Assignment 2 SPM 2022 Report

Prasanna Bartakke EE19B106

September 6, 2022

Round key	Value(4 bytes)
RK_0	[0x40, 0xdc, 0x56, 0xd3]
RK_1	[0x2a, 0x15, 0xb0, 0x57]
RK_{34}	[0x6c, 0x89, 0xf8, 0x4]
RK_{35}	[0x5, 0xa5, 0xad, 0x5c]
$RK_2 \oplus WK_0$	[0x50, 0x94, 0x2f, 0xa0]
$RK_3 \oplus WK_1$	[0xf9, 0xff, 0x6c, 0x21]

Explanation

The r-round encryption function can be described as follows:

$$C_0^0|C_1^0|C_2^0|C_3^0 = P_0|P_1 \oplus WK_0|P_2|P_3 \oplus WK_1$$

$$\forall i \in 0 < i \leq r$$

$$C_0^i = C_1^{i-1} \oplus F_0(C_0^{i-1}, RK_{2i-2})$$

$$C_1^i = C_2^{i-1}$$

$$C_2^i = C_3^{i-1} \oplus F_1(C_2^{i-1}, RK_{2i-1})$$

$$C_3^i = C_0^{i-1}$$

and,

$$C_0|C_1|C_2|C_3 = C_3^r|C_0^r \oplus WK_2|C_1^r|C_2^r \oplus WK_3$$

where $P_0|P_1|P_2|P_3$is the plaintext, $C_0|C_1|C_2|C_3$ is the ciphertext, $RK_{2i-2}, RK_{2i-1}$are the rounds keys and $WK_0|WK_1|WK_2|WK_3$ is the whitening key. The function F_0 takes in two 4 byte inputs, X and RK, returns Y, and is defined as follows:

$$X_0|X_1|X_2|X_3 = X_0 \oplus RK_0|X_1 \oplus RK_1|X_2 \oplus RK_2|X_3 \oplus RK_3$$

$$Y_0|Y_1|Y_2|Y_3 = T_{00}[X_0] \oplus T_{01}[X_1] \oplus T_{02}[X_2] \oplus T_{03}[X_3]$$

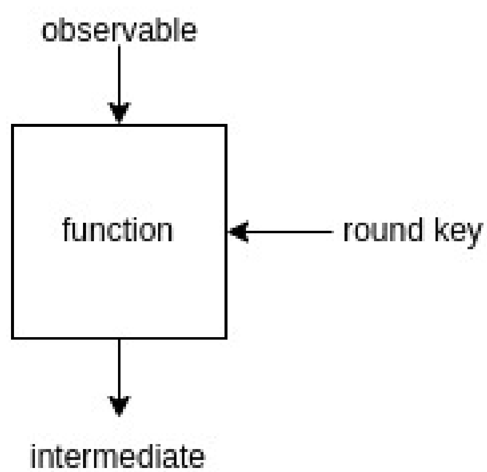
The function $F_1$is similar to F_0, and is defined as follows:

$$X_0|X_1|X_2|X_3 = X_0 \oplus RK_0|X_1 \oplus RK_1|X_2 \oplus RK_2|X_3 \oplus RK_3$$

$$Y_0|Y_1|Y_2|Y_3 = T_{10}[X_0] \oplus T_{11}[X_1] \oplus T_{12}[X_2] \oplus T_{13}[X_3]$$

Power Attacks

To implement a power attack, we first need to perform N encryption operations using N random plaintexts $P(n), n \in \{1, ..., N\}$ with the same key. We capture the corresponding power trace $Tr(P(n))$, having 18000 samples, and the ciphertext $C(n)$. Let RK_i be the round key to be attacked. RK_i can be split in 4 bytes, denoted by $RK_{i,b}, 0 \leq b < 4$. We guess the round key one byte at a time by varying it from 0 to 255. Each round can be represented as follows:



In the first round, the observable is $C_0^0 = P_0$, and the round key used is RK_0. The intermediate value is $F_0(C_0^0, RK_0)$. Similarly, for RK_1 used in the first round, the observable is $C_2^0 = P_2$, and the intermediate value is $F_1(C_2^0, RK_1)$.

In both DOM and CPA methods the Hamming weight model is used. Let $HW(x)$ denote the hamming weight of x.

DOM

The select function of DOM is defined as follows:

$$D(P(n), b, RK_{i,b}) = 0, HW(intermediate) < 16$$

else,

$$D(P(n), b, RK_{i,b}) = 1, HW(intermediate) > 16$$

Depedending on the value of D, the power traces are classified in two sets,

$$T_0 = \{Tr(P(n))|D(P(n), b, RK_{i,b}) = 0\}$$

and

$$T_1 = \{Tr(P(n))|D(P(n), b, RK_{i,b}) = 1\}$$

Then, the difference of means of both the sets are calculated. There is an obvious peak in the difference if the value of the key guess is correct. The code for this approach is present in the file ee19b106_dom.ipynb.

CPA

In correlation power analysis, the correct part of the power trace is corrleated with the hamming weight of the intermediate value. The key guess resulting in the maximum correlation is selected as the correct key value. The code for this approach is present in the file ee19b106_cpa.ipynb.

In case of RK_{34} and RK_{35} we go in the reverse order. The observables are $C_0 = C_3^r$ and $C_2 = C_1^r$. The intermediate values are $F_0(C_3^r, RK_{34})$ and $F_1(C_1^r, RK_{35})$ used in the calculation of C_0^r and C_2^r respectively.

In the second round, the intermediate values are $F_0(C_0^1, RK_2)$ and $F_1(C_2^1, RK_3)$. They can be simplified as follows:

$$F_0(C_0^1, RK_2) = F_0(C_1^0 \oplus F_0(C_0^0, RK_0), RK_2)$$

$$= F_0(P_1 \oplus WK_0 \oplus F_0(C_0^0, RK_0), RK_2)$$

$$= F_0(P_1 \oplus F_0(C_0^0, RK_0), RK_2 \oplus WK_0)$$

Here, the observable is $P_1 \oplus F_0(C_0^0, RK_0)$, as we know the correct value of RK_0 now. The key which we will guess is $RK_2 \oplus WK_0$ and using the DOM and CPA methods, the correct value of $RK_2 \oplus WK_0$ is calculated. Similarly,

$$F_1(C_2^1, RK_3) = F_1(P_3 \oplus F_1(C_2^0, RK_1), RK_3 \oplus WK_1)$$

and we get the value of $RK_3 \oplus WK_1$.

The higher the number of traces used, the higher is the difference of means in DOM and correlation in CPA. For CPA, all the traces were used as the difference in correlation was not significant for fewer number of traces. In DOM, there is a clear distinction between the correct key and remaining keys after around 500 traces. As it takes a long time to run the key guess, the following analysis has been done only for RK0. Other keys should follow a similar pattern.

Number of traces used = 100

	0	1	2	3
0	BF 0.020	DC 0.030	14 0.022	94 0.023
1	D3 0.020	D7 0.023	81 0.019	E7 0.021
2	A6 0.020	F4 0.020	48 0.019	B8 0.021
3	52 0.019	D9 0.020	A1 0.019	BF 0.020
4	87 0.019	88 0.020	DE 0.019	58 0.020

Number of traces used = 200

	0	1	2	3
0	40 0.017	DC 0.028	81 0.016	C1 0.015
1	1C 0.015	32 0.016	25 0.015	D3 0.015
2	A6 0.014	76 0.015	1A 0.014	41 0.014
3	5A 0.013	E2 0.015	67 0.014	4F 0.014
4	25 0.013	C7 0.014	3A 0.014	E9 0.014

Number of traces used = 300

	0	1	2	3
0	40 0.017	DC 0.026	56 0.015	D3 0.016
1	5A 0.013	EC 0.013	81 0.014	AF 0.012
2	1C 0.012	76 0.012	25 0.013	13 0.012
3	CB 0.012	6A 0.011	8A 0.013	C1 0.012
4	A6 0.012	25 0.011	2B 0.012	DA 0.012

Number of traces used = 400

	0	1	2	3
0	40 0.017	DC 0.028	56 0.015	D3 0.015
1	41 0.011	76 0.010	81 0.012	DA 0.011
2	7B 0.011	9D 0.010	16 0.011	3A 0.010
3	9D 0.010	D5 0.010	C7 0.010	64 0.010
4	9C 0.010	BB 0.010	3C 0.010	5E 0.010

Number of traces used = 500

	0	1	2	3
0	40 0.018	DC 0.028	56 0.014	D3 0.015
1	7B 0.012	9D 0.011	81 0.011	0B 0.010
2	3C 0.010	FC 0.010	67 0.010	FF 0.010
3	41 0.009	D5 0.010	70 0.010	58 0.010
4	8E 0.009	60 0.009	E1 0.009	94 0.009

Number of traces used = 1000

	0	1	2	3
0	40 0.016	DC 0.030	56 0.014	D3 0.014
1	E1 0.008	9D 0.012	2F 0.008	45 0.009
2	7B 0.007	D5 0.011	89 0.007	CA 0.009
3	1B 0.007	E5 0.010	C3 0.007	C4 0.009
4	C2 0.006	FC 0.010	4A 0.007	02 0.008

Number of traces used = 2000

	0	1	2	3
0	40 0.015	DC 0.030	56 0.014	D3 0.014
1	E1 0.006	A3 0.010	55 0.006	CA 0.011
2	71 0.006	D5 0.009	81 0.006	45 0.009
3	43 0.006	98 0.009	3E 0.006	02 0.009
4	28 0.006	FC 0.009	BC 0.005	41 0.009

Number of traces used = 5000

	0	1	2	3
0	40 0.015	DC 0.029	56 0.014	D3 0.015
1	71 0.006	0D 0.009	55 0.007	CA 0.011
2	1C 0.005	D5 0.009	81 0.006	45 0.009
3	C2 0.005	A3 0.009	4A 0.006	2A 0.009
4	5A 0.005	D0 0.008	1D 0.005	02 0.009

Number of traces used = 12000

	0	1	2	3
0	40 0.015	DC 0.030	56 0.014	D3 0.015
1	71 0.005	0D 0.009	55 0.007	CA 0.010
2	C2 0.005	D0 0.009	81 0.006	02 0.009
3	1C 0.005	A3 0.009	4A 0.006	45 0.008
4	43 0.005	BA 0.009	2D 0.006	41 0.008

The above tables show the DOM values for different key guesses. We can get the correct key guess with high confidence from around 300-400 number of power traces.