Ioannis Kaklamanis

Email
Homepage
LinkedIn
Google Scholar

Education

- **Yale University** — New Haven, CT
  PhD Student in Computer Science — *May 2029 (Expected)*

  Coursework: Post-Quantum Cryptography, Zero-Knowledge Proofs, Real-World Cryptography, Cryptography and Computation, Computer Networks

- **Massachusetts Institute of Technology** — Cambridge, MA
  Master of Engineering in Electrical Engineering and Computer Science — *June 2023*
  GPA: 5.0/5.0
- **Massachusetts Institute of Technology** — Cambridge, MA
  Bachelor of Science in Computer Science and Engineering — *May 2022*
  Bachelor of Science in Mathematics
  GPA: 4.7/5.0

  Coursework: Cryptography and Cryptanalysis (G), Applied Cryptography and Security (G), Distributed Algorithms (G), Advanced Complexity Theory (G), Seminar in Discrete Mathematics, Advances in Computer Vision

Experience

- **Yale Graduate School of Arts and Sciences** — New Haven, CT
  Graduate Researcher; Yale Applied Cryptography Laboratory — *August 2023 - present*
  Advisor: Prof. Fan Zhang
  - Verifiable Aggregate Receipts protocols, with applications to user engagement auditing.
  - Censorship Resistance vs Throughput in Multi-Proposer BFT protocols.
  - Cross-chain interoperability protocols, with a focus on cross-rollup composability.
  - Single sign-on (SSO) protocols with anonymity and unlinkability guarantees.
  - Single Secret Leader Election (SSLE) protocols with accountability.
  - Registration-based Encryption.

- **Chainlink Labs** — New Haven, CT (remote)
  Research Intern — *June - October 2025*
  Mentor: Dr. Gregory Neven
  - Designed an identity system using the Chainlink Confidential Compute service as a “credential re-certifier”.
  - The system enables on-chain credentials that maintain user privacy and unlinkability.

- **Yale CPSC 364 (Blockchains) and CPSC 467 (Cryptography)** — New Haven, CT
  Teaching Fellow — *September - December 2023; January - May 2025*
  - Grading problem sets and exams, writing problems for problem sets and exams, holding office hours.

- **MIT class “Mathematics for Computer Science”** — Cambridge, MA
  Teaching Assistant — *September 2021 - May 2022; January - May 2023*
  - Taught two recitations per week, graded exams, wrote problems for problem sets and exams, held office hours.

- **MIT CSAIL: Networks and Mobile Systems Group** — Cambridge, MA
  Graduate Research Assistant (June 22 - May 23); Undergraduate Researcher (Feb - May 22) — *February 2022 - May 2023*
  Advisor: Prof. Mohammad Alizadeh
  - Demonstrated leader bottleneck in HotStuff, a state-of-the-art leader-based BFT consensus protocol.
  - Designed and implemented protocols for fault-tolerant broadcast in bandwidth-constrained networks.

- **MathWorks Engineering Development Group (EDG)** — Somerville, MA (remote)
  Software Engineering Intern — *June - August 2021*

- Created a Product Suggestion Service using Machine Learning and Deep Learning models (LSTM, BERT, SVM)

- **MIT Computer Science and Artificial Intelligence Lab (CSAIL)** Athens, Greece (remote)
  Undergraduate Researcher; Project: Decoding the Language of Non-Human Species *July - December 2020*
  - Developed and used Deep Learning algorithms to process sounds made by whales.
  - Created end-to-end pipeline for automatic source separation to attribute sounds to whales.

Publications, Preprints & Awards

- F Elsheimy*, **I Kaklamanis***, S Wadhwa*, C Papamanthou, and F Zhang. *Censorship Resistance vs Throughput in Multi-Proposer BFT Protocols.* 2026. Cryptology ePrint Archive, Paper 2026/126. https://eprint.iacr.org/2026/126
- **I Kaklamanis**, W Wang, H Malvai, and F Zhang. *Verifiable Aggregate Receipts with Applications to User Engagement Auditing.* 2025. Cryptology ePrint Archive, Paper 2025/2330. https://eprint.iacr.org/2025/2330
- J Alupotha, M Barbaraci, **I Kaklamanis**, A Rawat, C Cachin, and F Zhang. *Anonymous Self-Credentials and their Application to Single-Sign-On.* 2025. Cryptology ePrint Archive, Paper 2025/618. https://eprint.iacr.org/2025/618
- **Ioannis Kaklamanis** and Fan Zhang. *CRATE: Cross-Rollup Atomic Transaction Execution.* 2025. arXiv: https://doi.org/10.48550/arXiv.2502.04659
- **I. Kaklamanis**, L. Yang, and M. Alizadeh. 2022. Poster: Coded Broadcast for Scalable Leader-Based BFT Consensus. ACM SIGSAC Conference on Computer and Communications Security (CCS '22). https://doi.org/10.1145/3548606.3563494
- Boquila (Unlinkable User Single Sign-On) was the winning project of the 2024 IC3 Blockchain Camp Hackathon.
- MEng Thesis: Fault Tolerant Broadcast in Bandwidth-Constrained Networks

Service

- Sub-reviewer for:
  - Asiacrypt 2024
  - USENIX 2025
  - TCC 2025
  - Eurocrypt 2026
  - CRYPTO 2026

Skills and Interests

- **Languages**: Proficient in Greek, English, French. Working knowledge of Spanish.
- **Technical**: Python, Go, Java, Rust, C++, LaTeX, Javascript, Circom, Noir
- **College Activities**: Alpha Delta Phi, GEL, UPOP