Chair of Computer Engineering
Prof. Dr. Stefan Katzenbeisser
Florian Frank
Felix Klement

Passau, 16.11.2021

Winter Semester 2021/22

Hardware-Based Security

Exercise 2

Submission: 23.11.2021, 12:00, Übungskasten 1 (Exercise box 1) or StudIP
Discussion: 23.11.2021, 16:00-18:00 or 24.11.2021, 10:00-12:00

If you have questions about the exercises and their evaluation, please contact Mr. Florian Frank at Frank.Florian@uni-passau.de or Mr. Felix Klement at Felix.Klement@uni-passau.de.

In this Exercise, you can gather at most **42 points**.

1. Task: Postprocessing of True Random Number Generators - Theoretical Background (11 points)

1. In which cases is post-processing required for true random number generators? (2 points)
2. Name 3 well known post processing techniques? What are their potential shortcomings? (9 points)

2. Task: Postprocessing of True Random Number Generators - Theoretical Background (15 points)

Two TRNGs should be compared. These TRNGs return the following sequences:

Output TRNG 1:

00100000000011111100000000100100
01111111111111100000100011010101
10000001110111111111111111100100
00000011111111001011101111111111
11111011111011110111010111101111

Output TRNG 2:

00110110100110110010000111000010
00111110001101111101111000100001
01001000110100111110000111001100
00111000000001100010110001101000
11010110101010010010101010111001

1. Compare the quality of the output of the two given TRNGs? What can you observe? (2 points)
2. Apply the Von-Neumann correction to these two random sequences. (5 points)
3. Apply the parity based method on the sequence given in the previous task. Calculate the resulting sequence using a chunk size of 16. (6 points)
4. What do you observe when comparing these two post-processing methods? (2 points)

3. **Task:** Cellular automata shift register (6 points)

Assume the binary integers $10101111_2 = 175_{10}$ and $11110010_2 = 242_{10}$. Use these integers to produce the relevant cellular automata shift register, based on the following tables. Please fill in all the tables, including the two auxilliary ones. (6 points)

Rule	175	242	175	175	242	175	242	242
State 0	0	1	1	1	0	1	1	0
State 1								

Table 1: Cellular automata shift register

Number	0	1	2	3	4	5	6	7
Neighbourhood								
Rule result								

Table 2: Rule 175

Number	0	1	2	3	4	5	6	7
Neighbourhood								
Rule result								

Table 3: Rule 242

4. **Task:** Physical Unclonable Functions - Theoretical Background (10 points)

1. Name 3 PUF applications, and explain briefly how the PUF can be used for them. (3 points)
2. Explain how the optical PUF works. What are its disadvantages? (2 points)
3. Think of a way to create an optical PUF yourself with simple means? (3 points)
4. Explain how the ring oscillator PUF works. What is its problem? (2 points)