Contact Information

Address:	Department of Electrical and Computer Engineering University of Delaware Newark, DE 19716-2586 (302) 841-1895
E-mail:	andy@novocin.com
URL:	https://prof.ninja

Personal Data

Date of Birth:	June 12, 1983
Place of Birth:	Jacksonville, Florida
Nationality:	USA
Marital status:	Married with Two Daughters

Education

2001–2003	BS	Mathematics	Florida State University
2003–2006	MS	Mathematics	Florida State University
2006–2008	PhD	Mathematics	Florida State University

Dissertation Adviser: Mark van Hoeij

Dissertation Title:

Factoring Univariate Polynomials over the Rationals

Career Themes:

Providing service by designing practical solutions to difficult problems. If a tool is needed to solve a problem then expertise is built or a collaboration is formed. Mentoring students in how to solve meaningful problems creates exponential impact.

Employment History

- Assistant Professor at University of Delaware January 2016 to present
- Adjunct Professor at University of Delaware September 2014 to December 2015.
- Founding Partner at Golden Egg Labs LLC., September 2016 to present.
- CFO and CTO of Estate Auctions Inc. September 2012 to November 2014, Presently a majority shareholder
- Post-doctorate/Adjunct Associate Professor with Symbolic Computation Group at University of Waterloo, Canada. September 2011 to August 2014.
- Post-doctorate with the Arénaire project at ENS Lyon, France. September 2009 through August 2011.

- ANR post-doctorate with the LAREDA group at Montpellier, France. September 2008 through August 2009.

Teaching Honors

- *Excellence in Teaching Award* for College of Engineering, University of Delaware, 2018.
- *Horn Faculty Fellow* from the Horn Program in Entrepreneurship, University of Delaware, 2017.
- *Dwight Goodner Teaching Fellowship* from the Department of Mathematics, Florida State University, 2006.

Training other Faculty

- Co-PI, *FLC Effective Teaching* working group, University of Delaware, 2017-present.
- Lead Workshops on *Online Tools for Experiential Learning*, Annual VIP Consortium, Georgia Tech, 2016-present.
- Lead Workshops on *Intercollegiate Collaboration*, Annual VIP Consortium, Georgia Tech, 2017-present.
- Co-PI, *FLC Inclusive Teaching* leadership group, University of Delaware, 2018.
- Participant, *FLC Faculty Observation Program* University of Delaware, 2017.

FIXME TODO is add grants

Teaching Experience: Current Appointment (31 sections)

- Created all of these courses from scratch
- CPEG466 Independent Study Client-Side Engineering, summer 2018
- CPEG676 Online Secure Software Design, spring 2018
- CPEG676 Online Applied Cryptography, spring 2018
- CPEG472/672 Applied Cryptography, spring 2018 (2 sections)
- CPEG466 Independent Study User-Experience, Winter 2018
- CPEG470/670 Web Application Security, fall 2017 (2 sections)

- CPEG476/676 Secure Software Design, fall 2017 (2 sections)
- CPEG470/670 Web Application Security, spring 2017 (2 sections)
- CPEG472/672 Applied Cryptography, spring 2017 (2 sections)
- CPEG672 Online Applied Cryptography, spring 2017
- CPEG676 Online Secure Software Design, spring 2017
- ELEG467 Cloud Cryptography VIP course (4 sections)
- ELEG467 Cyber Security Scholars course (2 sections)
- CPEG476/676 Secure Software Design, fall 2016 (2 sections)
- CPEG472/672 Web Application Security, spring 2016 (2 sections)
- CPEG470/670 Applied Cryptography, spring 2016 (2 sections)
- CISC220 Data Structures, spring 2016 (2 sections)
- CISC479 Client-side engineering, winter 2016

Teaching Experience: UD Adjunct (14 sections)

- CISC220 Data Structures, fall 2015 (2 sections)
- CISC106 Intro Computer Science for Engineers (Python), fall 2015
- CISC437 Database Systems, summer 2015
- MATH202 Statistics II, summer 2015
- CISC866 Independent Study User-Experience, summer 2015
- MATH549 Coding Theory and Cryptography, spring 2015 (2 sections)
- CISC474 Advanced Web Technologies, spring 2015
- MATH210 Discrete Mathematics, spring 2015
- MATH202 Statistics II, winter 2015 (2 sections)
- CISC822 Algebraic Algorithms fall 2014
- CISC320 Introduction to Algorithms, fall 2014

Teaching Experience: Previous Institutions

- Introduction to Functional Programming II, Summer 2012 (Scheme to Python)
- Calculus II, spring 2008
- Modern Algebra, spring 2007
- Linear Algebra, fall 2006
- Calculus I, summer 2006
- Calculus I, spring 2006
- two sections of Trigonometry, fall 2005
- Conducted recitations Pre-Calculus course, summer 2005
- Pre-Calculus, spring 2005

University of Delaware Service

- Director, Vertically Integrated Projects program
- Director, Cybersecurity Scholars program
- Director, Cyber UN CTF Team
- Director, UD Blockchain Initiative
- Member, College of Engineering Diversity Committee
- Member, Electrical and Computer Engineering Undergraduate Curriculum Committee
- Project Lead, Admissions Analytical Engine
- Project Lead, Geltzeiler Trading Lab TraderEx Software
- Mentor, Solve ABET Platform
- Inventor, Blue Hen Investment Club Polling Platform
- Undergraduate Advisor for the ECE department
- Organizer, Weekly Friday Mini-Hackathons
- Organizer, Annual Intercollegiate VIP Mid-Atlantic Invitational
- Faculty Sponsor, Linux Users Group
- Faculty Sponsor, Hacking Club

- Faculty Sponsor, Options Club
- Faculty Sponsor, AI Club

Peer-Reviewed Papers

- Bruce Weber, Andrew Novocin, Jonathan Wood, and John Roberts. Cryptocurrencies and distributed ledger technologies - a literature review for the swift institute. Technical report, University of Delaware, 2018
- Andrew Novocin, David Saunders, Alexander Stachnik, and Bryan Youse. 3-ranks for strongly regular graphs. In *PASCO'2015—Proceedings of the 2015 International Workshop on Parallel Symbolic Computation*, pages 101–108. ACM, New York, 2015
- Mustafa Elsheikh, Andy Novocin, and Mark Giesbrecht. Ranks of quotients, remainders and p-adic digits of matrices. *(submitted) Electronic Journal of Linear Algebra*, 2014
- Mark van Hoeij, Jürgen Klüners, and Andrew Novocin. Generating subfields. *J. Symbolic Comput.*, 52:17–34, 2013
- Mustafa Elsheikh, Mark Giesbrecht, Andy Novocin, and B. David Saunders. Fast computation of Smith forms of sparse matrices over local rings. In *ISSAC 2012—Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, pages 146–153. ACM, New York, 2012
- Mark van Hoeij and Andrew Novocin. Gradual sub-lattice reduction and a new complexity for factoring polynomials. *Algorithmica*, 63(3):616–633, 2012
- Andrew Novocin, Damien Stehlé, and Gilles Villard. An LLL-reduction algorithm with quasi-linear time complexity [extended abstract]. In *STOC'11—Proceedings of the 43rd ACM Symposium on Theory of Computing*, pages 403–412. ACM, New York, 2011
- Mark van Hoeij, Jürgen Klüners, and Andrew Novocin. Generating subfields. In *ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, pages 345–352. ACM, New York, 2011
- William Hart, Mark van Hoeij, and Andrew Novocin. Practical polynomial factoring in polynomial time. In *ISSAC 2011—Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, pages 163–170. ACM, New York, 2011

- William Hart and Andrew Novocin. Practical divide-and-conquer algorithms for polynomial arithmetic. In *International Workshop on Computer Algebra in Scientific Computing*, pages 200–214. Springer, Berlin, Heidelberg, 2011
- Mark van Hoeij and Andrew Novocin. Gradual sub-lattice reduction and a new complexity for factoring polynomials. In *LATIN 2010: theoretical informatics*, volume 6034 of *Lecture Notes in Comput. Sci.*, pages 539–553. Springer, Berlin, 2010
- Andrew Novocin. *Factoring univariate polynomials over the rationals*. ProQuest LLC, Ann Arbor, MI, 2008. Thesis (Ph.D.)–The Florida State University

Conference Posters

- *Simplifying Algebraic Extensions*, poster presented at the International Symposium on Symbolic and Algebraic Computation, 2004, University of Cantabria
- *Early Termination Factorization*, poster presented at the International Symposium on Symbolic and Algebraic Computation, 2007, University of Waterloo
- *Factorization of Univariate Polynomials over the Rationals*, International Symposium on Symbolic and Algebraic Computation, 2008, Research Institute for Symbolic Computation

Ongoing Undergraduate Projects

Every semester, including summers and winters, I oversee teams of undergraduates through software deliverables and research projects. This activity allows for rapid exploration of cutting-edge technology and practical portfolio-worthy experience for the students. Here is a list of teams I have overseen:

- **Fully Homomorphic Encryption** This team works on deploying FHE schemes, improving practical performance, designing common algorithms to take advantage of low-circuit depth approaches, and reading many advanced papers.
- **Blockchain Applications** This team implements applications of blockchain technologies and has created educational material for workforce development in distributed ledgers. They have deployed voting software called VoteLock which was used in the Hen Hatch Competition.
- **Machine Learning** This team deploys the latest machine learning algorithms to various applications in demand around campus. They have built prototypes for local companies, the admissions department, and won an intercollegiate VIP competition on natural language processing.

- **LocalCoin Payment System and UBI** This team aims at high-speed, reliable, trustworthy crypto-backed payment exchanges that are localized by GPS coordinates. They formed an advisory council in the greater Philadelphia area and developed a plan by which the local coin could be used to form an experimental universal basic income in economically depressed areas.
- **Serverless Architectures** This team builds web applications for non-profits, student groups, institutions, and start-ups using scalable architectures. The goal is to have meaningful web services whose cost is a function of use. They have built many products for local industry and the innovative architectures that they have developed allow for lean start-ups to deploy rapidly.
- **Biometric ATM Security** This team built an innovative system for detecting identity without having to store biometric data. It uses threshold cryptography to allow for noisy inter-device identification. One goal is a secure cardless ATM, but generally to provide reliable decentralized authentication systems.
- **UD Red Team** This team performs cybersecurity audits for local small companies that are worried about their data security. They have trained in ethical hacking and developed professional procedures for handling real clients. This team is a collaboration of the cybersecurity scholars and VIP: Cloud Crypto team. They also do security testing of products built by all of my other teams.
- **Secure Data Transporter** This team built a prototype device for the Delaware Health Information Network which allows medical records to be securely transported from hospitals to legal firms when courtcases require records. The goal is reliable security that no red team would find leakages in and which can save hospitals and legal firms a great deal.
- **Virtual Experience** This team built virtual and augmented reality experiences using 3d-printed parts and the latest technologies. They have prototypes in education, real estate, and gaming.
- **Environmental Informatics** This new team is working on taking advanced analytics and machine learning and enhancing the reports that the University currently provides to state partners related to weather and water. They collaborate regularly with Aberdeen Proving Grounds and our deparment of Earth, Ocean, and Environment.

Grants

- NSF Award 1757353, RII Track 1 - Water Security in Delaware's Changing Coastal Environment, $23M ($19.2M from NSF and $3.8M from Delaware State),

Messer, Sparks, Kalavacharla, Michael, and DSouza, October 2018 - September 2023. Co-Lead for the Data Core, $280K, overseeing the partnership with the U.S. Army's Communications, Electronic, Research and Development Center (CERDEC) and the Intelligence and Information Warfare Directorate (I2WD).

- The Leona M and Harry B Helmsley Charitable Trust award 2015PG - OEDU043, The Vertically Integrated Projects (VIP) Consortium, $5M, Coyle, January 2015 - December 2017. Andrew Novocin UD subgrantee Q3552 - G15, $129K.
- Donation to enhance collaboration of Cybersecurity Scholars and Lerner College, $75000.
- Donation to assist ECE VIP teams, $5000 per team per year.
- University of Delaware Cybersecurity Initiative Grant to form and run the Cybersecurity Scholars, $30000.
- Horn Faculty Fellowship, $4500.
- Co-PI FLC Effective Teaching Group, $500.

Software

- Several custom enterprise interfaces to third party apps using TamperMonkey.
- Managing the building of scalable platform for 501c3, The Larger Story.
- Built LTI for real-time feedback system for online courses using Wiley's platform.
- Oversaw building of peer-evaluation tools for the VIP consortium.
- Developed mobile-first virtual-reality tours for University of Delaware.
- Developed real-time analytics platform for non-profits running donation drives.
- Designed and launched vip.udel.edu with platform and admin backends.
- Developed fast and simple mobile survey systems for audience interactivity.
- Created high performance attacks on the Table Maker's Dilemma and Pseudo-Random detection using C and Python.
- Created marketing software used by local radio stations for promoting events via mobile apps using Backbone, PHP.
- Created an inventory system for antiques companies allowing a mobile-driven workflow and consignor transparency.

- Created a web-driven eBay listing platform to streamline and parallelize the process of listing items via the eBay API.
- Created a boutique URL shortening platform for generating keyword rich, SEO friendly links.
- Created many data-driven analytics tools for understanding buying behaviors, pricing trends, analyzing employee utilization, and other key metrics 2012-2014.
- Developed full-stack enterprise workflow for Estate Auctions Inc. (LAMP, iOS, HTML5, jQuery, Backbone components).
- Cofounded Manandy Software Services spring 2014 (EaselJS, BackboneJS, MongoDB, NodeJS, iOS)
- Lead developer for the SalesTablet project (iOS and HTML5/JS business application).
- Co-Author of FLINT a highly optimized C-library for number theory
- (with Bill Hart) Developed and implemented fast polynomial factoring algorithm over the integers.
- Developed and implemented efficient new lattice reduction package.
- (with Mark van Hoeij and Juergen Klueners) Developed and implemented a new algorithm for finding all subfields of a given field extension.
- Contributor to SAGE Computer Algebra System

Other Professional Experiences & Skills

- Initiated Exponential Tech Working Group
- Post-quantum key exchange implementation
- LocalCoin as blockchain-based UBI experiment in Philly area
- Secure Data Transfer project for DHIN
- Oversaw many undergraduate student research posters
- Created series of practical crash courses on high-value tech topics started fall 2016.
- Oversaw a blockchain-based voting system launching in early 2017.

- Oversaw the creation of a penetration testing consultancy for small businesses, fall 2016.
- Organized weekly mini-hackathons beginning Fall 2015.
- Lead undergraduate research project on symbolic numeric methods in linear algebra 2015.
- Lead independent study on user experience and user testing summer 2015.
- Created the options club in association with the Blue Hen Investment Club Spring and Fall 2015 at University of Delaware.
- Managed creation of statistical problem set generator for University of Delaware statistical courses.
- Managed creation of inventory solutions for Seaford Bowling Lanes spring 2015.
- Managing a team of 5-15 employees 2012-2016.
- Organized many 'coding sprints' 2011-current.
- Organized Lattice Reduction Reading Group 2012.
- Design Consultant for Sensory Fitness Device 2012.
- Organized Graduate Student Seminar 2004-2006.
- Tutor at Florida State Math Help Center 2002-2005.
- Organized a series of lectures on *Class Field Theory*.
- Gave several series of talks for Florida State Algebra Seminar.
- Expertise in Python, C, C++, HTML, CSS, Javascript, PHP, Apache, Linux, SQL, Firebase (any web tech and many computer algebra systems).
- Primary operator of the Pat Thomas Planetarium from 2002-2006.
- Private Mathematics Tutor from 1999 - present.
- Heavily involved with a US FIRST Robotics team from 1999-2001.

Major areas of research interest

- High performance cryptography
- Algorithmic analysis including computational complexity

- Computer Algebra including Computational Algebraic Number Theory
- Lattice Reduction algorithms and applications (RSA attacks, integer factorization, pseudo-random detection)
- Asymptotically fast algorithms for arithmetic on integers, matrices, and polynomials

Invitations/projects

- Series of invited talks on high ROI life principles, Fall 2016.
- Director of the Vertically Integrated Projects program, beginning Spring 2016.
- Director of the University of Delaware Cyber Scholars program, beginning Spring 2016.
- CISC Theory Seminar October 2015, University of Delaware.
- Math-Club lecture May 2015, Univeristy of Delaware.
- ECCAD 2014 Duke University.
- Webmaster for ISSAC 2013.
- Founded *SCG Compressed Sensing Workgroup* 2012
- University of Warwick, Warwick, England December 18th, 2011
- University of Delaware, Newark, Delaware, December 2nd, 2011
- IDACCR, Princeton, New Jersey, November 30th, 2011
- University of Western Ontario, ORCCA JLM, November 4th, 2011
- Université de Rennes, France, May 13th, 2011
- Institut de Mathématiques de Bordeaux, France, May 5th, 2011
- Codage et Cryptographie, St. Pierre d'Oléron, April 3-8, 2011
- Computer Algebra Group, Limoges, France, March 10th, 2011
- EPFL, Lausanne, Switzerland, February 18th, 2011
- LaReDa Group, Lyon, France, February 1st, 2011
- Computer Algebra Group, Paderborn Germany, December 2nd, 2010

- SIAM/MSRI Workshop on Hybrid Methodologies for Symbolic Numeric Computation, Berkeley California, November 18th, 2010
- TaMaDi Project, September 8th, 2010
- SAGE days 23, Leiden, the Netherlands, July 2010
- 21st Rencontres Arithmétiques de Caen 2010, June 23-25, Caen France
- Chair of the poster committee for ISSAC 2009, July 28-31, Seoul, South Korea
- CACAO group, INRIA Nancy, June 23, 2009
- Algorithms group, INRIA Paris-Rocquencourt, June 22 2009
- LIX at École Polytechnique, Mar. 24-25 2009, Paris France
- 2nd SCIEnce workshop, Jan. 19-21 2009, École Polytechnique, Paris, France
- Warwick Mathematics Institute, Dec. 11-26th, 2008, Coventry, UK
- Computational Mathematics Work Group, August 16th, 2008, Kassel, Germany
- Mathematics Department, August 6th, 2008, Dusseldorf, Germany
- American Institute of Mathematics, The computational complexity of polynomial factorization, Workshop, May 2006, Palo Alto, California
- ACA 2003, North Carolina State University