Nicholas Jankovic

nickjankovic@gatech.edu • nickjankovic.com

SUMMARY

First-year PhD student at the Georgia Institute of Technology advised by Prof. Vassilis Zikas. Previously received a Bachelor's in Computer Science and Applied Mathematics at Brown University, where I worked with Prof. Anna Lysyanskaya. My interests lie in theoretical cryptography, with previous work on anonymous credentials and ongoing research in secure multi-party computation and post-quantum zero-knowledge proofs.

EDUCATION

Georgia Institute of Technology (PhD) Expected Graduation: May 2031

- Pursuing a PhD under advisor Vassilis Zikas; School of Cybersecurity and Privacy
- Awarded the GT Presidential Fellowship

Brown University (Bachelor's) Graduated: May 2026

- GPA of 4.0/4.0; departmental honors; awarded Senior Prize in Computer Science
- Double concentrating in Computer Science (B.S.) and Applied Mathematics (B.A.)
- Relevant Coursework: Theoretical Cryptography, Mathematical Cryptography, Applied Cryptography, Abstract Algebra, Real Analysis, Theory of Computation, Proof Assistants for Projective Geometry, Quantum Physics, Differential Eqs

International School Bangkok (Thailand – IB Curriculum) Graduated: May 2022

- Full IB score of 45/45 and full SAT superscore of 1600/1600

RESEARCH EXPERIENCE

Two-Round Secure Multi-Party Computation with Abort in the Asynchronous Setting Current

- Ongoing with Prof. Vassilis Zikas: can a new definition of asynchrony support secure-with-abort MPC without input loss from honest parties?

Collaborative zk-SNARKs from Post-Quantum Assumptions Current

- Ongoing with Prof. Alex Ozdemir: can a post-quantum polynomial commitment be devised for the multiparty setting?

"Non-Interactive Threshold Mercurial Signatures with Applications to Threshold DAC" Spring 2025 - Fall 2026

- Co-authored with Anna Lysyanskaya, Scott Griffy, and Arup Mondal
- Extended existing mercurial signature to create the first non-interactive threshold mercurial signature
- Further modified construction to realize threshold delegatable anonymous credentials, proving security of modifications
- Primary author of the unforgeability and pk class-hiding proofs for the extended signature scheme in the generic group model, a task that was highly non-trivial and amounted to over 30 pages of appendix material
- Pre-print of paper available here

"Temperature, Frequency, and Young's Modulus of a Ching" 2021

- Worked with mentor in high school to develop physics project, collect data, write paper, and undergo editing process
- Research demonstrates validity of a new method to determine the elasticity constant of certain metals
- Published in the International Scholastic Journal of Science

WORK EXPERIENCE

Cryptography Head TA — Brown University Fall 2025

- Head TA for Prof. Anna Lysyanskaya's Introduction to Cryptography course for undergrad and grad students
- Selected and designed homework/exam problems and wrote solutions; held office hours to guide students through proofs; graded solutions and provided feedback on mathematical clarity and rigor; responded to student questions

Technical Architect Intern — ADT Summer 2024

- Received Technical Intern Award for work done building, pitching, and deploying solution adopted by the team
- Collaborated with Enterprise Arch. team to analyze team data in Jira, process it in BigQuery, and display it in Tableau