Final Assignments on Course on Advanced Side Channel Analysis
February 2019

1. We have studied TVLA in the class. It is used to detect the presence of side channel leakage in a cryptographic algorithm. In this assignment we will analyse different ways of computing TVLA. To compute specific TVLA follow the following steps:
Compute the switching activity during the ninth round by xoring the 9th round first byte and 10th round first byte. Partition the side channel traces into two bins depending upon the MSB of the switching activity during the ninth round. Compute the mean and variance of each bin and apply the TVLA formula to compute specific TVLA.

(a) Compute specific TVLA using the given set of side channel traces (_DATA1_keyset_attack_9.csv)

(b) Compute specific TVLA using the new side channel traces that is uploaded in the web portal. Note the difference between the TVLA values. In the new set of traces, we have introduced some random jitters in the traces to misalign the traces. This is the reason behind the change in TVLA values between case i and case ii.

(c) Perform correlation power attack (CPA) on new set of side channel traces. Observe the difference in the result compared to the scenario when you apply CPA on the aligned traces. [40 points]

2. Consider a round of a block cipher as depicted in Fig. 1 which has overall $T$ rounds. The rounds are indexed by $i$, where $1 \leq i \leq T$ and each block is of $2n$ bits, where each half is of $n$ bits. Each round is denoted as $R_k, (x_i, y_i) = (x_{i+1}, y_{i+1}) = ((S^{-a}(x^i) + y^i) \oplus k^i, S^b(y^i) \oplus (S^{-a}(x^i) + y^i) \oplus k^i)$, where $k^i$ is the round key also of size $n$ bits. The transformation $S^{-a}(x)$ indicates a cyclic right shift of the $n$ bit word $x$ by $a$ bits, while the transformation $S^b(x)$ denotes a cyclic left shift of the $n$ bit word by $b$ bits. The $n$ bit word $x$ is stored as $(x_{n-1}, \ldots, x_0)$.

An attacker named Captain Speck has an embedded device which implements the above cipher with the key internal to the hardware. The attacker has access to the input plaintext and the ciphertext, which are
denoted as \((x_1, y_1)\) and \((x_{T+1}, y_{T+1})\) respectively. He has the ability to inject bit faults in the registers and he attempts to use it to break the cipher. Help him to do so by answering the following questions:

(a) If the attacker induces a bit fault in the register \(y^T\) when the last round is being operated, show that the attacker can also ascertain which bit is faulted from the ciphertexts.

(b) For the last round of the cipher prove the equation:

\[
k^T_j = x^T_{(j+a) \mod n} \oplus (y^{T+1} \oplus x^{T+1})_{(j+b) \mod n} \oplus c_j \oplus x^{T+1}_j
\]

Here, for an \(n\)-bit word \(x^T\), \(x^T_j\) denotes the \(j\)-th bit of the word and \(c_j\) is the \(j\)-th bit of the carry generated \(i.e.\) the carry input to the \(j\)-th bit position.

(c) Assume that the fault is induced in the 0\(^{th}\) bit of the register \(y^T\), \(i.e.\) \(y^T_0\) when the last round is operated by the hardware. Show how can the attacker retrieve the 0-th key bit of the last round, \(i.e.\) \(k^T_0\).

\[\text{HINT for part (c): Prove first that } (x^{T+1} \oplus x^{(T+1)^*})_0 = 1, \text{ where } x^{(T+1)^*} \text{ corresponds to left part of the faulty ciphertext. Then use the Hamming Weight of } (x^{T+1} \oplus x^{(T+1)^*})\]

3. Consider an exponentiation algorithm \(y = x^b\), where \(b\) is a secret exponent which is of 8 bits. The exponents are denoted as \(b_7, \ldots, b_0\). The exponent can be considered to be made of 2 nibbles (4-bits). An attacker is able to inject random faults in either of the two nibbles (when one nibble is affected the other is error free). Note that since the fault is random, some of the bits inside the faulty nibble may be unaffected too! The attacker obtains the results of \(y = x^b\) and \(y = x^{b'}\), \(i.e.\) \(b'\) is the faulty exponent
under the above fault model. Develop an algorithm for the attacker to obtain the exponent bits. Also calculate the expected number of remaining exponents for one fault induction and two fault inductions. \[20 \text{ points}\]

Remember if $X$ is a random variable, expectation of $X$ is computed as $E(X) = \sum_i (x_i p_i)$, where $x_i$ is a possible value of the random variable $X$, and which occurs with probability $p_i$. The sample points are denoted by $i$.

**Bonus Assignment [20 points]**

1. In this experiment, our objective will be to perform deep learning based methodologies to retrieve the secret key for both aligned and misaligned traces that has been uploaded in the web portal. You are advised to go through the following paper for this exercise: “Non-Profiled Deep Learning-Based Side-Channel Attacks” (https://eprint.iacr.org/2018/196.pdf). This paper describes the methodology of deep learning to perform side channel attack on aligned traces. Our job is to implement this attack and modify it accordingly for its application on misaligned traces.

2. Another methodology to perform side channel attack on misaligned traces is to convert the multivariate traces into univariate one using linear discriminant analysis (LDA) method. In this experiment, we will first use LDA to convert both set of multivariate side channel traces into univariate trace and perform CPA on them. In your submission, add a comparison document to illustrate differences in all of these attacks.