

**Akhilesh Anilkumar Siddhanti**

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

**UNDERGRADUATE DETAILS**

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

**SUMMER INTERNSHIP/WORK EXPERIENCE**

<b>Undergraduate Research Thesis, Indian Statistical Institute, Kolkata</b> · 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.	<b>Aug 2018 – May 2019</b>
<b>Research Intern, HESL, Nanyang Technological University</b> · 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.	<b>May 2018 – July 2018</b>
<b>Research Intern, Indian Statistical Institute, Kolkata</b> · Attacked stream cipher Lizard using TMDTO attacks. · Developed a new technique of Algebraic TMDTO Attacks, demonstrating an attack on ACORN v3.	<b>May 2017 – July 2017</b>
<b>Software Development Intern, ESSAR Group, India</b> · Automated the form-filling process for the HR department of ESSAR Power Gujarat Limited.	<b>May 2016 – July 2016</b>

**PUBLICATIONS**

<b><u>Finding Fault Locations With Machine Learning: Case Study With CLX-128.</u></b> Used Deep Neural Networks to identify fault locations in a stream cipher.	<b>(Under Review)</b>
<b><u>A TMDTO Attack Against Lizard</u></b> Cryptanalysis of stream cipher Lizard with a time complexity faster than brute-force search.	<b>IEEE Transactions on Computers</b>
<b><u>A Differential Fault Attack on Plantlet</u></b> Demonstrating a Differential Fault Attack on Plantlet with minimum fault requirements.	<b>IEEE Transactions on Computers</b>
<b><u>Certain Observations on ACORN v3 and Grain v1 (Invited paper)</u></b> An extended work of conditional TMDTO attack on ACORN v3 and Grain v1.	<b>Journal of Hardware and Systems Security</b>
<b><u>Differential Fault Attack on SIMON with Very Few Faults</u></b> Showed how block ciphers can also be vulnerable to fault attacks, like stream ciphers.	<b>Indocrypt 2018</b>
<b><u>Differential Fault Attack on Grain v1, ACORN v3 and Lizard</u></b> Mounted fault attacks on popular stream ciphers using numerous optimizations.	<b>SPACE 2017</b>
<b><u>Differential fault attack on hardware stream ciphers -- A technical survey (Invited talk)</u></b> A survey of various fault attack techniques employed to cryptanalyze stream ciphers.	<b>RICAM Special Semester</b>

<b>EXTRA CURRICULAR ACTIVITIES</b>
<ul style="list-style-type: none"><li>• I am a tech-enthusiast, and keep myself updated with the latest technology and gadgets.</li><li>• I have won national level competitions in Vedic Mathematics and Abacus. I also hold an orange belt in Karate.</li><li>• My favorite sports are Badminton and Table Tennis. I am also fond of playing Chess.</li></ul>