A High-performance VLSI Architecture of the PRESENT Cipher and Its Implementations for SoCs

Abstract—**The essence of internet-of-things (IoT) and cyber-physical systems (CPS) infrastructures is primarily based on privacy and security of communicated data. In these resource-constrained applications, lightweight cryptography plays a vital role for data security. In this paper, we propose a high-performance and power-efficient VLSI architecture for the PRESENT block cipher and its integration in a system-on-chip (SoC) environment. The architecture is based on 8-bit datapath and requires 48 clock cycles for processing of 64-bit plaintext and 128-bit key. The architecture is validated using Xilinx Virtex-5 xc5vfx50 FPGA device, where it consumes 84 slices, provides 379.78 MHz maximum frequency and 506.37 of Mbps throughput. It consumes 36.57 mW of dynamic power, 57.95 nJ energy and provides 0.91 nJ/bit energy/bit. In comparison to an exiting architecture, the proposed architecture provides much improved performance. Further, an ASIC implementation of the architecture is done in SCL 180 nm technology for its usage as an intellectual-property (IP) core in SoCs. The core consumes 1785, 2-input NAND gate equivalent (GE), with 1.55 mm^2 area and can be operated up to 448 MHz clock frequency. At 100 MHz clock frequency, 0.273 mW of total power dissipation, 133 Mbps throughput, 130 nJ energy and 16.36 nJ/bit energy/bit is obtained.**

Index Terms—**Lightweight cryptography; PRESENT block cipher; VLSI architectures; ASIC; SoCs.**

1. Introduction

Recent proliferation of internet-of-things (IoT) [1], cyber-physical systems (CPS) [2] and edge computing [3] technologies enable devices to interconnect through Internet. With these enablers, a new class of applications is emerging by an amalgamation of machine learning and artificial intelligence (AI) techniques. These applications heavily rely on communicated data that can be between human-machines or their any combinations. A pervasive computing infrastructure is shown in Figure 1, where, small computing devices of credit-card sized are deployed for fulfilling the need of sensing, control, communication and computation. The ever-increasing deployment trend bring a substantial change in the design of electronic circuits and systems [1]. Accordingly, application and system developers are focused toward design of applications, related intellectual-properties (IPs) and system-on-chips (SoCs) that are optimized for resource, latency, power and bandwidth design metrics.

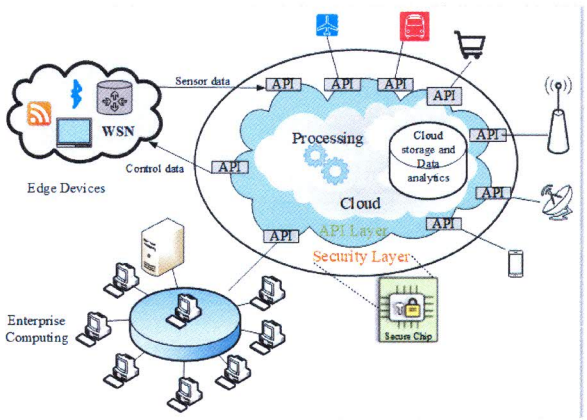

Figure 1. An infrastructure of cutting-edge IoT, CPS and edge computing technologies.

In a gamut of emerging IoTs applications, secure communication mechanism for restricting access of information is very crucial [2], [4] and [5]. Here, for securing electronic data, cryptography is very important. In encryption operation of cryptography, data is converted into a secure form which is known as ciphertext. Symmetric key cryptography algorithms and their hardware solutions that provide very low area and energy requirements for IoT applications are ideally suited [4], [6]. Efficient implementations for the criptographic algorithms are much dependent on selection of appropriate architectures as per the need of performance and energy metrics. In the lightweight cryptography context, ISO/IEC 29192-2 has standardized symmetric block cipher algorithm PRESENT in year 2012 [7]. The algorithm provides adequate level of security goals and hardware-oriented performance attributes. This makes it a preferred choice in lightweight cryptographic based applications [8].

In this paper we propose a high-performance and power-efficient custom architecture for the PRESENT block cipher and its VLSI implementations. The architecture works on the 64-bit input and of 128-bit user key. It processes 8-bit data at a time and provides ciphertext in 48 clock cycles, with registered inputs and outputs. An FPGA implementation of the proposed architecture is done in Xilinx Virtex-5 xc5vfx50 FPGA device and compared with the architecture of [9]. Here, the proposed architecture works on 50.8% increased maximum frequency, 28.8% improved throughput