Abstract

Wireless body area network (WBAN) devices are resource-constraint devices, in particular for energy. Therefore, it is essential to select the cipher implementation with minimum energy consumption. Determining optimum cipher implementation is an arduous task due to lack of uniform platform for comparison and deviations in measuring and reporting the performance metrics. Hence, it is important to model the performance of the cipher design. This article presents a novel energy model for light-weight block cipher hardware implementation based on the design parameters. The model usage is then demonstrated by studying the energy trend versus the number of rounds. It shows that there exists an optimum number of rounds per cycle to minimize energy.