Akhilesh Anilkumar Siddhanti
M.S. in Computer Science
College of Computing,
Georgia Institute of Technology, Atlanta - 30332
Email: akhilesh@gatech.edu
Mobile: (470) 775-1825
Links: LinkedIn, Google Scholar, DBLP

UNDERGRADUATE DETAILS

B.E. (Hons) Computer Science & M.Sc. (Hons) Mathematics **Aug 2014 – May 2019**
BITS Pilani KK Birla Goa Campus
Electives: Artificial Intelligence, Cryptography, Number Theory, Combinatorics, Algebra 2, Comm. Algebra, Cosmology

SUMMER INTERNSHIP/WORK EXPERIENCE

Undergraduate Research Thesis, Indian Statistical Institute, Kolkata **Aug 2018 – May 2019**
· Analysing and developing a Physically Unclonable Function resilient to SAC property.
· Mounting a fault attack on stream cipher Enocoro.
· Studied Cube and Integral attacks on stream ciphers.

Research Intern, HESL, Nanyang Technological University **May 2018 – July**
2018
· Designing an automated fault attack software (still in progress).
· Modelled an Arbiter-based hardware PUF using minimal parameters.
· Studied Pseudo-boolean constraints and ways to use existing SAT solvers to solve them.

Research 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.

PUBLICATIONS

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.

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 (Invited paper) **Journal of Hardware and Systems Security**
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.

Differential Fault Attack on Grain v1, ACORN v3 and Lizard **SPACE 2017**
Mounted fault attacks on popular stream ciphers using numerous optimizations.

Differential fault attack on hardware stream ciphers -- A technical survey (Invited talk) **RICAM Special Semester**
A survey of various fault attack techniques employed to cryptanalyze stream ciphers.

EXTRA CURRICULAR ACTIVITIES

- I am a tech-enthusiast, and keep myself updated with the latest technology and gadgets.
- I have won national level competitions in Vedic Mathematics and Abacus. I also hold an orange belt in Karate.
- My favorite sports are Badminton and Table Tennis. I am also fond of playing Chess.