# Curriculum Vitae

## Udaya Parampalli

---

Professor, School 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 (Ph.D.)** 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 (M.Tech.)** 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 (B.E.)** 1985
Department of Electronics and Communications, Malnad College of Engineering, Hassan, **University of Mysore, India**

### PROFESSIONAL MEMBERSHIP

Senior Member, Institute of Electrical and Electronics Engineers, Inc, Start date: 15, Nov. 1989.

Member, The Institute of Electronics, Information and Communication Engineers, Start date: 23, Feb. 2017.

### CURRENT AND PREVIOUS APPOINTMENTS

| Time | Appointments |
|---|---|
| Jan. 2019 onwards | Professor, Department of Computing and Information Systems, The University of Melbourne, Australia |
| Jan. 2014 to 2018 | Associate Professor and Reader, Department of Computing and Information Systems, The University of Melbourne, Australia |
| 2016 | Visiting Professor, Department of Electrical Engineering, , I.I.T Kanpur, India |
| Sep. 2003 to 2013 | Senior Lecturer, Department of Computing and Information Systems, The University of Melbourne, Australia. |
| Feb. 2000 to Aug. 2003 | Lecturer, Department of Computer Science and Software Engineering, The 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 an interdisciplinary background in Electrical Engineering (Signal Processing and Communications), Mathematics (Coding Theory, Discrete Mathematics) and Computer Science (Algorithms, Cryptography and Networking). He has made strong research contributions in several areas of computer science with an applied mathematics focus. In particular, he is considered a leading international expert in pseudo-random sequence design and coding, and an emerging expert in network security and cryptography.

**RESEARCH INTERESTS**

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

**RESEARCH GRANTS AND PROJECTS**

Udaya Parampalli's research has been supported by research grants from ARC, DIISRTE and The University of Melbourne, totalling more than $2,500,000. They are listed below:

- Secure Big Data Analytics Platforms, with Data61
    - U Parampalli, Data61 - SSA – Contract- A Robust and Reliable Tele-medical data Security and Authentication System using Spread Spectrum Steganography, 2017.
    - U Parampalli, Data61 - SSA – Contract- On the design of private, anonymous and trustless protocols in public blockchains, 2017.
- C, Leckie, A. Ahmad, R. Kotagiri, U. Parampalli, S. Karunasekera, B Rubinstein, V. Teague, T. Alpan, T. McCormack and M. Palaniswami,, Academic Centres of Cyber Security Excellence (ACSE) program, Department of Education and Training, $950,287.
- 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.
- M. Kuijper 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 $24,222.

**RESEARCH STUDENT SUPERVISION**

**Mentoring Post-Doctoral Research Associates.**

1. Dr. Arunthavanathan Senthuran, 2016-2017.
2. Dr. Akram Hourani, 2016, now lecturer at RMIT University.
3. Dr. Rong Liu, 2014-2015, Southwest Jiaotong University, supported by China Scholarship Council.
4. Dr. Shuxia Ma, 2015-2016, Southwest Jiaotong University, China Scholarship Council.
5. Dr. Xinwen Wu during 2002-2004, who is now a senior lecturer at Griffith University, Queensland.
6. Dr. Silvana Medos, now a tutor at RMIT University.

**Current Research Higher Degree (RHD) (PhD and Masters by Research) Students (Primary Supervision)**.

1. Ge Yang (Ph.D, topic: Authentication of devices for Internet of Things, co-supervisor Dr. Vanessa Teague).
2. Peter Eze (Ph.D, topic: Novel Information Hiding Through Spread Spectrum Steganography, co-supervisor Prof. Rob Evans).
3. Renlord Yang (Ph.D, topic: Trust-less protocols and the design of next generation decentralized, private, anonymized applications on public blockchains, co-supervisor Dr. Toby Murray).
4. Patrick Vicky (Ph.D, topic: Novel Information Hiding Schemes, co-supervisor Prof. Rob Evans).
5. Partha De (Ph.D, topic: Design of Side-Channel Resistant Light Weight Cryptography, MIPP Student co-supervisor Dr. Chittaranjan Mandal (I.I.T Kharagpur)).
6. Lakshmi Jagathamma Mohan (Ph.D, topic: Secure Repair in Large Scale Distributed Storage Systems , co-supervisor Dr Aaron Harwood), **Submitted awaiting examination reports.**

**Current Research Higher Degree (RHD) (PhD and Masters by Research) Students (Co-Supervision)**.

1. Kim Ramchen (Ph.D, topic:Privacy Preserving Genomics, co-supervision with Dr. Vanessa Teague).
2. Nicholas Akinyokun (Ph.D, topic:Secure voter registration and eligibility checking for Nigerian elections, co-supervision with Dr. Vanessa Teague).
3. Leyla Roohi (Ph.D, topic:Privacy-preserving computations for Australian metadata, co-supervision with Dr. Vanessa Teague).
4. Shuo Wang (Ph.D, topic: Differentially Private Data Aggregation Methods and Application for Social Systems Data Analysis and Visualization, co-supervision with Professor Richard O. Sinnott), Submitted awaiting examination reports, **Submitted awaiting examination reports.**
5. Yang Lu (Ph.D, topic: Semantic-based Trust Management in Clinical Collaborations, co-supervision with Professor Richard O. Sinnott)**, Submitted awaiting examination reports**.

**Current Visiting PhD Students: None**

**Past Visiting PhD Students.**

1. Wei Wu (Ph.D, topic: Privacy preserving data mining in cloud computing environment, Visiting Student from NUDT, China co-supervisor Ming Xian), 2016-17.
2. Qifa Yan (Ph.D, topic: Coded Cashing, Visiting Student from SouthWest Jiao Tong University, China co-supervisor Xioahu Tang), 2016.
3. Kun Huang (Ph.D, topic: Secrecy Capacity of Distributed Storage Codes, Visiting Student from NUDT, China co-supervisor Ming Xian), 2015-16.
4. Shi-Feng Sun (Ph.D, topic: Non Malleable Public key Cryptography, Visiting Student from Shanghai Jiao Tong University, China co-supervisor Dawu Gu),2016-17.

**Completed RHD research students/Students with submitted thesis.**

1. Qifa Yan (Ph.D, topic: Coded Cashing, Visiting Student from SouthWest Jiao Tong University, China co-supervisor Xioahu Tang), 2017.

2. Kun Huang (Ph.D, topic: Secrecy Capacity of Distributed Storage Codes, Visiting Student from NUDT, China co-supervisor Ming Xian), 2017
3. Shi-Feng Sun (Ph.D, topic: Non Malleable Public key Cryptography, Visiting Student from Shanghai Jiao Tong University, China co-supervisor Dawu Gu), 2017, now a post-doctoral fellow at CHUK, Hong Kong
4. Zilong Liu, Visting Student from NTU (2014), co-supervision with A/Prof. Guan Yong Liang, now a Research Fellow, School of Electrical & Electronic Engineering, Nanyang Technological University (NTU), Singapore.
5. Janaka Weerathunga Yapa Seneviratne (Masters 2014), co-supervision with A/Prof. L. Kulik.
6. Kim Ramchen (Masters 2011), Thesis: Electronic Voting, co-supervision with Dr. V. Teague.
7. Dr. Peter Hyun Jeen LEE (PhD 2011), Thesis: Identity-based Encryption and its Applications using Bilinear Maps, was a Post doctoral Scholar, University of New Castle, United Kingdom, now Security consultant at Optimal Payments Plc, Calgary.
8. 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.
9. Dr. Shivaramakrishnan Narayan (PhD 2009), Thesis: Secure Identity-based Signatures and Signcryptions Using Pairing, now with Optimal Payments Plc, Calgary, Alberta, Canada.
10. 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.
11. Ana Jancic (Masters 2009- Deakin University), Thesis: Authentication in Public Key Encryption Schemes.
12. Andrew J. Newlands (Masters 2004), Thesis: On Cryptanalysis of steam ciphers.

**Minor Thesis Students (MSc (Computer Science)-75 point, MIT-25 point) (Selected Examples)**

1. Bumsik Ahn, MIT, topic: Analysis of malware for cloud-based mobile devices), 2015.
2. Rahul Sharma, MIT, topic: Software Architecture for Cloud Storage, 2015.
3. Johanes Gunawan Siregar, MIT, topic: Software Architecture for Cloud Storage, 2015.
4. César Martinez D'Granda, MIT, sensor network communication scenario for Smart Grid Electricity, 2015.
5. Hongyu Liang, MIT, topic: various vulnerabilities of SSH protocol, 2015.
6. Ai Jian, MIT, topic: Relative performance of SSL and TLS against various popular attacks, 2015.
7. Wenjiw Shen, MIT, topic: Cryptographic method to store user data on website, 2016.
8. Shangzhi Yang, MIT, topic: Exploring the parallelism of SHA-3 families, 2016, Semester 1.
9. Renlord Yang, MSc(CS), topic: Safe acceptance of zero-confirmation transactions in Bitcoins, 2016.

**UNIVERSITY TEACHING**

He has designed and developed several subjects over 17 years in the areas of algorithms networks, cryptography and security. He designed the subject "Applied and Cryptography coding" in 2001, revised in 2008, and with the introduction of the Melbourne model he redesigned the subject with the name Applied Cryptography and Security.

In 2008, after returning from sabbatical in Canada, he redesigned the "Algorithms and Data structures" subject by utilizing the results from mathematical recursion in parallel with the algorithmic recursion usually employed in computer science.

**Subjects**

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

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.

He mentored Dr. Masud Mushtagi (In 2015 and 2016 Semester 2) and Chien Aun Chanto (In 2017) to teach and deliver COMP90007.

**Subjects Developed**

He has developed two new subjects "Applied Cryptography and Coding" and "Cryptography and Security" after joining the University of Melbourne. he developed new material for Networks Communications and Algorithms and Data Structures subjects. In 2009, he developed a new subject called "Cryptography and Security" as a post graduate subject addressing the "*Nine principles guiding teaching and learning"*, CSHE report, University of Melbourne. The proposed subject requires a background in mathematics and a postgraduate standing in computing.

**PROFESSIONAL SERVICE**

**General Program Committee Chair:**

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

**General Chair and Steering Committee member:**

- Australasian Information Security Conference (ACSW-AISC) 2018, January 30 – 2 February, 2018, Brisbane, Australia.

**Guest Editor:**

- Topical section on Sequences and Applications, the Journal of Cryptography and Communications, 2016.
- Special Section on Signal Design and Its Applications in Communications, IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2016.

**Program Committee Co-Chair:**

- The Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA'17), September 24-28, 2017, Hokkaido University, Sapporo, Japan.
- 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.

**Thesis Reviews**: I have reviewed 22 Ph.D. and 3 master's theses in the area of mathematics, coding, cryptography, security.

**LEADERSHIP**

Udaya Parampalli is a world leader in sequences research and has been regular reviewer of journals and conferences in the area. He was the general chair of SETA-2014 (see above) and a program chair of two international conference series devoted to area of sequences and coding: SETA and IWSDA.

He is the chairman of the Technical Program Committee of 16th Australasian Conference on Information Security and Privacy Melbourne, Australia (ACISP 2011) and a member of program committee in ACSIP for many years.

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

Udaya Parampalli leads accreditation activities in the School of Computing and Information systems. He coordinated the Computing and Information System Department's 2013 and 2018 accreditation submissions for its degrees with Engineers Australia (EA) and the Australian Computing Society (ACS).

**RESEARCH TARINING ENGAGEMENT**

- Leader of the "IITK engagement" in the Melbourne-India Postgraduate Program (http://mipp.unimelb.edu.au/).
- Organized MIPP conference at IIT Kanpur, April 2015.
- Organized MIPP conference, Melbourne, January 2017.
- Organized CSC2017, a research conference of participating universities in the IRRTF research network and new international experts in coding area.

**SERVICE TO THE UNIVERSITY**

**Accreditation:** He leads the School of CIS in professional accreditation activities

- Led 2018 and 2013 accreditation process for the Engineers Australia (EA) and the Australian Computing Society (ACS) accreditation leading to professional accreditation of ME, MIT and MIS courses.
- Organized ACS graduate interviews on 11th May 2016 for the ACS accreditation team, leading to full professional accreditation of the Master of Information Technology (MIT) course.
- I coordinated activities for submission for the EUR-ACE accreditation of Engineering degrees leading successful accreditation.
- Led again renewal of ACS-EA accreditation visit for ME, MIT and MIS courses. Organized MIPP conference, Melbourne, January 2017.
- Also initiated first time successful submission of CIS undergraduate majors (B.Sc(Computing and Software Systems) and BDES(computing)) for ACS accreditation. The programs have been accepted to receive accreditation at the exit meetings with conditions.

**Officer for Academic Honesty.** Chair School process on handling academic honesty issues.

**Other Service**

- Department's Timetable coordinator from 2003 to 2011.
- Member of Safety Committee from 2006 to 2007

***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. Presented a short Course on "Codes for Distributed Storage", organized by Department of Electrical Engineering, IIT Kanpur and supported by MHRD under GIAN (Global Initiative of Academic Networks), India.
2. Keynote speaker: International Forum on Advances in Information Coding and Wireless Communications 2013, Chengdu, China,
3. Keynote presentation, "Cryptographic Solutions for Cloud Security", the International Symposium on Cloud and Services Computing, Surathkal, India, December 16-19, 2012.
4. 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.
5. Plenary Talk, "Low Correlation Zone Sequences over Finite Fields and Rings", IWSDA 2009, Fukuoka, Japan, October 19-23, 2009.
6. Invited talk, "Low Correlation Zone Sequences", Workshop on Sequence Design and Its Applications in Communications and Cryptography, 4-6 December, Melbourne, 2008.
7. 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 2013 to September 2013: Visited Prof. Guang Gong, University of Waterloo, Canada.
2. September 2013 to October 2013: Visited Xioahu Tang, SouthWest Jiatong University, China.
3. July 2008 to December 2008: Visited Prof. Rei Safavi-Naini and Prof. Hugh Williams Department of Computer Science, University of Calgary, Alberta, Canada.
4. December 27, 2008 to January 14, 2009, Visited Prof. Pinghi Fan, SouthWest Jiatong University, China.
5. December 2010, Visited Prof. C. Ding and Dr. W.H. Mow, Hong Kong University of Science and Technology, Hong Kong.
6. December 2011 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: 52 in career, 6 under review.
- Papers in refereed conference proceedings: 84 in career.
- Google Scholar Citations as of April 2018: 1465, 742 since 2013.
- h-index:19 i10-index:31
- Each entry is followed by ERA Rank information if available and the percentage of my contribution to the publication.

**Journal Impact Metrics for top most journals among the publications:**

| **Journal** | **Number** | **Cite-score** | **Citescore Rank with category** | **Citescore Percentile ($99^{th}$=top)** | **JIF Impact Factor** | **Category JIF** | **JIF Quartile** | **JIF Ranking In Category** |
|---|---|---|---|---|---|---|---|---|
| IEEE Transactions on Information Theory | **22** | **3.14** | **#11/194. Libr. & Info. Sc.** | **94th** | **2.679** | **Comp. Sc., Info. Systems** | **Q2** | **43 of 146** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Same as above | **ditto** | **ditto** | **#78/513, Info. Systems** | **85th** | **2.679** | **Eng. Elec.&Elect** | **Q2** | **74 of 262** |
| Designs Codes and Cryptography | **2** | **1.09** | **#161/398 Appl. Maths** | **59th** | **1.009** | **Maths. Appl.** | **Q2** | **109 of 255** |
| IEEE Transactions Communication | **1** | **5.26** | **#33/642 Elec.&Elec. Engg** | **94th** | **4.058** | **Eng. Elec.&Elect** | **Q1** | **33 of 262** |
| IEEE Transactions on Knowledge and Data Engineering | **1** | **5.40** | **#17/513 Comp Sc. Appl.** | **96th** | **3.438** | **Comp. Sc., Info. Systems** | **Q1** | **21 of 146** |

**Edited Book of Conference Proceedings**

[B8] K-U Schmidt and U Parampalli, Special Issue on Sequences and Their Applications, Topical Collections, Journal of Cryptography and Communications, Discrete Structures, Boolean Functions and Sequences, ISSN: 1936-2447 (Print) 1936-2455 (Online), 2017. [equal authors]

[B7] Hideyuki Torii, Xiaohu Tang and Udaya Parampalli. Proceedings of 2017 International Workshop on Signal Design and Its Applications in Communications (IWSDA), September 24-28, 2017, Sapporo, Hokkaido, Japan, IEEE Press, 199 pages, 2017. [equal authors]

[B6] 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. [equal authors]

[B5] 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, 201. [equal authors]

[B4] 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. [equal authors]

[B3] 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. [equal authors]

[B2] 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.

[B1] Pinghi Fan, Parampalli Udaya, Xiaohu Tang and Naoki Suehiro. Proceedings of 2007 International Workshop on Signal Design J39]and Its 40] mmunications (IWSDA07), September 23-27, 2007, Chengdu, China, IEEE Press, 385 pages, 2007. [equal authors]

**Book Chapters**

[B2] 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: Vol. 7 Communications and Radar Signal Processing, Sergios Theodoridis, Rama Chellappa (ed.), Academic Press, United States, pp. 317-363, 2017. [equal authors]

[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. [equal authors]

**Journals**

[J53] P. Tan, Z Zhou, H Yan and U. Parampalli. Optimal Cyclic Locally Repairable Codes Via Cyclotomic Polynomials, IEEE Trans. Inform. Theory, Vol 57, Issue 6, pp 3831-3840, 2011. [Rank A*, equal authors]

[J52] K. Huang, U. Parampalli, M. Xian, Improved Upper Bounds on Systematic-Length for Linear Minimum Storage Regenerating Codes, Accepted October 26, 2018, IEEE Trans. Information Theory. [Rank A*, Supervisor]

**[**J51] Z Zhou, T Helleseth and U. Parampalli. A Family of Complex Roots of Unity Sequences with Asymptotically Optimal Correlation, IEEE Transactions on Information Theory, Vol 64, Issue 4, pp 2896 - 2900, 2018. [Rank A*, equal authors]

[J50] P. Eze, P. Udaya, R. Evans, "Medical Image Watermark and Tamper Detection Using Constant Correlation Spread Spectrum Watermarking". World Academy of Science, Engineering and Technology, International Science Index 135, International Journal of Computer, Electrical, Automation, Control and Information Engineering, 12(3), 107 – 114, 2018, Digital Article Identifier (DAI) http://scholar.waset.org/1307-6892/10008924. [equal authors]

[J49] Z. Liu, Y. L. Guan, U. Parampalli, and S. Hu, Spectrally-Constrained Sequences: Bounds and Constructions, IEEE Transactions on Information Theory, Vol 64, Issue 4, pp 2571 - 2582, 2018. [Rank A*, equal authors]

[J48] L. J Mohan, P. I. S. Caneleo, U Parampalli and Aaron Harwood, Geo-aware erasure coding for high-performance erasure-coded storage clusters, Annals of Telecommunications, Volume 73, Issue 1-2, pp 139–152, February 2018. [Supervisor]

[J47] R. Luo and U. Parampalli, Cyclic codes over M2(F2+uF2), Journal Cryptography and Communications, pp 1–9, Special Issue on Sequences and Their Applications, https://doi.org/10.1007/s12095-017-0266-1, Springer US, 2017. [equal authors]

[J46] S.F Sun, D. Gu, U. Parampalli, Y. Yu and B. Qin. Public key encryption resilient to leakage and tampering attacks. Journal of Computer and System Sciences, pp 142-156, Vol 89, 2017. DOI: 10.1016/j.jcss.2017.03.004 [Rank A*, Supervisor]

[J45] H. Han, D. Peng , U. Parampalli, Z. Ma, and H. Liang. Construction of low-hit-zone frequency hopping sequences with optimal partial Hamming correlation by interleaving techniques. Designs, codes and Cryptography, 84(3): 401 - 414, September 2017. [Rank A, Supervisor]

[J44] H. Han, D. Peng and U. Parampalli. New sets of optimal low-hit-zone frequency-hopping sequences based on m-sequences. Cryptography and Communication 9(4): 511 –522, June 2017. DOI:10.1007/s12095-016-0192-7[Supervisor]

[J43] Q. Yan, U. Parampalli, X. Tang, Q. Chen, Online Coded Caching with Random Access. IEEE Communications, 21(3):552 - 555, 2017. DOI:10.1109/LCOMM.2016.2631552. [Supervisor]

[J42] K. Huang, U. Parampalli, M. Xian, On Secrecy Capacity of Minimum Storage Regenerating Codes, IEEE Trans. Information Theory 63(03): 1510-1524, 2017. [Rank A*, Supervisor]

[J41] Luo Rong, Udaya Parampalli, Self-Dual Cyclic Codes over Z4+uZ4 , IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E100-A No.4 pp. 969-974, 2017. [Rank C, equal authors]

[J40] K. Huang, U. Parampalli, M. Xian, Security Concerns in Minimum Storage Cooperative Regenerating Codes. IEEE Trans. Information Theory 62(11): 6218-6232, 2016. [Rank A*, Supervisor]

[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. [Rank A*, equal authors]

[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. [Rank A*, Supervisor]

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

[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. [Supervisor]

[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. [Rank A*, Supervisor]

[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. [Supervisor]

[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. [Supervisor]

[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. [Rank A*, equal authors]

[J31] Z Zhou, X Tang, X. Niu and U. Parampalli. New Classes of Frequency Hopping Sequences with Optimal Partial Correlation, IEEE Trans. Inform. Theory, Vol 58, Issue 1, 453 - 458, 2012. [Rank A*, equal authors]

[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. [Rank A*, equal authors]

[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. [Rank B, equal authors]

[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. [Rank A*, equal authors]

[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. [Rank A*, equal authors]

[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. [Rank B, equal authors]

[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. [Rank C, equal authors]

[J24] X. Tang and U. Parampalli. On the Noncyclic Property of Sylvester Hadamard Matrices, IEEE Trans. Inform. Theory, Vol 56, Issue 9, pp 4653-4658, 2010. [Rank A*, equal authors]

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

[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. [equal authors]

[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. [equal authors]

[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. [Supervisor]

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

[J18] M. Abdun, C. A. Leckie, C 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. [Rank A, Supervisor]

[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. [Rank B, Supervisor]

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

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

[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. [equal authors]

[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. [Rank A*, equal authors]

[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. [Rank A*, equal authors]

[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. [Rank A*, equal authors]

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

[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. [Rank A, equal authors]

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

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

[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. [Rank B, equal authors]

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

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

[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. [Rank A*, equal authors]

[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. [Rank A*, equal authors]

[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. [Rank A*, equal authors]

**International Conference Proceedings**

Pan Tan, Zhengchun Zhou, Haode Yan and Udaya Parampalli

[C85] Ge Yao and U. Parampalli, Transformation algorithm for NLFSRs in hardware-oriented stream cipher, In the Proceedings of SETA-2018, International Conference on Sequences and Applications, Hong Kong, October 1-6, 2018.[Supervisor]

[C84] P. Eze, U. Parampalli, R. Evans, D. Liu, “Spread Spectrum Steganographic Capacity Improvement for Medical Image Security in Teleradiology”, (Accepted Date April 9, 2018), To appear at 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Honolulu, Hawaii, USA, 17th – 21st July 2018. [Supervisor]

[C83] Y Lu, RO Sinnott, K Verspoor, U Parampalli, “Privacy-Preserving Access Control in Electronic Health Record Linkage”, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), pp 1079-1090, 2018.

[C82] Ge Yao and U. Parampalli, ``Improved Sprout Cipher to Resist the Divide and Conquer based Key Recovery Attack," In the Proceedings of Australasian Information Security Conference (AISC 2014), Australasian Computer Science Week, (Accepted Date November 2017), January 2018, Brisbane, Australia. [Supervisor]

[C81] P. U Eze, U. Parampalli and R.J Evans “Medical Image watermark and Tamper Detection using Constant Correlation Spread Spectrum Watermarking” [accepted to appear in] ICDSP 2018: 20th International Conference on Digital Signal Processing, Berlin, Germany, 21-22nd May, 2018. [Supervisor]

[C80] Hourani, A.,Evans, R.,Moran, W.,Sithamparanathan, K.,Parampalli, U, Efficient range-doppler processing for random stepped frequency radar in sutomotive applications In: Proceedings of the IEEE 85th Vehicular Technology Conference (VTC 2017), Sydney, Australia, 4-7 June 2017. [equal authors]

[C79] P. U. Eze, U Parampalli., U.C Iwuchukwu and N.Onuekwusi “Challenges and Prospects of Blind Spread Spectrum Medical Image Watermarking” In Proceedings of 3rd IEEE International Conference on Electro-Technology for National Development, Federal University of Technology, Owerri, Nigeria, pp. 10 - 18 , Nov 7 -10, 2017. [Supervisor]

[C78] P. Vicky and U. Parampalli, ``Novel Authentication Scheme with Pseudorandom Sequences in the Frequency Domain of Images," in Proceedings of the Eighth International Workshop on Signal Design and Its Applications in Communications (IWSDA'17), pp. 140-144, 2017 © IEEE [Supervisor]

[C77] S. Raghavan, S.V Raghavan and U. Parampalli. Re-Engineering Simultaneous Internet Sessions Process-separated Browsers. 2017. DOI:10.1145/3014812.3014884 [10%]

[C76] 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. [Supervisor]

[C75] T. Kojima, T. Tachikawa, A. Oizumi, Y. Yamaguchi and U Parampalli, Tone code: A novel method for covert communications based on musical components, In the Proceedings of 2016 International Symposium on Information Theory and its Applications (ISITA 2016), pp. 335-339, 2016. [equal authors]

[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. [Supervisor]

[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, 12th International Conference on the Design of Reliable Communication Networks (DRCN16), IEEE Press, pp 123-129, Paris, March 15-17, 2016. [Supervisor]

[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. [Supervisor]

[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. [equal authors]

[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. [Supervisor]

[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. [Supervisor]

[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. [equal authors]

[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. [Supervisor]

[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. [Supervisor]

[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. [Supervisor]

[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. [Supervisor]

[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. [equal authors]

[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. [equal authors]

[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. [Supervisor]

[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. [Supervisor]

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

[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. [equal authors]

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

[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. [equal authors]

[C55] T. Matsumoto, S. Matsufuji, 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 Conference on Information Technology and Ocean Engineering (CICC-ITOE2011), Macau, China, March 5-6, Vol. 2, pp.66-70, 2011. [equal authors]

[C54] T. Kojima, N. Ohtani, T. Matsumoto, U Parampalli. On Multiple Information Embedding by Digital Watermarking 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. [equal authors]

[C53] O. Moreno, 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. [equal authors]

[C49] 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. [equal authors]

[C48] 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. [equal authors]

[C47] 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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [Supervisor]

[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 Communication), July 26-29, pp .306-311, 2008. [Supervisor]

[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. [Supervisor]

[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. [equal authors]

[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. [Supervisor]

[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. [Supervisor]

[C37] S. Boztas 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. [equal authors]

[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. [Supervisor]

[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. [Supervisor]

[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. [Supervisor]

[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. [Supervisor]

[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. [equal authors]

[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. [Supervisor]

[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. [Supervisor]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[C15] P. Udaya and S. Boztas. 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. [equal authors]

[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. [equal authors]

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

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

[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. [equal authors]

**Other Publications**

[O1] S T Kojima, X Tang, U Parampalli, Forward to Special Section on Signal Design and Its Applications in Communications, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2017. [equal authors]

[O2] T. Kojima, X. Tang and U. Parampalli. Special Section on Signal Design and Its Applications in Communications FOREWORD. Oxford University Press, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E100A (4). 2017. [equal authors]