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

Curriculum Vitae

Brief Profile: 1-2 paragraphs (not exceeding 500 words)

1. Name: Dr. Kunwar Singh
2. Designation: Assistant professor
3. Office Address: 205,CSE Department, NIT Trichy
4. Telephone (Direct) (Optional):

   Telephone : 0431-250 Extn 3212
   (Optional):

   Mobile (Optional):
5. Email (Primary): kunwar@nitt.edu Email (Secondary) : kunwar20812gmail.com
6. Field(s) of Specialization: Cryptography

7. Employment Profile :

Job Title	Employer	From	To
Lecturer	AEC Agra, SGI group	August 2004	August 2006
Assistant Professor	NIT Trichy	September 2006	Till now

8. Academic Qualifications (From Highest Degree to High School):

Examination	Board / University	Year	Division/ Grade	Subjects
PhD	IIT Madras	2015	CGPA-8.25	Computer Science
MTech	JNU New Delhi	2001	First / 6.9	Computer Science
BTech	IIT Delhi	1995	CGPA-4.4	Mechanical Engineering
10+2	GIC Chhinka	1989	Second/59%	Maths, Physics, Chemistry
10th	GIC Chhinka	1987	First/61	Maths, Science, English

9. Academic/Administrative Responsibilities within the University

Position	Faculty/Department/ Centre/Institution	From	To
Member, anti-ragging Committee	NIT Trichy	July 2016	

Member, Community Radio station (CRS)-Programme	NIT Trichy	November 2016	
Member, MTech 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)
2017	B.Tech students	TCS Best B.Tech project award	2017	

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

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

14. Details of Major R&D Projects:

Title of Project	Funding Agency	Duration		Status
		From	To	Ongoing/ Completed
Research and Development of Lightweight Stream Cipher	DST	January 2018	January 2021	Ongoing
Funding Agency for the Project specimen	SERB	2nd Feb 2022	Feb 2025	Ongoing

15. Number of PhDs guided:

Name of the PhD Scholar	Title of PhD Thesis	Role(Supervisor/ Co-Supervisor)	Year of Award
Koteswararao CH	Secure Multi-party Computation	Supervisor	2021

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 23rd 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	Date (s)	Role	Venue

	(International/ National/ Local)			
Introduction to Cryptography	National Level Workshop	30th May to 4th June 2016	Organizing Secretary	NIT Trichy
Cryptology (NWC 2017)	National Level Conference	28th to 30th September 2017	Organizing Secretary	NIT Trichy
Blockchain and Smart Contract Technologies 2019 (BSCT 2019)	National Level Conference	7th to 10th November	Organizing Secretary	NIT Trichy
Blockchain and Smart Contract Technologies 2021 (BSCT 2021)	National Level Workshop	25th to 29th June 2021	Organizing Secretary	NIT Trichy
Introduction to Cryptography	National Level Workshop	24th to 28th November 2021	Organizing Secretary	NIT Trichy

18. Invited Talks delivered

Topic	Date	Inviting Organization
Technical talk on \Bitcoin Wallet International Conference on Current Trends in Advanced Computing (ICCTAC 2020)	6th to 07th May 2020	Bangalore
Tutorial talk on \Bitcoin ". National Conference on Blockchain and Smart Contract Technologies 2019 (BSCT 2019)	7th to 10th November 2019.	NIT Trichy

\Elliptic curve cryptosystem. National Conclave on Network Security and Cryptography.	September 23rd2016.	Department of Computer Applications, Saintgits College of Engineering, Kottayam, Kerala.
Provable secure encryption scheme	15th September 2016	Department of Computer Science and Engineering, PSGCollege of technology Coimbatore
Mathematical foundation on Cryptography	30th May 2016	Department of Computer Science and engineering, NIT Trichy
Public Key Cryptography	5th August 2016	Department of Computer Science and engineering, NIT Trichy
Recent Trends In Cryptography	5th 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
Life Member	IEEE	

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.
Australia	December 10--14	To present a paper in international conference ISPEC/MONAMI 2017 held in Melbourne, Australia.
Philippines.	October 21-23	To present a paper in international conference MobiSec 2018 held in Cebu, Phillipines.

21. Publications

(A) Refereed Research Journals:

Author(s)	Title of Paper	Journal	Volume (No.)	Page numbers	Year	Impact Factor of the Journal (Optional)
Kunwar Singh , Karthika S K,	Theoretical Analysis of Biases in TLS En cryption Scheme Chacha 128	Int. J. of Ad Hoc and Ubiquitous Computing (IJAHUC) (SCI)			2022	
Kunwar Singh, KKC Deepti, S. K. Karthika	Improved related-cipher attack on Salsa and ChaCha	International journal information technology, Springer.			2022	
Kunwar Singh Ch Koteswara Rao.	Oblivious Stable Sorting Protocol and Oblivious Binary Search Protocol for Secure Multi-party Computation	Journal of High Speed Networks.			2021	
Kunwar Singh, S Mercy Shalinie, Dharani J, K	A PrivacyPreserving Framework for	Computers Security,			2022	

Sundarakantham,	Endorsement Process in Hyperledger Fabric					
Kunwar Singh, C. Pandu Rangan, Richa Agarwal, Samir Sheshank	Lattice based Unidirectional PRE and PRE+ Schemes	IET Information Security (SCI)			2020	
Kunwar Singh, C. Pandu Rangan, Richa Agarwal, Samir Sheshank	Provably Secure Lattice-Based Identity Based Unidirectional PRE and PRE+ Schemes	Journal of Information Security and Applications (SCI)	54		2020	
Kunwar Singh , Ch Koteswara Rao	Securely Solving Privacy Preserving Minimum Spanning Tree Algorithms in Semi-honest Model	Int. J. of Ad Hoc and Ubiquitous Computing (IJAHUC) (SCI)	34	1-10	2020	
Kunwar Singh, Gaurav Srivastava, Richa Agrawal, Rajeev Tripathi and Kshirasagar Naik	A Hierarchical Identity-based Security for Delay Toler ant Networks using Lattice-based Cryptography	Peer-to-Peer Networking and Applications (SCI), Springer	13	348 - 367	2020	
Kunwar Singh, KKC Deepti	Cryptanalysis of reduced round Salsa and ChaCha	IET Information Security (SCI).	13	591 – 602	2019	
Kunwar Singh Pratyush Dikshit	Weighted threshold ECDSA for securing bitcoin wallet	ACCENTS Transactions on Information Security, pp.	2(6)	43-51	2017	
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	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	1-12	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 Karthika SK	Theoretical Analysis of Biases in Chacha 128-bits			5th International Symposium on Mobile Internet Security (MobiSec 2021),	Jeju Island, South Korea.	2021
Kunwar Singh Sudarshan	Secure Distributed Medical Record			3rd International Workshop on Blockchains	Paris, France	2021

Parthasarathy Akash Harikrishnan, Gautam Narayanan, Lohith J. J	Storage using Blockchain and Emergency Sharing Using Multi-Party Computation			and Smart Contracts workshop (BSC 2021)		
Kunwar Singh Amalan Joseph Antony	Enhancing Privacy in a Blockchain based Public Key Infrastructure	Third ISEA Conference on Security and Privacy (ISEA-ISAP)		IEEE.	IIT Guwahati.	2020
Kunwar Singh C.H. Koteswara	RaoSecurely Solving Privacy Preserving Minimum Spanning Tree Algorithms in Semi-honest Model		1-10	International conference MobiSec	Cebu, Phillipines	2018
Kunwar Singh KKC Deepti	Cryptanalysis of Salsa and ChaCha	Mobile Networks and Management Springer	324–338	9th EAI International Conference on Mobile Networks and Management (MONAMI 2017)	Melbourne, Australia.	2017
Kunwar Singh Pratyush Dikshit.	Efficient Weighted Threshold ECDSA for Securing Bitcoin Wallet	Asia Security Privacy		IEEE.	NIT Surat.	2017
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.	Cryptanalysis of Unidirectional	Springer Berlin Heidelberg	564-575	Information and Communication Technology-	Bali, Indonesia	2014

Banerjee	Proxy Re-Encryption Scheme			EurAsia Conference		
Prashant Kumar Mishra, Kunwar Singh, Sudhanshu Baruntar	ID-Based Threshold Signcryption and Group Unsigncryption	Springer Berlin Heidelberg	35-44	International Conference on Security in Computer Networks and Distributed Systems	Trivendrum, India	2012
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 signcryption 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