

# 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 5 > Class Test 2

**Started on** Thursday, 18 March 2021, 5:00 PM

**State** Finished

**Completed on** Thursday, 18 March 2021, 6:00 PM


**Time taken** 59 mins 56 secs

**Grade** 19.00 out of 25.00 (76%)

### Question 1

Complete

Mark 1.00 out of 1.00

 Flag question

Let  $\gamma$  and  $\alpha$  be the primitive elements in  $GF(2^k)$  and  $GF(2^n)^m$ , where  $k=mn$  and let  $P(X)$ ,  $Q(Y)$ ,  $R(Z)$  be the irreducible polynomials used to construct fields  $GF(2^n)$ ,  $GF(2^n)^m$  and  $GF(2^k)$  respectively. The condition to check the isomorphic mapping is


Select one:

- ☐ a.  $R(\gamma) = 0$  and  $R(\alpha) \equiv 1 \pmod{P(X)Q(Y)}$
- ☐ b.  $R(\alpha) = 0$  and  $R(\gamma) \equiv 0 \pmod{P(X)Q(Y)}$
- ☐ c.  $R(\alpha) = 0$  and  $R(\alpha) \equiv 0 \pmod{P(X)Q(Y)}$
- ☒ d.  $R(\gamma) = 0$  and  $R(\alpha) \equiv 0 \pmod{P(X)Q(Y)}$

### Question 2

Complete

Mark 0.00 out of 1.00

 Flag question

In the MixColumn operation of AES, the modulo operation is performed with the polynomial

Select one:

- ☐  $X^8 + 1$
- ☒ None of the above
- ☐  $X^4 + 1$
- ☐  $X^8 + X^5 + 1$

### Question 3

Complete

Mark 2.00 out of 2.00

Flag question

Let A be the Affine Transformation matrix of AES SBox. Let  $A' = TAT^{-1}$  be the transformation matrix in the composite field, where T is the matrix defining the isomorphic mapping.

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \quad A' = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}$$

The difference in the required number of XOR gates for the hardware implementation of affine transformation using A and A' is

Select one:

- ☒ 20
- ☐ 22
- ☐ 18
- ☐ 32

### Question 4

Complete

Mark 5.00 out of 5.00

Flag question

Bob knows that an AND gate leaks information regarding its inputs. So in order to hide the information about the input he tried to mask them using multiplicative masking, as described below:

Let a and b be the inputs to an AND gate and let  $m_a$  and  $m_b$  be the masks of a and b respectively. Then,

$$a_m = a \cdot m_a$$

$$b_m = b \cdot m_b$$

Let  $y_m = a_m \cdot b_m$  and  $m_y = m_a \cdot m_b$ , then  $y = y_m \cdot m_y^{-1}$

But even after implementing the masked AND gate, Bob figured out that there is a certain amount of leakage about the input values. He tried to quantify by computing the probability of  $a=0$  given that  $y_m = 0$ . Compute this probability:

Answer:

### Question 5

Complete

Mark 5.00 out of 5.00

Flag question

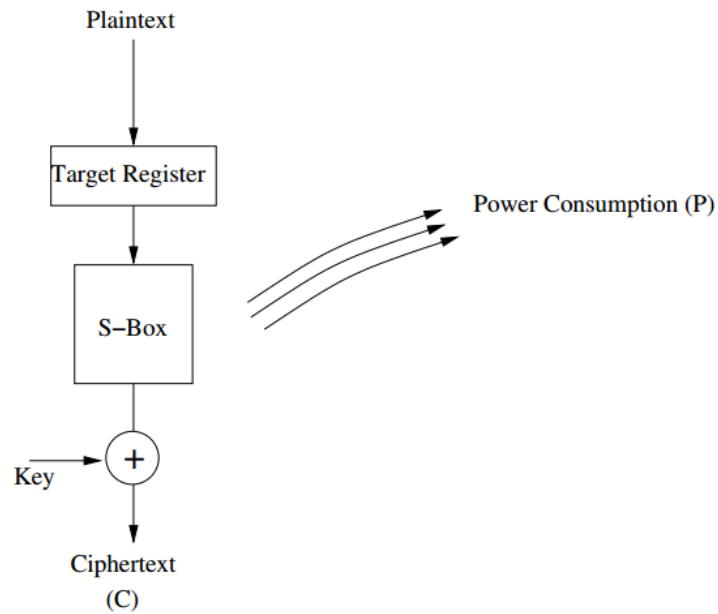
Consider a toy cipher as shown in the below Figure implemented on a smart card. The cipher has a 4-bit plaintext that is not visible to the adversary. However, the adversary has access to the ciphertexts and also the corresponding power consumptions which are represented as integer values. The S-Box of the cipher is as in the following table:

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[X]	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

The adversary runs the encryptions several times until it obtains all the unique 16 ciphertext values (denoted as C) at least once. It also notes the corresponding power values denoted as P which are denoted in the following table:

C	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
P	10	15	20	5	10	5	5	15	15	5	10	10	0	15	10	10

The key is either 0101 or 1010. Apply the Difference-of-Mean (DOM) technique to determine which is the correct key byte. Target the MSB of the input of the S-Box. Correct key byte is 1010.



### Question 6

Complete

Mark 1.00 out of 1.00

Flag question

Suppose an attacker induces a fault in an AES SBOX and the attacker does not have access to the original ciphertext. Then what kind of fault injection is required to obtain the key

Select one:

- ☒ Biased fault
- ☐ Multibit Fault
- ☐ None of the above

**Question 7**

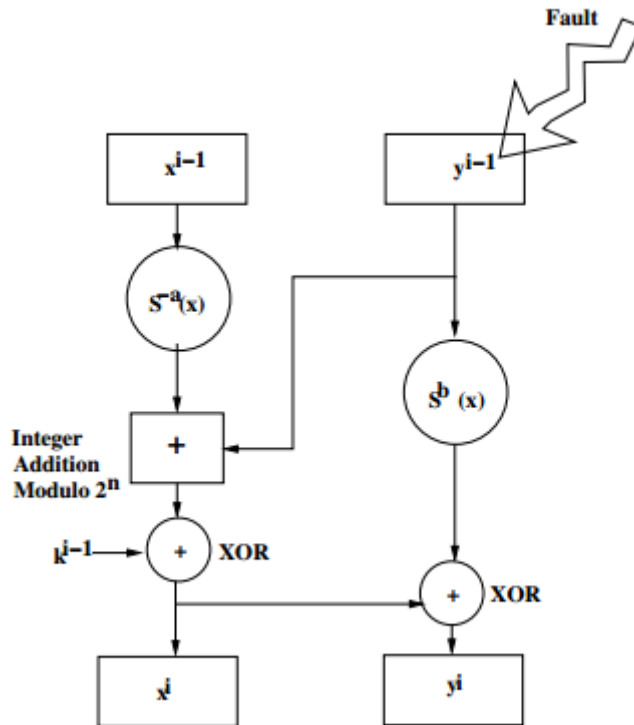
Complete

Mark 0.00 out of 5.00

Flag question

Consider a round of a block cipher as depicted in the figure below, which has overall  $T$  rounds. The rounds are indexed by  $i$ , where  $1 \leq i \leq T$  and each block is of  $2n$  bits, where each half is of  $n$  bits. Each round is denoted as  $R_{k^i}(x_i, y_i) = (x_{i+1}, y_{i+1}) = ((S^{-a}(x^i) + y^i) \oplus k^i, S^b(y^i) \oplus (S^{-a}(x^i) + y^i) \oplus k^i)$ , where  $k^i$  is the round key also of size  $n$  bits. The transformation  $S^{-a}(x)$  indicates a cyclic right shift of the  $n$  bit word  $x$  by  $a$  bits, while the transformation  $S^b(x)$  denotes a cyclic left shift of the  $n$  bit word by  $b$  bits. The  $n$  bit word  $x$  is stored as  $(x_{n-1}, \dots, x_0)$ .

An attacker named Captain Speck has an embedded device that implements the above cipher with the key internal to the hardware. The attacker has access to the input plaintext and the ciphertext, which are denoted as  $(x_1, y_1)$  and  $(x_{T+1}, y_{T+1})$  respectively. He has the ability to inject faults in the registers and he attempts to use it to break the cipher. If the attacker induces a bit fault in the register  $y^T$  when the last round is being operated, which of the following equations helps the attacker ascertain the faulty bit from the ciphertexts ( $x^{j*}$  or  $y^{j*}$  represents the faulty  $n$  bit block at round  $j$ ).




Select one:

- ☐  $S^{-ab}(x^{T+1} \oplus x^{(T+1)*} \oplus y^{T+1} \oplus y^{(T+1)*})$
- ☒  $S^{-a}(x^{T+1} \oplus x^{(T+1)*} \oplus y^{T+1} \oplus y^{(T+1)*})$
- ☐ None
- ☐  $S^{-b}(x^{T+1} \oplus y^{T+1} \oplus y^{(T+1)*})$

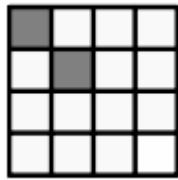
**Question 8**

Complete

Mark 5.00 out of 5.00

 Flag question

Mr. Spillover wants to attack the AES by inducing a single byte fault on the first byte in the 8th round of execution. However, while inducing the fault, he spills it in multiple bytes along the diagonal, as shown in the figure below. He goes to Prof. Pacifier for help. Prof. Pacifier says that he will still be able to extract the key. Explain how the attack will still work briefly. You can write the answer in pen and paper and upload the picture also.

[Finish review](#)**QUIZ NAVIGATION**[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#)[Finish review](#)You are logged in as Srijan Das [Log out](#)