

National Institute of Technology, Tiruchirappalli: Performa for CV of Faculty/ Staff Members

station (CRS)-Programme			
Member, M.Tech project committee	CSE Department	July 2016	May 2016

10. Academic/Administrative Responsibilities outside the University

Position	Institution	From	To
Reviewer of question papers	Pondicherry University	18th October	
External Examiner for comprehensive examination	NIT Karaikal	30th November	

11. Awards, Associateships etc.

Year of Award	Name of the Award	Awarding Organization
2013	Best Paper Award	International conference MIST 2013 held in Busan, South Korea.

12. Fellowships: None

Year of Award	Name of the Fellowship	Awarding Organization	From (Month/Year)	To (Month/Year)

13. Details of Academic Work

- (i) Curriculum Development
Designed the following courses:
UG Level: 1. Principle of cryptography 2. Advanced Cryptograph
2. Discrete structure
PG Level: Mathematics foundation of computer science
- (ii) Courses taught at Postgraduate and Undergraduate levels:
Data Structure
Design and analysis of Algorithm
Automata and Formal Languages
Combinatorics and Graph Theory
Discrete Mathematics
Principles of cryptography
C- Language
Database Management Systems
Information security
Computer graphics
Computer Organisation

National Institute of Technology, Tiruchirappalli: Performa for CV of Faculty/ Staff Members

- (iii) Projects guided at Postgraduate level: 15 PG projects
- (iv) Other contribution(s)

14. Details of Major R&D Projects: None

Title of Project	Funding Agency	Duration		Status
		From	To	Ongoing/ Completed

15. Number of PhDs guided: None

Name of the PhD Scholar	Title of PhD Thesis	Role(Supervisor/ Co-Supervisor)	Year of Award

16. Participation in Workshops/ Symposia/ Conferences/ Colloquia /Seminars/ Schools etc. (mentioning the role)

Date (s)	Title of Activity	Level of Event (International/ National/ Local)	Role (Participant/ Speaker/ Chairperson, Paper presenter, Any other)	Event Organized by	Venue
September 23 rd 2016	National Conclave on Network Security and Cryptography	National	Invited Speaker	Department of Computer Applications, Saintgits College of Engineering, Kottayam, Kerala.	

17. Workshops/ Symposia/ Conferences/ Colloquia/Seminars Organized (as Chairman/ Organizing Secretary/ Convenor / Co-Convenor)

Title of Activity	Level of Event (International/ National/ Local)	Date (s)	Role	Venue
Introduction to Cryptography	National Level	30 th May to 4 th June 2016	Organizing Secretary	NIT Trichy

National Institute of Technology, Tiruchirappalli: Performa for CV of Faculty/ Staff Members

--	--	--	--

18. Invited Talks delivered

Topic	Date	Inviting Organization
Provable secure encryption scheme	15 th September 2016	Department of Computer Science and Engineering, PSGCollege of technology Coimbatore
Mathematical foundation on Cryptography	30 th May 2016	Department of Computer Science and engineering, NIT Trichy
Public Key Cryptography	5 th August 2016	Department of Computer Science and engineering, NIT Trichy
RECENT TRENDS IN CRYPTOGRAPHY	5 th November 2015	Department of Computer Science and engineering, Thiagarajar College of Engineering, Madurai, Tamilnadu

19. Membership of Learned Societies

Type of Membership (Ordinary Member/ Honorary Member / Life Member)	Organization	Membership No. with date
Life Member	Cryptology Research Society of India	417

20. Academic Foreign Visits

Country	Duration of Visit	Programme
Japan	November 8-9	To present a paper in international conference MIST 2012 held in Fukuoka, Japan.
South Korea	October 24-25	To present a paper in international conference MIST 2013 held in Busan, South Korea.
Indonesia	April 14-17	To present a paper in international conference AsiaARES 2014 held in Bali, Indonesia.

21. Publications

(A) Refereed Research Journals:

Author(s)	Title of Paper	Journal	Volume	Page	Year	Impact Factor of the Journal

**National Institute of Technology, Tiruchirappalli:
Performa for CV of Faculty/ Staff Members**

			(No.)	numbers		(Optional)
Kunwar Singh, C.Pandu Rangan, A.K.Banerjee	Lattice Based Identity Based Resplittable Threshold Public Key Encryption Scheme	International Journal of Computer Mathematics	93	289-307	2016	.577
Kunwar Singh, C. Pandu Rangan, A. K. Banerjee	Lattice Based Mix Network for Location Privacy in Mobile System	Mobile Information Systems	2015		2015	1.462
Kunwar Singh, C. Pandu Rangan, A. K. Banerjee	Lattice Based Universal Re-encryption for Mixnet	Journal of Information Science and Information Security (JISIS)	4	1-11	2014	
Kunwar Singh, C. Pandu Rangan, A. K. Banerjee	Lattice Based Identity Based Proxy Re-Encryption Scheme	Journal of Information Science and Information Security (JISIS)	3	38-51	2013	
Kunwar Singh, C. Pandu Rangan, A. K. Banerjee	Lattice based efficient threshold public key encryption scheme	Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (jowua)	4	93-107	2013	
Kunwar Singh, C. Pandu Rangan, A. K. Banerjee	Lattice Based ForwardSecure Identity Based Encryption Schemes with Shorter Ciphertext	Journal of Information Science and Information Security (JISIS)	3	5-19	2013	
Kunwar Singh, C. Pandu Rangan, A. K. Banerjee	Lattice Based ForwardSecure Identity Based Encryption Schemes	Journal of Information Science and Information security (JISIS)	2	118- 128	2012	

(B) Conferences/Workshops/Symposia Proceedings

Author(s)	Title of Abstract/ Paper	Title of the Proceedings	Page numbers	Conference Theme	Venue	Year
Kunwar Singh, C. Pandu Rangan, A. K. Banerjee	Lattice based Identity based Unidirectional Proxy Re-Encryption Scheme	Springer International Publishing	76-91	International Conference on Security, Privacy, and Applied Cryptography Engineering	IIT Kharagpur, India	2014
Kunwar Singh, C. Pandu Rangan, A. K. Banerjee	Efficient Lattice HIBE in the Standard Model with Shorter Public Parameters	Springer Berlin Heidelberg	542-553	Information and Communication Technology-EurAsia Conference	Bali, Indonesia	2014
Kunwar Singh, C. Pandu Rangan, A. K. Banerjee	Cryptanalysis of Unidirectional Proxy Re-Encryption Scheme	Springer Berlin Heidelberg	564-575	Information and Communication Technology-EurAsia Conference	Bali, Indonesia	2014
Prashant Kumar Mishra, Kunwar	ID-Based Threshold Signcryption and	Springer Berlin Heidelberg	35-44	International Conference on	Trivendrum, India	2012

National Institute of Technology, Tiruchirappalli: Performa for CV of Faculty/ Staff Members

Singh, Sudhanshu Baruntar	Group Unsignryption			Security in Computer Networks and Distributed Systems		
Kunwar Singh, C. Pandu Rangan, A. K. Banerjee	Adaptively Secure Efficient Lattice (H)IBE in Standard Model with Short Public Parameters	Springer Berlin Heidelberg	153-172	Security, Privacy, and Applied Cryptography Engineering	Chennai, India	2012
Kunwar Singh	Identity based signcrytion revisited	IEEE	1-7	International Conference on Information Technology and e- Services (ICITeS'2012)	Sousse, Tunisia	2012

(C) Books & Monographs: None

Author(s)	Title of Book/Monograph	Name of Publishers	Year of Publication	ISSN/ISBN Number