Curriculum Vitae of Dr Sujata Mohanty
Assistant Professor, NIT, Rourkela-769008, Odisha, India

PERSONAL PARTICULARS

Name: Dr. Sujata Mohanty

Present Address: **Assistant Professor**
Department of Computer Science and Engineering
N.I.T., Rourkela,
Rourkela-769008, Odisha, India
Phones (O): 0661-2462363
(R): 0661-2463363
Email: sujata.nitrkl@gmail.com, sujatam@nitrkl.ac.in

❖ *EDUCATIONAL QUALIFICATIONS*

BTech in Computer Science and Engineering

MTech in Computer Science and Engineering

PhD in Computer Science and Engineering

❖ *RESEARCH INTEREST*

- Information security, Cryptography, Financial security
- Security in Cloud Computing and IoT, malware analysis
- public key and Identity based cryptosystems

❖ *PUBLICATIONS*

A. JOURNAL:

1. S. S. Sahoo, **Sujata Mohanty**, and BanshidharMajhi, A Secure Three Factor based Authentication Scheme for Health care Systems using IoT Enabled Devices, Journal of Ambient Intelligence and Humanized Computing, Springer (Accepted)
2. Susmita Mandal, **Sujata Mohanty**, and BanshidharMajhi, CL-AGKA: certificateless authenticated group key agreement protocol for mobile networks, Wireless Networks (Springer), Vol. 26, pages 3011–3031(2020)
3. S. S. Sahoo, **Sujata Mohanty**, and BanshidharMajhi, Improved Biometric-Based Mutual Authentication and Key Agreement Scheme Using ECC, Wireless Personal Communications, Springer, Vol. **111**, pages 991–1017(2020). DOI https://doi.org/10.1007/s11277-019-06897-8

4. S. S. Sahoo, **Sujata Mohanty**, and BanshidharMajhi, An Improved and Secure Two-factor Dynamic ID Based Authenticated Key Agreement Scheme for Multiserver Environment, Wireless Personal Communications, Springer, 101(3), pp. 1307-1333, 2018, DOI: 10.1007/s11277-018-5764-8
5. Susmita Mandal, **Sujata Mohanty**, and BanshidharMajhi, Cryptanalysis and Enhancement of an Anonymous Self-Certified Key Exchange Protocol, Wireless Personal Communications, Springer, 99(2), pp. 1-29, 2018, DOI: 10.1007/s11277-017-5156-5
6. Susmita Mandal, **Sujata Mohanty**, and BanshidharMajhi, Design of electronic payment system based on authenticated key exchange, Electronic Commerce Research, Springer, 18(2), pp. 359-388, 2018, DOI: 10.1007/s10660-016-9246-3
7. S.K. Nayak, Sujata Mohanty, and BanshidharMajhi, CLB-ECC: Certificateless Blind Signature Using ECC, Journal of Information Processing Systems (JIPS),Vol: 13, No: 4, pp 970- 986, 2017, DOI: 10.3745/JIPS.03.0029
8. Susmita Mandal, **Sujata Mohanty**, and BanshidharMajhi, An ID-based authenticated three-party key exchange protocol, ACCENTS Transactions on Information Security, Vol 2(7), DOI: 10.19101/TIS.2017.27002
9. Sujata Mohanty, BanshidharMajhi, and Subhalaxmi Das, A secure electronic cash based on a certificateless group signcryption scheme, (2013) Mathematical and Computer Modelling (Elsevier), Vol 58 (1-2) PP. 186 – 195, doi: 10.1016/j.mcm.2012.06.004
10. Sujata Mohanty and BanshidharMajhi, A strong designated verifiable dl based signcryption scheme, (2012) Journal of Information Processing Systems 8 (4) PP. 567 – 574, DOI: 10.3745/JIPS.2012.8.4.567
11. **Sujata Mohanty**, BanshidharMajhi "A Novel Group Signature Scheme based upon DLP", Journal of Information Security Research, pp.9-14, 3(1), 2012, **(DLINE)**

B. INTERNATIONAL CONFERENCES:

1. S. S. Sahoo, Sujata Mohanty, Chaotic Map based Privacy Preservation User Authentication Scheme for WBANs, ***TENCON 2019 - 2019 IEEE Region 10 Conference (TENCON)***, Kochi, India, 2019, pp. 1037-1042, **DOI:** 10.1109/TENCON.2019.8929338.
2. M. Polai, S. Mohanty and S. S. Sahoo, "A Lightweight Mutual Authentication Protocol for Wireless Body Area Network," ***2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)***, Noida, India, 2019, pp. 760-765, doi: 10.1109/SPIN.2019.8711643
3. S. S. Sahoo, S. Mohanty and M. Polai, "A Secure Biometric Based User Authentication Scheme for Multi-Server Environment Using Chaotic Map," ***2019 6th International Conference on Signal Processing and Integrated Networks (SPIN)***, Noida, India, 2019, pp. 637-642, doi: 10.1109/SPIN.2019.8711751

4. S. S. Sahoo and S. Mohanty, "Cloud-Assisted Privacy Preserving Authentication Scheme for Telecare Medical Information Systems," IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Indore, India, pp. 1-6, doi: 10.1109/ANTS.2018.8710128
5. Susmita Mandal, **Sujata Mohanty**, and BanshidharMajhi, Universally verifiable certificatelesssigncryption scheme for MANET, Proceedings of the International Conference on Microelectronics, Computing & Communication Systems, Lecture Notes in Electrical Engineering, Springer, 453, pp. 77-89, 2018, DOI: 10.1007/978-981-10-5565-2_7
6. S. S. Sahoo, **Sujata Mohanty**, and BanshidharMajhi, A light weight three factor based authentication scheme for multi-server environment using smart cards, Proceedings of the the 7th International Conference on Communication and Network Security, ACM International Conference Proceeding Series, pp. 43-47, 2017, DOI: 10.1145/3163058.3163069
7. Susmita Mandal, **Sujata Mohanty**, and BanshidharMajhi, An ID-based non-interactive deniable authentication protocol based on ECC, Proceedings of the the 7th International Conference on Communication and Network Security, ACM International Conference Proceeding Series, pp. 48-52, 2017, DOI: 10.1145/3163058.3163070
8. **Sujata Mohanty**, S Paban Kumar PB, K Hanok, A Timestamped signature scheme with Message Recovery, Intrenational Conference of High Perfermance Computing and application (ICHPCA 2014), DOI: 0.1109/ICHPCA.2014.7045299
9. SusmitaMondal, **Sujata Mohanty**, Multiparty Key Exchange with Perfect Forward Secrecy, 13th International Conference on Infermation Technology (ICIT 2014), DOI: 10.1109/ICIT.2014.30
10. Aliva Panda, **Sujata Mohanty**, BanshidharMajhi, A Novel Group Blind Signature base on Discrete Logarithm Problem, Second International Conference on "Emerging Research in Computing, Information, Communication and Applications" ERCICA-2014
11. **Sujata Mohanty**, BanshidharMajhi, and Vinay Iyre. A strong designated verifiable group signature scheme, Proceedings - 2013 IEEE International Multi Conference on Automation, Computing, Control, Communication and Compressed Sensing, iMac4s 2013 PP.518-523, doi: 10.1109/iMac4s.2013.6526468
12. Nayak, S.K.,, Majhi, B., **Mohanty, S**. An ECDLP based untraceable blind signature scheme, (2013) Proceedings of IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT 2013 PP. 829 – 834, doi: 10.1109/ICCPCT.2013.6528937
13. S. Das, **S. Mohanty**, B. Majhi, A novel designated receiver based convertible multi-signcryption scheme, (2011) International Conference on Recent Trends in Information Technology, ICRTIT 2011 PP. 102 – 106, doi: 10.1109/ICRTIT.2011.5972300

14. S. Das, **S., Mohanty**, B. Majhi, A convertible designated verifible blind multi-signcryption scheme (2011) Communications in Computer and Information Science 193 CCIS (PART 4) PP. 549 – 556, doi: 10.1007/978-3-642-22726-4_57

15. **Sujata Mohanty** and BanshidharMajhi, A secure multi authority electronic voting protocol based on blind signature, (2010) ACE 2010 - 2010 International Conference on Advances in Computer Engineering PP. 271 – 273, doi: 10.1109/ACE.2010.82

16. **Sujata Mohanty** and BanshidharMajhi, A digital signature scheme with message recovery and without one-way hash function, (2010) ACE 2010 - 2010 International Conference on Advances in Computer Engineering PP. 265 – 267, doi: 10.1109/ACE.2010.89

17. **Sujata Mohanty**, BanshidharMajhi, and SK Baral, A novel time-stamped signature scheme based upon DLP, (2012) 2012 1st International Conference on Recent Advances in Information Technology, RAIT-2012 PP. 6 – 10, doi: 10.1109/RAIT.2012.6194469
18. **Sujata Mohanty**, SS Sahoo, and BanshidharMajhi, Certificateless nominative signature scheme based upon DLP, International Conference on Electrical, Electronics, and Optimization Techniques, ICEEOT 2016, pp. 1241-1245
19. ShreeyaSwagatikaSahoo, **Sujata Mohanty,** Sourav Kumar Sunny**,** and BanshidharMajhi, An Improved Authentication Scheme for Multiserver Environment using Smart cards, 5th International Conference on Advanced Computing, Networking, and Informatics (ICACNI 2017), Springer, June 2017.
20. **Sujata Mohanty**, Prasad Manikant, A Universally Verifiable Blind Signcryption Scheme with message Recovery, 2nd International Conference on Signal Processing and Integrated Networks (SPIN 2015), DOI: 10.1109/SPIN.2015.7095417

❖ MEMBERSHIPS IN PROFESSIONAL BODIES:

- Member of Institution of Engineers (MIE)

- Life Member of Computer Society of India (CSI)
- Life Member of Institution of Electronics and Telecommunication Engineers *(*IETE*)*
- Life Member of Indian Society of Technical Education (ISTE)

❖ PhD STUDENDS GUIDED:

(i) **Name**: Susmita Mandal
Research Area: Design of Key Exchange Protocol and its variants
Status: Passed out.

(ii) **Name:**Shreeya SwagatikaSahoo
Research Area: Analysis and Design of User Authentication Scheme in Multi-server Environment
Status: Thesis submitted

(iii) **Name:** Manabhanjan Pradhan
Research Area: Dynamic Authentication in Block Chain

Status: Ongoing

(iv) **Name:** Swati PriyambadaSatpathy
Research Area: Security in Cloud-aided lightweight certificateless authentication protocol
Status: Ongoing

❖ **Courses Taught:**

- Cryptography and Network Security
- Digital Logic Design
- Cryptographic Foundation
- Intrusion Detection System
- Parallel Algorithm
- Microprocessor and Microcontroller
- Computer Systems Architecture
- System Analysis and Design
- Foundation of Computer Security

❖ **Program chair, reviewer etc of International Conference**
1. International Conference on Computational Intelligence in Data Mining (ICCIDM-2015)
2. International Conference on Data mining and Advanced Computing (SAPIENCE 16)

❖ **Teaching Experience:**
Assistant Professor in department of CS, NIT Rourkela from 14th August 2008 to till date.

It is declared that all the information given above is true to the best of my knowledge and belief.

Date: 14-08-2020 **(SUJATA MOHANTY)**

Place: Rourkela