Nicolas Swanson

Linkedin | Website | nicswanson@vt.edu

Interests

Mathematical Cryptography, Elliptic Curves, and Quantum Computing.

Education

2024 - Present	Ph.D. Mathematics (Cryptography)	at **University of Waterloo**	(GPA: –/4.0)
2022 - 2024	M.S. Mathematics	at **Virginia Tech**	(GPA: 3.9/4.0)
2020 - 2022	B.S. Applied Discrete Mathematics -Computer Science Minor	at **Virginia Tech**	(GPA: 4.0/4.0)

Publications

1. Travis Morrison, Jason LeGrow, Jamie Sikora, and Nicolas Swanson (2024) *Masking Countermeasures Against Side-Channel Attacks on Quantum Computers.* QCE 2024. Conference in 2024.

2. Nicolas Swanson (2024) *Deciding if a Genus 1 Curve has a Rational Point.* Master's Thesis. Virginia Tech ETDs.

3. Nicolas Swanson and Eric Ufferman (2022) *A lower bound on the failed zero-forcing number of a graph.* Involve, a Journal of Mathematics. See it on the publisher's website.

Teaching Employment

Fall 2024	Instructor of Record for Calculus 1	Virginia Tech
2022 - 2023	Teaching Assistant for Discrete Mathematics	Virginia Tech
2020 - 2023	Private Tutor for Mathematics	Virginia Tech

Honors and Awards

July 2024	Mordell 100 Travel Grant	MIT
July 2024	Switzerland Summer School Travel Grant	Virginia Tech
June 2024	DQC&C Travel Grant	CCI
April 2024	Graduate Student Geometry and Topology Conference Travel Grant	MSU
Nov. 2023	Richmond MAAGC Conference Travel Grant	VCU
August 2023	Quantum Side-Channel Attacks Research Grant	CCI
April 2023	Commonwealth Cyber Initiative Innovation Scholarship	CCI
May 2022	Outstanding Senior in Applied Discrete Mathematics	Virginia Tech

Talks and Presentations

Jan 2025	**Invited talk:** Protecting Quantum Computations	JMM Seattle, WA
June 2024	**Invited talk:** Transpilers that Secure Quantum Computation	DQC&C Arlington, VA
July 2024	Protecting Expensive Quantum Computations	Cryptography & Coding Theory, Switzerland
April 2024	Masking countermeasures against quantum side-channel attacks	CCI Symposium
April 2024	Quantum side-channel attacks (poster)	CCI Symposium
April 2024	A lower bound on the failed zero forcing number	AMS Spring Eastern Sectional
Nov 2023	Distinguishing elliptic curves from pointless curves (poster)	MAAGC, Richmond VA
Dec 2023	Failed zero forcing numbers	VTMath Graduate Student Seminar
Nov 2023	Fujisaki Okamoto for KEMs and Kyber	Quantum Cryptography Class Seminar
Nov 2023	Side-channel attacks on quantum computers	CCI Graduate Student Summit
April 2023	Quantum side-channel attacks (poster)	Virginia Tech Quantum Symposium
April 2022	Broadening participation in undergraduate research panelist	Virginia Tech

Outreach

Educational Math YouTube Channel (@QualityMathVisuals)	Jan 2023 – Present
Math Circle Leader	Oct 2023 - Present

Research Projects

Distinguishing Elliptic Curves from Pointless Curves (Masters Thesis) VT ETDs

Many sources suggest a folklore procedure to determine if a smooth, genus 1 curve has a rational point. This procedure terminates conditional on the Tate-Shafarevich conjecture. We write down this algorithm and give an exposition for descent in our context.

Masking Countermeasures for Side-Channel Attacks on Quantum Computers Preprint

Jason Legrow, Travis Morrison, Jamie Sikora, and I propose a modification to the transpililation process of a quantum computer to safeguard against side-channel attacks. More broadly, we demonstrate that if it is feasible to shield a specific subset of gates from side-channel attacks, then it is possible to conceal all information in a quantum algorithm with only a linear increase in overhead. We provide concrete examples of this protection, specifically with virtual gates on IBM's quantum computers, which are undetectable to previously studied side-channel attacks.

The Ideas of Kyber and Dilithium Preprint

Joint work with Julia Shapiro; we provide exposition on security reductions and implementations of the LWE based post-quantum public key encryption protocol Kyber and the digital signature Dilithium. We emphasise the assumptions and non-tightness of the proofs used in security proofs, while keeping the math accessible to anyone with a familiarity of linear algebra.

The Failed Zero Forcing Number of a Graph Article

Joint work with Dr. Ufferman, in an undergraduate research project we solved a previously open problem in Graph Theory. Dependent on the number of vertices, we gave a lower bound for an NP-hard graph isomorphism invariant called the failed zero forcing number of a graph.

Programming Skills

Advanced:	Java, Javascript, Python, and MAGMA.
Familiar:	C, C++, SQL, PHP, Swift, and SAGE.

Professional Memberships

American Mathematical Society	Sept 2023 – Present
Society of Industrial and Applied Mathematics	Sept 2023 – Present
Association for Women in Mathematics	Oct 2022 – Present

Last updated: August 9, 2024