# HARDWARE IMPLEMENTATION OF ADVANCED CRYPTOGRAPHIC HASH FUNCTION ON FPGAs

**ATULIIKA SHUKLA[1], SUMIT SHARMA[2] & RAVI MOHAN[3]**

[1]EC Department, Shri Ram Institute of Technology, Jabalpur, Madhya Pradesh, India

[2]HOD, EC Department, Shri Ram Institute of Technology, Jabalpur, Madhya Pradesh, India

[3]HOD, ME/M.Tech EC Department, Shri Ram Institute of Technology, Jabalpur, Madhya Pradesh, India

## ABSTRACT

A cryptographic hash function is a deterministic procedure whose input is an arbitrary block of data and output is a fixed-size bit string, which is known as the (Cryptographic) hash value. Cryptographic hash functions are the workhorses of cryptography, and can be found everywhere. Originally created to make digital signatures more efficient, they are now used to secure the very fundamentals of our information infrastructure, message authentication codes (MACs), [1] secure web connections, encryption key management.

Here is an algorithm which is implemented on FPGA. An essential part of this work is hardware performance evaluation of the hash function algorithms. In this work we present efficient hardware implementations and hardware performance evaluations of the algorithm. We implemented and investigated the performance of efficient hardware architectures on latest Xilinx FPGAs. we conclude the results in the form of chip area consumption, throughput and throughput per area on most recently released devices from Xilinx on which implementations have not been reported yet. We have achieved substantial improvements in implementation results from all of the previously reported work. This work serves as performance investigation of the given algorithm on most up-to-date FPGAs.

**KEYWORDS:** Hash Function, SHA-3, Skein, Threefish, FPGA