CURRICULUM VITAE

Spyros S. Magliveras
7700 Dorchester Rd.
Boynton Beach, Florida 33472
(561)-737-1393 / (561)-297-0274
email: spyros@fau.edu
internet: http://euler.math.fau.edu/spyros/spyros

UNIVERSITY EDUCATION:

B.E.E (Electrical Engineering) University of Florida, 1961
M.A. (Mathematics) University of Florida, 1963
Ph.D. (Mathematics) University of Birmingham, England, 1970

TEACHING and RESEARCH EXPERIENCE:

Teaching Assistant, Mathematics, University of Florida, 1961-1962. Interim Instructor, Mathematics, University of Florida, 1962-1963. Instructor, Mathematics, Florida Presbyterian College, 1963-64. Programming Analyst, Systems Analyst, Institute for Social Research, University of Michigan, 1965-68. Teaching Fellow, Mathematics, University of Michigan, 1964-68. Research Fellow, University of Michigan, 1968. Research Fellow, University of Birmingham, England, 1968-70. Assistant Professor, Mathematics, SUNY, Oswego, 1970-73. Associate Professor, Mathematics, SUNY, Oswego, 1973-78. Visiting Associate Professor, Mathematics, SUNY, Binghamton, Spring 1976. Professor, Mathematics, SUNY, Oswego, 1978. Associate Professor, Computer Science and Mathematics, UNL, 1978-83. Professor, Mathematics and Computer Science, UNL, 1983. Visiting SERC Professor, University of Birmingham, England, 1984-85. Professor, Computer Science, UNL, 1984-present. Distinguished Professor, holding the *Henson Chair for Communication and Information Theory*, UNL 1991-2001. Visiting Research Professor, Centre for Applied Cryptography, C&O Department, University of Waterloo, 1999. Visiting Research Professor, Mathematics Department, University of Rome "La Sapienza", Jan 15 - March 15, 2000. Visiting Research Professor, Mathematics Department, University of Western Australia - Perth, April & May, 2000. *Henson Professor Emeritus*, University of Nebraska - Lincoln, Dec. 2000 - date. Professor of Mathematics, Florida Atlantic University, Dec. 2000 - date.

ADMINISTRATIVE EXPERIENCE:

Acting Chair intermittently (1985-89), and for the academic year 1989-1990. Prime mover in establishing the *Center for Communication and Information Science*, and Codirector (1987 - 1991), Director (1997), a Research Center established under The *Nebraska Research Initiative*, (budget about $400,000 per year). Chair, Department of Mathematical Sciences, Florida Atlantic University, August 2004 - May 2009. Director of the *Center for Cryptology and Information Security* (CCIS), an NSA/DHS designated National Center of Academic Excellence in Information Assurance Research , Florida Atlantic University, 2003-2013; Assoc. Director CCIS, 2013-date.

AWARDS AND SPONSORED RESEARCH:

1. NSF Undergraduate Research Grant in Mathematics, University of Florida, 1959-60.
2. Work under NSF grant GS-1873, with Prof. D. C. Pelz, Ann Arbor, Michigan, 1968.

3. Research Fellow, University of Michigan, Summer, 1968.

4. Research Fellow, University of Birmingham, England, 1968-70.

5. SUNY Research Foundation grant to investigate *Transitive Extensions of the Higman- Sims Simple Group*, 1971, $3,000.

6. Visiting Scholar, Mathematics Department, University of Michigan, Summer, 1971.

7. Research Associate at the Center for Human Growth and Development, University of Michigan, Summer, 1971, $7,000.

8. SUNY Research Foundation grant to study *Transitive Extensions of Finite Simple Groups*, 1973, $5,000.

9. Associate Director, CAUSE project, NSF Grant, # SER76-15934, 1976-78, $182,000 plus matching funds.

10. Summer Research Fellowship, UNL Research Council, 1979, *On Transitive Extensions of Groups*, $5,000.

11. Director, NSF Grant SPI-7901519, 1979-80, $26,414.

12. Summer Research Fellowship, UNL Research Council, 1981, *On t-Designs and Groups*, $5,000.

13. Director, DEC: An $83,340 Digital Equipment Corporation equipment grant for research in Computer Science, Summer, 1982.

14. Director, NSF/NSA Research Grant # MDA904-82-H-001, 1982-84, $61,314 to study *A New Cryptosystem from Permutation Groups.*

15. SERC (U.K.) Senior Research Fellowship, $14,550, University of Birmingham, Birmingham, England, 1984-85.

16. Maude Fling Research Fellowship, 1986, *On Projective Planes of Order not a Power of a Prime*, $5,000.

17. CCIS: Codirector, Center for Communication and Information Sciences, under the Governor of Nebraska Research Initiative, (1988) $320,000 ; (1989) $380,000; (1990) $450,000.

18. *Director*, Analysis and Implementation of PGM Encryption, projects [1] and [2], US West Communications and CCIS, 1989, $51,000.

19. Director, NSA MDA904-89-H-2044, *Combinatorial Designs and Applications*, two year grant, 1989-1991, with Earl S. Kramer $115,388.

20. Grant to visit the National Australian University in December, 1990, $3,500.

21. Director, NSA MDA904-91-H-0032, *Combinatorial Designs*, two year grant, 1991-1993, with Earl S. Kramer $117,592.

22. DFG (Deutsche Forschungsgemeinschaft) & *Institut für Experimentelle Mathematik* University of Essen, Germany - DM 10,000. Granted for period September 9, through November 10, 1992, for work in cryptology.

23. Natural Sciences and Engineering Research Council of Canada: *International Scientific Exchange Award*, $7,600, granted for 1992-93.

24. A second DFG grant (Deutsche Forschungsgemeinschaft) & *Institut für Experimentelle Mathematik* , University of Essen, Germany - DM 10,000. Granted for Summer of 1992, for work in cryptology.

25. NSA MDA904-93-H-3049, with matching from CCIS, *Combinatorial Designs*, two year grant, 1993-1995, with E. S. Kramer and D. R. Stinson $169,637.

26. National Science Foundation, Grant # NCR-9505845, for research on *A Coding Theoretic Approach to Lossless Image Compression* $182,708 + CCIS matching $36,541, for 1995-1998.

27. National Security Agency, grant MSFPF-95-G-091, with matching from CCIS, *Designs and other Combinatorial Problems*, with E. S. Kramer and D. R. Stinson $40,009 + CCIS matching $14,812, for 1995-1996.

28. DFG (Deutsche Forschungsgemeinschaft) & *Institut für Experimentelle Mathematik* University of Essen, Germany - DM 8,000. Granted for May, 1996, for work in cryptology.

29. PI: NSF/REU program, summer 1997, for undergraduate student research in Data Compression, $5,000.

30. Co-PI: UN Foundation, with S. Reichenbach (PI) and others, $100,000.

31. Co-PI: Proposal with K. Sayood et al, *Mobile Communications Research Project*, Neb. Res. Initiative 1998, (4 yr grant: 1998-2002) $251,000 per year.

32. PI: National Science Foundation, grant CCR-9610138, *Topics in Unconditionally Secure Cryptography*, with D.R. Stinson, (1997-2000), $95,316.

33. CO-PI : Federal Earmark 2003-05, DOD/DISA $ 2 million, *Secure Telecommunication Networks*, with Dean Karl K. Stevens, Dean Mohammad Ilyas and Prof. Paul Hart.

34. CO-PI : National Science Foundation, MRI-0521410 , *Acquisition of a NUMA-based Supercomputer for High Performance Computing*, with Jie Wu (PI), Hanqi Zhuang, Shen Li Qiu, and Borko Furht (Co-PI's) (2005), $447,190.

35. CO-PI : Federal Earmark 2007-08, DOD/DISA, $ 1 million, *Secure Telecommunication Networks*, project : *Pervasive Computing - Security in GIG-like Architectures*, with Karl K. Stevens, Mohammad Ilyas, Rainer Steinwandt and others.

36. PI: FAU Tech Fee Proposal ($26,000) to aquire a multinode parallel computing cluster for teaching and research. The cluster (kokowin) has been placed at the FAU Jupiter campus, and operations began in early April, 2015.

PATENTS

1. Spyros S. Magliveras, Tran van Trung, and Tamas Horváth, *A Secret Key Cryptosystem and Method Utilizing Factorizations of Permutation Groups of Arbitrary Order 2^L.* US Patent # 6,038,317 issued on March 14, 2000.

2. Daniel Socek, Hari Kalva and Spyros Magliveras, *Methods for Encrypting and Compressing Video*, US Patent #8,189,664 B2, issued on May 29, 2012.

PROFESSIONAL AND HONORARY SOCIETIES

Institute of Combinatorics and its Applications, Fellow

ΣT / $T B \Pi$ honorary engineering society

$\Sigma \Xi$ national research society

Kappa Mu Epsilon

PROFESSIONAL SERVICE

1. Fellow of the Institute of Combinatorics and its Applications.
2. Member of the Council for the Institute of Combinatorics and its Applications.
3. Editor, *Journal of Combinatorial Designs*, 2000-2005.
4. Has refereed for the Journal of Comb. Theory (A) , Journal of Discrete Math., Ars Combinatoria, SIGSAM Bulletin, Annals of Discrete Math., European Journal of Combinatorics, JCMCC, Australasian J. of Combinatorics, the Journal for Designs, Codes & Cryptography, Intern. J. of Algebra and Computation, and the J. of Comb. Designs.
5. Referee for NSF, NSA, NSERC grant proposals in Computer Science, Combinatorics, Coding Theory and Cryptology.
6. General Chair for *Crypto '92*. The international IACR conference to be held at the University of California - Santa Barbara, in August 1992, ex-officio member of the Board of Directors, IACR.
7. Guest Editor for JCMCC, (for the Proceedings of the *Ninth Midwestern Conference on Combinatorics, Cryptography & Computing*)
8. Principal organizer of an International Geometry Conference, the *First Pythagorean Conference*, which took place during June 1-7, 1996, on the island of Spetses - Greece.
9. Co-Editor of the Proceedings of the *First Pythagorean Conference*
10. Ph.D. external examiner for several universities world wide.
11. Principal organizer of the *Crypto/Codes* Conference, June 1 - 7, 1997, Lincoln, NE., USA.
12. Principal organizer of the *Second Pythagorean Conference*, May 30 - June 6, 1999, Pythagoreion, Samos - Greece.
13. Co-Editor of the Proceedings of the *Second Pythagorean Conference*, Birkhäuser, vol. 67, 2000.
14. Principal organizer of the *Third Pythagorean Conference*, which took place on June 1 - 7, 2003, Faliraki, Rhodes - Greece.
15. Program Committee member for *Tatracrypt 2003*, "Third Central European Cryptology Conference", Bratislava, Slovakia, June 26-28, 2003.
16. Program Committee member for *WartaCrypt 2004*, "Fourth Central European Cryptology Conference", Bedlewo, Poland, July 1-3, 2004.

17. Co-Editor of the Proceedings of the "Third Pythagorean Conference", DCC 32, Kluwer, 2004.

18. Program Committee member for the *5th Central European Conference on Cryptography* MoraviaCrypt '05, Brno, Czech Republic, June 15 - 17, 2005.

19. Program Committee member for the *6th Central European Conference on Cryptography* NyirCrypt '06, Nyiregyhaza, Hungary, June 15 - 17, 2006.

20. Founder, Editor and one of three Managing Editors, *Journal of Mathematical Cryptography*, *W. de Gruyter*, 2005- date.

21. Program Committee member for the *7th Central European Conference on Cryptography* TatraCrypt '07, Smolenice Castle, Slovakia, June 22-24, 2007.

22. Program Committee member for the *8th Central European Conference on Cryptography* CECC '08, Technical University of Graz, Austria, July 22-24, 2008.

23. Program Committee member for the *9th Central European Conference on Cryptography* CECC '09, at Třebič. Brno University of Technology, Czech Republic, June 23-26, 2009.

24. Principal organizer of the *Fourth Pythagorean Conference*, which will take place on May 30-June 4, 2010, on the Greek Island of Corfu.

25. General Chair for *ISC 2010*. The "International Information Security Conference" and member of Steering Committee and Program Committee. (http://brain.math.fau.edu/ cdfg09/) to be held in Boca Raton, Florida during October 25–28, 2010.

NOMINATIONS - HONORS

1. Nominated for an Excellence in Teaching Award, University of Nebraska - Lincoln, 1980. Mathematics.

2. Nominated for an ORCA Excellence in Research Award, University of Nebraska - Lincoln, 1983-84.

3. Recipient of the AMOCO Award of Distinguished Teaching, University of Nebraska - Lincoln, 1984.

4. Honorary Senior Research Fellow, University of Birmingham - England, 1985.

5. Recipient of the *Paul and Betty Henson Distinguished Professorship* in Communication and Information Science, University of Nebraska - Lincoln, 1991 - 2000.

6. Recipient of a J.D. Edwards Professorship, University of Nebraska - Lincoln, 2000.

7. *Paul and Betty Henson Distinguished Professor Emeritus* in Communication and Information Science, University of Nebraska - Lincoln, 2000 - date.

8. Recipient of a *Service to Students* award, University of Nebraska - Lincoln, 2000.

9. Recipient of the ICA **Euler gold medal** award for lifetime research in Combinatorial Mathematics, 2001.

10. Recipient of the *Charles E. Schmidt College of Science - Teacher of the Year* award, a *A Warren Lloyd Holtzman* grant award, 2010.

RESEARCH INTERESTS

Cryptology, Finite Groups, Combinatorics, Computational Algebra, Coding Theory, Image Compression, Design & Complexity of Algorithms, Algebraic Computer Science, Finite Geometries, Computer Networks.

COLLOQUIA AND INVITED ADDRESSES

1 *On Groups, Graphs and Designs*, Clarkson University, Postdam, N.Y. fall 1976.

2 *On Combinatorial Designs of Room Type Induced by Primitive Group Actions*, Humbolt State University, summer 1980.

3 *Representation Theory of Finite Groups*, University of Western Ontario, London, Ontario Canada, April 1980.

4 Presented an Invited Address on *Geometries, Groups and the New Six Designs* at the University of Athens, Greece, summer, 1982.

5 Invited speaker, *Six Designs Exist!*, London Mathematical Society, Symposium on Computational Group Theory, Durham University, England, July - August, 1982.

6 Invited Speaker, Conference on Modular Representations of Finite Groups, Birmingham University, England, July, 1983.

7 Invited speaker, *Recent Applications of Computational Group Theory to Combinatorics.* First Cayley Conference, Birmingham University, England, June 12-16, 1984.

8 Presented a series of lectures on *Computational Methods in Algebra and Geometry* at the "Federico Enriques" Mathematical Institute, Mathematics Department, University of Milano, November 22 - December 10, 1984.

9 Presented a seminar to the "Instituto Per La Matematica Applicata, Consiglio Nazionale delle Ricerche", Genova, Italy, on *Random Number Generators From Permutation Groups*, December 6, 1984.

10 Presented a seminar to the "University College of Wales, at Aberystwyth" on *Recent Results in Combinatorial Designs.* February 1, 1985.

11 Presented a seminar to the Department of Pure Mathematics at the University of Nottingham, on *Simple 6-Designs from Permutation Groups*, February 8, 1985.

12 Presented a seminar to the Computer Science Group, University of Nottingham, on *Applications of Logarithmic Signatures of Nonabelian Groups to Cryptography.* February 13, 1985.

13 Presented a lecture at the General Mathematics Colloquium, University of Birmingham, on *Cryptography in Transition*, March 13, 1985.

14 Presented a seminar to the Mathematics Department of the University of Manchester, on *Applications of Group Theory to Cryptography*, May 7, 1985.

15 Presented a seminar to the Computer Science Department, Rochester Institute of Technology, Rochester, N.Y., on *Groups, Designs and Error Correcting Codes*, May 19, 1986.

16 Presented a Colloquium to the Mathematics Department at Colorado State University on *Logarithmic Signatures of Finite Groups.* February 3, 1989.

17 Presented a Colloquium to the Department of Mathematics, Statistics and Computer Science, Marquette University, Milwaukee, WI., on *Cryptography and Computational Group Theory.* February 9, 1989.

18 Presented two invited talks at US WEST Advanced Technologies, Denver, Colorado, on July 24, 1989, *Cryptography Today*, and *Properties of Cryptosystem PGM*

19 Presented a Colloquium on *Cryptology* at the University of Nebraska - Omaha, Nov 18, 1989.

20 Official Guest of *Slovenská Vysoká Škola Technická V Bratislave*, May 31 - June 17, 1990. Presented a Colloquium on *Applications of Computational Group Theory.*

21 Presented a Colloquium at the *Slovak Academy of Sciences* on *Groups and Resolutions of Combinatorial Designs.*

22 Presented a talk at the CC seminar, EE Department, University of Nebraska - Lincoln, October 2, 1990, *Cryptography Today.*

23 Presented a Colloquium at the Australian National University, Mathematics Research Section, on *Computational Group Theory and Cryptography*, Canberra, Australia, Dec. 11,1990.

24 Presented a Colloquium at The Wesleyan University, on *Cryptology*, Lincoln, Nebraska, November 13, 1991.

25 Presented a Colloquium at The Michigan Technological University, on *Cryptography Today*, Houghton, Michigan, March 25, 1992.

26 Colloquium at *The Institute for Experimental Mathematics* - University of Essen, on *Cryptography*, Essen, October 21, 1992.

27 Colloquium at the *Mathematics Department* - University of Heidelberg, Germany, on *a New Public Key Cryptosystem from Permutation Groups*, Heidelberg, November October 21, 1992.

28 A series of three talks at the *Combinatorics & Optimization* Department, University of Waterloo, on *Designs from their automorphism groups*, Waterloo, Canada, Jan. 19, 26 and Feb 2, 1993.

29 Colloquium at the *Mathematics Department* - State University of New York - College at Oswego, on *Cryptology - From Prehistory to Modern Times*, Oswego, N.Y., February 10, 1993.

30 Colloquium at the *Mathematics* and *CS* Departments, McMaster University, *Logarithmic signatures of finite groups and cryptosystem PGM*, Hamilton, Canada, March 10, 1993.

31 Colloquium at the *Computer Science*, University of Toronto, *Tame logarithmic signatures beget wild ones* Toronto, Canada, March 22, 1993.

32 Colloquium at the *Mathematics & Computer Science Departments*, Michigan Technical University, *Trap-door, one-way functions from factorization bases in finite groups.* Houghton, Mich., May 6, 1993.

33 Colloquium at *The Institute for Experimental Mathematics* - University of Essen, on *Public Key Cryptography from Groups*, Essen, June 23, 1993.

34 Colloquium at *RWTH, University of Aachen, Lehrstuhl D für Mathematik* Aachen, Germany - on *Cryptography from factorizatons in non solvable groups*, May 3, 1996.

35 Colloquium at *The Institute for Experimental Mathematics* - University of Essen, on *Using Treecodes in Lossless image compression*, May 14, 1996.

36 Colloquium at *Discrete and Statistical Sciences* - University of Auburn, on *Large Sets of t-Designs*, Auburn, October 24, 1996.

37 Invited talk at the IEEE Computer Society, Nebraska Chapter Section metting, *Optimal Codes for Lossless Image Compression*, November, 21, 1996.

38 Colloquium at the University of Nebraska - Omaha, Computer Science Department, on *Codes in Lossless Image Compression*, March 18, 1997.

39 Colloqium at the University of Rome ("La Sapienza"), Mathematics Department, on *Secret- and Public key Cryptography based on Groups*, February 24, 2000.

40 Colloquium at the University of Bayreuth (Germany), Mathematics & Computer Science Department, *Intractibility of certain group factorizations and two new public-key cryptosystems*, April 6, 2000.

41 Colloquium at the *Technical Slovak University*, Bratislava, Slovakia, *One-way, trap door functions from group factorizations*, April 17, 2000.

42 Colloquium at the *University of Western Australia*, Perth, Australia, *Secret- and public-key cryptosystems from covers of Finite Groups*, May 24, 2000.

43 Colloquium at *The Institute for Experimental Mathematics* - University of Essen, on *New Results in Groups and Cryptography,* June 11, 2001.

44 CCIS Colloquium at *Florida Atlantic University*, on *Non-abelian cryptography,* March 22, 2012.

45 Colloquium at *The Institute for Quantum Computing* - University of Waterloo, Canada, *Group-theoretic cryptography*, a post-quantum alternative. May 13, 2013.

CONFERENCE PAPERS, ADVANCED INSTITUTES

1. *On Weak Equivalence of Transitive Permutation Representations of Finite Groups*, National AMS meeting, Miami, Fla., 1964.
2. Finite Group Theory Institute, University of Michigan, summer, 1968.
3. NATO Summer Research Institute on Finite Groups, Oxford University, summer, 1969 (invitation).
4. Mathematisches Forschungsinstitut Oberwolfach, Conference on Finite Geometries, April, 1970 (invitation).
5. *The Maximal Subgroups of the Higman-Sims Simple Group*, AMS meeting, University of Illinois, Urbana, November, 1970.
6. National AMS meeting, Atlantic City, NJ, January, 1971.
7. Algebra Symposium, Carleton University, Ottawa, Canada, November, 1971 (invitation).
8. Gainesville Conference on Finite Groups, Gainesville, Fla., March, 1972.
9. Linear Groups Conference at East Lansing, Michigan, March, 1973 (invitation).

10. *On Methods of Determining Subgroup Structures of Finite Groups*, Galway Conference on Finite Groups and computation, Galway, Ireland, summer, 1973 (invitation).

11. NATO Institute on Combinatorics, Nijenrode Castle, Breukelen, The Netherlands, July, 1974 (invitation).

12. *The Non-existence of Rank-3 Transitive Extensions of the Higman-Sims Simple Group*, Park City Conference on Finite Groups, Park City, Utah, February, 1975.

13. ACM Symposium on Symbolic and Algebraic Computation, Yorktown Heights, N.Y., August, 1976 (participant & reviewer).

14. International Symposium on Information Theory, Cornell University, Ithaca, N.Y., October, 1977 (invitation).

15. *Tiling the Power Set with Projective Planes*, Symposium on Combinatorics, New York Academy of Science, New York, N.Y., Spring, 1978.

16. International Conference on Optimization and Combinatorial Designs, Fort Collins, Co., June, 1978, (session chairman).

17. *t-Designs from the Mathieu Groups*, Nebraska Academy of Sciences, MAA regional meeting at Wesleyan University, April, 1979.

18. *t-Designs from the large Mathieu Groups*, Part II (contributed Paper), Tenth Southeast Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic University, Boca Raton, Fla., April, 1979.

19. Conference on Geometry and Groups, University of Michigan, Ann Arbor, Michigan, March, 1980 (invitation).

20. *Some New Combinatorial Designs of Room-type*, Nebraska Academy of Sciences MAA regional meeting at Doane College, Crete, Nebraska, April, 1980.

21. *Coherent Room Rectangles from Permutation Groups* (contributed paper), Eleventh Southeast Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic University, Boca Raton, Fla., March, 1980.

22. *A New Cryptosystem from Permutation Groups* (contributed paper), Twelfth Southeast Conference on Combinatorics, Graph Theory and Computing, LSU, Baton Rouge, La., March, 1981.

23. *Some New 5-designs from Permutation Groups* (contributed paper), Thirteenth Southeast Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic University, Boca Raton, Fla., February, 1982.

24. *Six Designs Exist !*, London Mathematical Society, Symposium on Computational Group Theory, Durham University, England, July - August, 1982. (invitation).

25. *Exceptional t-Designs*, Nebraska Academy of Sciences MAA regional meeting, University of Nebraska - Omaha, January, 1983.

26. *Simple 6-(33,8,36) Designs from* $P\Gamma L(2, 32)$, Fourteenth Southeast Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic University, Boca Raton, Florida, February, 1983.

27. Conference on Modular Representations of Finite Groups, Birmingham University, England, July, 1983 (invitation)

28. *The Status of Constructions of New Simple t-Designs at the University of Nebraska Lincoln*, Fifteenth Southeast Conference on Combinatorics Graph Theory and Computing, Louisiana State University, Baton Rouge, 1984.

29. *Invited speaker* - First Cayley Conference, Birmingham University, Birmingham, England, June 12-16, 1984, *Recent Applications of Computational Group Theory to Combinatorics.*

30. EUROCAL '85, European Conference on Symbolic and Algebraic Computation, J. Kepler University, Linz, Austria, Spring 1985.

31. Mathematisches Forschungsinstitut Oberwolfach, Finite Geometries Conference, May 26 - June 1, 1985. *New Infinite Families of Simple 5-Designs*, (invitation).

32. *Invited speaker*, Working Conference on Aspects of Formulation and Design - Computational Group Theory, *A Knowledge Base System for Finite Groups and their Geometries*, University of Birmingham - England, June 26-28, 1985.

33. International Conference *Groups - St. Andrews 1985*, sponsored by the London Mathematical Society and the Edinburgh Mathematical Society at the University of Andrews, Scotland; July 27 - August 3, 1985, (invitation).

34. Seventeenth Southeastern International Conference on Combinatorics Graph Theory and Computing, Florida Atlantic University, Boca Raton, Fla., February, 1986.

35. *Panelist,* AMS - University of South Dakota meeting, Vermilion, *Discrete Structures.* April 11-12, 1986.

36. International Conference on Finite Geometry and Combinatorics, Deinze, Belgium, June 1 - 7, 1986, *Does Primitivity on Lines imply Primitivity on Points?* (invitation).

37. 29th Midwest Symposium on Circuits and Systems, August 11 - 12, 1986. Coauthored two papers, presented one. (Coding Theory session chair)

38. Eighteenth Southeastern International Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic University, Fla., February, 1987. *The Number of Classes Under Permutation Equivalence of q-valued $n \times m$ Incidence Matrices*

39. First Vermont Summer Workshop on Combinatorics, June 17-20, 1987, *The Possibility of a New Infinite Family of Room Rectangles*, (invitation).

40. *Organizer*, AMS Special Session on *Finite Geometries and Combinatorial Designs*, Lincoln, Nebraska, October 1987.

41. *Invited speaker*, XXth Ohio State - Denison Mathematics Conference, February 25-27, 1988, Granville, Ohio, *The Steiner Systems S(2,4,25) with Nontrivial Automorphism Group.*

42. Design Theory Conference, Auburn University, March 21-25, 1988, (invitation.)

43. Mathematisches Forschungsinstitut Oberwolfach, Computational Group Theory, May 21 - 25, 1988. *On Leavitt's Algorithm for large knapsacks.* (invitation.)

44. Combinatorics '88, International Conference on Incidence Geometries and Combinatorial Structures, Ravello, Italy, May 23 - 28, 1988. Co-authored two papers, presented one : *On certain Steiner Systems with automorphisms*, (invitation.)

45. Crypto '88, The annual conference of the International Association for Cryptographic Research, UC Santa Barbara, California, August 21-25, 1988, Rump Session. *Properties of a cryptosystem based on logarithmic signatures of permutation groups.*

46. *Invited speaker*, National AMS meeting in Phoenix Arizona, Jan. 1989, in the Special Session on Computational Group Theory, presented a paper on *Cryptographic Applications of Computational Group Theory.*

47. Twentieth Southeastern International Conference on Combinatorics Graph Theory and Computing, Florida Atlantic University, Boca Raton, Fla., February, 1989, (session chair,) *The Linear Complexity Profile of Cryptosystem PGM.*

48. *Invited speaker*, American Mathematical Society, Special Session on *Codes and Designs, Loyolla University, Chicago, Ill.* May 19-20, 1989, presented a paper on *Possible Automorphism Groups of an S(3,5,26).*

49. Third Vermont Summer Workshop on Combinatorics and Graph Theory, Stow, Vermont, June 13-19, 1989, presented a paper on *On the Steiner Systems S(3,5,26)*, (invitation.)

50. Crypto '89, The annual conference of the International Association for Cryptographic Research, UC Santa Barbara, August 20-24, 1989, presented paper on *Properties of Cryptosystem PGM.*

51. *Invited speaker*, talk on *Algebraic Cryptosystems*, Third Auburn Combinatorics Conference, March 21-24, 1990.

52. *Invited speaker*, American Mathematical Society, Regional meeting #855 - Manhattan, Kansas, Special Session on *Groups and Geometries*, March 16 - 17, 1990. Talk on *Orthogonal Resolutions of Combinatorial Designs.*

53. Combinatorics '90, Gaeta - Italy, May 20 - 27 1990, Presented a paper on *Large Sets of t-designs.*

54. Participated in the *Fourth Czechoslovak Symposium on Combinatorics* at Prahatice, Czechoslovakia - June 10 - 16, 1990.

55. Crypto '90, The annual conference of the International Association for Cryptographic Research, UC Santa Barbara, August 11-15, 1990.

56. *Invited speaker*, Fifth Carbondale Combinatorics Conference, Southern Illinois University - Carbondale, November 1-3, 1990, *Resolutions of t-designs.*

57. Sixteenth Australasian Conference on Combinatorial Mathematics and Combinatorial Computing, Talk on *Large sets of* $t-(v,k,\lambda)$ *designs.* Massey University, Palmerston North, New Zealand, December 3-7, 1990.

58. Design Theory Conference, Auburn University, March 19-23, 1991.

59. Third Vermont Conference on Combinatorics, talk: *On automorphisms of an S(3,5,26)*; Stow, Vermont, June 25-30, 1991, (invitation.)

60. Crypto '91, The annual conference of the International Association for Cryptographic Research, UC Santa Barbara, August 11-15, 1991, was elected *General Chair* for Crypto '92.

61. *Invited speaker*, 21st Annual Manitoba Conference on Numerical Mathematics and Computing, October 3-5, 1991.

62. *Organizer*, $6MC^4$:*Sixth Midwestern Conference on Combinatorics, Cryptography and Computing*, held at The University of Nebraska – Lincoln, on October 31 – November 2, 1991.

63. Twenty third Southeastern International Conference on Combinatorics Graph Theory and Computing, Florida Atlantic University, Boca Raton, Fla., February 3 – 7, 1992, (session chair.)

64. General Chair: Crypto '92, The annual conference of the International Association for Cryptographic Research, UC Santa Barbara, August 16-20, 1992.

65. Mathematisches Forschungsinstitut Oberwolfach, Combinatorics, November 1 - 7, 1992. *New infinite families of large sets of t-designs*, (invitation).

66. Twenty fourth Southeastern International Conference on Combinatorics Graph Theory and Computing, Florida Atlantic University, *Tree-codes in Lossless Image compression*, Boca Raton, Fla., February 22 – 26, 1993, (session chair.)

67. International Conference on Group Theory, *Logarithmic signatures and factorization in Finite Groups* Spetses, Greece, July 13-23, 1993.

68. Crypto '93, The annual conference of the International Association for Cryptographic Research, UC Santa Barbara, August 16-20, 1993, (session chair).

69. Eight Midwestern Conference in *Combinatorics, Cryptography & Computing*, Wichita, Kansas, October 20-23, 1993. paper: *Maximum order complexity in DNA*, (session chair.)

70. Fifth Auburn Combinatorics Conference, Auburn University, March 23 - 26, 1994.

71. Mathematisches Forschungsinstitut Oberwolfach, Combinatorics, April 16 - 23, 1994, conference on *Codes & Designs*, paper: *Block transitive resolutions of t-designsn and Room rectangles*, (invitation).

72. Vermont Summer Workshop in Combinatorics, June 14-20, 1994, Univ. of Vermont, Burlington, VT. (invitation).

73. *Invited speaker*, Second Upper-Michigan Combinatorics Workshop on *Codes, Designs, and Geometries*, Michigan Technological University, Houghton, Michigan, August 17-20, 1994.

74. Crypto '94, The annual conference of the International Association for Cryptographic Research, UC Santa Barbara, August 21-25, 1994, paper: *A parallel Permutation Multiplier for a PGM Crypto-chip*, with Tamás Horváth & Tran van Trung,

75. *Organizer*, $9MC^4$:*Ninth Midwestern Conference on Combinatorics, Cryptography and Computing*, held at The University of Nebraska – Lincoln, on October 20-22, 1994.

76. Sixth Auburn Combinatorics Conference, Auburn University, March 23 - 25, 1995, (invitation).

77. DIMACS workshop on Groups and Computation, June 7-10, 1995 *A Cryptosystem Based on Permutation Groups*, (invitation).

78. 25th Manitoba Conference on Combinatorial Mathematics and Computing, September 29 - October 1, 1995, (invitation.)

79. Session chair, $10MC^4$:*Tenth Midwestern Conference on Combinatorics, Cryptography and Computing*, held at Southern Illinois University, Carbondale, IL. on October 18 – 21, 1995.

80. Seventh Auburn Combinatorics Conference, Auburn University, March 20 - 24, 1996.

81. *Principal Organizer* of the *First Pythagorean Conference* An International Research Conference in *Geometry, Combinatorial Designs and Applications* to be held on the island of Spetses, Greece on June 1-7, 1996. The workshop is co-sponsored by several international Institutions.

82. Data Compression Conference, Snowbird, Utah, March 25 - 27, 1997. *A lexical permutation sorting algorithm*, with Z. Arnavut.

83. Eighth Auburn Combinatorics Conference, Auburn University, March 27 - 30, 1997.

84. *Crypto/Codes 1997*, May 31 - June 4, 1997, Lincoln, Nebraska. Principal conference organizer. An event sponsored by the Discrete and Exp. Math. AOS, UNL, and affiliate (CSE, Math-Stats, EE.) Departments.

85. Keynote speaker at the Twelveth Midwestern Conference on Combinatorics, Cryptography and Computing, *On large sets of t-designs*. Indiana State University, Terre Haute, Ind., October 29 - Nov. 2, 1997.

86. Combinatorics '98, Palermo - Italy, *Semiregular Large Sets of t-designs*, June 15 - 20 1998.

87. *Invited speaker*, IMA Workshop on *Coding, Cryptography and Designs*, Institute of Mathematics and its Applications, University of Minnesotta, Minneapolis, July 6 - 18, 1998.

88. *Principal Organizer* of the *Second Pythagorean Conference* An International Research Conference in *Geometry, Combinatorial Designs and Applications* held at Pythagoreion, Samos, Greece on May 31-June 5, 1999. The workshop was co-sponsored by several international Institutions.

89. *Plenary Speaker*, Regional Conference in the Mathematical Sciences, University of Nebraska - Lincoln, *Groups in Cryptology*, October 27, 2000

90. *Plenary Speaker*, TatraCrypt'01, Liptovsky Jan, Slovakia "The Central European Conference in Cryptography", June 21-23, 2001.

91. *Plenary Speaker*, NSF - EPSCoR Conference, *Diversity of Informatics*, Session on Computer and Information Security, *Towards New Public Key Cryptosystems*, Lincoln, Nebraska, April 4-5, 2002

92. *Invited Speaker*, "Group theoretic cryptography", Canadian Mathematical Society, Summer Meeting 2002, *Université Laval*, Quebec City, June 15-17, 2002, *Session on Cryptology,*

93. *Invited Speaker*, "Non-solvable groups in cryptography", HajduCrypt '02, Second Central European Conference on Cryptology, Debrecen, Hungary, July 4-6, 2002.

94. *Plenary Speaker*, "Trap doors from subgroup chains and recombinant bilateral transversals", VII Spanish Meeting on Cryptology & Information Security , Oviedo, Asturias, Spain, 5-7 September, 2002.

95. *First Irsee Conference*, Finite Geometries, Irsee, Germany, Feb 16-21, 2003.

96. *Plenary Speaker*, "Something Euler Might Have Liked", 34^{th} *Southeastern Conference on Combinatorics, Graph Theory and Computing*, Boca Raton, Florida; March 7, 2003.

97. Principal Organizer, Third Pythagorean Conference, *Geometry, Combinatorial Designs and Cryptology.* Faliraki, Rhodes, Greece, June 1-7, 2003

98. *Plenary Speaker*, "Cryptographic Primitives Based on Groups of Hidden Order", TatraCrypt 2003, "The Third Central European Conference on Cryptology", Bratislava, Slovakia, June 26-28, 2003.

99. *Program Committee Member*, WartaCrypt '04, "The Fourth Central European Conference on Cryptology", Bedlewo, Poland, July 1-3, 2004.

100. *Plenary Speaker*, "Group theoretic methods in the construction of large sets of t-designs", Algebraic Combinatorics & Applications (ALCOMA '05), *Designs and Codes*, April 3-10, 2005, Thurnau, Germany.

101. *Program Committee Member*, MoraviaCrypt '05, "The Fifth Central European Conference on Cryptology", Brno, Czech Republic, June 15-17, 2005.

102. *Plenary Speaker*, "Ten Lectures in Cryptology, Groups and Geometry", *Summer School on Combinatorial Geometries "Giuseppe Tallini"*, Potenza - Italy, September 5-9, 2005.

103. *Program Committee Member*, NyirCrypt '06, "The Sixth Central European Conference on Cryptology", Nyiregyhaza, Hungary, June 15-17, 2006.

104. *Invited Speaker*, "New Approaches to Designing Public Key Cryptosystems Based on Finite Groups", 2006 SIAM Discrete Math. MS32, *Cryptography & Security* Victoria, Canada, June 28, 2006.

105. *Plenary Speaker*, "Group Theoretic Cryptography", TatraCrypt '07, The Seventh Central European Conference on Cryptography, Smolenice Castle, Slovakia, June 22-24, 2007.

106. *Plenary Speaker*, "Large sets of t-designs and orthogonality", Conference on Combinatorial Designs (in honor of Alex Rosa's 70th birthday), Bratislava, Slovakia, July 2-6, 2007.

107. *Participant - First Istanbul Design Theory and Combinatorics Conference*, In honor of Curt Lindner's 70^{th} birthday. Koç University, Istanbul, June 15 -21, 2008.

108. *Plenary Speaker*, "Orthogonal resolutions of t-designs", *Combinatorics 2008.* International conference on pure and applied combinatorics and its connection with Geometry, Graph Theory and Algebra. Costermano, Lake Garda (VR), Italy, June 22 - 28, 2008.

109. *Plenary Speaker*, "Group factorizations and non-abelian discrete logarithms", 8^{th} *Central European Conference on Cryptography* CECC. Institut für Mathematik; Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie, TU, Graz, Austria, July 2 - 4, 2008.

110. *Plenary Speaker*, "Non-abelian discrete logarithms and minimal logarithmic signatures", 22^{nd} *Midwest Conference on Combinatorics, Cryptography and Computing*, UNLV, Las Vegas, Nevada, October 22 - 24, 2008.

111. *Participant*, *NormFest 2009*, International Conference on Finite Geometry to honor Norman L. Johnson, University of Texas, San Antonio, March 26-29, 2009.

112. *Participant - CDFG 2009*: "Cryptology, Designs, and Finite Groups 2009" Conference. In honor of Spyros Magliveras' 70^{th} birthday. Dearfield Beach, Florida, May 17–22, 2009.

113. *Participant*, *CCA 2009* : "Combinatorial Configurations and their Applications 2009", Michigan Technical University, Houghton, Michigan, August 6–8, 2009.

114. *Plenary Speaker*, *MJdR* "A Conference in honor of Prof. Marialuisa J. de Resmini", Università di Roma, *La Sapienza*, Rome, Italy, September 23–25, 2009.

115. *Plenary Speaker*, *LaueFest*, "A Conference in honor of Professor Dr. Reinhard Laue", Universität Bayreuth, Bayreuth, Germany, January 30, 2010.

116. *Principal Organizer* of the *Fourth Pythagorean Conference* An Advanced Research Workshop in *Geometry, Combinatorial Designs and Cryptology* held in Corfu, Greece on May 30-June 4, 2010.

117. *Plenary Speaker*, at the "NATO Advanced Study Institute", Opatija, Croatia, June 7–11, 2010.

118. *Invited Speaker*, at the *Centre de Recherches Mathématiques* (CRM), "Workshop on Complexity and Group-based Cryptography", August 30-September 3, 2010
(http://www.crm.umontreal.ca/Complex10/index_e.php)

119. *General Chair and Principal Organizer* of *ISC 2010 : The 13^{th} Information Security Conference*, Annual International Conference on all aspects of Information Security and Applied Cryptology, Boca Raton, Florida , October 25-28 , 2010. (http://math.fau.edu/ $\sim$ isc2010/)

120. *Plenary Speaker*, at the "Second Istanbul Design Theory, Graph Theory and Combinatorics Conference", *Resolutions of t-designs, orthogonality and group-theoretic constructions*, Istanbul, Turkey, June 27–July 1, 2011.

121. *Participant*, 43^{rd} *Southeastern Conference on Combinatorics, Graph Theory and Computing*, Boca Raton, Florida, March 5-9, 2012.

122. *Plenary Speaker*, at "Trung-Fest", workshop in honor of Prof. Tran van Trung, on *Groups, Designs and Cryptography* at the Institute for Experimetal Mathematics, University of Duisburg-Essen, June 21-22, 2012.

123. *Program Committee member, Participant and session Chair*, Tatracrypt 2012 - the 12th Central European Conference on Cryptology , July 2-4, 2012, Smolenice, Slovakia.

124. *Participant*, 44^{rd} *Southeastern Conference on Combinatorics, Graph Theory and Computing*, Boca Raton, Florida, March 4-8, 2013.

125. *Program Committee member*, Second International Workshop on Modern Cryptography and Security Engineering, http://mocrysen2013.inria.fr/ to be held on 2–6 September 2013, in Regensburg, France.

126. *Participant*, 45^{th} *Southeastern Conference on Combinatorics, Graph Theory and Computing*, Boca Raton, Florida, March 3-7, 2014.

127. *Program Committee member, Participant and Session Chair*, 14^{th} *Central European Conference on Cryptology*, Alfréd Rényi Institute of Mathematics and Math. Dept. of the Central European Univ., Budapest, Hungary, May 21-23, 2014.

128. *Invited Speaker*, SIAM Conference on Discrete Mathematics, Session on Designs, *On Large Sets*, Mineapolis, Minnesota, June 16-19, 2014.

129. *Participant*, 46^{th} *Southeastern Conference on Combinatorics, Graph Theory and Computing*, Boca Raton, Florida, March 3-7, 2014.

130. *Plenary Speaker*, Algebraic Combinatorics and Applications - The First annual Kliakhandler Conference, *New Large Sets of Geometric Designs*, Michigan Technological University, Houghton, Michagan, August 26-30, 2015.

REFEREED PUBLICATIONS:

[1] S.S. Magliveras and D. Pelz, Correlational Properties of Simulated Panel Data with Causal Connections Between Variables, *Monogram, ISR-ICPR, Survey Research Center Publications*, Ann Arbor, 1968.

[2] S.S. Magliveras, The Subgroup Structure of the Higman-Sims Simple Group, *Bull. Amer. Math. Soc.*, vol. 77, No. 4 (1971), pp. 535-539.

[3] E.S. Kramer and S.S. Magliveras, Some Mutually Disjoint Steiner Systems, *J. Comb. Th. (A)*, vol. 17, No. 1 (1974), pp. 39-44.

[4] S.S. Magliveras, On Transitive Extensions of the Higman-Sims Simple Group, *J. Alg.,* vol. 30, No. 1-3 (1974), pp. 317-319.

[5] S.S. Magliveras, The Non-existence of Rank-3 Transitive Extensions of the Higman-Sims Simple Group, *Proceedings of the Utah Conference on Finite Groups*, Academic Press, (1976), pp 457-469.

[6] E.S. Kramer and S.S. Magliveras, A $57 \times 57 \times 57$ Room-type Design, *Ars Combinatoria,* **9** (1980), pp. 163-166.

[7] E.S. Kramer, S.S. Magliveras, D.M. Mesner, Some Resolutions of S(5,8,24), *J. Comb. Th. (A)*, **29** (1980), pp. 166-173.

[8] E.S. Kramer, S.S. Magliveras, D.M. Mesner, t-Designs from the Large Mathieu Groups, *Discrete Math.,* **36** (1981), pp. 171-189.

[9] E.S. Kramer, D.L. Kreher, S.S. Magliveras and D.M. Mesner, Coherent Room Rectangles from Permutation Groups, *Ars Combinatoria,* **9** (1981), pp. 101-111.

[10] E.S. Kramer, S.S. Magliveras, D.M. Mesner, An Assortment of Room-type Designs, *Ars Combinatoria,* **11** (1981), pp. 9-29.

[11] S.S. Magliveras and D.W. Leavitt, Simple 6-(33,8,36) Designs from $P\Gamma L(2, 32)$, *Proc. of the Durham Computational Group Theory Symposium,* Academic Press, (1983), pp. 337-352.

[12] S.S. Magliveras and D.W. Leavitt, Simple Six-Designs Exist!, *Congr. Numer.,* **40** (1983), pp. 195-205.

[13] S.S. Magliveras, B.A. Oberg and A.J. Surkan, A New Random Number Generator from Permutation Groups, *Rend. del Sem. Matemat. e Fis. di Milano,* **LIV** (1984), pp. 203-223.

[14] E.S. Kramer, S.S. Magliveras and D.W. Leavitt, Construction Procedures for t-Designs and the Existence of New Simple 6-designs, *Annals of Discrete Mathematics,* **26** (1985), pp. 247-274.

[15] S.S. Magliveras and L.C. Yu, On Methods of Determining Subgroups Structures of Finite Groups, *Eleuth. Greek Math. J. Semin.,* vol A (1986), pp. 37-67.

[16] S.S. Magliveras, L. DiMartino, J. Siemons, Primitivity on Points Implies Primitivity on Lines, *Congr. Numer.,* **55** (1986), pp. 77-80.

[17] S.S. Magliveras and K.C. Tam, On the Ternary Code of the Desarguesian Plane of Order 9, *Proceedings of the 29th Midwest Symposium on Circuits and Systems,* Elsevier Publ. Co. (1986), pp. 968-971.

[18] S.S. Magliveras, A Cryptosystem from Logarithmic Signatures of Finite Groups, *Proceedings of the 29th Midwest Symposium on Circuits and Systems,* Elsevier Publ. Co. (1986), pp. 972-975.

[19] E.S. Kramer, S.S. Magliveras and V.D. Tonchev, On Steiner Systems S(2,4,25) Invariant Under a Group of Order 9, *Annals of Discrete Mathematics,* **34** (1987), pp. 307-314.

[20] S.S. Magliveras, N. Tsolas and Y.S. Shen, On the Number of Classes under Permutation Equivalence of q-valued $m \times n$ Incidence Arrays, *Congr. Numerant.,* **59** (1987), pp. 211-216.

[21] S.S. Magliveras and T.E. Plambeck, New Infinite Families of Simple 5-Designs, *J. Comb. Th. (A)*, **44** (1987), pp. 1-5.

[22] D.A. Klarner and S.S. Magliveras, Tilings of a Block with Blocks, *Europ. J. Combinatorics,* **9** (1988), pp. 317-330.

[23] S.S. Magliveras, and K.C. Tam, The Number of Classes under Permutation Equivalence of Multidimensional, q-valued Incidence Matrices, *Proc. 30th Midwest Symp. Circuits and Systems,* Elsevier Publ. Co. (1988), pp. 1004-1008.

[24] E.S. Kramer, and S.S. Magliveras, Coloring the Perfect Squared Square, *J. Rec. Math.,* **20** (1988), pp. 1-6.

[25] E.S. Kramer, S.S. Magliveras and R. Mathon, The Steiner Systems S(2,4,25) with Nontrivial Automorphism Group, *J. Discr. Math.,* **77** (1989), pp. 137-157.

[26] S.S. Magliveras and N.D. Memon, Properties of Cryptosystem PGM, *Advances in Cryptology*, Lecture Notes in Comp. Sc., Springer Verlag, **435** (1989), pp. 447-460.

[27] S.S. Magliveras and N.D. Memon, Random Permutations from Logarithmic Signatures, *Computing in the 90's, First Great Lakes Comp. Sc. Conf., Lecture Notes in Computer Science, Springer-Verlag* **507** (1989), pp. 91-97.

[28] S.S. Magliveras and E.S. Kramer, Editors, Finite Geometries and Combinatorial Designs, *AMS volume in Contemporary Math. Series,* **111** (1990) 312 pages, ISBN 0-8218-5118-7, ISSN 0271-4132.

[29] S.S. Magliveras and N. Memon, The Linear Complexity Profile of Cryptosystem PGM, *Congr. Numerant.,* **72** (1990), pp. 51-60.

[30] S.S. Magliveras, N.D. Memon, and K.C. Tam, Complexity Tests of Cryptosystem PGM, *Congr. Numerant.* **79** (1990), pp. 61-68.

[31] E.S. Kramer, S.S. Magliveras, Tran van Trung and Qiu-Rong Wu, Some perpendicular arrays for arbitrarily large t, *J. of Discrete Math.*, **97** (1991) pp. 101-110.

[32] E.S. Kramer, S.S. Magliveras and D.R. Stinson, Some small large sets of t-designs, *Australasian J. Comb.,* **3** (1991) pp. 191-205.

[33] N.D. Memon, S.S. Magliveras and K. Sayood, Prediction Trees and Lossless Image Compression, *Proceedings of the Data Compression Conference,* Editors: J. A. Storer and M. C. Cohn, *IEEE Comp. Soc. Press*, (1991), pp. 83-92.

[34] N.D. Memon, K. Sayood and S.S. Magliveras, Lossless image compression using a codebook of prediction trees, *IEEE Comp. Soc. Press,* Proc. Data Compression Conference, (1992), pp. 245.

[35] N.D. Memon, K. Sayood and S.S. Magliveras, Lossless image compression with efficient scanning patterns, *Proc. Twenty Sixth Annual Conf. on Infor. Sciences and Systems,* Princeton, (1992), pp. 256.

[36] C.J. Colbourn, S.S. Magliveras and R.A. Mathon, Transitive Steiner and Kirkman triple systems of order 27, *Math. of Computation,* **58**, No 197 (1992), pp. 441-450.

[37] E.S. Kramer, S.S. Magliveras and Tran van Trung, Possible automorphism groups of an S(3,5,26), J. Comb. Math. & Comb. Comp., **12** (1992), pp. 119-127.

[38] S.S. Magliveras and N.D. Memon, The Algebraic Properties of Cryptosystem PGM, *J. of Cryptology*, **5** (1992), pp. 167-183.

[39] C.J. Colbourn, S.S. Magliveras and D.R. Stinson, Steiner Triple Systems of Order 19 with Nontrivial Automorphism Group, *Math. of Computation,* **59**, No 199 (1992) pp. 283-295.

[40] E.S. Kramer, S.S. Magliveras, and E.A. O'Brien, Some new large sets of t-designs, *Australasian J. Comb.*, **7** (1993) pp. 189-193.

[41] S.S. Magliveras, N.D. Memon and K. Sayood, Tree-codes in Lossless Image Compression, *Congr. Numer.,* **95** (1993), pp. 117-130.

[42] N.D. Memon, K. Sayood and S.S. Magliveras, Simple method for enhancing the performance of lossy plus lossles image compression schemes, *J. Electr. Imaging* 2(3), (1993), pp. 245-252.

[43] N.D. Memon, K. Sayood and S.S. Magliveras, Reversible compression of multispectral images, *Proc. of the AIAA Computing in Aerospace 9 Conference,* (1993), pp. 148-156.

[44] N. D. Memon, K. Sayood and S. S. Magliveras, Efficient scan patterns for image decorrelation, Proceedings of the Thirty First Annual Allerton Conference on Communications, Control and Computing, September (1993), pp. 463-472.

[45] N.D. Memon, K. Sayood and S. Magliveras, Lossless Compression of Multispectral Image Data, *IEEE Trans. Geosc. Rem. Sensing,* **32** No. 2, (1994), pp. 282-289.

[46] T. Horváth, S.S. Magliveras and Tran van Trung, A Parallel Permutation Multiplier for a PGM Crypto-chip, *Advances in Cryptology*, Lecture Notes in Comp. Sc., Springer Verlag, **839** (1994), pp. 108-113.

[47] D. Memon, K. Sayood and S.S. Magliveras, Lossless Image Compression with a Codebook of Block Scans, *IEEE Trans. Sel. Areas of Communication*, **13**, No 1, (1995), pp. 24-31.

[48] S.S. Magliveras, Leo Chouinard and Robert Jajcay Finite Groups and Designs, *CRC Handbook of Combinatorial Designs*, CRC Press, C.J. Colbourn and J.H. Dinitz, eds.,(1996), pp. 587-615.

[49] M. Atici, S.S. Magliveras, D.R. Stinson and Wandi Wei, Some Recursive Constructions for Perfect Hash Families, *Journal of Combinatorial Designs*, **4**, No.5, (1996), pp. 353-363.

[50] S.S. Magliveras and Wandi Wei, Enumeration of certain binary vectors, *Australasian J. Comb.*, **14** (1996), pp. 61 - 75.

[51] R.A. Liebler, S.S. Magliveras and S.V. Tsaranov, Block transitive Resolutions of t-designs and Room rectangles, *J. for Stat. Plan. & Inference,* **58**, (1997), pp. 119-133.

[52] Z. Arnavut and S.S. Magliveras, Block sorting and compression, *Proceedings Data Compression Conference*, IEEE Computer Society Press, (1997), pp. 181 - 190.

[53] M.J. de Resmini, J.W.P. Hirschfeld, and S.S. Magliveras, Editors, Proceedings of the *First Pythagorean Conference*, London Math. Soc. Lecture Notes, Cambridge Univ. Press., **245**, (1997), pp. 1-258.

[54] Z. Arnavut and S.S. Magliveras, A lexical permutation sorting algorithm. *The Computer Journal,* **58**, No. 5, (1997), pp. 292-295.

[55] Y.M. Chee and S.S. Magliveras, A few more large sets of $t-$Designs. *Journal of Combinatorial Designs.*, **6**, No. 4, (1998), pp. 293 – 308.

[56] S.S. Magliveras and Wandi Wei, The number of classes under permutation equivalence of choice functions in $X^{\binom{X}{k}}$, *Australasian J. Comb.,* **17** (1998) pp. 289-294.

[57] C. Cusack, and S.S. Magliveras, Semiregular Large Sets of t-Designs. *Designs, Codes and Cryptography*, **18** (1999), pp. 81 – 87.

[58] M.J. de Resmini, J.W.P. Hirschfeld, and S.S. Magliveras, Editors, Proceedings of the *Second Pythagorean Conference*, Journal of Geometry, Springer-Verlag, **67** (2000), pp. 1 – 235.

[59] Valér Čanda, S. Magliveras, Tran van Trung, Tamás Horváth, Symmetric Block Ciphers Based on Group Bases, Proceedings of SAC 2000, *Selected Areas in Cryptography*, Springer-Verlag LNCS **2012**, (2000) pp. 89 – 105.

[60] R. Laue, S.S. Magliveras and A. Wassermann, New large sets of t-designs, *Journal of Combinatorial Designs*, **9**, No 1, (2001), pp. 40 – 59.

[61] I. Bluskov, and S.S. Magliveras On the Number of Mutually Disjoint Cyclic Designs and Large Sets of Designs, JSPI, **95**, Nos 1-2, (2001), pp. 133 – 142.

[62] O. Grošek, S.S. Magliveras and Wandi Wei, On the Security of a Public-Key Cryptosystem, Proceedings of the *Public-key Cryptography and Computational Number Theory* Conference, September 2000, Stefan Banah International Mathematics Center, Warsaw, Poland, Editor: Walter de Gruyter, Berlin - New York (2001), pp. 71 – 75.

[63] Xukai Zou, Byrav Ramamurthy, and Spyros S. Magliveras, Chinese Remainder Theorem Based Hierarchical Access Control for Secure Group Communication , International Conference on Information and Communication Security, November 2001, Xi'an, China. Lecture Notes in Computer Science (LNCS), **vol. 2229** (2001), Springer-Verlag, pp. 381–385

[64] S.S. Magliveras, Tran van Trung and D.R. Stinson, *New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups*, J. Cryptology, **15**, (2002), pp. 285 – 297.

[65] Xukai Zou, B. Ramamurthy and S. Magliveras, *Routing techniques for wireless ad hoc networks – classification and comparison*, Proceedings of the Sixth World Multiconference on Systemics, Cybernetics, and Informatics, July, 2002, Orlando, Florida.

[66] Spyros S. Magliveras, *Secret- and Public-key Cryptosystems from Group Factorizations*, Tatra Mt. Math. Pub., **25**, (2002), pp. 11 - 22.

[67] Xukai Zou, Spyros S. Magliveras and Byrav Ramamurthy, *A dynamic conference scheme extension with efficient bursty operation*, *Cong. Numerantium* **158** (2002), pp. 83 – 92.

[68] Xukai Zou, Byrav Ramamurthy, and Spyros Magliveras *Efficient Key Management for Secure Group Communications with Bursty Behavior*, Proceedings of International Conference on Communication, Internet, and Information Technology, Virgin Islands, November 2002, pp. 148 – 153.

[69] J.C. Birget, S.S. Magliveras and Wandi Wei, *Trap doors from subgroup chains and recombinant bilateral transversals*, in the Proceedings of RECSI VII, Asturias - Spain, 2002, pp. 31 – 48.

[70] Wandi Wei, Tran van Trung, Spyros S. Magliveras and Frederick Hoffman, *Cryptographic primitives based on groups of hidden order*, Tatra Mt. Math. Publ. **29** (2004), pp. 147 – 155.

[71] Wandi Wei, Tran van Trung and Spyros S. Magliveras, *Signature Schemes Based on a Group of Hidden Order*, submitted to the Journal of Cryptology.

[72] Xukai Zou, Spyros S. Magliveras and Byrav Ramamurthy, *A GCD attack resistant CRTHACS for secure group communications*, Proceedings of International Conference on Information Technology, ITCC 2004, April 5-7, (2004), Las Vegas, NV, USA, pp. 153 – 154.

[73] O. Grošek, M.J. de Resmini, J.W.P. Hirschfeld, and S.S. Magliveras, Editors, Proceedings of the "Third Pythagorean Conference", *Designs, Codes and Cryptography*, Kluwer, **32**, (2004) Nos 1-3, pp. 1 – 396.

[74] Xukai Zou, Byrav Ramamurthy and Spyros S. Magliveras, *Secure Group Communications Over Data Networks*, ISBN 0-387-22970-1, Springer (2005), pp. 1 – 172.

[75] S.S. Magliveras, Tran van Trung, and Wandi Wei, *New approaches to designing public-key cryptosystems based on finite groups*, accepted for presentation at MoraviaCrypt '05, Brno, The Czech Republic, 15-17 June, (2005).

[76] Daniel Socek, Shujun Li, Spyros Magliveras, and Borko Furht, *Enhanced 1-D Chaotic Key-Based Algorithm for Image encryption*, IEEE / CreateNet SecureComm '05, Athens Greece, September 5 - 9, (2005), pp. 406-408.

[77] Daniel Socek, and Spyros S. Magliveras, *General Access Structures in Audio Cryptography*, presented at the IEEE-EIT Conference, Lincoln, NE., May 22-25, (2005).

[78] B. Wu, J. Wu, E.B. Fernandez, and Spyros S. Magliveras, *Secure and Efficient Key Management in Mobile Ad Hoc Networks*, IPDPS, IEEE Computer Soc., (2005), ISBN 0-7695-2312-9.

[79] Otokar Grošek, Spyros Magliveras, Ján Ťapuška, and Wandi Wei, *Is Rijndael really independent of the field polynomial*, Tatra Mt. Publ. **33** (2006), pp. 51 – 69.

[80] Jean-Camille Birget, Spyros S. Magliveras, and Michal Sramka, *On public-key cryptosystems based on combinat. group theory*, Tatra Mt. Publ. **33** (2006), pp. 137 – 148.

[81] Daniel Socek, Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Culibrk and Borko Furht, *A permutation based correlation-preserving encryption method for digital videos*, ICIAR 2006, September 18-20, 2006, Póvoa de Varzim, Portugal, LNCS 4141 Springer (2006), pp. 547-558.

[82] Leo G. Chouinard II, Robert Jajcay and Spyros S. Magliveras, *Finite Groups and Designs*, Handbook of Combinatorial Designs, C.J. Colbourn and J.H. Dinitz editors, Chapman & Hall / CRC ISBN 1-58488-506-8, (2007), pp. 819-847.

[83] Daniel Socek, Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Culibrk and Borko Furht, *New approaches to encryption and steganography for digital videos*, *Multimedia Systems Journal*, **13**, no. 3, Springer-Verlag, (2007), pp. 191-204.

[84] Daniel Socek, Hari Kalva, Spyros S. Magliveras, Oge Marques, Dubravko Culibrk and Borko Furht, *Digital Video Encryption Algorithms Based on Correlation Preserving Permutations*, *EURASIP Journal on Information Security*, vol. 2007, Article ID 52965, 15 pages, 2007.

[85] B. Wu, J. Wu, E. B. Fernandez, M. Ilyas, and S. S. Magliveras, *Secure and efficient key management in mobile ad hoc networks*, J. of Network and Computer Applications, Academic Press, issn 1084-8045 **30**, no. 3, (2007), pp. 937-954.

[86] S.S. Magliveras, Tran van Trung and Wandi Wei, *Primitive sets in a lattice*, Austral. J. Comb. **40** (2008), pp. 173-186.

[87] S. S. Magliveras, P. Svaba, Tran van Trung and P. Zajac, *On the security of a realization of cryptosystem MST_3*, Tatra Mt. Publ. **41** (2008), pp. 1–13.

[88] S. S. Magliveras, Wandi Wei and Xukai Zou , *Notes on the CRTDH Group Key Agreement Protocol*, 28^{th} International Conference on Distributed Computing Systems Workshops, IEEE Computer Society, DOI 10.1109/ICDCS.Workshops.2008.36, pp. 406 – 411.

[89] Wolfgang Lempken, Spyros S. Magliveras, Tran van Trung and Wandi Wei, *A public key cryptosystem based on non-abelian finite groups*, J. Cryptology, **22**, (2009) pp. 62 – 74.

[90] Spyros S. Magliveras, *Large sets of t-designs from groups*, Mathematica Slovaca, vol. **59**, no 1, (2009) pp. 1–20.

[91] Lee Klingler, Spyros S. Magliveras, Fred Richman, and Michal Sramka, *Discrete logarithms for finite groups*. Computing **85** (2009), pp. 3–19.

[92] Paula Carrillo, Hari Kalva, and Spyros S. Magliveras, *Compression independent reversible encryption for privacy in video surveillance*, EURASIP J. on Information Security, Article ID 429581, (2009), 13 pages.

[93] Cafer Çalışkan and Spyros S. Magliveras, *Subplanes of projective planes of order 121*, J. Geom. **97** (2010), pp. 17-27.

[94] Ivana Ilić and Spyros S. Magliveras, *Weak discrete logarithms in non-abelian groups*, J. of Combinatorial Math. and Comb. Computing (JCMCC) **74** (2010), pp. 3–11.

[95] Cafer Çalışkan and Spyros S. Magliveras, *Reconstructing a VW plane from its colineation group*, J. of Combinatorial Math. and Comb. Computing (JCMCC) **74** (2010), pp. 117–127.

[96] Nidhi Singhi, Nikhil Singhi and Spyros S. Magliveras, *Minimal logarithmic signatures for finite groups of Lie type*, Designs, Codes and Cryptography (DCC), **55** (2010), pp. 243–260.

[97] Cafer Çalışkan, Spyros S. Magliveras and Lucille C. Yu, *Combinatorial methods for determining subgroup structures of finite groups*, Rendiconti di Matematica, serie VII, **30**, no 1 (2010), pp. 121–144.

[98] Markus Grassl, Ivana Ilić, Spyros S. Magliveras, and Rainer Steinwandt, *Cryptanalysis of the Tillich-Zémor hash function*, J. Cryptology, (JOC) **24** (2011), pp. 148 – 156.

[99] Ivana Ilić, and Spyros S. Magliveras, *Crypto applications of combinatorial group theory*, Information Security, Coding Theory and Related Combinatorics, D. Crnković and V. Tonchev (Eds.), ASI-NATO volume, IOS Press (2011) pp. 1 – 16.

[100] Kenneth Matheis , and Spyros S. Magliveras, *Generating rooted trees of m nodes uniformly at random*, Information Security, Coding Theory and Related Combinatorics, D. Crnković and V. Tonchev (Eds.), ASI-NATO volume, IOS Press (2011) pp. 17 – 26.

[101] Spyros S. Magliveras, Tran van Trung, and Wandi Wei, *On Jacobsthal Binary Sequences*, Information Security, Coding Theory and Related Combinatorics, D. Crnković and V. Tonchev (Eds.), ASI-NATO volume, IOS Press (2011) pp. 27 – 37.

[102] Mike Burmester, Gene Tsudik, Spyros S. Magliveras, and Ivana Ilić (Co-Editors), *Information Security*. Thirteenth International Conference, ISC2010, October 2010, Boca Raton, FL. Lecture Notes in Computer Science (LNCS), **vol. 6531** (2011), Springer-Verlag, pp. 001–423.

[103] Ivana Ilić, Spyros Magliveras and Nicola Pace, *Decomposing the Higman-Sims graph into double Petersen graphs*, J. of Combinatorial Math. and Comb. Computing (JCMCC) **vol. 80** (2012), pp. 267–275.

[104] Arrigo Bonisoli, James Hirschfeldt and Spyros Magliveras, *Geometry, combinatorial designs and cryptology*, DCC *Designs, Codes and Cryptography*, Springer, **vol. 64** Numbers 1-2 (2012), 1-2 doi 10.1007/s10623-011-9607-9.

[105] Emre Kolotoğlu, Spyros Magliveras and Nicola Pace, *Related decompositions and new constructions of the Higman-Sims and Hall-Janko graphs*, Australasian J. Combinatorics, **vol. 54** (2012), pp. 217-230.

[106] Emre Kolotoğlu and Spyros Magliveras, *On large sets of projective planes of orders 3 and 4*, Discrete Math. **313** (20) (2013), pp. 2247-2252.

[107] Emre Kolotoğlu and Spyros Magliveras, *On the possible automorphism groups of a Steiner quintuple system of order 21*, J. Comb. Designs (JCD) 22: 495-505. doi10.1002/jcd.21370.

[108] Krishna T. Magar and Spyros Magliveras, *A new construction of the Hoffman-Singleton graph using a well known peculiarity of* $\mathbb{A}_6$, Cong. Numerant. **215** (2013), pp. 97-103.

[109] Michael Epstein, and Spyros S. Magliveras, *The covering number of the Mathieu group* M_{24}, J. Algebra Comb. Discrete Appl. **3** (3) (2016), pp. 155-158.

[110] Michael Epstein, Spyros S. Magliveras, and Daniela Nikolova-Popova, *The covering numbers of* $\mathbb{A}_9$ *and* $\mathbb{A}_{11}$ JCMCC **101** (2017), pp. 23-36.

[111] Michael Hurley, Bal Khadka ans Spyros S. Magliveras, *Some new large stets of geometric designs of type* $LS[3][2, 3, 2^8]$, J. Algebra Comb. Discrete Appl. **3** (3) (2016), pp. 165-176.

[112] Dieter Jungnickel, Spyros S. Magliveras, Vladimir D. Tonchev and Alfred Wassermann, *On classifying Steiner triple systems by their 3-rank* In: MACIS 2017 (J. Blömer et al., Eds.). *Lecture Notes in Computer Science* **10693** (2018), pp 295–305, Springer, New York.

[113] Dieter Jungnickel, Spyros S. Magliveras, Vladimir D. Tonchev and Alfred Wassermann, *The classification of Steiner triple systems on 27 points with 3-rank 24*, Designs, Codes and Cryptography, DCC 87(4):831-839,2019. DOI:10.1007/s10623-018-0502-5.

[114] Michael Hurley, Oscar Lopez, Spyros S. Magliveras, *Some New Familes of 2-Resolutions*, Chapter 16 of *50 Years of Combinatorics, Graph Theory, and Computing*, 2019.

COURSES TAUGHT:

i) Mathematics:
undergraduate: Calculus I, II & III; Ordinary Differential Equations; Advanced Mathematics for Engineers & Scientists; Linear Algebra; Abstract Algebra I & II; Combinatorics; Number Theory; Probability & Statistics.
graduate: Cryptography; Cryptanalysis; General Group Theory; Finite Groups; Algebra I & II; Algebraic Coding Theory; Combinatorics; Approximation of Functions; Representation Theory; Character Theory; Finite Geometries, Combinatorial Designs.

ii) **Computer Science:**
undergraduate: Introduction to Computer Science; Discrete Mathematics; Data Structures; Design and Analysis of Algorithms; Numerical Analysis I & II; Numerical Linear Algebra; Information Retrieval; Computer Organization; Computer Architecture; Microprocessors; Computer Networks; Error Correcting Codes; Computer & Networks Security.
graduate: Operations Research; Information Retrieval; Networks; Combinatorial methods; Coding Theory ; Data Encryption ; Complexity of Algorithms; Advanced Cryptology; Computational Algebra; Computational methods in Group Theory; Computational methods in Number Theory; Information Theory; Data Compression.

SUPERVISOR OF Ph.D. and MASTERS STUDENTS:

Completed Ph.D. dissertations:

1. Donald L. Kreher, Ph.D., University of Nebraska - Lincoln (1984), *Algebraic Methods in the Theory of Combinatorial Designs.*
2. Nasir D. Memon, Ph.D., University of Nebraska - Lincoln (1992), *Image Compression Using Efficient Scan Patterns.*
3. Robert Jajcay, Ph.D., University of Nebraska - Lincoln (1995), *Vertex-Transitive Graphs and Maps and their Automorphism Groups.*
4. Wan-Di Wei, Ph.D., University of Nebraska - Lincoln/Technical Slovak Univ. (1995), *A Contribution to Nine Selected Problems in Computer Science.*
5. Ziya Arnavut, Ph.D., University of Nebraska - Lincoln (1995), *Permutation Techniques in Lossless Image Compression.*
6. Chuck Cusack, Ph.D., University of Nebraska - Lincoln (2000), *Group Factorizations in Cryptography.*
7. Xukai Zou, Ph.D., University of Nebraska - Lincoln (2000), *Secure Group Communications and Hierarchical Access Control.*
8. Ayan Mahalanobis, Ph.D., Florida Atlantic University (2005), *Diffie-Hellman Key Exchange Protocol, its Generalization and Nilpotent Groups.*
9. Daniel Socek, Ph.D., Florida Atlantic University (2006), *Permutation-Based Transformations for Digital Multimedia Encryption and Steganography.*
10. Michal Sramka, Ph.D., Florida Atlantic University (2006), *New Results in Group Theoretic Cryptology.*
11. Vladimir Božović, Ph.D., Florida Atlantic University (2008), *Algebraic and Combinatorial Aspects of Groups Factorizations.*
12. Cafer Çalişkan, Ph.D., Florida Atlantic University (2010), *On Projective Planes.*
13. Ivana Ilić, Ph.D., Florida Atlantic University (2010), *Disrete Logarithm Problem in Non-abelian Groups.*
14. Kenneth Matheis, Ph.D., Florida Atlantic University (2010), *An Algebraic Attack on Block Ciphers.*

15. Nikhil Singhi, Ph.D., Florida Atlantic University (2011), *The Existence of Minimal Logarithmic Signatures for Classical Groups.*

16. Nidhi Singhi, Ph.D., Florida Atlantic University (2011), *On the Minimal Logarithmic Signature Conjecture.*

17. Nicola Pace, Ph.D., Florida Atlantic University (2012), *Coset Intersection Problem and Application to 3-Nets.*

18. Emre Kolotoğlu, Ph.D., Florida Atlantic University (2013), *Construction of Combinatorial Designs with Prescribed Automorphism Groups.*

19. Krishna B. Thapa Magar, Ph.D., Florida Atlantic University (2015), *Low Rank Transitive Representations, Primitive Extensions, and the Collision Problem in $PSL_2(q)$.*

20. Bal Kumar Khadka, Ph.D., Florida Atlantic University (2016), *Optimization techniques for Lattice Basis Reduction.*

21. Michael Hurley, Ph.D. Florida Atlantic University (2016), *New Geometric Large sets*,

22. Michael B. Epstein, Ph.D. Florida Atlantic University (2019), *The Covering Number of Some Finite Simple Groups.*

23. Oscar Lopez, Ph.D. Florida Atlantic University (2019), *An Algorithmic Approach to Tran Van Trung's Basic Recursive Construction of t-designs.*

Completed Masters theses:

1. Lucille Yu, M.Sc. (1973) "On Methods for Determining Subgroup Structures of Finite Groups."

2. Kok Tam, M.Sc. (1977) "On Low Rank Primitive Extensions of Simple Groups."

3. Behshad Rejaidehkordi, M.Sc. (1983) "A Hardware Implementation of Cryptosystem PGM."

4. Azza M. El-Tahan, M.Sc. (1985) "Invariant Factors of Finite Simple Groups."

5. Kwok-Kwong Tam M.Sc. (1988) "Algorithms in the Construction of Steiner Systems with Automorphisms of Prime Order."

6. Barbara L. Kess, M.Sc. (1988) "A Simulation of Parallel Processing."

7. Frank Stephen Smutniak, M.Sc. (1991) "Speech Processing Toolkit."

8. Rory Larson, M.Sc. (1992) "Genetic Algorithms and Finite Projective Planes."

9. Chadderdon Price, M.Sc. (1992) "Maximum Order Complexity and DNA Sequences."

10. Serafim Maroulis, M.Sc. (1996) "XPGM."

11. Charles A. Cusack, M.Sc. (1998) "Semiregular Large Sets."

12. Xiaolin Tang, M.Sc. (1999) "Factorizations in Small Finite Groups."

13. Catalin I. Tomai, M.Sc. (1999) "A study of treecodes in lossless Image Compression."

14. Huimin Diao, M.Sc. (1999) "Treecode applications in lossless Image Compression."

15. Hui Dang, M.Sc. (1999) "Performance of Factorization Procedures for Large Integers."

16. Alexandr Yekushev, M.Sc. (1999) "Techniques in Small Group Factorizations."

17. Hui Xu, M.Sc. (1999) "Recovery of Logarithmic Signatures from Black-box Permutations."
18. Sun Xun, M.Sc. (1999) "A Multidimentional Integer Knapsack Solver Utilizing the L-cube and SV algorithms."
19. Hanchang Fan, (2000) "Group Factorizations and Cryptography."
20. Guang Chen, M.Sc. (2000) "Implementation and Demonstration for Some Error-Correcting Codes."
21. Yifang Ye, M.Sc. (2000) "The Defect of Integer Knapsacks and Related Algorithms."
22. Suqin Wang, M.Sc (2000) "Tree Codes in Lossless Image Compression."
23. Daniel Socek, M.Sc. (2002) "Deterministic and Non-Deterministic Basis Reduction Techniques for NTRU Lattices."
24. Bernd, Losert, M.Sc. (2010), Florida Atlantic University, "*Quantum algorithms and the Hidden Subgroup Problem*".
25. Olga Yurevna Shukina, M.Sc. (2013), Florida Atlantic University, "*Implementation and Comparison of the Golay and First Order Reed-Muller Codes*".
26. Jesse Victor Adamski, M.Sc. (2013), Florida Atlantic University, "*Computing Automorphism Groups of Projective Planes*".

Completed M.Sc. Final Projects:

1. Hong Ye, M.Sc. (1998) "A free internet stocks retriever."
2. Krishnan Srarangarajan, M.Sc. (1998) "Experiments with Treecodes."
3. An Hoon Sang, M.Sc. (1998) "Factorization experiments in finite groups."
4. Hong Yuan, M.Sc. (1999) "Video encryption over the Internet."