

Design and FPGA-based implementation of Smartcard Reader

Yeshesvee Koul, Ankita Pathak

Abstract— This paper describes about the Implementation and Simulation of a Smart Card Reader design on Xilinx Spartan-3E FPGA Basys 2 board. This Smart Card reader design is in compliance with ISO/IEC 7816-3 standard. The code is described in Verilog at RTL level. A Smart Card reader hardware was used for verification purpose. The Smart Card reader design worked in synchronization with the hardware

Index Terms—Smart Card, ISO/IEC 7816-3 standard, Answer-To-Reset, FPGA

I. INTRODUCTION

Smart Cards are called ‘smart’ because they have a chip embedded in it which can store data and transmit it digitally. Smart Cards are used for identification, data access, and conducting financial transactions. It can be used to store money and information electronically and can help to transfer it in a secure but portable medium. It acts like a mini-computer. They come in standard sizes defined by ISO/IEC standard. They offer enhanced security than conventional magnetic stripe cards, hence smart cards are becoming a common part of our everyday lives. Since smart cards are in use globally, the International Standard Organization has laid some standards so that they are universally compatible. ISO/IEC 7816 is a series of standards specifying integrated circuit cards and the use of such cards for interchange. These cards are identification cards intended for information exchange negotiated between the outside world and the integrated circuit in the card. As a result of an information exchange, the card delivers information (computation result, stored data), and/or modifies its content (data storage, event memorization). ISO/IEC 7816 is divided into fourteen parts out of which ISO/IEC 7816-3 specifies electrical interface and transmission protocols for card with contacts. In this

Manuscript received Feb , 2016.

Yeshesvee Koul, pursuing M.Tech in VLSI Design at C-DAC, Noida, in affiliation with GGSIPU, New Delhi, India.+91-9971106310

Ankita Pathak, pursuing M.Tech in VLSI Design at C-DAC, Noida, in affiliation with GGSIPU, New Delhi, India.+91-8285243618

paper, the card reader design presented is for a contact smart card.

II. SYSTEM DEVELOPMENT

A. Block Diagram

Figure 1 shows the general block diagram of smart card reader system. The code is burned in FPGA memory. The I/O ports on FPGA board are used for exchanging signals between FPGA board and smart card directly.

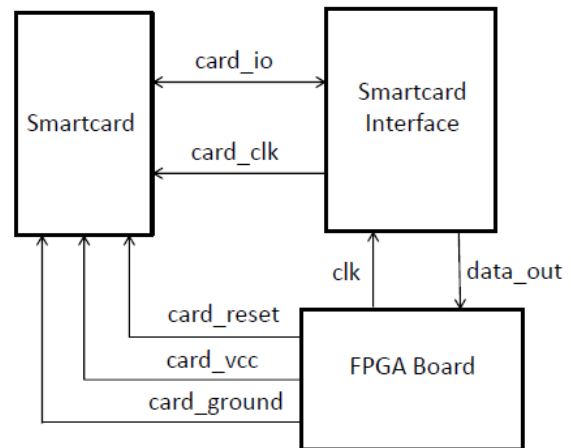


Figure 1. General Block diagram

The FPGA board issues a reset signal to smart card and the card responds with an Answer To Reset (ATR). An Answer To Reset (ATR) is a message output by a contact Smart Card conforming to ISO/IEC 7816-3 standards, following electrical reset of the card's chip by a card reader. After correct Answer To Reset is obtained from the card, the communication between card and card reader takes place via T=0 protocol which is again mentioned in ISO/IEC 7816-3 standard.

B. Smart Card Reader

Figure 2 shows the more detailed block diagram of smart card reader. Various modules involved are explained below:

Baud Rate Counter: The ISO standard aligns with the use of two widely used external clock frequencies, 3.579545 MHz

and 4.91522 MHz. The former frequency is the more widely used (being based on the NTSC colour sub carrier frequency)

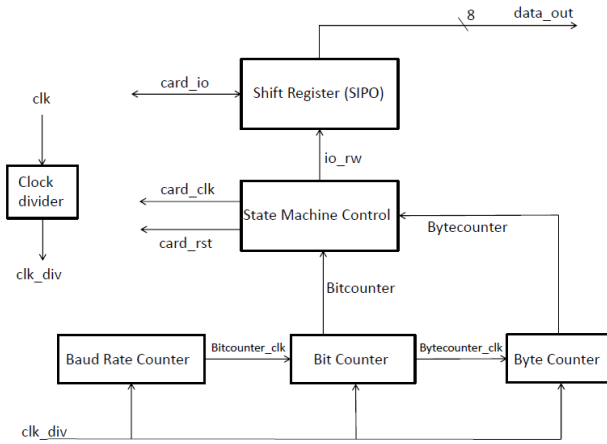


Figure 2. Smart Card Reader

and results in a clock divider of 372 in order to produce a 9600 bit per second (not exact but within tolerance) serial communication speed. The purpose of baud rate counter is to count 372 clock cycles. When 372 clock cycles have been counted, its value is reset.

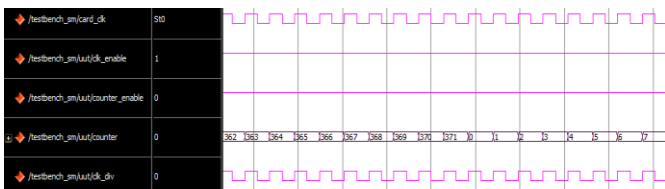


Figure 3. Output waveform of Baud Rate Counter

Clock Divider: Clock available from FPGA board is 50MHz. Clock divider divides this frequency by 14 to obtain frequency of 3.57 MHz.

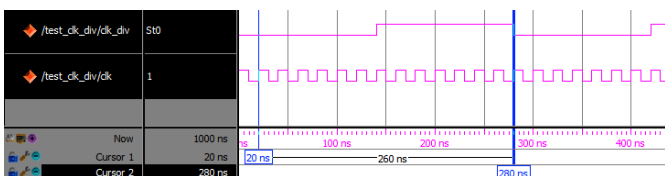


Figure 4. Output Waveform of Clock Divider

$$T_{clk} = 20 \text{ ns}$$

$$f_{clk} = \frac{1}{20\text{ns}} = 50 \text{ MHz}$$

$$T_{clkdiv} = 280 \text{ ns}$$

$$f_{clkdiv} = \frac{1}{280\text{ns}} = 3.57 \text{ MHz}$$

Bit Counter: 372 clock cycles constitute 1 etu. For asynchronous transmission, it takes 1 etu to transfer 1 bit and 12 etu for transmission of 1 character frame. The purpose of bit counter is to count all the 12 bits in one character frame. When 12 bits have been received, this counter is reset and starts counting next 12 bits.

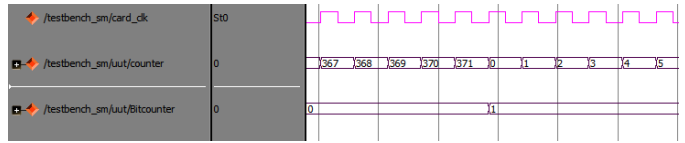


Figure 5(a). Output Waveform of Bit Counter

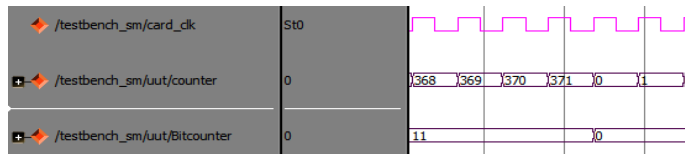


Figure 5(b). Output Waveform of Bit Counter

Byte Counter: Since a character frame consists of 12 etu, byte counter counts number of characters (or bytes) received.

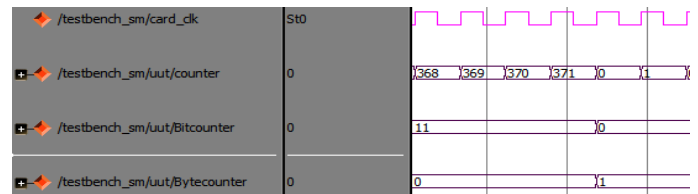


Figure 6 – Output Waveform of Byte counter

Shift Register: It is a Serial In Parallel Out (SIPO) shift register. It receives serial data from card via card I/O pin (C7) and saves it parallel in a data buffer. Data is sampled at every 186th clock cycle. When 12 etu are completed, i.e., when bit counter counts 11, bit2 to bit9 of the received character frame is the byte which gets saved in data_out register.

State Machine: It is conceived as an abstract machine that can be in one of a finite number of states. The machine is in only one state at a time; the state it is in at any given time is called the current state. It can change from one state to another when initiated by a triggering event or condition; this is called a transition. A particular FSM is defined by a list of its states, and the triggering condition for each transition.

C. Smart Card Reader Hardware

Figure 7 shows the reader hardware used. It had following contacts:

VCC (C1)

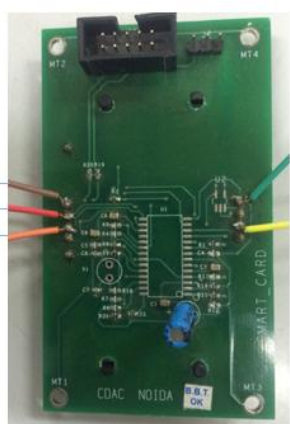
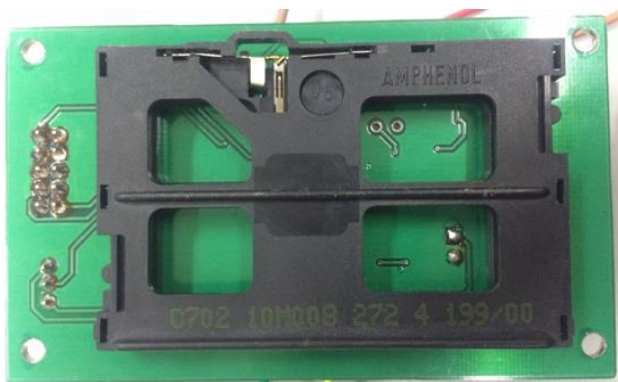
This contact is used to supply the card with power.

RST (C2)

This contact is used to provide the card with reset signal.

CLK (C3)

This contact is used to provide the card with clock signal.



C1 (VCC) ←
 C2 (RESET) ←
 C3 (CLOCK) ←

→ C5 (GND)
 → C7 (I/O)

Figure 7. Top & Bottom View of Reader Hardware

GND (C5)

This contact is connected with ground.

I/O (C7)

This contact is used as input (reception mode) or output (transmission mode).

III. SYSTEM OPERATION

The FPGA board issues a reset signal to smart card and the card responds with an Answer To Reset (ATR). An Answer To Reset (ATR) is a message output by a contact Smart Card conforming to ISO/IEC 7816-3 standards, following electrical reset of the card's chip by a card reader. After correct Answer To Reset is obtained from the card, the communication between card and card reader takes place via T=0 protocol which is again mentioned in ISO/IEC 7816-3 standard.

IV. RESULTS

A. Simulation Output

Card is inserted into the card acceptor. By following the ISO/IEC 7816-3 standard, sequence to activate smart card contacts is to set reset to high, go to the Wait state, and wait for a low signal from the card, the start bit of the TS for Answer to Reset. There is a baud rate counter counting to 372 for every bit received or sent to synchronize the data transmission. The received bits are sampled at the 186th count, which is in the center of each bit received. Two other counters are used, one to count bits for each character and one to count bytes received or sent. After 19 Answer to Reset characters are received, the smart card reader interface is now ready to send commands and receive responses based on the T=0 protocol.



Figure 8. Simulation Output Waveform

B. Synthesis Results

Table 1: Device Utilization Summary

Selected Device : 3s100ecp132-4		
Number of Slices:	47 out of 960	4%
Number of Slice Flip Flops:	73 out of 1920	3%
Number of 4 input LUTs:	69 out of 1920	3%
Number of bonded IOBs:	13 out of 83	15 %
Number of GCLKs:	2 out of 24	8%

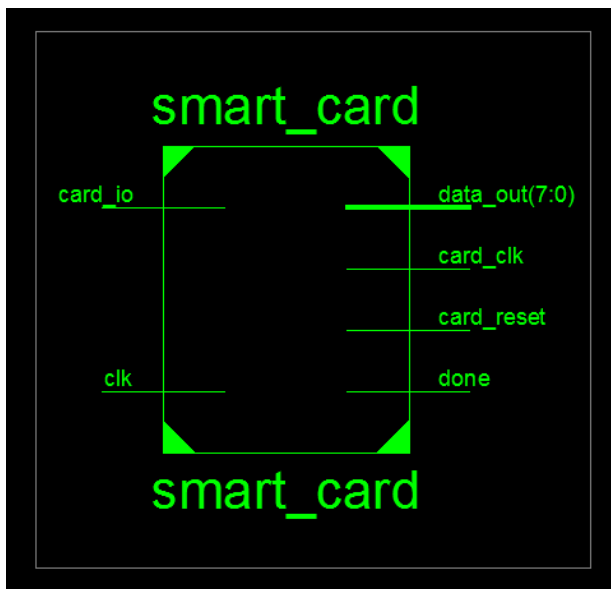


Figure 9. Top level Schematic

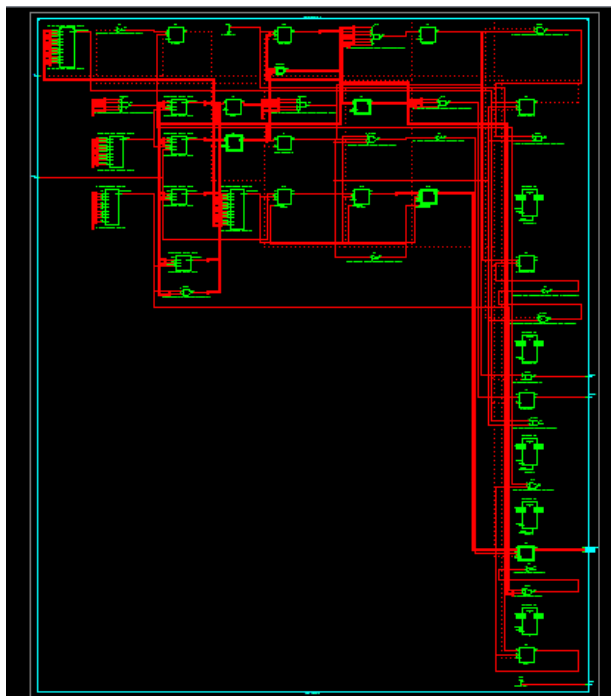


Figure 10. RTL Schematic

C. Hardware Setup

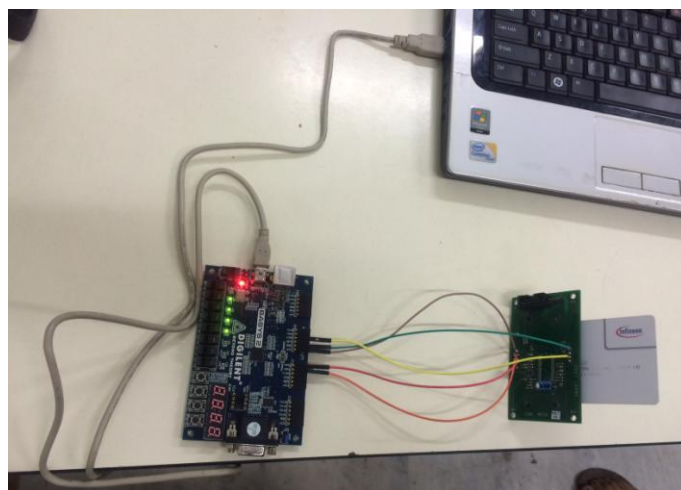


Figure 10. Experimental Set-up

The experimental setup consists of Basys 2 FPGA Board which has Xilinx Spartan 3E FPGA & Smart Card Hardware along with connecting wires and cable.

REFERENCES

- [1] J. Patil, "Implementation of Smart Card Reader Using CPLD," International Conference on Computers and Devices for Communication, 2009.
- [2] Saylee S. Bidwai, Sandeep S. Bidwai "Manifestation of a Smart Card Reader using VLSI Technology", IJCST Vol. 3, Issue 1, Jan. – March 2012.
- [3] International standard , ISO/IEC 7816-3 third edition 2006-11-01.
- [4] Wolfgang Rankl and Wolfgang Effing, Smart Card Handbook, 2nd Edition. New York: John Wiley & Sons, 2004.
- [5] David B Everett, "Smart Card Tutorial", <http://www.smartcard.co.uk/tutorials/sct-itsc.pdf>, Sep 1992.
- [6] K. Parnel, "Using CoolRunner CPLDs in Smart Card Reader Applications", <http://www.xilinx.com/xapp118.pdf>, May 18, 2000.
- [7] https://en.wikipedia.org/wiki/Card_reader#Smart_card
- [8] https://en.wikipedia.org/wiki/ISO/IEC_7816



Yesheesvee Koul received B.Tech in Electronics Instrumentation & Control from YMCA University of Science & Technology, Faridabad, Haryana. She is currently pursuing M.Tech in VLSI Design from C-DAC, Noida affiliated to Guru Gobind Singh Indraprastha University, New Delhi. She has been a student

member of IEEE from 2010-2011



Ankita Pathak received B.Tech in Electronics & Communication from Invertis University, Bareilly, UP. She is currently pursuing M.Tech in VLSI Design from C-DAC, Noida affiliated to Guru Gobind Singh Indraprastha University, New Delhi.