Emil Volcheck

3040 Guilford Avenue
Baltimore MD 21218-3925

volcheck@acm.org
http://emilvolcheck.com

Employment

National Security Agency

Cryptographic Vulnerability Analyst, since 2000

- promoted to Grade 14 in 2010
- Team Lead (first-line supervisor) since 2008
- Security Education Academic Liaison (SEAL), since 2010

Cryptologic Mathematician (grade 12), 1995–2000

As a member of the NSA Cryptographic Services Division, my duties are to identify vulnerabilities in and attacks against cryptographic algorithms, functions, products, applications, and systems; to teach, mentor, and coach colleagues and interns; to manage software development on evaluation projects.

My work in the following areas has been recognized or won awards:

- improving the security of commercial cryptography products and government information systems;
- research in public key cryptography;
- speech compression applications.

As a first-line supervisor, my responsibilities include annual performance and promotion reviews for 9 employees.

As SEAL for Towson University, I support their Center of Academic Excellence in Information Assurance Education.

Senior Member of the Association for Computing Machinery (ACM) (2011)

Research Institute for Symbolic Computation,
Johannes Kepler University, Linz, Austria

Lise Meitner Postdoctoral Fellow, 1994–1995

Conducted research on algorithms for algebraic curves and taught a graduate seminar on this topic.

Education

UCLA Dept. of Mathematics	Ph.D.	1994
RWTH Aachen, Germany, Mathematics	Fulbright grant	1988
University of Delaware	Honors B.S.	1987

Research

My research deals with algorithmic questions posed by the theory of plane algebraic curves, such as, resolving singularities, computing in the divisor class group (Jacobian variety) of a curve, testing for absolute irreducibility, and computing the automorphism group of a curve.

Co-organized biennial AMS Special Sessions on “Computational Algebraic and Analytic Geometry for Low-dimensional Varieties” at the AMS/MAA Joint Mathematics Meetings (7 sessions, 1999–2011).

Publications

On Computing the Weierstrass Points of a Plane Algebraic Curve (with M. Heiligman), NSA Technical Report, 1998.

On Computing the Dual of a Plane Algebraic Curve, Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation, ACM Press.

Resolving Singularities and Computing in the Jacobian of a Plane Algebraic Curve, Ph.D. thesis, UCLA, 1994.

Computing in the Jacobian of a Plane Algebraic Curve, Proceedings of the First Algorithmic Number Theory Symposium, Springer-Verlag, 1994.

Noether's S-transformation Simplifies Curve Singularities Rationally, Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation, ACM Press.

Inherited Collineation Groups of Spreads of PG(3,p), Senior thesis, University of Delaware, 1987.

I am also the author of several NSA technical reports on public key cryptography, network security, and speech compression.

Presentations

"Computing with Algebraic Curves: a survey of recent results", contributed to the International Congress of Mathematicians, Berlin, 1998

"On Computing the Weierstrass Points of a Plane Algebraic Curve", Fourth Applications of Computer Algebra Conference, Prague, August 1998

"Testing Torsion Divisors for Symbolic Integration"

Florida State University, Mathematics, October 1996

University of Delaware, Computer and Information Sciences, Nov. 1996

American University, Mathematics and Statistics, October 1998

"Addition in the Jacobian of a Curve over a Finite Field", invited presentation at the Computational Number Theory Conference, Mathematisches Forschungsinstitut Oberwolfach, June 1995

Teaching

At Loyola University of Maryland, I taught "Abstract Algebra" (MA 441). Course material on web at `http://abstractalgebra.net/`.

At NSA, I taught "An Introduction to Elliptic Curves" (MA-562).

At UCLA, I served as Instructor for Intermediate Algebra (Math A) and Precalculus (Math 1) and as Teaching Assistant for a three-quarter introduction to programming with C++ (PIC 10) and a one-quarter advanced topics course, Symbolic Computation with Maple (PIC 197).

Professional Service

Association for Computing Machinery (ACM)

Baltimore ACM Chapter, `http://bacm.us/`

- Chair, 2008–2010
- Reestablished Chapter in 2008

ACM Special Interest Group for Symbolic and Algebraic Manipulation (SIGSAM)
`http://sigsam.org/`

- Chair, 2003–2007
- Secretary and Information Director, 1999–2003
- *SIGSAM Bulletin: Communications in Computer Algebra*:
  Associate Editor for Technical Reports, 1997–1999

US Public Policy Council of the ACM (USACM)
`http://usacm.acm.org/`

- Special Interest Group Representative, since 2005

Mathematics Community

Towson University, CoSMiC Scholars Program Advisory Board, since 2008

AMS/MAA/SIAM Joint Committee on Employment Opportunities (JCEO)

- Chair, 2007–2008
- AMS Representative, 2006–2008

Young Mathematicians' Network, `http://youngmath.net/`

- Member of Editorial Board, 1995–2004

SIAM Washington-Baltimore Section, Secretary, 1996–2005

Community Service

Charles Village Community Benefits District Management Authority
http://charlesvillage.org/

- Board of Directors (public office), 2004–2006, 2011–present
- Served on Governance, Safety & Sanitation Committees.

Election Technician (Baltimore City) 2006, 2008 general elections
Baltimore Ethical Society, http://bmorethical.org/

- Public Relations Committee: Chair, since 2010
- Executive Board (ex officio), since 2010

Baltimore Coalition of Reason, http://BaltimoreCoR.org/

- Coordinator, since 2009

Abell Improvement Association, http://abellimprovement.org/

- Secretary, Webmaster, 2003–2005