Research and Design of high-security configurable RO-PUF based on FPGA

VEGINATI ARAVIND
ECE A,AP19110020044
SRM UNIVERSITY AP
MANGALAGIRI,GUNTUR,AP

P.Sabari Priya
ECE A,AP19110020009
SRM UNIVERSITY AP
MANGALAGIRI,GUNTUR,AP

A.Sriya
ECE A,AP19110020058
SRM UNIVERSITY AP
MANGALAGIRI,GUNTUR,AP

P.N.V.Koteswararao
ECE A,AP19110020011
SRM UNIVERSITY AP
MANGALAGIRI,GUNTUR,AP

G. Satwik
ECE A,AP19110020067
SRM UNIVERSITY AP
MANGALAGIRI,GUNTUR,AP

Abstract—With the development of electronic equipment, several security concerns have been raised. Due to the lack of reliability and uniqueness of traditional RO-PUF a new configurable R0-PUF is proposed based on the delay characteristics of the ring oscillator. This paper proposes a RO-PUF configurable structure based on RO grouping. Thereby increases the randomness and complexity of the overall structure. This design makes the configurable RO-PUF more flexible and increases the number of CRP' s. Finally the response generated by RO-PUF is subjected to error correction.

This design is implemented in Xilinx' s spartan series FPGA chip.

Introduction

With the rapid development of integrated circuit technology and the popularization of electronic equipment, various information security issues such as malicious insertion of Trojan horse files are raised. In order to protect user data and product information, Electronic products' anti-counterfeiting encryption technology is particularly important. Physical Unclonable Function (PUF) provides new ideas for solving such information security problems. Aiming at the lack of reliability and uniqueness of the traditional configurable ring oscillator physical unclonable function (ROPUF) due to the simple configurable path, a configurable RO-PUF is proposed based on the delay characteristics of the ring oscillator.Ease of Use

RO CONCEPT:

It is a device composed of an odd number of NOT gates in a ring, whose output oscillates between two voltage levels, representing true or false the NOT gate , or inverters are attached in chains and the output of the last inverter is in feedback of the first.

RC RO (RECONFIGURABLE RING OSCILLATOR)

In the traditional RO-PUF there is no grouping of RO' s involved which raised several security concerns.

In this project we are trying to group the RO' s which increases the number of paths by 9 times from the traditional RO-PUF. Additionally it also increases the randomness.

PUF CONCEPT:

Puf is a physical unclonable function. It is a physical object that produces a physically defined "digital fingerprint" output (response) for a particular input and conditions (challenge) that acts as a unique identification.

RO-PUF principle:

RO-PUF is mainly composed of a ring oscillator, multiplexer, counter, etc.

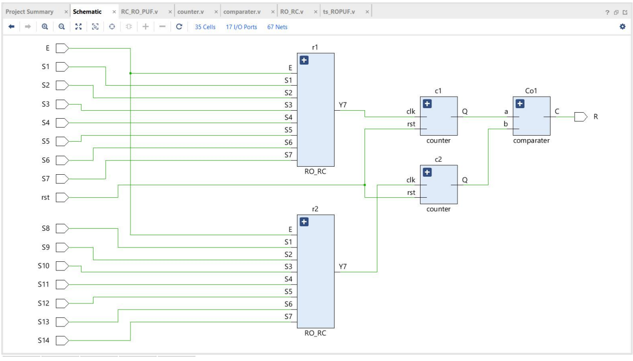
The data selector MUX receives the output signals of the two ring oscillators and the external input excitation signal of the system.

Then the two counters respectively count the oscillation frequencies of the two ROs in the same time period, and finally output through the comparator.

Oscillation frequency result, the result is logic 1 or 0.

DESIGN SECTION:

In order to increase the complexity of the RO structure and generate a larger number of CRPs, this paper proposes a RO-PUF configurable structure based on RO grouping. In this structure, the ROs in the configurable ROPUF are first divided into several groups. If there are N-ROs in the RO-PUF, the ROs are divided into N/2 groups. The overall structure of the configurable RO-PUF requires that the macro structure of the RO be consistent, that is, the effects of process deviations are excluded. The number and structure of the ROs must be exactly the same.



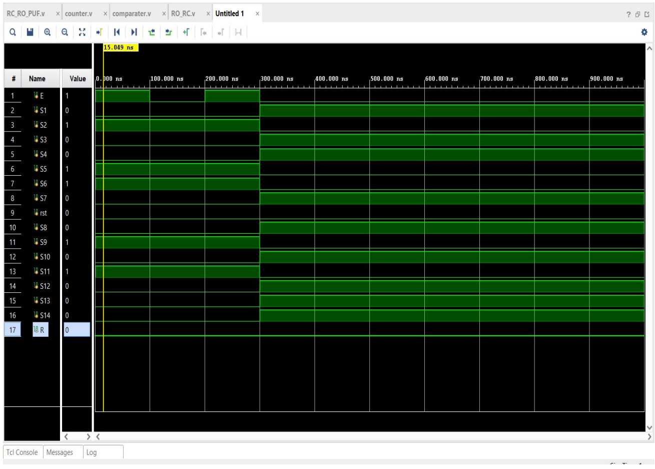
HDL CODE AND IMPLEMENTATIONS:

```
module RO_RC(E,S1,S2,S3,S4,S5,S6,S7,Y7);

input E, S1, S2, S3, S4, S5, S6, S7
;

output
Y7;

wire
A1,A2,A3,A4,A5,A6,A7,B1,B2,B3,B4,B5,B6,B7,
Y1,Y2,Y3,Y4,Y5,Y6,Y7;

nand #1 a1(A1,E,A7);

nand #1 a2(B1,E,B7);

MUX_2x1 M1(A1,B1,S1,Y1);

not #1 n1(A2,Y1);

not #1 t1(B2,Y1);

MUX_2x1 M2(A2,B2,S2,Y2);

not #1 n2(A3,Y2);

not #1 t2(B3,Y2);

MUX_2x1 M3(A3,B3,S3,Y3);

not #1 n3(A4,Y3);

not #1 t3(B4,Y3);

MUX_2x1 M4(A4,B4,S4,Y4);

not #1 n4(A5,Y4);

not #1 t4(B5,Y4);

MUX_2x1 M5(A5,B5,S5,Y5);

not #1 n5(A6,Y5);

not #1 t5(B6,Y5);

MUX_2x1 M6(A6,B6,S6,Y6);

not #1 n6(A7,Y6);

not #1 t6(B7,Y6);

MUX_2x1 M7(A7,B7,S7,Y7)

endmodule
```

HDL CODE RC_ROPUF

```
module RC_RO_PUF(

input
E,S1,S2,S3,S4,S5,S6,S7,rst,S8,S9,S10,S11,S12,S13,S
14,

output R

        );

        wire Y7,Q,Y8,Q1;

        RO_RC r1 (E,S1,S2,S3,S4,S5,S6,S7,Y7);

        counter c1 (Y7,rst,Q);

        RO_RC r2
(E,S8,S9,S10,S11,S12,S13,S14,Y8);

        counter c2 (Y8,rst,Q1);

        comparater Co1 (Q,Q1,R);

        endmodule
```

RESULTS/WAVEFORMS:



#	Name	Value
1	E	1
2	S1	0
3	S2	1
4	S3	0
5	S4	0
6	S5	1
7	S6	1
8	S7	0
9	rst	0
10	S8	0
11	S9	1
12	S10	0
13	S11	1
14	S12	0
15	S13	0
16	S14	0
17	R	0

OBSERVATIONS:

)S1 to S7 are the inputs for first RC_RO

2)S8 to s14 are the inputs for second RC_RO

3)If the first counter gives output greater than the second counter (a>b) then the comparator gives the response as 1

4)If a<=b then comparator gives the response as 0

SYNTHESIS REPORT:

```
Copyright 1986-2020 Xilinx, Inc. All Rights Reserved.

-------------------------------------------------------------------
-------------------------------------------

| Tool Version : Vivado v.2020.1 (win64) Build
2902540 Wed May 27 19:54:49 MDT 2020

| Date            : Sun Nov 21 13:08:22 2021

| Host            : LAPTOP-9D840CG3 running
64-bit major release   (build 9200)

| Command        : report_utilization -file
RC_RO_PUF_utilization_synth.rpt -pb
RC_RO_PUF_utilization_synth.pb

| Design         : RC_RO_PUF

| Device         : 7z020clg484-1

| Design State : Synthesized

-------------------------------------------------------------------
-------------------------------------------


Utilization Design Information


Table of Contents

-----------------

1. Slice Logic

1.1 Summary of Registers by Type

2. Memory

3. DSP

4. IO and GT Specific

5. Clocking

6. Specific Feature

7. Primitives

8. Black Boxes
```

9. Instantiated Netlists

1. Slice Logic

```
+------------------------+------+-------+-----------+-------+
|          Site Type          | Used |
Fixed | Available | Util% |
+------------------------+------+-------+-----------+-------+
| Slice LUTs*                 |     4 |
      0 |       53200 | <0.01 |
|    LUT as Logic             |     4 |
      0 |       53200 | <0.01 |
|    LUT as Memory           |     0 |
   0 |       17400 |   0.00 |
| Slice Registers            |     2 |
   0 |      106400 | <0.01 |
|    Register as Flip Flop |     2 |
0 |      106400 | <0.01 |
|    Register as Latch      |     0 |
   0 |      106400 |   0.00 |
| F7 Muxes                       |     0 |
      0 |       26600 |   0.00 |
| F8 Muxes                       |     0 |
      0 |       13300 |   0.00 |
+------------------------+------+-------+-----------+-------+
```

* Warning! The Final LUT count, after physical optimizations and full implementation, is typically lower. Run opt_design after synthesis, if not already completed, for a more realistic count.

1.1 Summary of Registers by Type

```
+-------+--------------+-------------+--------------+
| Total | Clock Enable | Synchronous | Asynchronous |
+-------+--------------+-------------+--------------+
| 0       |                   _ |
   - |                 - |
| 0       |                   _ |
   - |              Set |
| 0       |                   _ |
   - |           Reset |
| 0       |                   _ |
Set |                 - |
| 0       |                   _ |
Reset |                 - |
| 0       |                 Yes |
   - |                 - |
| 0       |                 Yes |
   - |              Set |
| 0       |                 Yes |
   - |           Reset |
| 0       |                 Yes |
Set |                 - |
| 2       |                 Yes |
Reset |                 - |
+-------+--------------+-------------+--------------+
```

2. Memory

```
+----------------+------+-------+-----------+-------+
|      Site Type    | Used | Fixed |
Available | Util% |
+----------------+------+-------+-----------+-------+
| Block RAM Tile |     0 |      0 |
   140 |   0.00 |
|    RAMB36/FIFO* |     0 |      0 |
   140 |   0.00 |
|    RAMB18          |     0 |      0 |
      280 |   0.00 |
+----------------+------+-------+-----------+-------+
```

* Note: Each Block RAM Tile only has one FIFO logic available and therefore can accommodate only one FIFO36E1 or one FIFO18E1. However, if a FIFO18E1 occupies a Block RAM Tile, that tile can still accommodate a RAMB18E1

3. DSP

```
+-----------+------+-------+-----------+-------+

| Site Type | Used | Fixed | Available | Util% |

+-----------+------+-------+-----------+-------+

| DSPs           |        0 |         0 |
220 |   0.00 |

+-----------+------+-------+-----------+-------+
```

4. IO and GT Specific

```
+-----------------------------+------+-------+-----------+----
---+

|                Site Type               |
Used | Fixed | Available | Util% |

+-----------------------------+------+-------+-----------+----
---+

| Bonded IOB                                |
   3 |         0 |            200 |    1.50 |

| Bonded IPADs                            |
0 |         0 |                2 |    0.00 |

| Bonded IOPADs                           |
0 |         0 |            130 |    0.00 |

| PHY_CONTROL                               |
0 |         0 |                4 |    0.00 |

| PHASER_REF                                |
   0 |         0 |                4 |    0.00|

| OUT_FIFO                                  |
   0 |         0 |            16 |    0.00 |

| IN_FIFO                                   |
   0 |         0 |            16 |    0.00 |

| IDELAYCTRL                              |
   0 |         0 |                4 |    0.00 |

| IBUFDS                                     |
   0 |         0 |            192 |    0.00 |

| PHASER_OUT/PHASER_OUT_PHY     |        0 |
   0 |              16 |    0.00 |

| PHASER_IN/PHASER_IN_PHY         |        0 |
      0 |              16 |    0.00 |

| IDELAYE2/IDELAYE2_FINEDELAY |        0 |
   0 |            200 |    0.00 |

| ILOGIC                                     |
   0 |         0 |            200 |    0.00 |

| OLOGIC                                     |
   0 |         0 |            200 |    0.00 |

+-----------------------------+------+-------+-----------+----
---+
```

5. Clocking

```
+------------+------+-------+-----------+-------+

|    Site Type | Used | Fixed | Available | Util% |

+------------+------+-------+-----------+-------+

| BUFGCTRL     |        0 |         0 |
   32 |    0.00 |

| BUFIO          |        0 |         0 |
   16 |    0.00 |

| MMCME2_ADV |        0 |         0 |
   4 |    0.00 |

| PLLE2_ADV    |        0 |         0 |
   4 |    0.00 |

| BUFMRCE       |        0 |         0 |
   8 |    0.00 |
| BUFHCE       |     0 |     0 |
   72 |   0.00 |

| BUFR          |     0 |     0 |
   16 |   0.00 |

+------------+------+-------+-----------+-------+


6. Specific Feature

-------------------


+-------------+------+-------+-----------+-------+

|   Site Type   | Used | Fixed | Available |
Util% |

+-------------+------+-------+-----------+-------+

| BSCANE2       |     0 |     0 |
      4 |   0.00 |

| CAPTUREE2     |     0 |     0 |
   1 |   0.00 |

| DNA_PORT      |     0 |     0 |
      1 |   0.00 |

| EFUSE_USR     |     0 |     0 |
   1 |   0.00 |

| FRAME_ECCE2 |     0 |     0 |
   1 |   0.00 |

| ICAPE2         |     0 |     0 |
      2 |   0.00 |

| STARTUPE2     |     0 |     0 |
   1 |   0.00 |

| XADC           |     0 |     0 |
      1 |   0.00 |

+-------------+------+-------+-----------+-------+


7. Primitives

------------


+----------+------+--------------------+

| Ref Name | Used | Functional Category |

+----------+------+--------------------+

| LUT2       |      5 |
   LUT |

| IBUF       |      2 |
      IO |

| FDRE       |      2 |            Flop &
Latch |

| OBUF       |      1 |
      IO |

+----------+------+--------------------+


8. Black Boxes

-------------


+----------+------+

| Ref Name | Used |

+----------+------+


9. Instantiated Netlists

-----------------------


+----------+------+

| Ref Name | Used |

+----------+------+
```

CONCLUSIONS:

(1)We have successfully increased the number of CRP’s by increasing the paths

(2)We have increased the security by increasing the randomness of the output

REFERENCES:

https://www.sciencedirect.com/science/article/pii/S1877050921004920

A.

•

•

•

•

•

•

•

•

•

•

•

II.

A.

1)

2)

a)

b)

c)

B.

C.

a)

TABLEI.

a.

Fig.1.

[1]

[2]

[3]

[4]

[5]

[6]

[7]