I, Kaustav Brahma, a third year undergraduate student at IIT Kharagpur, in the department of Electronics and Electrical Communication Engineering was the recipient of the IIT Kharagpur Foundation (IITKGPF) International Internship Scholarship for my internship at MIT during the summers (May-July) of 2018.

I worked as a research intern at the Microsystems Technology Lab (MTL) in MIT under the guidance of Professor Anantha P. Chandrakasan. During my internship I worked on the side-channel profiling of a cryptographic engine which performs encryption using Elliptic Curve Cryptography (ECC).

The research included extensive literature survey for the first 2 weeks to come up with metrics we could use to quantify the amount of information being leaked by the cryptographic engine by side channel attacks. I also tried to figure out the side channel attacks which would work on the given engine and leak information from it.

After this I worked on setting up a system which could be used to extract and save the side-channel leaked signals from the chip, which had the cryptographic engine. The system was then automated to collect and save the traces for multiple trials of side-channel attack on the chip.

These saved side-channel traces were then used to conduct statistical tests to quantify the amount of information being leaked from the cryptographic engine. This part of the research included programming on Matlab.

I was able to come up with a metric which could be used to quantify the amount of information being leaked by the cryptographic engine. The results obtained by using this statistical metric were in accordance to the expected output.