Shibam **GHOSH**

PhD Student, University of Haifa, Haifa, Israel

Room 558, Port Campus, University of Haifa

+972587858750 | shibam.math@gmail.com | ShibamCrS

I am currently pursuing my **PhD** in the **Department of Computer Science** at the **University of Haifa**, under the supervision of Prof. Orr Dunkelman. I began my doctoral studies in October 2020. Before this, I completed my master's thesis as a research intern at **INRIA, Paris**, under the guidance of Anne Canteaut and Léo Perrin.

Research Interests

- Cryptanalysis of Symmetric-key Primitives
- Symmetric-key Primitive Design
- Lightweight Cryptography
- White-box Cryptography
- Provable Security

Education

Indian Statistical Institute — *Kolkata, India*

Master of Technology in Cryptology and Security — *2018 – 2020*

Presidency University — *Kolkata, India*

Master of Science in Mathematics — *2015 – 2017*

Krishnagar Government College — *Krishnagar, India*

Bachelor of Science in Mathematics — *2012 – 2015*

Research Experience

University of Haifa — *Haifa, Israel*

PhD Student — *Oct 2020 – Currently*

- Supervisor: Prof. Orr Dunkelman
- My PhD research has centered on cryptanalysis, focusing on the design and analysis of symmetric primitives.
- A significant portion of my work is dedicated to the algebraic cryptanalysis of these primitives. Some key contributions:
  - An enhanced Fast Fourier Transform-based key-recovery attack on 6-round **AES**.
  - Algebraic cryptanalysis of NIST LwC candidates **Ascon**, **KNOT**, and **TinyJAMBU**.
  - Distinguishers derived from the structural symmetry of **SHA3**, **Xoodyak**, and the Belarusian standard **bash**.
  - Division property-based fault attacks on the **GIFT** and **Present** ciphers.
- In addition to cryptanalysis, I have co-designed the tweakable block cipher **QARMAv2**, tailored for memory protection.
- My research also extends into the area of re-keying techniques, where I have analyzed the security of the IETF/ISO standard Advanced CryptoPro Key Meshing (**ACPKM**) internal rekeying technique, widely used in Russian variants of TLS and CMS.

Institut national de recherche en sciences et technologies du numérique (INRIA) — *Paris, France*

Research Intern — *Jan – July, 2020*

- Supervisor: Anne Canteaut, Léo Perrin
- Master's Dissertation: On the QIC of quadratic APN functions (available online here)
- My master's research focused on cryptographic Boolean functions, with particular emphasis on the Big APN Problem.
- Our goal was to generate quadratic APN functions of size ≥ 8.
- The search for APN permutations and their classification has been an open challenge for over 25 years.
- Our core approach involved representing a quadratic vectorial Boolean function using a cubic structure called a Quadratic Indicator Cube (QIC) and identifying the criteria associated with this cube that are necessary and sufficient for a function to be APN.

Publications

Journal Articles

1. Roberto Avanzi, Subhadeep Banik, Orr Dunkelman, Maria Eichlseder, Shibam Ghosh, Marcel Nageler, and Francesco Regazzoni. The QARMAv2 Family of Tweakable Block Ciphers. *IACR Transactions on Symmetric Cryptology*, 2023(3):25–73, 2023 (DOI)

2. Orr Dunkelman, Shibam Ghosh, and Eran Lambooij. Practical Related-Key Forgery Attacks on Full-Round TinyJAMBU-192/256. *IACR Trans. Symmetric Cryptol.*, 2023(2):176–188, 2023 (DOI)

3. Orr Dunkelman, Shibam Ghosh, and Eran Lambooij. Attacking the IETF/ISO Standard for Internal Re-keying CTR-ACPKM. *IACR Trans. Symmetric Cryptol.*, 2023(1):41–66, 2023 (DOI)

Conference Papers

1. Orr Dunkelman, Shibam Ghosh, Nathan Keller, Gaëtan Leurent, Avichai Marmor, and Victor Mollimard. Partial Sums Meet FFT: Improved Attack on 6-Round AES. In *Advances in Cryptology – EUROCRYPT 2024*, pages 128–157. Springer, 2024 (DOI)

2. Anup Kumar Kundu, Shibam Ghosh, Dhiman Saha, and Mostafizar Rahman. Divide and Rule: DiFA - Division Property Based Fault Attacks on PRESENT and GIFT. In *ACNS (1)*, volume 13905 of *Lecture Notes in Computer Science*, pages 89–116. Springer, 2023 (DOI)

3. Orr Dunkelman, Shibam Ghosh, and Eran Lambooij. Full Round Zero-Sum Distinguishers on TinyJAMBU-128 and TinyJAMBU-192 Keyed-Permutation in the Known-Key Setting. In *INDOCRYPT*, volume 13774 of *Lecture Notes in Computer Science*, pages 349–372. Springer, 2022 (DOI)

4. Nilanjan Datta, Avijit Dutta, and Shibam Ghosh. INT-RUP Security of SAEB and TinyJAMBU. In *INDOCRYPT*, volume 13774 of *Lecture Notes in Computer Science*, pages 146–170. Springer, 2022 (DOI)

5. Shibam Ghosh and Orr Dunkelman. Automatic Search for Bit-Based Division Property. In *LATINCRYPT*, volume 12912 of *Lecture Notes in Computer Science*, pages 254–274. Springer, 2021 (DOI)

6. Shibam Ghosh and Léo Perrin. Some Experimental Results on Quadratic APN Functions. In *Boolean Functions and their Applications (BFA) 2021*, 2021 (available online here)

Under Submission

1. Ravi Anand, Shibam Ghosh, Takanori Isobe, and Rentaro Shiba. Quantum key recovery attacks on 4-round iterated even-mansour with two keys. Cryptology ePrint Archive, Paper 2024/1278, 2024 (Accepted and forthcoming at the 27th Information Security Conference (ISC 2024), eprint)

2. SAHIBA SURYAWANSHI, Shibam Ghosh, Dhiman Saha, and Prathamesh Ram. Simple Vs Vectorial: Exploiting Structural Symmetry to Beat the ZeroSum Distinguisher Applications to SHA3, Xoodyak and Bash. Cryptology ePrint Archive, Paper 2024/052, 2024 (under submission to DCC, eprint)

3. Automatically Verifying Differential Characteristics and Learning Key Conditions (Major Revision, FSE 2024)

4. ToFA: Towards Fault Analysis of GIFT and GIFT-like Ciphers Leveraging Truncated Impossible Differentials

Research Talks Delivered

2024	**Partial Sums Meet FFT: Improved Attack on 6-Round AES**, Eurocrypt, 2024	*Zurich, Switzerland*
2023	**Attacking the IETF/ISO Standard for Internal Re-keying CTR-ACPKM**, FSE, 2023	*Kobe, Japan*
2022	**Full Round Zero-Sum Distinguishers on TinyJAMBU-128 and TinyJAMBU-192**, Indocrypt, 2022	*Kolkata, India*
2021	**Automatic Search for Bit-based Division Property**, Latincrypt, 2021	*Vitual*
2021	**Some Experimental Results on Quadratic APN Functions**, BFA, 2021	*Vitual*

Technical Projects

Improved Attack on 6-Round AES

Practical Attacks

- I have presented a Fast Fourier Transform-based key-recovery attack on 6-round **AES** at Eurocrypt 2024.
- The attack is fully implemented in C and verified on Amazon AWS servers.
- The source code is available in my git and published in IACR artifact.

Forgery Attacks on NIST Lightweight Crypto Finalist TinyJAMBU

Practical Attacks

- I have implemented a practical related-key forgery attack on the **TinyJAMBU**-v2 with 256/192-bit keys in C.
- Part of this work was published at FSE 2023 and the source code is available in my git.

Automatic Tools For Algebraic Attacks

Tools In Cryptanalysis

- I have prepared Pyhon-based automatic tools for cryptanalysis of NIST lightweight ciphers using MILP, SAT, and CP, available in my git.

Automatic Tool for Verifying Differential Characteristics

Tools In Cryptanalysis

- This project involves developing a tool using publicly available #SAT solvers that thoroughly verifies differential characteristics.
- The tool calculates the expected probability of differential characteristics while considering the cipher's key schedule.
- This tool also estimates the size of the key-space that validates the characteristic and deduces conditions for these keys.
- The paper is being submitted and the tool will appear soon in my git.

Ongoing Projects

Security Analysis of Arm's Pointer Authentication Code (PAC)

Practical Attacks

- This project focuses on the Qarma cipher, utilized in the Arm A-profile and M-profile architectures as a Pointer Authentication Code.
- Pointer Authentication is important to mitigate Return-Oriented Programming (ROP) exploits.
- We are preparing an SAT-solver-based automatic tool to search differential properties of Qarma.

White-Box Secure Cipher

Primitive Design

- We aim to propose an Even-Mansour variant of white-box secure cipher family
- The main objective is to achieve space-hardness and longevity security in specific adversarial environments.

Embedded Code Encryption

Primitive Design

- We aim to propose a low-latency block cipher intended to support external memory encryption.
- My primary contribution is in the analysis of the block cipher.

Teaching Experience

University of Haifa

Haifa, Israel

Teaching Assistant

2022 – 2024

- Introduction to cryptography, Spring Semester, 2022 (lecturer in charge: Prof. Orr Dunkelman)
- Introduction to cryptography, Spring Semester, 2023 (lecturer in charge: Prof. Orr Dunkelman)
- Introduction to cryptography, Spring Semester, 2024 (lecturer in charge: Prof. Orr Dunkelman)
- Israeli School on Biometrics, 2024 (lecturer in charge: Prof. Orr Dunkelman)

Other Professional Activities

Reviewer

- Asiacrypt 2024
- Selected Areas in Cryptography (SAC) 2024
- Designs, Codes and Cryptography (DCC) 2024, 2023, 2022

Awards

2021	**Israeli Science Foundation (ISF) Fellowship**, Israeli Science Foundation (ISF)	*Haifa, Israel*
2020	**Data Science Research Center (DSRC) Fellowship**, University of Haifa	*Haifa, Israel*
2020	**Awarded departmental-topper prize**, Indian Statistical Institute	*Kolkata, India*
2019	**Rank 88 in National Eligibility Test**, Council of Scientific and Industrial Research (CSIR), India	*Kolkata, India*

Technical Skills

- C, C++ ●●●●○
- python, SageMath ●●●●○
- Rust ●●●○○
- Git ●●●●○
- Qiskit ●●●○○

Languages

Native Bengali
Fluent English, Hindi