Alessandro Baccarini

Curriculum Vitae

Contact Information

Email		abaccarini@proton.me
Website		abaccarini.github.io
LinkedIn		alessandro-baccarini
GitHub		abaccarini
Scholar		1132 citations, April 2025

Research Interests

My interests span across areas of information security, applied cryptography, and privacy-enhancing technologies. I design and implement protocols for secure multi-party computation (MPC) based on secret sharing for a variety of practical applications, such as privacy-preserving machine learning, sustainability, and outsourcing. Additionally, I research how to quantify information disclosure from arbitrary secure function evaluations through information-theoretic approaches. I am also interested in quantum-resilient 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 — Sep. 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 — 2017 – 2019
Full tuition support and stipend (academic year + summer).

Projects and Experience

Threshold Decryption for FHE — Sep. 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× 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.

MPC and Privacy-Preserving Machine Learning — 2020 – Present
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× 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 an algebraic optimization for secure quantized neural network inference that significantly improved efficiency and led to an over 2× improvement over prior works.

PICCO Compiler — 2022 – Present
University at Buffalo — Repository

- Core developer and maintainer of *PICCO*, a source-to-source compiler 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 support extensibility to stronger security settings.
- Integrated ring-based protocol constructions into the compiler to support general-purpose computation over integer and floating-point inputs.
- Mentored two 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.

Information Disclosure Analysis from Secure Function Evaluation 2021 – Present
University at Buffalo Repository

- Designed a novel information-theoretic approach for evaluating the information disclosure about private inputs from the output of secure function evaluations.
- 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 data-driven techniques to quantify the information leakage of complex descriptive statistical measures.
- Awarded first place $2000 cash prize from the 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.

Talks and Presentations

- *Understanding Information Disclosure from Secure Computation Output: Analytical and Data-Driven Analysis*. The RAND Corporation. Virtual. April 16, 2025.
- *Understanding Information Disclosure from Secure Computation Output: Analytical and Data-Driven Analysis*. Intel Labs. Virtual. March 11, 2025.
- *Secure Multi-party Computation for Privacy-preserving Machine Learning*. Supra. Virtual. February 13, 2025.
- *New Directions in Secure Multi-party Computation: Techniques and Information Disclosure Analysis*. Riverside Research. Lexington, MA. February 5, 2025.
- *Secure Multi-party Computation for Privacy-preserving Machine Learning*. The MITRE Corporation. Virtual. January 27, 2025.
- *Understanding Information Disclosure from Secure Computation Output: A Study of Average Salary Computation*. ACM CODASPY. Porto, Portugal. June 20, 2024.
- *Multi-Party Replicated Secret Sharing over a Ring with Applications to Privacy-Preserving Machine Learning*. Privacy Enhancing Technologies Symposium. Lausanne, Switzerland. July 11, 2023.
- *Understanding Information Disclosure from Secure Computation Output: A Study of Average Salary Computation*. Great Lakes Security Day. Rochester, NY. April 21, 2023.

Professional Service

Conference Committees

IEEE Symposium on Security and Privacy, poster program committee 2025

USENIX Security Symposium, artifact evaluation committee 2023, 2024

Refereeing

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, learning-with-errors, differential privacy, information theory

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

Developer Git, SVN, CMake, GDB, Neovim, VS Code, Unix

Libraries GMP, GMPFR, GSL, SageMath, OpenSSL, NumPy, 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