# Prof. Somitra Kumar Sanadhya

| | |
|---|---|
| Name | : Prof Somitra Kumar Sanadhya |
| Current Affiliation | : Department of Computer Science & Engineering Indian Institute of Tech, Jodhpur, Rajasthan, India |
| Ph.D | : Indian Statistical Institute, Kolkata |
| Research Interests | : |

- Cryptology: Hash functions, block ciphers, cryptanalysis
- Quantum cryptography & quantum computing
- Blockchain and cryptocurrency security
- Cybersecurity engineering and secure protocols
- Hardware security: True Random Number Generators (TRNGs), Physically Unclonable Functions (PUFs)

| | |
|---|---|
| Website | : https://research[dot]iitj[dot]ac[dot]in/researcher/somitra-kumar-sanadhya |
| Brief CV | : |

Prof. Sanadhya earned his B.Tech from IIT Delhi, M.Tech from JNU Delhi, and completed his Ph.D. at ISI Kolkata in 2009. His doctoral work made significant contributions in the cryptanalysis of hash functions, particularly SHA 256 and SHA 512. He began his academic career as Assistant Professor at IIT Ropar, where he also served as Head of the Department of Computer Science & Engineering. He later joined IIT Jodhpur as Associate Professor and was promoted to full Professor in 2021. He currently serves as: Dean of Digital Infrastructure & Automation (DIA) and Chief Information Security Officer (CISO) In addition to his administrative roles, he has led and collaborated on high-impact research projects, mentored Ph.D. scholars, and actively served the cryptographic research community through conference organization and reviewing.


- Baddour, Issa, Dip Sankar Banerjee, and Somitra Kumar Sanadhya. "SideLink: Exposing NVLink to Covert and Side-Channel Attacks Official Work-in-Progress Paper." In International Conference on Security, Privacy, and Applied Cryptography Engineering, pp. 6-15. Cham: Springer Nature Switzerland, 2024.
- Jati, Arpan, Naina Gupta, Anupam Chattopadhyay, and Somitra Kumar Sanadhya. "A configurable crystals-kyber hardware implementation with side-channel protection." ACM transactions on embedded computing systems 23, no. 2 (2024): 1-25.
- Anandakumar, N. Nalla, Mohammad S. Hashmi, and Somitra Kumar Sanadhya. "Field Programmable Gate Array based elliptic curve Menezes-Qu-Vanstone key agreement protocol realization using Physical Unclonable Function and true random number generator primitives." IET Circuits, Devices & Systems 16, no. 5 (2022): 382-398.
- …
- …