Indian Institute of Technology (IIT-Kharagpur)

SPRING Semester, 2018
COMPUTER SCIENCE AND ENGINEERING

CS60004: Hardware Security

Mid-Term Examination

Full Marks: 40

Time allowed: 2 hours

INSTRUCTIONS: Attempt all Questions.

1. (a) Consider the following 4-input boolean function:

$$f(x_1, x_2, x_3, x_4) = (x_1 \cdot x_2) + (x_3 \cdot x_4)$$

Describe a gate-level masked implementation of this boolean function. (7 marks)

2. Consider a substitution-permutation network with a 64-bit state and a 64-bit round key described in Figure 1, where **S** is a non-linear 4×4 S-Box. Observe that the S-Box layer is followed by a bit-permutation layer and a bit-wise round-key XOR layer. Note that a *nibble* is a collection of 4 consecutive bits (a 4-bit equivalent of a byte). Also, assume that the expected number of solutions to the equation:

$$\mathbf{S}^{-1}(x) \oplus \mathbf{S}^{-1}(x \oplus A) = B$$

for known A and B and unknown x is 1.

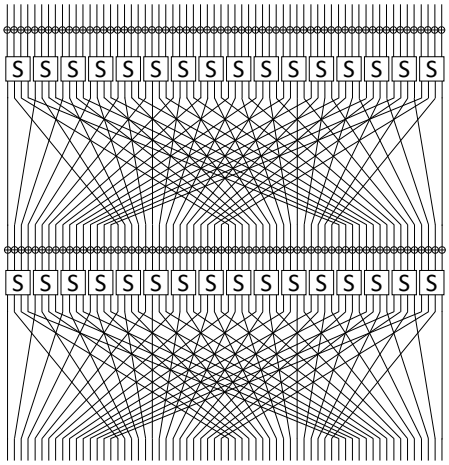

Figure 1: To rounds of a substitution-permutation network

(a) Suppose an attacker introduces a *fixed* single-nibble fault of Hamming Weight x at the input of round r in an iterated implementation of this SPN structure. Prove that the faulty input value for any nibble in round $(r + 2)$ takes at most 2^x values. (7 marks)

(b) Now consider a practical fault attack in which an adversary can actually inject a specific (and known) single-nibble fault of Hamming Weight x at the input of round r in an iterated implementation of this SPN structure Weight x. Describe a fault attack methodology to recover the $(r + 2)^{\text{th}}$ round-key from the correct and faulty outputs of the $(r + 2)^{\text{th}}$ round of this SPN structure. (6 marks)

(c) Remark on the possible values of x for which the fault attack is practically feasible, and the expected number of fault injections required for each such x for complete key-recovery (2 marks)