Notification number: COE/Ph.D./(Notification)/525/2022

Date of Award: 08/12/2022

Name of the Scholar: Deena Nath Gupta

Name of the Supervisor: Prof. Rajendra Kumar

Name of the Department/Centre: Department of Computer Science

Topic of Research: Designing of Lightweight Security Scheme for IoT

Finding

I proposed a lightweight security scheme to secure the communications under an IoT environment. My security scheme includes four main modules, DeeR-Gen, DeeR-Hash, DeeR-MA, and DeeR-Crypt. DeeR-Gen is a random number generation module that is used to generate secret keys. The proposed methodology is best in class as it takes only 245 GE on ASIC to execute, lowest among other random number generators. DeeR-Hash is a sponge based hash construction used to get an 80-bit digest. The proposed algorithm is a combination of three modules, DeeRSponge, DeeRStateUpdate, and DeeR-Hash. DeeR-Hash takes 984 GE on ASIC, again lowest among its class. DeeR-MA is a lightweight mutual authentication protocol that provides reader verification, tag verification, and mutual authentication. The Reader needs only 1004 GE on ASIC for mutual authentication, suitable for a lightweight environment. The fourth and final module is DeeR-Crypt. It is used for a simple encryption/decryption procedure and takes only 594 GE on ASIC for its execution. In sum, we can say that the proposed security scheme needs only 2801 GE on ASIC for its complete operation. The required GE is lowest amongst other lightweight proposals and hence I termed it as the best security scheme for IoT devices.