Theodoulos Garefalakis

Curriculum Vitae

PERSONAL

Date of birth :	10 September 1972
Place of birth :	Heraklion, Crete, Greece
Nationality :	Greek
Address :	Department of Mathematics and Applied Mathematics University of Crete 70013 Heraklion Greece
e-mail :	tgaref@uoc.gr

POSITIONS

Nov. 2019 - present	Professor, Dept. of Mathematics and Applied Mathematics, Univ. of Crete, Greece;
Sep. 2013 - Nov. 2019	Associate Prof., Dept. of Mathematics and Applied Mathematics, Univ. of Crete, Greece;
Mar. 2010 - Jun. 2010	Visiting Professor, School of Mathematics and Satistics Carleton Univ., Canada;
Oct. 2004 - Aug. 2013	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.

FUNDING

1. University of Crete, Grant no 10316, title "Primitive and completely normal elements", 2019.
2. University of Crete, Grant no 3744, title "Normal Bases for Finite Fields", 2013 – 2015.

JOURNAL PUBLICATIONS

1. T. Garefalakis, G. Kapetanakis, "Further results on the Morgan-Mullen conjecture", *Designs Codes and Cryptography*, **87**, 2639 – 2654, 2019.
2. T. Garefalakis, G. Kapetanakis, "On the existence of primitive completely normal bases of finite fields", *Journal of Pure and Applied Algebra*, **223**(3), 909 – 921, 2019.
3. T. Garefalakis, G. Kapetanakis, "Enumerating permutation polynomials", *Finite Fields and Their Applications*, **47**, 85 – 93, 2017.
4. F.E. Brochero Martínez, T. Garefalakis, L. Reis, E. Tzanaki, "On the multiplicative order of the roots of $bX^{q^r+1} - aX^{q^r} + dX - c$", *Finite Fields and Their Applications*, **47**, 33 – 45, 2017.
5. T. Garefalakis, G. Kapetanakis, "A note on the Hansen – Mullen conjecture for self-reciprocal irreducible polynomials", *Finite Fields and Their Applications*, **35**, 61 – 63 , 2015.
6. T. Garefalakis, G. Kapetanakis, "On the Hansen – Mullen conjecture for self-reciprocal irreducible polynomials", *Finite Fields and Their Applications*, **18**(4), 832 – 841, 2012.
7. 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.

8. T. Garefalakis, "On the action of $\mathrm{GL}_2(\mathbf{F}_q)$ on irreducible polynomials over $\mathbf{F}_q$", *Journal of Pure and Applied Algebra*, **215**(8), 1835 – 1843, 2011.

9. T. Garefalakis, "Self-reciprocal irreducible polynomials with prescribed coefficients", *Finite Fields and Applications*, **17**(2), 183 – 193, 2010.

10. I.F. Blake, T. Garefalakis, "A transform property of Kloosterman sums", *Discrete Applied Mathematics*, **158**, 1064 – 1072, 2010.

11. 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.

12. I.F. Blake, T. Garefalakis, "Polynomial appoximation of Bilinear-Diffie-Hellman maps", *Finite Fields and Applications*, **14**(2), 379 – 389, 2008.

13. T. Garefalakis, "Irreducible polynomials with consecutive zero coefficients", *Finite Fields and Applications*, **14**(1), 201 – 208, 2008.

14. T. Garefalakis, "The hidden number problem with non-prime modulus", *JP Journal of Algebra, Number Theory and Applications*, **8**(2), 193 – 211, 2007.

15. 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.

16. 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.

17. T. Garefalakis, "The generalized Weil pairing and the discrete logarithm problem on elliptic curves", *Theoretical Computer Science*, **321**(1), 59 – 72, 2004.

18. J. Dankers, T. Garefalakis, R. Schaffelhofer and T. Write, "Public key infrastructure in mobile systems", *Electronics & Communication Engineering Journal*, **14**(5), 2002.

19. T. Garefalakis, D. Panario, "Polynomials over Finite Fields Free from Large and Small Degree Irreducible Factors", *J. of Algorithms*, **44**(1), 98 – 120, 2002.

20. I.F. Blake, T. Garefalakis, "On the security of the Digital Signature Algorithm", *Designs Codes and Cryptography*, **26**(1), 87 – 96, 2002.

21. 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.

22. 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.

TEACHING

Undergraduate courses:

1. Computer Algebra and Applications (Spring 2004)
2. Calculus I (Fall 2004)
3. Linear Algebra I (Fall 2005, Fall 2011)
4. Symbolic Computation (Fall 2005, Fall 2006)
5. Introduction to Cryptology (Spring 2006, Spring 2011, Spring 2013, Spring 2015)
6. Applied Algebra (Spring 2007, Fall 2007, Spring 2014, Spring 2017)
7. Algebra (Fall 2008, Fall 2013)
8. Introduction to Linear Algebra (Spring 2009, Fall 2017, Fall 2020, Fall 2022)
9. Analytic Geometry (Fall 2010, Fall 2012)
10. Discrete Mathematics (Fall 2013)
11. Geometry and Linear Algebra (Fall 2014, Fall 2015)
12. Field and Galois Theory (Spring 2015)
13. Foundations of Mathematics (Fall 2016, Spring 2020)
14. Number Theory (Spring 2018)
15. Algebra II (Spring 2019)

Graduate courses:

1. Cryptography (Spring 2005, Spring 2017, Spring 2022)
2. Coding theory (Fall 2006, Spring 2008, Spring 2012, Spring 2016, Spring 2018)

3. Algebra II (Fall 2009, Fall 2015, Fall 2018)

SUPERVISION

Ph.D. Theses:

1. Georgios Kapetanakis, "Polynomials with special properties over finite fields", 2015.

M.Sc. Theses:

1. Stella Fourfoulaki, "Applications of Fourier Transform to coding theory", 2018.
2. Georgia Tsaloli, "List decoding of Generalized Reed-Solomon codes", 2017.
3. Anastasia Aidini, "Cryptosystems based on error-correction codes", 2016.
4. Iro Mavrogianni, "The covering radius of linear codes", 2015.
5. Dimitris Megremis, "The LLL algorithm and applications to cryptography", 2014.
6. Iliana Margariti, "Elements is finite fields with given order and traces", 2011.
7. Giorgos Kapetanakis, "The prime number theorem in function fields", 2008.
8. Anastasia Panoui, "Almost perfect non-linear functions", 2008.
9. Alexandros Syngelakis, "Optimal normal bases for Galois extensions", 2008.
10. Andreas Tsilifonis, "Applications of the Weil pairing to digital signature schemes", 2004.
11. Maria Christopoulou, "Cryptographic algorithms based on non-linear systems of equations", 2004.

Undegraduate Theses:

1. Stella Chamilaki, "Homomorphic Cryptography: Paillier's Cryptosystem", 2020.
2. Lambrini Ananiadi, "Gauss periods in finite fields", 2014.
3. Yiorgos Tzanakis, "Dirichlet's theorem for polynomials in arithmetic progression", 2008.
4. Christina Kokkinou, "Primitive normal bases of finite fields", 2007.