William J. Martin
Department of Mathematical Sciences, Worcester Polytechnic Institute, Worcester MA 01609
W: (508) 831-6764 office: (508) 831-5316 cell: upon request e-mail: martin@wpi.edu

EDUCATION:
Ph.D., Combinatorics & Optimization; 1992, University of Waterloo, Waterloo, Canada

M.A., Mathematics (with distinction); 1986, State University of New York at Potsdam

B.A., Computer Science and Mathematics; 1986, State Univ. New York at Potsdam

PERSONAL:
Date of Birth: 4 July 1962;
U.S. Citizen; Canadian citizen; married; two children.

REGULAR POSITIONS HELD:
Professor, Mathematical Sciences and Computer Science, Worcester Polytechnic Institute (July 2009 to present) Externally funded research, teaching, service.

Associate Professor, Mathematical Sciences and Computer Science, Worcester Polytechnic Institute (August 2000 to June 2009) Externally funded research, teaching, service.

Associate Department Head, Mathematical Sciences, Worcester Polytechnic Institute (July 2004 to June 2006) Administrative duties, managing the teaching mission of the department.

Associate Professor, Mathematics & Statistics, University of Winnipeg (July 1998 to Sept. 2001) Externally funded research; teaching at all undergraduate levels; administrative duties.

Assistant Professor, Mathematics & Statistics, University of Winnipeg (Sept. 1993 to June 1998)

VISITING RESEARCH POSITIONS:
Long-Term Visitor, ICERM (Institute for Computational and Experimental Research in Mathematics), Brown University (January–May 2014)
Visiting Scholar, Mathematical Sciences, University of Delaware (September–December 2013)
Visiting Scholar, Mathematics, Massachusetts Institute of Technology (July 2006 to June 2007)
Visiting Associate Professor, Center for Applied Cryptographic Research, University of Waterloo (July 1999 to July 2000)
Visiting Assistant Professor, Mathematics & Statistics, University of Vermont (Sept. 1992 to Sept. 1993)
Visiting Lecturer, Postdoctoral Fellow, Combinatorics & Optimization, University of Waterloo (May to Aug., 1992).

Summer Research Associate, Government Network Planning Center, AT&T Bell Laboratories, Holmdel, NJ (Summers 1986, 1987, 1988) Programming; some research in graph theory and optimization.

RESEARCH INTERESTS:
Applications of algebra and combinatorics to problems in computer science and mathematics. Structure of association schemes, especially the study of designs and codes within association schemes. Combinatorial methods in cryptography. Also: graph theory; computational complexity; graph algorithms and networks; algebra; topological methods in combinatorics.

PUBLICATIONS: *(refereed, unless otherwise denoted)*

1. G. Çetin, Y. Doröz, B. Sunar and W.J. Martin, "Arithmetic using word-wise homomorphic encryption," to appear in: *ArcticCrypt 2016*, Longyearbyen, Svalbard, Norway, July 17-22, 2016.
2. J.H. Koolen, W. Lee, W.J. Martin and H. Tanaka, "Arithmetic completely regular codes," *Discrete Math. Theor. Comput. Sci.* **17** no. 3 (2016), 59–76.
3. X. Ye, T. Eisenbarth and W.J. Martin, "Bounded, yet sufficient? How to determine whether limited side channel information enables key recovery," in: *Smart Card Research and Advanced Applications* Vol. **8968** LNCS, pp. 215–232.
4. W.J. Martin and C.L. Steele, "On the ideal of the shortest vectors in the Leech lattice and other lattices," *J. Algebraic Combin.* **41** no. 3 (2015), 707–726.
5. J.A. Davis, W.J. Martin and J.B. Polhill, "Linking systems in nonelementary abelian groups," *J. Combin. Theory Ser. A* **123** no. 1 (2014), 92-103.
6. E. Van Dam, W.J. Martin and M. Muzychuk, "Uniformity in association schemes and coherent configurations: cometric Q-antipodal schemes and linked systems," *J. Combin. Theory, Ser. A* **120**, no. 7 (2013), 1401–1439.
7. Y. Hu, W.J. Martin and B. Sunar, "Enhanced Flexibility for Homomorphic Encryption Schemes via CRT," 10th International Conference on Applied Cryptography and Network Security (ACNS '12), June 2012, Singapore. [conference version]
8. J.H. Koolen, W. Lee and W.J. Martin, "Characterizing completely regular codes from an algebraic viewpoint," in: Combinatorics and Graphs, Contemporary Mathematics, Vol. 531 (R. A. Brualdi, et al., eds.), American Math. Soc., 2010.
9. W.J. Martin and B. Sunar, "Resilient functions: Just how resilient are the they?" pp. 17–34 in: Error-Correcting Codes, Finite Geometries and Cryptography, Contemporary Mathematics, Vol. 523 (A.A. Bruen and D.L. Wehlau, eds.), American Math. Soc., 2010.
10. N.L. LeCompte, W.J. Martin, and W. Owens, "On the equivalence between real mutually unbiased bases and a certain class of association schemes," *Europ. J. Combin.* **31** no. 6 (2010), 1499–1512.
11. W.J. Martin and H. Tanaka, "Commutative association schemes," *Europ. J. Combin.* **30** no. 6 (2009), 1497–1525.

12. W.J. Martin and J.S. Williford, "There are finitely many Q-polynomial association schemes with given first multiplicity at least three." *Europ. J. Combin.* **30** no. 3 (2009), 698–704.
13. C.D. Godsil, S.A. Hobart and W.J. Martin, "Representations of directed strongly regular graphs," *Europ. J. Combin.* vol. **28** no. 7 (2007), 1980–1993.
14. W.J. Martin, M. Muzychuk and J.S. Williford, "Imprimitive cometric association schemes: constructions and analysis," *J. Algebraic Combin.* vol. **25** no. 4 (2007), 399–415.
15. W.J. Martin and T.I. Visentin, "A dual Plotkin bound for (T, M, S)-nets," *IEEE Trans. Inform. Theory*, vol. **53** no. 1 (2007), 411–415.
16. W.J. Martin, D.R. Stinson and B. Sunar, "A provably secure true random number generator with built-in tolerance to active attacks." *IEEE Trans. Computers*, vol. **56** no. 1 (2007), 109–119.
17. W.J. Martin, M. Muzychuk and J.S. Williford, "Some new constructions of imprimitive cometric association schemes," To appear, proceedings of "Algebraic Combinatorics",an international conference in honour of Eiichi Bannai's 60th birthday, June 26-30, 2006, Sendai, Japan (not refereed).
18. W.J. Martin, "(t, m, s)-Nets" (6 pages), a section in the CRC Handbook of Combinatorial Designs (2nd ed.), C.J. Colbourn and J.H. Dinitz, eds., CRC Press (2006) (invited, not refereed).
19. W.J. Martin, "Completely regular codes: a viewpoint and some problems." *Proceedings of 2004 Com2MaC Workshop on Distance-Regular Graphs and Finite Geometry*, July 24 - 26, 2004, Pusan, Korea (invited, not refereed).
20. W.J. Martin and B.E. Sagan, "A new notion of transitivity for sets of permutations." *Journal of the London Mathematical Society*, vol. **73** (2006), 1–13.
21. A.E. Brouwer, C.D. Godsil, J.H. Koolen and W.J. Martin, "Width and dual width of subsets in polynomial association schemes." *J. Combin. Th. Ser. A*, vol. **102** (2003), 255–271.
22. W.J. Martin, "A physics-free introduction to quantum error-correcting codes." *Util. Math.* vol. **65** (2004), 133–158.
23. W.J. Martin, "Symmetric designs, sets with two intersection numbers and Krein parameters of incidence graphs." *J. Combin. Math. Combin. Comput.* vol. **38** (2001), 185-196.
24. W.J. Martin, "Design systems: combinatorial characterizations of Delsarte T-designs via partially ordered sets." pp. 223-239 in: Codes and Association Schemes, ed. A. Barg and S. Litsyn. AMS DIMACS Series in Discrete Mathematics and Theoretical Computer Science, vol. **56**, 2001.
25. W.J. Martin, "Minimum distance bounds for s-regular codes." *Des. Codes Cryptogr.* vol. **21** *(Special issue dedicated to Dr. Jaap Seidel on the occasion of his 80th birthday, Oisterwijk, 1999.)* (2000), 181-187.

26. W.J. Martin, "Linear programming bounds for ordered orthogonal arrays and (T, M, S)-nets." pp368-376, in: *Monte Carlo and quasi-Monte Carlo Methods 1998 (Claremont, CA)* (eds. H. Niederreiter and J. Spanier), Springer-Verlag, Berlin, 2000.
27. W.J. Martin and D.R. Stinson, "Association schemes for ordered orthogonal arrays and (T, M, S)-nets." *Canad. J. Math.* vol. **51** no. 2 (1999), 326-346.
28. W.J. Martin and D.R. Stinson, "A generalized Rao bound for ordered orthogonal arrays and (t, m, s)-nets." *Canad. Math. Bull.* vol. **42** no. 3 (1999), 359-370.
29. W.J. Martin, "Designs in product association schemes." *Des. Codes Cryptogr.* vol. **16** no. 3 (1999), 271-289.
30. W.J. Martin, "Completely regular designs." *J. Combin. Designs* vol. **6** no. 4 (1998), 261-273.
31. W.J. Martin, "Mixed block designs." *J. Combin. Designs* vol. **6** no. 2 (1998), 151-163.
32. J.H. Dinitz and W.J. Martin, "The stipulation polynomial of a uniquely list-colorable graph." *Australasian J. Combin.* vol. **11** (1995), 105-115.
33. W.J. Martin and X.J. Zhu, "Anticodes for the Grassman and bilinear forms graphs." *Designs, Codes and Crypt.* vol. **6** (1995), 73-79.
34. C.D. Godsil and W.J. Martin, "Quotients of association schemes." *J. Combin. Th. Ser. A,* vol. **69**, no. 2 (1995), 185-199.
35. W.J. Martin, "Completely regular designs of strength one." *J. Alg. Combin.* vol. **3** (1994), 177-185.

REPORTS: *(non-refereed)*

- W.J. Martin, Completely Regular Subsets, Ph.D. dissertation, Department of Combinatorics and Optimization, University of Waterloo, Canada
- W.J. Martin, "Completely regular codes in the Odd graphs."
- W.J. Martin and R.R. Zhu, "On the classification of distance-regular graphs by eigenvalue multiplicity." University of Waterloo Research Report CORR 92-06, 1992.
- W.J. Martin, "SurvNet: a survivable network design tool. User's guide and programmer's manual" AT&T Bell Laboratories internal memorandum (23 pages), 1987.

TEACHING EXPERIENCE:
Courses delivered (for example, 3000 level represents a course aimed at 3rd year undergraduates):

1000-2000 level
Calculus
Linear Algebra
Discrete Mathematics
Number Theory
Combinatorics
Applied Algebra
Proofs in Contemp Math
Math of Decision Making

3000-4000 level
Advanced Calculus
Modern Algebra
Intro. Topology
Linear Programming
Discrete Optimization
Game Theory
Mathematical Discovery and Invention

5000 level
Algebra
Graph Theory
Discrete Mathematics I
Hardness vs. Randomness
Association Schemes
Coding Theory

Individualized Reading Courses
Graph Algorithms
Error-Correcting Codes
Algebraic Geometry
Hyperelliptic Curve Cryptography
Quantum Algorithms
Lie Groups and Lie Algebras
Cohomology

GRANTS:

Awarded:

- National Science Foundation (PI): Workshop: *Systems of Lines: Applications of Algebraic Combinatorics* NSF DMS, Award # 1541272, $25,000 (Randy Paffenroth, co-PI).
- National Science Foundation (co-PI): TWC:Small: *Towards Practical Fully Homomorphic Encryption* (Oct. 2013 to Sep. 2016) $499,780. (B. Sunar, PI)
- National Security Agency (Steering Committee Member): *Conference Series: Discrete Mathematics Days in the Northeast* Sept. 2012 to April 2014. $14,940 (preliminary budget) (Rosa Orellana, PI)
- Slovenian Research Agency (ARRS) (US Team leader): *US-Slovenia bilateral cooperation grant.* 2012-2013. 3920 euros. (K. Kutnar, PI)
- National Security Agency (PI): *Some problems in association schemes* (Jan. 2012 to Jan. 2014). $78,377.
- National Science Foundation (co-PI): TC:Small: *Homomorphic Encryption for Cloud Privacy* (Aug. 2011 to Jul. 2013). $312,888. (B. Sunar, PI)

- National Security Agency (PI): *Problems in cometric association schemes* (Jan. 2010 to Jan. 2012). $67,959.
- National Science Foundation (co-PI): CT-ER: *Exploring Physical Functions for Lightweight and Robust Cryptography* (Sept. 2008 to Aug. 2010). $149,797 (B. Sunar, PI)
- National Security Agency (PI): *Problems in association schemes* (Jan. 2007 to Jan. 2009). $59,000.
- CIMPA (International Centre for Pure and Applied Mathematics, Nice, France): Summer School on SemiDefinite Programming Techniques in Coding Theory, Manila, Philippines
- Worcester Polytechnic Institute Educational Development Council internal grant: "The Calculus Dialogues" $5640 (with P. Christopher)
- Slovenian Research Agency (ARRS) (participant): *Open problems in association schemes* 2006–2008. $19,000.(A. Jurišić, PI)
- National Security Agency (PI): Conference Grant *Discrete Mathematics Day at WPI*, 2005. $1,500.
- NSF (co-PI): Equipment Grant *Mathematical Sciences Computational Research Environment (SCREMS)*, 2005. $125,328. (M. Humi, PI)
- National Security Agency (PI): Conference Grant *Discrete Mathematics Day at WPI*, 2003. $3,000.
- National Science Foundation (co-PI): ITR:SI *Implementing Public-Key Cryptosystems for Secure Information Infrastructure* $436,000 (Sept. 2001 to Sept. 2004). (B. Sunar, PI)
- MITACS, a Canadian Network of Centres of Excellence, (Team member, on a team of twelve researchers): *Project in Elliptic Curve Cryptography and Algebraic Combinatorics.* Cdn $291,000 per year (S. Vanstone, PI)
- National Science and Engineering Research Council (PI): Individual Grant. Cdn $48,500 (April 1997 to March 2001)
- National Science and Engineering Research Council (PI): Individual Grant Cdn $24,000 (April 1994 to March 1997)
- National Science and Engineering Research Council (PI): Equipment Grant. Cdn $16,000 (April 1996)
- National Science and Engineering Research Council (co-PI): Equipment Grant. Cdn $30,000 (April 1994)
- University of Winnipeg Start-up grant (PI). Cdn $9,176 (1993-4)

RECENT SERVICE ACTIVITIES:

- Discrete Mathematics Advisory Panel, National Security Agency, 2011-2013.
- NSF panel member, Washington
- referee for over ten journals in the past four years
- Book proposal reviewer, Cambridge University Press.
- Grant proposal reviewer, National Security Agency
- Workshop proposal reviewer, European Science Foundation
- Grant proposal reviewer, Austrian Science Fund.
- Special session organizer, "Computer Algebra and Combinatorics" ASCM '05, Seoul Korea, December 2005.
- Organizing committee chair, Discrete Mathematics Day at WPI (May 2003, September 2005, May 2010)
- Associate Department Head, Mathematical Sciences, Worcester Polytechnic Institute, July 2004 to June 2006.
- Arts and Science Summer Undergraduate Research Fellow Selection Committee, 2016
- Committee on Appointments and Promotions, Worcester Polytechnic Institute, 2014-2017
- Search Committee, Chemical Engineering Department Head, Worcester Polytechnic Institute, 2014-2015
- Undergraduate Committee, Mathematical Sciences, Worcester Polytechnic Institute, 2011-2012 academic year.
- Graduate Committee, Mathematical Sciences, Worcester Polytechnic Institute, 2010-2011 academic year.
- Personnel Committee, Mathematical Sciences, Worcester Polytechnic Institute, 2010-2011 academic year.
- Tenure Committee, Mathematical Sciences, Worcester Polytechnic Institute, 2008-2010 academic years.
- Teaching Evaluation Committee, Mathematical Sciences, Worcester Polytechnic Institute, 2009-2010 academic year.
- Chair, Graduate Committee, Mathematical Sciences, Worcester Polytechnic Institute, 2007-2008 academic year.

RESEARCH STUDENT SUPERVISION:

Postdoctoral Fellow:

- Sho Suda (Ph.D. Tohoku University, Japan), 2010.
- Hajime Tanaka (Ph.D. Kyushu University, Japan), 2007

PhD:

- Brian Kodalen (in progress)

MSc:

- Corre Steele (project, Industrial Math, 2016)
- Chao Li (project, Computer Science, 2015)
- Aaron Nahabedian (project, Industrial Math, 2010)
- Jonathan Adler (thesis, Applied Mathematics, 2008) *"Graph Decompositions and Monadic Second Order Logic"*
- Ronald Lesniak (project, Industrial Math, 2006)
- Serdar Pehlivanoglu (thesis, CS, 2005) *"Rijndael Circuit-Level Cryptanalysis"*

Undergraduate (Summer):

Tara Taylor, Cindy Lau, Nick LeCompte, Will Owens, Justin Kahn, Eric Reich, Corre Steele.

LECTURES:

Recent and Notable Invited Lectures: (contributed and older lectures omitted)

- Plenary speaker, "Q-Polynomial association schemes and the nearest neighbor graph", International Workshop on Algebraic Aombinatorics, Anhui University, Hefei China, October 28-31, 2016.
- Discrete Mathematics Seminar, "A Tale of Two Design Theories", University of Delaware, March 7, 2016 (The same talk was given, on invitation, in the Brandeis University Combinatorics Seminar, February 23, 2016.)
- Opening plenary speaker, "Some problems arising in quantum information theory", CanaDAM, Canadian Conference on Discrete and Algorithmic Mathematics, University of Saskatchewan, Saskatoon SK Canada, June 1-4, 2015.
- Expository talk entitled "Quantum information theory", BIRS workshop Mathematics of Communications: Sequences, Codes and Designs (15w5139), Banff AB Canada, January 25-30, 2015.

- Invited speaker (40 min): "Nice Euclidean configurations from incidence matrices and characters of designs", Workshop on Algebraic Design Theory and Hadamard Matrices, Lethbridge, Alberta, July 10, 2014
- Tutte seminar (50 min, invited): "Some problems concerning finite point sets on the unit sphere" Department of Combinatorics & Optimization, University of Waterloo, June 20, 2014.
- Invited session speaker (30 mins): "Graph homotopy, ideals of finite varieties and a surprising duality". Modern Trends in Algebraic Graph Theory, Villanova University, June 3, 2014
- Rocky Mountain Algebraic Combinatorics Seminar "Almost orthogonal vectors in Euclidean space"., Colorado State University, April 25, 2014.
- Colloquium: "Promise, progress, and problems in homomorphic encryption", Department of Electrical and Computer Engineering, University of Maryland, College Park, April 8, 2014
- Invited (30 min): "Ideals of polytopes and graph homotopy", BruceFest 2014, Gainesville, FL, March 25, 2014.
- Colloquium: "Almost orthogonal vectors in Euclidean space". Department of Econometrics and Operations Research, Tilburg University, March 4, 2014.
- Invited (50 min): "Girth and dual girth parameters in polynomial association schemes". Colloquium on Galois Geometry to the memory of Frederic Vanhove, One day colloquium on Galois Geometry in Ghent, Belgium, February 28, 2014.
- 37th Australasian Conference on Combinatorial Mathematics and Combinatorial Computing, University of Western Australia, December 9-13, 2013.
- International Workshop on Algebraic Combinatorics, Hebei Normal University, Shijiazhuang, Hebei, China, November 17-21, 2013.
- Rocky Mountain Mathematics Consortium Summer School 2013 (ten lectures), University of Wyoming, June 17-28, 2013.
- Workshop on Algebraic Combinatorics, Shanghai Jiao Tong University, Shanghai, September 15, 2011.
- Graphs, Designs and Algebraic Combinatorics 2011, University of Regina, Regina, SK, July 20, 2011.
- IPM20, Tehran, Iran, May 19, 2009
- Geometric and Algebraic Combinatorics 4, Oisterwijk, the Netherlands, August, 2008
- 2004 Com2MaC Conference on Association Schemes, Codes and Designs, Pusan National University, Busan, Korea (July 19 - 23, 2004).