ABSTRACT

Name of student: **Nikhil Mittal** Roll no: **17111056**

Degree for which submitted: **Master of Technology**

Department: **Computer Science & Engineering**

Thesis title: **Cryptanalysis of Round-Reduced Keccak**

Name of Thesis Supervisor: **Prof. Manindra Agrawal and Dr. Shashank Singh**

Month and year of thesis submission: **June, 2019**

In this thesis, we study the cryptanalysis of round reduced variants of Keccak hash function. The Keccak hash function is based on sponge construction which is different from previous Sha standards. Keccak faced a lot of cryptanalysis since it was declared as the winner of the Sha-3 contest. The techniques such as computing partial solutions, linearization etc. are used for the cryptanalysis of round-reduced Keccak. These techniques are very effective for mounting preimage attacks on 2 to 3 rounds of round-reduced Keccak.

The main contribution of the thesis is a cryptanalysis of 2 rounds of round reduced Keccak$[r := 800 - 384, c := 384]$. The best-known preimage attack for this variant of Keccak has the time complexity of $O(2^{64})$. We propose a preimage attack with an improved time and space complexity of $O(2^{44})$. We further analyze the linear structure technique provided by Guo *et al.* and suggested preimage attacks for 3 rounds of Keccak-256 and 4 rounds of Keccak-224.