Oliwia M. Kempinski

100 Florida Ave NE #1110, Washington, DC 20002
Nr.: +1 (973) 592-2098 Email: oliwia1406@gmail.com

EDUCATION

Doctor of Philosophy (Ph.D.), Computer Science
University of Maryland, College Park (Expected Graduation: May 2029)
Research: Programming Languages and Cryptography, focusing on secure DSLs, Zero-Knowledge Proofs, and blockchain applications
GPA: 4.00

Bachelor of Science (B.S.), Mathematical Finance (Minor: Computer Science)
Seton Hall University, Stillman School of Business (Graduated: May 2024)
GPA: 3.99

PUBLICATIONS (peer-reviewed)

Cryptographic personas: Responsible pseudonyms without de-anonymization. ***IEEE S&P*, 2026**
R. Woelfel, **O. Kempinski**, H. Kailad, E. Shroyer, I. Miers, G. Kaptchuk
Under review at *IEEE Symposium on Security and Privacy*, 2026.

Design Support for Multitape Turing Machines. ***TFPiE*, 2025**
M. Morazán, **O. Kempinski**, A. Garced
Presented at *Trends in Functional Programming in Education*, 2025.

The Implementation of FSM Computation Graphs for Students. ***IFL*, 2024**
M. Morazán, **O. Kempinski**, A. Garced
Presented at the *International Symposium on Implementation and Application of Functional Languages*, 2024.

Visualizing Composed Turing Machines. ***SPLASH*, 2024**
M. Morazán, T. Minić, **O. Kempinski**
Presented at the *ACM SIGPLAN Conference on Systems, Programming, Languages, and Applications: Software for Humanity*, 2024.

Using Computation Graphs to Explain Nondeterminism to Students. ***SPLASH*, 2024**
M. Morazán, **O. Kempinski**
Presented at the *ACM SIGPLAN Conference on Systems, Programming, Languages, and Applications: Software for Humanity*, 2024.

Visualizing Why Nondeterministic Finite-State Automata Reject. ***ICFP*, 2023**
O. Kempinski, M. Morazán
Presented at the *ACM International Conference on Functional Programming*, 2023.

RESEARCH PROJECTS

Featherweight ZK **2025 – Present**

- Designing a domain-specific language for zero-knowledge proofs with information-flow control and cost analysis, extending programming-languages theory to cryptographic applications
- Building a Rocq (formerly Coq) mechanization of the type system proving termination-insensitive noninterference, and developing a compiler backend targeting Noir circuits for deployment as a local language within Pirouette, enabling secure endpoint projections
- Exploring future impact: Potential to extend verification beyond today's local-only smart-contract semantics, by introducing a framework for global reasoning about blockchain choreographies that proves multi-party security and privacy properties and projects them to verifiable local behavior using zero-knowledge proofs

zk-AML (Anti-Money Laundering) **2025 – Present**

- Designing privacy-preserving AML compliance protocols using zk-promises to prove regulatory checks without revealing transaction details
- Developing multiple propagation mechanisms to ensure liveness even when participants drop offline, including distributed manager-assisted recovery and witness-encryption-based callback propagation
- Formalizing trust assumptions and message-passing guarantees, balancing regulatory accountability with cryptographic anonymity for multi-party financial systems

AI Security in Encrypted Messaging **2025 – Present**

- Investigating security risks of LLM-based assistants in end-to-end encrypted platforms, analyzing whether conversation summarization leaks sensitive user context
- Exploring patterns-of-life attacks and conducting black-box spear-phishing experiments to measure if leaked summaries suffice for target reconstruction and persona inference

Cryptographic Personas **2025**

- Proposed a new framework for responsible pseudonyms in end-to-end encrypted messaging systems (e.g., Signal) without de-anonymization, and integrated protocol into a prototype client-server system
- Implemented zk-promises, enabling anonymous commitments and callback verification, and extended it with support for folding proofs and Privacy Pass-style precomputation to improve scalability

FSM (Finite State Machines) **2022 – 2024**

- Co-developed FSM, an educational programming language for the Automata Theory classroom, designed to help students visualize and simulate finite-state machines
- Supported deployment and curriculum integration; FSM is now used for teaching across multiple universities

RELEVANT EXPERIENCE

Computer Science Research Assistant **2022 – Present**

- Conducted research in Programming Languages and Cryptography, contributing to the projects mentioned above

Computer Science Teaching Assistant **2022 – 2025**

- Tutored, graded, and delivered recitations for introductory CS courses and upper-level Programming Languages courses
- Provided group and one-on-one support to students, and oversaw other student tutors
- Presented research on state-based machines to an upper-level Automata Theory class as guest speaker at University of Lisbon

President of Association for Computing Machinery (ACM) Chapter at Seton Hall University **2023 – 2024**

- Tasked with starting the chapter at Seton Hall University

GRANTS, HONORS & AWARDS

- Member of Beta Gamma Sigma, the International Business Honors Society 2023 – Present
- Member of the National Society of Collegiate Scholars 2023 – Present
- Seton Hall University Academic Scholarship 2020 – 2024
- Seton Hall University Athletic Scholarship 2020 – 2024
- Stillman School of Business Mutual Benefit Life Scholarship 2023
- Mendoza Global Ambassador Program Scholarship 2023
- PLMW $500.00 (*ICFP* 2023) 2023
- ACM SIGPLAN $1,500.00 (*ICFP* 2023) 2023
- Big East Conference All-Academic Team 2021 – 2023
- Seton Hall University Dean's List 2021 – 2023
- ITA Scholar-Athlete 2021 – 2023
- Scholar Athlete of the Year 2021

VARSITY AND SPORT EXPERIENCE

Division 1 Varsity Women's Tennis Team, Big Ten Conference, University of Maryland **2024 – 2025**
Division 1 Varsity Women's Tennis Team, Big East Conference, Seton Hall University **2020 – 2024**

- Devoted 25+ hours every week to practicing, conditioning, mental training, team bonding, competing and traveling while maintaining a full academic course load
- Represented Seton Hall's and University of Maryland's Women's Tennis Program as student-athlete
- Played as number 1 seated player of the Seton Hall team, assuming the leader's position

SKILLS

- Languages: German, Polish (native); English, Spanish (fluent); Latin (proficient)
- Programming Languages: Rust, Rocq (formerly Coq), Racket, FSM, Haskell, Dafny, Python, Java, Mathematica
- Cryptography: RISC Zero, Noir, Arkworks, Groth16, PLONK, Solidity

VOLUNTEER WORK

Virtualization Chair Volunteer at *ICFP* 2023 **2023**

- Monitored the virtual platforms of the conference as virtualization chair

Member of a Highly Gifted High School Program at Markgraefin-Wilhelmine-Gymnasium Bayreuth, Germany **2012 – 2020**

- Selected through 3 competitive admission exams (incl. IQ testing) at age 10 for an accelerated program for highly gifted students
- Completed rigorous advanced curriculum, participated in research projects and competitions, and engaged in community service (e.g., forensic psychiatry, youth mentoring, environmental projects)

Piano Player in Church **2012 – 2020**

- Volunteered to perform in church in Germany before moving to the U.S.