***PUBLICATIONS*:**

I. IN THE PEER REVIEWED JOURNALS:

1. Sahadeo Padhye, *Partial Known Plaintext Attack on Koyama Scheme.* Information Processing Letters, Vol.96 No.3 pp. 96-100 (2005). **(SCI Journal, Impact Factor – 0.5). Elsevier Journal**

2. Sahadeo Padhye, A *Signature Scheme Based on Singular Cubic Curve*, International Journal of Mathematical Science. Vol.4, No.2, pp.261-266 (2005).

3. Sahadeo Padhye, *A Fast RSA Type Signature Scheme*, Varahmihir Journal of Computer and Information Science*,* Vol.1 No.1 pp.80-82 (2006).

4. Sahadeo Padhye and B.K.Sharma, *A Fast Semantically Secure Public key Cryptosystem Based on Singular Cubic Curve*. International Journal of Network Security, Vol.3, No. 2, pp.164-170, Sept. 2006. (**SCImago Journal**)

5. Sahadeo Padhye *, On D-RSA Public Key Cryptosystem*. International Arab Journal of Information Technology, Vol 3, No.4 pp.336-338, October (2006). **(SCI & SCOP"US Journal, Impact Factor- 1.2)**

6. Sahadeo Padhye *, Cryptanalysis of Koyama Scheme.* International Journal of Network Security, Vol.2, No.1, pp.73-80, January (2006). Publisher-National Chung Hsing University, Taiwan (**SCImago Journal**)

7. Sahadeo Padhye and Navaneet Ojha, *Fast RSA Type Cryptosystem.* International Journal of Computer Science and Information Technology, Vol.3 no. 1, June 2010, pp. 93-94. Serial Publication.

8. Rajeev Anand Sahu and Sahadeo Padhye, *ID-Based Digital Signature Scheme from Bilinear Pairing: A Survey*, Frontiers of Electrical and Electronic Engineering in China Vol.6, No. 4, pp. 487-500, December, 2011. Springer Publication.

9. Rajeev Anand Sahu and Sahadeo Padhye, *Efficient Multi-Proxy Signature Scheme from Bilinear Pairing*, Journal of International Academy of Physical Sciences Vol.15 No. 01, 2011 pp. 59-68.

10. Sahadeo Padhye*, Singular Cubic Curve Based PKC: As Secure as Factoring*, International Journal of Cryptography and Security, Vol.1 No. 2 pp. 10-13, July- 2011. Bioinfo Publication.

11. Shivendu Mishra**,** Rajeev Anand Sahu and Sahadeo Padhye, *An Efficient Multi Proxy System for Proxy Signature Scheme*. Journal of Information Security Research, Vol. 2 No. 1, pp.1-12, March 2011.DLINE Journal.

12. Rajeev Anand Sahu and Sahadeo Padhye, *Efficient ID-based multi-proxy multi-signature scheme based on CDHP*, International Journal of Applied Mathematics and Informatics, Volume 5, Issue. 4, pp 275-281, 2011. NAUN Journals.

13. Navaneet Ojha and Sahadeo Padhye, *Another Generalization of Weak Keys in RSA With Prime Sharing LSBS*, Applied Mathematical Sciences, Vol. 6, no. 7, 309 – 318, January 2012. HIKARI Ltd.

14. Rajeev Anand Sahu and Sahadeo Padhye, Efficient ID-based Proxy Multi-Signature Scheme in Random Oracle. Frontiers of Computer Science , 6(4): 421-428, August (2012). Springer Publication. (**SCI & Scopus Journal, Impact Factor 4.2)**

15. Debiao He, Sahadeo Padhye and Jianhua Chen, *An Efficient Certificate Less Two Party Authenticated Key agreement Protocol*. Computer and Mathematics with Application 64(6): 1914-1926 September (2012). Elsevier Publication (**SCI & Scopus Journal, Impact Factor-2.9)**

16. Navaneet Ojha and Sahadeo Padhye, *Weak Keys in RSA Over the Work of Blomer & May*, International Journal of Network Security Vol. 14, No. 2, March 2012, pp. 80-85. National Chung Hsing University, Taiwan (**SCImago Journal**)

17. Namita Tiwari and Sahadeo Padhye, *Provable Secure Proxy Signature Scheme Without Bilinear Pairing*, International Journal of Communication Systems; April 2013 vol. 26, Issue. 5, pp. 644-650. Wiley Publication **(SCI & SCOPUS Journal, Impact Factor 1.8)**

18. Namita Tiwari and Sahadeo Padhye, Analysis on the Generalization of Proxy Signature, Security and Communication Network ; Vol.6, Issue 5, April 2013, pp. 549-556. (**SCI & SCOPUS Journal, Impact Factor- 1.9)**

19. Namita Tiwari, Sahadeo Padhye and Debiao He, Efficient ID-based Multi Proxy Multi Signature without Bilinear Maps in ROM, Annals of Telecommunication Vol.68 Issue 3, pp. 231-137 April (2013). (**SCI Journal**, **Impact Factor 1.9**).

20. Namita Tiwari and Sahadeo Padhye, Provable Secure ID-Based Designated Verifier Proxy Signature Without Pairings, Journal of Discrete Mathematical Sciences & Cryptography (Taru Publication & Taylor and Francis) Vol. 17, No.3, pp.199-212, Sept. 2014. (**SCOPUS**, **SCImago Journal , Impact factor 1.76)**

21. Namita Tiwari, Sahadeo Padhye and Debiao He, Provably Secure Proxy Multi-Signature Scheme Based On ECC. Information Technology and Control, Vol..43, N. 2, pp. 198-203, 2014. Published by Kaunas University of Technology (**SCI & SCOPUS Journal**, **Impact Factor 1.1**)

22. Navaneet Ojha and Sahadeo Padhye, Cryptanalysis of Multiprime RSA with Secret Key greater then Public Key. International Journal of Network Security Vol.16 No.01, pp.53-57 January (2014). National Chung Hsing University, Taiwan (**SCImago Journal**)

23. Sahadeo Padhye and Namita Tiwari, ECDLP based Certificate-less Proxy Signature scheme with Message Recovery. Transactions on Emerging Telecommunications Technologies, Vol. 26, Issue 3, pp. 346-354, March 2015 .Wiley Publication. (**SCI & SCOPUS Journal**, **Impact Factor 3.3**).

24. Rajeev Anand Sahu and Sahadeo Padhye, ID-Based Multi-proxy Multi-Signature Scheme Provable Secure in Random Oracle Model. Transactions on Emerging Telecommunications Technologies. (Wiley Publication) Vol. 26 Issue-4, pp. 547-558, April 2015. (**SCI Journal**, **Impact Factor 3.3**).

25. Rajeev Anand Sahu and Sahadeo Padhye, Provable Secure Identity-Based Multi-proxy Signature Scheme, International Journal of Communication Systems, Vol.28, Issue 3, pp. 497-512, January 2015. **(SCI & SCOPUS Journal, Impact Factor 1.8)**

26. Namita Tiwari and Sahadeo Padhye, Provable Secure Multi-Proxy Signature Scheme Without Bilinear Maps. International Journal of Network Security. Vol.17, No.6, PP.736-742, Nov. 2015 (**SCImago Journal**)

27. Rajeev Anand Sahu, Sahadeo Padhye and Navaneet Ojha, Efficient and Provable Secure Scheme for Delegation of Signing Rights between the Groups. Annals of Telecommunication, October 2015, Volume 70, Issue 9, pp 369-379. (**SCI & SCOPUS Journal**, **Impact Factor 1.9**).

28. Sonika Singh and Sahadeo Padhye, Generalization of NTRU Cryptosystem, Security and Communication Network. Volume 9, Issue 18, December 2016, Pages: 6315–6334 (Wiley Publication) (**SCI Journal, Impact Factor- 1.9).**

29. Sonika Singh and Sahadeo Padhye, MaTRU-KE: A Key Exchange Protocol Based On MaTRU Cryptosystem. International Journal of Communication System, 2018 : Vol. 32(4), pp. e3886, 1-16 **(SCI & SCOPUS Journal, Impact Factor 1.8) (10-03-2019)**

30. Swati Rawal and Sahadeo Padhye, Cryptanalysis of ID Based Proxy-Blind Signature Scheme. ICT Express , Vol 6(1), pp. 20-22, 2020. (Elsevier Publication), (**SCOPUS Journal, Impact Factor 5.4**)

31. Sonika Singh and Sahadeo Padhye , Identity based Blind Signature Scheme over NTRU Lattices. Information Processing Letters, Vol. 155 (2020), pp. 1-3. 105898 (**SCI Journal, Impact Factor – 0.5**). Elsevier Journal

32. Swati Rawal, Sahadeo Padhye and Debiao He, Lattice Based Undeniable Signature Scheme Annals of Telecommunications, Vol. 77, pp.119–126 (2022) (**SCI Journal, Impact Factor 1.9**). Springer Journal

33. Swati Rawal and Sahadeo Padhye, A Quantum Resistant Anonymous Proxy Signature Scheme, Sadhana: Academy Proceeding in Engineering Sciences, (2022) 47:41, pp. 1-8. (**SCI Journal, Impact Factor 1.6**), Springer Journal.

34. Satyam Omar, Sahadeo Padhye, and Dhananjoy Dey ,*Cryptanalysis of Multivariate Threshold Ring Signature Schemes,* Information Processing Letters, Vol 181, Article 106357, pp. 1-5, 2023 (**SCI Journal, Impact Factor – 0.5**). Elsevier Journal

35. Satyam Omar, Sahadeo Padhye, and Dhananjoy Dey, Anonymous Proxy Signature Scheme Based on Multivariate Polynomials over Finite Field. Journal of Algebra and its Applications, 2024, 2450156, pp. 1-21. (**SCI Journal, Impact Factor 0.8**), **World Scientific Publishing.**

36. Satyam Omar, Sahadeo Padhye, and Dhananjoy Dey, A Multivariate Convertible Group Signature Scheme. SN Computer Science (2023) 4:735 pp. 1-12. 5 (**SCOPUS Journal, Impact Factor 1.2**), Springer journal.

37. Ramakant Kumar, Sahadeo Padhye, A Lattice Based Single Share Secret Sharing Scheme, SN Computer Science, (2023) 4:811 pp.1-10 (**SCOPUS Journal, Impact Factor 1.2**), Springer journal.

38. Prashanta Majee, Sonu Bai, and Sahadeo Padhye, Inertial Mann Type Algorithms For A Finite Collection Of Equilibrium Problems And Fixed Point Problem of Demicontractive Mappings The Journal of Analysis, Vol. 32, pp. 447-469, 2024. (**SCOPUS Journal, Impact Factor 0.8**) , Springer Journal.

39. Prashanta Majee, Sonu Bai, and Sahadeo Padhye, On Some Novel Methods for Generalized Fermat-Torricelli Problem in Hilbert Spaces. Results in Mathematics, Vol 79, Vol. 1, Article No. 5, pp. 1-35 . 2024 (**SCI Journal, Impact Factor 2.2)** Springer Journal.

40. Prashanta Majee, Sonu Bai, and Sahadeo Padhye, On some fast iterative methods for split variational inclusion problem and fixed point problem of demicontractive mappings. Computational and Applied Mathematics, Vol. 43, Article No. 105, pp. 1-29, 2024(**SCI Journal, Impact Factor 2.6**) Springer Journal.

41. Ramakant Kumar, Sahadeo Padhye, Improved Lattice based multistage secret sharing scheme, Sadhana: Academy Proceeding in Engineering Sciences, Volume 50, article number 68, (2025). (**SCI Journal, Impact Factor 1.6**), Springer Journal.

42. Ramakant Kumar, Sahadeo Padhye, A Lattice-Based Ring Signature Scheme with Gradual Revelation of Non-Signers, International Journal of Information Technology, Volume 17, pages 567–574, (2025).(SCOPUS Journal, Impact Factor 4.8), Springer Journal.

43. Rohitkumar R Upadhyay, Sahadeo Padhye, Advancements in Fully Homomorphic Encryption over the Integers: A Comprehensive Survey and Analysis. Surveys in Mathematics and its Applications Volume 19 (2024), 245 – 299 (December 3-2024) (**Scopus Journal**)

44. Ramakant Kumar, Sahadeo Padhye, Cryptanalysis of a Lattice Based Multi-signature Scheme, National Science Academy Letters, https://doi.org/10.1007/s40009-024-01583-1 (Accepted 25-11-2024) (**SCI Journal, Impact Factor 1.2**), Springer Journal.

45. Satyam Omar, Sahadeo Padhye and Dhananjoy Dey, Linkable Ring Signature Scheme Based on Multivariate Polynomial Over Finite Field. Advances in Mathematics of Communications. Volume 19, Issue 5: 1301-1319, 2025. American Institute of Mathematical Science (AIMS) Publication. (**SCI Journal, Impact Factor 0.8**), AIMS Journal.

46. Rohit Kumar R Upadhyay, Sahadeo Padhye, Efficient and Secure MPC through Integration of FHE and Proxy Re-encryption. SN Computer Science, Vol.6(90), pp. 1-10, 2025. (**SCOPUS Journal**, **Impact Factor 1.2),** Springer journal.

47. Sonika Singh, Swati Rawal, Sahadeo Padhye, Namita Tiwari, Identity based Proxy Blind Signature Scheme Using NTRU Lattices. Information and Computation. Vol. 304 (2025) 105284 (**SCI Journal, Impact Factor 0.8**)

48. Satyam Omara, Sahadeo Padhye, Dhananjoy Dey, Devansh Mehrotra, A Multivariate Convertible Undeniable Signature Scheme. Information and Computation, Vol. 304 (2025) 105286. (**SCI Journal, Impact Factor 0.8**)

49. Ramakant Kumar, Sahadeo Padhye, Chained Time Lock Puzzle with Small Puzzle Size. Information and Computation, Volume 304 (2025), Article No. 105301 (**SCI Journal, Impact Factor 0.8**)

50. Swati Rawal, Sahadeo Padhye, Ramakant Kumar and Debiao He. Lattice Based Signatures with Additional Functionalities. Surveys in Mathematics and its Applications, Vol. 20 (2025), pp. 267-317. (**Scopus Journal**) (**Q3, Impact Factor 0.45**)

II. IN THE PROCEEDING OF PEER REVIED CONFERENCES/BOOK CHAPTERS

1. Sahadeo Padhye*, Cyclic Attack On RSA Type Cryptosystem Based On Singular Cubic Curve.* Proceeding of International Conference On Discrete Mathematics And Its Application. Norosa Publishing House Pvt. Ltd. ISBN 81-7319-731-8, Editor- M. Sathumadhavan, pp. 120-130 (2006). Dec.09-11, 2004, Amrita Institute of Technology, Coiambatore Tamilnadu (India). ISBN - 81-7319-731-8

2. Sahadeo Padhye *, A Rabin Type Scheme Based on Singular Cubic Curve*. Proceeding of the 9th National Workshop on Cryptology under India Mathematics Year-2009, Aug 7-9, 2009. pp.34-36. SVNIT Surat, India.

3. Rajeev Anand Sahu and Sahadeo Padhye, *An ID-Based Multi Proxy Multi-Signature Scheme*. Proceeding of IEEE International Conference on Computer & Communication Technology ICCCT-2010, pp. 60-63, 2010. Sept. 17-19, 2010 MNNIT, Allahabad, India. ISBN- 978-1-4244-9031-8

4. Navneet Kumar Ojha and Sahadeo Padhye, *The Additional Result Over The Work of Blomer and May,* Proceeding of IEEE International Conference on Computer & Communication Technology ICCCT-2010 , pp. 75-80, 2010. Sept. 17-19, 2010 MNNIT, Allahabad, India. ISBN- 978-1-4244-9031-8

5. Rajeev Anand Sahu and Sahadeo Padhye, *ID-based multi-proxy multi-signature scheme from bilinear pairing*, Proceedings of 5th International Conference of Computer Engineering Applications (CEA'11), 2011 pp. 43-48. WSEAS Press Puerto Morelos, Mexico. Jan. 29-31, 2011. ISBN- 978-960-474-270-7

6. Shivendu Mishra**,** Rajeev Anand Sahu, Sahadeo Padhye and R.S. Yadav, *An ID-Based Signature Scheme From Bilinear Pairing Based on k-plus Problem*. Proceeding of IEEE 3rd International Conference on Electronics Computer Technology (ICECT 2011), pp. 104-107, 2011. April 8-10, 2011 Kanyakumari India. **ISBN-** 978-1-4244-8678-6

7. Namita Tiwari and Sahadeo Padhye, *New Proxy Signature Scheme with Message Recovery Using Verifiable Self-Certified Public Keys***.** Proceeding of IEEE International Conference on Computer & Communication Technology ICCCT-2011, pp. 539-544. Sept. 15-17, 2011. MNNIT, Allahabad, India. ISBN- 978-1-4577-1383-5

8. Namita Tiwari and Sahadeo Padhye, *An ID-based Designated Verifier proxy signature scheme without bilinear pairings*. Proceeding of 5th Indian International Conference on Artificial Intelligence (IICAI-11), pp. 756-768, 2011. Dec. 14-16, 2011. Siddaganga Institute of Technology, Tumkur India. ISBN -978-0-9727412-8-6

9. Shivendu Mishra**,** Rajeev Anand Sahu, Sahadeo Padhye and R.S. Yadav, *Efficient ID-Based Multy-Proxy Signature Scheme From Bilinear Pairing Based on k-plus Problem*. Integrated Computing Technology, Communication in Computer and information Science (CCIS) Vol. 165, pp. 113–122, 2011, Springer-Verlag 2011. ISBN-978-3-642-22246-7.

10. Rajeev Anand Sahu and Sahadeo Padhye, *Efficient ID-Based Signature Scheme from Bilinear Map*, *Advances in Parallel Distributed Computing,* Communication in Computer and information Science (CCIS)Vol. 203, pp. 301-306 Springer-Verlag 2011. ISBN-978-3-642-24036-2.

11. Namita Tiwari and Sahadeo Padhye, *An ID-based proxy multi signature scheme without bilinear pairings*, Security Aspect in Information Technology, Lecture Notes in Computer Scienec,(LNCS) Vol. 7011, pp. 83–92, 2011, M. Joy et al (Eds). Springer-Verlag Berlin Heidelberg 2011. ISBN-9783642245855.

12. Navaneet Ojha and Sahadeo Padhye, *Generalization of Weger's Attack*, Informatic Engineering and Information Science Part-II, Communication in Computer and information Science (CCIS) Vol.251 pp. 141-150, 2011. Springer-Verlag 2011. ISBN-978-3-642-25326-3

13. Rajeev Anand Sahu and Sahadeo Padhye, *New ID-Based Proxy Multi Signature From Pairing*. Informatic Engineering and Information Science Part-II, Communication in Computer and information Science (CCIS) Vol.251 pp. 174-184, 2011. Springer-Verlag 2011. ISBN-978-3-642-25326-3.

14. Namita Tiwari and Sahadeo Padhye, *Security Analysis of Proxy Blind Signature Scheme based on Factoring and ECDLP*. Advances in Computer Science and Information Technology, Lecture Notes of Institute for Computer Science, Social Informatics and Télécommunications Engineering (LNICST) Vol.85, pp. 100–108, 2012 Springer-Verlag Berlin Heidelberg 2011. ISBN-9783642273070.

15. Sahadeo Padhye and Namita Tiwari, "*Improved proxy signature scheme without bilinear pairings*", In: Singh K., Awasthi A.K. (eds) Quality, Reliability, Security and Robustness in Heterogeneous Networks. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, LNICST Vol. 115, pp. 682–688, 2013. ISBN- 978-3-642-37949-9, Springer, Verlag.

16. Sahadeo Padhye and Namita Tiwari, Efficient ID-Based Proxy Blind Signature with Pairing Free Realization. Proceeding of 3rd International Conference on Innovative Engineering Technology (ICIET'2016) pp.40-43, 2016. August 5-6, 2016. Rajamangala University of Technology Thanyaburi, Bangkok, Thailand. ISBN-ISBN 978-93-84468-65-1. (Published by IIE)

17. Sonika Singh and Sahadeo Padhye, Cryptanalysis of NTRU With n Public Keys. Proceeding in IEEE Asia Security and Privacy Conference 2017, pp. 1-6, January 29-31, 2017. CED NIT Surat (Gujrat). DOI - 10.1109/ISEASP.2017.7976980. ISBN No. 978-1-5090-5942-3.

18. Sonika Singh, Sahadeo Padhye, "*A Self Proxy Signature Scheme Over NTRU Lattices*". In: Latifi S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 738, pp. 68-74, April, 2018 . ISBN: 978-3-319-77028-4. Springer, Cham.

19. Swati Rawal and Sahadeo Padhye, Threshold Ring Signature with message block sharing. In Proceeding of 2nd ISEA Conference on Security and Privacy (ISEA-ISAP 2018), January 9-11, 2019, Malaviya National Institute of Technology Jaipur, India. Springer book Communications in Computer and Information Science CCIS Vol. 939, pp.261-274, 2019, Springer Nature, Singapur. ISBN-979-981-13-7560-6. Springer Nature Singapur Pte Ltd..

20. Swati Rawal and Sahadeo Padhye , Untracebility of partially blind signature scheme over lattices, The 15th International Conference on Information Security and Cryptology Nanjing, China | December 6-8 2019. In Z. Liu and M. Yung (Eds.), Information Security and Cryptology, Lecture Notes in Computer Science (LNCS), Vol. 12020, pp. 452–459, 2020. ISBN 978-3-030-42921-8, Springer Nature Switzerland AG 2020.

21. Satyam Omar and Sahadeo Padhye, Multivariate Linkable Group Signature Scheme, 3rd International Conference On Computing and Communication Systems (I3CS-2020), August 10-11, 2020 , Department of Information Technology, North-Eastern Hill University, Shillong, In Arnab Kumar Maji, Goutam Saha, Sufal Das, Subhadip Basu, João Manuel R. S. Tavares (Eds.). Lecture Notes in Networks and Systems (LNNS), Vol 170, pp. 623-632, 2020. ISBN -978-981-33-4084-8. Springer Nature Switzerland.

22. Satyam Omar, Sahadeo Padhye and Dhananjoy Dey, A New Identity-Based Multivariate Signature Scheme, 7th International conference on Mathematics and Computing, March 2-5, 2021, IIEST, Shibpur, West Bangal. In: Giri D., Raymond Choo KK., Ponnusamy S., Meng W., Akleylek S., Prasad Maity S. (eds) Proceedings of the Seventh International Conference on Mathematics and Computing. Advances in Intelligent Systems and Computing, vol 1412, pp 79-91, 2022. Springer, Singapore. https://doi.org/10.1007/978-981-16-6890-6_7. ISBN: 978-981-16-6890-6. (Jan 2022)

23. Swati Rawal and Sahadeo Padhye, A Post Quantum Signature Scheme for Secure User Certification System. Proceeding of 6th International Conference Information, Communication & Computing Technology (ICICCT-2021), On May 08 , 2021, Saturday, JAGAN INSTITUTE OF MANAGEMENT STUDIES (JIMS) Sector-5, Rohini, Delhi-110085New Delhi, India. In Mahua Bhattacharya Latika Kharb Deepak Chahal (Eds.), Information and Communication Technology, Communications in Computer and Information Science (CCIS) book series, Volume 1417, pp. 52-62, 2021. ISBN- 978-3-030-88378-2. Springer Nature Switzerland. (Oct 2021)

24. Sonika Singh, Sahadeo Padhye, Ankan Pal, Generalization of Lattice-Based Cryptography on Hypercomplex Algebras. In: Stănică, P., Gangopadhyay, S., Debnath, S.K. (eds) Security and Privacy. Lecture Notes in Electrical Engineering (LNEE), vol 744, pp. 67-79, 2021. Springer, Singapore. ISBN: 978-981-33-6781-4.

25. Sonika Singh and Sahadeo Padhye, A Lattice-based Key Exchange Protocol over NTRU-NIP, International Conference on Cryptology & Network Security with Machine Learning (ICCNSML-2022), PSIT Kanpur 16-18, December, 2022. In. Bimal K Roy, Atul Chaturvedi, Boaz Tsaban, and Sartaj Ul Hasan (eds), Proceeding

published by Springer publication, Book Series Algorithm for Intelligent System, pp. 325-334, ISBN: 978-981-99-2229-1

26. Satyam Omar, Sahadeo Padhye, and Dhananjoy Dey, Multivariate Aggregate and Multi Signature Scheme, International Conference on Cryptology & Network Security with Machine Learning (ICCNSML-2022), PSIT Kanpur 16-18, December 2022. In. Bimal K Roy, Atul Chaturvedi, Boaz Tsaban, and Sartaj Ul Hasan (eds)Proceeding published by Springer publication, Series Algorithm for Intelligent System , pp. 71-76, ISBN: 978-981-99-2229-1

27. Ramakant Kumar, Sahadeo Padhye, Cryptanalysis of lattice based threshold changeable multi-secret sharing scheme, International Conference on Cryptology & Network Security with Machine Learning (ICCNSML-2022), PSIT Kanpur 16-18, December 2022. In. Bimal K Roy, Atul Chaturvedi, Boaz Tsaban, and Sartaj Ul Hasan (eds), Proceeding published by Springer publication, Series Algorithm for Intelligent System, pp. 317-327, ISBN: 978-981-99-2229-1

28. Satyam Omar, Sahadeo Padhye and Dhananjoy Dey, *A New Identity-Based Multivariate Signature Scheme*, In: Giri D., Raymond Choo KK., Ponnusamy S., Meng W., Akleylek S., Prasad Maity S. (eds) Proceedings of the Seventh International Conference on Mathematics and Computing. Advances in Intelligent Systems and Computing, vol 1412, pp 79-91, 2022. Springer, Singapore. https://doi.org/10.1007/978-981-16-6890-6_7. ISBN: 978-981-16-6890-6. (Jan 2022)

29. Rohit Kumar R Upadhyay, Sahadeo Padhye, Enhancing FHE Over the Integers: Beyond Binary Numbers and Batch Processing. International Conference on Cryptology & Network Security with Machine Learning (ICCNSML-2023), PSIT Kanpur 27 – 29 October, 2023**.** Chaturvedi, A., Hasan, S.U., Roy, B.K., Tsaban, B. (eds) Cryptology and Network Security with Machine Learning. ICCNSML 2023. Lecture Notes in Networks and Systems, vol 918. Springer, Singapore. https://doi.org/10.1007/978-981-97-0641-9_22, ISBN: 978-981-97-0641-9.

30. Rohit Kumar Upadhyay and Sahadeo Padhye, Multi-Key Fully Homomorphic Encryption Scheme Over Integers. RedCySec 2023, International Conference on Recent Development in Cyber Security, June 16-17, 2023, Sharda University. In: Roy, N.R., Tanwar, S., Batra, U. (eds) Cyber Security and Digital Forensics. REDCYSEC 2023. Proceeding published in Lecture Notes in Networks and Systems, vol 896, pp. 203-215 Springer, Singapore. ISBN: 978-981-99-9811-1.

31. Satyam Omar, Sahadeo Padhye, and Dhananjoy Dey, Multivariate Partially Blind Signature Scheme. In: Shukla, A., Murthy, B.K., Hasteer, N., Van Belle, JP. (eds) Computational Intelligence. Lecture Notes in Electrical Engineering, vol 968, 143-155, 2023 (Feb. 2023) Springer, Singapore. https://doi.org/10.1007/978-981-19-7346-8_13. ISBN: 978-981-19-7346-8.

32. Ramakant Kumar, Sahadeo Padhye, and Swati Rawal; Cryptanalysis of Short and Provable Secure Lattice-Based Signature Scheme, In Francesco Regazzoni, Bodhisatwa Mazumdar, Sri Parameswaran (eds). Lecture Notes in Computer Science (LNCS) Vol. 14412, pp. 86-91, 2023, Springer Book Series. https://doi.org/10.1007/978-3-031-51583-5, ISBN 978-3-031-51583-5 (December 2023).

33. Rohitkumar R Upadhyay and Sahadeo Padhye, Enhancing FHE over Integers: Beyond Binary Numbers and Batch Processing. In: Chaturvedi, A., Hasan, S.U., Roy, B.K., Tsaban, B. (eds) Cryptology and Network Security with Machine Learning. ICCNSML 2023. Lecture Notes in Networks and Systems, vol 918, pp. 317-327. Springer, Singapore. https://doi.org/10.1007/978-981-97-0641-9_22, ISBN: 978-981-97-0641-9 (April 2024).

IV. IN THE EPRINT ARCHIVE

INTERNATIONAL ASSOCIATION OF CRYPTOLOGIC RESEARCH:

1. Sahadeo Padhye*, A Public Key Cryptosystem Based on Singular Cubic Curve*. Eprint Archive-2005/109, http://eprint.iacr.org/2005/109.pdf.
2. Sahadeo Padhye, *An Efficient Variant of RSA Cryptosystem*, Eprint-Archive-2005/392 http://eprint.iacr.org/2005/392.pdf.

3. Sahadeo Padhye, *On Security of Koyama Scheme*, Eprint Archive-2005/153, http://eprint.iacr.org/2005/153.pdf
4. Sahadeo Padhye, *A Public Key Cryptosystem Based on Pell Equation*. Eprint Archive-2005/191, http://eprint.iacr.org/2006/119.pdf

IN THE EPRINT ARXIVE OF CORNELL UNIVERSITY

1. R Pandey, S Padhye, *Extended Generalized Flett's Mean Value Theorem*, arXiv preprint: arXiv:1604.07248, Cornell University.