# Indian Institute of Technology Kharagpur

**SPRING Semester, 2023**
**COMPUTER SCIENCE AND ENGINEERING**

**CS60004: Hardware Security**

**Class Test – 2**

**Full Marks: 30**

**1 hour**

1. An SBox transformation of AES is defined as $Y = AX^{-1} + B$ where $A$ and $B$ together define an Affine mapping. In this question, we only consider the optimization of the matrix $A$ in terms of hardware resources. The original matrix A for AES is given below.

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

Let $T$ be the matrix defining the isomorphic mapping from $GF(2^8)$ to $GF((2^4)^2)$. A candidate matrix $T$ and $T^{-1}$ are given below.

$$T = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} \quad T^{-1} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

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

(a) After transformation we get another matrix $A'$ which is to be used in place of $A$ for performing the Affine transformation. Derive relationship between $A$ and $A'$. (5 marks)

(b) Compare the complexity of the circuit in term of number of XOR gates required for constructing the multiplication with $A$ (resp. $A'$). (5 marks)

2. Consider the composite field $GF((2^4)^2)$ with irreducible polynomial $x^2 + x + \alpha^{14}$, where $\alpha$ is the primitive element of $GF(2^4)$. Every element in this field is represented as $a_1x + a_0$, where $a_1$ and $a_0 \in GF(2^4)$. We would like to transform all the elements of $GF(2^8)$ to $GF((2^4)^2)$ using the transformation matrix given in Q1. It can be easily observed that any element $\beta$ in $GF(2^8)$ can be transformed into $GF((2^4)^2)$ as $T(\beta)$. For example, $\{2\} \in GF(2^8)$ can be denoted as 0000 0010. Thus, $T(2) \in GF((2^4)^2)$ can be denoted as 0010 1110 $= ax + \alpha^{11}$, where $\alpha$ is the primitive element of $GF(2^4)$, modulo $x^4 + x + 1$. During the computation of the MixColumns matrix of AES in the composite field of $GF((2^4)^2)$ the transformation can be given by

   (a) $T(3)(a_1x + a_0) = T(2)(a_1x + a_0) + (a_1x + a_0)$

   (b) $T(3)(a_1x + a_0) = T(1)(a_1x + a_0) + (a_1x + a_0)$

   (c) $T(3)(a_1x + a_0) = T(2)(a_0x + a_1) + (a_1x + a_0)$

   (d) None of the above

(5 marks)

3. Consider the following 4-input Boolean function: $f(x_1, x_2, x_3, x_4) = (x_1x_2) + (x_3x_4)$. What is the number of XOR gates in the gate-level masked implementation of this Boolean function? (5 marks)

4. Mr. Spillover wants to attack the AES by inducing a single byte fault on the first byte in the $8^{th}$ round of execution. However, while inducing the fault, he spills it in multiple bytes along the diagonal, as shown in Fig. 1. 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.

Figure 1: Input to the $8^{th}$ round of AES, gray boxes denote the faulty bytes

(10 marks)