LAB REPORT- SMART CARD

Author : Kumar, Chander
Matriculation No. : 03709108
Group : 03

First part: Smartcard Cloning & AES Decryption Implementation

Date: 06/05/2019
Task 1: Literature Review
It was decided that all group members will go through the script and reference material and get a detailed idea about what is required in the lab and how will it be carried out.

Date: 08/05/2019
Task 2: Team Selection and Work Distribution
Team was divided into two groups and decision about which group will carry out which task was made. I was assigned task to implement AES-128 Decryption.

Date : 11/05/2019
Task 3: Literature Understating : FIPS-197 AES Document.
I spent time in reading the FIPS-197 Document thoroughly. And tried to implement basic functional blocks like Add RoundKey, InverseShiftRows etc.

Date : 20/05/2019
Task 4: Key Expansion Module,Verifcation with NIST tables and Integration of Original Key :
Implemented Key expansion module and integrated with all other functions of AES Decryption. Algorithm was verified step by step along with the NIST Test vectors given in the FIPS-197 Document. Also Integrated Key provided by DPA team and verified results online.

Date : 29/05/2019
Task 5: Optimizing of InvMixColoumns function and precomputaion of few modules :
As Key expansion was taking so much time so precomputed the Key Expansion and stored in Array. Inverse Mix Coloumn function was taking too much time because of GF multiplication so, replaced normal function with xtime based implementation.

Also tried to implement the GF multiplication with Log and Antilog tables but it was taking more time than xtime based implementaion

Date : 04/06/2019
Task 6: Preparation of slides for the presentation
Prepared slides and also re-read the FIPS-197 document to prepare myself for the presentation.

Second part: DPA Countermeasures and Benchmarks

Date : 08/06/2019
Task 1: Discussion for different DPA Countermeasures and RNG
Done some literature review regarding the implementation of Shuffling, Masking etc. Explored different options available for TRNG and PRNG. And divided team work.

Date : 13/06/2019
Task 2: Research for Countermeasures and implementation of Shuffling:
Studied how countermeasures can be implemented espacially different possibilities for shuffling and chose Fischer-Yates shuffling. Implemented for now with rand() as RNG.

Date : 18/06/2019

Task 3: Implementation Dummy operations:

Implemented Dummy operations using srand() and rand() for just 100 dummy operations same as InverseSubBytes.

Date : 21/06/2019

Task 4: Implementation of Masking and verfication of all countermeasures :

Studied about implementation of masking and chose boolen masking. Implemented masking. And verified all three countermeasures separately and in combination. And provided sample traces to DPA team so that they can improve their and check their script.

Date : 28/06/2019

Task 5: Implementaion of all countermeasures with own PRNG :

Integated own PRNG in countermeasures implementation. And verified output for each countermeasurs by playing video.

Date : 02/07/2019

Task 6: Optimization, Benchmarking and providing different traces to DPA team :

Done optimization in code reagrding the execution time and code size e.g. same no. of dummy operation for each AES decryption and different Input and Out masks for InvSubBytes array. checked implementaion with different numbers of dummy operations. Done bechmarking for all countermeasures separately and in combination. Provided all the required traces to DPA team.

Date : 09/07/2019

Task 7: Preparation of slides for the presentation

Prepared slides and also revised the DPA countermeasure concepts to prepare myself for the presentation.