Douglas Robert Stinson

Last updated: December 7, 2023

University of Waterloo
David R. Cheriton School of Computer Science
Waterloo Ontario, N2L 3G1, Canada

Email: dstinson@uwaterloo.ca
Homepage: https://cs.uwaterloo.ca/~dstinson/
Orcid: https://orcid.org/0000-0001-5635-8122

Personal

Date of birth: June 2, 1956

Place of birth: Guelph, Ontario, Canada

Canadian Citizen

Married, two children

Education

BMath (Hon.), Combinatorics and Optimization and Pure Mathematics, University of Waterloo, 1978.

MSc, Mathematics, Ohio State University, 1980.

PhD, Combinatorics and Optimization, University of Waterloo, 1981. Thesis title: *Some classes of frames, and the spectra of skew Room squares and Howell designs*. PhD Advisor: R. Mullin.

Academic Appointments

NSERC post-doctoral fellow, University of Manitoba, Department of Computer Science, 1981–1982.

Assistant professor (NSERC university research fellow), University of Manitoba, Department of Computer Science, 1982–1983.

Associate professor (NSERC university research fellow), University of Manitoba, Department of Computer Science, 1983–1986.

Full professor (NSERC university research fellow), University of Manitoba, Department of Computer Science, 1986–1991 (on leave, 1990–1991).

Full professor, University of Nebraska, Computer Science and Engineering Department, 1990–1998.

Full professor, University of Waterloo, Department of Combinatorics and Optimization, 1998–2002.

Full professor, University of Waterloo, David R. Cheriton School of Computer Science, 2002–2019.

Professor emeritus, University of Waterloo, David R. Cheriton School of Computer Science, 2019–.

Adjunct professor, University of Waterloo, David R. Cheriton School of Computer Science, 2019–2025.

Adjunct research professor, School of Mathematics and Statistics, Carleton University, 2022–2027.

Awards and Recognition

Honourable mention, Putnam Mathematics Competition, 1977.

University of Waterloo Alumni Gold Medal in Mathematics, 1978.

University of Waterloo Alumni PhD Gold Medal, 1981.

NSERC University Research Fellow, University of Manitoba, 1982–1989.

Rh Institute Award for Outstanding Contribution to Scholarship and Research in the Natural Sciences, University of Manitoba, 1985.

Foundation Fellow of the Institute of Combinatorics and its Applications, 1990.

1994 Hall Medal, awarded by the Institute of Combinatorics and Its Applications. Hall Medals recognize extensive quality research with substantial international impact by Fellows of the ICA in mid-career.

Visiting Professional Associate Award, University of Manitoba, 1996.

NSERC/Certicom Industrial Research Chair in Cryptography, University of Waterloo, 1998–2003.

Mathematics Faculty Fellowship, University of Waterloo, 2001–2004.

University Research Chair, University of Waterloo, 2005–2011. The University of Waterloo recognizes exceptional achievement and pre-eminence in a particular field of knowledge through the designation "University Research Chair", a title which may be held for up to seven years.

Outstanding performance award (for outstanding contribution in teaching and scholarship), University of Waterloo, 2005, 2008, 2013.

Elected and inducted as a *Fellow of the Royal Society of Canada*, 2011. Fellows are elected by their peers in recognition of outstanding scholarly, scientific and artistic achievement. Election to the academies of the Royal Society of Canada is the highest honour a scholar can achieve in the Arts, Humanities and Sciences.

Appointed as *University Professor*, University of Waterloo, 2013. The University of Waterloo recognizes exceptional scholarly achievement and international pre-eminence through the designation "University Professor".

The conference *Stinson66 – New Advances in Designs, Codes and Cryptography* was held at the Fields Institute, Toronto, from June 13–17, 2022. The purpose of the conference was to celebrate my 66th birthday and highlight my contributions to the fields of designs, codes, cryptography, and their connections.

2022 Stanton Medal, awarded by the Institute of Combinatorics and Its Applications. Stanton Medals honour significant lifetime contributions to promoting the discipline of combinatorics through advocacy, outreach, service, teaching and/or mentoring.

Supervision

Postdoctoral Fellows

1. Guang Gong, 1998, University of Waterloo.
2. Ruizhong Wei, 1998–2000, University of Waterloo.
3. Yongge Wang, 1999–2000, University of Waterloo.

4. Palash Sarkar, 2000–2001, University of Waterloo.
5. Mark Chateauneuf, 2000–2001, University of Waterloo.
6. Paolo D'Arco, 2001–2002, University of Waterloo.
7. Dameng Deng, 2003–2004, University of Waterloo.
8. Mridul Nandi, 2006–2007, University of Waterloo.
9. Maura Paterson, 2008, visiting Post-Doc from Royal Holloway.
10. Noman Mohammed, 2012, University of Waterloo.
11. Souradyuti Paul, 2013, University of Waterloo.
12. Navid Nasr Esfahani, 2021–2022, University of Waterloo.

PhD Students

1. Eric Seah, PhD, 1987 (CS, University of Manitoba). Thesis title: *On the enumeration of one-factorizations and Howell designs using orderly algorithms*.
2. Demeng Chen, PhD, 1994 (CS, University of Manitoba, co-supervised with R. Stanton). Thesis title: *Large sets of disjoint packings and large sets of disjoint GDDs*.
3. K. Gopalakrishnan, PhD, 1994 (CSE, University of Nebraska). Thesis title: *A study of correlation-immune, resilient and related cryptographic functions*.
4. Mustafa Atici, PhD, 1996, (CSE, University of Nebraska). Thesis title: *Hash functions: recursive constructions and applications to cryptography*.
5. Ruizhong Wei, PhD, 1998, (Math, University of Nebraska). Thesis title: *Traceability schemes, frameproof codes, key distribution patterns and related topics – a combinatorial approach*.
6. Khoongming Khoo, PhD, 2004 (C&O, University of Waterloo, co-supervised with G. Gong). Thesis title: *Sequence design and construction of cryptographic boolean functions*.
7. James Muir, PhD, 2005 (C&O, University of Waterloo). Thesis title: *Efficient integer representations for cryptographic operations*.
8. Jooyoung Lee, PhD, 2005 (C&O, University of Waterloo). Thesis title: *Combinatorial approaches to key predistribution for distributed sensor networks*.
9. Jason Hinek, PhD, 2007 (SCS, University of Waterloo, co-supervised with M. Giesbrecht). Thesis title: *On the security of some variants of RSA*.
10. Atefeh Mashatan, PhD, 2009 (C&O, University of Waterloo). Thesis title: *Message authentication and recognition protocols using two-channel cryptography*.
11. Jiang Wu, PhD, 2009 (SCS, University of Waterloo). Thesis title: *Cryptographic protocols, sensor network key management, and RFID authentication*.
12. Greg Zaverucha, PhD, 2011 (SCS, University of Waterloo). Thesis title: *Hash families and cover-free families with cryptographic applications*.
13. Mehrdad Nojoumian, PhD, 2012 (SCS, University of Waterloo). Thesis title: *Novel secret sharing and commitment schemes for cryptographic applications*.

14. Colleen Swanson, PhD, 2013 (SCS, University of Waterloo). Thesis title: *Unconditionally secure cryptography: signature schemes, user-private information retrieval, and the generalized Russian cards problem.*
15. Kevin Henry, PhD, 2015 (SCS, University of Waterloo). Thesis title: *Secure protocols for key predistribution, network discovery, and aggregation in wireless sensor networks.*
16. Jalaj Upadhyay, PhD, 2015 (SCS, University of Waterloo). Thesis title: *Integrity and privacy of large data*.
17. Navid Nasr Esfahani, SCS, PhD 2021 (SCS, University of Waterloo). Thesis title: *Generalizations of all-or-nothing transforms and their application in secure distributed storage*.

Masters Students

1. Wendy White, MSc, 1990 (CS, University of Manitoba). Thesis title: *The construction and implementation of authentication and secrecy codes*.
2. Mustafa Atici, MSc, 1994 (CSE, University of Nebraska). Thesis title: *Optimal information and average information rates of the connected graphs on six vertices*.
3. Sharon Lim, MSc, 1996 (CSE, University of Nebraska). Thesis title: *A "C" implementation of two classes of authentication codes*.
4. Phil Eisen, MMath, 1999 (C&O, University of Waterloo). Thesis title: *Threshold visual cryptography schemes*.
5. Jason Chen, MMath, 2000 (C&O, University of Waterloo). Thesis title: *A survey on traitor tracing schemes*.
6. James Muir, MMath, 2001 (C&O, University of Waterloo). Thesis title: *Techniques of side channel cryptanalysis*.
7. Kyung-Mi Kim, MMath, 2003 (C&O, University of Waterloo). Thesis title: *Perfect hash families: constructions and applications*.
8. Hao-Hsien Wang, MMath, 2005 (SCS, University of Waterloo). Thesis title: *Desired features and design methodologies of secure authenticated key exchange protocols in the public-key infrastructure setting*.
9. Kar-Yee Au, MMath, 2005 (SCS, University of Waterloo). Thesis title: *Unconditionally secure authentication codes and digital signatures*.
10. Sheng Zhang, MMath, 2005 (SCS, University of Waterloo). Thesis title: *Algorithms for detecting cheaters in threshold schemes*.
11. Jiayuan Sui, MMath, 2008 (SCS, University of Waterloo). Thesis title: *A security analysis of some physical content distribution systems*.
12. Kevin Henry, MMath, 2008 (SCS, University of Waterloo). Thesis title: *The theory and applications of homomorphic cryptography*.
13. Jalaj Upadhyay, MMath, 2011 (SCS, University of Waterloo). Thesis title: *Generic attacks on hash functions*.
14. Chuan Guo, SCS, MMath, 2015 (SCS, University of Waterloo). Thesis title: *Fingerprinting codes and related combinatorial structures*.

15. Bailey Kacsmar, SCS, MMath, 2018 (SCS, University of Waterloo). Thesis title: *Designing efficient algorithms for combinatorial repairable threshold schemes*.

16. Shannon Veitch, SCS, MMath, 2022 (SCS, University of Waterloo). Thesis title: *Contextualizing alternative models of secret sharing*.

Undergraduate Research Assistants

1. Shannon Veitch, 2018, 2019.

Teaching (University of Waterloo)

Combinatorics and Optimization

Combinatorial Cryptography (C&O 739W): Fall 1998.

Combinatorial Designs (C&O 434/634): Fall 1999, Winter 2002.

Mathematics of Public-Key Cryptography (C&O 485/685): Fall 2000, Fall 2001.

Computer Science

Topics in Cryptography, Security and Privacy: Unconditionally Secure Cryptography (CS 858): Spring 2008, Winter 2010, Spring 2019.

Cryptography / Network Security (CS 758): Fall 2002, Fall 2003, Fall 2005, Winter 2007, Fall 2010, Spring 2012, Fall 2013, Winter 2015, Spring 2016.

Computer Security and Privacy (CS 458/658): Fall 2010, Winter 2010, Spring 2012, Fall 2012, Fall 2013, Fall 2014 (two sections), Spring 2016.

Algorithms (CS 341): Fall 2003, Winter 2004, Winter 2006 (two sections), Spring 2013 (two sections), Winter 2015, Fall 2015 (two sections), Winter 2017 (two sections), Winter 2019 (two sections).

Data Structures and Data Management (CS 240): Fall 2004, Fall 2008, Fall 2011.

PhD Thesis External Examiner

R. Rees, Queen's University, 1986. Thesis title: *On certain* $(1,2)$*-factorizations of the complete graph*.

S. Furino, University of Waterloo, 1989. Thesis title: *α-resolvable structures*.

M. Yu, Simon Fraser University, 1990. Thesis title: *Tree decompositions of complete graphs*.

I. Bluskov, Simon Fraser University, 1997. Thesis title: *New designs and coverings*.

I. Adamczak, Michigan Technological University, 2003. Thesis title: *Tight incomplete block designs*.

L. Keliher, Queen's University, 2003. Thesis title: *Linear cryptanalysis of substitution-permutation networks*.

K. C. Gupta, Indian Statistical Institute, 2004. Thesis title: *Cryptographic and combinatorial properties of boolean functions and S-boxes*.

E.-Y. C. Park, University of Toronto, 2007. Thesis title: *Combinatorial techniques for key distribution and information storage*.

L. Howard, University of Victoria, 2009. Thesis title: *Nets of order $4m+2$: linear dependence and dimensions of codes*.

P. Wang, University of Calgary, 2015. Thesis title: *Secure communication over adversarial channel*.

H. T. Poon, Ryerson University, 2018. Thesis title: *Theory and application of encrypted sequential data processing: search and computation.*

Thaís Bardini Idalino, University of Ottawa, 2019. Thesis title: *Fault tolerance in cryptographic applications using cover-free families*.

Editorial Work

Member of editorial board of *Journal of Combinatorial Mathematics and Combinatorial Computing*, 1987–2019.

Member of editorial board of *Designs, Codes and Cryptography*, 1990–1998.

Editor-in-chief, *Journal of Combinatorial Designs*, 1993–2002.

Member of editorial board of *Journal of Cryptology*, 1993–1997.

Advisory editor for *CRC Handbook of Combinatorial Designs*, C. J. Colbourn and J. H. Dinitz (eds.), CRC Press, 1996.

Member of editorial board of *Aequationes Mathematicae*, 1996–2001.

Associate editor for complexity and cryptography, *IEEE Transactions on Information Theory*, 1997–1999.

Guest editor, (with Charlie Colbourn and John van Rees), special volume of *Designs, Codes and Cryptography* in honour of Ron Mullin, 2002.

Member of editorial board of *Advances in Mathematics of Communications*, 2006–2012.

Associate editor of *Discrete Mathematics*, 2007–2012; member of editorial board, 2013–.

Member of editorial board of *Journal of Combinatorial Designs*, 2003–2023; honorary editor, 2023–.

Series editor, *Chapman & Hall/CRC Cryptography and Network Security Series*, 2004–.

Member of editorial board of *Contributions to Discrete Mathematics*, 2005–2019.

Member of editorial board of *IET Information Security*, 2005–2013.

Member of editorial board of *Journal of Mathematical Cryptology*, 2006–2019.

Guest editor, (with Ian Blake and Alfred Menezes), special volume of *Designs, Codes and Cryptography* in memory of Scott Vanstone, 2015.

External Service (Selected)

Member of NSERC (Canada) Mathematics Grant Selection Committee, 1993–1996.

Member of NSERC (Canada) scientific evaluation committee for the *Pacific Institute for the Mathematical Sciences*, 1996.

Member of the *Canadian Mathematics Society Research Committee*, 2000–2003 (chair, 2001–2002).

Member of the Corporation of the *Fields Institute*, 2004–2006.

Member of the Scientific Advisory Board of the *Banff International Research Station*, 2005–2008.

President of the *Institute of Combinatorics and its Applications*, 2016–2022.

Invited Talks (Selected)

Tenth Australian Conference on Combinatorial Mathematics, Adelaide, Australia, Australia, August 1982, invited one-hour talk.

Canadian Mathematics Society Summer Meeting, Vancouver, June 1983.

NSERC Summer Workshop on Latin Squares and their Application, Vancouver, July–August 1983.

AMS Meeting, Special session on finite geometries and combinatorial designs, Lincoln, Nebraska, November 1987.

First Auburn Combinatorics Conference, Auburn, Alabama, March 1988, two invited one-hour talks.

Institute For Mathematics and its Applications Workshop on Design Theory and Applications, Minneapolis, June 1988.

Fifteenth Australasian Conference on Combinatorial Mathematics and Combinatorial Computing, Brisbane, Australia, July 1989, invited one-hour talk.

Fourth Carbondale Combinatorics Conference, Carbondale, Illinois, November 1989, invited one-hour talk.

23rd Southeastern International Conference on Combinatorics, Graph Theory and Computing, Boca Raton, Florida, February 1992, two invited one-hour talks (designated I.C.A. lecturer).

Waterloo 92, Waterloo, Ontario, June 1992, invited one-hour talk (plenary speaker).

Sixth Cumberland Conference on Graph Theory and Computing, Memphis, May 1993, invited 50-minute talk (featured speaker).

Fourteenth British Combinatorial Conference, University of Keele, UK, July 1993, invited one-hour talk.

Sixth Vermont Summer Workshop on Combinatorics, Burlington, Vermont, June 1994, invited one-hour talk.

Second Workshop on Selected Areas in Cryptography, Ottawa, May 1995, invited 45-minute talk.

R. C. Bose Memorial Conference, Fort Collins, Colorado, June 1995.

25th Manitoba Conference on Combinatorial Mathematics and Computing, Winnipeg, September 1995, invited one-hour talk.

Security in Communication Networks, Amalfi, Italy, September 1996, invited 50-minute talk.

Public Key Solutions 1997, Toronto, April 1997, invited 45-minute talk.

Canadian Mathematics Society 1997 Summer Meeting, Symposium on Finite Geometries and Applications, Winnipeg, June 1997, invited 50-minute talk.

Public Key Solutions 1998, Toronto, April 1998, invited 30-minute talk.

Ninth SIAM Conference on Discrete Mathematics, Toronto, July 1998, invited one-hour talk.

Winnipeg Combinatorial Mathematics Conference, Winnipeg, September 1998, two invited one-hour talks.

Workshop on Combinatorics and Communications Applications, Royal Holloway, UK, April 1999, invited one-hour talk.

Tenth Postgraduate Combinatorial Conference, Royal Holloway, UK, April 1999, invited one-hour talk.

Twelfth Cumberland Conference on Combinatorics, Graph Theory and Computing, Louisville, Kentucky, May 1999, invited 50-minute talk (principal speaker).

Canadian Mathematics Society 1999 Summer Meeting, St. John's, Newfoundland, May 1999, invited one-hour talk (plenary speaker).

Canadian Mathematics Society 2000 Summer Meeting, Hamilton, June 2000, Session on *Cryptography and Number Theory*.

Tenth SIAM Conference on Discrete Mathematics, Minneapolis, June 2000, Minisymposium on *Applications of Combinatorial Designs to Computing and Communications*.

Fourteenth Midwestern Conference on Combinatorics, Cryptography and Computing, Wichita, Kansas, October 2000, invited one-hour talk.

Second Lethbridge Workshop on Designs, Codes, Cryptography and Graph Theory, Lethbridge, Alberta, July 2001, three invited one-hour talks (main speaker).

Thirty-third Southeastern International Conference on Combinatorics, Graph Theory, and Computing, Boca Raton, Florida, March 2002, two invited one-hour talks.

Atlantic Association for Research in the Mathematical Sciences (AARMS) Summer School, St. John's, Newfoundland, August 2002, invited one-hour public lecture.

AARMS Workshop on Combinatorial Designs and Related Topics, St. John's, Newfoundland, July 2003, invited one-hour talk (main speaker).

Cryptography Short Course, Canadian Mathematics Society Winter Meeting, Vancouver, December 2003, invited one-hour talk.

IEEE Wireless Communications and Networking Conference, New Orleans, April 2005, invited talk (special session on wireless security).

Nineteenth Midwestern Conference on Combinatorics, Cryptography and Computing, Rochester, NY, October 2005, invited one-hour talk.

Fields Institute Workshop on Covering Arrays: Constructions, Applications and Generalizations, Ottawa, May 2006, invited 90-minute tutorial.

SIAM Conference on Discrete Mathematics, Victoria, June 2006, Minisymposium on *Design Theory*.

Workshop on Cryptography: Underlying Mathematics, Provability and Foundations, Toronto, November, 2006, invited 50-minute talk.

1st Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM 2007), Banff, May 2007, Minisymposium on *Combinatorial Designs*.

CMS-MITACS Joint Conference (Canadian Mathematics Society Summer Meeting), Winnipeg, June 2007, Session on *Finite Combinatorics*.

Information Systems Security Colloquium (ISS 2008), Concordia University, Montréal, May 2008, invited one-hour talk.

SIAM Conference on Discrete Mathematics, Burlington, June 2008, Minisymposium on *Cryptography*.

Fields Institute Workshop on New Directions in Cryptography, Ottawa, June 2008, invited one-hour talk.

Information Security in a Quantum World, Institute for Quantum Computing, Waterloo, August 2008, two invited 50-minute lectures.

Centre for Information Security and Cryptography, University of Calgary, Distinguished Lecture Series, October, 2008, invited one-hour talk.

22nd Midwestern Conference on Combinatorics, Cryptography and Computing, Las Vegas, October 2008, invited one-hour talk (keynote speaker).

Cryptology, Designs and Finite Groups 2009, Deerfield Beach, Florida, May 2009, invited one-hour talk (plenary speaker).

2nd Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM 2009), Montréal, May 2009, Minisymposium on *Combinatorial Design Theory*.

Combinatorial Configurations and their Applications (CCA 2009), Houghton, Michigan, August 2009, two invited one-hour talks.

Fourth Pythagorean Conference (An Advanced Research Workshop in Geometry, Combinatorial Designs & Cryptology), Corfu, Greece, May 2010, invited one-hour talk (plenary speaker).

Canadian Mathematics Society Winter Meeting, Vancouver, December 2010, Session on *Theory and Application of Sequences and Arrays*.

Linear Algebraic Techniques in Combinatorics/Graph Theory, Banff International Research Station for Mathematical Innovation and Discovery, February, 2011, invited 45-minute talk.

3rd Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM 2011), Victoria, June 2011, Minisymposium on *Designs and Codes*.

Ninth Annual Conference on Privacy, Security and Trust (PST 2011), Concordia University, Montréal, July 2011, invited one-hour talk (keynote speaker).

QKD Summer School 2011, Institute for Quantum Computing, Waterloo, July 2011, three hours of lectures on *Information-theoretic Cryptography*.

New Fellows Presentations, Royal Society of Canada Annual Conference, Ottawa, November 2011, invited 20-minute talk.

Forty-third Southeastern International Conference on Combinatorics, Graph Theory, and Computing, Boca Raton, Florida, March 2012, two invited one-hour talks.

WilsonFest, Pasadena, California, March 2012, invited 50-minute talk (featured speaker).

SIAM Conference on Discrete Mathematics, Halifax, June 2012, Minisymposium on *Design Theory*.

5th International Symposium on Foundations & Practice of Security (FPS 2012), Montréal, October 2012, one-hour keynote talk.

4th Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM 2013), St. John's, June 2013, Minisymposium speaker: *Eric Mendelsohn: Colleagues and Descendants*.

QKD Summer School 2013, Institute for Quantum Computing, Waterloo, July 2013, three hours of lectures on *Information-theoretic Cryptography*.

Selected Areas in Cryptography (SAC 2013), Burnaby BC, August 2013, 20th anniversary distinguished speaker, 90-minute talk.

Distinguished Lecture, University of North Carolina at Charlotte, College of Computing and Informatics, April 2014.

Workshop on Algebraic Design Theory and Hadamard Matrices (ADTHM 2014), Lethbridge, Alberta, July 2014, invited 50-minute talk (plenary speaker).

QKD Summer School 2015, Institute for Quantum Computing, Waterloo, July 2015, three hours of lectures on *Information-theoretic Cryptography*.

29th Midwestern Conference on Combinatorics and Combinatorial Computing, Charleston, October 2015, invited one-hour talk (keynote speaker).

Forty-eighth Southeastern International Conference on Combinatorics, Graph Theory, and Computing, Boca Raton, Florida, March 2017, invited one-hour talk (plenary speaker).

6th Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM 2017), Toronto, June 2017, invited speaker in the minisymposium *In Honour of the Work of Alex Rosa*.

Alex Rosa 80, Mikulov, Czech Republic, June 2017, invited participant and speaker.

QKD Summer School 2017, Institute for Quantum Computing, Waterloo, July 2015, six hours of lectures on *Fundamentals of Cryptography* and *Information-theoretic Cryptography*.

Canadian Mathematics Society Winter Meeting, Waterloo, December 2017, Session on *Design Theory*.

Combinatorics 2018, Arco, Italy, June 2018, plenary speaker, invited 50-minute talk.

Conference on Combinatorics and its Applications In Celebration of Charlie Colbourn's 65th Birthday, Singapore, July 2018, keynote speaker, invited 50-minute talk.

7th Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM 2019), Vancouver, May 2019, invited speaker in the minisymposium on *Design Theory*.

ArasuFest, Kalamata, Greece, August 2019, invited 45-minute talk.

Selected Areas in Cryptography (SAC 2019), Waterloo, August 2019, invited speaker, 50-minute talk.

QKD Summer School 2019, Institute for Quantum Computing, Waterloo, August 2019, three hours of lectures on *Information-theoretic Cryptography*.

8th Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM 2021) (online), May 2021, invited speaker in the minisymposium on *Practical Applications of Design Theory*.

CMS 75th+1 Anniversary Summer Meeting (online), June 2021, invited speaker in the session on *Graph Decompositions*.

28th British Combinatorial Conference (online), July 2021, invited speaker in the minisymposium on *Codes and Cryptography*.

CMS Winter Meeting (online), December 2021, invited speaker in the session on *Mathematics of Digital Communication*.

Ontario Combinatorics Workshop, University of Ottawa, May 2023, plenary speaker.

9th Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM 2023), Winnipeg, June 2023, invited speaker in the minisymposium on *Design Theory and Coding Theory*.

Selected Areas in Cryptography (SAC 2023), Fredericton, August 2023, I delivered the Stafford Tavares lecture, an invited 50-minute talk.

CRM / UOttawa Distinguished Colloquium, Ottawa, November 2023.

Research Grants

NSERC operating grant (Pure and Applied Mathematics), 1982–1985, $15,865.

NSERC operating grant (Computing and Information Sciences), 1985–1987, $35,200.

NSERC operating grant (Computing and Information Sciences), 1987–1990, $95,700.

NSERC operating grant (Computing and Information Sciences), 1990–1992, $63,800, *Cryptographic Protocols, Combinatorial Designs, and Fast Computation in Finite Fields*.

NSF (Computer and Computation Research, Theory of Computing), 1992–1994, $76,574 (plus $5,000 matching funds from the Center for Communication and Information Science, University of Nebraska), *Combinatorial Cryptography*.

NSA (Mathematical Sciences Program), 1993–1995, $84,000 (plus $21,000 matching funds from the Center for Communication and Information Science, University of Nebraska), *Combinatorial Designs*, joint grant with E. Kramer and S. Magliveras.

NSF (Computer and Computation Research, Theory of Computing), 1994–1997, $95,868 (plus $23,732 matching funds from the Center for Communication and Information Science, University of Nebraska), *Combinatorial Cryptography*.

NSA (Mathematical Sciences Program), 1996–1997, $40,000 (plus $11,300 matching funds from the Center for Communication and Information Science, University of Nebraska), *Designs and Other Combinatorial Problems*, joint grant with E. Kramer and S. Magliveras.

University of Nebraska Foundation, 1997, $96,972, *Electronic Commerce Systems Laboratory*, joint grant with 13 others.

NSF (Computer and Computation Research, Theory of Computing), 1997–1998, $95,316 (plus $6,354 matching funds from the Center for Communication and Information Science, University of Nebraska), *Topics in Unconditionally Secure Cryptography*.

NSERC research grant (Computing and Information Sciences), 1998–2002, $164,340, *Applications of Combinatorial Designs to Computer Science*.

NSERC/Certicom research grant (industrial research chair), 1998–2003, $357,500, *Unconditionally Secure Cryptography*.

CITO, 1998–2000, $220,000, *Information Security Technology and Applied Cryptography*, joint grant with G. Agnew, A. Hasan, A. Menezes and S. Vanstone.

MITACS, 1999–2000, $206,000, *Applied Cryptography*, co-principal investigator (with S. Vanstone).

ORDCF, 1999–2004, $827,500, *Centre for Applied Cryptographic Research*, co-principal investigator (with S. Vanstone).

MITACS, 2000–2001, $130,000, *Applied Cryptography*, co-principal investigator (with S. Vanstone).

CITO, 2000–2002, $200,000, *Information Security Technology and Applied Cryptography*, joint grant with G. Agnew, A. Hasan, A. Menezes, M. Mosca and S. Vanstone.

NSERC discovery grant (Computing and Information Sciences - B), 2002–2006, $184,000, *Topics in Cryptography*.

Open Text, 2004–2007, $60,000, *Data Security*, joint grant with G. Gong, A. Hasan and A. Menezes.

NSERC discovery grant (Computing and Information Sciences - B), 2006–2011, $250,000, *Topics in Cryptography*.

NSERC collaborative research and development grant, 2007–2008, $25391, joint grant with G. Gong, A. Hasan and A. Menezes.

MITACS, 2008–2010, $240,000, *Useful Privacy-Enhancing Technologies* joint grant with R. Safavi-Naini, I. Goldberg (co-PIs) and 7 others.

NSERC Strategic Project, 2009–2012, $450,000, *Computer and Communication Platform Security and Content Protection* joint grant with G. Gong, A. Hasan and A. Menezes.

MITACS, 2010–2012, $240,000, *Useful Privacy-Enhancing Technologies* joint grant with R. Safavi-Naini, I. Goldberg (co-PIs) and 7 others.

NSERC discovery grant (Computing and Information Sciences - B), 2011–2016, $245,000, *Cryptography and Cryptographic Protocols*.

NSERC CREATE grant, 2012–2017, $1,650,000, *Building a Workforce for the Cryptographic Infrastructure of the 21st Century*, joint grant with M. Mosca (PI) and 7 others.

NSERC discovery grant (Computer Science), 2016–2025, $316,000, *Unconditionally Secure Cryptography*.

Publications

Books

1. D. R. Stinson. *An Introduction to the Design and Analysis of Algorithms*. Charles Babbage Research Centre, Winnipeg, Manitoba, 1985 (second edition, 1987), 213 pp.
2. J. H. Dinitz and D. R. Stinson (eds.). *Contemporary Design Theory: A Collection of Surveys*. John Wiley & Sons, New York, 1992, 639 pp.
3. D. R. Stinson (ed.). *Advances in Cryptology – CRYPTO '93 Proceedings*. Lecture Notes in Computer Science, vol. 773. Springer-Verlag, Berlin, 1994, 492 pp.
4. D. R. Stinson. *Cryptography: Theory and Practice*. CRC Press, Inc., Boca Raton, 1995, 434 pp.

5. D. L. Kreher and D. R. Stinson. *Combinatorial Algorithms: Generation, Enumeration & Search*. CRC Press, Inc., Boca Raton, 1999, 329 pp.
6. D. R. Stinson and S. Tavares (eds.). *Selected Areas in Cryptography – SAC 2000 Proceedings*. Lecture Notes in Computer Science, vol. 2012. Springer-Verlag, Berlin, 2001, 339 pp.
7. D. R. Stinson. *Cryptography: Theory and Practice, Second Edition*. Chapman & Hall/CRC, Boca Raton, 2002, 339 pp.
8. D. R. Stinson. *Combinatorial Designs: Constructions and Analysis*. Springer-Verlag, New York, 2004, 316 pp.
9. D. R. Stinson. *Cryptography: Theory and Practice, Third Edition*. Chapman & Hall/CRC, Boca Raton, 2006, 616 pp.
10. A. Biryukov, G. Gong and D. R. Stinson (eds.). *Selected Areas in Cryptography – SAC 2010 Proceedings*. Lecture Notes in Computer Science, vol. 6544. Springer-Verlag, Berlin, 2011.
11. D. R. Stinson and M. B. Paterson. *Cryptography: Theory and Practice, Fourth Edition*. Chapman & Hall/CRC, Boca Raton, 2018, 580 pp.
12. D. R. Stinson. *Techniques for Designing and Analyzing Algorithms*. Chapman & Hall/CRC, Boca Raton, 2021, 444 pp.

Refereed Conference Papers

13. R. C. Mullin and D. R. Stinson. Near-self-complimentary designs and a method of mixed sums. *Lecture Notes in Mathematics* **686** (1978), 59–67 (International Conference on Combinatorial Theory, Canberra, 1977).
14. R. C. Mullin, D. R. Stinson, and W. D. Wallis. Skew squares of low order. *Congressus Numerantium* **23** (1978), 413–434 (Eighth Manitoba Conference on Numerical Mathematics and Computing, 1978).
15. D. R. Stinson. A generalization of Howell designs. *Congressus Numerantium* **33** (1981), 321–328 (Twelfth Southeastern Conference on Combinatorics, Graph Theory and Computing, 1981).
16. D. R. Stinson. Determination of a covering number. *Congressus Numerantium* **34** (1982), 429–440 (Eleventh Manitoba Conference on Numerical Mathematics and Computing, 1981).
17. D. R. Stinson and G. H. J. van Rees. Some large critical sets. *Congressus Numerantium* **34** (1982), 441–456 (Eleventh Manitoba Conference on Numerical Mathematics and Computing, 1981).
18. D. R. Stinson. Room squares and subsquares. *Lecture Notes in Mathematics* **1036** (1983), 86–95 (Combinatorial Mathematics X, Adelaide, 1982).
19. C. J. Colbourn, M. J. Colbourn, and D. R. Stinson. The computational complexity of recognizing critical sets. *Lecture Notes in Mathematics* **1073** (1984), 248–253 (Graph theory, Singapore 1983).
20. S. Judah, R. C. Mullin, and D. R. Stinson. A note on the covering numbers $g(1,3;v)$. *Congressus Numerantium* **45** (1984), 305–310 (Fifteenth Southeastern Conference on Combinatorics, Graph Theory and Computing, 1984).
21. D. R. Stinson. Some constructions and bounds for authentication codes. *Lecture Notes in Computer Science* **263** (1987), 418–425 (Advances in Cryptology – CRYPTO '86).
22. D. R. Stinson and S. A. Vanstone. A combinatorial approach to threshold schemes. *Lecture Notes in Computer Science* **293** (1988), 330–339 (Advances in Cryptology – CRYPTO '87).

23. E. F. Brickell and D. R. Stinson. Authentication codes with multiple arbiters. *Lecture Notes in Computer Science* **330** (1988), 51–55. (Advances in Cryptology – EUROCRYPT '88).

24. D. R. Stinson. A construction for authentication/secrecy codes from certain combinatorial designs. *Lecture Notes in Computer Science* **293** (1988), 355–366 (Advances in Cryptology – CRYPTO '87).

25. E. Seah and D. R. Stinson. A perfect one-factorization for K_{40}. *Congressus Numerantium* **68** (1989), 211–214 (Eighteenth Manitoba Conference on Numerical Mathematics and Computing, 1988).

26. E. F. Brickell and D. R. Stinson. The detection of cheaters in threshold schemes. *Lecture Notes in Computer Science* **403** (1990), 564–577 (Advances in Cryptology – CRYPTO '88).

27. R. C. Mullin, D. R. Stinson, and W. D. Wallis. Sets of properly separated permutations. *Congressus Numerantium* **80** (1991), 185–191 (Twentieth Manitoba Conference on Numerical Mathematics and Computing, 1990).

28. E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *Lecture Notes in Computer Science* **537** (1991), 242–252 (Advances in Cryptology – CRYPTO '90).

29. D. R. Stinson. Combinatorial characterizations of authentication codes. *Lecture Notes in Computer Science* **576** (1992), 62–73 (Advances in Cryptology – CRYPTO '91).

30. D. R. Stinson. Universal hashing and authentication codes. *Lecture Notes in Computer Science* **576** (1992), 74–85 (Advances in Cryptology – CRYPTO '91).

31. D. R. Stinson. Resilient functions and large sets of orthogonal arrays. *Congressus Numerantium* **92** (1993), 105–110 (Twenty-second Manitoba Conference on Numerical Mathematics and Computing, 1992).

32. C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *Lecture Notes in Computer Science* **658** (1993), 1–24 (Advances in Cryptology – EUROCRYPT '92).

33. D. R. Stinson. New general lower bounds on the information rate of secret sharing schemes. *Lecture Notes in Computer Science* **740** (1993), 170–184 (Advances in Cryptology – CRYPTO '92).

34. J. Bierbrauer, K. Gopalakrishnan and D. R. Stinson. Bounds for resilient functions and orthogonal arrays. *Lecture Notes in Computer Science* **839** (1994), 247–256 (Advances in Cryptology – CRYPTO '94).

35. C. Blundo, A. Giorgio Gaggia and D. R. Stinson. On the dealer's randomness required in secret sharing schemes. *Lecture Notes in Computer Science* **950** (1995), 35–46 (Advances in Cryptology – EUROCRYPT '94).

36. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson. Constructions and bounds for visual cryptography. *Lecture Notes in Computer Science* **1099** (1996), 416–428 (23rd International Colloquium on Automata, Languages and Programming).

37. M. Atici and D. R. Stinson. Universal hashing and multiple authentication. *Lecture Notes in Computer Science* **1109** (1996), 16–30 (Advances in Cryptology – CRYPTO '96).

38. C. Blundo, L. Frota Mattos and D. R. Stinson. Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution. *Lecture Notes in Computer Science* **1109** (1996), 387–400 (Advances in Cryptology – CRYPTO '96).

39. D. R. Stinson. On the connections between universal hashing, combinatorial designs and error-correcting codes. *Congressus Numerantium* **114** (1996), 7–27 (Twenty-fifth Manitoba Conference on Combinatorial Mathematics and Computing, 1995).

40. K. Kurosawa, T. Johansson and D. R. Stinson. Almost k-wise independent sample spaces and their cryptologic applications. *Lecture Notes in Computer Science* **1233** (1997), 409–421 (Advances in Cryptology – EUROCRYPT '97).

41. D. R. Stinson and R. Wei. Key preassigned traceability schemes for broadcast encryption. *Lecture Notes in Computer Science* **1556** (1999), 144–156 (Selected Areas in Cryptography, 1998).

42. G. Gong, T. A. Berson and D. R. Stinson. Elliptic curve pseudorandom sequence generators. *Lecture Notes in Computer Science* **1758** (2000), 34–48 (Selected Areas in Cryptography, 1999).

43. D. R. Stinson and R. Wei. Unconditionally secure proactive secret sharing scheme with combinatorial structures. *Lecture Notes in Computer Science* **1758** (2000), 200–214 (Selected Areas in Cryptography, 1999).

44. B. Masucci and D. R. Stinson. Metering schemes for general access structures. *Lecture Notes in Computer Science* **1895** (2000), 72–87 (Sixth European Symposium on Research in Computer Security, ESORICS 2000).

45. C. Blundo, A. De Bonis, B. Masucci and D. R. Stinson. Dynamic multi-threshold metering schemes. *Lecture Notes in Computer Science* **2012** (2001), 131–144 (Selected Areas in Cryptography, 2000).

46. D. R. Stinson and R. Strobl. Provably secure distributed Schnorr signatures and a (t, n) threshold scheme for implicit certificates. *Lecture Notes in Computer Science* **2119** (2001), 417–434 (Sixth Australasian Conference on Information Security and Privacy, ACISP 2001).

47. P. Sarkar and D. R. Stinson. Frameproof and IPP codes. *Lecture Notes in Computer Science* **2247** (2001), 117–126 (INDOCRYPT 2001).

48. P. D'Arco and D. R. Stinson. Generalized zig-zag functions and oblivious transfer reductions. *Lecture Notes in Computer Science* **2259** (2002), 87–102 (Selected Areas in Cryptography, 2001).

49. K. Khoo, G. Gong and D. Stinson. A new family of Gold-like sequences (extended abstract). *Proceedings of the IEEE International Symposium on Information Theory*, 2002, p. 181.

50. P. D'Arco and D. R. Stinson. On unconditionally secure robust distributed key distribution centers. *Lecture Notes in Computer Science* **2501** (2002), 346–363 (ASIACRYPT 2002 Proceedings).

51. C. Blundo, P. D'Arco, A. De Santis and D. R. Stinson. New results on unconditionally secure distributed oblivious transfer. *Lecture Notes in Computer Science* **2595** (2003), 291-309 (SAC 2002 Proceedings).

52. P. D'Arco and D. R. Stinson. Fault tolerant and distributed broadcast encryption. *Lecture Notes in Computer Science* **2612** (2003), 262–279 (Topics in Cryptography, CT-RSA 2003).

53. J. A. Muir and D. R. Stinson. Alternative digit sets for nonadjacent representations. *Lecture Notes in Computer Science* **3006** (2004), 306–319 (SAC 2003 Proceedings).

54. J. Lee and D. R. Stinson. Deterministic key predistribution schemes for distributed sensor networks. *Lecture Notes in Computer Science* **3357** (2005), 294–307 (SAC 2004 Proceedings).

55. J. A. Muir and D. R. Stinson. New minimal weight representations for left-to-right window methods. *Lecture Notes in Computer Science* **3376** (2005), 366–383 (CT-RSA 2005).

56. J. Lee and D. R. Stinson. A combinatorial approach to key predistribution for distributed sensor networks. *IEEE Wireless Communications and Networking Conference (WCNC 2005)*, vol. 2, pp. 1200–1205.

57. J. Lee and D. R. Stinson. Tree-based key distribution patterns. *Lecture Notes in Computer Science* **3897** (2006), 189–204 (SAC 2005 Proceedings).

58. P. C. Li, D. R. Stinson, G. H. J. van Rees and R. Wei. On $\{123, 124, 134\}$-free hypergraphs. *Congressus Numerantium* **183** (2006), 161–174 (Thirty-seventh Southeastern International Conference on Combinatorics, Graph Theory and Computing, 2006).

59. J. Wu and D. R. Stinson. Minimum node degree and κ-connectivity for key predistribution schemes and distributed sensor networks. *Proceedings of the First ACM Conference on Wireless Network Security (WiSec 2008)*, pp. 119–124.

60. J. Sui and D. R. Stinson. A critical analysis and improvement of AACS drive-host authentication. *Lecture Notes in Computer Science* **5107** (2008), 37–52 (13th Australasian Conference on Information Security and Privacy, ACISP 2008).

61. S. R. Blackburn, K. M. Martin, M. B. Paterson and D. R. Stinson. Key refreshing in wireless sensor networks. *Lecture Notes in Computer Science* **5155** (2008), 156–170 (International Conference on Information Theoretic Security, ICITS 2008).

62. J. Wu and D. R. Stinson. Authorship proof for textual document. *Lecture Notes in Computer Science* **5284** (2008), 209–223 (Information Hiding 2008).

63. K. Gopalakrishnan and D. R. Stinson. Applications of orthogonal arrays to computer science. *Lecture Notes Series in Mathematics (Ramanujan Mathematical Society)* **7** (2008), 149–164 (International Conference on Discrete Mathematics, ICDM 2006).

64. A. Mashatan and D. R. Stinson. A new message recognition protocol for ad hoc pervasive networks. *Lecture Notes in Computer Science* **5339** (2008), 378–394 (Seventh International Conference on Cryptology and Network Security, CANS 2008).

65. J. Wu and D. R. Stinson. How to improve security and reduce hardware demands of the WIPR RFID protocol. *2009 IEEE International Conference on RFID*, pp. 192–199.

66. I. Goldberg, A. Mashatan and D. R. Stinson. A new message recognition protocol with full recoverability for ad hoc pervasive networks. *Lecture Notes in Computer Science* **5536** (2009), 219–237 (7th International Conference on Applied Cryptography and Network Security, ACNS '09).

67. J. Wu and D. R. Stinson. A highly scalable RFID authentication protocol. *Lecture Notes in Computer Science* **5594** (2009), 360–376 (14th Australasian Conference on Information Security and Privacy, ACISP '09).

68. G. M. Zaverucha and D. R. Stinson. Group testing and batch verification. *Lecture Notes in Computer Science* **5973** (2010), 140–157 (ICITS 2009).

69. M. Nojoumian and D. R. Stinson. Brief announcement: secret sharing based on the social behaviors of players. *Proceedings of the 29th ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing* (2010), 239–240.

70. M. Nojoumian and D. R. Stinson. Unconditionally secure first-price auction protocols using a multicomponent commitment scheme. *Lecture Notes in Computer Science* **6476** (2010), 266–280 (ICICS 2010).

71. K. Henry and D. R. Stinson. Secure network discovery in wireless sensor networks using combinatorial key pre-distribution. *2011 IEEE Workshop on Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec 2011)*, pp. 34–43.

72. C. Swanson and D. R. Stinson. Unconditionally secure signature schemes revisited. *Lecture Notes in Computer Science* **6673** (2011), 100–116 (ICITS 2011).

73. M. Nojoumian and D. R. Stinson. Social secret sharing in cloud computing using a new trust function. *Tenth Annual Conference on Privacy, Security and Trust (PST 2012)*, pp. 161–167.

74. M. Nojoumian and D. R. Stinson. Socio-rational secret sharing as a new direction in rational cryptography. *Lecture Notes in Computer Science* **7638** (2012), 18–37 (Conference on Decision and Game Theory for Security, GameSec 2012).

75. K. Henry, M. B. Paterson and D. R. Stinson. Practical approaches to varying network size in combinatorial key predistribution schemes. *Lecture Notes in Computer Science* **8282** (2014) 89–117 (SAC 2013 Proceedings).

76. M. Nojoumian and D. R. Stinson. Efficient sealed-bid auction protocols using verifiable secret sharing. *Lecture Notes in Computer Science* **8434** (2014), 302–317 (10th International Conference on Information Security Practice and Experience, ISPEC 2014).

77. D. R. Stinson. Looking back—my life as a mathematician and cryptographer. *Lecture Notes in Computer Science* **11959** (2020) 1–18 (SAC 2019 Proceedings).

Book Chapters

78. R. C. Mullin, P. J. Schellenberg, D. R. Stinson, and S. A. Vanstone. Some results on the existence of squares. In "Combinatorial Mathematics, Optimal Designs and their Applications", North-Holland, 1980, pp. 257–274 (*Annals of Discrete Mathematics*, vol. 6).

79. D. R. Stinson and W. D. Wallis. Some designs used in constructing skew Room squares. In "Combinatorics '79", North-Holland, 1980, pp. 171–175 (*Annals of Discrete Mathematics*, vol. 8).

80. D. R. Stinson. Hill-climbing algorithms for the construction of combinatorial designs. In "Algorithms in Combinatorial Design Theory", North-Holland, 1985, pp. 321–334 (*Annals of Discrete Mathematics*, vol. 26).

81. C. J. Colbourn, M. J. Colbourn, and D. R. Stinson. The computational complexity of finding subdesigns of combinatorial designs. In "Algorithms in Combinatorial Design Theory", North-Holland, 1985, pp. 59–66 (*Annals of Discrete Mathematics*, vol. 26).

82. J. D. Horton, B. K. Roy, P. J. Schellenberg, and D. R. Stinson. On decomposing graphs into isomorphic uniform $2-$factors. In "Cycles in Graphs", North-Holland, 1985, pp. 297–320 (*Annals of Discrete Mathematics*, vol. 27).

83. E. Seah and D. R. Stinson. Some perfect one-factorizations for K_{14}. In "Combinatorial Design Theory", North-Holland, 1987, pp. 419–436 (*Annals of Discrete Mathematics*, vol. 34).

84. D. R. Stinson and W. D. Wallis. Graphs which are not leaves of maximal partial triple systems. In "Combinatorial Design Theory", North-Holland, 1987, pp. 449–460 (*Annals of Discrete Mathematics*, vol. 34).

85. D. R. Stinson. The construction of nested cycle systems. In "Coding Theory and Design Theory, Part II, Design Theory", Springer-Verlag, 1990, pp. 362–367 (*IMA Volumes in Mathematics and its Applications*, vol. 21).

86. J. H. Dinitz and D. R. Stinson. On the existence of Room squares with subsquares. In "Finite Geometries and Combinatorial Designs", American Mathematical Society, 1990, pp. 73–91 (*Contemporary Mathematics*, vol. 111).

87. J. H. Dinitz and D. R. Stinson. A brief introduction to design theory. In "Contemporary Design Theory – A Collection of Surveys", John Wiley & Sons, Inc., 1992, pp. 1–12.

88. J. H. Dinitz and D. R. Stinson. A survey of Room squares and related designs. In "Contemporary Design Theory – A Collection of Surveys", John Wiley & Sons, Inc., 1992, pp. 137–204.

89. J. H. Dinitz and D. R. Stinson. A few more Room frames. In "Graphs, Matrices and Designs", Marcel Dekker, Inc., 1993, pp. 133–146.

90. D. R. Stinson. Combinatorial designs and cryptography. In "Surveys in Combinatorics, 1993", Cambridge University Press, 1993, pp. 257–287 (*London Mathematical Lecture Note Series*, vol. 187).

91. D. R. Stinson. Coverings. In "The CRC Handbook of Combinatorial Designs", CRC Press, Inc., 1996, pp. 260–265.

92. D. R. Stinson. Packings. In "The CRC Handbook of Combinatorial Designs", CRC Press, Inc., 1996, pp. 409–413.

93. K. Gopalakrishnan and D. R. Stinson. Applications of designs to cryptography. In "The CRC Handbook of Combinatorial Designs", CRC Press, Inc., 1996, pp. 549–557.

94. K. Gopalakrishnan and D. R. Stinson. Derandomization. In "The CRC Handbook of Combinatorial Designs", CRC Press, Inc., 1996, pp. 558–560.

95. C. J. Colbourn, J. H. Dinitz and D. R. Stinson. Applications of combinatorial designs to communications, cryptography and networking. In "Surveys in Combinatorics, 1999", Cambridge University Press, 1999, pp. 37–100 (*London Mathematical Lecture Note Series*, vol. 267).

96. J. H. Dinitz and D. R. Stinson. A singular direct product for bicolorable Steiner triple systems. In "Codes and Designs", Walter de Gruyter, 2002, pp. 87–97 (*Ohio State University Mathematical Research Institute Publications*, vol. 10).

97. M. Qu, D. Stinson and S. Vanstone. Cryptanalysis of the Sakazaki-Okamoto-Mambo ID-based key distribution system over elliptic curves. In "Finite Fields with Applications to Coding Theory, Cryptography and Related Areas", Springer-Verlag, 2002, pp. 263–269 (*Sixth International Conference on Finite Fields and Applications*).

98. D. R. Stinson. Bent functions. In "Handbook of Combinatorial Designs, Second Edition", CRC Press, Inc., 2006, pp. 337–339.

99. K. Gopalakrishnan and D. R. Stinson. Correlation-immune and resilient functions. In "Handbook of Combinatorial Designs, Second Edition", CRC Press, Inc., 2007, pp. 355–357.

100. D. M. Gordon and D. R. Stinson. Coverings. In "Handbook of Combinatorial Designs, Second Edition", CRC Press, Inc., 2007, pp. 365–373.

101. K. Gopalakrishnan and D. R. Stinson. Derandomization. In "Handbook of Combinatorial Designs, Second Edition", CRC Press, Inc., 2007, pp. 389–391.

102. D. R. Stinson, R. Wei and J. Yin. Packings. In "Handbook of Combinatorial Designs, Second Edition", CRC Press, Inc., 2007, pp. 550–556.

103. K. Gopalakrishnan and D. R. Stinson. Secrecy and authentication codes. In "Handbook of Combinatorial Designs, Second Edition", CRC Press, Inc., 2007, pp. 606–611.

104. K. Gopalakrishnan and D. R. Stinson. Threshold and ramp schemes. In "Handbook of Combinatorial Designs, Second Edition", CRC Press, Inc., 2007, pp. 635–639.

105. C. Guo, D. R. Stinson and Tran van Trung. On symmetric designs and binary frameproof codes. In *Springer Proceedings in Mathematics and Statistics*, "Algebraic Design Theory and Hadamard Matrices", Springer, 2015, pp. 125–136.

106. D. R. Stinson. Combinatorial designs and cryptography, revisited. In "50 Years of Combinatorics, Graph Theory, and Computing", CRC Press, 2020, pp. 335–358.

107. D. R. Stinson. Orthogonal and strong frame starters, revisited. In "New Advances in Designs, Codes and Cryptography, Stinson66 Conference Proceedings", Springer, 2024, pp. 379–392.

Journal Papers

108. D. R. Stinson. Determination of a packing number. *Ars Combinatoria* **3** (1977), 89–114.

109. D. R. Stinson. A note on the existence of 7 and 8 mutually orthogonal Latin squares. *Ars Combinatoria* **6** (1978), 113–115.

110. R. C. Mullin, D. R. Stinson, and W. D. Wallis. Concerning the spectrum of skew Room squares. *Ars Combinatoria* **6** (1978), 277–291.

111. D. R. Stinson. The existence of 30 mutually orthogonal Latin squares. *Ars Combinatoria* **7** (1979), 153–170.

112. D. R. Stinson. The distance between units in rings – an algorithmic approach. *Utilitas Mathematica* **15** (1979), 281–292.

113. D. R. Stinson. A generalization of Wilson's construction for mutually orthogonal Latin squares. *Ars Combinatoria* **8** (1979), 95–105.

114. J. H. Dinitz and D. R. Stinson. Boss block designs. *Ars Combinatoria* **9** (1980), 59–68.

115. D. S. Archdeacon, J. H. Dinitz, D. R. Stinson, and T. W. Tillson. Some new row-complete Latin squares. *Journal of Combinatorial Theory A* **29** (1980), 395–398.

116. J. H. Dinitz and D. R. Stinson. A note on Howell designs of odd side. *Utilitas Mathematica* **18** (1980), 207–216.

117. D. R. Stinson. A skew Room square of order 129. *Discrete Mathematics* **31** (1980), 333–335.

118. J. H. Dinitz and D. R. Stinson. The construction and uses of frames. *Ars Combinatoria* **10** (1980), 31–54.

119. B. A. Anderson, R. C. Mullin, and D. R. Stinson. More skew Room squares. *Utilitas Mathematica* **18** (1980), 201–205.

120. D. R. Stinson. A general construction for group-divisible designs. *Discrete Mathematics* **33** (1981), 89–94.

121. J. H. Dinitz and D. R. Stinson. A fast algorithm for finding strong starters. *SIAM Journal on Algebraic and Discrete Methods* **2** (1981), 50–56.

122. J. H. Dinitz and D. R. Stinson. The spectrum of Room cubes. *European Journal of Combinatorics* **2** (1981), 221–230.

123. J. H. Dinitz and D. R. Stinson. Further results on frames. *Ars Combinatoria* **11** (1981), 275–288.

124. D. R. Stinson. Some results concerning frames, Room squares, and subsquares. *Journal of the Australian Mathematical Society A* **31** (1981), 376–384.

125. P. J. Schellenberg, D. R. Stinson, S. A. Vanstone, and J. W. Yates. The existence of Howell designs of side $n+1$ and order $2n$. *Combinatorica* **1** (1981), 289–301.

126. A. Hartman and D. R. Stinson. A note on one-factorizations. *Utilitas Mathematica* **20** (1981), 155–162.

127. D. R. Stinson. The spectrum of skew Room squares. *Journal of the Australian Mathematical Society A* **31** (1981), 475–480.

128. D. R. Stinson. The non-existence of a $(2,4)-$frame. *Ars Combinatoria* **11** (1981), 99–106.

129. D. R. Stinson. Some constructions for frames, Room squares, and subsquares. *Ars Combinatoria* **12** (1981), 229–267.

130. R. C. Mullin, R. G. Stanton, and D. R. Stinson. Perfect pair-coverings and an algorithm for certain $1-2$ factorizations of the complete graph K_{2s+1}. *Ars Combinatoria* **12** (1981), 73–80.

131. R. C. Mullin, D. R. Stinson, and S. A. Vanstone. Kirkman triple systems containing maximum subdesigns. *Utilitas Mathematica* **21C** (1982), 283–300.

132. D. R. Stinson. The existence of Howell designs of odd side. *Journal of Combinatorial Theory A* **32** (1982), 53–65.

133. A. Hartman, R. C. Mullin, and D. R. Stinson. Exact covering configurations and Steiner systems. *Journal of the London Mathematical Society* **2** (1982), 193–200.

134. D. R. Stinson. Applications and generalizations of the variance method in combinatorial designs. *Utilitas Mathematica* **22** (1982), 323–333.

135. D. R. Stinson. A short proof of a theorem of de Witte. *Ars Combinatoria* **14** (1982), 79–86.

136. J. H. Dinitz and D. R. Stinson. MOLS with holes. *Discrete Mathematics* **44** (1983), 145–154.

137. D. R. Stinson. The non-existence of certain finite linear spaces. *Geometriae Dedicata* **13** (1983), 429–434.

138. P. Erdös, R. C. Mullin, V. Sós, and D. R. Stinson. Finite linear spaces and projective planes. *Discrete Mathematics* **47** (1983), 49–62.

139. D. R. Stinson and W. D. Wallis. Snappy constructions for triple systems. *Gazette of the Australian Mathematical Society* **10** (1983), 84–88.

140. D. R. Stinson and W. D. Wallis. Twofold triple systems without repeated blocks. *Discrete Mathematics* **47** (1983), 125–128.

141. J. H. Dinitz and D. R. Stinson. On non-isomorphic Room squares. *Proceedings of the American Mathematical Society* **89** (1983), 175–181.

142. J. H. Dinitz, D. R. Stinson, and W. D. Wallis. Room squares with holes of sides 3, 5, and 7. *Discrete Mathematics* **47** (1983), 221–228.

143. R. G. Stanton and D. R. Stinson. Perfect pair-coverings with block sizes 2, 3, and 4. *Journal of Combinatorics, Information and Systems Sciences* **8** (1983), 21–25.

144. C. C. Lindner, R. C. Mullin, and D. R. Stinson. On the spectrum of resolvable orthogonal arrays invariant under the Klein group K_4. *Aequationes Mathematicae* **26** (1983), 176–183.

145. D. R. Stinson. A comparison of two invariants for Steiner triple systems: fragments and trains. *Ars Combinatoria* **16** (1983), 69–76.

146. C. C. Lindner and D. R. Stinson. The spectrum for the conjugate invariant subgroups of perpendicular arrays. *Ars Combinatoria* **18** (1983), 51–60.

147. D. R. Stinson. On scheduling perfect competitions. *Ars Combinatoria* **18** (1984), 45–49.

148. D. R. Stinson. A short proof of the non-existence of a pair of orthogonal Latin squares of order 6. *Journal of Combinatorial Theory A* **36** (1984), 373–376.

149. B. A. Anderson, P. J. Schellenberg, and D. R. Stinson. The existence of Howell designs of even side. *Journal of Combinatorial Theory A* **36** (1984), 23–55.

150. D. R. Stinson and G. H. J. van Rees. Some improved results concerning the Cordes problem. *Ars Combinatoria* **17** (1984), 117–128.

151. D. R. Stinson. Pair-packings and projective planes. *Journal of Australian Mathematical Society A* **37** (1984), 27–38.

152. D. R. Stinson and W. D. Wallis. An even side analogue of Room squares. *Aequationes Mathematicae* **27** (1984), 201–213.

153. E. Billington, R. G. Stanton, and D. R. Stinson. On λ-packings with block-size four ($v \not\equiv 0 \bmod 3$). *Ars Combinatoria* **17A** (1984), 73–84.

154. R. C. Mullin and D. R. Stinson. Holey SOLSSOMs. *Utilitas Mathematica* **25** (1984), 159–169.

155. D. R. Stinson and G. H. J. van Rees. The equivalence of certain equidistant binary codes and symmetric BIBDs. *Combinatorica* **4** (1984), 357–362.

156. C. C. Lindner and D. R. Stinson. Steiner pentagon systems. *Discrete Mathematics* **52** (1984), 67–74.

157. D. R. Stinson and S. A. Vanstone. A note on non-isomorphic Kirkman triple systems. *Journal of Combinatorics, Information and Systems Sciences* **9** (1984), 113–116.

158. D. R. Stinson and H. Ferch. 2000000 Steiner triple systems of order 19. *Mathematics of Computation* **44** (1985), 533–535.

159. D. R. Stinson and L. Zhu. On sets of three MOLS with holes. *Discrete Mathematics* **54** (1985), 321–328.

160. D. R. Stinson and S. A. Vanstone. Some non-isomorphic Kirkman triple systems of orders 39 and 51. *Utilitas Mathematica* **27** (1985), 199–205.

161. D. R. Stinson and S. A. Vanstone. A Kirkman square of order 51 and block-size 3. *Discrete Mathematics* **55** (1985), 107–111.

162. D. S. Archdeacon, J. H. Dinitz, and D. R. Stinson. V-squares. *Ars Combinatoria* **19** (1985), 161–174.

163. D. R. Stinson. Isomorphism testing of Steiner triple systems: canonical forms. *Ars Combinatoria* **19** (1985), 213–218.

164. D. R. Stinson. The spectrum of nested Steiner triple systems. *Graphs and Combinatorics* **1** (1985), 189–191.

165. W. L. Kocay, D. R. Stinson, and S. A. Vanstone. On strong starters in cyclic groups. *Discrete Mathematics* **56** (1985), 45–60.

166. D. R. Stinson and S. A. Vanstone. A few more balanced Room squares. *Journal of the Australian Mathematical Society A* **39** (1985), 344–352.

167. D. R. Stinson. Room squares with maximum empty subarrays. *Ars Combinatoria* **20** (1985), 159–166.

168. D. R. Stinson and E. Seah. 284457 Steiner triple systems of order 19 contain a subsystem of order 9. *Mathematics of Computation* **46** (1986), 717–729.

169. A. Rosa and D. R. Stinson. One-factorizations of regular graphs and Howell designs of small order. *Utilitas Mathematica* **29** (1986), 99–124.

170. E. Seah and D. R. Stinson. An enumeration of non-isomorphic one-factorizations and Howell designs for the graph K_{10} minus a one-factor. *Ars Combinatoria* **21** (1986), 145–161.

171. C. J. Colbourn, W. L. Kocay, and D. R. Stinson. Some NP-complete problems for hypergraph degree sequences. *Discrete Applied Mathematics* **14** (1986), 239–254.

172. D. R. Stinson. Concerning the spectrum of perpendicular arrays of triple systems. *Discrete Mathematics* **61** (1986), 305–310.

173. D. R. Stinson. Holey perpendicular arrays. *Utilitas Mathematica* **30** (1986), 31–43.

174. D. R. Stinson. The equivalence of certain incomplete transversal designs and frames. *Ars Combinatoria* **22** (1986), 81–87.

175. D. R. Stinson and S. A. Vanstone. Orthogonal packings in $PG(5,2)$. *Aequationes Mathematicae* **31** (1986), 159–168.

176. R. Rees and D. R. Stinson. On resolvable group-divisible designs with block-size 3. *Ars Combinatoria* **23** (1987), 107–120.

177. E. Ihrig, E. Seah, and D. R. Stinson. A perfect one-factorization for K_{50}. *Journal of Combinatorial Mathematics and Combinatorial Computing* **1** (1987), 217–219.

178. E. Seah and D. R. Stinson. An assortment of new Howell designs. *Utilitas Mathematica* **31** (1987), 175–188.

179. D. R. Stinson. Frames for Kirkman triple systems. *Discrete Mathematics* **65** (1987), 289–300.

180. D. R. Stinson and L. Zhu. On the existence of MOLS with equal-sized holes. *Aequationes Mathematicae* **33** (1987), 96–105.

181. J. H. Dinitz and D. R. Stinson. A hill-climbing algorithm for the construction of one-factorizations and Room squares. *SIAM Journal on Algebraic and Discrete Methods* **8** (1987), 430–438.

182. R. C. Mullin and D. R. Stinson. Pairwise balanced designs with block sizes $6t+1$. *Graphs and Combinatorics* **3** (1987), 365–377.

183. A. Assaf, E. Mendelsohn, and D. R. Stinson. On resolvable coverings of pairs by triples. *Utilitas Mathematica* **32** (1987), 67–74.

184. D. R. Stinson. On the existence of skew Room frames of type 2^n. *Ars Combinatoria* **24** (1987), 115–128.

185. D. R. Stinson. Some constructions and bounds for authentication codes. *Journal of Cryptology* **1** (1988), 37–51.

186. E. Seah and D. R. Stinson. On the enumeration of one-factorizations of complete graphs containing prescribed automorphism groups. *Mathematics of Computation* **50** (1988), 607–618.

187. D. R. Stinson. On the spectrum of nested 4-cycle systems. *Utilitas Mathematica* **33** (1988), 47–50.

188. D. R. Stinson and S. A. Vanstone. A combinatorial approach to threshold schemes. *SIAM Journal on Discrete Mathematics* **1** (1988), 230–237.

189. R. Rees and D. R. Stinson. Kirkman triple systems with maximum subsystems. *Ars Combinatoria* **25** (1988), 125–132.

190. C. C. Lindner, C. A. Rodger, and D. R. Stinson. Embedding cycle systems of even length. *Journal of Combinatorial Mathematics and Combinatorial Computing* **3** (1988), 65–69.

191. E. Seah and D. R. Stinson. A perfect one-factorization for K_{36}. *Discrete Mathematics* **70** (1988), 199–202.

192. D. R. Stinson. A construction for authentication/secrecy codes from certain combinatorial designs. *Journal of Cryptology* **1** (1988), 119–127.

193. C. J. Colbourn and D. R. Stinson. Edge-coloured designs with block size four. *Aequationes Mathematicae* **36** (1988), 230–245.

194. R. Rees and D. R. Stinson. On the existence of Kirkman triple systems containing Kirkman subsytems. *Ars Combinatoria* **26** (1989), 3–16.

195. R. Rees and D. R. Stinson. On the existence of incomplete designs of block size four having one hole. *Utilitas Mathematica* **35** (1989), 119–152.

196. P. J. Schellenberg and D. R. Stinson. Threshold schemes from combinatorial designs. *Journal of Combinatorial Mathematics and Combinatorial Computing* **5** (1989), 143–160.

197. D. R. Stinson. A new proof of the Doyen-Wilson theorem. *Journal of the Australian Mathematical Society A* **47** (1989), 32–42.

198. B. Alspach, P. Schellenberg, D. R. Stinson, and D. Wagner. The Oberwolfach problem and factors of uniform odd length cycles. *Journal of Combinatorial Theory A* **52** (1989), 20–43.

199. J. H. Dinitz and D. R. Stinson. Some new perfect one-factorizations from starters in finite fields. *Journal of Graph Theory* **13** (1989), 405–415.

200. K. T. Phelps, D. R. Stinson, and S. A. Vanstone. The existence of simple $S_3(3, 4, v)$. *Discrete Mathematics* **77** (1989), 255–258.

201. C. C. Lindner, C. A. Rodger, and D. R. Stinson. Nesting of cycle systems of odd length. *Discrete Mathematics* **77** (1989), 191–203.

202. R. Rees and D. R. Stinson. On combinatorial designs with subdesigns. *Discrete Mathematics* **77** (1989), 259–279.

203. E. S. Kramer, D. L. Kreher, R. Rees, and D. R. Stinson. On perpendicular arrays with $t \geq 3$. *Ars Combinatoria* **28** (1989), 215–223.

204. D. R. Stinson and L. Teirlinck. A construction for authentication/secrecy codes from 3-homogeneous permutation groups. *European Journal of Combinatorics* **11** (1990), 73–79.

205. D. Chen and D. R. Stinson. Recent results on combinatorial constructions for threshold schemes. *Australasian Journal of Combinatorics* **1** (1990), 29–48.

206. C. C. Lindner, C. A. Rodger, and D. R. Stinson. Small embeddings for partial cycle systems of odd length. *Discrete Mathematics* **80** (1990), 273–280.

207. D. R. Stinson. The combinatorics of authentication and secrecy codes. *Journal of Cryptology* **2** (1990), 23–49.

208. C. C. Lindner and D. R. Stinson. Nesting of cycle systems of even length. *Journal of Combinatorial Mathematics and Combinatorial Computing* **8** (1990), 147–157.

209. D. R. Stinson. Some observations on parallel algorithms for fast exponentiation in $GF(2^n)$. *SIAM Journal on Computing* **19** (1990), 711–717.

210. R. Rees and D. R. Stinson. On the number of blocks in a perfect covering of v points. *Discrete Mathematics* **83** (1990), 81–93.

211. R. C. Mullin and D. R. Stinson. Pairwise balanced designs with odd block sizes exceeding 5. *Discrete Mathematics* **84** (1990), 47–62.

212. E. F. Brickell and D. R. Stinson. The detection of cheaters in threshold schemes. *SIAM Journal on Discrete Mathematics* **4** (1991), 502–510.

213. E. S. Kramer, S. S. Magliveras, and D. R. Stinson. Some small large sets of $t-$designs. *Australasian Journal of Combinatorics* **3** (1991), 191–205.

214. D. R. Stinson and L. Zhu. Orthogonal Steiner triple systems of order $6m+3$. *Ars Combinatoria* **31** (1991), 33–63.

215. C. J. Colbourn, J. H. Dinitz, and D. R. Stinson. Spanning sets and scattering sets in Steiner triple systems. *Journal of Combinatorial Theory A* **57** (1991), 46–59.

216. C. J. Colbourn, A. Rosa, and D. R. Stinson. Pairwise balanced designs with block sizes 3 and 4. *Canadian Journal of Mathematics* **43** (1991), 673–704.

217. D. R. Stinson and L. Zhu. On the existence of three MOLS with equal-sized holes. *Australasian Journal of Combinatorics* **4** (1991), 33–47.

218. D. R. Stinson. A survey of Kirkman triple systems and related designs. *Discrete Mathematics* **92** (1991), 371–393.

219. D. Chen, R. G. Stanton, and D. R. Stinson. Disjoint packings on $6k+5$ points. *Utilitas Mathematica* **40** (1991), 129–138.

220. D. R. Stinson. Designs constructed from maximal arcs. *Discrete Mathematics* **97** (1991), 387–393.

221. D. R. Stinson. On bit serial multiplication and dual bases in $GF(2^m)$. *IEEE Transactions on Information Theory* **37** (1991), 1733–1736.

222. C. C. Lindner, C. A. Rodger, and D. R. Stinson. Nestings of directed cycle systems. *Ars Combinatoria* **32** (1991), 153–159.

223. R. Rees and D. R. Stinson. Frames with block size four. *Canadian Journal of Mathematics* **44** (1992), 1030–1049.

224. C. J. Colbourn, D. R. Stinson, and L. Teirlinck. A parallelization of Miller's $n^{\log n}$ technique. *Information Processing Letters* **42** (1992), 223–228.

225. D. R. Stinson and Y. J. Wei. Some results on quadrilaterals in Steiner triple systems. *Discrete Mathematics* **105** (1992), 207–219.

226. D. Chen, C. C. Lindner, and D. R. Stinson. Further results on large sets of disjoint group-divisible designs. *Discrete Mathematics* **110** (1992), 35–42.

227. E. F. Brickell and D. R. Stinson. Some improved bounds on the information rate of perfect secret sharing schemes. *Journal of Cryptology* **5** (1992), 153–166.

228. D. R. Stinson. An explication of secret sharing schemes. *Designs, Codes and Cryptography* **2** (1992), 357–390.

229. C. J. Colbourn, S. S. Magliveras, and D. R. Stinson. Steiner triple systems of order 19 with nontrivial automorphism group. *Mathematics of Computation* **59** (1992), 283–295.

230. C. A. Rodger and D. R. Stinson. Nesting directed cycle systems of even length. *European Journal of Combinatorics* **13** (1992), 213–218.

231. D. R. Stinson. Combinatorial characterizations of authentication codes. *Designs, Codes and Cryptography* **2** (1992), 175–187.

232. D. Chen and D. R. Stinson. On the construction of large sets of disjoint group-divisible designs. *Ars Combinatoria* **35** (1993), 103–115.

233. S. A. Vanstone, D. R. Stinson, P. J. Schellenberg, A. Rosa, R. Rees, C. J. Colbourn, M. Carter, and J. Carter. Hanani triple systems. *Israel Journal of Mathematics* **83** (1993), 305–319.

234. D. R. Stinson. An explicit formulation of the second Johnson bound. *Bulletin of the ICA* **8** (1993), 86–92.

235. D. R. Stinson and L. Zhu. Towards the spectrum of Room squares with subsquares. *Journal of Combinatorial Theory A* **63** (1993), 129–142.

236. A. M. Hamel, W. H. Mills, R. C. Mullin, R. Rees, D. R. Stinson, and J. Yin. The spectrum of PBD$(\{5, k^*\}, v)$ for $k = 9, 13$. *Ars Combinatoria* **36** (1993), 7–26.

237. K. Gopalakrishnan, D. G. Hoffman and D. R. Stinson. A note on a conjecture concerning symmetric resilient functions. *Information Processing Letters* **47** (1993), 139–143.

238. D. R. Stinson. Decomposition constructions for secret sharing schemes. *IEEE Transactions on Information Theory* **40** (1994), 118–125.

239. D. R. Stinson and L. Zhu. On the existence of certain SOLS with holes. *Journal of Combinatorial Mathematics and Combinatorial Computing* **15** (1994), 33–45.

240. D. R. Stinson. Combinatorial techniques for universal hashing. *Journal of Computer and System Sciences* **48** (1994), 337–346.

241. D. R. Stinson. Universal hashing and authentication codes. *Designs, Codes and Cryptography* **4** (1994), 369–380.

242. J. H. Dinitz, D. R. Stinson and L. Zhu. On the spectra of certain classes of Room frames. *Electronic Journal of Combinatorics* **1** (1994), paper #R7, 21pp.

243. C. Blundo, A. De Santis, D. R. Stinson, and U. Vaccaro. Graph decompositions and secret sharing schemes. *Journal of Cryptology* **8** (1995), 39–64.

244. D. R. Stinson and J. L. Massey. An infinite class of counterexamples to a conjecture concerning non-linear resilient functions. *Journal of Cryptology* **8** (1995), 167–173.

245. K. Gopalakrishnan and D. R. Stinson. Three characterizations of non-binary correlation-immune and resilient functions. *Designs, Codes and Cryptography* **5** (1995), 241–251.

246. C. Blundo, L. Frota Mattos and D. R. Stinson. Multiple key distribution maintaining user anonymity via broadcast channels. *Journal of Computer Security* **3** (1994/95), 309-323.

247. R. S. Rees and D. R. Stinson. Combinatorial characterizations of authentication codes II. *Designs, Codes and Cryptography* **7** (1996), 239–259.

248. J. Bierbrauer, K. Gopalakrishnan and D. R. Stinson. Orthogonal arrays, resilient functions, error-correcting codes and linear programming bounds. *SIAM Journal on Discrete Mathematics* **9** (1996), 424–452.

249. M. Atici, S. S. Magliveras, D. R. Stinson and W.-D. Wei. Some recursive constructions for perfect hash families. *Journal of Combinatorial Designs* **4** (1996), 353–363.

250. K. Gopalakrishnan and D. R. Stinson. A short proof of the non-existence of certain cryptographic functions. *Journal of Combinatorial Mathematics and Combinatorial Computing* **20** (1996), 129–137.

251. C. J. Colbourn, J. H. Dinitz and D. R. Stinson. More thwarts in transversal designs. *Finite Fields and Their Applications* **2** (1996), 293–303.

252. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson. Visual cryptography for general access structures. *Information and Computation* **129** (1996), 86–106.

253. K. Gopalakrishnan and D. R. Stinson. A simple analysis of the error probability of two-point based sampling. *Information Processing Letters* **60** (1996), 91–96.

254. C. Blundo, A. Giorgio Gaggia and D. R. Stinson. On the dealer's randomness required in secret sharing schemes. *Designs, Codes and Cryptography* **11** (1997), 235-259.

255. D. L. Kreher and D. R. Stinson. Small group divisible designs with block size four. *Journal of Statistical Planning and Inference* **58** (1997), 111–118.

256. C. J. Colbourn, D. R. Stinson and L. Zhu. More frames with block size four. *Journal of Combinatorial Mathematics and Combinatorial Computing* **23** (1997), 3–19.

257. C. Blundo and D. R. Stinson. Anonymous secret sharing schemes. *Discrete Applied Mathematics* **77** (1997), 13–28.

258. D. R. Stinson. On some methods for unconditionally secure key distribution and broadcast encryption. *Designs, Codes and Cryptography* **12** (1997), 215–243.

259. D. L. Kreher, D. R. Stinson and L. Zhu. On the maximum number of fixed points in automorphisms of prime order of 2-$(v, k, 1)$ designs. *Annals of Combinatorics* **1** (1997), 227–243.

260. C. Blundo, L. Frota Mattos and D. R. Stinson. Generalized Beimel-Chor schemes for broadcast encryption and interactive key distribution. *Theoretical Computer Science* **200** (1998), 313–334.

261. D. R. Stinson and R. Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM Journal on Discrete Mathematics* **11** (1998), 41–53.

262. J. Bierbrauer, K. Gopalakrishnan and D. R. Stinson. A note on the duality of linear programming bounds for orthogonal arrays and codes. *Bulletin of the ICA* **22** (1998), 17–24.

263. K. Kurosawa, K. Okada, H. Saido, and D. R. Stinson. New combinatorial bounds for authentication codes and key predistribution schemes. *Designs, Codes and Cryptography* **15** (1998), 87–100.

264. D. R. Stinson and Tran van Trung. Some new results on key distribution patterns and broadcast encryption. *Designs, Codes and Cryptography* **14** (1998), 261–279.

265. D. R. Stinson. Some results on nonlinear zigzag functions. *Journal of Combinatorial Mathematics and Combinatorial Computing* **29** (1999), 127–138.

266. C. Blundo, A. De Santis and D. R. Stinson. On the contrast in visual cryptography schemes. *Journal of Cryptology* **12** (1999), 261–289.

267. W. J. Martin and D. R. Stinson. A generalized Rao bound for ordered orthogonal arrays and (t, m, s)-nets. *Canadian Mathematical Bulletin* **42** (1999), 359–370.

268. W. J. Martin and D. R. Stinson. Association schemes for ordered orthogonal arrays and (T, M, S)-nets. *Canadian Journal of Mathematics* **51** (1999), 326–346.

269. D. R. Stinson and R. Wei. An application of ramp schemes to broadcast encryption. *Information Processing Letters* **69** (1999), 131–135.

270. R. Rees, D. R. Stinson, R. Wei and G. H. J. van Rees. An application of covering designs: Determining the maximum consistent set of shares in a threshold scheme. *Ars Combinatoria* **53** (1999), 225–237.

271. D. R. Stinson, Tran van Trung and R. Wei. Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. *Journal of Statistical Planning and Inference* **86** (2000), 595–617.

272. D. R. Stinson, R. Wei and L. Zhu. New constructions for perfect hash families and related structures using combinatorial designs and codes. *Journal of Combinatorial Designs* **8** (2000), 189–200.

273. D. R. Stinson, R. Wei and L. Zhu. Some new bounds for cover-free families. *Journal of Combinatorial Theory A* **90** (2000), 224–234.

274. D. L. Kreher and D. R. Stinson. Pseudocode: a LaTeX style file for displaying algorithms. *Bulletin of the ICA* **30** (2000), 11–24.

275. M. Atici, D. R. Stinson and R. Wei. A new practical algorithm for the construction of a perfect hash function. *Journal of Combinatorial Mathematics and Combinatorial Computing* **35** (2000), 127–145.

276. G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson. Extended capabilities for visual cryptography. *Theoretical Computer Science* **250** (2001), 143–161.

277. D. R. Stinson. Something about all or nothing (transforms). *Designs, Codes and Cryptography* **22** (2001), 133–138.

278. J. N. Staddon, D. R. Stinson and R. Wei. Combinatorial properties of frameproof and traceability codes. *IEEE Transactions on Information Theory* **47** (2001), 1042–1049.

279. C. J. Colbourn, J. H. Dinitz and and D. R. Stinson. Quorum systems constructed from combinatorial designs. *Information and Computation* **169** (2001), 160–173.

280. K. Kurosawa, T. Johansson and D. R. Stinson. Almost k-wise independent sample spaces and their cryptologic applications. *Journal of Cryptology* **14** (2001), 231–253.

281. B. Masucci and D. R. Stinson. Efficient metering schemes with pricing. *IEEE Transactions on Information Theory* **47** (2001), 2835–2844.

282. D. R. Stinson. Some baby-step giant-step algorithms for the low hamming weight discrete logarithm problem. *Mathematics of Computation* **71** (2002), 379–391.

283. P. A. Eisen and D. R. Stinson. Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels. *Designs, Codes and Cryptography* **25** (2002), 15–61.

284. C. J. Colbourn, D. L. Kreher, J. P. McSorley and D. R. Stinson. Orthogonal arrays of strength three from regular 3-wise balanced designs. *Journal of Statistical Planning and Inference* **100** (2002), 191–195.

285. C. Blundo, B. Masucci, D. R. Stinson and R. Wei. Constructions and bounds for unconditionally secure non-interactive commitment schemes. *Designs, Codes and Cryptography* **26** (2002), 97–110.

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

287. D. R. Stinson. Universal hash families and the leftover hash lemma, and applications to cryptography and computing. *Journal of Combinatorial Mathematics and Combinatorial Computing* **42** (2002), 3–31.

288. M. Chateauneuf, A. C. H. Ling and D. R. Stinson. Slope packings and coverings, and generic algorithms for the discrete logarithm problem. *Journal of Combinatorial Designs* **11** (2003), 36–50.

289. C. Blundo, P. D'Arco, A. De Santis and D. R. Stinson. Contrast optimal threshold visual cryptography schemes. *SIAM Journal on Discrete Mathematics* **16** (2003), 224–261.

290. D. R. Stinson and R. Wei. Generalized cover-free families. *Discrete Mathematics* **279** (2004), 463–477.

291. W. Ogata, K. Kurosawa, D. R. Stinson and H. Saido. New combinatorial designs and their applications to authentication codes and secret sharing schemes. *Discrete Mathematics* **279** (2004), 383–405.

292. D. R. Stinson. Attack on a concast signature scheme. *Information Processing Letters* **91** (2004), 39–41.

293. D. Deng, D. R. Stinson and R. Wei. The Lovász local lemma and its applications to some combinatorial arrays. *Designs, Codes and Cryptography* **32** (2004), 121–134.

294. J. H. Dinitz and D. R. Stinson. On the maximum number of different ordered pairs of symbols in sets of latin squares. *Journal of Combinatorial Designs* **13** (2005), 1–15.

295. J. H. Dinitz, P. Dukes and D. R. Stinson. Sequentially perfect and uniform one-factorizations of the complete graph. *Electronic Journal of Combinatorics* **12** (2005), paper #R1, 12pp.

296. J. H. Dinitz and D. R. Stinson. On assigning referees to tournament schedules. *Bulletin of the ICA* **44** (2005), 22–28.

297. J. A. Muir and D. R. Stinson. Alternative digit sets for nonadjacent representations. *SIAM Journal on Discrete Mathematics* **19** (2005), 165–191.

298. K. A. Lauinger, D. L. Kreher, R. S. Rees and D. R. Stinson. Computing transverse t-designs. *Journal of Combinatorial Mathematics and Combinatorial Computing* **54** (2005), 33–56.

299. J. A. Muir and D. R. Stinson. Minimality and other properties of the width-w nonadjacent form. *Mathematics of Computation* **75** (2006), 369–384.

300. P. D'Arco, W. Kishimoto and D. R. Stinson. Properties and constraints of cheating-immune secret sharing schemes. *Discrete Applied Mathematics* **154** (2006), 219–233.

301. D. R. Stinson. Some observations on the theory of cryptographic hash functions. *Designs, Codes and Cryptography* **38** (2006), 259–277.

302. K. Khoo, G. Gong and D. Stinson. A new characterization of bent and semi-bent functions on finite fields. *Designs, Codes and Cryptography* **38** (2006), 279–295.

303. J. A. Muir and D. R. Stinson. On the low hamming weight discrete logarithm problem for non-adjacent representations. *Applicable Algebra in Engineering, Communication and Computing* **16** (2006), 461–472.

304. W. Ogata, K. Kurosawa and D. R. Stinson. Optimum secret sharing scheme secure against cheating. *SIAM Journal on Discrete Mathematics* **20** (2006), 79–95.

305. J. Lee and D. R. Stinson. Common intersection designs. *Journal of Combinatorial Designs* **14** (2006), 251–269.

306. J. H. Dinitz, A. Ling and D. R. Stinson. Fault tolerant routings with minimum optical index. *Networks* **48** (2006), 47–55.

307. D. Deng, D. R. Stinson, P. C. Li, G. H. J. van Rees and R. Wei. Constructions and bounds for splitting systems. *Discrete Mathematics* **307** (2007), 18–37.

308. B. Sunar, W. J. Martin and D. R. Stinson. A provably secure true random number generator with built-in tolerance to active attacks. *IEEE Transactions on Computers* **56** (2007), 109–119.

309. M. Nandi and D. R. Stinson. Multicollision attacks on some generalized sequential hash functions. *IEEE Transactions on Information Theory* **53** (2007), 759–767.

310. J. H. Dinitz, A. C. H. Ling and D. R. Stinson. Perfect hash families from transversal designs. *Australasian Journal of Combinatorics* **37** (2007), 233–242.

311. D. R. Stinson and R. Wei. Some results on query processes and reconstruction functions for unconditionally secure 2-server 1-round binary private information retrieval protocols. *Journal of Mathematical Cryptology* **1** (2007), 33–46.

312. D. R. Stinson. Unconditionally secure chaffing and winnowing with short authentication tags. *Advances in Mathematics of Communications* **1** (2007), 269–280.

313. D. R. Stinson and S. Zhang. Algorithms for detecting cheaters in threshold schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing* **61** (2007), 169–191.

314. C. Blundo, P. D'Arco, A. De Santis and D. R. Stinson. On unconditionally secure distributed oblivious transfer. *Journal of Cryptology* **20** (2007), 323–373.

315. D. R. Stinson and J. Wu. An efficient and secure two-flow zero-knowledge identification protocol. *Journal of Mathematical Cryptology* **1** (2007), 201–220.

316. A. Mashatan and D. R. Stinson. Noninteractive two-channel message authentication based on hybrid-collision resistant hash functions. *IET Information Security* **1** (2007), 111–118.

317. D. R. Stinson. Generalized mix functions and orthogonal equitable rectangles. *Designs, Codes and Cryptography* **45** (2007), 347–357.

318. D. R. Stinson, R. Wei and K. Chen. On generalized separating hash families. *Journal of Combinatorial Theory A* **115** (2008), 105–120.

319. J. Lee and D. R. Stinson. On the construction of practical key predistribution schemes for distributed sensor networks using combinatorial designs. *ACM Transactions on Information and System Security* **11-2** (2008), article No. 1, 35 pp.

320. D. R. Stinson and G. M. Zaverucha. Some improved bounds for secure frameproof codes and related separating hash families. *IEEE Transactions on Information Theory* **54** (2008), 2508–2514.

321. S. R. Blackburn, T. Etzion, D. R. Stinson and G. M. Zaverucha. A bound on the size of separating hash families. *Journal of Combinatorial Theory A* **115** (2008), 1246–1256.

322. M. B. Paterson and D. R. Stinson. Two attacks on a sensor network key distribution scheme of Cheng and Agrawal. *Journal of Mathematical Cryptology* **2** (2008), 393–403.

323. A. Mashatan and D. R. Stinson. Interactive two-channel message authentication based on interactive-collision resistant hash functions. *International Journal of Information Security* **8** (2009), 49–60.

324. M. B. Paterson, D. R. Stinson and R. Wei. Combinatorial batch codes. *Advances in Mathematics of Communications* **3** (2009), 13–27.

325. J. Sui and D. R. Stinson. A critical analysis and improvement of AACS drive-host authentication. *International Journal of Applied Cryptography* **1** (2009), 169–180.

326. H. Cao, J. Dinitz, D. Kreher, D. R. Stinson and R. Wei. On orthogonal generalized equitable rectangles. *Designs, Codes and Cryptography* **51** (2009), 225–230.

327. K. Henry, D. R. Stinson and J. Sui. The effectiveness of receipt-based attacks on ThreeBallot. *IEEE Transactions on Information Forensics and Security* **4** (2009), 699–707.

328. J. Wu and D. R. Stinson. An efficient identification protocol secure against concurrent-reset attacks. *Journal of Mathematical Cryptology* **3** (2009), 339–352.

329. A. Mashatan and D. R. Stinson. Practical unconditionally secure two-channel message authentication. *Designs, Codes and Cryptography* **55** (2010), 169–188.

330. M. B. Paterson and D. R. Stinson. Yet another hat game. *Electronic Journal of Combinatorics* **17(1)** (2010), paper #R86, 12 pp.

331. G. M. Zaverucha and D. R. Stinson. Anonymity in shared symmetric key primitives. *Designs, Codes and Cryptography* **57** (2010), 139–160.

332. K. M. Martin, M. B. Paterson and D. R. Stinson. Key predistribution for homogeneous wireless sensor networks with group deployment of nodes. *ACM Transactions on Sensor Networks* **7-2** (2010), article No. 11, 27 pp.

333. S. R. Blackburn, A. Panoui, M. B. Paterson and D. R. Stinson. Honeycomb arrays. *Electronic Journal of Combinatorics* **17(1)** (2010), paper #R172, 10 pp.

334. M. Nojoumian, D. R. Stinson and M. Grainger. An unconditionally secure social secret sharing scheme. *IET Information Security* **4** (2010), 202–211.

335. I. Goldberg, A. Mashatan and D. R. Stinson. On message recognition protocols: recoverability and explicit confirmation. *International Journal of Applied Cryptography* **2** (2010), 100–120.

336. K. M. Martin, M. B. Paterson and D. R. Stinson. Error decodable secret sharing and one-round perfectly secure message transmission for general adversary structures. *Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences* **3** (2011), 65–86.

337. S. R. Blackburn, M. B. Paterson and D. R. Stinson. Putting dots in triangles. *Journal of Combinatorial Mathematics and Combinatorial Computing* **78** (2011), 23–32.

338. G. M. Zaverucha and D. R. Stinson. Short one-time signatures. *Advances in Mathematics of Communications* **5** (2011), 473–488.

339. J. Wu and D. R. Stinson. Three improved algorithms for multipath key establishment in sensor networks using protocols for secure message transmission. *IEEE Transactions on Dependable and Secure Computing* **8** (2011), 929–937.

340. R. C.-W. Phan, J. Wu, K. Ouafi and D. R. Stinson. Privacy analysis of forward and backward untraceable RFID identification schemes. *Wireless Personal Communications* **61** (2011), 69–81.

341. J. H. Dinitz, P. R. J. Östergård and D. R. Stinson. Packing Costas arrays. *Journal of Combinatorial Mathematics and Combinatorial Computing* **80** (2012), 385–40.

342. S. R. Blackburn, D. R. Stinson and J. Upadhyay. On the complexity of the herding attack and some related attacks on hash functions. *Designs, Codes and Cryptography* **64** (2012), 171–193.

343. J. H. Dinitz, M. B. Paterson, D. R. Stinson and R. Wei. Constructions for retransmission permutation arrays. *Designs, Codes and Cryptography* **65** (2012), 325–351.

344. C. M. Swanson and D. R. Stinson. Extended combinatorial constructions for peer-to-peer user-private information retrieval. *Advances in Mathematics of Communications* **6** (2012), 479–497.

345. D. R. Stinson. Nonincident points and blocks in designs. *Discrete Mathematics* **313** (2013), 447–452.

346. M. Nojoumian and D. R. Stinson. On dealer-free dynamic threshold schemes. *Advances in Mathematics of Communications* **7** (2013), 39–56.

347. M. B. Paterson and D. R. Stinson. A simplified combinatorial treatment of constructions and threshold gaps of ramp schemes. *Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences* **5** (2013), 229–240.

348. M. B. Paterson, D. R. Stinson and J. Upadhyay. A coding theory foundation for the analysis of general unconditionally secure proof-of-retrievability schemes for cloud storage. *Journal of Mathematical Cryptology* **7** (2013), 183–216.

349. D. R. Stinson, C. Swanson and Tran van Trung. A new look at an old construction: constructing (simple) 3-designs from resolvable 2-designs. *Discrete Mathematics* **325** (2014), 23–31.

350. M. B. Paterson and D. R. Stinson. A unified approach to combinatorial key predistribution schemes for sensor networks. *Designs, Codes and Cryptography* **71** (2014), 433–457.

351. C. M. Swanson and D. R. Stinson. Combinatorial solutions providing improved security for the generalized Russian cards problem. *Designs, Codes and Cryptography* **72** (2014), 345–367.

352. D. R. Stinson and J. Upadhyay. Is extracting data the same as possessing data? *Journal of Mathematical Cryptology* **8** (2014), 189–207.

353. C. M. Swanson and D. R. Stinson. Additional constructions to solve the generalized Russian cards problem using combinatorial designs. *Electronic Journal of Combinatorics* **21** (2014), paper #P3.29, 31 pp.

354. M. Kendall, K. M. Martin, S.-L. Ng, M. B. Paterson and D. R. Stinson. Broadcast-enhanced key predistribution schemes. *ACM Transactions on Sensor Networks* **11** (2014), Article 6, 33 pp.

355. M. Nojoumian and D. R. Stinson. Sequential secret sharing as a new hierarchical access structure. *Journal of Internet Services and Information Security* **5** (2015), 24–32.

356. C. Swanson and D. R. Stinson. Extended results on privacy against coalitions of users in user-private information retrieval protocols. *Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences* **7** (2015), 415–437.

357. C. Guo, D. R. Stinson and Tran van Trung. On tight bounds for binary frameproof codes. *Designs, Codes and Cryptography* **77** (2015), 301–319 (Special Issue on Cryptography, Codes, Designs and Finite Fields: In Memory of Scott A. Vanstone).

358. M. B. Paterson and D. R. Stinson. Optimal constructions for ID-based one-way-function key predistribution schemes realizing specified communication graphs. *Journal of Mathematical Cryptology* **9** (2015), 215–225.

359. K. Henry and D. R. Stinson. Linear approaches to resilient aggregation in sensor networks. *Journal of Mathematical Cryptology* **9** (2015), 245–272.

360. C. M. Swanson and D. R. Stinson. Unconditionally secure signature schemes revisited. *Journal of Mathematical Cryptology* **10** (2016), 35–67.

361. M. B. Paterson, D. R. Stinson and Yongge Wang. On encoding symbol degrees of array BP-XOR codes. *Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences* **8** (2016), 19–32.

362. M. B. Paterson and D. R. Stinson. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. *Discrete Mathematics* **339** (2016), 2891–2906.

363. D. S. Archdeacon, J. H. Dinitz, A. Mattern and D. R. Stinson. On partial sums in cyclic groups. *Journal of Combinatorial Mathematics and Combinatorial Computing* **98** (2016), 327–342.

364. P. D'Arco, N. Nasr Esfahani and D. R. Stinson. All or nothing at all. *Electronic Journal of Combinatorics* **23(4)** (2016), paper #P4.10, 24 pp.

365. X. Ma, D. R. Stinson and R. Wei. An optimization problem for combinatorial key predistribution. *Journal of Combinatorial Mathematics and Combinatorial Computing* **99** (2016), 225–235.

366. C. Guo and D. R. Stinson. A tight bound on the size of certain separating hash families. *Australasian Journal of Combinatorics* **67** (2017), 294–303.

367. T. M. Laing, K. M. Martin, M. B. Paterson and D. R. Stinson. Localised multisecret sharing. *Cryptography and Communications – Discrete Structures, Boolean Functions and Sequences* **9** (2017), 581–597.

368. W. J. Martin and D. R. Stinson. Some nonexistence results for strong external difference families using character theory. *Bulletin of the ICA* **80** (2017), 79–92.

369. N. Nasr Esfahani and D. R. Stinson. Computational results on invertible matrices with the maximum number of invertible 2×2 submatrices. *Australasian Journal of Combinatorics* **69** (2017), 130–144.

370. D. R. Stinson. Ideal ramp schemes and related combinatorial objects. *Discrete Mathematics* **341** (2018), 299–307.

371. D. R. Stinson and R. Wei. Combinatorial repairability for threshold schemes. *Designs, Codes and Cryptography* **86** (2018), 195–210.

372. N. Nasr Esfahani, Ian Goldberg and D. R. Stinson. Some results on the existence of t-all-or-nothing transforms over arbitrary alphabets. *IEEE Transactions on Information Theory* **64** (2018), 3136–3143.

373. T. M. Laing and D. R. Stinson. A survey and refinement of repairable threshold schemes. *Journal of Mathematical Cryptology* **12** (2018), 57–81.

374. D. R. Stinson. A brief retrospective look at the Cayley-Purser public-key cryptosystem, 19 years later. *Bulletin of the ICA* **83** (2018), 84–97.

375. M. B. Paterson, D. R. Stinson and J. Upadhyay. Multi-prover proof-of-retrievability. *Journal of Mathematical Cryptology* **12** (2018), 203–220.

376. D. R. Stinson. Bounds for orthogonal arrays with repeated rows. *Bulletin of the ICA* **85** (2019), 60–73.

377. D. L. Kreher and D. R. Stinson. Nonsequenceable Steiner triple systems. *Bulletin of the ICA* **86** (2019), 64–68.

378. C. J. Colbourn, D. R. Stinson and S. Veitch. Constructions of optimal orthogonal arrays with repeated rows. *Discrete Mathematics* **342** (2019), 2455–2466. [This paper is an *Editors' Choice selection* for 2019.]

379. B. Kacsmar and D. R. Stinson. A network reliability approach to the analysis of combinatorial repairable threshold schemes. *Advances in Mathematics of Communications* **13** (2019), 601–612.

380. D. L. Kreher and D. R. Stinson. Block-avoiding sequencings of points in Steiner triple systems. *Australasian Journal of Combinatorics* **74** (2019), 498–509.

381. D. L. Kreher, D. R. Stinson and S. Veitch. Block-avoiding point sequencings of directed triple systems. *Discrete Mathematics* **343** (2020), article 111773, 10 pp.

382. D. L. Kreher, D. R. Stinson and S. Veitch. Block-avoiding point sequencings of Mendelsohn triple systems. *Discrete Mathematics* **343** (2020), article 111799, 7 pp.

383. D. R. Stinson and S. Veitch. Block-avoiding point sequencings of arbitrary length in Steiner triple systems. *Australasian Journal of Combinatorics* **77** (2020), 87–99.

384. W. J. Martin and D. R. Stinson. Some bounds arising from a polynomial ideal associated to any t-design. *Journal of Algebra, Combinatorics, Discrete Structures and Applications* **7** (2020), 161–181.

385. D. R. Stinson. Designing progressive dinner parties. *Bulletin of the ICA* **89** (2020), 93–101.

386. M. Buratti and D. R. Stinson. New results on modular Golomb rulers, optical orthogonal codes and related structures. *Ars Mathematica Contemporanea* **20** (2021), 1–27.

387. M. B. Paterson and D. R. Stinson. On the equivalence of authentication codes and robust $(2,2)$-threshold schemes. *Journal of Mathematical Cryptology* **15** (2021), 179–196.

388. D. R. Stinson. On partial parallel classes in partial Steiner triple systems. *Discrete Mathematics* **344** (2021), article 112279, 7 pp.

389. D. R. Stinson. A die problem. *Bulletin of the ICA* **92** (2021), 109–113.

390. N. Nasr Esfahani and D. R. Stinson. On security properties of all-or-nothing transforms. *Designs, Codes and Cryptography* **91** (2021), 2857–2867.

391. N. Nasr Esfahani and D. R. Stinson. Asymmetric all-or-nothing transforms. *Mathematical Cryptology* **1** (2021), 89–102.

392. M. J. Stinson and D. R. Stinson. An analysis and critique of the scoring method used for sport climbing at the 2020 Tokyo Olympics. *Bulletin of the ICA* **94** (2022), 13–34.

393. M. Buratti and D. R. Stinson. On resolvable Golomb rulers, symmetric configurations and progressive dinner parties. *Journal of Algebraic Combinatorics* **55** (2022), 141–156. [Special Issue in Honor of the 65th Birthday of Professor K. T. Arasu.]

394. D. R. Stinson and R. Wei. On maximum parallel classes in packings (in Chinese). *Scientia Sinica Mathematica* 53 (2023), 217–232. [English version can be found at `https://arxiv.org/abs/2202.06311`.]

395. D. R. Stinson. Some new results on skew frame starters in cyclic groups. *Discrete Mathematics* **346** (2023), article 113476, 10 pp.

396. D. R. Stinson. In the frame. *Bulletin of the ICA* **97** (2023), 60–89.

397. M. B. Paterson and D. R. Stinson. Splitting authentication codes with perfect secrecy: new results, constructions and connections with algebraic manipulation detection codes. *Advances in Mathematics of Communications* **17** (2023), 1364-1387.

398. N. Nasr Esfahani and D. R. Stinson. Rectangular, range and restricted AONTS: three generalizations of all-or-nothing transforms. *Advances in Mathematics of Communications* **18** (2024), 26–38.

399. S. R. Blackburn, N. Nasr Esfahani, D. L. Kreher and D. R. Stinson. Constructions and bounds for codes with restricted overlaps. To appear in *IEEE Transactions on Information Theory* (published online, August, 2023).

400. S. Veitch and D. R. Stinson. Unconditionally secure non-malleable secret sharing and circular external difference families. To appear in *Designs, Codes and Cryptography* (published online, November, 2023).

401. W. J. Martin and D. R. Stinson. Dispersed graph labellings. To appear in *Australasian Journal of Combinatorics*.

Submitted Papers and Papers in Preparation

J. Hall, D. Horsley and D. R. Stinson. Bounds on data limits for all-to-all comparison from combinatorial designs. Submitted for publication.

M. B. Paterson and D. R. Stinson. Circular external difference families, graceful labellings and cyclotomy. Submitted for publication.

D. L. Kreher and D. R. Stinson. On min-base palindromic representations of powers of 2. In preparation.

Other Publications and Technical Reports (Incomplete List)

D. R. Stinson. Recent results on resilient functions. *SAC '94 Workshop Record*, pp. 30–39.

D. R. Stinson. Visual Cryptography & Threshold Schemes. *Dr. Dobb's Journal*, Vol. 23, Issue 4, April 1998, pp. 36–43.

D. R. Stinson. Visual Cryptography & Threshold Schemes. *IEEE Potentials*, Vol. 18, No. 1, Feb./March 1999, pp. 13–16.

C. J. Colbourn, D. R. Stinson and G. H. J. van Rees. Preface: in honour of Ronald C. Mullin. *Designs, Codes and Cryptography* **26** (2002), 5–6.

M. J. Hinek and D. R. Stinson. An inequality about factors of multivariate polynomials. *CACR Technical Report 2006-15*, University of Waterloo.

D. R. Stinson and J. Wu. A zero-knowledge identification and key agreement protocol. *IACR ePrint 2007/116*.

J. Wu and D. R. Stinson. On the security of the ElGamal encryption scheme and Damgård's variant. *IACR ePrint 2008/200*.

D. R. Stinson. Comments on a sensor network key redistribution technique of Cichon, Golebiewski and Kutylowski. *IACR ePrint 2011/259*.

I. Blake, A. Menezes and D. Stinson. Guest editorial: special issue in honor of Scott A. Vanstone. *Designs, Codes and Cryptography* **77** (2015), 287–299 (Special Issue on Cryptography, Codes, Designs and Finite Fields: In Memory of Scott A. Vanstone).

N. Nasr Esfahani and D. R. Stinson. A list of close to AONT matrices found by computer search. *CACR Technical Report 2016-8*, University of Waterloo.

D. L. Kreher, D. R. Stinson and S. Veitch. Good sequencings for small directed triple systems. `https://arxiv.org/abs/1907.11186`

D. L. Kreher, D. R. Stinson and S. Veitch. Good sequencings for small Mendelsohn triple systems. `https://arxiv.org/abs/1909.06475`

D. R. Stinson. Ralph Stanton—a brief remembrance. *Bulletin of the ICA* **99** (2023), 16–18.

Software distribution

D. L. Kreher and D. R. Stinson. The CTAN `macros/latex/contrib/pseudocode/` directory, Comprehensive TeX Archive Network, January 14, 2005.