Indian Institute of Technology Kharagpur

SPRING Semester, 2016
COMPUTER SCIENCE AND ENGINEERING

CS60004: Hardware Security

Assignment–1

Full Marks: 20

Time allowed: N/A hours

INSTRUCTIONS: Do this assignment in two member teams, one submission per team would be evaluated. Your final submission should consist of all code, preferably in `Matlab`, detailed documentation on how to run the code (in the form of a README file or a PDF user manual), and a detailed report in PDF format. The report should contain plot/tables to summarize your findings. No credit will be given until you satisfactorily explain your findings during a live demo to the teacher or the TA. No need to e-mail your submissions, bring it with you during the demo to submit it. Date of demo is tentatively 15th March 2016.

1. For the *Arbiter PUF* (APUF) experimental dataset uploaded on *Moodle*, perform the *Support Vector Machine* (SVM) based modelling attack. Note that (a) the data represents ten 64-bit APUF instances; (b) the format is `.mat` readable by `Matlab`, and, (c) the challenges and responses are in binary (0/1). Take 70% of the total *Challenge-Response Pair* (CRP) dataset for training purposes for each APUF instance, and test the accuracy of your model for the remaining 30% of the CRP dataset. You should submit your complete code, and report the modelling accuracy obtained for each of the 10 instances. (5 marks)

2. Repeat the modelling exercise of Question-(1) for the simulated dataset provided, and comment on the relative levels of modelling accuracy obtained between the experimental and simulated datasets in your report. (3 marks)

3. Select the CRP dataset for the first seven experimental APUF instances, and construct the CRP dataset for a *Lightweight Secure PUF* (LSPUF) for parameters $k = 7$, $m = 6$, $x = 6$ and $s = 0$, assuming no input permutation network. Now, launch the cryptanalytic attack on LSPUF as taught in class, and report the levels of accuracy obtained. Make any reasonable assumption that you might wish to make, and state it clearly in your report. (6 marks)

4. Simulate a 64–bit *Enhanced ROPUF* with parameter $e = 0.5$, by generating oscillation frequencies for 64 ring oscillators within a reasonable range, using a random number generator (preferably one that generates random numbers following a certain statistical distribution, e.g. the `normrnd()` library function of `Matlab`). Now, launch the cryptanalytic attack taught in class for different Hamming Weights (HW = 3, 4, 5 and 6) of the challenge bitstring, **assuming helper data is not available**, and report whether and to what extent your cryptanalytic probability of success matches the theoretically predicted success probability. Make any reasonable assumption that you might wish to make, and state it clearly in your report. (6 marks)