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:	http://prof.ninja

Personal Data

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

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. When a tool is needed to solve a problem expertise is built or a collaboration is formed.

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

- *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.
- *PIE Excellence in Teaching Nominee* from Florida State University, 2007.

Teaching Experience

- Web Application Security, spring 2017
- Applied Cryptography, spring 2017 (also online)

- Secure Software Design, spring 2017 online
- Cloud Cryptography VIP team mentor, ongoing
- Cyber Security Scholars training course, ongoing
- Secure Software Design, fall 2016
- Creating Online Applied Cryptography Course for Wiley, summer 2016.
- Web Application Security, spring 2016.
- Applied Cryptography, spring 2016.
- Data Structures, spring 2016 (two sections).
- Client-side engineering, winter 2016.
- Data Structures, fall 2015 (honors as well).
- Intro Computer Science for Engineers (Python), fall 2015.
- Database Systems, summer 2015.
- Statistics II, summer 2015.
- Coding Theory and Cryptography, spring 2015 (honors as well).
- Advanced Web Technologies, spring 2015.
- Discrete Mathematics, spring 2015.
- Statistics II, winter 2015 (2 sections).
- Algebraic Algorithms fall 2014.
- Introduction to Algorithms, fall 2014.

- 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, Cubersecurity Scholars program
- Member, College of Engineering Diversity Committee
- Member, Electrical and Computer Engineering Undergraduate Education Committee
- Undergraduate Advisor for the ECE department
- Organizer, Friday Mini-Hackathons

Peer-Reviewed Papers

- (with D. Saunders, A. Stachnik, B. Youse) *3-Ranks for Strongly Regular Graphs*, proceedings Parallel Symbolic Computation 2015.

- (with M. Elsheikh, M. Giesbrecht, D. Saunders) *Fast Computation for Smith Forms of Sparse Matrices Over Local Rings*, proceedings International Symposium on Symbolic and Algebraic Computation 2012.
- (with J. Klüners and M. van Hoeij) *Generating subfields*, (conference version) proceedings International Symposium on Symbolic and Algebraic Computation 2011 and (journal version) accepted to Journal of Symbolic Computation 2012.
- (with M. van Hoeij) *Gradual sub-lattice reduction and a new complexity for factoring polynomials* (extended abstract) proceedings LATIN 2010 and (journal version) ALGORITHMICA 2012.
- (with D. Stehlé and G. Villard) *An LLL-reduction algorithm with quasi-linear time complexity*, proceedings Symposium on Theory of Computing 2011.
- (with B. Hart and M. van Hoeij) *Practical Polynomial Factoring in Polynomial Time*, proceedings International Symposium on Symbolic and Algebraic Computation 2011.
- (with B. Hart) *Practical divide-and-conquer algorithms for polynomial arithmetic*, proceedings Computer Algebra in Scientific Computing 2011.

Pre-Prints/Submissions

- (with M. Elsheikh, M. Giesbrecht) *Ranks of Quotients, Remainders and p-Adic Digits of Matrices*, submitted to The Electronic Journal of Linear Algebra, 2014.
- (with D. Saunders, Q. Xiang, A. Stachnik) *Handling Linear Recurrences with Insufficient Data*, pre-print.

- (with B. Hart, M. van Hoeij) *Factoring Univariate Polynomials*, preparing for Annals of Mathematics.

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

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

- 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.
- Lead two independent studies on data management and web scraping 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 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