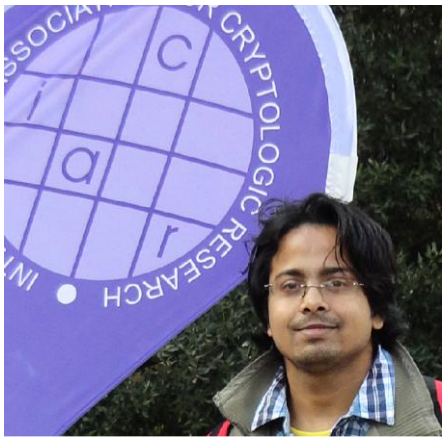
CURRICULUM-VITAE



Rajeev Anand Sahu
Assistant Professor
C R Rao Advanced Institute of Mathematics Statistics and Computer Science (AIMSCS)
Hyderabad Central University Campus
Hyderabad-500046
India.

Email: **rajeevs.crypto@gmail.com**

Address (for correspondence):

C R Rao Advanced Institute of Mathematics, Statistics and Computer Science (AIMSCS)
Hyderabad Central University Campus
Gachibowli, Hyderabad (Andhra Pradesh)
India.
Pin Code-500046

Address (Permanent):

Village and Post – Hardi (Jarwe)
Tehsil - Janjgir
Distt. – Janjgir - Champa (Chhattisgarh)
Pincode - 495668

Contact +91-8008344426
Passport No. : H2642648

ACADEMIC QUALIFICATION

COURSE	DATE/YEAR OF PASSING	BRANCH /SUBJECTS	BOARD / UNIVERSITY	Marks[%]	Division
Ph. D. (Mathematics)	May/2013	**Cryptography**	National Institute of Technology, Allahabad India	-	-
Masters in Science (M Sc.) (Mathematics)	May/2005	**Mathematics**	Guru Ghasi Das Central University Bilaspur (C.G.), India	**83.9%**	First
Bachelor of Science (B. Sc.)	May/2003	Mathematics, Physics, Chemistry	Guru Ghasi Das Central University Bilaspur (C.G.), India	**65.5%**	First
Intermediate (10+2)	May/2000	Mathematics, Physics, Chemistry, English, Hindi	M.P. Board, Bhopal India	**62.4%**	First
High School (10)	May/1998	Maths., Science, Social Science, English, Hindi	M.P. Board, Bhopal India	**77.6%**	First

COURSES STUDIED DURING Ph.D. COURSE WORK

SUBJECT	GRADE OBTAINED	FINAL CPI
Foundation of Cryptography	B+	**8.0 on 10 Scale**
Advanced Algorithm Techniques	B+	

TITLE OF Ph. D. THESIS

"Some Variants of ID-Based Proxy Signature Scheme from Bilinear Pairings"

THESIS SUPERVISOR

Dr. Sahadeo Padhye (www.mnnit.ac.in/images/stories/Sahadeo_Padhye_profile.pdf)

ACADEMIC EXPERIENCES

S/N	Name and address of employer	Title of position held	Dates of appointment	Pay scale and Grade	Full or part-time status	Brief description of duties and responsibilities
1.	National Institute of Technology (NIT) Raipur- 492010, India	Lecturer	August 2005-September 2007	@ INR 150 per lecture (fixed)	Part-Time	Teaching engineering/applied mathematics at undergraduate and postgraduate level
2.	National Institute of Technology (NIT) Raipur- 492010, India	Lecturer	October 2007-December 2008	INR 15,000 per month (fixed)	Contract	Teaching engineering/applied mathematics at undergraduate and postgraduate level
3.	C R Rao AIMSCS, Hyderabad Central University Campus, Hyderabad-500046, India	Assistant Professor	26 October 2012 – till date	15,600-39,100 With Basic 30,000 + AGP 8,000	Ad-hoc	Research in cryptography and cryptanalysis in connection to various projects for the Govt. of India.

COMPUTER PROFICIENCY

- **Languages** : C, C++. (gmp)
- **Operating System** : Windows, VISTA, LINUX.
- **Software Packages** : SAGE, PBC Library, MATLAB, Mathematica.

RESEARCH INTEREST

Identity-Based Cryptography.
Searchable Encryption
Elliptic Curve Cryptography.
Digital Signatures- Proxy signature, Anonymous signature.
Side Channel Analysis
Post Quantum Cryptology
Computation of Discrete Logarithms.

PROJECT (Currently Working)

1. **Project title**: System Engineering to Prevent Side Channel Cryptanalysis.
   (Sanctioned by: National Technical Research Organization **(NTRO)**, New Delhi, India.)

2. **Project title**: Post Quantum Cryptology.
   (Sanctioned by: Defense Research and Development Organization **(DRDO)**, New Delhi, India.)

PROJECT (Proposed to work)

Project title: Computation of discrete logarithms over finite fields of large characteristics using function field sieve method.

MEMBERSHIP IN SCIENTIFIC ORGANIZATIONS

1. Member of International Association of Cryptologic Research **(IACR)** Ref No. 20110125.
2. Life member of Cryptology Research Society of India **(CRSI)**, Membership No. L/300.
3. Graduate Student Member of **IEEE**, Membership No. 91272813.
4. Life member of Indian Mathematical Society **(IMS)**, Membership No. S-10-32.

ACHIEVEMENTS/HONORS / SCHOLARSHIPS / AWARDS/ GRANTS

1. Received the **Young Scientist award** in Mathematics for the year 2010 by '**International Academy of Physical Sciences'** in international conference CONIAPS XII at Rajshtan University Jaipur, India during 22-24 December 2010.

2. Selected for the **Ph.D. Student Stipend** to attend the Workshop on Elliptic Curve Cryptography-2010 (ECC-2010) in **Microsoft Research** Redmond, Washington, **USA** during October 18-22' 2010.

3. Selected for the **IEEE S&P Stipend** of $1500 to attend the IEEE Symposium on Security and Privacy at **University of California, Berkeley USA** during May 22-25' 2011, in association with IACR.

4. Selected for the **Qualcomm Stipend** to attend the **Eurocrypt 2012** at **University of Cambridge, UK** during April 15-19, 2012.

5. Selected for the **Stipend** (Registration Waive) to attend the C**rypto 2014,** International Cryptology Conference at the University of California, Santa Barbara (UCSB) during August 17-21, 2014.

6. Selected for the **ITS Grant** form Department of Science and Technology (DST) New Delhi, India to present a research paper in the International Conference **CEA'11 at Puerto Morelos, Mexico** during January 29-31' 2011.

7. Received **Grant** form Cryptology Research Society of India (CRSI) to present a research paper in an International Conference **CEA'11 at Puerto Morelos, Mexico** during January 29-31' 2011.

8. Received the **NBHM International Travel Support** by National Board for Higher Mathematics, to attend **Eurocrypt'2012** at **University of Cambridge, UK** during April 15-19, 2012.

9. Received **Grant** form Cryptology Research Society of India (CRSI) to present a research paper in an International Conference **ICICS 2014** at Hong Kong University, **Hong Kong**, China during December 16-17, 2014.

LIST OF SELECTED PUBLICATIONS

1. Francesco Buccafurri, Rajeev Anand Sahu and Vishal Saraswat, Efficient Proxy Signature Scheme from Pairings, International Conference on Security and Privacy- **SECRYPT 2016**, Lisbon, Portugal (Accepted).

2. Venu Nalla, Rajeev Anand Sahu and Vishal Saraswart, Differential Fault Attack on SIMECK, CS^2@ **HiPEAC** Conference, Prague, Czech Republic **2016**. DOI: 10.1145/2858930.2858939

3. Rajeev Anand Sahu and Vishal Saraswart, Efficient and Secure Many-to-One Signature Delegation, The 17th International Conference on Information and Communication Security- **ICICS 2015**, Beijing, China, **LNCS** Vol. 9543, Springer-Verlag.

4. Francesco Buccafurri, Gianluca Lax, Rajeev Anand Sahu and Vishal Saraswat, Practical and Secure Integrated PKE+PEKS with Keyword Privacy, 12th International Conference on Security and Cryptography- **SECRYPT 2015**, Colmar, France, In: (Ed.) Mohammad S. Obaidat, Pascal Lorenz, and Pierangela Samarati, SciTePress, pp. 448-453.

5. Rajeev Anand Sahu, Sahadeo Padhye and Navaneet Ojha, Efficient and Provable Secure Scheme for Delegation of Signing Rights between the Groups, **Annals of Telecommunications**, Springer **2015**, Vol. 70, Issue 9, pp. 369-379.
(SCI journal, Impact Factor: 0.722)

6. Vishal Saraswat and Rajeev Anand Sahu, An Anonymous Proxy Multi-signature with Accountability, E-Business and Telecommunications (Book Chapter), **CCIS** Vol. 554, Springer, **2015**, pp. 234-254.

7. Rajeev Anand Sahu and Vishal Saraswat, Secure and Efficient Scheme for Delegation of Signing Rights, The 16th International Conference on Information and Communication Security- **ICICS 2014**, Hong Kong, In: (Ed.) L. Hui et al. LNCS Vol. 8958, Springer-Verlag, pp. 258-273.

8. Vishal Saraswat and Rajeev Anand Sahu, A Secure Anonymous Proxy Multi-signature Scheme, 11th International Conference on Security and Cryptography- **SECRYPT 2014**, Vienna, Austria, In: (Ed.) Mohammad S. Obaidat and Andreas Holzinger, SciTePress, pp. 55-66. 2014.

9. Rajeev Anand Sahu and Sahadeo Padhye, Identity-Based Multi-proxy Multi-Signature Scheme Provable Secure in Random Oracle Model, **Transactions on Emerging Telecommunications Technologies**, Wiley, 2013. Vol 26, Issue 4, pp. 547-558.
(SCI journal, Impact Factor: 1.354)

10. Rajeev Anand Sahu and Sahadeo Padhye, Provable Secure Identity-Based Multi-proxy Signature Scheme, **International Journal of Communication Systems**, Wiley, 2013. Vol. 28, Issue 3, pp. 497-512.
(SCI journal, Impact Factor: 1.099)

11. Rajeev Anand Sahu and Sahadeo Padhye, Efficient ID-Based Proxy Multi-Signature Scheme Secure in Random Oracle, **Frontiers of Computer Science**, Springer, 2012, volume 6(4), pp. 421-428.
(SCI journal, Impact Factor: 0.660)

12. Rajeev Anand Sahu and Sahadeo Padhye, Efficient ID-Based Signature Scheme from Bilinear Map, **PDCTA-2011**, Tirunelveli, India, In: (Ed.) D. Nagamalai et al., **CCIS** Vol. 203, Springer-Verlag, pp. 301-306.

13. Rajeev Anand Sahu and Sahadeo Padhye, New ID-Based Proxy Multi-Signature from Pairings, **ICIEIS-2011**, University Technology, Malaysia, In: (Ed.) A. Abd Manaf et al., **CCIS** Vol. 251(2), Springer-Verlag, pp. 174-184.

14. Shivendu Mishra, Rajeev Anand Sahu, Sahadeo Padhye and Rama Shankar Yadav, Efficient ID-Based Multi-proxy Signature Scheme from Bilinear Pairing based on k-plus Problem, **INTECH-2011**, Sao Carlos, Brazil, In: (Ed.) E. R. Hruschka Jr. et al., CCIS Vol. 165, Springer-Verlag, pp. 113-122.

CONFRENCES/WORKSHOPS/SYMPOSIUMS ATTENDED

1) 10th International Conference on Cryptology in India **INDOCRYPT'2009**, December 13-16, 2009, held at Indian National Science Academy (INSA) **New-Delhi, India**.

2) National Instructional Workshop on Cryptology **NIWC 2010**, May 5-7, 2010, held in Manipur University Imphal, **Manipur**, **India.**

3) 11th International Conference on Cryptology in India **INDOCRYPT'2010**, December 13-15, 2010, held in Hyderabad Marriott Hotel & and Convention Centre, **Hyderabad**, **India**.

4) 5th WSEAS International Conference of Computer Engineering and Applications **CEA'11**, January 29-31, 2011, held in **Puerto Morelos, Mexico**.

5) IEEE Symposium on Security and Privacy 2011, **IEEE S&P'11**, May 22-25, 2011, held at Claremont resort, Oakland **Berkeley, California USA**.

6) **'Eurocrypt 2012'**, April 15-19, 2012, held in faculty of Music, Concert Hall, **Cambridge University, Cambridge UK.**

7) 13th International Conference on Cryptology in India **INDOCRYPT'2012**, December 09-12, 2012, held at Indian Statistical Institute, **Kolkata, India**.

8) National Instructional Workshop on Cryptology **NIWC 2014,** June 5-9, 2014, held at MNNIT Allahabad, **India.**

9) 18th Workshop on Elliptic Curve Cryptography **ECC 2014,** October 8-10, 2014, held at IMSc Chennai, India.

10) 16th International Conference on Information and Communication Security- **ICICS 2014,** December 16-17, 2014, held at the University of Hong Kong**, Hong Kong.**

11) National Instructional Workshop on Cryptology **NIWC 2015,** May 18-22, 2015, held at Himachal Pradesh University, Shimla, **India.**

TALK/LECTURE

- **Resource person** – Workshop on Pragmatic Cryptanalysis 2016, February 23-27, 2016, C R Rao AIMSCS, Hyderabad, India.
- **Resource person** - National Instructional Workshop on Cryptology (NIWC) -2015, May 18-22, 2015, Himachal Pradesh University, Shimla, India.
- **Resource person** - National Instructional Workshop on Cryptology (NIWC) -2014, June 5-9, 2014, National Institute of Technology Allahabad, India.
- **Resource person** – Seminar on 'Mathematics of Cryptography' at University of Hyderabad, December 2014, Hyderabad, India.
- **Resource person** - Refresher Course on 'Network Security and Cryptography' at Jawahar Lal Nehru Technical University (JNTU), October 2013, Hyderabad, India.

PC Member

SPACE 2016, ICICS 2015, PDCTA 2014

ABROAD VISITS

1. Presented paper in 5th WSEAS International Conference on Computer Engineering and Applications **(CEA'11)**, in **Puerto Morelos, Mexico** during January 29-31, 2011.
2. Attended the IEEE Symposium on Security and Privacy 2011, **(IEEE S&P'11)**, at Claremont resort, Oakland **Berkeley, California USA** during May 22-25, 2011.
3. Attended **'Eurocrypt 2012'** an International Conference in Cryptology, in the **University of Cambridge, UK** during April 15-19, 2012.
4. Presented paper in 16th International Conference on Information and Communication Security- **ICICS 2014,** at the University of Hong Kong**, Hong Kong** during December 16-17, 2014**.**

THESIS SUPERVISED

Masters Thesis

1. Student: Chetan Prakash Sharma
   Thesis title: Power Analysis of SIMON.

2. Student: Nitish Vyas
   Thesis title: Fault Analysis of SPECK.

3. Student: Jatin Kumar Kumawat
   Thesis title: Implementation of an Integrated Searchable Encryption.

4. Student: Karmaram Kala
   Thesis title: Hardware Implementation of SNOW 2.0 for DPA

5. Student: Rahul Kumawat
   Thesis title: Software Implementation of SNOW 2.0 for DPA.

6. Student: Rakesh Kumar
   Thesis title: McEliece Cryptosystem.

REFERENCES

1. **Dr. Sahadeo Padhye (Thesis Advisor)**
   Assistant Professor
   Department of Mathematics
   Motilal Nehru National Institute of Technology (MNNIT) Allahabad-211004
   India

   E-mail: sahadeomathrsu@gmail.com
   Contact : +91-9453256043 (Mob.)

2. **Dr. Vishal Saraswat**
   Assistant Professor
   C R Rao Advanced Institute of Mathematics Statistics and Computer Science, University of Hyderabad Campus,
   Hyderabad-500046,
   India

   E-mail: vishal.saraswat@gmail.com
   Contact: +91- 97035-72379

PERSONAL DETAILS

Gender	Male
Date of birth	17 July 1982
Marital status	Married
Nationality	Indian
Languages known	Hindi, English
Father's name	Mr. Vijay Kumar Sahu
Mother's name	Mrs. Prabha Sahu
Hobbies	Reading Biographies of Mathematicians, Solving mathematical puzzles, Poetry writing.
Sports	Badminton, Chess

DECLARATION

I do here by declare that the above furnished details are true and correct to the best of my knowledge and belief.

Place: Hyderabad, India **RAJEEV ANAND SAHU**