralized Smart Contracts OOPSLA 2022 at SPLASH 2022, Auckland, New Zealand Research Meeting with Bank of Canada, University of Toronto	<i>Dec 2022</i> <i>Jul 2022</i>
Automated Auditing of Price Gouging TOD Vulnerabilities in Smart Contracts ICBC 2022, Shanghai, China (virtual)	<i>May 2022</i>
Checking Robustness Between Weak Transactional Consistency Models ANR Project AdeCoDS Meeting, LIP6, Sorbonne University (virtual) IRIF Verification Seminar, Paris Diderot University (virtual) ESOP 2021, Luxembourg, Luxembourg (virtual)	<i>Jun 2021</i> <i>May 2021</i> <i>Mar 2021</i>
Behavioral Simulation for Smart Contracts COVID papers at SPLASH 2022, Auckland, New Zealand GROUP SEMINAR, University of Toronto (virtual) SEMINAR UM6P-CS, Morocco (virtual) PLDI 2020, London, UK (virtual)	<i>Dec 2022</i> <i>Dec 2021</i> <i>Jul 2020</i> <i>Jun 2020</i>
Robustness Against Transactional Causal Consistency IRIF Verification Seminar, Paris Diderot University CONCUR 2019, Amsterdam, Netherlands	<i>Dec 2019</i> <i>Sep 2019</i>
Checking Robustness Against Snapshot Isolation ANR Project AdeCoDS Kick-off Meeting, IRIF, Paris Diderot University CAV 2019, New York City, USA	<i>Nov 2019</i> <i>Jul 2019</i>
Formal Analysis of Engineering Systems Based on Signal-Flow-Graph Theory NSV 2016 at CAV 2016, Toronto, Canada	<i>Jul 2016</i>
Hierarchical Verification of Quantum Circuits 8th NASA Formal Methods Symposium (NFM 2016), Minneapolis, USA (virtual)	<i>Jun 2016</i>
Formal Analysis of Power Electronic Systems Hardware Verification Group Meeting, Concordia University	<i>Oct 2015</i>
On the Formal Analysis of Photonic Signal Processing Systems Hardware Verification Group Meeting, Concordia University	<i>May 2015</i>

❖ Recent media articles on the work published in C17

Blockchain Security Firm Quantstamp Hopes to Battle Flash Loan Attacks With New Service	<i>CoinDesk - Aug 2023</i>
Quantstamp unveils tool to detect DeFi flash loan vulnerabilities	<i>THE BLOCK - Aug 2023</i>