CURRICULUM VITAE

Theodoulos Garefalakis

Personal

Date of birth :	10 September 1972
Place of birth :	Heraklion, Crete, Greece
Nationality :	Greek
Address :	Department of Mathematics University of Crete 714 09 Heraklion Greece
e-mail :	theo@math.uoc.gr

Positions

Oct. 2004 - present	Assistant Prof., Dept. of Mathematics Univ. of Crete, Greece
Mar. 2004 - Sep. 2004	Assistant Prof. (contract position), Dept. of Applied Mathematics Univ. of Crete, Greece;
Sep. 2002 - Jun. 2003	Post-doctoral fellow, Department of Mathematics and Department of Electrical and Computer Engineering, Univ. of Toronto, Canada;
Mar. 2001 - Jul. 2002	Post-doctoral research assistant, Department of Mathematics, Royal Holloway College, Univ. of London, England;
Sep. 2000 - Feb. 2001	Post-doctoral fellow, Department of Electrical and Computer Engineering, Univ. of Toronto, Canada;

Education

Feb. 1997 - Aug. 2000	Ph.D. Department of Computer Science, Univ. of Toronto, Canada; Supervisors: A. Borodin, D. Panario
Sep. 1995 - Jan. 1997	M.Sc. Department of Computer Science, Univ. of Toronto, Canada; Supervisor: A. Borodin
Sep. 1990 - Jun. 1995	B.Sc. Department of Computer Science, Univ. of Crete, Greece;

Awards and Distinctions

- Distinction, Ministry of Defense, Greece, 2000-2002.
- Mary H. Beatty Fellowship, University of Toronto, 1998-1999.
- Connaught Fellowship, University of Toronto, 1997-1998.

- University of Toronto Open Fellowship , 1995-1997.

Journal Publications

1. M. Christopoulou, T. Garefalakis, D. Thomson, D Panario, “The trace of an optimal normal element and low complexity normal bases”, *Designs Codes and Cryptography* (to appear).
2. T. Garefalakis, “The hidden number problem with non-prime modulus”, *JP Journal of Algebra, Number Theory and Applications*, **8**(2), 193 – 211, 2007.
3. I.F. Blake, T. Garefalakis, “Polynomial appoximation of Bilinear-Diffie-Hellman maps”, *Finite Fields and Applications* (to appear).
4. T. Garefalakis, “Irreducible polynomials with consecutive zero coefficients”, *Finite Fields and Applications*, **14**(1), 201 – 208, 2008.
5. I.F. Blake, T. Garefalakis, I.E. Shparlinski, “On the bit security of the Diffie-Hellman key”, *Appl. Algebra in Engin., Commun. and Computing*, **16**(6), 397 – 404, 2006.
6. I.F. Blake, T. Garefalakis, “On the complexity of the discrete logarithm and the Diffie-Hellman problems”, *J. of Complexity*, **20**(2-3), 148 – 170, 2004.
7. J. Dankers, T. Garefalakis, R. Schaffelhofer and T. Write, “Public key infrastructure in mobile systems”, *Electronics & Communication Engineering Journal*, **14**(5), 2002.
8. T. Garefalakis, D. Panario, “Polynomials over Finite Fields Free from Large and Small Degree Irreducible Factors”, *J. of Algorithms*, **44**(1), 98 – 120, 2002.
9. T. Garefalakis, “The generalized Weil pairing and the discrete logarithm problem on elliptic curves”, *Theoretical Computer Science*, **321**(1), 59 – 72, 2004.
10. I.F. Blake, T. Garefalakis, “On the security of the Digital Signature Algorithm”, *Designs Codes and Cryptography*, **26**(1), 87 – 96, 2002.
11. S.R. Blackburn, T. Garefalakis, “Cryptanalysis of a Cryptosystem due to Yoo, Hong, Lee, Lim, Yi and Sung”, *Electronics Letters*, **37**(18), 1118 – 1119, 2001.
12. T. Garefalakis, D. Panario, “The Index Calculus Method Using Non-Smooth Polynomials”, *Mathematics of Computation*, **70**(235), 1253 – 1264, 2001.

Refereed Conference Publications

1. M. Christopoulou, T. Garefalakis, D. Thomson, D Panario, “The trace of an optimal normal element and low complexity normal bases” extended abstract in *Workshop on Coding and Cryptography 2007* (edited by D. Augot, N. Sendrier and J.-P. Tillich), INRIA, 79-88, 2007.

2. T. Garefalakis, C.J. Mitchell, "Securing Personal Area Networks", *13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Lisboa, Portugal, September, 2002, pp. 1257 – 1259.

3. T. Garefalakis, "The generalized Weil pairing and the discrete logarithm problem on elliptic curves", *Lecture Notes in Computer Science*, 2286 (2002), 118 – 130.

4. T. Garefalakis, "A New Family of Randomized Algorithms for List Accessing", *5th European Symposium on Algorithms*, Graz, Austria, *Lecture Notes in Computer Science*, 1284 (1997), 200-216.

Theses

1. T. Garefalakis, "On the discrete logarithm problem in finite fields and on elliptic curves", Ph.D. thesis, Department of Computer Science, University of Toronto, September 2000.

2. T. Garefalakis, "A Family of Randomized Algorithms for List Accessing", M.Sc. Thesis, Department of Computer Science, University of Toronto, February 1997.

Unpublished Manuscripts

1. T. Garefalakis, " Complexity issues related to bilinear maps", December 2002.

2. T. Garefalakis, "On the Decision Diffie Hellman problem on special elliptic curves", October 2000.

3. T. Garefalakis, "Primality Testing, Integer Factorization, and Discrete Logarithms", Qualifying Depth Oral Report, Department of Computer Science, University of Toronto, March 1998.

Lectures

1. "The hidden number problem with non-prime modulus"
   Discrete Mathematics Seminar, Department of Mathematics, University of Crete, Jul. 2005.

2. "Traceable multisignature and group signature schemes from bilinear maps"
   Crypto Seminar, Department of Electrical and Computer Engineering, Univ. of Toronto, Apr. 2003.

3. "On the security of the Digital Signature Algorithm"
   Information Security Seminar, Information Security Group, Royal Holloway, Univ. of London, Mar. 2002.

4. "The Weil pairing: cryptographic applications"
   Colloquium, School of Mathematics and Statistics, Carleton Univ., Jan. 2002.

5. "Lattice basis reduction in cryptanalysis: two recent results"
   Ottawa/Carleton Combinatorics and Optimization Seminar, School of Mathematics and Statistics, Carleton Univ., Jan. 2002.

6. "The generalized Weil pairing and its applications in cryptography"
   Crypto Seminar, Department of Computer Science, Bristol Univ., Jan. 2001.

7. " The generalized Weil pairing and its applications in cryptography"
   Pure Math Seminar, Department of Mathemetics, Royal Holloway College, Univ. of London, Dec. 2000.

8. "On the Discrete Logarithm Problem on Elliptic Curves"
   Applied Number Theory Seminar, Department of Mathematics, Univ. of Toronto, Mar. 2000.

9. "The Discrete Logarithm Problem on Elliptic Curves"
   Informal Complexity Seminar Series, Department of Computer Science, Univ. of Toronto, Mar. 2000.

10. "Basic Notions on Elliptic Curves I"
    Informal Complexity Seminar Series, Department of Computer Science, Univ. of Toronto, Feb. 2000.

11. "Basic Notions on Elliptic Curves II"
    Informal Complexity Seminar Series, Department of Computer Science, Univ. of Toronto, Feb. 2000.

12. "Analytic Methods in Combinatorics"
    Graduate Student Seminar Series, Department of Computer Science, Univ. of Toronto, May 1998.

13. "Mellin Transform and Asymptotics"
    lecture series, Department of Computer Science, Univ. of Toronto, Feb. 1998.

14. "A New Family of Randomized Algorithms for List Accessing"
    presentation at the *5th Annual European Symposium on Algorithms*, Graz, Austria, Sep. 1997.

Teaching

Undergraduate courses:

1. Computer algebra and applications (Spring 2004)
2. Calculus I (Fall 2004)
3. Linear algebra I (Fall 2005)
4. Symbolic computation (Fall 2005, Fall 2006)
5. Introduction to cryptology (Spring 2006)
6. Applied Algebra (Spring 2007, Fall 2007)

Graduate courses:

1. Cryptography (Spring 2005)
2. Coding theory (Fall 2006, Spring 2008)

Supervision

1. Undergraduate Thesis of Christina Kokkinou, “Primitive normal bases of finite fields”, 2007 (in Greek).
2. M.Sc. Thesis of Andreas Tsilifonis, “Applications of the Weil pairing to digital signature schemes”, 2004 (in Greek).
3. M.Sc. Thesis of Maria Christopoulou, “Cryptographic algorithms based on non-linear systems of equations”, 2004 (in Greek).