# Simulation and implementation of SHA-3 algorithm on FPGA

Yaghob Mirchi*,Dr. Siyavosh Amin nejad,

**Abstract Secure cryptographic hash functions are core components in many applications like challenge-response authentication systems or digital signature schemes. Many of these applications are used in cost-sensitive markets and thus low budget implementations of such components are very important. In 2012 the National Institute of Technology (NIST) ed the KECCAK algorithm as the hash function to be standardized as SHA-3, after a five year long competition cf. During and after the contest, various implementations of KECCAK for hardware platforms have been proposed and evaluated. However, very few results for non-standard implementations were published. Since SHA-3 has not become operational yet and it has been presented through only a few workshops, first the aim of this study is to investigate this algorithm and to discuss how it works. Then, it will be evaluated by using Matlab software. After software checking through Quarts application, it'll be hardware reviewed by Verilog language. And at last, the algorithm will be implemented on EP2C20F484C7N board and the results will be compared with their actual amounts which were presented by Keccak. key words:**

**Keywords : Keecak, the algorithm SHA-3, evaluate the software, hardware reviews, implementation**