

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. T. Garefalakis, G. Kapetanakis, “On the Hansen – Mullen conjecture for self-reciprocal irreducible polynomials”, *Finite Fields and Their Applications*, to appear.
2. M. Christopoulou, T. Garefalakis, D. Panario, D. Thomson, “Gauss periods as constructions of low complexity normal bases”, *Designs Codes and Cryptography*, **62**(1), 43 – 62, 2012.
3. T. Garefalakis, “On the action of $GL_2(\mathbb{F}_q)$ on irreducible polynomials over \mathbb{F}_q ”, *Journal of Pure and Applied Algebra*, **215**, 1835 – 1843, 2011.
4. T. Garefalakis, “Self-reciprocal irreducible polynomials with prescribed coefficients”, *Finite Fields and Applications*, **17**(2), 183 – 193, 2010.
5. I.F. Blake, T. Garefalakis, “A transform property of Kloosterman sums”, *Discrete Applied Mathematics*, **158**, 1064 – 1072, 2010.
6. M. Christopoulou, T. Garefalakis, D. Thomson, D Panario, “The trace of an optimal normal element and low complexity normal bases”, *Designs Codes and Cryptography*, **49**(1-3), 199 – 215, 2008.
7. T. Garefalakis, “The hidden number problem with non-prime modulus”, *JP Journal of Algebra, Number Theory and Applications*, **8**(2), 193 – 211, 2007.
8. I.F. Blake, T. Garefalakis, “Polynomial approximation of Bilinear-Diffie-Hellman maps”, *Finite Fields and Applications*, **14**(2), 379 – 389, 2008.
9. T. Garefalakis, “Irreducible polynomials with consecutive zero coefficients”, *Finite Fields and Applications*, **14**(1), 201 – 208, 2008.
10. 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.
11. 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.
12. J. Dankers, T. Garefalakis, R. Schaffelhofer and T. Write, “Public key infrastructure in mobile systems”, *Electronics & Communication Engineering Journal*, **14**(5), 2002.
13. T. Garefalakis, D. Panario, “Polynomials over Finite Fields Free from Large and Small Degree Irreducible Factors”, *J. of Algorithms*, **44**(1), 98 – 120, 2002.
14. T. Garefalakis, “The generalized Weil pairing and the discrete logarithm problem on elliptic curves”, *Theoretical Computer Science*, **321**(1), 59 – 72, 2004.
15. I.F. Blake, T. Garefalakis, “On the security of the Digital Signature Algorithm”, *Designs Codes and Cryptography*, **26**(1), 87 – 96, 2002.

16. 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.
17. 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.

Lectures

1. “Self-reciprocal irreducible polynomials with prescribed coefficients”, *Fields-Carleton Finite Fields Workshop*, School of Mathematics and Statistics, Carleton Univ., Jul. 2010.
2. “Self-reciprocal irreducible polynomials with prescribed coefficients”, *Number Theory Seminar*, School of Mathematics and Statistics, Carleton Univ., Apr. 2010.
3. “Polynomial approximation of bilinear Diffie-Hellman maps”, *Theoretical Computer Science and Discrete Mathematics Seminar*, Department of Mathematics, Aristotle Univ. of Thessaloniki, Apr. 2008.
4. “The bit security of the Diffie-Hellman key”, *Theoretical Computer Science and Discrete Mathematics Seminar*, Department of Mathematics, Aristotle Univ. of Thessaloniki, Feb. 2006.

5. "The hidden number problem with non-prime modulus"
Discrete Mathematics Seminar, Department of Mathematics, University of Crete, Jul. 2005.
6. "Traceable multisignature and group signature schemes from bilinear maps"
Crypto Seminar, Department of Electrical and Computer Engineering, Univ. of Toronto, Apr. 2003.
7. "On the security of the Digital Signature Algorithm"
Information Security Seminar, Information Security Group, Royal Holloway, Univ. of London, Mar. 2002.
8. "The Weil pairing: cryptographic applications"
Colloquium, School of Mathematics and Statistics, Carleton Univ., Jan. 2002.
9. "Lattice basis reduction in cryptanalysis: two recent results"
Ottawa/Carleton Combinatorics and Optimization Seminar, School of Mathematics and Statistics, Carleton Univ., Jan. 2002.
10. "The generalized Weil pairing and its applications in cryptography"
Crypto Seminar, Department of Computer Science, Bristol Univ., Jan. 2001.
11. "The generalized Weil pairing and its applications in cryptography"
Pure Math Seminar, Department of Mathematics, Royal Holloway College, Univ. of London, Dec. 2000.
12. "On the Discrete Logarithm Problem on Elliptic Curves"
Applied Number Theory Seminar, Department of Mathematics, Univ. of Toronto, Mar. 2000.
13. "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, Spring 2011)
6. Applied Algebra (Spring 2007, Fall 2007)
7. Algebra (Fall 2008)

8. Introduction to Linear Algebra (Spring 2009)
9. Analytic Geometry (Fall 2010)
10. Linear Algebra II (Fall 2011)

Graduate courses:

1. Cryptography (Spring 2005)
2. Coding theory (Fall 2006, Spring 2008, Spring 2012)
3. Algebra II (Fall 2009)

Supervision

1. Dimitris Megremis, undergraduate thesis, in progress.
2. Giorgos Kapetanakis, Doctoral student, in progress.
3. Iliana Margariti, “Elements in finite fields with given order and traces”, 2011 (M.Sc. Thesis, in Greek).
4. Yiorgos Tzanakis, “Dirichlet’s theorem for polynomials in arithmetic progression”, 2008 (Undergraduate thesis, in Greek).
5. Giorgos Kapetanakis, “The prime number theorem in function fields”, 2008 (M.Sc. Thesis, in Greek).
6. Anastasia Panoui, “Almost perfect non-linear functions”, 2008 (M.Sc. Thesis, in Greek).
7. Alexandros Syngelakis, “Optimal normal bases for Galois extensions”, 2008 (M.Sc. Thesis, in Greek).
8. Christina Kokkinou, “Primitive normal bases of finite fields”, 2007 (Undergraduate Thesis, in Greek).
9. Andreas Tsilifonis, “Applications of the Weil pairing to digital signature schemes”, 2004 (M.Sc. Thesis, in Greek).
10. Maria Christopoulou, “Cryptographic algorithms based on non-linear systems of equations”, 2004 (M.Sc. Thesis, in Greek).