Akhilesh Siddhanti

www.akhilesh.tech | +1-470-775-1825 | akhilesh@gatech.edu | Linkedin: akhilesh-siddhanti | Github: akhileshsiddhanti

Education

Georgia Institute of Technology Atlanta, GA
Master of Science in Computer Science, ML Specialization Aug. 2019 – Dec. 2020

Birla Institute of Technology and Science Goa, India
B.E. (Hons) Computer Science and M.Sc. (Hons) Mathematics (dual degree) Aug. 2014 – May. 2019

Technical Proficiency

C, C++, Java, Python, HTML, CSS, Javascript, Tensorflow, Matlab, SQL, SAGE, LaTeX.

Experience

Undergraduate Thesis Intern at Indian Statistical Institute, Kolkata Jan 2014 – Oct 2016

- Analysing and developing a Physically Unclonable Function resilient to SAC property.
- Studied Cube and Integral attacks on stream ciphers.

Intern, HESL, Nanyang Technological University May 2018 – July 2018

- Modelled an Arbiter-based hardware PUF using minimal parameters.
- Studied Pseudo-boolean constraints and ways to use existing SAT solvers to solve them.

Intern, Indian Statistical Institute, Kolkata May 2017 – July 2017

- Attacked stream cipher Lizard using TMDTO attacks.
- Developed a new technique of Algebraic TMDTO Attacks, demonstrating an attack on ACORN v3.

Software Development Intern, ESSAR Group, India May 2016 – July 2016

- Automated the form-filling process for the HR department of ESSAR Power Gujarat Limited.
- Technologies used: ASP.NET framework, HTML, CSS, Javascript, SQL.

Publications

A TMDTO Attack Against Lizard **IEEE Transactions on Computers**
Cryptanalysis of stream cipher Lizard with a time complexity faster than brute-force search.

A Differential Fault Attack on Plantlet **IEEE Transactions on Computers**
Demonstrating a Differential Fault Attack on Plantlet with minimum fault requirements.

Certain Observations on ACORN v3 and Grain v1 **Journal of HASS**
An extended work of conditional TMDTO attack on ACORN v3 and Grain v1.

Differential Fault Attack on SIMON with Very Few Faults **INDOCRYPT 2018**
Showed how block ciphers can also be vulnerable to fault attacks, like stream ciphers.

Certain Observations on ACORN v3 **SPACE 2017**
Cryptanalysis of stream cipher ACORN v3 using SAT solving techniques.

Finding Fault Locations With Machine Learning: Case Study With CLX-128 (Under Review)
Used Deep Neural Networks to identify fault locations in a stream cipher.

Analysis of Strict Avalanche Criterion in variants of Arbiter based PUFs (Under Review)
Designed a novel S-PUF construction and reduced bias to zero for the first time.

Projects

ANN-aided fault location identification for stream ciphers

Implemented Artificial Neural Networks to find fault locations in a stream cipher (waiting for publication).

Surfboard - Surf the web, only using your keyboard!

Developed a web extension in Javascript to help differently-abled browse the web only using a keyboard.

Positions of Responsibility

Mentor, Quark Summer Time Project - Machine Learning Course **April 2016 - July 2016**

- Mentored 26 students for the course, ”Introduction to Machine Learning”, which involved tasking, checking assignments and solving doubts.
- Guided students on a final project titled ”Detecting Fake Currency Notes from UCI repository”.

Extra-curriculars

I am a Linux fan and a tech enthusiast, and keep myself updated with the latest tech gadgets in market.