Curriculum Vitae

Udaya Parampalli

Associate Professor and Reader, Department of Computing and Information Systems, The University of Melbourne.

EDUCATIONAL QUALIFICATIONS

The Graduate Certificate in University Teaching (GCUT) 2012
Centre for the Study of Higher Education, Melbourne Graduate School of Education,
The University of Melbourne, Victoria, Australia

Doctor of Philosophy (PhD) 1993
Department of Electrical Engineering, **Indian Institute of Technology, Kanpur, India**
Supervisor: Professor M.U. Siddiqi
Thesis title: Polyphase and Frequency Hopping Sequences Obtained from Finite Fields and Rings

Master of Technology (MTech) 1987
Department of Electrical Engineering, **Indian Institute of Technology, Kanpur, India**
Supervisor: Professor M.U. Siddiqi
Thesis title: Linear Feedback Shift Register Synthesis for Sequences over Finite Fields and Rings

Bachelor of Engineering (BE) 1985
Department of Electronics and Communications, Malnad College of Engineering, Hassan, **Mysore University, India**

CURRENT AND PREVIOUS APPOINTMENTS

Jan. 2014 to Present: Associate Professor and Reader, Department of Computing and Information Systems, University of Melbourne, Australia
Sep. 2003 to 2013: Senior Lecturer, Department of Computing and Information Systems, University of Melbourne, Australia.
Jun. 2008 to Dec. 2008: Visiting Professor, Department of Computer Science, University of Calgary, Canada.
Feb. 2000 to Aug. 2003: Lecturer, Department of Computer Science and Software Engineering, University of Melbourne, Australia.
Jul. 1997 to Feb. 2000: ARC Research Associate Department of Mathematics, RMIT University, Australia.
Nov. 1992 to Jun. 1997: Member, Research Staff Central Research Laboratory, Bangalore, India.
Jan. 1992 to Nov. 1993: Research Associate Department of Electrical Engineering, I.I.T, Kanpur, India.

AWARDS AND HONORS

1. Senior Member of the Institute of Electrical and Electronic Engineers.
2. “Excellence of research” award for outstanding contributions to research in Computer Science at the University of Melbourne in 2008.
3. 1995-96 Research & Development Award from Bharat Electronics, India, for working on a project to develop a digital encryptor for a satellite network.

RESEARCH EXPERIENCE

Overview

Udaya Parampalli has made significant contributions to information theory, coding and information security. He has produced more than 100 publications (39 in journals, 72 in conferences, 5 edited books and 1 book chapter). Most of his journal papers are in the top international journals in the field, such as IEEE Transactions on Information Theory (Impact factor 3.009, Eigen factor 0.07729, Article Influence Score 1.897).

He has made significant fundamental discoveries in the area of sequences and codes over finite rings. He was one of the first researchers to employ the trace map over the finite ring Z_4 to construct a family of optimal quadriphase sequences. A generalization of these sequences which encompasses the original optimal family is adopted in the 3G wideband CDMA standard [see 3GPP TS 25.213 V5.4.0 (2003-09) on http://www.3gpp.org/]. Results in his PhD thesis are also used in CDMA communications with biphase, quadriphase and frequency hopping modulation and the significance of the results was recognized internationally. He was the first author to use finite rings to construct frequency hopping sequences. One of the biphase sequence families discovered by him is referred to in the literature as the family of *Udaya- Siddiqi sequences*. This is a unique family of 2^n binary sequences of period $2(2^n-1)$ with out-of- phase auto and cross correlations equal to the square root of the length, and is the largest known family with such a property. The correlation parameters of this family are better than Gold codes by a factor $1/\sqrt{2}$, thus enabling an increased number of users in communication applications without experiencing degradation due to interference.

RESEARCH INTERESTS

- Codes for Storage and Security.
- Trust and Privacy in Networks.
- Sequences for communication and security.
- Cryptography
- Combinatorics
- Error correcting codes

UNIVERSITY TEACHING

Subjects

433253 or 433293 or COMP2003: Algorithms and Data structures (2000-2011),
433353: Networks and Communications (2001-2009),
433645: Computer Security,
433522 or COMP90007, Internet Technologies,
COMP90038: Algorithms and Complexity,

New subjects developed (including syllabus, lecture notes, tutorials, assessment and website)
433448: Applied Cryptography and Coding.
COMP90043: Cryptography and Security.

Prior to 2000:
1998-1999: RMIT University: MA941, a postgraduate/honours course in Applied Cryptography University and Lectures on Polynomial Transforms and Boolean Algebra
1985-1992: Teaching assistant for Basic Electrical Science and Electronics Laboratories.

RESEARCH GRANTS AND PROJECTS

- R. Evans and Dr. K. Sithamparanathan and U. Parampalli, ARC Discovery “Cognitive Radars for Automobiles”, 2015-2017, AUD $324,900.
- S. Halgamuge, M. Ashokkumar, W. Harley, P. Bhalla, U. Parampalli, and T. Chan, Melbourne-India Postgraduate Program (MIPP), International Research and Research Training Fund (IRRTF), The University of Melbourne, 2014, AUD $300,000.
- U. Parampalli et, al, Research Networks or Consortia (RNC), “Communications Sensing and Coding (CSC) Research Network”, International Research and Research Training Fund (IRRTF), The University of Melbourne, 2014, AUD $150,000.
- U. Parampalli, L. Kulik, E. Manias, E. Ozanne and F. J. M. Sanchez, “Smart Companion: RFID and Broadband Technologies for Medication Management for Patients and Older People with Chronic Illness”, Institute for a Broadband Enabled Society (IBES), The University of Melbourne, 2012-2013, AUD $70,000.
- C. Humphreys, G. McCarthy, S. Howard, M. Spriggs, U. Parampalli, “Working in the Cloud-Developing Identity Resources for Care Leavers”, Carlton Connect Initiatives Fund, The University of Melbourne Fund: AUD $40,000.
- U. Parampalli, B. Moran, X. Wang, S. Boztas, N. Cooley, The Australia-China Group Missions, “Advancing Agriculture and Food Security Using Information Fusion Technologies in Sensing and Communications” supported by the Department of Industry, Innovation, Science, Research and Tertiary Education (DIISRTE), 2012-2013, AUD $45,000.

- U. Parampalli, “Z4 Sequence Design for Wireless Communications” (CH090262) of Australia-China Special Fund for S&T Cooperation - International Science Linkages Program, with Prof. Xiaohu Tang, Southwest Jiatong University, China and A/Prof. Serdar Boztas, RMIT University, Australia, 2010-2011, AUD $79,732.
- U. Parampalli, “Novel Constructions of Secure and Efficient Hybrid Identifier based Systems, MRDGS Grant, 2009 (Near Miss ARC DP) AUD $35,000.
- U. Parampalli, Melbourne Research Grants Scheme, “Novel techniques for generation and analysis of sequences for security and communications”, MRDGS Grant (Near Miss ARC DP), 2003-2004, AUD $30,000.
- Kuijper M and U. Parampalli, ARC Discovery Project DP0209243, “Innovative Decoding Methods for Increased Error Correction of Reed-Solomon Codes and Related Ring Codes”, Australian Research Council, 2002-2004, AUD $235,000.
- U. Parampalli, “Pseudo-random Sequences from Finite Rings”, MRCEGS Project, University of Melbourne, 2000-2001, AUD $14,000.
- U. Parampall, “Public key Infrastructure for Network Security”, MRDGS Project, University of Melbourne, 2001-2002, 24, AUD $222.

RESEARCH STUDENT SUPERVISION

Current Research Higher Degree (RHD) (PhD and Masters by Research) Students:

1. Lakshmi Jagathamma Mohan, Topic Distributed Storage Code Architectures.
2. Leyla Roohi, Topic: Topic: Privacy-preserving computations for Australian Metadata, co-supervision with Vanessa Teague.
3. Yang Lu, Topic: Trust-based Interaction Models in Virtual Communities, co-supervision with Rich Sinnot.
4. Shuo Wang, Topic: Location Security of Tweeters through Differential Privacy, co-supervision with Rich Sinnot.
5. Kun Huang, Visiting Student, Topic: Security Capacity of Storage Codes.
6. Shifeng Sun, Visiting Student, Topic: Non Malleable Public Key Cryptography,
7. Hongyu Han, Visiting Student, Topic: Frequency Hopping Sequences.

Completed RHD research students:

1. Zilong Liu, Visting Student from NTU (2014), co-supervision with A/Prof. Guan Yong Liang.
2. Janaka Weerathunga Yapa Seneviratne (Masters 2014), co-supervision with A/Prof. L. Kulik.
3. Kim Ramchen (Masters 2011), Thesis: Electronic Voting, co-supervision with Dr. V. Teague.
4. Dr. Peter Hyun Jeen LEE (PhD 2011), Thesis: Identity-based Encryption and its Applications using Bilinear Maps, From July 2013, Post doctoral Scholar, University of New Castle, United Kingdom.
5. Dr. Giannakis Antoniou (PhD 2010) Thesis:Technologies Avoiding Privacy Incidents in Hostile Environments (1st supervisor, with Prof Leon Sterling and Prof. Lynn Batten), now a lecturer in Computer Science ,The Philips College – Nicosia, Cyprus.
6. Dr. Shivaramakrishnan Narayan (PhD 2009), Thesis: Secure Identity-based Signatures and Signcryptions Using Pairing, now with Optimal Payments Plc, Calgary, Alberta, Canada.
7. Dr. Abdun Mahmood (PhD 2008), Thesis: Hierarchical Clustering and Summarization of Network Traffic Data, (co-supervised with A/Prof. Chris Leckie) now a Lecturer at UNSW, Canberra.
8. Ana Jancic (Masters 2009- Deakin University), Thesis: Authentication in Public Key Encryption Schemes.
9. Andrew J. Newlands (Masters 2004), Thesis: On Cryptanalysis of steam ciphers.
10. Rema Hariharan, Monash University, co-supervision with Prof. Tom Hall, Thesis: Near Perfect Sequences of Odd and Even length.

SERVICE TO THE UNIVERSITY

- CIS Coordinator for 2013 Engineers Australia-Australian Computer Society Accreditation.
- Department’s Timetable coordinator from 2003 to 2011.
- Member of Safety Committee from 2006 to 2007.

PROFESSIONAL SERVICE

General Program Committee Chair:

- SETA-2014, “International Conference on SEQUENCES AND THEIR APPLICATIONS” 2014, Melbourne, Australia.

Program Committee Co-Chair:

- SETA-2016, “International Conference on SEQUENCES AND THEIR APPLICATIONS 2016”, October, 2016, Chengdu, China.
- 2015 International Workshop on Signal Design and Its Applications in Communications (IWSDA15), September 13-18, 2015, Bengaluru, India.

- Australasian Information Security Conference (ACSW-AISC) 2014, January 20 - 23 2014, Auckland, New Zealand.
- Australasian Information Security Conference (ACSW-AISC 2013), January 29 - February 1, 2013, Adelaide, Australia.
- 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011.
- 2007 International Workshop on Signal Design and Its Applications in Communications (IWSDA07), September 23-27, 2007, Chengdu, China.

Program Committee Member:

- SETA-2012, “International Conference on SEQUENCES AND THEIR APPLICATIONS 2012”, June 4-8, 2012, Waterloo, Canada.
- SETA-2010, “International Conference on SEQUENCES AND THEIR APPLICATIONS 2010”, September 12 – 17, 2010, Telecom ParisTech, Paris, France.
- APCC-2010, “16th Asia-Pacific Conference on Communications – Coding Theory & DSP for Communications”, Auckland, New Zealand, Oct. 31 to Nov. 3, 2010.
- IWSDA’09, “International Workshop on Sequence Design and its Applications in Communications”, October 19–23, 2005, Fukuoka, Japan.
- Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC- 18), June 8-12, 2009, Taragonna, Spain.
- SETA-08, “International Conference on SEQUENCES AND THEIR APPLICATIONS 2008”, September 14 – 18, 2008, Kentucky, USA.
- Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17), December 16- 20, 2007, Bangalore, India.
- SETA06, “International Conference on SEQUENCES AND THEIR APPLICATIONS 2006”, September 24 – 28, 2006, Beijing, CHINA.
- IWSDA’05, “International Workshop on Sequence Design and its Applications in Communications”, October 10–14, 2005, Shimonoseki, Yamaguchi, Japan.
- International Conference on Communications, Circuits and Systems, (ICCCAS 2005), Hong Kong, China, May 2005.
- Polynomial Cryptography, July 7-12, 2004, Melbourne, Australia.

Leadership

Udaya Parampalli leads the Security group in the Department of Department of Computer Science and Software Engineering, University of Melbourne, Australia.

He is the chairman of the Technical Program Committee of 16th Australasian Conference on Information Security and Privacy Melbourne, Australia (ACISP 2011).

Udaya Parampalli coordinated the Computing and Information System Department’s 2013 accreditation submissions for its degrees with Engineers Australia (EA) and the Australian Computing Society (ACS). We have now EA and ACS accreditations for university’s software engineering courses.

Workshop Organization

Udaya Parampalli, “Pairing Based Cryptography workshop”, Australian Mathematical Sciences Institute (AMSI) (http://www.cs.mu.oz.au/pbc06/), 2006.

Udaya Parampalli (With Serdar Boztas), “Grant for Workshop on Sequence Design and Its Applications in Communications and Cryptography”, Australian Mathematical Sciences Institute (AMSI) (http://user.gs.rmit.edu.au/infosec/amsiworkshop/), 2008.

SELECTED INVITED TALKS, WORKSHOP PRESENTATIONS AND VISITS

1. Keynote presentation, “Cryptographic Solutions for Cloud Security”, the International Symposium on Cloud and Services Computing, Surathkal, India, December 16-19, 2012.
2. Keynote presentation, “Cryptographic Techniques for Cloud Security”, International Conference On Emerging Trends in Electrical, Communication and Information Technologies (ICECIT-2012), Anantapur, India, December 22-24, 2012.
3. Plenary Talk, “Low Correlation Zone Sequences over Finite Fields and Rings”, IWSDA 2009, Fukuoka, Japan, October 19-23, 2009.
4. Invited talk, “Low Correlation Zone Sequences”, Workshop on Sequence Design and Its Applications in Communications and Cryptography, 4-6 December, Melbourne, 2008.
5. Invited Tutorial: “Cryptographic Principles in Sensor Network” at the International Conference on Intelligent Sensing and Information Processing, Chennai, December 14-17, 2005.

Selected International Visits:

1. July 2008 to December 2008: Visited Prof. Rei Safavi-Naini and Prof. Hugh Williams Department of Computer Science, University of Calgary, Alberta, Canada.
2. December 27, 2008 to January 14, 2009, Visited Prof. Pinghi Fan, SouthWest Jiatong University, China.
3. December 2010, Visited Prof. C. Ding and Dr. W.H. Mow, Hong Kong University of Science and Technology, Hong Kong.
4. December, 2011 and 2012 Visited Prof. Xiaohu Tang, SouthWest Jiatong University, China.

PUBLICATIONS

Udaya Parampalli’s publications have also appeared under the name **P Udaya** or **U Parampalli**.

Publication summary

- Papers in refereed journals: 39 in career, 26 since July 2005, 3 under review.
- Papers in refereed conference proceedings: 72 in career, 50 since 2005.
- Google Scholar Citations as on 10 October 2015: 969, 594 since 2010.
- h-index 16 i10-index 24

Book and Book Chapters

[B8] A. Al-Hourani, R. Evans, P. M. Farrell, B. Moran, M. Martorella, S. Kandeepan, S. Skafidas, U. Parampalli, Millimeter-wave Integrated Radar Systems and Techniques, Book Title, Academic Press Library in Signal Processing: Volume 2 Communications and Radar Signal Processing, to appear, 2017.

[B7] X. Tang, U. Parampalli and Tetsuya Kojima. Proceedings of 2015 International Workshop on Signal Design and Its Applications in Communications (IWSDA15), September 13-18, 2015, Bengaluru, India, IEEE Press,2015.

[B6] X. Tang, U. Parampalli and T. Kojima. Proceedings of 2015 International Workshop on Signal Design and Its Applications in Communications (IWSDA15), September 13-18, 2015, Bengaluru, India, IEEE Press,2015.

[B5] U. Parampalli and I. Welch, Eds. Information Security 2014, Proceedings of the Twelfth Australasian Information Security Conference (AISC 2014), Auckland, New Zealand, 20 - 23 January 2014, Volume 149 in the Conferences in Research and Practice in Information Technology Series. Published by the Australian Computer Society Inc., 2014.

[B4] C. Thomborson and U. Parampalli, Eds. Information Security 2013, Proceedings of the Eleventh Australasian Information Security Conference (AISC 2013), January 29 - February 1, 2013, Adelaide, Australia, Volume 138 in the

Conferences in Research and Practice in Information Technology Series. Published by the Australian Computer Society Inc., 2013.

[B3] U. Parampalli and P. Hawkes, Proceedings, Information Security and Privacy, 16th Australasian Conference, ACISP 2011, Melbourne, Australia, July 11-13, 2011, Lecture Notes in Computer Science, Volume 6812, 2011.

[B2] Pinghi Fan, Parampalli Udaya, Xiaohu Tang and Naoki Suehiro. Proceedings of 2007 International Workshop on Signal Design and Its Applications in Communications (IWSDA07), September 23-27, 2007, Chengdu, China, IEEE Press, 385 pages 2007.

[B1] Serdar Boztas and P. Udaya. Partial Correlations of Sequences and Their Applications, In CODES OVER RINGS, Edited by Patrick Sole, Series on Coding Theory and Cryptology – Vol. 6, ISSN: 1793-2238, July 2009.

Journals

[J44] Q Yan, U Parampalli, X Tang, Q Chen, Online Coded Caching with Random Access, Accepted Date: December 14, 2016, To appear in IEEE Communications Letters, 2017.

[J43] K. Huang, U. Parampalli, M. Xian, On Secrecy Capacity of Minimum Storage Regenerating Codes, IEEE Trans. Information Theory 63(03): 1510-1524, 2017.

[J42] K. Huang, U. Parampalli, M. Xian, Security Concerns in Minimum Storage Cooperative Regenerating Codes. IEEE Trans. Information Theory 62(11): 6218-6232, 2016.

[J41] H. Han, D. Peng, U. Parampalli, Zheng Ma and H. Liang, Construction of low-hit-zone frequency hopping sequences with optimal partial Hamming correlation by interleaving techniques, Accepted Date: August 2016, To appear in Des. Codes Cryptogr. (2016). doi:10.1007/s10623-016-0274-8

[J40] H. Han, D. Peng and U. Parampalli, New sets of optimal low-hit-zone frequency-hopping sequences based on m-sequences, First Online: 18 June 2016, To appear in Cryptogr. Commun. (2016). doi:10.1007/s12095-016-0192-7.

[J39] J Li, X Tang, U Parampall, A Framework of Constructions of Minimum Storage Regenerating Codes with the Optimal Update/Access Property for Distributed Storage Systems Based on Invariant Subspace Technique. IEEE Transactions on Information Theory, Vol. 61, Issue 4, pp 1920-1932, 2015.

[J38] Z. Liu, U. Parampalli, Y. L. Guan and S. Boztas, “Optimal Odd-Length Binary Z-Complementary Pairs," IEEE Transactions on Information Theory, Vol 60, Issue 9, pp 5768 - 5781, 2014.

[J37] U Parampalli. S. Boztas. A class of quaternary noncyclic Hadamard matrices, Australian Journal of Combinatorics, Vol 60, Issue 3, 255-262, 2014.

[J36] Z. Liu, Y. L. Guan and U. Parampalli, “New Complete Complementary Codes for the Peak-to-Mean Power Control in MC-CDMA," IEEE Transactions on Communications, Vol 60, Issue 3, pp 1356-1366, 2014.

[J35] Z. Liu, U. Parampalli, Y. L. Guan and S. Boztas, “A New Weight Vector for a Tighter Levenshtein Bound on Aperiodic Correlation," IEEE Transactions on Information Theory, Vol 60, Issue 2, pp 1356-1366, 2014.

[J34] Z. Liu, U. Parampalli and Y. L. Guan, “On Even-Period Binary Z-Complementary Pairs with Large ZCZs", IEEE Signal Processing Letters, vol. 21, no. 3, pp. 284-287, Mar. 2014.

[J33] Z. Liu, U Parampalli, Y. L. Guan, S. Boztas. Constructions of Optimal and Near-Optimal Quasi-Complementary Sequence Sets from Singer Difference Sets, IEEE Wireless Communication Letters, Vol. 2, no. 5, 487-490, Oct. 2013.

[J32] U Parampalli. X. Tang, S. Boztas. On the Construction of Binary Sequence Families With Low Correlation and Large Sizes, IEEE Trans. Inform. Theory, Vol 59, Issue 2, 1082- 1089, 2013.

[J31] Z Zhou, X Tang, X. Niu and U. Parampalli. New Classes of FrequencyHopping Sequences With Optimal Partial Correlation, IEEE Trans. Inform. Theory, Vol 58, Issue 1, 453 - 458, 2012.

[J30] Z Zhou, X Tang, Y. Yang and U. Parampalli A Hybrid Incomplete Exponential Sum With Application to Aperiodic Hamming Correlation of Some Frequency-Hopping Sequences, IEEE Trans. Inform. Theory, Vol 58, Issue 10, 6610 – 6615, 2012.

[J29] Y. Yang, X. Tang and U. Parampalli. Authentication codes from difference balanced Functions , International Journal of Foundations of Computer Science, Vol 22, Issue 6, pp 1417-1429, 2011.

[J28] Z Zhou, X Tang, D Peng and U. Parampalli. New Constructions for Optimal Sets of Frequency-Hopping Sequences, IEEE Trans. Inform. Theory, Vol 57, Issue 6, pp 3831-3840, 2011.

[J27] Y. Yang, X.H. Tang, U. Parampalli and D.Y. Peng. New Bound on Frequency Hopping Sequence Sets and Its Optimal Constructions, IEEE Trans. Inform. Theory, Vol 57, Issue 11, pp 7605-7613, 2011.

[J26] Z. Zhou, X. Tang, U. Parampalli and D. Peng. New p-ary sequence family with low correlation and large linear span, Applicable Algebra in Engineering, Communication and Computing, Vol 22, Issue 4, pp 301-309, 2011.

[J25] T. Matsumoto, S. Matsufuji, T. Kojima and U. Parampalli. Orthogonal and ZCZ Sets of Real-Valued Periodic Orthogonal Sequences from Huffman Sequences, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences Vol. E94-A No.12 pp.2728-2736, 2011.

[J24] X. Tang andU. Parampalli.On the Noncyclic Property of Sylvester Hadamard Matrices, IEEE Trans. Inform. Theory, Vol 56, Issue 9, pp 4653-4658, 2010.

[J23] U. Parampalli and X. Tang. Low Correlation Zone Sequences from Inter- leaved Construction, Invited Paper, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences Vol. E93-A No.11 pp. 2220-2226, 2010.

[J22] T Z. Zhou, X. Tang and U. Parampalli. A Large Class of p-Ary Cyclic Codes and Sequence Families, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E93-A No.11 pp. 2272-2277, 2010.

[J21] O. Moreno, A.Z. Tirkel, U. Parampalli and R.G. van SCHYNDEL. New Families of Arrays in Two Dimensions for Watermarking Applications, Electronics Letters Vol. 46, Issue 22, pp. 1500-1502, 2010.

[J20] P. H. Lee, S. Narayan, U. Parampalli, Secure Communication in Mobile AdHoc Network using Efficient Certificateless Encryption, Journal of Networks, Vol 4, No. 8, pp 687-697, 2009.

[J19] S. Narayan and P. Udaya, Efficient Identity based Signature Algorithm, IEEE Information Security, Vol 2, No. 4, pp 108-118, 2008.

[J18] M. Abdun, Leckie, C. A. Leckie and P. Udaya, An Efficient Clustering Scheme to Exploit Hierarchical Data in Network Traffic Analysis. IEEE Transactions on Knowledge and Data Engineering. 20 (6): 752-767, 2008.

[J17] G. Antoniou, L. Sterling, S. Gritzalis, U. Parampalli, Privacy and Forensics investigation process: The ERPINA protocol. The ERPINA protocol, Computer Standards & Interfaces, 30 229-236, 2008.

[J16] X. Tang, P. Udaya and P. Fan. Generalized Binary Udaya-Siddiqi Sequences, IEEE Trans. Inform. Theory, 53:1-6, March, 2007.

[J15] X. Tang and P. Udaya. A Note on the Optimal Quadriphase Sequences Families, IEEE Trans. Inform. Theory, 53: 433-436, January, 2007.

[J14] X-W.Wu, M. Kuijper and P. Udaya, Lower Bound on Minimum Lee Distance of Algebraic-Geometric Codes over Finite Fields, IEE Electronics Letters, Vol. 43:820-822, issue 15, 2007.

[J13] X. Tang, P. Udaya and P. Z. Fan. A New Family of Nonbinary Sequences with Three Level Correlation Property and Large Linear Span, IEEE Trans. Inform. Theory, 51:2906-2914. August, 2005.

[J12] X. Wu, M. Kuijper and P. Udaya. A Root-Finding Algorithm for List Decoding of Reed-Muller Codes IEEE Trans. Inform. Theory, 51:1190-1196, March, 2005.

[J11] X. Wu, M. Kuijper and P. Udaya. Lee-metric decoding of BCH and Reed Solomon codes. Electronics Letters, 39:1522–1524, No. 21, 2003.

[J10] K.J. Horadam and P. Udaya. A new class of ternary cocyclic Hadamard codes. Appl. Algebra Engrg. Comm. Comput., 14:65–73, 2003.

[J9] K.J. Horadam and P. Udaya. A New Construction of Central Relative (pa, pa, pa, 1)-Difference Sets. Designs Codes and Cryptography, 27:281–295, 2002.

[J8] A. Bonnecaze, P. Sol´e, and P. Udaya. Tricolore 3-designs in Type III codes, newblock Discrete Mathematics, 241:129–139, 2001.

[J7] K.J. Horadam and P. Udaya. Cocyclic Hadamard Codes. IEEE Trans. Inform. Theory, 46:1545–1550, 2000.

[J6] P. Udaya. and M. U. Siddiqi. Generalized GMW Quadriphase Sequences satisfying the Welch bound with Equality. Appl. Algebra Engrg. Comm. Comput., 10:203–225, 2000.

[J5] A. Bonnecaze and P. Udaya. Cyclic Codes and Self-dual Codes over F2+uF2. IEEE Trans. Inform. Theory, 45:1250–1255, 1999.

[J4] P. Udaya and A. Bonnecaze. Decoding of Cyclic Codes over F2+uF2. IEEE Trans. Inform. Theory, 45:2148–2157, 1999.

[J3] P. Udaya and M. U. Siddiqi. Optimal and Suboptimal Quadriphase Sequences Derived from Maximal Length Sequences over Z4. Appl. Algebra Engrg. Comm. Comput., 9:161–191, 1998.

[J2] P. Udaya and M. U. Siddiqi. Optimal Large Linear Complexity Frequency Hopping Patterns Derived from Polynomials Residue Class Rings. IEEE Trans. Inform. Theory, 44:1492–1503, 1998.

[J1] P. Udaya and M. U. Siddiqi. Optimal Biphase Sequences with Large Linear Complexity Derived from Sequences over Z4. IEEE, Trans. on Inform.Theory, 42:206–216, 1996.

International Conference Proceedings

[C75] S-F Sun, U Parampalli, TH Yuen, Y Yu, D Gu, Efficient completely non-malleable and RKA secure public key encryptions, Lecture Notes in Computer Science, ACISP2016, 9723: 134-150, 2016

[C74] S-F Sun, D Gu, JK Liu, U Parampalli, TH Yuen TH, Efficient Construction of Completely Non-Malleable CCA Secure Public Key Encryption, 11th ACM Asia Conference on Computer and Communications Security (ASIA CCS), Xian, PEOPLES R CHINA, 30 May 2016, pages 901-906, Jun 2016.

[C73] P. I. S. Caneleo , L. J Mohan, U Parampalli and Aaron Harwood, On improving recovery performance in erasure code based geo-diverse storage clusters, to appear in the Proceedings of International Conference on Design of Reliable Communication Networks (DRCN), DRCN 2016, Accepted Date 10-1-2016, Paris, March 15-17, 2016.

[C72] L. J Mohan, R.Harold, P. I. S. Caneleoz, U Parampalli and Aaron Harwood, Benchmarking the performance of Hadoop triple replication and erasure coding on a nation-wide distributed cloud, NetCod 2015 International Symposium on Network Coding, pp 61- 65, Sydney, 2015.

[C71] R. Luo, U Parampalli, Self-dual Cyclic Codes Over Z4 + uZ4, Proceedings of International Workshop on Signal Design and its Applications in Communications, IWSDA’15, Bengaluru, pp 57-61, 2015.

[C70] Z Liu, YL Guan, S Hu, U Parampalli, Optimal spectrally-constrained sequences, Proceedings of IEEE International Symposium on Information Theory(ISIT) 2015, Hong Kong, pp 2692-2696, 2015.

[C69] J Seneviratne, U Parampalli, L. Kulik, An Authorised Pseudonym System for Privacy Preserving Location Proof Architectures, In the Proceedings of Australasian Information Security Conference (AISC 2014), CRPIT, Vol. 149, ACS, pp. 47-56, 2014.

[C68] T. Kojima, T. Tachikawa, A. Oizumi, Y. Yamaguchi and U Parampalli, A disaster prevention broadcasting based on data hiding scheme using complete complementary codes, In the Proceedings of 2014 International Symposium on Information Theory and its Applications (ISITA 2014), pp. 45-49, 2014.

[C67] Z. Liu, Y.L. Guan and U Parampalli. On A New Construction of Zero Correlation Zone Sequences from Generalized Reed-Muller Codes, Proceedings of 2014 IEEE Information Theory Workshop (ITW-2014), Hobart, Australia, November 2-5, 591-595, 2014

[C66] Z. Liu, Y.L. Guan and U Parampalli S. On optimal binary Z-complementary pair of odd period, Proceedings of IEEE International Symposium on Information Theory(ISIT) 2013, Istanbul, Turkey, July 7-12, pp 3130-3134, 2013.

[C65] Z. Liu, Y.L. Guan U Parampalli and S. Boztas. Quadratic Weight Vector for Tighter Aperiodic Levenshtein Bound, Proceedings of IEEE International Symposium on Information Theory (ISIT) 2013, Istanbul, Turkey, July 7-12, pp 3125-3129, 2013.

[C64] S. M. Erfani, S. Karunasekera, C. Leckie, and U. Parampalli. A Privacy-Preserving Data Aggregation in Participatory Sensing Networks, Proceedings of IEEE ISSNIP 2013, IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing, Melbourne, 2 – 5 April 2013.

[C63] Z. Zhou, X. Tang, Y, Yang and U. Parampalli. On the Aperiodic Hamming Correlation of Frequency-Hopping Sequences from Norm Functions. Proceedings of SETA-2012, International Conference on Sequences and Applications, Waterloo, Canada, June 4-8, 2012.

[C62] S. Boztas and U Parampalli. Low Probability of Intercept Properties of Some Binary Sequence Families with Good Correlation Properties, Accepted (Date April 16, 2012) for Proceedings of IEEE International Symposium on Information Theory(ISIT) 2012, July 1 -6, Cambridge, MA, U.S.A, 2012.

[C61] P. Lee, U Parampalli, S.Narayan, Efficient Identity-based Signcryption without Random Oracles, In the Proceedings of Australasian Information Security Conference (AISC 2012), CRPIT, Vol. 125, ACS, pp. 3-14, 2012. [

[C60] Z. Xu, R. Zhang, R Kotagiri, U Parampalli. An Adaptive Algorithm for Online Time Series Segmentation with Error Bound Guarantee, Accepted, Proceedings of Joint Conference-EDBT(15th International Conference on Extending Database Technology) and ICDT (International Conference on Database Theory), Accepted date: 8, January 2012, Berlin, Germany, March 26-30, 2012.

[C59] U Parampalli, K. Ramchen and V. Teague. Efficiently Shuffling in Public, Public Key Cryptography – PKC 2012, LNCS 7293, Pages 431-448, 2012.

[C58] S. Boztas and U Parampalli. On the relative abundance of nonbinary sequences with perfect autocorrelations, Proceedings of IEEE International Symposium on Information Theory(ISIT) 2011, Saint-Petersburg, Russia, July 31-August 5, pp 494-498, 2011.

[C57] T. Matsumoto, S. Matsufuji, T. Kojima and U Parampalli. A generation method of an orthogonal set of real-valued periodic orthogonal sequencesfrom Huffman sequences, Proceedings of Australian Communications Theory Workshop (AusCTW), 2011, Melbourne, Australia, Jan. 31-Feb. 3, pp 66 - 70, 2011.

[C56] T. Kojima, N. Ohtani, T. Matsumoto and U Parampalli. A blind digital watermarking scheme based on complete complementary codes, Proceedings of Australian Communications Theory Workshop (AusCTW), 2011, Melbourne, Australia, Jan. 31-Feb. 3, pp 1-6, 2011.

[C55] T. Matsumoto, S. Mstsufuji, T. Kojima, U Parampalli. A Generation Method of a ZCZ Set of Real-Valued Periodic Orthogonal Sequences from Huffman Sequences, Proceedings of the 2011 2nd International Conference on Innovative Computing and Communication and 2011Asia-Pacific Confer ence on Information Technology and Ocean Engineering (CICC-ITOE2011), Macau, China, March 5-6, Vol. 2, pp.66-70, 2011.

[C54] T. Kojima, N. Ohtani, T. Matsumoto, U Parampalli. On Multiple Information Embedding by DigitalWatermarking Based on Complete Complementary Codes, Proceedings of 2011 International Workshop on Signal Design and its Applications in Communications (IWSDA 2011), Guilin, China, Oct..10-14, pp 157-161, IEEE Press (New Jersey), 2011.

[C53] O Moremo, A Tirkel, R van Schyndel, U Parampalli. New families of 2D and 3D arrays for sub-image watermarking, Proceedings of the Fourth International Conference on Network and System Security (NSS) 2010, Melbourne, Australia, Sep.1-3, pp 340-344, IEEE Press (New Jersey), 2011.

[C52 U Parampalli. X. Tang, S. Boztas. On the construction of binary sequence families with low correlation and large sizes, Proceedings of IEEE International Symposium on Information Theory (ISIT) 2010, Austin, Texas, U.S.A, June 13 -18, pp 1253-1257, IEEE Press (New Jersey), 2011.

[C51] S. Boztas and U Parampalli. Nonbinary Sequences with Perfect and Nearly Perfect Autocorrelations , Proceedings of IEEE International Symposium on Information Theory(ISIT) 2010, Austin, Texas, U.S.A, June 13 -18, pp 1300-1304, IEEE Press (New Jersey), 2011.

[C50] P. Udaya, X. Tang and Serdar Boztas. On the Construction of Binary Sequence Families with Low Correlation and Large Sizes, IEEE International Symposium on Information Theory, Texas, June 13-18, 2010.

[C49] Serdar Boztas and P. Udaya. Nonbinary Sequences with Perfect and Nearly Perfect Autocorrelations, IEEE International Symposium on Information Theory, Texas, June 13-18, 2010.

[C48] Yang Yang, X. Tang and P. Udaya. Optimal Authentication Codes from Difference Balanced Functions, Sequence Families, Sequences and Their Applications - SETA 2010, LNCS 6338, pp. 298-304, 2010.

[C47]. Yang Yang, X. Tang and P. Udaya. Optimal Authentication Codes from Differnece Balanced Functions, Sequence Families, Sequences and Their Applications - SETA 2010, LNCS 6338, pp. 298-304, 2010.

[C46]. U. Parampalli. Low Correlation Zone Sequences over Finite Fields and Rings, Invited Talk, IWSDA 2009, Fukuoka, Japan, October 19-23, pp 1-1, 2009.

[C45] D. Wu, P. Fan, H. Li, U. Parampalli. Optimal Variable-Weight Optical Orthogonal Codes via Cyclic Difference Families, ISIT 2009, South Korea, June 28-July 3, pp 448-452, 2009.

[C44] G. Antoniou, L. Batten, S. Narayan and U. Parampalli. A Privacy Preserving E-Payment Scheme, Intelligent Distributed Computing III, SCI 237, LNCS 5376, pp 197-202, 2009.

[C43] G. Antoniou, L. Batten, and U. Parampalli. An Anonymity Revocation Technology for Anonymous Communication, In Information Systems Development, Towards a Service Provision Society, 17th International Conference on Information Systems Development (ISD-2008), Springer Science and Business Media, pp 329-337, 2009.

[C43] P. Lee, S.Narayan, P. Udaya. Secure Communication in Mobile Ad Hoc Network Using Efficient Certificateless Encryption, In the Proceedings of SECRYPT 2008, SECRYPT 2008: International Conference on Security and Cryptography Proceedings, Porto, Portugal: INSTICC (Institute for Systems and Technologies of Information, Control and Communica-tion), July 26-29, pp .306-311, 2008.

[C41] S. Narayan, P. Udaya, P. Lee. Identity Based Signcryption Without Random Oracles/, In the Proceedings of SECRYPT 2008, International Conference on Security and Cryptography Proceedings, Porto, Portugal: I NSTICC (Institute for Systems and Technologies of Information, Control and Communication), July 26-29, pp. 342- 347, 2008.

[C40]. P. Udaya and S. Boztas. On Partial Correlations of Various Z 4 Sequence Families, Sequences and Their Applications - SETA 2008, LNCS 5203, pp 332-344, 2008.

[C39] G. Antoniou, L. Batten and U. Parampalli. Designing Information Systems Which Manage or Avoid Privacy Incidents, Intelligence and Security Informatics, LNCS 5376, pp 131-142, 2008.

[C38] G. Antoniou, L. Batten, U. Parampalli. A Trusted Approach to E-Commerce, W. Jonker and M.Petkovic (Eds.): SDM 2008, LNCS 5159, pp. 119-132.

[C37] S. Bozta¸s and P. Udaya. Partial Correlations of Galois Ring Sequences, The third International Workshop on Sequence Design and Its Applications to Communications, October 23-27, Chengdu, China, pp 157-161, 2007.

[C36] Narayan S, P. Udaya. A Provably Secure Multi-Receiver Identity-Based Signcryption Using Bilinear Maps. SECRYPT 2007: International Conference on Security and Cryptography Proceedings. pp 305-308. Setubal, Portugal: INSTICC (Institute for Systems and Technologies of Information, Control and Communication), 2007.

[C35] G. Antoniou, A. Jancic, P. Udaya, L. Sterling. Applying a cryptographic scheme in the RPINA protocol, Proceedings of the Second Annual Workshop on Digital Forensics & Incident Analysis (WDFIA07), B. Preneel, S. Gritzalis, S. Kokolakis, T. Tryfonas (Eds.), August 2007, Samos, Greece, IEEE Computer Society Press.

[C34] G. Antoniou, P. Udaya and L. Batten. Monitoring employees' emails without violating their privacy right. PDCAT07, The 8th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT07), Adelaide, Dec. 3-6, pp 46-50, 2007.

[C33] A. Mahmood, C Leckie and P. Udaya. A Scalable Sampling Scheme for Clustering in Network Traffic Analysis, INFOSCALE 2007, The Second International Conference on Scalable Information Systems June 6-8, 2007, Suzhou, China, 2007.

[C32]. P. Udaya, S. Narayan and V. Teague. A Secure Electronic Voting Scheme Using Identity based Public Key Cryptography, Proceedings of SAR-SSI 2007, Annecy, France, June 12-16, pp 287-302, 2007.

[C31] P. Lee and P. Udaya. A Secure Protocol for Certified Email with Sender Pseudonymity using Identity Based Encryption, Proceedings of SAR-SSI 2007, Annecy, France, June 12-16, pp 407-410, 2007.

[C30] A. Mahmood, C Leckie and P. Udaya. Echidna: Efficient Clustering of Hierarchical Data for Network Traffic Analysis Proceedings of Networking 2006, Lecture notes in Computer Science, 3976:1092-1098, 2006.

[C29] X. Tang and P. Udaya. New Recursive Construction of Low Correlation Zone Sequences The Second International Workshop on Sequence Design and Its Applications to Communications, October 10-14, Shimonoseki, Yamaguchi, Japan, pp 86-89, 2005.

[C28] X. Wu, M. Kuijper and P. Udaya. On the Decoding radius of Lee-Metric Decoding of Algebraic-Geometric Codes, IEEE International Symposium on Information Theory, Adelaide, September 4-9, pp 1191-1195, 2005.

[C27] X. Tang and P. Udaya. New Construction of Low Correlation Zone Sequences from Hadamard Matrices, IEEE International Symposium on Information Theory, Adelaide, September 4-9, pp 482-486, 2005.

[C26] M. Kuijper, X. Wu and P. Udaya. Behavioral Models over Rings—Minimal Representations and Applications to Coding and Sequences. Proceedings of International Federation Automatic Control Workshop (IFAC-2005), Prague, July 2005, pp 1-6, 2005.

[C25] X.Wu, M. Kuijper and P. Udaya. Improved Decoding of Algebraic-Geometric Codes with Respect to the Lee Metric, Australian Communications Theory Workshop 2005, Brisbane, February 2-4, pp 111-115, 2005.

[C24] X. Tang, P. Udaya and P. Z. Fan. Quadriphase Sequences Obtained from Binary Quadratic Form Sequences. Proceedings of SETA-2004, International Conference on Sequences and Applications, Korea, Lecture notes in Computer Science, Vol 3486, pp 243-254, 2005.

[C23]. X. Tang, P. Udaya and P. Z. Fan. New Families of p-ary Sequences from Quadratic Form With Low Correlation and Large Linear Span. Proceedings of SETA-2004, International Conference on Sequences and Applications, Korea, Lecture notes in Computer Science, Vol 3486, pp 255-265, 2005.

[C22] X. Tang, P. Udaya and P. Fan. Generalized Binary Udaya-Siddiqi sequences. IEEE International Symposium on Information Theory, Chicago, June 27- July 2, pp 84, 2004.

[C21] X. Wu, M. Kuijper and P. Udaya. A Class of Algebraic-Geometric Codes for Lee-Metric and Their Decoding, IEEE International Symposium on Information Theory, Chicago, June 27- July 2, pp 77, 2004.

[C20] P. Udaya, X. Wu and M. Kuijper. List Lee-Metric Decoding Algorithm for Generalized Reed-Solomon Codes Over Communicative Rings with Identity 10th National Conference on Communications (NCC 2004), Bangalore, January 30-February 1, pp. 244-248, 2004.

[C19] P. Udaya, X. Tang and P. Fan. On Connection between Z4 and Quadratic form Sequences. 10th National Conference on Communications (NCC 2004), Bangalore, January 30-February 1, pp. 239-243, 2004.

[C18] X. Wu, M. Kuijper and P. Udaya. On Lee-Metric Decoding of Algebraic- Geometric Codes, Australian Communications Theory Workshop 2004, Newcastle, February 4-6, pp. 82-85, 2004.

[C17] X. Wu, M. Kuijper and P. Udaya. A Lee-Metric Decoding Algorithm for Reed-Solomon Codes over GF(p). 7th International Symposium on DSP for Communication Systems (DSPCS), Coolangatta, December 8-11, pp. 26-31, 2003.

[C16] K. J. Horadam and P. Udaya. A new class of ternary cocyclic Hadamard codes. IEEE International Symposium on Information Theory, Lausanne, July 1-6, pp 175, 2002.

[C15] P. Udaya and S. Bozta¸s. On the Aperiodic Correlation Function of Galois Ring m-sequences. Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of 14th International Symposium, AAECC-14, Melbourne (Selected papers), Australia, Editors S. Bozta¸s and I. E. Shparlinski, Lecture notes in Computer Science, 2227:229-238, 2001.

[C14] P. Udaya and K.J. Horadam. Cocyclic Hadamard Codes from Semifields Proceedings, 2000 IEEE International Symposium on Information Theory, Sorrento, Italy, page 31, 2000.

[C13] P. Udaya. Euclid’s Algorithm and LFSR synthesis. Proceedings, 2000 IEEE International Symposium on Information Theory, Sorrento, Italy, page 420, 2000.

[C12] P. Udaya. Cocyclic Generalized Hadamard Matrices over GF(p^n) and their Related Codes. Proceedings, International Symposium AAECC-13, Honolulu, Hawaii, USA, pages 35–36, 1999.

[C11] A. Bonnecaze, P. Sol´e, and P. Udaya. Strong 4−colored 5−designs. Proceedings, International Symposium AAECC-13, Honolulu, Hawaii, USA, page 112, 1999.

[C10] P. Udaya. Cocyclic Generalized Hadamard Matrices over Abelian Groups. Proc. Joint American and Australian Mathematical Society meeting, Melbourne, Australia, July 11-16, 1999.

[C9] P. Udaya. Designs in Codes over Quarternary Rings. Proc. Joint American and Australian Mathematical Society meeting, Melbourne, Australia, July 11-16, 1999.

[C8] P. Udaya and A. Bonnecaze. Cyclic Codes over a Linear Companion of Z4. Procedings 1998 IEEE International Symposium on Information Theory, Cambridge, Massachusetts, USA, page 398, 1998.

[C7] P. Udaya, H.S. Madhusudhana and M. Sethuraman. An Implementation of Security System Based on Discrete Exponentiation over Finite Fields, Information Security Conference INFOSEC 94, Bangalore, India, 1994.

[C6] P. Udaya, H.S. Madhusudhana and M. Sethuraman. A short note on Indian Corporate Security (Invited), Information Security Conference INFOSEC 94, Bangalore, India, 1994.

[C5]. H.S. Madhusudhana, P. Udaya and M. Sethuraman. Summaries of NIST and Escrow schemes of US, Information Security Conference INFOSEC 94, Bangalore, India, 1994.

[C4] P. Udaya and M. U. Siddiqi. Optimal and Suboptimal Biphase Sequences of Period 2(2r − 1) and Linear Complexity r(r + 3)/2. IEEE International Symposium on Information Theory, San Antonio, Texas, USA, 1993.

[C3] P. Udaya and M. U. Siddiqi. Slow Frequency Hopping Patterns Derived from Polynomial Residue Class Rings. IEEE International Symposium on Information Theory, San Antonio, Texas, January, 1993.

[C2] P. Udaya and M. U. Siddiqi. Sequences over Residue Class Polynomial Rings for Frequency Hopping. Recent Results Session IEEE International Symposium on Information Theory, Budapest, Hungary, June 23-29, 1991.

[C1] P. Udaya and M. U. Siddiqi. Large Linear Complexity Sequences over Z4 for Quadriphase Modulated Communication Systems having Good Correlation Properties. IEEE International Symposium on Information Theory, Budapest, Hungary, June 23-29, 1991.

References: Available on Request.