MC 5, Universitätsstraße 140
Bochum 44799, Germany
anirban.chakraborty@mpi-sp.org
www.an1rb4n.in/
anirban-chakraborty-b20926aa
QzcCWLMAAAAJ
homepages/73/2286-3

Anirban Chakraborty

Current Position

Postdoctoral Researcher at Max Planck Institute for Security and Privacy, Germany

Visiting Researcher at Chair of Computer Security, Ruhr Universität Bochum

June 2024–*Present* I am a postdoctoral researcher at the Max Planck Institute for Security and Privacy, jointly hosted by *Peter Schwabe* and *Yuval Yarom*. Additionally, I am a visiting researcher at Ruhr Universität Bochum. Previously, I was a PhD student under the supervision of *Debdeep Mukhopadhyay* at the Indian Institute of Technology Kharagpur, India. My research focuses on microarchitectural and hardware security, particularly side-channel leakage, speculative execution, and secure processor design. I also develop automated techniques for analysing the security of cryptographic software and trusted execution environments, bridging hardware security, systems security, and software analysis.

Education

2018 - 2024 **Ph.D Degree, Computer Science and Engineering**, *Indian Institute of Technology Kharagpur, India*, Thesis: Exploring Side-Channel Leakages in Modern Computer Architectures

2011–2015 **B.Tech Degree, Computer Science and Engineering**, *Maulana Abul Kalam Azad University Of Technology, (erstwhile West Bengal University Of Technology), DGPA – **8.3/10***

Peer-Reviewed Conference Publications

[c21] Annika Wilde, Marco Gutfleisch, Felix Reichmann, Anirban Chakraborty, Yuval Yarom, Angela Sasse, Ghassan Karame: **"They don't care about this": A Systematic Study of TEE Build Reproducibility in the Wild**: *33rd ACM Conference on Computer and Communications Security (CCS 2026), The Hague, Netherlands, November, 2026*. (accepted).

[c20] Gianmarco Lusvardi, Mauro Andreolini, Luca Ferretti, Yuval Yarom, Anirban Chakraborty: **0xELF: Reverse Engineering Framework for Flexo-Generated Weird Machines**: *29th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2026), Lancaster, UK, October, 2026*.

[c19] Roland Czerny, Simon Lammer, Lukas Giner, Anirban Chakraborty, Daniel Gruss: **Fast and Secure LLC Caches via Spatial Windows**: *23rd Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2026), Chania, Greece: July, 2026*.

[c18] Yanik Kleibrink, Anirban Chakraborty, Yuval Yarom: **General Store: Speculative Address Translation in x86 Processors**: *Proceedings of the Microarchitecture Security Conference 2026, Leuven, Belgium: February, 2026*.

[c17] Anirban Chakraborty*, Nimish Mishra*, Sayandeep Saha, Sarani Bhattacharya, Debdeep Mukhopadhyay: **Systematic Evaluation of Randomized Cache Designs against Cache Occupancy**: *34th USENIX Security Symposium (Usenix 2025), Seattle, WA, USA: August, 2025*. (*Equal Contribution).

[c16] Bhuvnesh Chaturvedi, Anirban Chakraborty, Ayantika Chatterjee, Debdeep Mukhopadhyay: **IND-CPA^C: A New Security Notion for Conditional Decryption in Fully Homomorphic Encryption**: *16th International Conference on Post-Quantum Cryptography (PQCRYPTO 2025), Taipei, Taiwan: April, 2025*.

[c15] Bhuvnesh Chaturvedi, Anirban Chakraborty, Ayantika Chatterjee, Debdeep Mukhopadhyay: **Model Stealing Attacks On FHE-based Privacy-Preserving Machine Learning through Adversarial Examples**: *23rd International Conference on Cryptology And Network Security (CANS 2024), Cambridge, UK: September, 2024*.

[c14] Bhuvnesh Chaturvedi, Anirban Chakraborty, Ayantika Chatterjee, Debdeep Mukhopadhyay: **"Ask and Thou Shall Receive": Reaction-based Full Key Recovery Attacks on FHE**: *29th European Symposium on Research in Computer Security (ESORICS 2024), Bydgoszcz, Poland: September, 2024*.

[c13] Anirban Chakraborty, Nimish Mishra, Debdeep Mukhopadhyay: **Shesha: Multi-head Microarchitectural Leakage Discovery in new-generation Intel Processors**: *33rd USENIX Security Symposium (Usenix 2024), Philadelphia, PA, USA: August, 2024*.

[c12] Animesh Singh, Smita Das, Anirban Chakraborty, Rajat Sadhukhan, Ayantika Chatterjee, Debdeep Mukhopadhyay: **FHEDA: Efficient Circuit Synthesis with Reduced Bootstrapping for Torus FHE**: *9th IEEE European Symposium on Security and Privacy (EuroS&P 2024), Vienna, Austria: July, 2024*.

[c11] Nimish Mishra, Rahul Arvind Mool, Anirban Chakraborty, Debdeep Mukhopadhyay: **Plug Your Volt: Protecting Intel Processors against Dynamic Voltage Frequency Scaling based Fault Attacks**: *61th ACM/IEEE Design Automation Conference (DAC 2024), San Francisco, California, USA: July, 2024*.

[c10] Nimish Mishra, Tridib Lochan Dutta, Shubhi Shukla, Anirban Chakraborty, Debdeep Mukhopadhyay: ***Too Hot to Handle*: Novel Thermal Side-Channels in Power Attack protected Intel processors**: *IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington DC, USA: May, 2024*.

[c9] Nimish Mishra, Anirban Chakraborty, Debdeep Mukhopadhyay: **Faults in Our Bus: Novel Bus Fault Attack to Break ARM TrustZone**: *The Network and Distributed System Security Symposium (NDSS 2024), San Diego, CA, USA: Feb-March, 2024*.

[c8] Anirban Chakraborty, Sarani Bhattacharya, Sayandeep Saha, Debdeep Mukhopadhyay: **Are Randomized Caches Truly Random? Formal Analysis of Randomized-Partitioned Caches**: *IEEE International Symposium on High-Performance Computer Architecture (HPCA 2023), Montreal, Canada: February 2023*.

[c7] Rajat Sadhukhan, Anirban Chakraborty, Debdeep Mukhopadhyay: **FUNDAE: Fault Template Attack on SUNDAE-GIFT AEAD Scheme**: *Asian Hardware Oriented Security and Trust Symposium (AsianHOST 2022), Singapore: December, 2022*.

[c6] Nimish Mishra, Anirban Chakraborty, Urbi Chatterjee, Debdeep Mukhopadhyay: **Time's a Thief of Memory - Breaking Multi-tenant Isolation in TrustZones Through Timing Based Bidirectional Covert Channels**: *Smart Card Research and Advanced Applications Conference (CARDIS 2022), Birmingham, UK: November, 2022*.

[c5] Anirban Chakraborty*, Nikhilesh Singh*, Sarani Bhattacharya, Chester Rebeiro, Debdeep Mukhopadhyay: **Timed speculative attacks exploiting store-to-load forwarding bypassing cache-based countermeasures**: *59th ACM/IEEE Design Automation Conference (DAC 2022), San Francisco, California, USA: July, 2022*. (*Equal Contribution).

[c4] Rajat Sadhukhan, Anirban Chakraborty, Nilanjan Datta, Sikhar Patranabis, Debdeep Mukhopadhyay: **Light but Tight: Lightweight Composition of Serialized S-Boxes with Diffusion Layers for Strong Ciphers**: *Security, Privacy, and Applied Cryptography Engineering Conference (SPACE 2022), Jaipur, India: December, 2022*.

[c3] Anirban Chakraborty, Manaar Alam, Debdeep Mukhopadhyay: **A Good Anvil Fears No Hammer: Automated Rowhammer Detection Using Unsupervised Deep Learning**: *International Conference on Applied Cryptography and Network Security Workshop (ACNSW): Kamakura, Japan: June, 2021*.

[c2] Anirban Chakraborty, Sarani Bhattacharya, Sayandeep Saha, Debdeep Mukhopadhyay: **ExplFrame: Exploiting Page Frame Cache for Fault Analysis of Block Ciphers**: *IEEE Design, Automation and Test in Europe Conference (DATE): Grenoble, France: March, 2020*.

[c1] Anirban Chakraborty, Manaar Alam, Debdeep Mukhopadhyay: **Deep Learning Based Diagnostics for Rowhammer Protection of DRAM Chips**: *IEEE Asian Test Symposium (ATS): Kolkata, India: November, 2019*.

Peer-Reviewed Journal Publications

[j5] Shubhi Shukla, Abhijeet Singh, Rajdeep Chakraborty, Anirban Chakraborty, Harshal Mumbaikar, Manoj Kumar Munigala, Madhusudhan K N, Pabitra Mitra, Debdeep Mukhopadhyay: **Minimal Counters, Maximum Insight: Simplifying System Performance with HPC Clusters for Optimized Monitoring**: *IEEE Computer Architecture Letters (CAL): 177-180 (2025).*

[j4] Nimish Mishra, Kuheli Pratihar, Satota Mandal, Anirban Chakraborty, Ulrich Rührmair and Debdeep Mukhopadhyay: **CalyPSO: An Enhanced Search Optimization based Framework to Model Delay-based PUFs**: *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) (2024, issue 1): 501-526.*

[j3] Anirban Chakraborty, Manaar Alam, Vishal Dey, Anupam Chattopadhyay, Debdeep Mukhopadhyay: **A Survey on Adversarial Attacks and Defences**: *CAAI Transactions on Intelligence Technology 6(1) (2021): 25-45.*

[j2] Anirban Chakraborty, Sarani Bhattacharya, Manaar Alam, Sikhar Patranabis, Debdeep Mukhopadhyay: **RASSLE: Return Address Stack based Side-channel Leakage**: *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES) (2021, issue 2): 275-303.*

[j1] Sikhar Patranabis, Debapriya Basu Roy, Anirban Chakraborty, Naveen Nagar, Astikey Singh, Debdeep Mukhopadhyay, Santosh Ghosh: **Lightweight Design-for-Security Strategies for Combined Countermeasures Against Side Channel and Fault Analysis in IoT Applications**: *Journal of Hardware and Systems Security (HASS): 26 Sept, 2018.*

Manuscripts and Preprints

[i3] Xinrui Wang, Pascal Kosak, Christof Paar, Daniel Genkin, Yuval Yarom, Anirban Chakraborty: **Randomized Caches in Hardware: Challenges and Trade-offs**: *arXiv preprint arXiv:2611.00282 (2026).*

[i2] Bhuvnesh Chaturvedi, Anirban Chakraborty, Ayantika Chatterjee, Debdeep Mukhopadhyay: **vr^{2}FHE-Securing FHE from Reaction-based Key Recovery Attacks**: *IACR Cryptology ePrint Arch. 2023: 561 (2023).*

[i1] Anirban Chakraborty, Sarani Bhattacharya, Sayandeep Saha, Debdeep Mukhopadhyay: **Rowhammer induced intermittent fault attack on ECC-hardened memory**: *IACR Cryptology ePrint Arch. 2020: 380 (2020).*

Projects

October 2025 - Present — ***Microarchitectural Weird Machine***

Sponsor — *Deutsche Forschungsgemeinschaft (DFG), Germany*

Co-PI — This project aims to explore the emergent behavior of microarchitectural weird machines in modern computers. In this project, we 1) identify the essential properties of the processor architecture that enable microarchitectural weird machines as well as investigate the computational capabilities of microarchitectural weird machines, 2) identify novel offensive and defensive uses of microarchitectural weird machines, and 3) develop an automated framework to discover novel microarchitectural weird machines.

August 2023 - July 2024 — ***Security Exploration of Intel Server Platforms***

Sponsor — *Intel Corporation Inc., USA*

This Project aims to look at Intel's new generation server platform artefacts, which are often less explored in the context of security vulnerabilities. In this project, we 1) Develop methodologies for exploring vulnerabilities in trusted platform technologies like Intel SGX, TDX and TDX-IO, 2) Explore the possibilities of physical side channel attacks on Intel Platform Firmware Resilience (PFR), 3) Develop methodologies for exploring potential exposure to assets of multiple security technologies through out-of-band interface, and 4) Develop methodologies for exploring security vulnerabilities in Intel memory encryption technologies like TME and MKTME.

October 2022 - July 2024 ***AI Assisted Autonomous Verification of SoCs***

Sponsor *Intel Corporation Inc., India*

This project aims to explore the use of AI assisted techniques for system verification and faster verification closure. Our goal is to develop a semi-autonomous verification framework that can execute, modulate, and refine stimuli for faster coverage closure and enable investigating corner case scenarios at system level. In this project, my role is centered around developing an automated methodology for evaluating the vulnerability of processors against potential micro-architectural and side-channel attacks, with special focus on transient leakages and micro-architectural data sampling (MDS).

May 2018 - December 2023 ***Secure Resource-Constrained Communication Framework for Tactical Networks using Physically Unclonable Functions***

Sponsor *Defence Research and Development Organization, India*

The objective of this project is to develop a secure platform for interaction of multiple devices, which are components of tactical networks. The security mechanisms need to be extremely light-weight and protected against physical attacks due to their ubiquity. My role in this project revolved around designing a lightweight side-channel secure block cipher. The final outcome will be deployed for several defence applications, such as 1) Unmanned border applications, 2) Secured building automation, 3) Unmanned warfare. The networks fortified by these techniques are expected to subvert serious attacks often targeted by adversaries to create calamity and jeopardize the objectives.

June 2020- Sept 2022 ***Security Verification of HAL Real-Time Operating System***

Sponsor *Hindustan Aeronautics Limited, Bangalore, India*

HAL has developed an indigenous Real Time Operating System (HAL-OS) based on ARINC653 specification. As part of the security enhancement process for the HAL-OS, we have conducted an extensive security evaluation and proposed suitable countermeasures on HAL-OS. The work involved vulnerability analysis of HAL-OS by mounting various types of attacks to bypass the HAL-OS security policy. We have also proposed several security countermeasures that were implemented by HAL to make their OS robust against different attacks.

Professional Activities and Services

- **Program Committee:** ACNS 2025, CCS 2025, CHES 2026, USENIX SEC 2026, CCS 2026, WOOT 2026, EuroS&P 2026, USENIX SEC 2027, CHES 2027, EuroS&P 2027
- **Journal Reviewer:** TIFS, TC, CSUR, TACO, HASS
- **Artifact Evaluation:** CCS 2023, HPCA 2024

Scholastic and Personal Achievements

- Assigned **CVE-2026-5598**, **CVE-2026-18036**, and **CVE-2026-18040** for discovering constant-time violations leading to a timing channel in multiple post-quantum crypto schemes in BouncyCastle.
- Assigned **CVE-2024-14041** (jointly with other teams) for discovering non-constant-time division in message decoding and ciphertext compression in Kyber KEM in BouncyCastle.
- Assigned **CVE:2022-47549** (along with co-authors) for demonstrating bypass of signature verification and installing malicious trusted applications via electromagnetic fault injections in OPTEE.
- Discovered (along with co-authors) **integer overflow vulnerability** leading to NULL pointer dereference in Linaro TEE, leading to a patch in Linux kernel stable tree.
- Participated (on invitation) in **Intel Project Circuit Breaker Bug Bounty Program** for exploring vulnerability in Intel TDX technology and was awarded US$ 4500.
- **Speaker** at BlackHat Asia Briefings 2024, held in Singapore.
- **PhD Dissertation Award finalist** at IEEE HOST 2024.
- **Won ACM-India/IARCS Travel Grant** for HPCA 2023, held in Montreal, Quebec, Canada.
- **Winner** and **runner-up** at the Cyber Security Awareness Week (CSAW): Embedded Security Challenge (ESC) in India in 2022 and 2020, respectively.

Teaching

Winter 2026	**CPU Implementation** ○ *Co-Instructor: Xinrui Wang*
Summer 2026	**Introduction to CPU Design** ○ *Instructor: Prof. Yuval Yarom*
2025-2026	**Computer Architecture** ○ *Instructor: Prof. Yuval Yarom*
2025 - 2026	**Cache Attacks** ○ *Instructor: Prof. Yuval Yarom*
2024 - 2025	**Microarchitectural Attacks and Defenses** ○ *Instructor: Prof. Yuval Yarom*
2020 - 2023	**High Performance Computer Architecture** ○ *Instructor: Prof. Debdeep Mukhopadhyay*
2022 - 2023	**Parallel Algorithms** ○ *Instructor: Prof. Debdeep Mukhopadhyay*
Autumn 2021	**Programming and Data Structures** ○ *Instructor: Prof. Debdeep Mukhopadhyay*
Autumn 2019	**Discrete Mathematics** ○ *Instructor: Prof. Abhijit Das*
Spring 2019	**Algorithms Laboratory** ○ *Instructor: Prof. Abhijit Das*
2019 - 2023	**Hardware Security (NPTEL Online MOOC)** ○ *Instructor: Prof. Debdeep Mukhopadhyay*

Industry Experience

October 2015-May 2018 **Tata Consultancy Services Pvt. Ltd., Kolkata**, *Systems Engineer*
Mainframe and SAS developer under India's leading IT company. Developed and maintained software infrastructure that supported the entire production line of an international steel-producing company.

References

- **Dr. Yuval Yarom**, Professor, Chair of Computer Security, Faculty of Computer Science, Ruhr-University Bochum, Germany, yuval.yarom@rub.de
- **Dr. Debdeep Mukhopadhyay**, Professor, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, debdeep@cse.iitkgp.ac.in
- **Dr. Peter Schwabe**, Scientific Director, Max Planck Institute for Security and Privacy peter.schwabe@mpi-sp.org