Indian Institute of Technology Kharagpur

SPRING Semester, 2015
COMPUTER SCIENCE AND ENGINEERING

CS60004: Hardware Security

End–semester Examination

Full Marks: 60

Time allowed: 3 hours

INSTRUCTIONS: Special credit would be given for answers which are short and to–the–point.
Illegible handwriting would be penalized.
Answer QUESTION-1 and ANY THREE FROM THE REST.

1. (a) State the first-order necessary conditions that must hold for the solution(s) of a general (with both equality and inequality constraints) constrained optimization problem. (3 marks)

(b) Find the stationary point and the associated *Lagrange Multipliers* for the following constrained optimization problem: (6 marks)

$$\begin{aligned} \text{min.} \quad & f(\mathbf{x}) = 2x_1^2 - 2x_1x_2 + x_2^2 + 3x_3^2 + 2x_2x_3 - 2x_1 + x_2 - 3x_3 \\ \text{subject to:} \quad & x_1 + 2x_2 - x_3 = 1 \\ & -x_2 + x_3 = 2 \end{aligned}$$

(c) Assume that the function $f(\mathbf{x})$ is known to be *strictly convex* over $\mathbb{R}^3$. What is your conclusion about the nature of the solution you have obtained in part-(b)? (2 marks)

(d) Explain why an AND gate leaks wrt. power analysis. Also explain briefly the masking circuit for an AND gate to prevent this leakage. (4 marks)

2. (a) Give the geometrical interpretation of the (hard margin) *Support Vector Machine* (SVM) problem (assuming normalized distances), and derive the simplified optimization problem that is amenable to numerical solution. (8 marks)

(b) The numerical values of the *Lagrange Multipliers* for a SVM problem were found to be {0.2, 0.3, 0.0, 0.0, 0.1, 0.2}. Find the (normalized) separation between the decision hyperplanes. Derive the formula you use. (5 marks)

(c) Explain the concept of *Soft Margin SVM*, mentioning the modified optimization problem formulation. (2 marks)

3. (a) Consider the last 2-rounds of a Fiestel Cipher as depicted in Fig 1. The rounds are indexed by $T-2, T-1, T$. Each round is denoted as $R_{k^i}(x_i, y_i) = (x_{i+1}, y_{i+1}) = (y^i \oplus f(x_i) \oplus k^i, x^i)$. Assume a random fault e which occurs in the register x^{T-2}. Prove that the attacker can determine the fault from the correct and faulty ciphertexts, denoted as (x^T, y^T) and $((x^T)^*, (y^T)^*)$. (7 marks)

(b) Assume for performing a power attack, an adversary has access to the power leakage which at a time t can be obtained by the relation $L_t = a_t(P_{k^*} + c) + N_t$, where N_t is an independent noise signal with a multivariate Gaussian distribution with zero mean. Also the variance of the signal is significantly lesser compared to the variance of the noise. Further $a_t \in \mathcal{R}$ is a time dependent variable which is constant at every time instance. The random variable P_{k^*} is the deterministic leakage for the correct key k^*, and c is a constant. Answer the following questions in this regard:

(i) Define the Signal-to-Noise Ratio (SNR), $\alpha(t)$ of the traces wrt. power analysis. (2 marks)

(ii) Prove that $a_t = \frac{E(L_t)}{E(P_{k^*})+c}$. (2 marks)

(iii) Prove that the SNR, $\alpha(t) \approx \frac{\mu_L^2(t)}{\sigma_L^2(t)} \frac{Var(P_{k^*})}{(E[P_{k^*}]+c)^2}$, where $\mu_L = E[L_t]$ and $\sigma_L^2 = Var(L_t)$. (4 marks)

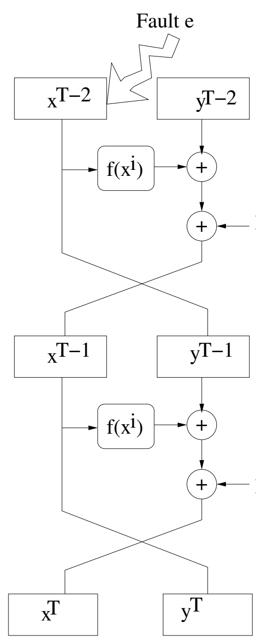

Figure 1: The last two rounds of a Fiestel Cipher

4. (a) Define **uniqueness**, **uniformity** and **reliability** metrics for a PUF with suitable mathematical expressions. Which of these parameters might be improved by addition of extra circuitry? (5 marks)

(b) Suppose the truth tables of three instances of an 4-bit *Arbiter PUF* circuit were found to be identical to those of AND4, NOR4 and XOR4 respectively. Calculate the *uniformity* and *uniqueness* metrics. (8 marks)

(c) Comment on the acceptability of the above PUF, by comparing the obtained metric values with the ideal values. (2 marks)

5. (a) Show that for an n-bit APUF circuit, determining the response for an arbitrary challenge is the same as solving a linear separation problem in n-dimensional space. (8 marks)

(b) Suppose the $\{p, q, r, s\}$ delay values (in arbitrary units) for the stages of an 4-bit APUF are: $\{\{22, 23, 17, 20\}, \{15, 14, 13, 9\}, \{20, 21, 22, 25\}, \{10, 12, 13, 16\}\}$. Determine the direction of a vector normal to the separating hyperplane for this APUF. Symbols have their usual meaning. (5 marks)

(c) What are the advantages and the disadvantages of the *Genetic Programming* based model building methodology? (2 marks)

6. (a) Consider a fault tolerant design of MixColumn of AES using byte-level parity bits, where the irreducible polynomial is $m(x) = x^8 + x^4 + x^3 + x + 1$. The MixColumn is defined as:

$$M = \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix}$$

The input column is denoted by the vector: $(s_{0,j}, s_{1,j}, s_{2,j}, s_{3,j})^T$. Also $p_{i,j}$ is the parity bit associated for the byte $s_{i,j}$ and $s_{i,j}^{(7)}$ is the most significant bit of $s_{i,j}$. Prove that the parity bits are transformed as follows:

$$\begin{aligned}
p_{0,j} &= p_{0,j} \oplus p_{2,j} \oplus p_{3,j} \oplus s_{0,j}^{(7)} \oplus s_{1,j}^{(7)} \\
p_{1,j} &= p_{0,j} \oplus p_{1,j} \oplus p_{3,j} \oplus s_{1,j}^{(7)} \oplus s_{2,j}^{(7)} \\
p_{2,j} &= p_{0,j} \oplus p_{1,j} \oplus p_{2,j} \oplus s_{2,j}^{(7)} \oplus s_{3,j}^{(7)} \\
p_{3,j} &= p_{1,j} \oplus p_{2,j} \oplus p_{3,j} \oplus s_{3,j}^{(7)} \oplus s_{0,j}^{(7)}
\end{aligned}$$

(8 marks)

(b) Prof Faulty is interested to publish a paper on fault analysis of AES. He has the idea of inducing a random byte fault at the input of the last round of AES. Explain whether he can launch a successful attack. If yes, prove that the attack works. If not, suggest a suitable alteration of the fault model and explain how it works. (7 marks)