A High-performance and Area-efficient VLSI Architecture for the PRESENT Lightweight Cipher

Jai Gopal Pandey, Tarun Goel*, Abhijit Karmakar
CSIR - Central Electronics Engineering Research Institute (CEERI)
* Academy of Scientific & Innovative Research (AcSIR), CSIR-CEERI Campus
Pilani-333031, India
jai@ceeri.res.in

Abstract— **Security and privacy are the prime concern in the emerging internet of things (IoT) and cyber physical systems (CPS) based applications. Lightweight cryptography plays an essential role for securing the data in this emerging pervasive computing environments. In this paper, we propose a high-performance and area-efficient VLSI architecture with 64-bit datapath for the PRESENT block cipher. The proposed architecture performs an integrated encryption/decryption operation for both 80-bit and 128-bit key lengths. The architecture is synthesized for the Virtex-5 XC5VLX110T FPGA device, available on the Xilinx ML-505 platform. It has been observed that the proposed architecture utilizes 0.73% and 0.87% of FPGA slices for 80-bit and 128-bit key lengths respectively. A throughput of 410 Mbps and power consumption is about 16 mW for both the key lengths.**

Keywords— Lightweight cryptography; PRESENT block cipher; Integrated encryption/decryption; VLSI architecture; FPGAs.

I. INTRODUCTION

The rapidly-growing area of internet of things (IoT) and cyber physical systems (CPS) is based on an ecosystem which eventually relies on billions of tiny interconnected computing-devices [1], [2]. The ability of selective computing, sensing, control and communication, makes these ever-ready devices effective, efficient and intelligent. Some of the day-to-day applications around these devices include car-locks, e-cash cards, electronic gadgets, digital lockers, secure communication, and many more. These tiny devices and their network create a wide-spread pervasive-computing infrastructure in emerging applications. Ever-increasing applications of these devices create an extensive demand of smart computing system and their energy-efficient field deployment. Besides design goals, security and privacy are the prime aspects of this IoT-based CPS infrastructure. Here, the field of cryptography and related ciphers provide a mechanism by which data can be efficiently secured. To secure the transmitted data through any electronic system, a variety of ciphers are used for years. The deployment trend of ciphers in electronic systems is shown in Fig. 1.

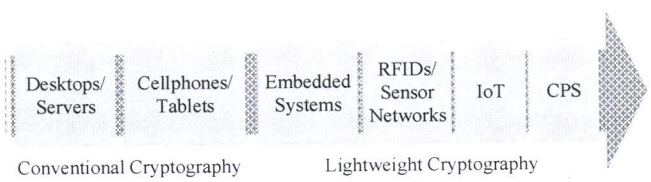

Fig. 1. Deployment trend of ciphers in electronic systems.

This research work has been carried out under the *SMDP-C2SD* project, sponsored by *MeitY, Govt. of India.*

As shown in the Fig. 1, majority of the conventional cryptographic algorithms has been developed around desktop/server centric environments. Therefore, many of these cryptographic algorithms are generally unsuitable for implementation in constrained devices which are used in the modern-age applications. In many conventional cryptographic standards, the trade-offs between security, performance and resource requirements were optimized for desktop and server environments. This makes the implementation of conventional ciphers difficult in resource-constrained applications, and their performance may not be acceptable. The shift from desktop based applications to small-devices centric applications bring a wide range of security and privacy concerns. Lightweight cryptography provides solution tailored for resource-constrained devices and their efficient VLSI implementations [3].

Recently national institute of standards and technology (NIST) provided a report containing an overview of lightweight cryptography and an outline of NIST's plan for standardizing the lightweight cryptographic algorithms [4]. Further, a detailed taxonomy of the lightweight block ciphers can be found in [3] and [5]. Systematic survey of lightweight-cryptography ciphers and their software and hardware implementations with detailed description and related discussions can be found in [3], [5] and [6]. Here, it has been emphasized that efficient implementation of the ciphers are closely dependent on the selection of appropriate architecture, as they result in low implementation complexity and high-performance in actual realizations. To propose a new architecture for the lightweight cryptography, there is always trade-offs between the three prime objectives i.e. security, cost and performance, which is shown in Fig. 2 [7].

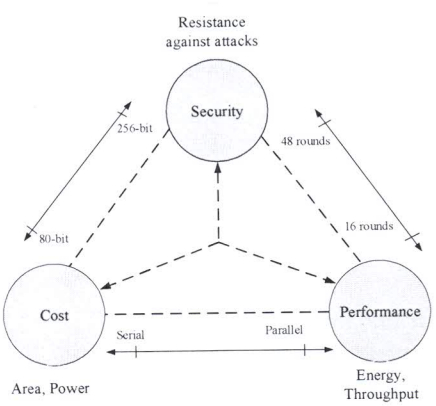

Fig. 2. Architectural trade-offs between security, cost and performance. Adapted from [7].