

EDUCATION

Tulane University

B.S. in Mathematics, GPA: 3.97

LA, 70118

2024 – 2028

EXPERIENCE

Undergraduate Researcher

Advisor: Mahir Bilen Can, Tulane University

New Orleans, LA

Aug 2025 – Present

- Algebraic geometry, algebraic coding theory, and post-quantum code-based cryptography
- Conduct research in **algebraic coding theory** and **post-quantum code-based cryptography**, focusing on structural properties of algebraic codes.
- Completed a rigorous self-study of Huffman and Pless's *Fundamentals of Error-Correcting Codes*, covering linear codes, bounds, cyclic codes, and decoding algorithms, and extended these tools to current research problems.
- Conduct original research on Niederreiter-type constructions, quasi-cyclic and quasi-circulant codes, and non-Hamming (NRT) metrics for post-quantum cryptographic applications.
- Authored multiple research manuscripts (currently under journal review), including work on post-quantum key encapsulation mechanisms and new structural bounds for metric-based codes .
- Develop proof-driven techniques using linear algebra, group actions, parity-check matrix analysis, and algebraic geometry to study decoding hardness, distance bounds, and resistance to structural and algebraic attacks.
- Participated in a Tulane Innovation Institute faculty research initiative focused on research translation and proposal development in cryptography.
- Regularly communicate research progress through technical notes, formal manuscripts, and seminar-style presentations.

QSPARC LABS

Co-Founder and CEO

New Orleans, LA

Aug 2025 – Present

- Post-quantum cryptography and secure protocol engineering
- Co-founded a cryptography startup developing post-quantum secure communication primitives and security architectures.
- Designed and prototyped multiple novel post-quantum cryptographic systems, including code-based key encapsulation mechanisms and secure message protection workflows.
- Conducted research on structured code-based encryption and post-quantum threat models, with emphasis on efficiency, deployability, and secure decoding strategies.
- Built reference and prototype implementations across Python, Rust, and C to validate cryptographic designs and system feasibility in both general-purpose and constrained environments.
- Implemented protocol-level cryptographic components and testing harnesses to support secure integration and evaluation.
- Lead financial planning, operational strategy, and long-term technical roadmapping; oversee research-to-product translation.
- Contribute to technical writing and intellectual property development, including multiple patent applications currently under review.
- Invited participant in an NSF-funded I-Corps-style innovation and commercialization mentorship program administered through MIT.

- Hyperplane arrangements, combinatorics, matroid theory
- Developed and delivered an advanced lecture series on hyperplane arrangements, bridging geometry, combinatorics, and algebra.
- Studied structural and enumerative invariants including intersection posets, geometric lattices, Möbius functions, and characteristic polynomials.
- Covered matroids, broken circuits, supersolvability, finite-field methods, and separating hyperplanes, based primarily on Stanley’s *An Introduction to Hyperplane Arrangements*.
- Led peer discussions connecting hyperplane arrangements to algebraic combinatorics, topology, and applications in coding theory and cryptography.

PUBLICATIONS

- [1] M. B. Can, S. Chakrabartty, and **E. Naig**, “Post-quantum key establishment on a self-powered timekeeping device”, Submitted for journal publication, 2025.
- [2] M. B. Can and **E. Naig**, “Lower bounds for minimum nrt distance from generator and parity-check matrices”, Submitted for journal publication, 2025.
- [3] M. B. Can and **E. Naig**, “Quasi-circulant trapdoor construction for niederreiter-type key encapsulation”, Submitted for journal publication, 2025.

SKILLS

- **Coding Languages:** Python, SQL, R, MATLAB, Java, JavaScript, Rust, C, C++
- **Tools:** Git, GitHub, \LaTeX , Linux

LANGUAGES

- **English:** Native
- **Chinese:** Conversational

SCHOLARSHIPS AND AWARDS

- Tulane Honors Scholar 2024–2028
- Deans List Tulane University Fall 2024
- Deans List Tulane University Spring 2025
- Deans List Tulane University Fall 2025

EXTRACURRICULAR ACTIVITIES

- Co-Founder and Vice President of Logistics, Tulane Science Olympiad 2025–Present
Co-founded Tulane’s first Science Olympiad invitational and led all logistical planning for a large-scale competition hosting 13 teams and over 450 students from multiple states. Managed outreach, registration, website development, test coordination, volunteer scheduling, and event execution. Secured and coordinated the use of chemistry, biology, and physics labs as well as over 60 classrooms across campus.
- Trip Leader, Tulane Outdoor Adventures 2024–Present
Lead outdoor trips for student groups, managing logistics, route planning, risk assessment, and participant safety. Coordinate pre-trip planning meetings and ensure compliance with university safety standards.
- Founder, Tulane Math Circle Spring 2025–Present
Founded and organize a weekly problem-solving seminar focused on proof-based mathematics. Prepare problem sets and lead collaborative discussions in algebra, combinatorics, and geometry.

COURSES

- MATH-2210: Multivariable calculus Fall 2024
- MATH-3660: Mathematics of Integration III Spring 2025
- MATH-2010: Math Modeling of World Spring 2025
- MATH-3090: Linear Algebra Spring 2025
- DATA-3530: GIS and Mapping Global Issues Spring 2025
- MATH-3000: Discrete Structures (UMSL) Summer 2025
- MATH-3110: Abstract Algebra I Fall 2025
- MATH-3050: Real analysis I Fall 2025
- MATH-3070: Introduction to Probability Fall 2025
- MATH-4120: Abstract Algebra II Spring 2026
- MATH-4060: Real Analysis II Spring 2026
- MATH-3200: Combinatorics Spring 2026

SELF STUDY

- Undergraduate Algebraic Geometry Summer 2025
Independent study of foundational algebraic geometry concepts with connections to modern coding theory and cryptography.
- Error Correcting Codes Summer 2025
Textbook: Huffman and Pless, Fundamentals of Error-Correcting Codes. Studied linear codes, bounds (Singleton, Hamming, Gilbert–Varshamov), cyclic and BCH codes, and algebraic decoding techniques.
- Real Analysis Fall 2025
Self-study of Rudin’s Principles of Mathematical Analysis (“Baby Rudin”), emphasizing rigorous real analysis, sequences and series, continuity, differentiation, and metric space methods.
- Smooth Manifolds and Differential Forms Winter 2025
Self-study of Spivak’s Calculus on Manifolds, covering multivariable integration, differential forms, and the inverse and implicit function theorems.

PERSONAL DEVELOPMENT

- Machine Learning Onramp Dec 2024
Completed the Machine Learning Onramp by MathWorks, gaining hands-on experience with fundamental machine learning concepts, algorithms, and practical MATLAB applications.
- Google AI Essentials Dec 2024
Acquired foundational knowledge in artificial intelligence, including machine learning, data science, and ethical AI practices, with practical insights into real-world applications.
- Google Data Analytics Certification Mar 2023
Developed strong skills in Microsoft Excel, SQL, Tableau, and R, with experience in preparing, processing, analyzing, and communicating data to support informed decision-making.