

MARK L. BAUER

Centre for Information Security and Cryptography
Department of Mathematics & Statistics
University of Calgary
Calgary, Alberta, Canada
T2N 1N4

work: (403) 2108456
fax: (403)282-5150
mbauer@math.uwaterloo.ca

ACADEMIC DEGREES

- Aug. 1995–Oct. 2001 **Ph.D., Mathematics,**
University of Illinois, Urbana-Champaign.
Aug. 1991–May 1995 **B.S., Mathematics, Business-Economics,**
Willamette University, magna cum laude.

FELLOWSHIPS and ACADEMIC POSITIONS

- Sept. 2003- **Assistant Professor,** Department of Mathematics and Statistics, University
of Calgary.
Jan. 2003- Aug. 2003 **Research Assistant Professor,** Centre for Applied Cryptographic Research,
University of Waterloo.
July 2001-Dec. 2002 **Cryptography Postdoctoral Fellowship,** Centre for Applied Cryptographic
Research, University of Waterloo.
July 2002–Aug. 2002 **Visiting Researcher.** University of Calgary, Calgary, AB.
March 2002–April 2002 **Visiting Researcher.** University of Calgary, Calgary, AB.
June 2001 **Visiting Researcher.** Laboratoire d'Informatique (LIX),
École polytechnique, France.
Aug. 2000–Aug. 2001 **VIGRE Fellowship,** University of Illinois
June 2000–Aug. 2000 **CRI Research Assistantship,** University of Illinois
Jan. 2000–May 2000 **Department of Education National Needs Fellowship,** University of Illinois.
February 2000 **Visiting Researcher.** University of Waterloo, Waterloo, ON.
Aug. 1999–Dec. 2000 **CRI Research Assistantship,** University of Illinois.
June 1999–Aug. 1999 **Research Assistant,** University of Illinois
Jan. 1999–May 1999 **Department of Education National Needs Fellowship,** University of Illinois.
Aug. 1995–2001 **Teaching Assistant,** University of Illinois, Urbana-Champaign.

AWARDS and ACADEMIC ACHIEVEMENTS

- May 2001 **Bateman Prize in Number Theory.**
May 2000 **Irving Reiner Award,** for excellence in algebra.
May 2000 **Hohn-Nash Award, 2nd Prize,** for computational mathematics.
Fall 1997, Fall 1998,
Spring 1999 Incomplete List of Teachers Ranked as Excellent by Their Students
Aug. 1997 **Distinction,** Number Theory Comprehensive Exam, University
of Illinois, Urbana-Champaign

PAPERS

1. M. Bauer, E. Teske, and A. Weng, Point counting on curves in large characteristic. Preprint (October 2003).
2. M. Bauer and S. Hamdy, On class group computations using the number field sieve (extended abstract). To appear in *Asiacrypt 2003, Lecture Notes in Computer Science*, Springer-Verlag.
3. M. Bauer, The arithmetic of certain cubic function fields. *Mathematics of Computation*, posted on June 17, 2003, PII S 0025-5718(03)01559-X (to appear in print).
4. M. Bauer and M. Bennett, Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation. *Ramanujan J.* **2** (2002), 209-270.
5. M. Bauer, A subexponential algorithm for solving the discrete logarithm problem in the Jacobian of hyperelliptic curves of large genus. Preprint (November 1999). Presented at *Conference on Public-key Cryptography 1999*, The Fields Institute.
5. *The Diophantine Equation $x^2 - D = cp^n$* , joint work with Michael Bennett, in preparation.
6. *Comparative Efficiency of Cubic Function Fields*, in preparation.
7. *Comments on Reducible Thue Equations*, joint work with Michael Bennett, in preparation.

CONFERENCES ATTENDED

Oct. 2001	5th Workshop on Elliptic Curve Cryptography , University of Waterloo.
Aug. 2001	8th Annual Workshop on Selected Areas in Cryptography , Fields Institute, University of Toronto.
Aug. 2000	Instructional Conference on Fermat's Last Theorem , University of Illinois, Urbana-Champaign.
May 2000	Millenial Number Theory Conference , University of Illinois, Urbana-Champaign.
March 2000	Illinois Graduate Number Theory Conference , University of Illinois, Urbana-Champaign. Co-organizer.
Nov. 1999	Midwest Arithmetical Geometry in Cryptography Workshop , University of Illinois, Urbana-Champaign.

PRESENTATIONS

- July 2004 **Polynomial Based Cryptography**, Melbourne, Australia.
The Discrete Logarithm Problem in Ideal Class Groups
- June 2004 **iCORE Banff Informatics Summit**, Banff, AB.
The Discrete Logarithm Problem and Cryptography.
- May 2004 **Fourth North-South Dialogue**, Red Deer College, Red Deer, AB.
Cryptographic Applications of Curves and Finite Fields.
- April 2004 **Simon Fraser Math Department Colloquium**, Simon Fraser University, Vancouver, BC.
A Cryptographic Application for Picard Curves.
- February 2004 **Elliptic Curve Cryptography Seminar**, University of Wisconsin, Madison, WI.
Point Counting on Picard Curves.
- February 2004 **Computer Security and Cryptography Seminar**, University of Wisconsin, Madison, WI.
Integer Factorization and the Discrete Logarithm Problem
- December 2003 **West Coast Number Theory Conference**, Monterey, CA.
Point Counting on Picard Curves
- May 2003 **Canadian Information Technology Security Symposium**, Ottawa, ON.
RSA: Present and Future.
- April 2003 **Math Careers Lecture Series**, Rice University, Houston, TX.
Elliptic Curves in Cryptography.
- April 2003 **Rice Math Department Colloquium**, Rice University, Houston, TX.
Function Fields in Cryptography.
- April 2003 **Special Math Colloquium**, University of Calgary, Calgary, AB.
Function Fields in Cryptography.
- Jan. 2003 **AMS Special Session: Computational Algebraic and Analytic Geometry for Low-dimensional Varieties**, Baltimore, MD. Invited Talk,
Arithmetic in Purely Cubic Function Fields.
- June 2002 **CMS Summer Meeting**, University of Laval, Quebec City, Quebec. Invited Talk,
Comparative Efficiency of Cubic Function Fields.
- April 2002 **Discrete Math Seminar**, University of Calgary, AB.
Solving the Generalized Ramanujan-Nagell Equation.
- February 2002 **Algebra & Number Theory Seminar**, McMaster University, Hamilton, ON.
Solving the Generalized Ramanujan-Nagell Equation.
- October 2000 **AMS Special Session on Low Genus Curves and Applications**, San Francisco State University, San Francisco, CA. Invited Talk,
The Arithmetic of Certain Cubic Function Fields.
- October 2000 **CEPS Conference**, University of Illinois, Urbana-Champaign,
The Current State of Elliptic Curve Cryptography.
- April 2000 **Number Theory Seminar**, University of Michigan, Ann Arbor, MI. *The Arithmetic of Certain Cubic Planar Curves.*
- Feb. 7, 2000 **Cryptography Seminar**, University of Waterloo, Waterloo, ON. *A Cryptographic Application of Certain Cubic Planar Curves.*
- June 1999 **Conference on the Mathematics of Public Key Cryptography**, The Fields Institute, Toronto, ON. Contributed Talk, *Discrete Log Problem in the Jacobian of Hyperelliptic Curves.*