

Curriculum Vitae

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

May 1, 2012

Personal information

date of birth June 2, 1956
place of birth Guelph, Ontario, Canada
citizenship Canadian
marital status Married, two children

Contact information

telephone (519)-888-4567, ext. 35590
fax (519)-885-1208
email dstinson@uwaterloo.ca
web page www.math.uwaterloo.ca/~dstinson/

Experience

Degrees held

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 positions

Research assistant, University of Waterloo, 1974–1978.

Teaching assistant, Ohio State University, 1978–1980.

Part-time lecturer, University of Waterloo, 1980–1981.

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.

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

Full professor, University of Waterloo, School of Computer Science, July 1, 2002–.

University Research Chair, University of Waterloo, 2005–2011.

Secondary appointments

Associate, Center for Communication and Information Science, University of Nebraska, 1990–1996.

Adjunct professor, University of Manitoba, Department of Computer Science, 1992–1998.

Visiting professor, University of Manitoba, Department of Computer Science, 1996–1997.

Full professor, University of Waterloo, Department of Computer Science (cross appointment), 2000–2002.

Full professor, University of Waterloo, Department of Combinatorics and Optimization (cross appointment), 2002–2010.

Adjunct professor, Michigan Technological University, Graduate Faculty, 2003.

Teaching and student supervision

Courses taught (since 1998)

Spring 2012	Unconditionally Secure Cryptography (CS 858) Computer Security and Privacy (CS 458/658)
Fall 2011	Data Structures and Data Management (CS 240)
Fall 2010	Cryptography / Network Security (CS 758) Computer Security and Privacy (CS 458/658)
Winter 2010	Unconditionally Secure Cryptography (CS 858) Computer Security and Privacy (CS 458/658)
Fall 2008	Data Structures and Data Management (CS 240), two sections
Spring 2008	Unconditionally Secure Cryptography (CS 858)
Winter 2007	Cryptography / Network Security (CS 758)
Winter 2006	Algorithms (CS 341), two sections
Fall 2005	Cryptography / Network Security (CS 758)
Fall 2004	Data Structures and Data Management (CS 240)
Winter 2004	Algorithms (CS 341)
Fall 2003	Cryptography / Network Security (CS 758) Algorithms (CS 341)
Fall 2002	Cryptography / Network Security (CS 758)
Winter 2002	Combinatorial Designs (C&O 434/634)
Fall 2001	Mathematics of Public-Key Cryptography (C&O 485/685)
Fall 2000	Mathematics of Public-Key Cryptography (C&O 685)
Fall 1999	Combinatorial Designs (C&O 434/634)
Fall 1998	Combinatorial Cryptography (C&O 739W)

Post-doctoral fellows supervised

Guang Gong, 1998, University of Waterloo.
Ruizhong Wei, 1998–2000, University of Waterloo.
Yongge Wang, 1999–2000, University of Waterloo.
Palash Sarkar, 2000–2001, University of Waterloo.
Mark Chateaufneuf, 2000–2001, University of Waterloo.
Paolo D’Arco, 2001–2002, University of Waterloo.
Dameng Deng, 2003–2004, University of Waterloo.
Mridul Nandi, 2006–2007, University of Waterloo.
Maura Paterson, 2008, visiting Post-Doc from Royal Holloway.

PhD students supervised

Eric Seah, PhD, 1987 (CS, University of Manitoba).
Thesis title: *On the enumeration of one-factorizations and Howell designs using orderly algorithms.*

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.*

K. Gopalakrishnan, PhD, 1994 (CSE, University of Nebraska).
Thesis title: *A study of correlation-immune, resilient and related cryptographic functions.*

Mustafa Atici, PhD, 1996, (CSE, University of Nebraska).
Thesis title: *Hash functions: recursive constructions and applications to cryptography.*

Ruizhong Wei, PhD, 1998, (Math, University of Nebraska).
Thesis title: *Traceability schemes, frameproof codes, key distribution patterns and related topics – a combinatorial approach.*

Khoongming Khoo, PhD, 2004 (C&O, University of Waterloo, co-supervised with G. Gong).
Thesis title: *Sequence design and construction of cryptographic boolean functions.*

James Muir, PhD, 2005 (C&O, University of Waterloo).
Thesis title: *Efficient integer representations for cryptographic operations.*

Jooyoung Lee, PhD, 2005 (C&O, University of Waterloo).
Thesis title: *Combinatorial approaches to key predistribution for distributed sensor networks.*

Jason Hinek, PhD, 2007 (SCS, University of Waterloo, co-supervised with M. Giesbrecht).
Thesis title: *On the security of some variants of RSA.*

Atefeh Mashatan, PhD, 2009 (C&O, University of Waterloo).
Thesis title: *Message authentication and recognition protocols using two-channel cryptography.*

Jiang Wu, PhD, 2009 (SCS, University of Waterloo).
Thesis title: *Cryptographic protocols, sensor network key management, and RFID authentication.*

Greg Zaverucha, PhD, 2011 (SCS, University of Waterloo).
Thesis title: *Hash families and cover-free families with cryptographic applications.*

Mehrdad Nojournian, SCS, PhD student, September 2008–.

Kevin Henry, SCS, PhD student, September 2008–.

Colleen Swanson, SCS, PhD student, January 2009–.

Jalaj Upadhyay, SCS, PhD student, September 2010–.

Masters students supervised

- Wendy White, MSc, 1990 (CS, University of Manitoba).
Thesis title: *The construction and implementation of authentication and secrecy codes.*
- Mustafa Atici, MSc, 1994 (CSE, University of Nebraska).
Thesis title: *Optimal information and average information rates of the connected graphs on six vertices.*
- Sharon Lim, MSc, 1996 (CSE, University of Nebraska).
Thesis title: *A “C” implementation of two classes of authentication codes.*
- Phil Eisen, MMath, 1999 (C&O, University of Waterloo).
Thesis title: *Threshold visual cryptography schemes.*
- Jason Chen, MMath, 2000 (C&O, University of Waterloo).
Thesis title: *A survey on traitor tracing schemes.*
- James Muir, MMath, 2001 (C&O, University of Waterloo).
Thesis title: *Techniques of side channel cryptanalysis.*
- Kyung-Mi Kim, MMath, 2003 (C&O, University of Waterloo).
Thesis title: *Perfect hash families: constructions and applications.*
- 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.*
- Kar-Yee Au, MMath, 2005 (SCS, University of Waterloo).
Thesis title: *Unconditionally secure authentication codes and digital signatures.*
- Sheng Zhang, MMath, 2005 (SCS, University of Waterloo).
Thesis title: *Algorithms for detecting cheaters in threshold schemes.*
- Jiayuan Sui, MMath, 2008 (SCS, University of Waterloo).
Thesis title: *A security analysis of some physical content distribution systems.*
- Kevin Henry, MMath, 2008 (SCS, University of Waterloo).
Thesis title: *The theory and applications of homomorphic cryptography.*
- Jalaj Upadhyay, MMath, 2011 (SCS, University of Waterloo).
Thesis title: *Generic attacks on hash functions.*

Service

University committees and administrative duties (since 2002)

- | | |
|-----------|--|
| 2011–2012 | Designated Chairs’ Pool (PhD Thesis Examinations) (UW)
Graduate Committee (SCS)
Awards Committee (SCS)
Managing board of the <i>Centre for Applied Cryptographic Research</i> |
| 2010–2011 | Tenure and Promotion Committee (SCS)
Managing board of the <i>Centre for Applied Cryptographic Research</i> |
| 2009–2010 | Graduate Recruiting Committee (SCS)
Outreach Committee (SCS)
Tenure and Promotion Committee (SCS)
Managing board of the <i>Centre for Applied Cryptographic Research</i> |
| 2008–2009 | Graduate Committee (SCS)
Commons Committee (SCS)
Mathematics Faculty Representative Council
Managing board of the <i>Centre for Applied Cryptographic Research</i> |

2007–2008	Director of Graduate Studies (SCS) Chair of Graduate Committee (SCS) Graduate Recruiting Committee (SCS) Tenure and Promotion Committee (SCS) Chair of Scholarship committee, NSERC rankings (SCS) Chair of Scholarship committee, OGS rankings (SCS) Chair of Cheriton Scholarship committee (SCS) Mathematics Faculty Representative Council Managing board of the <i>Centre for Applied Cryptographic Research</i>
2006–2007	Director of Graduate Studies (SCS) Chair of Graduate committee (SCS) Graduate Recruiting Committee (SCS) Chair of Scholarship committee, NSERC rankings (SCS) Chair of Scholarship committee, OGS rankings (SCS) Chair of Cheriton Scholarship committee (SCS) Mathematics Faculty Representative Council Managing board of the <i>Centre for Applied Cryptographic Research</i>
2005–2006	Mathematics Faculty Representative Council Managing board of the <i>Centre for Applied Cryptographic Research</i> Graduate committee (SCS) School Advisory Committee on Appointments (SCS) Scholarship committee, NSERC rankings (SCS)
2004–2005	Managing board of the <i>Centre for Applied Cryptographic Research</i> Graduate committee (SCS) Promotion and tenure committee (SCS) Scholarship committee, NSERC rankings (SCS)
2003–2004	Managing board of the <i>Centre for Applied Cryptographic Research</i> Graduate committee (SCS) Promotion and tenure committee (SCS) Scholarship committee, NSERC rankings (SCS)
2002–2003	Managing board of the <i>Centre for Applied Cryptographic Research</i> Graduate committee (SCS) Scholarship committee, NSERC rankings (SCS)

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.*

Editorial services

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

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 Professor Ron Mullin, 2002.

Member of editorial board of *Journal of Combinatorial Designs*, 2003–.

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

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

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

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

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

Associate editor of *Discrete Mathematics*, 2007–.

Conference organization

Co-organizer, *Sixth Midwestern Conference on Combinatorics, Cryptography and Computing*, University of Nebraska, Oct. 31–Nov. 1, 1991.

Co-organizer, *Ninth Midwestern Conference on Combinatorics, Cryptography and Computing*, University of Nebraska, Oct. 20–22, 1994.

Co-organizer, *Transversal Designs and Orthogonal Arrays Workshop*, Kitchener, April 21–26, 1997.

Co-organizer, *First Lincoln Workshop in Cryptology & Coding Theory*, University of Nebraska, June 1–4, 1997.

Member of organizing committee, *Canadian Mathematics Society 1999 Summer Meeting*, St. John's.

Co-chair, *Selected Areas in Cryptography 2000 (SAC '00)*, University of Waterloo.

Member of organizing committee, *Canadian Mathematics Society 2002 Summer Meeting*, Quebec City.

Member of organizing committee, *Eleventh SIAM Conference on Discrete Mathematics*, San Diego, 2002.

Member of organizing committee, *Canadian Mathematics Society 2003 Winter Meeting*, Vancouver. [Organizer of *Short Course in Cryptography*.]

Minisymposium organizer, *SIAM Conference on Discrete Mathematics*, Victoria, Canada, 2006.

Minisymposium organizer, *SIAM Conference on Discrete Mathematics*, Burlington, U.S.A., 2008.
Member of steering committee for *Security and Cryptography in Networks*, 2006–.
Member of steering committee for *International Conference on Information Theoretic Security*, 2007–.
Member of *Selected Areas in Cryptography* workshop organizing committee, 1999– (chair, 2002–2006).
Co-chair, *Selected Areas in Cryptography 2010 (SAC '10)*, University of Waterloo.
Member of the scientific committee of the theme *Network Security and Cryptography* for the MITACS Focus Period *Advances in Network Analysis and its Applications*, June 2010.

Program committee membership

CRYPTO '90, University of California Santa Barbara.
CRYPTO '93, University of California Santa Barbara (program chair).
EUROCRYPT '95, St. Malo, France.
CRYPTO '97, University of California Santa Barbara.
Selected Areas in Cryptography '98 (SAC '98), Queen's University, Kingston.
Public Key Solutions 1999 (PKS '99), Toronto, April 1999 (program chair).
Selected Areas in Cryptography '99 (SAC '99), Queen's University, Kingston.
Security in Communications Networks '99 (SCN '99), Amalfi.
CRYPTO 2000, University of California Santa Barbara.
Selected Areas in Cryptography 2001 (SAC '01), Fields Institute, Toronto.
CRYPTO 2001, University of California Santa Barbara.
Selected Areas in Cryptography 2002 (SAC '02), St. John's.
Third Conference on Security in Communication Networks (SCN '02), Amalfi, 2002.
EUROCRYPT 2003, Warsaw.
Selected Areas in Cryptography 2003 (SAC '03), Ottawa.
9th Australasian Conference on Information Security and Privacy (ACISP '04), Sydney, Australia.
Selected Areas in Cryptography 2004 (SAC '04), Waterloo.
Fourth Conference on Security in Communication Networks (SCN '04), Amalfi, Italy, 2004.
International Workshop on Coding and Cryptography (WCC '05), Bergen, Norway.
EUROCRYPT 2005, Aarhus, Denmark.
Selected Areas in Cryptography (SAC '05), Kingston.
ASIACRYPT 2005, Chennai, India.
11th Australasian Conference on Information Security and Privacy (ACISP '06), Melbourne, Australia.
Selected Areas in Cryptography (SAC '06), Montreal.
RSA Conference, Cryptographers' Track (CT-RSA 2007), San Francisco.
1st Canadian Discrete and Algorithmic Mathematics Conference (CanaDAM 2007), Banff.
International Conference on Information Theoretic Security (ICITS 2007), Madrid.
Selected Areas in Cryptography (SAC '07), Ottawa.

13th Australasian Conference on Information Security and Privacy (ACISP '08), Wollongong, Australia.

Central European Conference on Cryptography (CECC '08), Graz, Austria.

Selected Areas in Cryptography (SAC '08), Sackville, NB.

Cryptology, Designs and Finite Groups (CDFG 2009), Deerfield Beach, FL, 2009.

14th Australasian Conference on Information Security and Privacy (ACISP '09), Brisbane, Australia.

Selected Areas in Cryptography (SAC '09), Calgary, AB.

International Conference on Information Theoretic Security (ICITS 2009), Shizuoka, Japan.

Thirteenth Information Security Conference (ISC 2010), Boca Raton, Florida.

Ninth International Conference on Cryptology And Network Security (CANS 2010), Kuala Lumpur, Malaysia.

EUROCRYPT 2011, Tallinn, Estonia.

4th Canada-France MITACS Workshop on Foundations & Practice of Security, May, 2011, Paris.

16th Australasian Conference on Information Security and Privacy (ACISP '11), Melbourne, Australia.

Selected Areas in Cryptography (SAC 2011), Toronto.

17th Australasian Conference on Information Security and Privacy (ACISP '12), Wollongong, Australia.

Sequences and their Applications (SETA 2012), Waterloo.

Other professional activities

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

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 scientific committee for the *Centre de Recherches Mathématiques*, 1996–1997.

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

Member of the *Canadian Mathematics Society Doctoral Prize Committee*, 2000–2001.

Member of the *IEEE Information Theory Society Awards Committee*, 2002.

Member of the *MTU Combinatorics Research Institute Advisory Board*, Michigan Technological University, Houghton, MI, 2002–.

Member of the *Canada Research Chairs College of Reviewers*, 2002.

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

Member of the *Center for Information Security and Cryptography Technical Advisory Panel*, University of Calgary, 2005–.

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

Awards and recognition

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 invited 50-minute lectures.

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).

Awards

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.

Marshall Hall Medal, awarded by the Institute of Combinatorics and Its Applications, 1994.

Visiting Professional Associate Award, University of Manitoba, 1996.

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

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

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

Elected and inducted as a *Fellow of the Royal Society of Canada*, 2011.

Research

Research interests

Cryptography: authentication codes, pseudorandom number generation, key distribution schemes, traceability, public-key cryptosystems, signature schemes, hash functions, provable security.

Networks and distributed systems: distributed cryptographic protocols, multicast security, broadcast encryption, secret-sharing schemes, quorum systems.

Algorithms and computational complexity: combinatorial algorithms, randomized algorithms, parallel algorithms.

Construction of combinatorial structures with applications in computer science and cryptography: universal hashing, resilient functions, correlation-immune functions, cover-free families, perfect hash families, extractors and dispersers.

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.

Publications

Books

- [B1] D. R. STINSON. *An Introduction to the Design and Analysis of Algorithms*. Charles Babbage Research Centre, Winnipeg, Manitoba, 1985 (second edition, 1987), 213 pp.
- [B2] J. H. DINITZ AND D. R. STINSON (EDS.) *Contemporary Design Theory: A Collection of Surveys*. John Wiley & Sons, New York, 1992, 639 pp.
- [B3] D. R. STINSON (ED.) *Advances in Cryptology – CRYPTO '93 Proceedings*. Lecture Notes in Computer Science, vol. 773. Springer-Verlag, Berlin, 1994, 492 pp.
- [B4] D. R. STINSON. *Cryptography: Theory and Practice*. CRC Press, Inc., Boca Raton, 1995, 434 pp. [*Cryptographie: Theorie et Pratique*, French translation by Serge Vaudenay, International Thomson Publishing, Paris, 1996. Japanese translation by Kouichi Sakurai, 1996. Polish translation, 2005.]
- [B5] D. L. KREHER AND D. R. STINSON. *Combinatorial Algorithms: Generation, Enumeration & Search*. CRC Press, Inc., Boca Raton, 1999, 329 pp.
- [B6] 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.
- [B7] D. R. STINSON. *Cryptography: Theory and Practice, Second Edition*. Chapman & Hall/CRC, Boca Raton, 2002, 339 pp. [*Cryptographie: Theorie et Pratique, 2e Edition*, French translation by Serge Vaudenay, Gildas Avoine and Pascal Junod. Vuibert, Paris, 2003.]
- [B8] D. R. STINSON. *Combinatorial Designs: Constructions and Analysis*. Springer-Verlag, New York, 2004, 316 pp.
- [B9] D. R. STINSON. *Cryptography: Theory and Practice, Third Edition*. Chapman & Hall/CRC, Boca Raton, 2006, 616 pp.
- [B10] 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.

Papers in conference proceedings

- [C1] 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).
- [C2] 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).
- [C3] D. R. STINSON. A generalization of Howell designs. *Congressus Numerantium* **33** (1981), 321–328 (Twelfth Southeastern Conference on Combinatorics, Graph Theory and Computing, 1981).
- [C4] D. R. STINSON. Determination of a covering number. *Congressus Numerantium* **34** (1982), 429–440 (Eleventh Manitoba Conference on Numerical Mathematics and Computing, 1981).

- [C5] 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).
- [C6] D. R. STINSON. Room squares and subsquares. *Lecture Notes in Mathematics* **1036** (1983), 86–95 (Combinatorial Mathematics X, Adelaide, 1982).
- [C7] 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).
- [C8] 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).
- [C9] D. R. STINSON. Some constructions and bounds for authentication codes. *Lecture Notes in Computer Science* **263** (1987), 418–425 (Advances in Cryptology – CRYPTO '86). [This is a preliminary version of paper [J78].]
- [C10] 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). [This is a preliminary version of paper [J81].]
- [C11] 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).
- [C12] D. R. STINSON. A construction for authentication/secret codes from certain combinatorial designs. *Lecture Notes in Computer Science* **293** (1988), 355–366 (Advances in Cryptology – CRYPTO '87). [This is a preliminary version of paper [J85].]
- [C13] 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).
- [C14] 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). [This is a preliminary version of paper [J105].]
- [C15] 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).
- [C16] 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). [This is a preliminary version of paper [J120].]
- [C17] D. R. STINSON. Combinatorial characterizations of authentication codes. *Lecture Notes in Computer Science* **576** (1992), 62–73 (Advances in Cryptology – CRYPTO '91). [This is a preliminary version of paper [J124].]
- [C18] D. R. STINSON. Universal hashing and authentication codes. *Lecture Notes in Computer Science* **576** (1992), 74–85 (Advances in Cryptology – CRYPTO '91). [This is a preliminary version of paper [J134].]
- [C19] 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).
- [C20] 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). [This is a preliminary version of paper [J136].]
- [C21] 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).

- [C22] 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). [This is a preliminary version of paper [J141].]
- [C23] 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). [This is a preliminary version of paper [J147].]
- [C24] 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). [This is a preliminary version of paper [J145].]
- [C25] 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).
- [C26] 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). [This is a preliminary version of paper [J153].]
- [C27] 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).
- [C28] 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). [This is a preliminary version of paper [J173].]
- [C29] 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).
- [C30] 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).
- [C31] 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).
- [C32] 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).
- [C33] 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).
- [C34] 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).
- [C35] P. SARKAR AND D. R. STINSON. Frameproof and IPP codes. *Lecture Notes in Computer Science* **2247** (2001), 117–126 (INDOCRYPT 2001).
- [C36] 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).
- [C37] K. KHOO, G. GONG AND D. STINSON. A new family of Gold-like sequences (abstract). *Proceedings of the IEEE International Symposium on Information Theory*, 2002, p. 181.
- [C38] 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).

- [C39] 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). [This is a preliminary version of paper [J207].]
- [C40] 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).
- [C41] 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).
- [C42] 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).
- [C43] 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).
- [C44] 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. [Invited paper.]
- [C45] J. LEE AND D. R. STINSON. Tree-based key distribution patterns. *Lecture Notes in Computer Science* **3897** (2006), 189-204 (SAC 2005 Proceedings).
- [C46] 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).
- [C47] 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.
- [C48] 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).
- [C49] 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).
- [C50] J. WU AND D. R. STINSON. Authorship proof for textual document. *Lecture Notes in Computer Science* **5284** (2008), 209-223 (Information Hiding 2008).
- [C51] 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).
- [C52] 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).
- [C53] 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.
- [C54] 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).
- [C55] 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).
- [C56] G. M. ZAVERUCHA AND D. R. STINSON. Group testing and batch verification. *Lecture Notes in Computer Science* **5973** (2010), 140-157 (ICITS 2009).

- [C57] M. NOJOURMIAN 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.
- [C58] M. NOJOURMIAN 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).
- [C59] 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.
- [C60] C. SWANSON AND D. R. STINSON. Unconditionally secure signature schemes revisited. *Lecture Notes in Computer Science* **6673** (2011), 100–116 (ICITS 2011). Extended version: IACR ePrint 2011/104, <http://eprint.iacr.org/2011/104>.

Book chapters

- [BC1] 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).
- [BC2] 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).
- [BC3] 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).
- [BC4] 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).
- [BC5] 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).
- [BC6] 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). [Special volume in honour of Alex Rosa.]
- [BC7] 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). [Special volume in honour of Alex Rosa.]
- [BC8] 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).
- [BC9] 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).
- [BC10] 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.
- [BC11] 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.
- [BC12] J. H. DINITZ AND D. R. STINSON. A few more Room frames. In “Graphs, Matrices and Designs”, Marcel Dekker, Inc., 1993, pp. 133–146. [Festschrift in honour of Norman Pullman.]

- [BC13] 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).
- [BC14] D. R. STINSON. Coverings. In “The CRC Handbook of Combinatorial Designs”, CRC Press, Inc., 1996, pp. 260–265.
- [BC15] D. R. STINSON. Packings. In “The CRC Handbook of Combinatorial Designs”, CRC Press, Inc., 1996, pp. 409–413.
- [BC16] 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.
- [BC17] K. GOPALAKRISHNAN AND D. R. STINSON. Derandomization. In “The CRC Handbook of Combinatorial Designs”, CRC Press, Inc., 1996, pp. 558–560.
- [BC18] 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).
- [BC19] 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). [Special volume in honour of Dijen Ray-Chaudhuri.]
- [BC20] 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*).
- [BC21] D. R. STINSON. Bent functions. In “Handbook of Combinatorial Designs, Second Edition”, CRC Press, Inc., 2006, pp. 337–339.
- [BC22] 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. [This is an updated version of [BC16, §3.4].]
- [BC23] D. M. GORDON AND D. R. STINSON. Coverings. In “Handbook of Combinatorial Designs, Second Edition”, CRC Press, Inc., 2007, pp. 365–373. [This is an updated version of [BC14].]
- [BC24] K. GOPALAKRISHNAN AND D. R. STINSON. Derandomization. In “Handbook of Combinatorial Designs, Second Edition”, CRC Press, Inc., 2007, pp. 389–391. [This is an updated version of [BC17].]
- [BC25] D. R. STINSON, R. WEI AND J. YIN. Packings. In “Handbook of Combinatorial Designs, Second Edition”, CRC Press, Inc., 2007, pp. 550–556. [This is an updated version of [BC15].]
- [BC26] K. GOPALAKRISHNAN AND D. R. STINSON. Secrecy and authentication codes. In “Handbook of Combinatorial Designs, Second Edition”, CRC Press, Inc., 2007, pp. 606–611. [This is an updated version of [BC16, §3.1, 3.2].]
- [BC27] K. GOPALAKRISHNAN AND D. R. STINSON. Threshold and ramp schemes. In “Handbook of Combinatorial Designs, Second Edition”, CRC Press, Inc., 2007, pp. 635–639. [This is an updated version of [BC16, §3.3].]

Journal papers

- [J1] D. R. STINSON. Determination of a packing number. *Ars Combinatoria* **3** (1977), 89–114.
- [J2] D. R. STINSON. A note on the existence of 7 and 8 mutually orthogonal Latin squares. *Ars Combinatoria* **6** (1978), 113–115.
- [J3] R. C. MULLIN, D. R. STINSON, AND W. D. WALLIS. Concerning the spectrum of skew Room squares. *Ars Combinatoria* **6** (1978), 277–291.

- [J4] D. R. STINSON. The existence of 30 mutually orthogonal Latin squares. *Ars Combinatoria* **7** (1979), 153–170.
- [J5] D. R. STINSON. The distance between units in rings – an algorithmic approach. *Utilitas Mathematica* **15** (1979), 281–292.
- [J6] D. R. STINSON. A generalization of Wilson’s construction for mutually orthogonal Latin squares. *Ars Combinatoria* **8** (1979), 95–105.
- [J7] J. H. DINITZ AND D. R. STINSON. Boss block designs. *Ars Combinatoria* **9** (1980), 59–68.
- [J8] 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.
- [J9] J. H. DINITZ AND D. R. STINSON. A note on Howell designs of odd side. *Utilitas Mathematica* **18** (1980), 207–216.
- [J10] D. R. STINSON. A skew Room square of order 129. *Discrete Mathematics* **31** (1980), 333–335.
- [J11] J. H. DINITZ AND D. R. STINSON. The construction and uses of frames. *Ars Combinatoria* **10** (1980), 31–54.
- [J12] B. A. ANDERSON, R. C. MULLIN, AND D. R. STINSON. More skew Room squares. *Utilitas Mathematica* **18** (1980), 201–205.
- [J13] D. R. STINSON. A general construction for group-divisible designs. *Discrete Mathematics* **33** (1981), 89–94.
- [J14] 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.
- [J15] J. H. DINITZ AND D. R. STINSON. The spectrum of Room cubes. *European Journal of Combinatorics* **2** (1981), 221–230.
- [J16] J. H. DINITZ AND D. R. STINSON. Further results on frames. *Ars Combinatoria* **11** (1981), 275–288.
- [J17] D. R. STINSON. Some results concerning frames, Room squares, and subsquares. *Journal of the Australian Mathematical Society A* **31** (1981), 376–384.
- [J18] 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.
- [J19] A. HARTMAN AND D. R. STINSON. A note on one-factorizations. *Utilitas Mathematica* **20** (1981), 155–162.
- [J20] D. R. STINSON. The spectrum of skew Room squares. *Journal of the Australian Mathematical Society A* **31** (1981), 475–480.
- [J21] D. R. STINSON. The non-existence of a $(2, 4)$ –frame. *Ars Combinatoria* **11** (1981), 99–106.
- [J22] D. R. STINSON. Some constructions for frames, Room squares, and subsquares. *Ars Combinatoria* **12** (1981), 229–267.
- [J23] 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.
- [J24] R. C. MULLIN, D. R. STINSON, AND S. A. VANSTONE. Kirkman triple systems containing maximum subdesigns. *Utilitas Mathematica* **21C** (1982), 283–300.
- [J25] D. R. STINSON. The existence of Howell designs of odd side. *Journal of Combinatorial Theory A* **32** (1982), 53–65.
- [J26] 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.
- [J27] D. R. STINSON. Applications and generalizations of the variance method in combinatorial designs. *Utilitas Mathematica* **22** (1982), 323–333.

- [J28] D. R. STINSON. A short proof of a theorem of de Witte. *Ars Combinatoria* **14** (1982), 79–86.
- [J29] J. H. DINITZ AND D. R. STINSON. MOLS with holes. *Discrete Mathematics* **44** (1983), 145–154.
- [J30] D. R. STINSON. The non-existence of certain finite linear spaces. *Geometriae Dedicata* **13** (1983), 429–434.
- [J31] P. ERDÖS, R. C. MULLIN, V. SÓS, AND D. R. STINSON. Finite linear spaces and projective planes. *Discrete Mathematics* **47** (1983), 49–62.
- [J32] D. R. STINSON AND W. D. WALLIS. Snappy constructions for triple systems. *Gazette of the Australian Mathematical Society* **10** (1983), 84–88.
- [J33] D. R. STINSON AND W. D. WALLIS. Twofold triple systems without repeated blocks. *Discrete Mathematics* **47** (1983), 125–128.
- [J34] J. H. DINITZ AND D. R. STINSON. On non-isomorphic Room squares. *Proceedings of the American Mathematical Society* **89** (1983), 175–181.
- [J35] 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.
- [J36] 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.
- [J37] 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.
- [J38] D. R. STINSON. A comparison of two invariants for Steiner triple systems: fragments and trains. *Ars Combinatoria* **16** (1983), 69–76.
- [J39] 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.
- [J40] 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.
- [J41] D. R. STINSON AND G. H. J. VAN REES. Some improved results concerning the Cordes problem. *Ars Combinatoria* **17** (1984), 117–128.
- [J42] D. R. STINSON. Pair-packings and projective planes. *Journal of Australian Mathematical Society A* **37** (1984), 27–38.
- [J43] D. R. STINSON AND W. D. WALLIS. An even side analogue of Room squares. *Aequationes Mathematicae* **27** (1984), 201–213.
- [J44] E. BILLINGTON, R. G. STANTON, AND D. R. STINSON. On λ -packings with block-size four ($v \not\equiv 0 \pmod{3}$). *Ars Combinatoria* **17A** (1984), 73–84.
- [J45] R. C. MULLIN AND D. R. STINSON. Holey SOLSSOMs. *Utilitas Mathematica* **25** (1984), 159–169.
- [J46] D. R. STINSON AND G. H. J. VAN REES. The equivalence of certain equidistant binary codes and symmetric BIBDs. *Combinatorica* **4** (1984), 357–362.
- [J47] C. C. LINDNER AND D. R. STINSON. Steiner pentagon systems. *Discrete Mathematics* **52** (1984), 67–74.
- [J48] C. C. LINDNER AND D. R. STINSON. The spectrum for the conjugate invariant subgroups of perpendicular arrays. *Ars Combinatoria* **18** (1984), 51–60.
- [J49] D. R. STINSON. On scheduling perfect competitions. *Ars Combinatoria* **18** (1984), 45–49.
- [J50] 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.
- [J51] D. R. STINSON AND H. FERCH. 2000000 Steiner triple systems of order 19. *Mathematics of Computation* **44** (1985), 533–535.

- [J52] D. R. STINSON AND L. ZHU. On sets of three MOLS with holes. *Discrete Mathematics* **54** (1985), 321–328.
- [J53] D. R. STINSON AND S. A. VANSTONE. Some non-isomorphic Kirkman triple systems of orders 39 and 51. *Utilitas Mathematica* **27** (1985), 199–205.
- [J54] D. R. STINSON AND S. A. VANSTONE. A Kirkman square of order 51 and block-size 3. *Discrete Mathematics* **55** (1985), 107–111.
- [J55] D. S. ARCHDEACON, J. H. DINITZ, AND D. R. STINSON. V -squares. *Ars Combinatoria* **19** (1985), 161–174.
- [J56] D. R. STINSON. Isomorphism testing of Steiner triple systems: canonical forms. *Ars Combinatoria* **19** (1985), 213–218.
- [J57] D. R. STINSON. The spectrum of nested Steiner triple systems. *Graphs and Combinatorics* **1** (1985), 189–191.
- [J58] W. L. KOCAY, D. R. STINSON, AND S. A. VANSTONE. On strong starters in cyclic groups. *Discrete Mathematics* **56** (1985), 45–60.
- [J59] D. R. STINSON AND S. A. VANSTONE. A few more balanced Room squares. *Journal of the Australian Mathematical Society A* **39** (1985), 344–352.
- [J60] D. R. STINSON. Room squares with maximum empty subarrays. *Ars Combinatoria* **20** (1985), 159–166.
- [J61] 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.
- [J62] A. ROSA AND D. R. STINSON. One-factorizations of regular graphs and Howell designs of small order. *Utilitas Mathematica* **29** (1986), 99–124.
- [J63] 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.
- [J64] 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.
- [J65] D. R. STINSON. Concerning the spectrum of perpendicular arrays of triple systems. *Discrete Mathematics* **61** (1986), 305–310.
- [J66] D. R. STINSON. Holey perpendicular arrays. *Utilitas Mathematica* **30** (1986), 31–43.
- [J67] D. R. STINSON. The equivalence of certain incomplete transversal designs and frames. *Ars Combinatoria* **22** (1986), 81–87.
- [J68] D. R. STINSON AND S. A. VANSTONE. Orthogonal packings in $PG(5, 2)$. *Aequationes Mathematicae* **31** (1986), 159–168.
- [J69] R. REES AND D. R. STINSON. On resolvable group-divisible designs with block-size 3. *Ars Combinatoria* **23** (1987), 107–120.
- [J70] 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.
- [J71] E. SEAH AND D. R. STINSON. An assortment of new Howell designs. *Utilitas Mathematica* **31** (1987), 175–188.
- [J72] D. R. STINSON. Frames for Kirkman triple systems. *Discrete Mathematics* **65** (1987), 289–300.
- [J73] D. R. STINSON AND L. ZHU. On the existence of MOLS with equal-sized holes. *Aequationes Mathematicae* **33** (1987), 96–105.
- [J74] 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.

- [J75] R. C. MULLIN AND D. R. STINSON. Pairwise balanced designs with block sizes $6t + 1$. *Graphs and Combinatorics* **3** (1987), 365–377.
- [J76] A. ASSAF, E. MENDELSON, AND D. R. STINSON. On resolvable coverings of pairs by triples. *Utilitas Mathematica* **32** (1987), 67–74.
- [J77] D. R. STINSON. On the existence of skew Room frames of type 2^n . *Ars Combinatoria* **24** (1987), 115–128.
- [J78] D. R. STINSON. Some constructions and bounds for authentication codes. *Journal of Cryptology* **1** (1988), 37–51. [This is the final version of paper [C9].]
- [J79] 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.
- [J80] D. R. STINSON. On the spectrum of nested 4-cycle systems. *Utilitas Mathematica* **33** (1988), 47–50.
- [J81] D. R. STINSON AND S. A. VANSTONE. A combinatorial approach to threshold schemes. *SIAM Journal on Discrete Mathematics* **1** (1988), 230–237. [This is the final version of paper [C10].]
- [J82] R. REES AND D. R. STINSON. Kirkman triple systems with maximum subsystems. *Ars Combinatoria* **25** (1988), 125–132.
- [J83] 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.
- [J84] E. SEAH AND D. R. STINSON. A perfect one-factorization for K_{36} . *Discrete Mathematics* **70** (1988), 199–202.
- [J85] D. R. STINSON. A construction for authentication/secretory codes from certain combinatorial designs. *Journal of Cryptology* **1** (1988), 119–127. [This is the final version of paper [C12].]
- [J86] C. J. COLBOURN AND D. R. STINSON. Edge-coloured designs with block size four. *Aequationes Mathematicae* **36** (1988), 230–245.
- [J87] R. REES AND D. R. STINSON. On the existence of Kirkman triple systems containing Kirkman subsystems. *Ars Combinatoria* **26** (1989), 3–16.
- [J88] 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.
- [J89] P. J. SCHELLENBERG AND D. R. STINSON. Threshold schemes from combinatorial designs. *Journal of Combinatorial Mathematics and Combinatorial Computing* **5** (1989), 143–160.
- [J90] D. R. STINSON. A new proof of the Doyen-Wilson theorem. *Journal of the Australian Mathematical Society A* **47** (1989), 32–42.
- [J91] 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.
- [J92] 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.
- [J93] 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. [Special volume in honour of Haim Hanani.]
- [J94] C. C. LINDNER, C. A. RODGER, AND D. R. STINSON. Nesting of cycle systems of odd length. *Discrete Mathematics* **77** (1989), 191–203. [Special volume in honour of Haim Hanani.]
- [J95] R. REES AND D. R. STINSON. On combinatorial designs with subdesigns. *Discrete Mathematics* **77** (1989), 259–279. [Special volume in honour of Haim Hanani.]
- [J96] 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.
- [J97] D. R. STINSON AND L. TEIRLINCK. A construction for authentication/secretory codes from 3-homogeneous permutation groups. *European Journal of Combinatorics* **11** (1990), 73–79.

- [J98] D. CHEN AND D. R. STINSON. Recent results on combinatorial constructions for threshold schemes. *Australasian Journal of Combinatorics* **1** (1990), 29–48.
- [J99] 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.
- [J100] D. R. STINSON. The combinatorics of authentication and secrecy codes. *Journal of Cryptology* **2** (1990), 23–49.
- [J101] 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.
- [J102] D. R. STINSON. Some observations on parallel algorithms for fast exponentiation in $GF(2^n)$. *SIAM Journal on Computing* **19** (1990), 711–717.
- [J103] R. REES AND D. R. STINSON. On the number of blocks in a perfect covering of v points. *Discrete Mathematics* **83** (1990), 81–93.
- [J104] R. C. MULLIN AND D. R. STINSON. Pairwise balanced designs with odd block sizes exceeding 5. *Discrete Mathematics* **84** (1990), 47–62.
- [J105] E. F. BRICKELL AND D. R. STINSON. The detection of cheaters in threshold schemes. *SIAM Journal on Discrete Mathematics* **4** (1991), 502–510. [This is the final version of paper [C14].]
- [J106] 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.
- [J107] D. R. STINSON AND L. ZHU. Orthogonal Steiner triple systems of order $6m + 3$. *Ars Combinatoria* **31** (1991), 33–63.
- [J108] 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.
- [J109] 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.
- [J110] D. R. STINSON AND L. ZHU. On the existence of three MOLS with equal-sized holes. *Australasian Journal of Combinatorics* **4** (1991), 33–47.
- [J111] D. R. STINSON. A survey of Kirkman triple systems and related designs. *Discrete Mathematics* **92** (1991), 371–393.
- [J112] D. CHEN, R. G. STANTON, AND D. R. STINSON. Disjoint packings on $6k + 5$ points. *Utilitas Mathematica* **40** (1991), 129–138.
- [J113] D. R. STINSON. Designs constructed from maximal arcs. *Discrete Mathematics* **97** (1991), 387–393.
- [J114] D. R. STINSON. On bit serial multiplication and dual bases in $GF(2^m)$. *IEEE Transactions on Information Theory* **37** (1991), 1733–1736.
- [J115] C. C. LINDNER, C. A. RODGER, AND D. R. STINSON. Nestings of directed cycle systems. *Ars Combinatoria* **32** (1991), 153–159.
- [J116] R. REES AND D. R. STINSON. Frames with block size four. *Canadian Journal of Mathematics* **44** (1992), 1030–1049.
- [J117] 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.
- [J118] D. R. STINSON AND Y. J. WEI. Some results on quadrilaterals in Steiner triple systems. *Discrete Mathematics* **105** (1992), 207–219.
- [J119] 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.

- [J120] 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. [This is the final version of paper [C16].]
- [J121] D. R. STINSON. An explication of secret sharing schemes. *Designs, Codes and Cryptography* **2** (1992), 357–390.
- [J122] 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.
- [J123] C. A. RODGER AND D. R. STINSON. Nesting directed cycle systems of even length. *European Journal of Combinatorics* **13** (1992), 213–218.
- [J124] D. R. STINSON. Combinatorial characterizations of authentication codes. *Designs, Codes and Cryptography* **2** (1992), 175–187. [This is the final version of paper [C17].]
- [J125] D. CHEN AND D. R. STINSON. On the construction of large sets of disjoint group-divisible designs. *Ars Combinatoria* **35** (1993), 103–115.
- [J126] 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.
- [J127] D. R. STINSON. An explicit formulation of the second Johnson bound. *Bulletin of the ICA* **8** (1993), 86–92.
- [J128] D. R. STINSON AND L. ZHU. Towards the spectrum of Room squares with subsquares. *Journal of Combinatorial Theory A* **63** (1993), 129–142.
- [J129] A. M. HAMEL, W. H. MILLS, R. C. MULLIN, R. REES, D. R. STINSON, AND J. YIN. The spectrum of $\text{PBD}(\{5, k^*\}, v)$ for $k = 9, 13$. *Ars Combinatoria* **36** (1993), 7–26.
- [J130] 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.
- [J131] D. R. STINSON. Decomposition constructions for secret sharing schemes. *IEEE Transactions on Information Theory* **40** (1994), 118–125.
- [J132] 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.
- [J133] D. R. STINSON. Combinatorial techniques for universal hashing. *Journal of Computer and System Sciences* **48** (1994), 337–346.
- [J134] D. R. STINSON. Universal hashing and authentication codes. *Designs, Codes and Cryptography* **4** (1994), 369–380. [This is the final version of paper [C18].]
- [J135] 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.
- [J136] C. BLUNDO, A. DE SANTIS, D. R. STINSON, AND U. VACCARO. Graph decompositions and secret sharing schemes. *Journal of Cryptology* **8** (1995), 39–64. [This is the final version of paper [C20].]
- [J137] 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.
- [J138] K. GOPALAKRISHNAN AND D. R. STINSON. Three characterizations of non-binary correlation-immune and resilient functions. *Designs, Codes and Cryptography* **5** (1995), 241–251.
- [J139] 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.
- [J140] R. S. REES AND D. R. STINSON. Combinatorial characterizations of authentication codes II. *Designs, Codes and Cryptography* **7** (1996), 239–259.

- [J141] 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. [This is the final version of paper [C22].]
- [J142] 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.
- [J143] 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.
- [J144] C. J. COLBOURN, J. H. DINITZ AND D. R. STINSON. More on thwarts in transversal designs. *Finite Fields and Their Applications* **2** (1996), 293–303.
- [J145] G. ATENIESE, C. BLUNDO, A. DE SANTIS AND D. R. STINSON. Visual cryptography for general access structures. *Information and Computation* **129** (1996), 86–106. [This is the final version of paper [C24].]
- [J146] 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.
- [J147] 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. [This is the final version of paper [C23].]
- [J148] 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.
- [J149] 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.
- [J150] C. BLUNDO AND D. R. STINSON. Anonymous secret sharing schemes. *Discrete Applied Mathematics* **77** (1997), 13–28.
- [J151] D. R. STINSON. On some methods for unconditionally secure key distribution and broadcast encryption. *Designs, Codes and Cryptography* **12** (1997), 215–243.
- [J152] 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.
- [J153] 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. [This is the final version of paper [C26].]
- [J154] 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.
- [J155] 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.
- [J156] 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.
- [J157] 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.
- [J158] D. R. STINSON. Some results on nonlinear zigzag functions. *Journal of Combinatorial Mathematics and Combinatorial Computing* **29** (1999), 127–138.
- [J159] C. BLUNDO, A. DE SANTIS AND D. R. STINSON. On the contrast in visual cryptography schemes. *Journal of Cryptology* **12** (1999), 261–289.
- [J160] 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.

- [J161] 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.
- [J162] D. R. STINSON AND R. WEI. An application of ramp schemes to broadcast encryption. *Information Processing Letters* **69** (1999), 131–135.
- [J163] 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.
- [J164] 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.
- [J165] 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.
- [J166] D. R. STINSON, R. WEI AND L. ZHU. Some new bounds for cover-free families. *Journal of Combinatorial Theory A* **90** (2000), 224–234.
- [J167] D. L. KREHER AND D. R. STINSON. Pseudocode: a L^AT_EX style file for displaying algorithms. *Bulletin of the ICA* **30** (2000), 11–24.
- [J168] 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.
- [J169] G. ATENIESE, C. BLUNDO, A. DE SANTIS AND D. R. STINSON. Extended capabilities for visual cryptography. *Theoretical Computer Science* **250** (2001), 143–161.
- [J170] D. R. STINSON. Something about all or nothing (transforms). *Designs, Codes and Cryptography* **22** (2001), 133–138.
- [J171] 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.
- [J172] C. J. COLBOURN, J. H. DINITZ AND D. R. STINSON. Quorum systems constructed from combinatorial designs. *Information and Computation* **169** (2001), 160–173.
- [J173] 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. [This is the final version of paper [C28].]
- [J174] B. MASUCCI AND D. R. STINSON. Efficient metering schemes with pricing. *IEEE Transactions on Information Theory* **47** (2001), 2835–2844.
- [J175] D. R. STINSON. Some baby-step giant-step algorithms for the low hamming weight discrete logarithm problem. *Mathematics of Computation* **71** (2002), 379–391.
- [J176] 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.
- [J177] 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.
- [J178] 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. [Special volume in honour of Ron Mullin.]
- [J179] 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.

- [J180] 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.
- [J181] 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.
- [J182] 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.
- [J183] D. R. STINSON AND R. WEI. Generalized cover-free families. *Discrete Mathematics* **279** (2004), 463–477. [Special volume in honour of Zhu Lie.]
- [J184] 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. [Special volume in honour of Zhu Lie.]
- [J185] D. R. STINSON. Attack on a concast signature scheme. *Information Processing Letters* **91** (2004), 39–41.
- [J186] 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. [Special Issue for the Third Pythagorean Conference, An Advanced Research Workshop in Geometry, Combinatorial Designs & Cryptology.]
- [J187] 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.
- [J188] 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.
- [J189] J. H. DINITZ AND D. R. STINSON. On assigning referees to tournament schedules. *Bulletin of the ICA* **44** (2005), 22–28.
- [J190] J. A. MUIR AND D. R. STINSON. Alternative digit sets for nonadjacent representations. *SIAM Journal on Discrete Mathematics* **19** (2005), 165–191. [This is the final version of paper [C41].]
- [J191] K. A. LAUNGER, 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.
- [J192] J. A. MUIR AND D. R. STINSON. Minimality and other properties of the width- w nonadjacent form. *Mathematics of Computation* **75** (2006), 369–384.
- [J193] 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. [Special Issue on Coding and Cryptography.]
- [J194] D. R. STINSON. Some observations on the theory of cryptographic hash functions. *Designs, Codes and Cryptography* **38** (2006), 259–277.
- [J195] 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.
- [J196] 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. [Invited paper for special issue on mathematical techniques in cryptology.]
- [J197] W. OGATA, K. KUROSAWA AND D. R. STINSON. Optimum secret sharing scheme secure against cheating. *SIAM Journal on Discrete Mathematics* **20** (2006), 79–95.
- [J198] J. LEE AND D. R. STINSON. Common intersection designs. *Journal of Combinatorial Designs* **14** (2006), 251–269.
- [J199] J. H. DINITZ, A. LING AND D. R. STINSON. Fault tolerant routings with minimum optical index. *Networks* **48** (2006), 47–55.

- [J200] 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.
- [J201] 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.
- [J202] M. NANDI AND D. R. STINSON. Multicollision attacks on some generalized sequential hash functions. *IEEE Transactions on Information Theory* **53** (2007), 759–767.
- [J203] 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.
- [J204] 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.
- [J205] D. R. STINSON. Unconditionally secure chaffing and winnowing with short authentication tags. *Advances in Mathematics of Communications* **1** (2007), 269–280.
- [J206] D. R. STINSON AND S. ZHANG. Algorithms for detecting cheaters in threshold schemes. *Journal of Combinatorial Mathematics and Combinatorial Computing* **61** (2007), 169–191.
- [J207] 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. [This is the final version of paper [C39].]
- [J208] D. R. STINSON AND J. WU. An efficient and secure two-flow zero-knowledge identification protocol. *Journal of Mathematical Cryptology* **1** (2007), 201–220.
- [J209] 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.
- [J210] D. R. STINSON. Generalized mix functions and orthogonal equitable rectangles. *Designs, Codes and Cryptography* **45** (2007), 347–357.
- [J211] D. R. STINSON, R. WEI AND K. CHEN. On generalized separating hash families. *Journal of Combinatorial Theory A* **115** (2008), 105–120.
- [J212] 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.
- [J213] 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. [Special issue on information-theoretic cryptography.]
- [J214] 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.
- [J215] 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.
- [J216] 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.
- [J217] M. B. PATERSON, D. R. STINSON AND R. WEI. Combinatorial batch codes. *Advances in Mathematics of Communications* **3** (2009), 13–27.
- [J218] 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. [Invited paper; this is the final version of paper [C48].]
- [J219] 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.

- [J220] 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. [Special Issue on Electronic Voting.]
- [J221] J. WU AND D. R. STINSON. An efficient identification protocol secure against concurrent-reset attacks. *Journal of Mathematical Cryptology* **3** (2009), 339–352.
- [J222] A. MASHATAN AND D. R. STINSON. Practical unconditionally secure two-channel message authentication. *Designs, Codes and Cryptography* **55** (2010), 169–188.
- [J223] M. B. PATERSON AND D. R. STINSON. Yet another hat game. *Electronic Journal of Combinatorics* **17(1)** (2010), paper #R86, 12 pp.
- [J224] G. M. ZAVERUCHA AND D. R. STINSON. Anonymity in shared symmetric key primitives. *Designs, Codes and Cryptography* **57** (2010), 139–160.
- [J225] 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.
- [J226] S. R. BLACKBURN, A. PANOU, M. B. PATERSON AND D. R. STINSON. Honeycomb arrays. *Electronic Journal of Combinatorics* **17(1)** (2010), paper #R172, 10 pp.
- [J227] M. NOJOUMIAN, D. R. STINSON AND M. GRAINGER. An unconditionally secure social secret sharing scheme. *IET Information Security* **4** (2010), 202–211.
- [J228] 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.
- [J229] 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.
- [J230] 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.
- [J231] G. M. ZAVERUCHA AND D. R. STINSON. Short one-time signatures. *Advances in Mathematics of Communications* **5** (2011), 473–488.
- [J232] 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.
- [J233] 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.
- [J234] J. H. DINITZ, P. R. J. ÖSTERGÅRD AND D. R. STINSON. Packing Costas arrays. *Journal of Combinatorial Mathematics and Combinatorial Computing* **80** (2012), 385–403 (Ralph Stanton volume).
- [J235] 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.

Papers accepted for publication

C. M. SWANSON AND D. R. STINSON. Extended combinatorial constructions for peer-to-peer user-private information retrieval. To appear in *Advances in Mathematics of Communications*. ArXiv report 1112.2762, <http://arxiv.org/abs/1112.2762>.

J. H. DINITZ, M. B. PATERSON, D. R. STINSON AND R. WEI. Constructions for retransmission permutation arrays. To appear in *Designs, Codes and Cryptography*.

Preprints submitted for publication

M. B. PATERSON AND D. R. STINSON. A unified approach to combinatorial key predistribution schemes for sensor networks. IACR ePrint 2011/076, <http://eprint.iacr.org/2011/076>.

D. R. STINSON. Nonincident points and blocks in designs.

M. KENDALL, K. M. MARTIN, S.-L. NG, M. B. PATERSON AND D. R. STINSON. Broadcast-enhanced key predistribution.

M. NOJOUMIAN AND D. R. STINSON. On dynamic threshold schemes and sequential secret sharing.

Non-refereed publications and technical reports not submitted for publication (incomplete list)

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. [This is a reprint of the previous paper.]

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. Technical Report CACR 2006-15, University of Waterloo, 2006, <http://www.cacr.math.uwaterloo.ca/techreports/2006/cacr2006-15.pdf>.

D. R. STINSON AND J. WU. A zero-knowledge identification and key agreement protocol. IACR ePrint 2007/116, <http://eprint.iacr.org/2007/116>.

J. WU AND D. R. STINSON. On the security of the ElGamal encryption scheme and Damgård's variant. IACR ePrint 2008/200, <http://eprint.iacr.org/2008/200>.

M. NOJOUMIAN AND D. R. STINSON. Dealer-free dynamic secret sharing schemes with unconditional security. IACR ePrint 2009/268, <http://eprint.iacr.org/2009/268>.

D. R. STINSON. Comments on a sensor network key redistribution technique of Cichon, Golebiewski and Kutylowski. IACR ePrint 2011/259, <http://eprint.iacr.org/2011/259>.

D. R. STINSON. A problem concerning nonincident points and lines in projective planes. ArXiv report 1109/1573, <http://arxiv.org/abs/1109.1573>.

D. R. STINSON. A problem concerning nonincident points and blocks in Steiner triple systems. ArXiv report 1109.3847, <http://arxiv.org/abs/1109.3847>.

Software distribution

[S1] D. L. KREHER AND D. R. STINSON. The CTAN `macros/latex/contrib/pseudocode/` directory, Comprehensive TeX Archive Network, January 14, 2005.