



# FPGA Implementation of Mutual Authentication Protocol Using Modular Arithmetic

T.Sadaiyappan<sup>1</sup>, K.K.Manoj<sup>2</sup>, S.A.Subhasakthe<sup>3</sup>

<sup>1</sup>PG Scholar, VLSI Design & Bannari Amman Institute Of Technology, India

<sup>2</sup>PG Scholar, VLSI Design & Bannari Amman Institute Of Technology, India

<sup>3</sup>PG Scholar, VLSI Design & Bannari Amman Institute Of Technology, India

<sup>1</sup> sadaiyappanece@gmail.com; <sup>2</sup> kkm.apt@gmail.com; <sup>3</sup> sakteanand@gmail.com

---

**Abstract**— *Radio-Frequency Identification (RFID) is a modern technology that utilize radio frequencies to locate the object. In this paper, we study the radio-frequency identification (RFID) tag-reader mutual authentication (TRMA) scheme. Two improved authentication protocols for generating the Pad Gen function are described. In this project, a protocol for RFID tag-reader mutual authentication scheme is proposed which is hardware efficient. Modified MOD scheme is implemented in protocol system to reduce the hardware cost. The proposed mutual authentication protocol with consumes less logic elements and also more secure from external attacks. The proposed protocol is described in Verilog HDL and simulated using Xilinx ISE design suite 14.2.*

**Keywords**— *Radio frequency identification; mutual identification*

---

Full Text: <http://www.ijcsmc.com/docs/papers/January2014/V3I1201421.pdf>