

# Emil Volcheck

3040 Guilford Avenue  
Baltimore MD 21218-3925

volcheck@acm.org  
<http://acm.org/~volcheck>

## Employment

### National Security Agency

Senior Cryptologic Mathematician (grade 13) and  
Cryptographic Vulnerability Analyst, since 2000

Cryptologic Mathematician (grade 12), 1995–2000

As a member of the NSA Cryptographic Evaluations Center, 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.

### Research Institute for Symbolic Computation, Univ. 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.

## 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 the National Security Agency, I have 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).

**Teaching Portfolio attached.**

## Service

Association for Computing Machinery (ACM) Special Interest Group for Symbolic and Algebraic Manipulation (SIGSAM), Secretary, since 1999

Young Mathematicians’ Network, Member of Editorial Board, since 1995

SIAM Washington-Baltimore Section, Secretary, since 1996

ACM SIGSAM, Associate Editor for Technical Reports of the *SIGSAM Bulletin: Communications in Computer Algebra*, 1997–1999