Hardware Security EL9423
LAB 1

Ashik H. Poojari (ap4613)
Nimisha Limaye (nsl278)

March 8, 2017

Abstract

In this lab, we are implementing denial of service/functionality change and key leaking in RC5 design. We have designed the trojans in such a way that it takes up only 4 LUTs and 2 DSP48E1 blocks. The frequency of design with trojan has only decreased by 0.58% as compared with original RC5 design.

1. Introduction

RC5 is an encryption algorithm using a key of length 128 Bit with input and output data of length 64 Bit. The 4 bit input data and 128 Bit key are inputted using switches on the Nexys 4DDR board. After entering key, key valid button is pressed and signaled to enter the data. After entering the data, data valid button is pressed and the encryption and decryption of the data begins. In this lab, we are given task of inserting a DoS or functionality change trojan in the RC5 design along with leaking the key. This task is to be implemented only in the form of xilinx primitives and not via behavioral or structural code. Implementation of DoS trojan is explained in section 2, key leaking is explained in section 3, the area mapping of RC5 with and without trojan on Nexys 4DDR board is shown in section 5 and resource utilization and performance of RC5 with and without trojan are compared in section 5.

2. Denial of Service Trojan

2.1 Activation

The DOS Trojan is activated by temperature. When the temperature reaches a T_{HIGH} set point of 64°C an interrupt is triggered by the temperature. This is taken as input to the DOS trojan and is triggered. For this lab we will use a heat gun to trigger the temperature sensor, for demonstration purpose.

2.2 Function

The circuit starts to give faulty output when a temperature of 64°C is reached. According to Xilinx data-sheets, the Nexys 4DDR FPGA should work properly for temperatures upto 125°C. But due to the Trojan present, this circuit will start giving faulty encryption values as it reaches 64°C. We achieved this functionality by flipping one of the b_reg bits in the encryption logic. Since b_reg value is used by the rotate logic, it wrongly shuffles the output value. Hence, the DOS trojan functionality can be achieved easily.

2.3 Resource Utilization

We used just one LUT to implement this denial of service/functionality change trojan.

3. Key Leak Trojan

3.1 Activation

The activation of this trojan is temperature sensitive as well and is activated by the T_{HIGH} set point of 64°C.

3.2 Function

We are using two LEDs to leak the key information. One led is used to leak zeros and other to leak ones. These LEDs flicker depending on the key input. So if there are consecutive ones, then LEDs flicker for the number of times the one is present in the key contiguously. The LED flickers with a period of 32 ms at 50% duty cycle. So with the naked we cannot deduce the number of flickers. We need to record the flickering with a slow motion camera, and since mobile phones these days come with a slow motion camera, we are using the same to read the key. We are using two counters to implement the key leak function, one 7 bit counter to point to the 128 bit key and another counter for calculating the precise delay for LED flicker. The logic for counters is implemented in form of DSP48E1 xilinx primitive to acheive a small area footprint for the key leak trojan.

3.3 Resource Utilization

We used just 3 LUTs and 2 DSP48E1 (to realize precise delay using counter) for the key leak trojan part.

4. Area Mapping

The area mapping for RC5 with and without Trojan is shown in Fig 1 and Fig 2 respectively.

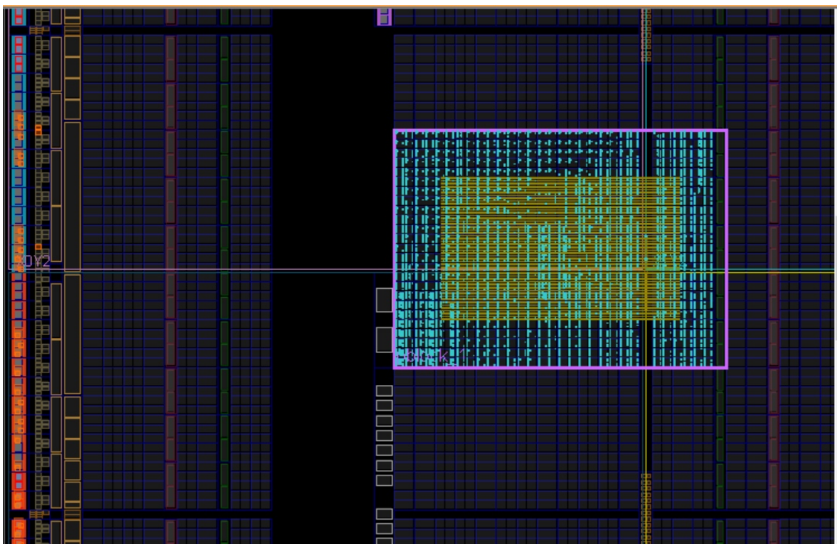

Figure 1: The Plan ahead of RC5 without Trojan.

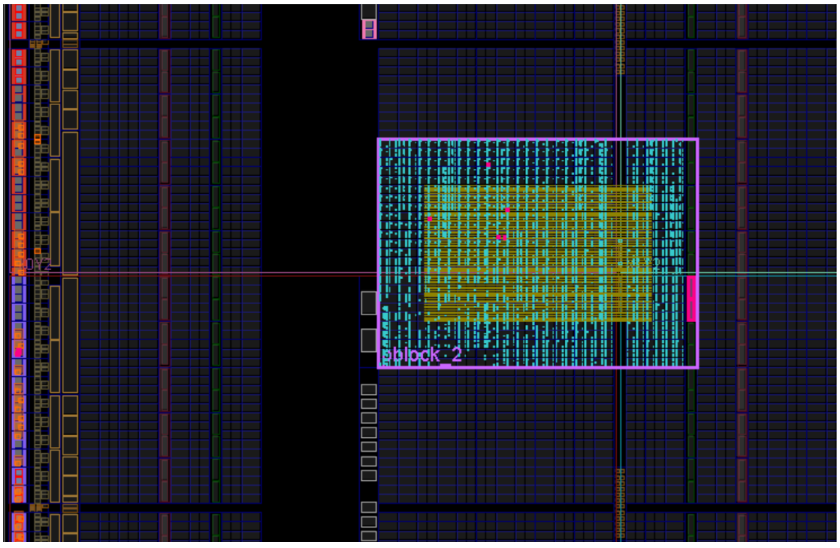

Figure 2: The Plan ahead of RC5 with Trojan. Here we can see pink colored highlight for Trojan LUT and Trojan DSP48E1 blocks.

5. Analysis Of RC5 With and Without Trojan

5.1 Resource Utilization

Utilization	RC5	Trojan RC5	Percentage Increase (%)
Slice Registers	1,690	1,695	0.29
Slice LUTs	2,700	2,746	1.73
IOBs	51	54	5.89
DSP48E1s	0	2	200

5.2 Performance Analysis

Hardware	Frequency(MHz)	Percentage decrease (%)
RC5	341.76	0
Trojan RC5	339.78	0.58

For demo please refer to the video

6. Conclusion

Trojan was inserted successfully in RC5 design to intentionally change the functionality when temperature crosses 64°C and leak the key via LEDs with fast enough frequency to notice that key is being leaked, but with slow enough frequency to catch it on slow motion camera.