Sumesh Manjunath Ramesh

✉ r.sumesh.manjunath@nyu.edu • in Linkedin

Education

New York University — **New York,USA**
Ph.D., Computer Science — *2017 - present*

IIIT Delhi — **New Delhi,INDIA**
Master of Technology, Computer Science & Engineering specialized in Information Security — *2011–2013*

Anna University — **Tamil Nadu,INDIA**
Bachelor of Engineering, Computer Science & Engineering — *2006–2010*

Publications

In Conference Proceedings

2019: **Sumesh Manjunath Ramesh** and Hoda AlKhzaimi. Side Channel Analysis of SPARX-64/128: Cryptanalysis and Countermeasures. In *Progress in Cryptology – AFRICACRYPT 2019*, pages 352–369. Springer International Publishing, 2019.

2015: Manish Shukla, **Sumesh Manjunath**, Rohit Saxena, Sutapa Mondal and Sachin Lodha. POSTER: WinOver Enterprise Dark Data. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, page 1674–1676, New York, NY, USA, 2015. Association for Computing Machinery.

2015: **Sumesh Manjunath R** Donghoon Chang and Somitra Kumar Sanadhya. PPAE: Practical Parazoa Authenticated Encryption Family. In Man-Ho Au and Atsuko Miyaji, editors, *Provable Security*, pages 198–211. Springer International Publishing, 2015.

Manuscripts

2023: **Sumesh Manjunath Ramesh** and Hoda Alkhzaimi. Power Leakage Model Based on Technology Library. Is It More Effective than Hamming Distance Model? Manuscript in submission, 2023.

2023: **Sumesh Manjunath Ramesh** and Hoda Alkhzaimi. DHABI FRAMEWORK: Pursuing Practical Links amidst Statistical Cryptanalysis and Side-Channel Analysis. Manuscript in submission, 2023.

2023: **Sumesh Manjunath Ramesh** Faisal Hameed and Hoda Alkhzaimi. Hybrid Generalization in Machine Learning-based Side Channel Analysis. Manuscript in submission, 2023.

Thesis

2013: **Sumesh Manjunath R**. Provably Secure Authenticated Encryption Modes. Master's thesis, Indraprastha Institute of Information Technology, 2013. Available at `https://repository.iiitd.edu.in/jspui/handle/123456789/100`.

Granted Patents

2020: Sutapa Mondal, **Sumesh Manjunath** and Rohi Saxena, Manish Shukla, Purushotam Gopaldas Radadia, Shirish Subhash Karande and Sachin Premsukh Lodha. *Systems and Methods for Sensitive Audio Zone Rearrangement*, March 24 2020. US Patent 10,599,864.

2019: **Sumesh Manjunath**, Manish Shukla, Sutapa Mondal, Rohit Saxena, Sachin Premsukh Lodha. *Systems and Methods for Estimating Temporal Importance of Data*, May 21 2019. US Patent 10,296,523 B2.

2019: **Sumesh Manjunath** Manish Shukla, Sachin Premsukh Lodha, Rohit Saxena and Sutapa Mondal. *Method and System for Efficient Selective Backup Strategy in an Enterprise*, February 5 2019. US Patent 10,198,322.

2019: Ravi Hanmant Mahamuni, Rohit Saxena and **Sumesh Manjunath**. *Automating a Process Associated with a Web Based Software Application*, July 23 2019. US Patent 10,362,090.

Research Experience

with Dr.Hoda Alkhzaimi **EMERATSEC Lab, NYUAD, UAE**
Senior Research Assistant *Sep 2023 – present*
Research exploration of symmetric cryptanalysis in the quantum world and design of side-channel resistant lightweight ciphers.

with Dr.Hoda Alkhzaimi **CCSAD, NYU Abu Dhabi, UAE**
Graduate Research Assistant *Jul 2017 – Aug 2023*
Research exploration on hardware implementation of lightweight block ciphers and their side-channel analysis, resulting in 1 publication and 3 under-review.

with Dr.Rajan M A, Senior Scientist **TCS Research, Bengaluru, INDIA**
Researcher *Apr 2016 – Jun 2017*
Contributed to a literature survey on private consensus algorithms for private blockchain applications in an enterprise.

with Dr.Sachin Lodha, Chief Scientist **TCS Research, Pune, INDIA**
Researcher *Jul 2013 – Mar 2016*
Developed Proof-of-Concepts for projects on Data Analytics and Password Management tools, resulting in 4 patents and 1 poster publication.

with Dr.Somitra Sanadhya and Dr.Donghoon Chang **IIIT Delhi, INDIA**
Research Assistant *Jan 2012 – May 2013*
Developed and proposed two Authenticated Encryption Modes, earning the Best Thesis Award in 2013, and subsequently published a variant of the results.

Research Projects

New York University Abu Dhabi, Abu Dhabi, UAE

Technology Leakage Power Library Model *2022 – 2023*
I am proposing a new leakage model for side-channel analysis based on the value of the power consumption of the technology library cell. This model extracts the secret key and is comparable to the Hamming distance model in linear correlation, with the potential to achieve a better success rate when non-linear correlation techniques are applied.

Framework to link Side-Channel Technique with Statistical Cryptanalysis *2019 – 2021*
I am proposing a novel technique that combines side-channel analysis (SCA) with statistical analysis to break real-world ciphers. The main idea is to extract values from the intermediate state through SCA and use them for key extraction through statistical techniques.

Side-Channel Analysis of ARX Cipher *Jan 2018 – Jul 2019*
I implemented correlation power analysis (CPA) on the SPARX ARX block cipher using the SAKURA-G board. Furthermore, I proposed a serialized threshold implementation of the SPARX block cipher to counter the CPA.

TCS Research, Bengaluru, INDIA

Analyze Consensus Protocols for Private Blockchain *Apr 2016 – Jun 2017*
I evaluated various consensus protocols for a private blockchain within an organization and actively contributed to the development of a consensus framework tailored for the private blockchain.

Tata Research Development and Design Center, Pune, INDIA

Enterprise Dark Data Analytics *Jul 2015 – Mar 2016*
I was involved in multiple projects. In one, I developed a framework to identify and analyze similar files within an enterprise. Additionally, I proposed a methodology for selectively backing up files with a minimal footprint. In another project. In another project, I designed and implemented a tool to identify a social network among employees based on email metadata.

Privacy Preserving Tool for Password Management *Jul 2013 – 2014*
I played a key role in the team that developed and deployed a privacy-focused tool to securely manage passwords from web applications within our organization.

IIIT Delhi, New Delhi, INDIA

Design Authenticated Encryption Modes *Jun 2012 - May 2013*
I designed two new authenticated encryption modes: FPAE, based on a random permutation-based hash mode called FP, and FWPAE, based on a random function-based hash mode called FWP.

Fellowships & Awards

2017 - 2023: ***NYUAD Global Ph.D. Student Fellowship*** of New York University Abu Dhabi, as a NYUAD Global Ph.D. Student Fellow.

2016: Received the ***High Performer Award*** for my contributions to research activities at TCS Research.

2013: Recipient of ***Best M.Tech. Thesis Award*** from ***Indraprastha Institute of Information Technology, Delhi,*** for my Master's thesis.

Talks

2021: Gave a talk on ***Attacks on Lightweight Ciphers: Pathways from Side-Channel Attacks to Differential Attacks*** at the TII Crypto Seminar 2021, UAE on January 28^{th}, 2021.

2019: Gave a talk on ***Side-Channel Analysis of SPARX-64/128: Cryptanalysis and Countermeasures*** at the 11^{th} International Conference on Cryptology, AFRICACRYPT 2019, Morocco on July 11^{th}, 2019.

2018: Gave an invited talk on ***Introduction to Cryptology*** at the Rochester Institute of Technology, Dubai on November 1^{st} 2018.

Professional Services

2022: I served as **Session Chair** for the session titled *"Cryptanalysis, Attacks, Countermeasures, and Provable Security"* at 21^{st} International Conference on Cryptology and Network Security (CANS 2022), Abu Dhabi, UAE.

2019-2021: I served as the **Program Chair** for the Applied Research Competition as part of the yearly Cyber Security Awareness Week **(CSAW)** in the MENA region, held at New York University Abu Dhabi, UAE.

2019-2023: I was part of the **organizing team** for Cyber Security Awareness Week **(CSAW)** in the MENA region, held at New York University Abu Dhabi, UAE.

Computer skills

Languages: C, C++, Verilog, LaTex.

Tools: Xilinx Vivado, Sakura-G Board.

Teaching Assistantship

Aug 2018 - Nov 2018: Cryptology Course Workshop at NYUAD for Emirati school kids.