Discipline of CSE, Indian Institute of Technology Indore.

Term Project, Spring Semester 2019-2020.
Cryptography and Network Security (CS 417/617)
Instructor: Dr. Bodhisatwa Mazumdar

Date: 27/05/2020 **Submission Deadline: 10/06/2020, 5 pm**

Instructions:

1. Form a group of three or four students for this term project submission.
2. Submission must be in a zip file with name, Roll1_Roll2_Roll3_Roll4.zip, to *bodhisatwa@iiti.ac.in*.
3. The submission must comprise a soft copy of the term project report, the codes, the set of inputs and outputs.
4. The report should elaborately describe the steps that you carried out for the experiments.
5. Marks obtained from this term project will solely depend upon the clarity of the report and the codes (the way they are commented).

1. *Persistent fault analysis* (PFA) on an encryption system recovers the secret key of the system by mounting fault while the encryption algorithm is running and then perform a statistical analysis to exploit such faults. The fault persists in the algorithm over multiple encryptions or queries, whereas it disappears when the device reboots. An instance of persistent fault can be given as toggling of an S-box lookup table entry in an SPN block cipher implementation. The toggle in teh S-box lookup table implementation can be reversed when the device is powered up again.

   Consider the persistent fault analysis on block ciphers in [1]. The project involves mounting a key recovery attack on a C/C++ implementation of DES cipher. In the report submission, the following points are to be discussed in detail:

   (i) Implement a functionally correct version of DES block cipher in C/C++. The code must be provided in the report.

   (ii) Mount PFA on each 6×4 S-box of the cipher. The strategy mentioned in Section 3.3 of [1] can be referred to. The attack algorithm or strategy must be mentioned in the report.

   (iii) Report the residual key entry with the respect to the number of ciphertexts or queries for each attack. Is the attack performance invariant of the S-box mapping? A thorough analysis of the attack must be mentioned in the report

   (iv) Report the complexity analysis of the attack.

References

[1] Fan Zhang, Xiaoxuan Lou, Xinjie Zhao, Shivam Bhasin, Wei He, Ruyi Ding, Samiya Qureshi, and Kui Ren. Persistent fault analysis on block ciphers. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pages 150–172, 2018.