






# ALESSANDRO BACCARINI

## *Curriculum Vitae*

### CONTACT INFORMATION

	Email	<a href="mailto:abaccarini@proton.me">abaccarini@proton.me</a>
	Website	<a href="https://abaccarini.github.io">abaccarini.github.io</a>
	Telegram	<a href="https://t.me/alessandro_baccarini">alessandro_baccarini</a>
	LinkedIn	<a href="https://www.linkedin.com/in/alessandro-baccarini">alessandro-baccarini</a>
	GitHub	<a href="https://github.com/abaccarini">abaccarini</a>

### 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

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

### WORK EXPERIENCE

<b>Research/Teaching Assistant</b> , Computer Science University at Buffalo	Jun. 2019 – July 2024
<b>Adjunct Assistant Professor</b> , Physics Fordham University	Aug. 2017 – May 2019
<b>Graduate Research Assistant</b> , Cybersecurity Fordham University	Aug. 2017 – May 2019

## AWARDS AND RECOGNITION

<b>Alan Selman Scholarship</b> , University at Buffalo First place \$2000 cash prize, focus in theoretical computer science.	Mar. 2024
<b>GSAS Centennial Scholarship</b> , Fordham University Tuition support, stipend for both academic years and summer semesters.	2017 – 2019

## PUBLICATIONS

### Thesis

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

### Conference Proceedings

- [2] **A. Baccarini**, M. Blanton, and S. Zou. Understanding Information Disclosure from Secure Computation Output: A Study of Average Salary Computation. *ACM Conference on Data and Application Security and Privacy (CODASPY)*, pages 187–198, 2024.
- [3] **A. Baccarini**, M. Blanton, and C. Yuan. Multi-Party Replicated Secret Sharing over a Ring with Applications to Privacy-Preserving Machine Learning. In *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2023(1):608-626, and in *Privacy Enhancing Technologies Symposium (PETS)*<sup>†</sup>, 2023.
- [4] **A. Baccarini** and T. Hayajneh. Evolution of Format Preserving Encryption on IoT Devices: FF1+. In *Hawaii International Conference on System Sciences (HICSS)*, pages 1628–1637, 2019.
- [5] A. Alhayajneh, **A. Baccarini**, and T. Hayajneh. Quality of Service Analysis of VoIP Services. In *IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 812–818, 2018.

### Refereed Journals

- [6] **A. Baccarini**, M. Blanton, and S. Zou. Understanding Information Disclosure from Secure Computation Output: A Comprehensive Study of Average Salary Computation. *ACM Transactions on Privacy and Security (TOPS)*, to appear.
- [7] A. Alhayajneh, **A. Baccarini**, G.M. Weiss, T. Hayajneh, and A. Farajidavar. Biometric Authentication and Verification for Medical Cyber Physical Systems. *Electronics*, 7(12):436, 2018.

---

<sup>†</sup>PETS is a conference that switched to organizing accepted papers in journal-style volumes and issues. It is currently listed as a journal in DBLP

- [8] K.N. Griggs, O. Ossipova, C.P. Kohlios, **A. Baccarini**, E.A. Howson, and T. Hayajneh. Health-care Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems*, 42(7):130, 2018.

## RESEARCH PROJECTS

### **MPC and Privacy-Preserving Machine Learning** University at Buffalo

2020 – Present  
[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 an algebraic optimization for secure quantized neural network inference that significantly improved efficiency and led to an over  $2\times$  improvement over prior works.

### **PICCO Compiler** University at Buffalo

2022 – Present  
[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 a summer REU student tasked with optimizing the compiler’s networking functionalities.

### **Disclosure Analysis from Secure Function Evaluation** University at Buffalo

2021 – Present  
[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.
- Applied our framework to complex descriptive statistical functions in conjunction with data-driven techniques to estimate the information disclosure.

## **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.

## **RELEVANT COURSE PROJECTS**

### **Implementation 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 obviously 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.

## **PROFESSIONAL SERVICE**

### **Conference Committees**

USENIX Security Symposium, artifact evaluation committee member

2024

USENIX Security Symposium, artifact evaluation committee member

2023

### **Conference and Journal 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, differential privacy, encryption, signatures and commitments, zero-knowledge proofs  
**Languages** C/C++, Python, Bash, Lua, Solidity, ~~TeX~~  
**Developer** Git, SVN, Neovim, VS Code, Unix  
**Libraries** GNU MP and MPFR, 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	3 semesters
CSE 4/531 Analysis of Algorithms	1 semester
CSE 542 Software Engineering Concepts	1 semester

At **Fordham University**:

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