

Alessandro Baccarini

Curriculum Vitae

Contact Information

✉ Email abaccarini@proton.me
🌐 Website abaccarini.github.io
🌐 LinkedIn alessandro-baccarini
🐙 GitHub abaccarini
📄 Scholar [1150 citations, May 2025](#)

Research Interests

My interests span across areas of information security, applied cryptography, and privacy-enhancing technologies. Concretely, I design and implement protocols for secure multi-party computation (MPC) and its application to privacy-preserving machine learning, compliance monitoring, and outsourcing. I simultaneously investigate mechanisms for quantifying private information leakage from secure computation. I am also interested in post-quantum cryptographic techniques.

Education

PhD, Computer Science, University at Buffalo Aug. 2024
Advisor: Marina Blanton
MS, Cybersecurity, Fordham University May 2019
Advisor: Thaier Hayajneh
BS, Physics, Fordham University May 2017
Minor, Mathematics

Work Experience

Cryptography Researcher, Contractor Sept. 2024 – Dec. 2024
Blockchain R&D Organization
Research Assistant, Computer Science Jun. 2019 – Aug. 2024
University at Buffalo
Teaching Assistant, Computer Science Jan. 2020 – May 2022
University at Buffalo
Adjunct Assistant Professor, Physics Aug. 2017 – May 2019
Fordham University
Graduate Research Assistant, Cybersecurity Aug. 2017 – May 2019
Fordham University

Awards and Recognition

Alan Selman Scholarship, University at Buffalo

Mar. 2024

First place \$2000 cash prize, focus in theoretical computer science.

GSAS Centennial Scholarship, Fordham University

Aug. 2017 – May 2019

Full Tuition support and stipend (academic year + summer).

Projects and Experience

Threshold Decryption for FHE

Sept. 2024 – Dec. 2024

Blockchain R&D Organization

- Analyzed distributed threshold decryption protocols for multi-party fully homomorphic encryption (FHE) schemes with applications in blockchain-based environments.
- Developed and evaluated an actively secure threshold decryption construction based on Shamir secret sharing over Galois rings in C++, yielding an up to $4\times$ performance improvement over prior works while maintaining robust security guarantees.
- Designed a threshold FHE distributed key generation protocol for an arbitrary underlying multi-party scheme, alongside developing a corresponding MP-SPDZ implementation.

PICCO Compiler

2022 – Present

University at Buffalo

[Repository](#)

- Core developer and maintainer of PICCO, a source-to-source MPC compiler library used to translate general-purpose programs into their secure implementations for deployment in a distributed setting.
- Extensively optimized existing field-based protocol implementations, while simultaneously performing a large-scale refactor to improve future maintainability and add support for stronger security settings.
- Implemented new ring-based protocol constructions to enable general-purpose computation over integer and floating-point inputs.
- Mentored REU students tasked with optimizing the compiler's networking functionalities, along with developing a web interface for entering private inputs and retrieving outputs of secure computation.

MPC and Privacy-Preserving Machine Learning

2020 – 2023

University at Buffalo

[Repository](#)

- Designed a comprehensive ring-based framework of replicated secret sharing multi-party protocols for an arbitrary number of parties in the semi-honest (passively secure), honest majority setting.
- Implemented protocol constructions in C++ and extensively benchmarked our framework, obtaining an up to $33\times$ performance gain over existing state-of-the-art secret sharing techniques.
- Applied techniques to privacy-preserving machine learning tasks, including (quantized) neural network inference and support vector machine classification.
- Discovered a novel layer optimization for secure quantized neural network inference that significantly improved efficiency and led to an over $2\times$ improvement over prior works.

Secure Computation Information Disclosure Analysis

2021 – Present

University at Buffalo

[Repository](#)

- Designed a novel information-theoretic approach for evaluating the information disclosure about private inputs from secure computation outputs.
- Comprehensively analyzed a practically significant statistical function (the average salary) through extensive theoretical and analytical analysis in a variety of computational configurations.
- Leveraged this methodology in conjunction with machine learning-based entropy estimation techniques to quantify the information leakage from complex descriptive statistical measures.
- Awarded first place \$2000 Alan Selman Scholarship for theoretical computer science for this work.

Blockchain Applications in Healthcare

2017 – 2019

Fordham University

- Led the design of one of the first frameworks that fused blockchain and healthcare into a HIPAA-compliant IoT remote patient monitoring system, based on the Ethereum protocol.
- Assisted in prototype smart contract development in Solidity to support real-time automated monitoring.

Significant Course Projects

Implementation and Analysis of the Apple PSI System

2021

University at Buffalo, *Security and Privacy in IoT*

[Repository](#)

- Developed a modified variant of Apple's private set intersection (PSI) system in Python to obliviously detect harmful media within a database through neural network-based perceptual hash functions.
- Implemented various necessary cryptographic primitives to build the framework, including secret sharing of private keys, HMAC key derivation and pseudorandom functions, and Diffie-Hellman group construction.

Quantum Secret Sharing of Classical Information

2020

University at Buffalo, *Applied Cryptography and Computer Security*

[Repository](#)

- Analyzed the Hillery-Buek-Berthiaume quantum secret sharing protocol of classical information, and implemented the construction in IBM's Python Qiskit framework.

Publications

Thesis

- [1] **Alessandro Baccarini**. *New Directions in Secure Multi-Party Computation: Techniques and Information Disclosure Analysis*. PhD thesis, University at Buffalo, 2024.

Conference Proceedings

- [2] **Alessandro Baccarini**, Marina Blanton, and Shaofeng Zou. Understanding information disclosure from secure computation output: A study of average salary computation. In *ACM Conference on Data and Application Security and Privacy (CODASPY)*, pages 187–198, 2024.

- [3] **Alessandro Baccarini** and Thaier Hayajneh. Evolution of format preserving encryption on IoT devices: FF1+. In *Hawaii International Conference on System Sciences (HICSS)*, pages 1628–1637, 2019.
- [4] Abdullah Alhayajneh, **Alessandro Baccarini**, and Thaier Hayajneh. Quality of service analysis of VoIP services. In *IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 812–818, 2018.

Refereed Journals

- [5] **Alessandro Baccarini**, Marina Blanton, and Shaofeng Zou. Understanding information disclosure from secure computation output: A comprehensive study of average salary computation. *ACM Transactions on Privacy and Security (TOPS)*, 28(1):1–36, 2024.
- [6] **Alessandro Baccarini**, Marina Blanton, and Chen Yuan. Multi-party replicated secret sharing over a ring with applications to privacy-preserving machine learning. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2023(1):608–626, 2023.
- [7] Abdullah Alhayajneh, **Alessandro Baccarini**, Gary Weiss, Thaier Hayajneh, and Aydin Farajidavar. Biometric authentication and verification for medical cyber physical systems. *Electronics*, 7(12):436, 2018.
- [8] Kristen Griggs, Olya Ossipova, Christopher Kohlios, **Alessandro Baccarini**, Emily Howson, and Thaier Hayajneh. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of Medical Systems*, 42(7):130, 2018.

Technical Presentations

- | | |
|--|-----------|
| • RAND Corporation, Engineering & Applied Sciences Dept. Virtual. | Apr. 2025 |
| • Intel Labs, Security & Privacy Research Group. Virtual. | Mar. 2025 |
| • Riverside Research, Secure & Resilient Systems Group. Lexington, MA. | Feb. 2025 |
| • MITRE Corporation, Cyber for Identity Trust & Assurance Dept. Virtual. | Jan. 2025 |
| • ACM CODASPY 2024. Porto, Portugal. | June 2024 |
| • PETS 2023. Lausanne, Switzerland. | July 2023 |
| • Great Lakes Security Day, RIT. Rochester, NY. | Apr. 2023 |
| • IEEE UEMCON 2018. New York, NY. | Nov. 2018 |

Professional Service

Conference Committees

- | | |
|--|------------|
| IEEE Symposium on Security and Privacy, poster jury | 2025 |
| USENIX Security Symposium, artifact evaluation committee | 2023, 2024 |

Refereeing

- Journal of Computer and System Sciences (JCSS)
- IEEE Transactions on Information Forensics and Security (TIFS)

IEEE Transactions on Dependable and Secure Computing (TDSC)
European Symposium on Research in Computer Security (ESORICS)
IEEE/ACM International Conference on Automated Software Engineering (ASE)
Multidisciplinary Digital Publishing Institute (MDPI) Entropy, Sensors, Symmetry, Information
Hawaii International Conference on System Sciences (HICSS)

Technical Skills

Cryptographic secure multi-party computation, secret sharing, homomorphic encryption, lattice cryptography, zero-knowledge proofs, differential privacy, information theory

Languages C/C++, Python, Rust, Bash, Lua, \LaTeX

Developer Version control (Git, SVN), CMake, Make, GDB, Valgrind, Neovim, VS Code

Platforms Docker, AWS EC2, GitHub, HPC Clustering, Linux, Unix, Windows

Libraries GMP, GMPFR, GSL, STL, OpenSSL, SageMath, MP-SPDZ, NumPy, Pandas, SciPy, Matplotlib, TensorFlow

Teaching

At the **University at Buffalo**:

CSE 116 Computer science II (Instructor)	2 semesters
CSE 4/529 Algorithms for Modern Computing Systems (TA)	3 semesters
CSE 4/531 Analysis of Algorithms (TA)	1 semester
CSE 542 Software Engineering Concepts (TA)	1 semester

At **Fordham University**:

PHYS 1511/12 Physics I/II Lab (Instructor)	4 semesters
--	-------------