AN AHB-PCI BRIDGE INTELLECTUAL PROPERTY CORE WITH AES-128 ENCRYPTOR/DECRYPTOR

Nguyen Hung Quan, Do Ngoc Quynh, Tran Kien Cuong,PhamThanh Hung, and Bui Quang Tung
IC Design Research & Education Center
6th quarter, LinhTrung ward., Thu Duc district, HCM city, Vietnam
E-mail: {quan.nguyenhung, quynh.dongoc, cuong.trankien,
hung.phamthanh, tung.buiquang}@icdrec.edu.vn

Abstract—**An AHB-PCI bridge, which is able to connect both Peripheral Component Interconnection(PCI) local bus version 2.3 and Advanced High-performance Bus(AHB), is integrated the AES-128 encryptor and decryptor to apply the security data exchange card.The encryptor enables to encipher data from PCI bus and the decryptor enables to decipher data from AHB bus. This design was implemented on Field Programmable Gate Array (FPGA) cardML555of Xilinx. Inc.**

Index Terms—**PCI2.3 specification,AMBA specification, Advanced Encryption Standard, FIPS-197.**

I. INTRODUCTION

PCIlocal bus is a high performance bus with multiplexed address and data lines. It is usedto connectthe highlyintegrated peripheral controller components, peripheral add-in cards, and processor/memory systems[1] [2].

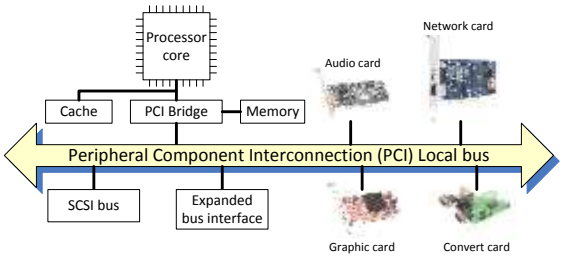

Fig 1. PCI bus system

The AHB bus is used to connect the processor cores and peripherals which require the high performance and high system clock frequency[3].

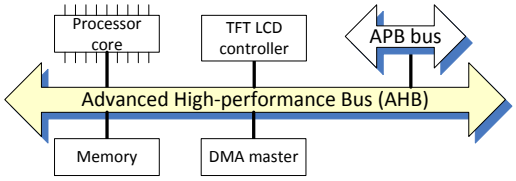

Fig 2.AHB bus system

The Advance Encryption Standard (AES) is a symmetric block cipher algorithm that is approved by Federal Information Processing Standards Publications (FISP)can be used to protect electronic data[4].

The PCI-AHB bridge intellectual property (IP) core not only connects to PCI 2.3 bus but also connects to AHB bus to exchange data between them. Besides, it is added encryption and decryption capabilityto support the security applications.

In order to test this IP core, a demo system is implemented on Virtex-5 FPGAboardML555of Xilinx. Inc. after is simulated and verified by VCS tool of Synopsys.

The features, main functions and structures of IP core will be described in §2 and §3.

II. PCI-AHB BRIDGE IP CORE ARCHITECTURE

A. *The Features*

The PCI-AHBBridge has the basic following basic features:

- PCI specification 2.3 compliant
  - Zero wait state burst mode
  - 33/66 MHz performance
  - 32/64-bit data path
  - Dual address cycle
  - Memory Read, Memory Write commands
  - Configuration Read and Write commands
  - Fast Back-to-Back Transactions
  - Type 0 Configuration space
  - Parity generation and parity error detection
- AHB2.0 interface compliant
- Synchronous AMBA and PCI clocks
- SSRAM accessible from both PCI and AHB bus, the memory spaces are separately
- Enable configuration of SSRAM capacity and FIFO depth
- Output encryption and input decryption with AES-128
- DMA handshaking interface

B. Block Diagram

The blocks of IP core are designed to exchange data between PCI 2.3 bus and AHB 2.0 bus. The function of some basic modules is showed as follows:

- PCI TARGET receives and responses requests of PCI initiator.
- AHB SLAVE receives and responses requests of AHB master.
- ARBITER arbitrates the read/write accesses from/to Synchronous Static Random Access Memory (SSRAM).
- AES-128 encryptor enciphers data, which is plaintext, from PCI bus before transferring to AHB bus.
- AES-128 decryptor deciphers data, which is ciphertext, from AHB bus before transferring to PCI bus.

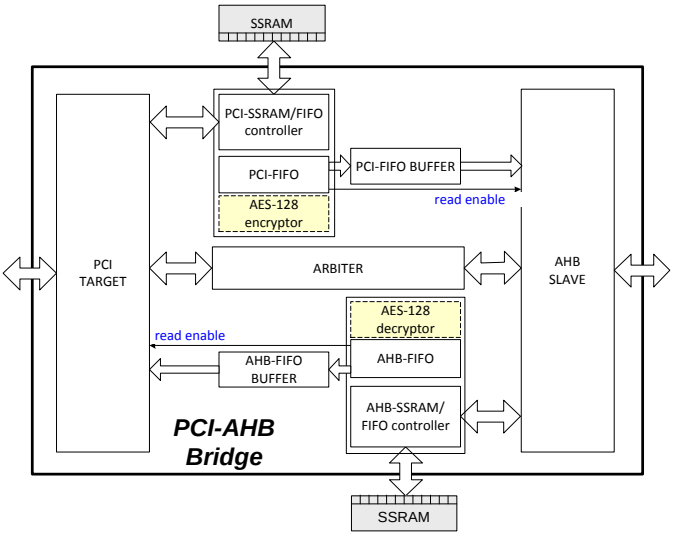

Fig1.Block diagram of PCIIP core

C. Operation Flow

For PCI-to-AHB flow, data of PCI host is stored into SSRAM. It is loaded to PCI-FIFO before is read by AHB master. If the encryption mode is active, data will be enciphered before is gotten by AHB master (Fig 3).

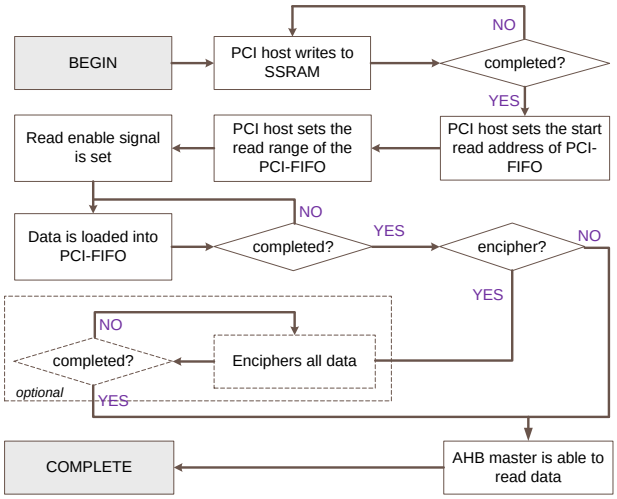

Fig 3. PCI-to-AHB flow

For AHB-to-PCI flow, the data transfer is shown asFig 4.

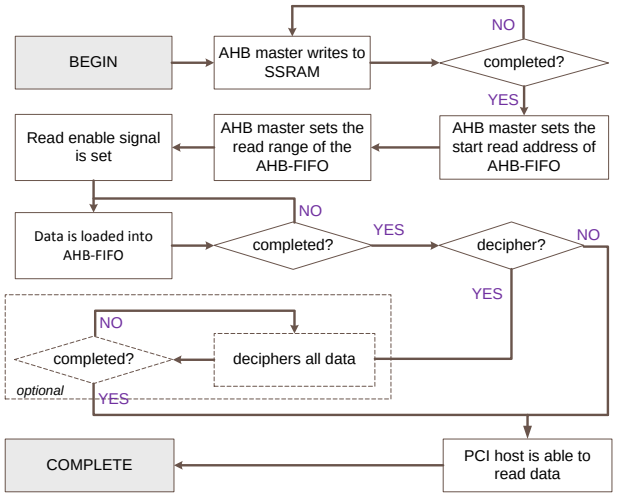

Fig 4.AHB-to-PCI flow

III. Analysis of Function and Application

A. PCI Target

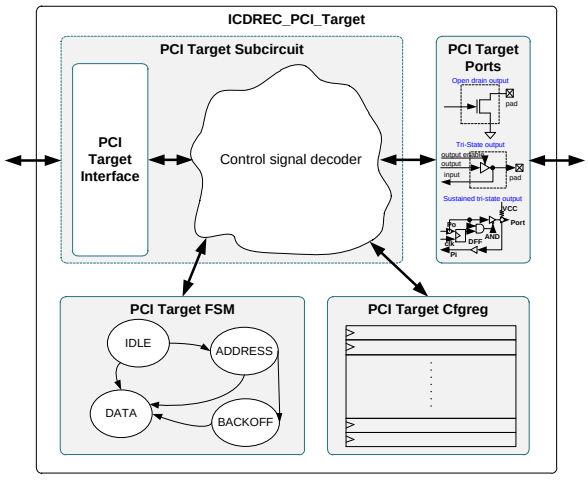

Fig 5. PCI target block diagram

The PCI target responds toall requests of PCI initiator when this device is selected.It can process these following commands:

- configuration read/write
- memory read/write
- memory read multiple
- dual address cycle
- memory read line
- memory write and invalidate

The request can be in single data or burst data mode. In the burst data mode, many consecutive addresses will be satisfied that doesn't need to send request signals again. This helps to increase the system performance for large data block transfer.

B. Arbiter

There are two FIFO modules which can read from the corresponding memory (AHBSSRAM and PCI SSRAM). These FIFO only read data from the memories. This data can be encrypted or decrypted before any transaction. Besides, the AHB bus can also access the data from AHBSSRAMand the PCI bus can also access data from PCI SSRAM. When the FIFO reads from its memory, it maybe disputed with the bus access (to the corresponding memory) if they read or write at the same time.

The control arbiter module is designed to handle and arbitrate when the bus and the FIFO access from the same memory. So, when any bus or FIFO wants to access data from the memory, it must sample its corresponding signals that the arbiter grants. Any address and control phase are true and can be handled when they havethe permission from the arbiter. There are some rules of arbitration as following:

1. If there are no subjects access data, all of the bus and the FIFO are allowed (have the permissions).
2. If there is only one subject accesses data, the arbiter always allows it and doesn't lock the others.
3. If there is the disputation, we have three rules:
   a. If the address of the bus and the address of the FIFO aren't the same, the winner is the one which is waiting (wait for lost but not wait for the other reasons).
   b. At the beginning of the arbitration, if the address of the bus and the address of the FIFO aren't the same, the winner is always the bus access.
   c. If the address of the bus and the address of the FIFO are the same, the winner is always the FIFO access.

C. AHBSlave

The AHB Slave is designed to communicate between AHB Master and the AHB memory space. There are two AHB memory spaces: the SSRAM memory and the functional register field. Both of them have the same offset address. The AHB bus must have two decode selection signals to access to them. At one time, only one select signal is active to access the AHBSSRAM or the functional register field.

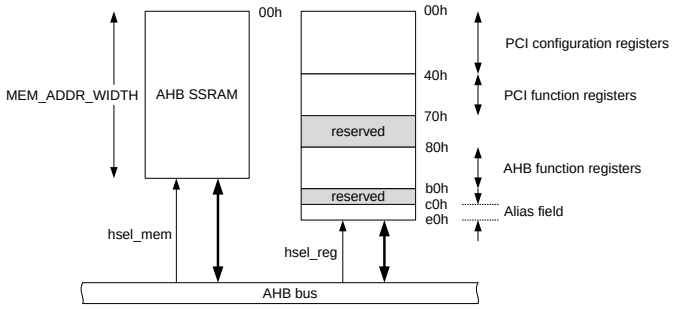

Fig 6.AHB memory space

About the functional registers, the AHB bus only writes into the AHB register region (80h-B0h) but it can read all of the functional regions (the configuration registers, the AHB registers and the PCI registers).

When the AHB bus wants to access the AHBSSRAM, it must have the permission from the arbiter.

We can use the AHB interface to communicate with the AHB master to transfer the data. We also use the DMA slave to transfer data directly. Note that the DMA slave only request the read command, the write command isn't supported.

D. AES-128 encryptor/decryptor

If the security mode is active, the output data, from PCI bus to AHB bus, will be enciphered with a 128-bit key and the input data, from AHB bus to PCI bus, will be deciphered with the same key. The encryption algorithm is shown as follows:

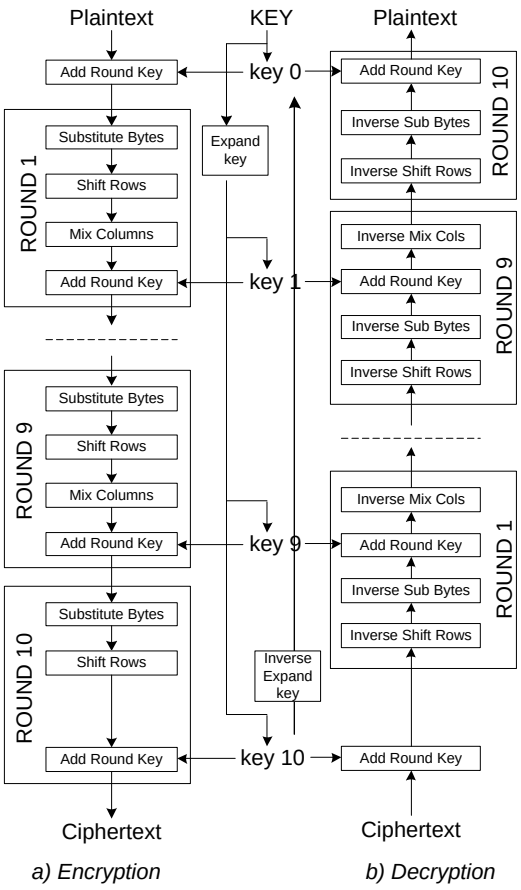

Fig 7. AES-128 encryption and decryption algorithm

E. Demo and application

The demo system, which is used to test IP core, is built as follows:

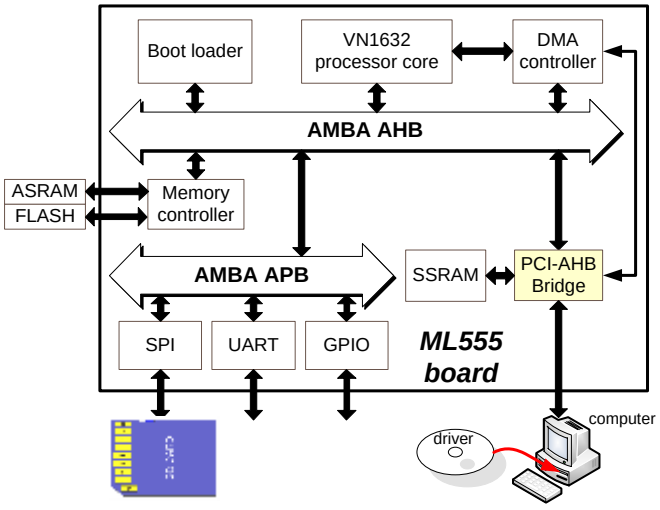

Fig 8. Demo system of PCI-AHB bridge IP core

At AHB bus side, the components are load into Xilinx-FPGA board ML555 and a VN1632[5] processor is used to control all operations. ThisML555 board is plugged in PCI slot of computer which is installed the suitable driver to identify PCI card and access data from SDCARD.

So, you are able to use a processor core to build a private application systemand connect to computer by PCI slot. Additionally, the exchange data can be protected by AES-128 encryption mechanism.

IV. CONCLUSION

This IP core has two outstanding features. First, it is the data exchange bridge between PCI 2.3 bus and AHB bus. Second, if the encryption mode is active, data from PCI master will be enciphered with AES-128 algorithm before sending and data from AHB master will be deciphered before is received by PCI master. The second feature supports to the security applications.

Up to now, the PCI-AHBbridge IP core was tested on FPGA board after had been simulated by VCS tool.

REFERENCES

[1] PCI Special Interest Group, "PCI local bus specification revision 2.3," March 29, 2002.

[2] PCI Special Interest Group, "PCI-to-PCI bridge architecture specification revision 1.1," December 18, 1998.

[3] ARM Ltd, "AMBATM specification revision 2.0," May 13, 1999.

[4] Federal Information Processing Standards Publications, "Announcing the ADVANCED ENCRYPTION STANDARD (AES)," November 26, 2001.

[5] ICDREC, *VN1632 RISC microprocessor user's manual*., 2010.