# Tapas Pal

Group Leader | Secure Computation & Communication, KASTEL SRL,
Karlsruhe Institute of Technology (KIT)
Ph.D. in Cryptography, IIT Kharagpur

Am Fasanengarten 5, 76131 Karlsruhe, Germany
(+49) 15510083039 tapas.pal@kit.edu
tapaspal9.github.io/homepage 0000-0001-6278-0418
Google Scholar DBLP IACR CryptoDB

## Research Profile

Cryptographer working on the foundations and real-world deployment of advanced public-key encryption. My research designs provably secure *functional*, *attribute-based*, and *registered* encryption schemes that decentralize trust, make computation on encrypted data *verifiable*, and bring strong privacy guarantees to cloud platforms, digital infrastructure, and AI systems. The work spans rigorous theory (pairing- and lattice-based constructions with formal security proofs) and applied impact (multiple international patents and industry technology due-diligence). Author of 20+ peer-reviewed papers at leading venues (Crypto, Eurocrypt, Asiacrypt, PKC, Journal of Cryptology).

**Research Interests** Functional & attribute-based encryption; registered and multi-authority encryption; verifiable computation on encrypted data; privacy-enhancing technologies; lattice- and pairing-based cryptography; witness encryption & obfuscation; threshold and post-quantum cryptography.

## Education

**Ph.D. in Cryptography**, Indian Institute of Technology Kharagpur, India 2016 – 2021
Advisor: Prof. Ratna Dutta. Thesis: *Designing Provably Secure Advanced Cryptographic Primitives — Witness Encryption, Fully Homomorphic Encryption, and Functional Encryption*. Defended 6 October 2021.

**M.Sc. in Mathematics**, Indian Institute of Technology Kharagpur, India 2014 – 2016
CGPA 9.47/10 · Batch Rank 2.

**B.Sc. (Honours) in Mathematics**, Scottish Church College, University of Calcutta, India 2011 – 2014
First Class First · 88.88%.

## Academic & Research Appointments

**Group Leader, Secure Computation & Communication**, KASTEL Security Research Labs, KIT, Germany 2024 – present
Lead a research group on privacy-enhancing technologies; research strategy, proposal coordination, and mentoring of early-career researchers.

**Postdoctoral Fellow, Social Informatics Laboratories**, NTT Corporation, Tokyo, Japan 2022 – 2023
Computing on encrypted data and advanced functional-encryption primitives.

**Visiting Researcher, Cyber Security Group**, University of St. Gallen, Switzerland 2023: Sep-Oct
Supervised the project on multi-client attribute-based unbounded inner-product functional encryption.

**Visiting Scientist, R. C. Bose Centre for Cryptology & Security**, ISI Kolkata, India 2021: Nov-Dec
Functional encryption and its applications.

**Research Intern, Cryptography & Information Security (CIS) Lab**, NTT Research, Inc., Sunnyvale, USA 2021: Feb-Oct
Functional encryption.

**Junior & Senior Research Fellow, Department of Mathematics**, IIT Kharagpur, India 2016 – 2021
Doctoral research in cryptography.

## Research Funding & Grants

**Swiss National Science Foundation (SNSF)**, University of St. Gallen 2023
*Multi-Client Unbounded Attribute-Based Inner Product Functional Encryption* — with PI Prof. Katerina Mitrokotsa. (Completed.)

## Selected Honours & Awards

**Competing position offers (declined)** 2023
Senior Researcher, Cyber Security Group, University of St. Gallen, Switzerland; and Senior Scientist / Lecturer, Cyber Security Research Group, University of Klagenfurt, Austria.

**ERCIM Postdoctoral Fellowship**, NTNU, Norway 2021
European Research Consortium for Informatics and Mathematics.

**Junior Research Fellowship (JRF), UGC**, Mathematical Sciences 2016
All-India Rank 78.

**Joint Admission Test for M.Sc. (JAM)**, Mathematics 2014
All-India Rank 121.

**Seven merit medals & prizes for excellence in Mathematics**, Scottish Church College 2013 – 2014
Including the Krishnalal De Medal (best performance in Mathematics), Pravat Kr. Ghosh Medal, Prof. Alexander Thomson Prize, and Dr. Alexander Duff Memorial Prize.

## Publications

In theoretical cryptography, author names are listed *alphabetically* by convention; my name is shown in **bold**. Full list: Google Scholar · DBLP · IACR CryptoDB.

**Bibliometrics:** Citations 205 · h-index 09 (Google Scholar, June 13, 2026).

### Peer-Reviewed Conference Proceedings

**[C1]** **CRYPTO 2026.** Shalini Banerjee, **Tapas Pal**, Andy Rupp, Daniel Slamanig. *Simple Public-Key Anamorphic Encryption and Signature using Multi-Message Extensions.* (To appear.) [ePrint]

**[C2]** **PKC 2026.** **Tapas Pal**, Robert Schädlich. *Registered Functional Encryption for Attribute-Weighted Sums with Access Control.* 29th Intl. Conf. on Practice and Theory of Public-Key Cryptography. [Proceedings] [ePrint]

**[C3]** **ASIACRYPT 2025.** **Tapas Pal**, Robert Schädlich. *A General Framework for Registered Functional Encryption via User-Specific Pre-Constraining.* Advances in Cryptology — ASIACRYPT 2025. [Proceedings] [ePrint]

**[C4]** **PKC 2025.** Subhranil Dutta, Aikaterini Mitrokotsa, **Tapas Pal**, Tomy Jenit. *Multi-Client Attribute-Based Unbounded Inner Product Functional Encryption, and More.* [Proceedings] [ePrint]

**[C5]** **ASIACRYPT 2024.** Pratish Datta, **Tapas Pal**, Shota Yamada. *Registered FE beyond Predicates: (Attribute-Based) Linear Functions and More.* Advances in Cryptology — ASIACRYPT 2024. [Proceedings] [ePrint]

**[C6]** **IEEE EuroS&P 2024.** Uddipana Dowerah, Subhranil Dutta, Frank Hartmann, Aikaterini Mitrokotsa, Sayantan Mukherjee, **Tapas Pal**. *SACfe: Secure Access Control in Functional Encryption with Unbounded Data.* [Proceedings] [ePrint]

**[C7]** **EUROCRYPT 2024.** Taiga Hiroka, Fuyuki Kitagawa, Tomoyuki Morimae, Ryo Nishimaki, **Tapas Pal**, Takashi Yamakawa. *Certified Everlasting Secure Collusion-Resistant Functional Encryption, and More.* Advances in Cryptology — EUROCRYPT 2024. [Proceedings] [ePrint]

**[C8]** **PKC 2023.** Pratish Datta, **Tapas Pal**. *Decentralized Multi-Authority Attribute-Based Inner-Product FE: Large Universe and Unbounded.* 26th Intl. Conf. on Practice and Theory of Public-Key Cryptography. [Proceedings] [ePrint]

**[C9]** **ASIACRYPT 2022.** Pratish Datta, **Tapas Pal**, Katsuyuki Takashima. *Compact FE for Unbounded Attribute-Weighted Sums for Logspace from SXDH.* Advances in Cryptology — ASIACRYPT 2022. [Proceedings] [ePrint]

**[C10]** **ASIACRYPT 2021.** Pratish Datta, **Tapas Pal**. *Compact Adaptively Secure FE for Attribute-Weighted Sums from $k$-Lin.* Advances in Cryptology — ASIACRYPT 2021. [Proceedings] [ePrint]

**[C11]** **ProvSec 2021.** Subhranil Dutta, **Tapas Pal**, Ratna Dutta. *Fully Secure Unbounded Zero Inner Product Encryption with Short Ciphertexts and Keys.* 15th Intl. Conf. on Provable and Practical Security. [Proceedings]

**[C12]** **ACISP 2021.** **Tapas Pal**, Ratna Dutta. *Chosen-Ciphertext Secure Functional Encryption from Constrained Witness PRF.* 26th Australasian Conf. on Information Security and Privacy. [Proceedings] [ePrint]

**[C13]** **ACISP 2021.** **Tapas Pal**, Ratna Dutta. *CCA-Secure Attribute-Hiding Inner Product Encryption from Minimal Assumption.* 26th Australasian Conf. on Information Security and Privacy. [Proceedings] [ePrint]

**[C14]** **LATINCRYPT 2021.** **Tapas Pal**, Ratna Dutta. *Attribute-Based Access Control for Inner Product Functional Encryption from LWE.* 7th Intl. Conf. on Cryptology and Information Security in Latin America. [Proceedings] [ePrint]

**[C15]** **CANS 2020.** **Tapas Pal**, Ratna Dutta. *Chosen-Ciphertext Secure Multi-Identity and Multi-Attribute Pure FHE.* 19th Intl. Conf. on Cryptology and Network Security. [Proceedings] [ePrint]

**[C16]** **ProvSec 2020.** **Tapas Pal**, Ratna Dutta. *Semi-Adaptively Secure Offline Witness Encryption from Puncturable Witness PRF.* 14th Intl. Conf. on Provable and Practical Security. [Proceedings] [ePrint]

**[C17]** **ACISP 2019.** **Tapas Pal**, Ratna Dutta. *Offline Witness Encryption from Witness PRF and Randomized Encoding in CRS Model.* 24th Australasian Conf. on Information Security and Privacy. [Proceedings] [ePrint]

### Journal Articles

**[J1]** **IACR CiC 2025.** Subhranil Dutta, **Tapas Pal**, Amit Kumar Singh, Sourav Mukhopadhyay. *Fully Collusion Resistant Traceable Identity-Based Inner Product Functional Encryption.* IACR Communications in Cryptology. [Journal]

**[J2]** **DCC 2024.** Pratish Datta, **Tapas Pal**, Katsuyuki Takashima. *Compact FE for Unbounded Attribute-Weighted Sums for Logspace from SXDH.* Designs, Codes and Cryptography. [Journal]

**[J3]** **TCS 2024.** 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 the Unbounded Setting.* Theoretical Computer Science, vol. 995. [Journal]

**[J4]** **JoC 2023.** Uddipana Dowerah, Subhranil Dutta, Aikaterini Mitrokotsa, Sayantan Mukherjee, **Tapas Pal**. *Unbounded Predicate Inner Product Functional Encryption from Pairings.* Journal of Cryptology, 36(29). [Journal] [ePrint]

**[J5]** **DCC 2023.** Pratish Datta, **Tapas Pal**. *Compact Adaptively Secure FE for Attribute-Weighted Sums from $k$-Lin.* Designs, Codes and Cryptography, 91, 2917–3034. [Journal] [ePrint]

### Manuscripts under Submission / Preprints

**[P1]** **Preprint 2025.** **Tapas Pal**, Robert Schädlich, Erkan Tairi. *Registered Functional Encryption for Pseudorandom Functionalities from Lattices: Registered ABE for Unbounded-Depth Circuits and Turing Machines, and More.* [ePrint]

## Patents

**[PT1]** **US 2024.** Pratish Datta, **Tapas Pal**. *Decentralized Multi-Authority Attribute-Based Encryption for Large Universe and Unbounded.* US Patent WO2024151871A1. [Google Patents]

**[PT2]** **US 2024.** Pratish Datta, **Tapas Pal**. *Compact Functional Encryption for Unbounded Attribute-Weighted Sums.* US Patent WO2024098074A2. [Google Patents]

**[PT3]** **US/JP/EPO 2023.** Pratish Datta, Monosij Maitra, **Tapas Pal**. *Decentralized Multi-Authority Attribute-Based Inner-Product Functional Encryption.* Patent EP4254858A1. [Google Patents]

**[PT4]** **US 2023.** Pratish Datta, **Tapas Pal**. *Compact Adaptively Secure Functional Encryption for Attribute-Weighted Sums.* US Patent WO2023014969A1. [Google Patents]

## Invited Talks & Research Visits

### Invited Talks

**Swiss Crypto Day**, ETH Zurich, Switzerland — Sep 2023
*Inner Product Functional Encryption for the Real World.*

**Research Seminar**, University of Auckland, New Zealand — Jun 2019
*From Functional Encryption to Indistinguishability Obfuscation.*

### Research Visits

**University of St. Gallen, Switzerland**, Cyber Security Group — 2023
Host: Prof. Katerina Mitrokotsa.

**IIT Madras, India** — 2019
Host: Prof. Shweta Agrawal.

**University of Auckland, New Zealand** — 2019
Host: Prof. Steven D. Galbraith.

## Teaching Experience

**Cryptography and Network Security — Teaching Assistant**, NPTEL / IIT Kharagpur — 2018 – 2020
Spring 2018, 2019, 2020.

**Introduction to Abstract and Linear Algebra — Teaching Assistant**, NPTEL / IIT Kharagpur — 2018 – 2020
Autumn 2018, 2019, 2020.

**Mathematics-II — Teaching Assistant**, IIT Kharagpur — 2019
Spring 2019.

## Professional Service

| | |
|---|---|
| **Program Committee** | PKC 2027; SPACE 2026; ACM CCS 2024, 2026; WWW 2026; INDOCRYPT 2024, 2025; ICSP 2024, 2025. |
| **External Reviewer** | CRYPTO 2022–2026; EUROCRYPT 2024–2026; ASIACRYPT 2024, 2025; TCC 2022, 2025; PKC 2023, 2024; ACNS 2022; AsiaCCS 2022; INDOCRYPT 2020, 2021. |
| **Journal Referee** | Journal of Cryptographic Engineering; Designs, Codes and Cryptography; IEEE Trans. Information Forensics & Security; IEEE Trans. Information Theory; IET Information Security; Advances in Mathematics of Communications; Computer Standards & Interfaces. |
| **Expert Reviewer** | American Mathematical Society (AMS): Mathematical Reviews Database |

## Industry Consulting & Knowledge Transfer

**Cryptography Consultant (pro bono)**, D11Z.Ventures GmbH & Co. KG Nov 2025
Technical due-diligence on a password-less access-control platform (MyCena); startup evaluation and advisory.

**Cryptography Consultant (pro bono)**, D11Z.Ventures GmbH & Co. KG Mar 2025
Technical due-diligence on cryptographic image-authenticity technology (TrustNXT); startup evaluation and advisory.

## Technical Skills & Languages

| | |
|---|---|
| **Programming** | C/C++. |
| **Scientific Computing** | MATLAB, Mathematica. |
| **Tools & Typesetting** | LaTeX, Linux. |
| **Languages** | Bengali (native); Hindi (fluent); English (fluent, full professional working proficiency). |

## References


**Prof. Ratna Dutta**
Dept. of Mathematics, IIT Kharagpur, India
ratna@maths.iitkgp.ac.in
facweb.iitkgp.ac.in/~ratna

**Dr. Andy Rupp**
Faculty of Science, Technology & Medicine,
University of Luxembourg, Luxembourg
andy.rupp@uni.lu
uni.lu/…/andy-rupp

**Dr. Ryo Nishimaki**
Distinguished Research Scientist,
Social Informatics Laboratories, NTT, Tokyo, Japan
ryo.nishimaki@ntt.com
nishimaki.info

**Prof. Sourav Mukhopadhyay**
Dept. of Mathematics, IIT Kharagpur, India
sourav@maths.iitkgp.ac.in
facweb.iitkgp.ac.in/~sourav

**Prof. Daniel Slamanig**
Department of Computer Science,
Universität der Bundeswehr München, Germany
daniel.slamanig@unibw.de
https://danielslamanig.info

**Prof. Katerina Mitrokotsa**
School of Computer Science,
University of St. Gallen, Switzerland
katerina.mitrokotsa@unisg.ch
cybersecurity.unisg.ch/people/Katerina