

Computer Science and Engineering

Course work portal

powered by Moodle v2x

Hardware Security

Home > My courses > Previous Years > 2020 > Spring Semester (2020-21) > Hardware Security > Topic 3 > Class Test 1

Started on Monday, 22 February 2021, 5:00 PM

State Finished

Completed on Monday, 22 February 2021, 5:35 PM

Time taken 35 mins 23 secs

Grade 15.00 out of 25.00 (60%)

Question 1

Complete

Mark 0.00 out of 1.00

Flag question

In Von Neumann architecture

Select one:

- ☐ a. None of the above
- ☐ b. There are two separate memory buses
- ☐ c. Memory hierarchy is used to make security better
- ☒ d. The memory is physically shared for data and instruction storage

The correct answer is: None of the above

Question 2

Complete

Mark 1.00 out of 1.00

Flag question

In the polynomial basis representation with irreducible polynomial $r(y) = y^2 + \tau y + \mu$, in the composite field $GF((2^4)^2)$ the inverse is represented as $(\delta_1 y + \delta_0)$. δ_1 and δ_0 belongs to

Select one:

- ☐ a. $GF((2^4)^2)$
- ☐ b. None of the above
- ☒ c. $GF(2^4)$
- ☐ d. $GF(2^8)$

The correct answer is: $GF(2^4)$

Question 3

Complete

Mark 0.00 out of 2.00

Flag question

The Karatsuba multiplier can be represented as follows:

$$A(X) = A_h X^{m/2} + A_l$$

$$B(X) = B_h X^{m/2} + B_l$$

$$C(X) = A(X)B(X) = A_h B_h X^m + Z_1 X^{m/2} + A_l B_l$$

Which of the following is a correct choice for Z_1 ?

Select one:

- ☐ a. $Z_1 = (A_l + A_h)(B_h + B_l) - A_h B_h + A_l B_l$
- ☐ b. Both
- ☒ c. None
- ☐ d. $Z_1 = (A_l - A_h)(B_h - B_l) + A_h B_h + A_l B_l$

The correct answer is: $Z_1 = (A_l - A_h)(B_h - B_l) + A_h B_h + A_l B_l$

Question 4

Complete

Mark 0.00 out of 5.00

Flag question

What is the minimum number of LUTs required to implement the following functions together on an FPGA. Assume that you can enter complement of signals~(say A') as input.

$$F1(A, B, C, D, E, F, G, H, I) = ABCDE + F'GHID'E'$$

$$F2(A, B, C, D, E, F, G, H, I) = ABCEF + F'GHI$$

Assume an LUT has 4 inputs

Answer:

The correct answer is: 4

Question 5

Complete

Mark 2.00 out of 2.00

Flag question

Let us assume that we have to perform an inverse on $GF(2^m)$, with an addition chain of length l using a quad circuit. The number of multiplications required

Select one:

- ☐ a. l
- ☐ b. $l-1$
- ☒ c. $l+1$
- ☐ d. None

The correct answer is: $l+1$

Question 6

Complete

Mark 0.00 out of 2.00

Flag question

The addition chains in Itoh-Tsujii inversion algorithm are used to reduce the number of multiplications required. Let $a \in GF(2^{163})$ and you are asked to find a^{-1} using following addition chain

[1, 2, 4, 5, 10, 20, 40, 80, 81, 162]

The number of squarings required with addition chains is

Select one:

- ☐ a. 162
- ☒ b. 163
- ☐ c. 164

The correct answer is: 162

Question 7

Complete

Mark 2.00 out of 2.00

Flag question

The delay of a squarer and a quad for Itoh-Tsujii Algorithm are the same; because

Select one:

- ☐ a. None of the above
- ☐ b. Quad requires lesser number of operations
- ☒ c. Both have the same delay of 1 LUT
- ☐ d. Quad requires lesser number of steps

The correct answer is: Both have the same delay of 1 LUT

Question 8

Complete

Mark 5.00 out of 5.00

Flag question

We construct the isomorphic mapping between $GF(2^4)$ and $GF(2^2)^2$. The primitive polynomials considered are

For $GF(2^4)$: $R(z) = z^4 + z^3 + 1$

For $GF(2^2)$: $Q(y) = y^2 + y + 1$

For $GF(2^2)^2$: $P(x) = x^2 + x + \{2\}$

Based on the above information answer the following question.

The primitive element γ in $GF(2^4)$ is

Select one:

- ☐ a. 04
- ☐ b. 11
- ☒ c. 02


☐ d. 09

The correct answer is: 02

Question 9

Complete

Mark 5.00 out of 5.00

 Flag question

Consider the following C code snippet used to perform a buffer overflow attack:

```
#include<stdio.h>

void simple_call()
{
    int buf[3];
    int *ret;
    ret = buf + ____(ii)__; //to point to the return address to main function
    *ret = *ret + ____(iii)__;
}

int main()
{
    int flag = 1;
    simple_call();
    flag = 0;
    if(flag == 1)
        printf("Statement skipped. Attack successful");
    else
        printf("Attack unsuccessful");
}
```

Here, ret pointer points to the return address of the simple_call(). The stack contains 3 consecutive locations for buf, followed by one location for ret, one location for the base pointer address of the main function, and one location for the return address to main function. Each location takes 4bytes.

i) If the start address of buf is 0xbffef98, the return address to the main function is _____.

[2 marks]

ii) What should the ret pointer be initialized to?

[1 marks]

iii) In the assembler code dump given below, the instruction in the red box corresponds to the statement (flag = 0). To skip this statement, by what value should ret be incremented?

[2 marks]

```
Dump of assembler code for function main:
0x0804843b <+0>:    push    ebp
0x0804843c <+1>:    mov     ebp,esp
0x0804843e <+3>:    and     esp,0xffffffff
0x08048441 <+6>:    sub     esp,0x20
0x08048444 <+9>:    mov     DWORD PTR [esp+0x1c],0x1
0x0804844c <+17>:   call    0x804841d <simple call>
0x08048451 <+22>:   mov     DWORD PTR [esp+0x1c],0x0
0x08048459 <+30>:   cmp     DWORD PTR [esp+0x1c],0x1
0x0804845e <+35>:   jne     0x804846e <main+51>
0x08048460 <+37>:   mov     DWORD PTR [esp],0x8048510
0x08048467 <+44>:   call    0x80482f0 <puts@plt>
0x0804846c <+49>:   jmp     0x804847a <main+63>
0x0804846e <+51>:   mov     DWORD PTR [esp],0x804852a
0x08048475 <+58>:   call    0x80482f0 <puts@plt>
0x0804847a <+63>:   leave
0x0804847b <+64>:   ret
End of assembler dump.
```

- i) the return address to the main function is 0xbffffac (i.e. increase by 20 bytes)
- ii) ret=buf+5
- iii) *ret = *ret +8

Finish review

QUIZ NAVIGATION

1 2 3 4 5 6 7 8 9

Show one page at a time

Finish review

