A Unified Architecture for AES/PRESENT Ciphers and its Usage in an SoC Environment

Jai Gopal Pandey, *Senior Member*, *IEEE*, Sanskriti Gupta, Abhijit Karmakar
CSIR-Central Electronics Engineering Research Institute (CEERI), Pilani, India-333031
{jai, abhijit}@ceeri.res.in, mailtosanskriti@gmail.com

***Abstract*—Electronic data security is of vital concern for secure communication applications of cyber-physical system (CPS) that relies on Internet-of-things (IoT) based technologies. To achieve multi-level data security, a combination of long-term secure cipher, advanced encryption standard (AES), and short-term secure cipher, PRESENT are deployed together for forming a common cipher chip. The core is used for secure audio application in an open source system-on-chip (FPGA-SoC) environment. An integrated implementation of the cores is done on FPGA-SoC and ASIC. FPGA implementation of the architecture on Xilinx xc5vlx110t-1-ff1136 FPGA device consumes 14% slices. Further, the design is implemented in SCL 180 nm CMOS ASIC technology, it takes 2×2 mm^2 die size containing 0.867 mm^2 standard cell area. At 100 MHz clock frequency, total power consumption of the chip is 11.9 mW.**

***Index Terms*—Cryptography, AES, PRESENT, VLSI architecture, ASIC, FPGA-SoC.**

I. Introduction

Electronic data security is must in ever-increasing deployment of cyber-physical system (CPS) and Internet of things (IoT) technologies. Some of the popular applications include, communication, electronic money transfer, automated teller machines (ATMs), computer networks, smart cards, e-commerce and many more [1], [2]. Long-term secure ciphers are useful for providing security of encrypted data that can not be easily broken by any cryptanalyst or by applying brute force attacks for longer duration of time (couple of months to years). Some of the applications of these type include classified documents, military deals, etc. Similarly, the short-term ciphers are suitable to protect data for couple of weeks, like digital locker, smart card, RFID tags, and so on. To achieve multi-level data security, a combination of long and short-term ciphers are useful in varying applications. A comparison of AES and PRESENT block ciphers in the context of their software implementation over low-cost smartphones has been provided in [3]. In another design [4] AES and PRESENT crypto engines have been integrated as co-processors for analyzing their energy/power suitability on an FPGA-based system-on-chip (FPGA-SoC) platform. In another implementation, a CMOS ASIC realization of AES core on 180 nm technology has been reported in [5].

In this paper an integrated architecture for realizing AES and PRESENT block ciphers is proposed and its FPGA-SoC implementation for a secure audio application is discussed. The architecture is able to perform encryption/decryption operations for both the ciphers. It is implemented on Xilinx xc5vlx110t-1-ff1136 FPGA device and consumes 14% slices. Additionally, the architecture is realized in SCL 180 nm CMOS technology, that fits in 2×2 mm^2 die size, containing 0.867 mm^2 standard cell area and consumes 11.9 mW of power. To ensure reliability, the design is passed through multiple iterations of global routing congestion (GRC), IR drop, IRMS and clock.

Rest of the paper is arranged as follows: An application of the core in open-source SoC design environment is provided in Section II. Section III provides a brief introduction of the AES and PRESENT block ciphers. The unified AES/PRESENT architecture is proposed in Section IV. Experimental results for FPGA and ASIC implementations are given in Section V. Finally, Section VI concludes the paper.

978-1-7281-3427-7/20/31.00/31.00

II. An Application of the Crypto Core in an Open Source SoC Environment

An open source SoC design suite by *Cobham Gaisler* is chosen to integrate the designed architecture as a custom IP core as in [6], [7]. The complete design suite and integration scheme is shown in Fig. 1. In this figure, the outer box represents the SoC design suite. Here, a variety of commonly used IP cores have been provided in a form of a package that is called *GRLIB*. The suite is also supported by a range of EDA tools and common utilities to debug, analyze, test and validate custom designs [7]. The IP cores are mostly vendor-independent and supported by commonly available tools for both ASIC and FPGAs environment. The advanced microcontroller bus architecture (AMBA) on-chip bus interface supports the core for the required communication. The custom cores can be interfaced through the AMBA advanced peripheral bus (APB) or advanced high-performance bus (AHB) by using appropriate bus interfaces. An interface of the unified AES/PRESENT custom-core in the LEON3 processor-based SoC design suite is shown in Fig. 1. The complete design is targeted for Xilinx ML-505 FPGA platform.

PRESENT crypto core is interfaced with *LEON3* processor through AMBA APB bus. The interfaced core is highlighted at bottom side in Fig. 1. Here, *LEON3* processor works as a master (mst) whereas cores behave as slaves (slv). Data is requested by LEON3 processor, enabling the APB bus with requisite read/write signals. Input of the AMBA APB/AHB bridge comes from the AHB bus that is called *ahbi* [6], [7]. As shown in Fig. 1, to encrypt/decrypt audio data the core

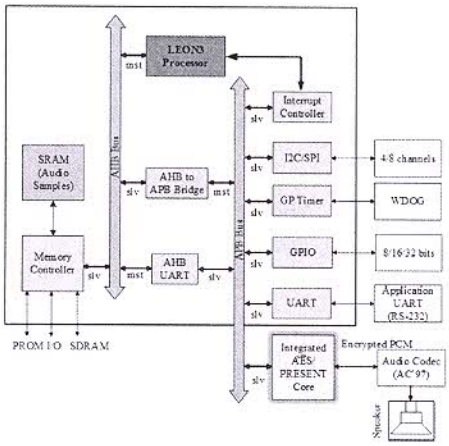


Fig. 1: An application of the unified core in a system-on-chip (SoC) environment.

is utilized by the LEON-3 processor. The audio samples are processed at 16 KHz sample rate and are kept in the SRAM. These audio samples are provided to the connected integrated crypto core. To process the audio data to the speaker the AC'97 audio codec has been used [8] that is available on the Xilinx ML-505 FPGA platform [9]. The processed audio output is available at the connected speaker, through AC'97 *Codec*.

III. AES and PRESENT Block Ciphers

AES cipher is used in myriad range of real-time security applications. The algorithm has been standardized by federal information processing standard publications (FIPS PUBS) [2]. It is a symmetric, round-based block cipher that works with a block size of 128 bits and key lengths of 128/192/256 bits. Depending upon the key length, the algorithm is referred as: AES-128, AES-192, and AES-256 [2].

Structure of PRESENT cipher is based on SP-network [10]. It requires 31 internal rounds with 64-bit data and 80/128-bit keys. These rounds perform XOR operation that is required to introduce a round key K_i for $0 \leq i \leq 31$. The last key (K_{31}) generated is used for the post-whitening operation. Additionally, the cipher also requires a non-linear substitution layer and a linear bit-wise permutation layer. The substitution operation needs a single 4-bit S-box that is used 16-times concurrently in each consecutive round. The pseudo-code and a top-level algorithm description is given in [10] and its hardware implementation is provided in [11].

IV. Proposed Architecture: Datapath, Controller and the Chip Overview

The architecture performs encryption/decryption operations for both AES/PRESENT ciphers. To implement them in the FPGA and ASIC environments, input/output(I/O) of the cores are shared to reduce the I/O count. 8-bit I/O ports are utilized for providing 128/64 bit input data, 128/80 bit user key and 128/64 bit output for AES/PRESENT ciphers respectively. In both the architectures, S-boxes are realized by area-optimized combinational logic. A macro-level design and its associated controller is depicted in Fig. 2 and Fig. 3 respectively.

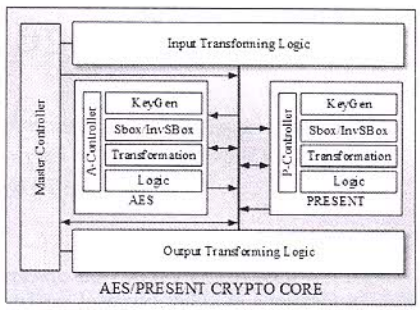


Fig. 2: A block diagram of the integrated crypto chip.

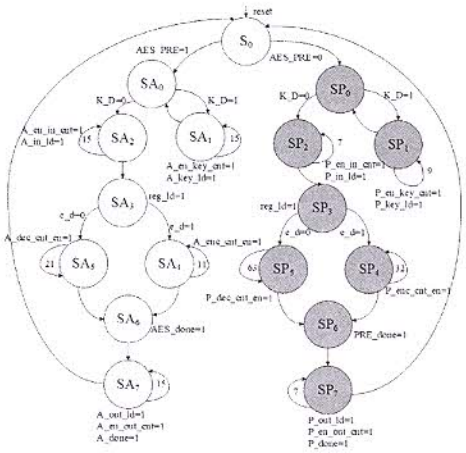


Fig. 3: A master controller of the proposed architecture.

The chip takes 8-bit data/key as input from input transforming logic and processed as per the selected cipher. Task of output transforming logic is to provide 8-bit ciphertext/plaintext and *done* signal. Depending upon *AES_PRE* select signal, '1'or '0', either AES or PRESENT cipher block gets activated. The ciphers have their own local controller which is shown as in Fig. 3 as *A-Controller* on left side and *P-Controller* on right side for AES and PRESENT ciphers respectively.

The AES core works with 128-bit data and key. Here the inputs are provided by a single 8-bit port (Input_A). In State SA_0, if the signal *K_D*='1', key is generated in State SA_1. Here, 128-bit key is obtained in 16 clock cycles. Until the user keeps the signal *K_D*='1', the key continues to update; otherwise, the State switches back to SA_0. Now, the State becomes SA_2 and here input data is captured in 16 clock cycles. After this, the State becomes SA_3, where the controller switches either for encryption or decryption operation. If signal *e_d*='1', then encryption is performed in State SA_4 and it takes 12 clock cycles. If the signal *e_d*='0', decryption operation is performed in the State SA_5 that consumes 22 clock cycles. After performing encryption/decryption operation the State becomes SA_6 where the signal *AES_done*='1'indicates

completion of the cipher operation. Now, to bring the 128-bit processed data to the 8-bit output port (Output) 16 clock cycles are required and for this State SA_7 is designated. By this the encryption/decryption latency for the AES cipher is 68/78 clock cycles. In the similar manner, the PRESENT cipher also works with 64-bit data and 80-bit key length through 8-bit input port and provides output through 8-bit port. Here, latency for encryption/decryption becomes 67/98 clock cycles. In both the ciphers, the sboxes are implemented in area-optimized combinational logic that compute at run-time.

Here the cipher blocks share common *reset* clock (*clk*), *enable*, *data_enable*, *key_data*, *ENC_DEC*, output ready (*Out_Ready*) and output enable (*OE*) as input signals. When the *ENC_DEC* signal is '1'or '0', we can select either encryption or decryption operation. With the active high input of the *enable* signal, the core gets activated and when the *data_enable* is high it receives the input. The signal *key_data* helps for multiplexing the user key/input data. When this signal is high, data is treated as user key otherwise as input data. This signal is initially high for 16/10 clock cycles for AES/PRESENT block ciphers. After that, in next 16/8 consecutive clock cycles it accepts plaintext/ciphertext for AES/PRESENT cipher. Output of the core is tri-stated that is controlled by the active low output enable (*OE*) signal. The core provides output when signal (*Out_Ready*) is at active high state. The controller raises *done* signal to active high and enables the output transforming logic to provide output for the next 16/8 consecutive clock cycles for AES/PRESENT cipher.

V. Experimental Results of FPGA and ASIC Implementations

Here results are obtained with input data/key as X"00". With 8-bit I/O ports, the encryption/decryption operations of AES cipher take 68/78 clock cycles and 67/98 clock cycles for PRESENT. The proposed architecture is implemented in an FPGA device of Xilinx. After successful validation of the architecture on a FPGA board, the design is targeted for an ASIC implementation. Details of the FPGA and ASIC implementations are arranged in following two subsections.

A. Results of an FPGA Implementation

The RTL design of the architecture is synthesized on Xilinx Virtex-5 xc5vlx110T-1-ff1136 FPGA device of Xilinx ML-505 platform [9]. The FPGA device utilization is given in Table I. Here, the architecture utilizes 8% LUTs and 7% registers; results in an overall 14% consumption of the FPGA slices. The IOBs utilization is 4%. The complete architecture runs at a maximum clock frequency of 164.25 MHz. The implemented design consumes a total of 1369.10 mW power on FPGA. Where, the dynamic/static components are 322.01/1047.09 mW respectively. The power is computed at the maximum operating frequency with thousands of random vectors.

A performance computation of the designed chip is provided in Table II. Here, latency, throughput, efficiency and energy for encryption (Enc) and decryption (Dec) operations for both the AES and PRESENT ciphers are provided.

TABLE I: Resource Consumption of the Proposed Architecture on Xilinx Virtex-5 xc5vlx110t-1ff1136 FPGA Device.

Elements	Available Resources	Used Resources	Resource Utilization (%)
Slice LUTs	69,120	5959	8
Slice Registers	69,120	5449	7
Total Slices	17,280	2528	14
Bonded IOBs	640	26	4
Number of BUFG/BUFGCTRLs	32	2	6

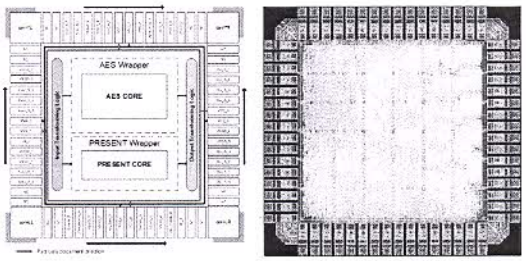
The latency of the designed architecture is 68/78 for the AES and 67/98 for teh PRESENT encryption and decryption operations. It results in throughput of 309.17/269.53 Mbps for AES and 156.89/107.26 Mbps for PRESENT cipher respectively. Here, throughput is computed as $throughput = (maximum\ frequency \times total\ no.\ of\ bits)/latency$. Similarly, efficiency of the design is calculated by expression: $efficiency = throughput/(total$ no. of slices). Energy consumption for encryption/decryption in AES cipher is 0.566/0.650 μJ and for PRESENT cipher is 0.558/0.816 μJ.

TABLE II: Performance of the Proposed Architecture on Xilinx Virtex-5 xc5vlx110t-1ff1136 FPGA Device.

Elements	AES		PRESENT	
	Enc	Dec	Enc	Dec
Latency	68	78	67	98
Throughput (Mbps)	309.17	269.53	156.89	107.26
Efficiency (Mbps/#Slices)	0.122	0.106	0.062	0.042
Energy (uJ)	0.566	0.650	0.558	0.816

B. Results of an ASIC Implementation in SCL 180 nm CMOS Technology

The integrated crypto cipher is implemented in SCL 180 nm technology which is a 4 metal layer process [12]. A top-level and layout view of the chip is shown in Fig. 4.



(a) (b)

Fig. 4: Proposed crypto chip (a) a top-level view. (b) layout view in SCL 180 nm CMOS technology.

Here, the overall die/core size are kept an integer multiple of the tile width (0.56 micron) and tile height (5.6 micron) in order to ensure abutment of the I/O pads [12]. The designed chip supports a 192 MHz maximum operating frequency on 180 nm technology node. However, 100 MHz clock frequency

is selected for analyzing the implemented results. A detailed break-up for the utilization of standard cells is given in Table III. Here the cell utilization of individual AES and PRESENT cores along with the interface logic resources is provided. This unified architecture requires 69092 NAND gate equivalent (GE). Here the gate count of AES and PRESENT is 41175, and 25143 respectively; whereas, the interface logic requires a total of 2774 GEs. A detail usage of all the parameters is shown in Table IV. The core utilization of the proposed design is 46.8 %, which is being calculated as: $core\ utilization = (standard\ cell\ area + macro\ cell\ area)/(total\ core\ area)$.

TABLE III: Standard Cell Count at 180 nm Technology.

Elements		No. of Cells	Cell Area (mm^2)
AES	AES Wrapper	1517	0.0629
	AES CORE	21707	0.4536
PRESENT	PRESENT Wrapper	862	0.0357
	PRESENT CORE	8960	0.2797
Interface Logic		89	0.0348
Total			0.8667

TABLE IV: An ASIC Implementation Result.

Elements	Area (mm^2)
Die Size	4.000
Standard cells	0.867
IO Pad Size	0.016
Corner Pad Size	0.063
Core Size	1.851

Here, current density is observed for different metal layers. It is for M1 (17.23 A/cm), M2 (3.19 A/cm), M3 (13.86 A/cm) and Top_M (26.58 A/cm) is substantially less than that of SCL 180 nm specified technology[12]. Computed maximum threshold limit of IR drop of the design for net VSS is found to be 61.6 mV and that for VDD net is obtained as 26.56 mV, which is within permissible limit of the foundry that is 0.1 V. Total power consumption of the design is 11.9 mW.

TABLE V: A Comparison of the Designed ASIC with Existing Implementations at 180 nm Technology.

Work	AES		PRESENT	
	Max. Freq. (MHz)	kGEs	Max. Freq. (MHz)	kGEs
[13]	152.00	6.20	-	-
[5]	50.50	4.20	-	-
[14]	300.00	124.00	-	-
[15]	-	-	200.00	27.03
Our Work	200.00	53.00	250.00	31.60

Table V provides result in 180 nm CMOS technology and it is compared with some of the existing work. Here, the design of [13], [5], [14] and [15] are selected for the comparison with the individual ciphers of the proposed design. The table contains some blank cells (-) because the referred work has implemented either of the two blocks i.e., AES or PRESENT cores. As evident from the above table that the proposed implementation can be operated at a much better speed in comparison with referred designs.

VI. Conclusion

The paper presented a unified VLSI architecture for achieving data security in IoT/CPS technologies. The architecture integrates AES and PRESENT block ciphers. The implemented design can be used to provide a multi-level data security, where long-term security can be established by AES cipher and short-term security by PRESENT. FPGA implementation on Xilinx xc5vlx110t-1-ff1136 FPGA device needs 8% LUTs and 7% registers that results in a total 14% consumption of the FPGA slices. The architecture can run at 164.25 MHz maximum clock frequency. Further, the architecture has been implemented in SCL 180 nm CMOS process technology on 2×2 mm^2 die size that consumes 11.9 mW power at 100 MHz clock rate. The core has been utilized as an IP for secure audio application in an FPGA-SoC environment.

Acknowledgement

This work has been done under the SMDP-C2SD project, sponsored by Ministry of Electronics and Information Technology (MeitY), Govt. of India. We would like to extend our sincere gratitude to MeitY, India and to the Director, CSIR-CEERI, Pilani, India for providing the necessary resources to carry out this research work.

References

[1] Serge Vaudenay. *A Classical Introduction to Cryptography: Applications for Communications Security*. Springer Science & Business Media, 2006.

[2] NIST FIPS Pub. 197: Advanced Encryption Standard (AES). *Federal information processing standards publication*, 197(441):0311, 2001.

[3] C. Andrés, M.S. Miguel, D.P. Arturo, et al. An evaluation of AES and PRESENT ciphers for lightweight cryptography on smartphones. In *2016 International Conference on Electronics, Communications and Computers (CONIELECOMP)*, pages 87–93. IEEE, 2016.

[4] Xu Guo, Zhimin Chen, and Patrick Schaumont. Energy and performance evaluation of an FPGA-based SoC platform with AES and PRESENT coprocessors. In *International Workshop on Embedded Computer Systems*, pages 106–115. Springer, 2008.

[5] Van-Lan Dao, Van-Phuc Hoang, Anh-Thai Nguyen, and Quy-Minh Le. A compact, low power AES core on 180nm CMOS process. In *2016 International Conference on IC Design and Technology (ICICDT)*, pages 1–5. IEEE, 2016.

[6] J. G. Pandey, T. Goel, M. Nayak, C. Mitharwal, A. Karmakar, and R. Singh. A high-performance VLSI architecture of the PRESENT cipher and its implementations for SoCs. In *2018 31st IEEE International System-on-Chip Conference (SOCC)*, pages 96–101. IEEE, 2018.

[7] J. Gaisler, S. Habinc, and E. Catovic. GRLIB IP Library User's Manual. *Aeroflex Gaisler*, 2010.

[8] Analog Devices. Ac'97 soundmax codec, 2016.

[9] Xilinx. Ml505/ml506/ml507 evaluation platform, 2018.

[10] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, and et al. PRESENT: An ultra-lightweight block cipher. In *CHES*, volume 4727, pages 450–466. Springer, 2007.

[11] Jai Gopal Pandey, Tarun Goel, and Abhijit Karmakar. Hardware architectures for PRESENT block cipher and their FPGA implementations. *IET Circuits, Devices & Systems*, 2019.

[12] Semi-Conductor Laboratory (SCL). PDK of 180 nm technology, 2018.

[13] Panu Hamalainen, Timo Alho, Marko Hannikainen, and Timo D Hamalainen. Design and implementation of low-area and low-power aes encryption hardware core. In *9th EUROMICRO conference on digital system design (DSD'06)*, pages 577–583. IEEE, 2006.

[14] Cast aes32 c. Cast: Digital ip cores and subsystems, Oct. 2014.

[15] Carsten Rolfes, Axel Poschmann, Gregor Leander, and Christof Paar. Ultra-lightweight implementations for smart devices–security for 1000 gate equivalents. In *International Conference on Smart Card Research and Advanced Applications*, pages 89–103. Springer, 2008.