

Sina Kamali

(+1) 548-384-7706 | sinakamali@uwaterloo.ca | cs.uwaterloo.ca/~s4kamali | [kamali-sina](https://github.com/kamali-sina) | [cnakamali](https://www.linkedin.com/in/cnakamali) | [Sina Kamali](https://www.instagram.com/sinakamali)

Education

Cheriton School of Computer Science, University of Waterloo

Waterloo, ON

MASTER OF MATH IN COMPUTER SCIENCE

Sep. 2023 - present

- GPA: 95/100 (4.0/4 in the U.S. GPA system)
- Related Courses: Foundations of Modern Cryptography · Advanced Topics in Security, Privacy, and Cryptography
Advanced Topics in Distributed Computing

College of Electric and Computer Engineering, University of Tehran

Tehran, Iran

B.SC. IN COMPUTER ENGINEERING (SOFTWARE ENGINEERING MAJOR)

Sep. 2018 - Jan. 2023

- GPA: 18.31/20 (3.861/4 in the U.S. GPA system)

Research Interests

- Privacy Enhancing Technologies
- Applied Cryptography

Publications

- IEEE S&P '25** Sina Kamali and Diogo Barradas. "Anix: Anonymous Blackout-Resistant Microblogging with Message Endorsing." 2025 IEEE Symposium on Security and Privacy (S&P). IEEE Computer Society, 2024. [PDF]
- USENIX Security '24** Patrick Tser Jern Kon, Sina Kamali, Jinyu Pei, Diogo Barradas, Ang Chen, Micah Sherr, and Moti Yung. "SpotProxy: Rediscovering the Cloud for Censorship Circumvention." In 33rd USENIX Security Symposium (USENIX Security 24), pp. 2653-2670. 2024. [PDF]
- arXiv preprint** Sina Kamali, Taha Fakharian, Shayan Shabihi, Alireza Arbabi, Mohammad Saadati, Pouriya Tajmehrabani, and Behnam Bahrak. "RPoA: Redefined Proof of Activity". arXiv preprint arXiv:2210.08923 (2022). [PDF]

Research Experience

Under the supervision of Prof. D. Barradas

University of Waterloo

RESEARCH ASSISTANT

Jan. 2023 - present

- Developing privacy-enhancing tools with the help of applied cryptography to help people in areas with heavy internet censorship or repeated shutdowns. Our previous work has resulted in two publications in USENIX Security '24 and IEEE S&P '25. We are currently focusing on using zero-knowledge proofs (ZKPs) with private information retrieval (PIR) techniques to create a secretive, anonymous, and bi-directional messaging system.

With Prof. A. Chen & Prof. M. Sherr

Universities of Waterloo, Michigan,
and Georgetown

COLLABORATED

Aug. 2023 - Feb. 2024

- Researched an alternative approach to censorship circumvention utilizing SpotVMs, cheap but volatile servers, to create a moving-target circumvention system. Our work resulted in a publication in USENIX Security '24.

Under the supervision of Prof. B. Bahrak

University of Tehran

RESEARCH ASSISTANT

Aug. 2021 - Jan. 2023

- Worked on an alternative blockchain consensus protocol based on Proof of Activity to combine the benefits of PoS and PoA protocols. Our work resulted in a paper that remains in preprint.

Under the supervision of Prof. P. Shariatpanahi

University of Tehran

RESEARCH ASSISTANT

Jun. 2022 - Jan. 2023

- Researched the possibility of an attack on networks that use the combination of PoS-based protocols and DAG-based network protocols, to prove that using this combination in deployments such as SPECTRE is insecure.

Teaching Experience

UNIVERSITY OF WATERLOO

Mentor WOMEN+ IN MATH, DIRECTED READING/RESEARCH PROGRAM

Jan. 2024 - present

Guest Lecturer CS489/698: PRIVACY, CRYPTOGRAPHY, DATA SECURITY, PROF. D. BARRADAS

Jul. 2024

Teaching Assistant CS459: PRIVACY, CRYPTOGRAPHY, DATA SECURITY, DR. A. KATI

Sep. 2024 - present

Teaching Assistant CS489/698: PRIVACY, CRYPTOGRAPHY, DATA SECURITY, PROF. D. BARRADAS
Teaching Assistant CS456: COMPUTER NETWORKS, PROF. N. LIMAM

May. 2024 - Aug. 2024

Jan. 2024 - May. 2024

UNIVERSITY OF TEHRAN

Supervising Teaching Assistant DISCRETE MATHEMATICS, PROF. S. MOHAMMADI Sep. 2021 - Aug. 2022
Mentor CRYPTOCURRENCIES, SUMMER OF CODE Jul. 2021 - Nov. 2021
Teaching Assistant DISCRETE MATHEMATICS, PROF. S. MOHAMMADI Jan. 2020 - Sep. 2021
Teaching Assistant COMPUTER NETWORKS, PROF. N. YAZDANI Aug. 2022 - Jan. 2023
Teaching Assistant DATA STRUCTURES, PROF. H. FAILI, PROF. F. FAGHIH Sep. 2020 - Aug. 2022
Teaching Assistant SOFTWARE ENGINEERING, PROF. R. KHOSRAVI Aug. 2022 - Jan. 2023
Teaching Assistant SOFTWARE TESTING, PROF. E. KHAMESPANAH Aug. 2022 - Jan. 2023
Teaching Assistant ARTIFICIAL INTELLIGENCE, PROF. M. MORADI, PROF. Y. YAGHOOBZADEH, H. FADAEI Jan. 2021 - Aug. 2022

Honors & Awards

2024 **Featured on**, CPI Student Newsletter Student Spotlights of November 2024 Waterloo, ON
2024 **Top Poster**, CPI Conference 2024 Waterloo, ON
2024 **Featured on**, CPI Student Newsletter Student Spotlights of June 2024 Waterloo, ON
2024 **Gained access**, RWC 2024 for volunteering Waterloo, ON
2024 **Received scholarship**, WiM Mentorship Award Waterloo, ON
2023 **Received scholarship**, International Master's Award of Excellence Waterloo, ON
2020 **President**, University of Tehran ACM Student Chapter Tehran, Iran
2018 **Ranked Top 0.1% in Konkour**, National Organization of Educational Testing (NOET) Tehran, Iran
2018 **Received scholarship**, Supporter Foundation of the University of Tehran Tehran, Iran

Professional Service

2024 **External Reviewer**, IEEE Network Operations and Management Symposium (NOMS) 2025 Waterloo, ON

Professional Developments

Switcharoo University of Waterloo

MIX-NETS ON PROGRAMMABLE SWITCHES

Jan. 2024 - Jul. 2024

- Researched implementing mix-nets at a switch level. Previous work had focused on implementing basic cryptography and packet chaffing, but the final piece, introducing arbitrary delays, was missing. We focused on introducing novel ways to add packet delays using smart switches.

Finger Printing GitHub Repositories University of Waterloo

I KNOW WHAT YOU CLONED LAST SUMMER

Apr. 2024 - Dec. 2024

- Researched fingerprinting the traffic generated by cloning and interacting with GitHub repositories. Our preliminary results were promising, with an accuracy upwards of 95% on closed-world attacks.

Bitcoin and Cryptocurrency Technologies, Prof. Arvind Narayanan Princeton University, Coursera

AN ONLINE CRYPTOCURRENCY COURSE

2020 - 2021

- During this course, which was part of the master's program at Princeton University, I learned fundamental concepts regarding Bitcoin and other cryptocurrencies. I learned about how they achieve decentralization(!), how mining is done, alternative consensus protocols, etc. During this course, I implemented a simple blockchain network.

Crystalline University of Tehran

A CRYPTOCURRENCY POWERED BY A REDEFINED POA PROTOCOL

Aug. 2021 - Sep. 2022

- Developed as a proof of concept on pure Python, this cryptocurrency incorporates a newly defined Proof of Activity as its primary consensus protocol. It was designed and researched by me and several other students of the University of Tehran.

DMCB University of Tehran

THE MODERATOR FOR DM CONTESTS OF UNIVERSITY OF TEHRAN

Jun. 2022 - Aug. 2022

- Developed as a moderator for the discrete mathematics course at the University of Tehran. DMCB was created using the Django framework.

Mini Kaggle

Divar

A KAGGLE CLONE MADE BY INTERNS AT DIVAR

Jun. 2021 - Sep. 2021

- A Kaggle clone made using the Django framework as a learning project at Divar in the summer of 2021. We used several software developing tools and libraries including Docker, Celery, Pandas, and etc. I learned how to effectively work as a software development team during this time.

Sins & Virtues

University of Tehran

A TEXT-BASED GAME CREATED AS A PASSION PROJECT

Feb. 2021 - present

- Developed as a passion project. At first, it was programmed using Python, but after further consideration, it was rewritten using C++. The game encapsulates a rich set of fun mechanics. Follow this link to learn more.

Work Experience

Sotoon

Tehran, Iran

SOFTWARE DEVELOPER

Jan. 2022 - Aug. 2022

- Worked on deploying older software on Docker Swarm and Kubernetes clusters. Worked on the official "Sooton Cli" programmed using GoLang. Learned a great deal about working as a team in software development and the agile methodology.

Divar

Tehran, Iran

SOFTWARE DEVELOPER INTERN

Jul. 2021 - Sep. 2021

- Learned a wide variety of software development tools in the workshops held by Divar. Some of these tools were Git(Professional), RPC protocols, Django Framework, Kubernetes, SQL, NO-SQL databases, etc. Furthermore worked on a small project in which we developed a Kaggle clone from scratch.

Notable Academic Projects

Smart Debt Handler

Cryptocurrency

A SMART CONTRACT MADE USING SOLIDITY

A smart debt handler similar to Splitwise, which tracks users' debts and updates them based on the loops users create between each other.

BTC Address Maker

Cryptocurrency

AN ADDRESS MAKER MADE USING PURE PYTHON

This project was developed to further understand the math and explicit details of creating a key pair. This project can make any kind of famous key pairs in either the test net or the main net.

Network Function Simulation

Computer Networks

A SIMULATION OF NETWORK FUNCTIONS

A complete simulation of network functions created using C++. It supports various network components and uses multi-threading to run the simulations simultaneously.

Multi-Threaded Prediction

Computer Networks

A MULTI-THREADED C PROGRAM THAT PREDICTS PRICES BASED ON TRAINED REGRESSION DATA

This project was created to toy with multi-threading concepts and to get more familiar with them.

Skills

Programming

High Intermediate: C++, Python, GoLang
Intermediate: C, Java, Javascript, Solidity
Beginner: Rust, Bash, LaTeX

Technologies

Git, Docker, Docker Swarm, Kubernetes, Ansible, Makefile

Software Engineering

Familiar with multiple object-oriented design patterns. Efficient with function-based designs. Fully familiar with Agile development and its concepts.

Web Development

Django, Django Rest, React, Spring

Operating Systems

Linux (Debian-based and Arch-based), MacOS

Languages

Persian Native

English Professional working proficiency · TOEFL: 113/120 [R:30, L:30, S: 26, W:27] (Oct. 2022)