Subhranil Dutta

Associate Research Fellow in Cryptography

Building 3, Room 232, Northfields Avenue
School of Computing & Information Technology
Institute of Cybersecurity and Cryptology (iC^2)
University of Wollongong, NSW 2500, Australia



Email: subhranild@uow.edu.au • subhranildutta17@gmail.com
Homepage: subhranildutta17.github.io • Mobile: (+91) 80 168 640 78
LinkedIn • Google Scholar • DBLP

Research Interests

Functional Encryption • Lattice-based Cryptography • Fully Homomorphic Encryption • Secure Cloud Computing • Private Set Intersection • Post-Quantum Multi-Party Computation

Education

2019–2024	**Doctor of Philosophy** in Cryptography Department of Mathematics, Indian Institute of Technology Kharagpur, India Supervisor: Prof. Sourav Mukhopadhyay · Defended: 23 July 2024 Dissertation: *Selected Constructive Approaches towards Linear Functional Encryption with Advanced Features for Cloud Computing*
2016–2018	**Bachelor of Education** Pandua Ideal Teachers' Training College, University of Gour Banga, India — 72.8%
2014–2016	**Master of Science** in Mathematics (Pure Mathematics) University of Gour Banga, India — 83.60%
2011–2014	**Bachelor of Science** in Mathematics Malda College, University of Gour Banga, India — 63.12%
2011	**Higher Secondary (10+2)**, West Bengal Council of Higher Secondary Education — 74.50%
2009	**Secondary (Class X)**, West Bengal Board of Secondary Education — 83.62%

Academic Appointments

Mar 2026–present	**Associate Research Fellow** Institute of Cybersecurity and Cryptology (iC^2), University of Wollongong, Australia Host: Prof. Willy Susilo
Oct 2025–Jan 2026	**Postdoctoral** CrIS Lab, Dept. of Computer Science and Automation, Indian Institute of Science (IISc) Bangalore, India Host: Prof. Arpita Patra
Sep 2024–Aug 2025	**Postdoctoral Researcher** — Swiss Government Excellence Scholarship (ESKAS) Institute of Computer Science (ICS-HSG), University of St. Gallen, Switzerland Host: Prof. Aikaterini (Katerina) Mitrokotsa Funded by Federal Commission for Scholarships for Foreign Students (FCS)
Jun 2024–Aug 2024	**Research Assistant** Institute of Computer Science (ICS-HSG), University of St. Gallen, Switzerland Host: Prof. Aikaterini (Katerina) Mitrokotsa
Feb 2021–Jan 2024	**Senior Research Fellow** (CSIR-SRF) Department of Mathematics, Indian Institute of Technology Kharagpur, India
Jan 2019–Jan 2021	**Junior Research Fellow** (CSIR-JRF) Department of Mathematics, Indian Institute of Technology Kharagpur, India

Publications

Bold: author of this CV · listed in reverse chronological order

Journal Articles

[J1] **Subhranil Dutta**, Tapas Pal, Amit Kumar Singh, Sourav Mukhopadhyay. Fully Collusion Resistant Traceable Identity-Based Inner Product Functional Encryption. *IACR Communications in Cryptology*, vol. 2, no. 1, 2025. doi:10.62056/av4fe0zn4
[IACR diamond open-access journal, est. 2024 · No impact factor yet · SCIE/Scopus indexing pending]

[J2] **Subhranil Dutta**, Ratna Dutta, Sourav Mukhopadhyay. Securing Data in the Cloud Using Pairing-Free Inner Product Functional Encryption with Unbounded Vector Size. *Theoretical Computer Science*, vol. 1031, art. no. 115085, 2025. doi:10.1016/j.tcs.2025.115085
[Indexed: SCIE, Scopus · Impact factor 1.1 (JCR 2025) · Scopus Q2, Computer Science (miscellaneous)]

[J3] **Subhranil Dutta**, Tapas Pal, Ratna Dutta. Reinforcing Privacy in Cloud Computing via Adaptively Secure Non-zero Inner Product Encryption and Anonymous Identity-Based Revocation in Unbounded Setting. *Theoretical Computer Science*, vol. 995, art. no. 114502, 2024. doi:10.1016/j.tcs.2024.114502
[Indexed: SCIE, Scopus · Impact factor 1.1 (JCR 2025) · Scopus Q2, Computer Science (miscellaneous)]

[J4] Uddipana Dowerah, **Subhranil Dutta**, Aikaterini Mitrokotsa, Sayantan Mukherjee, Tapas Pal. Unbounded Predicate Inner Product Functional Encryption from Pairings. *Journal of Cryptology*, vol. 36, no. 3, art. no. 29, 2023. doi:10.1007/s00145-023-09458-2
[Flagship IACR journal · Indexed: SCIE, Scopus · Impact factor 2.1 (JCR 2025) · JCR Q1, Mathematics, Applied]

Conference Proceedings

[C1] Wilson Tsuata, **Subhranil Dutta**, Aikaterini Mitrokotsa. Simulation Secure Quadratic Functional Encryption for Inner-Product and Quadratic Predicates. In *Public-Key Cryptography — PKC 2026*, LNCS vol. 16553, pp. 303–333, Springer, 2026. doi:10.1007/978-3-032-26737-5_10
[IACR conference · CORE Rank B · Springer LNCS · Indexed: Scopus, Web of Science CPCI]

[C2] **Subhranil Dutta**, Aikaterini Mitrokotsa, Tapas Pal, Jenit Tomy. Multi-Client Attribute-Based Unbounded Inner Product Functional Encryption, and More. In *Public-Key Cryptography — PKC 2025*, LNCS vol. 15678, pp. 3–37, Springer, 2025. doi:10.1007/978-3-031-91832-2_1
[IACR conference · CORE Rank B · Springer LNCS · Indexed: Scopus, Web of Science CPCI]

[C3] Uddipana Dowerah, **Subhranil Dutta**, Frank Hartmann, Aikaterini Mitrokotsa, Sayantan Mukherjee, Tapas Pal. SACfe: Secure Access Control in Functional Encryption with Unbounded Data. In *9th IEEE European Symposium on Security and Privacy (EuroS&P 2024)*, pp. 860–882, IEEE, 2024. doi:10.1109/EuroSP60621.2024.00053
[CORE Rank A · IEEE · Indexed: Scopus, Web of Science CPCI]

[C4] **Subhranil Dutta**, Ratna Dutta, Sourav Mukhopadhyay. Constructing Pairing-Free Unbounded Inner Product Functional Encryption Schemes with Unbounded Inner Product Policy. In *Innovative Security Solutions for Information Technology and Communications — SecITC 2022*, LNCS vol. 13809, pp. 102–116, Springer, 2022. doi:10.1007/978-3-031-32636-3_6
[Springer LNCS · Indexed: Scopus, Web of Science CPCI]

[C5] **Subhranil Dutta**, Tapas Pal, Ratna Dutta. Fully Secure Unbounded Zero Inner Product Encryption with Short Ciphertexts and Keys. In *Provable and Practical Security — ProvSec 2021*, LNCS vol. 13059, pp. 241–258, Springer, 2021. doi:10.1007/978-3-030-90402-9_13
[CORE Rank C · Springer LNCS · Indexed: Scopus, Web of Science CPCI]

Awards and Fellowships

2025	**Great Mind Postdoctoral Fellowship**, University of St. Gallen, Switzerland
2024	**ESKAS Swiss Government Excellence Scholarship**, Federal Commission for Scholarships for Foreign Students (FCS), University of St. Gallen, Switzerland Doctor of Philosophy awarded, IIT Kharagpur, India
2021	**CSIR Senior Research Fellowship (SRF)**, IIT Kharagpur
2019	**CSIR Junior Research Fellowship (JRF)**, IIT Kharagpur
2018	**GATE** qualified in Mathematics (MA) **CSIR-UGC NET** qualified for JRF, Mathematical Sciences
2017	**CSIR-UGC NET** qualified for Lectureship, Mathematical Sciences

Professional Service

Membership	International Association for Cryptologic Research (IACR)
Programme Committees	ACM ASIA APKC 2026; Indocrypt 2025; ICSP 2020, 2024, 2025
External Reviewer	Indocrypt 2021, 2024; ACM AsiaCCS 2025; CANS 2025; PETS 2025; GameSec 2025
Journal Reviewing	*Designs, Codes and Cryptography*; *Journal of Cryptographic Engineering*; *IEEE Trans. Information Forensics and Security*; *IEEE Trans. Dependable and Secure Computing*; *IEEE Trans. Computers*; *International Journal of Information Security*; among others

Teaching and Supervision

Student Supervision

2024	**Integrative Master Project** — Co-supervisor, University of St. Gallen, Switzerland

Teaching Assistantships

University of St. Gallen, Switzerland

2024–2025	Privacy-Preserving Cryptographic Protocols; Security & Privacy in Cloud-Assisted Computing

Indian Institute of Technology Kharagpur, India

2020–2022	Advanced Calculus (MA11003); Linear Algebra, Numerical & Complex Analysis (MA11004)

NPTEL / SWAYAM national online courses (instructor: Prof. Sourav Mukhopadhyay, IIT Kharagpur)

2020–2023	Fundamental Algorithms: Design and Analysis; Cryptography and Network Security; Introduction to Automata, Languages and Computation; Introduction to Abstract and Linear Algebra; Introduction to Algorithms and Analysis

Technical Skills and Languages

Computing	MATLAB, C/C++ (advanced) · LaTeX, OpenOffice, Microsoft Windows (intermediate) · HTML, Linux (basic)
Languages	Bengali (native) • English (near native) • Hindi (near native)

Referees: available on request.