A VLSI Architecture for the PRESENT Block Cipher with FPGA and ASIC Implementations

Jai Gopal Pandey[1], Tarun Goel[2], Mausam Nayak[1,3], Chhavi Mitharwal[1,3], Sajid Khan[4], Santosh K. Vishvakarma[4], Abhijit Karmakar[1], and Raj Singh[1]

[1] CSIR- Central Electronics Engineering Research Institute, Pilani, India- 333031
{jai,abhijit,raj}@ceeri.res.in
[2] Central Research Laboratory, Bharat Electronics Ltd., Bangalore, India-560013
{tarungoel.com}@gmail.com
[3] Banasthali Vidyapith, Vanasthali, Rajasthan, India-304022
{nayak.mausam,chhavimitharwal}@gmail.com
[4] Indian Institute of Technology Indore, Simrol, Indore, India-453552
{phd1601102015,skvishvakarma}@iiti.ac.in

Abstract. The infrastructure of internet-of-things (IoT) and cyber-physical systems (CPS) is based on the security of communicated data. Here, lightweight cryptography plays a vital role in IoT/CPS resource-constrained environments. In this paper, we propose an architecture for the PRESENT lightweight block cipher and its VLSI implementation in an FPGA and ASIC. The input-output ports of the architecture are registered and data-path is based on 8-bit. It requires 49 clock cycles for processing of 64-bit *plaintext* with 80-bit user key. The FPGA implementation of the proposed architecture is done in Xilinx Virtex-5 device in comparison to an existing design improved performance has been obtained. Further, an ASIC implementation of the architecture is done in SCL 180 nm technology where gate equivalent (GE) of the design is 1608 GEs and area of chip is 1.55 mm^2. At 100 MHz operating frequency, total power consumption of the chip is 0.228 mW. A throughput of 130.612 Mbps, energy 112.15 nJ, energy/bit 14.018 nJ /bit, and 0.813 efficiency is obtained.

Keywords: PRESENT block cipher· Lightweight cryptography· VLSI architecture· FPGA · ASIC.

1 Introduction

The foundation of internet-of-things (IoT) [1], cyber-physical systems (CPS) [2], [3] and edge computing [2] technologies heavily rely on communicated data. As shown in Fig. 1, data can be between human-to-machines and their any combination [4]. In this fast-growing computing infrastructure, small computing devices are deployed for sensing, control, communication and computation needs. Subsequently, deployment trend of devices for IoT/CPS applications, bring a drastic change in designing of electronic circuits and associated systems. Here, the design metrics are being optimized for resource, latency, power and bandwidth [1].