



# **Implementation of Radix-2 Montgomery Multiplier in VHDL**

Jaya Bansal

[jayabansal3@gmail.com](mailto:jayabansal3@gmail.com)

Jagdish Nagar

[jagdishnagar1@gmail.com](mailto:jagdishnagar1@gmail.com)

*Abstract* –Low power consumption and smaller area requirement are prime concern in fabrication of DSP system on FPGA. Modular arithmetic is core operation in cryptosystems since they are efficient when data size is large (1024 bits or greater). In this paper a novel architecture of radix-2 Montgomery multiplier is presented and implemented on Vertex-iv FPGA device. Simulation shows that our design performs faster in terms of clock frequency while it requires lower area.

*Keywords*– Radix-2 Montgomery multiplier, VHDL, FPGA.