Differential Power Analysis attack of CLEFIA Block cipher

V Ram Chandra Prasad

CS13M1019

A Thesis stage-2 Submitted to

Indian Institute of Technology Hyderabad

In Partial Fulfillment of the Requirements for

The Degree of Master of Technology

Under the guidance of Dr.M.V. Panduranga Rao & Dr. Vishal Saraswat

भारतीय प्रौद्योगिकी संस्थान हैदराबाद

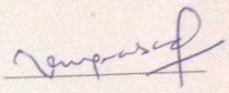
Indian Institute of Technology Hyderabad

Department of Computer Science Engineering

June, 2015

Declaration

I declare that this written submission represents my ideas in my own words, and where ideas or words of others have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the Institute and can also evoke penal action from the sources that have thus not been properly cited, or from whom proper permission has not been taken when needed.



(Signature)

(V.Ram Chandra Prasad)

CS13M1019

(Roll No.)

Approval Sheet

This thesis entitled Differential Power Analysis attack of CLEFIA Block cipher by V RAM CHANDRA PRASAD is approved for the degree of Master of Technology from IIT, Hyderabad.

_____

Examiner

_____

Examiner

_____

Dr M V Panduranga Rao
Adviser

_____

Dr Vishal Saraswat
Co-Adviser

_____

Chairman

Acknowledgements

I express my deep sense of gratitude to all who helped me during this thesis work. First, I would like to thank my supervisors, Dr. M V Panduranga Rao and Dr. Vishal Saraswat, for being a great mentor and advisers. Their advice, encouragement and critics are source of inspiration and causes behind the successful completion of this dissertation. The confidence shown on me by them, was the biggest source of inspiration for me. I thank to Dr. Allam Appa Rao, Director, Dr. Rajiv Anand Sahu, Assistant Professor, and researchers at CRRao AIMSCS, Hyderabad who helped me, guided me at the time I needed the most. I wish to express my sincere gratitude to R.Adm Ranjit Singh, DLRL for providing me all the facilities required for the completion of this thesis work.

Abstract

The objective of this research work is to mount Side channel attack particularly power analysis attack on FPGA Hardware implementation of CLEFIA block cipher. CLEFIA is claimed to be reliable cipher. CLEFIA specifications and design of algorithm is available to evaluation by public, cryptographers for performance and security analysis. CLEFIA is an international standardized cipher in ISO/IEC lightweight cryptography. It has four branch generalized Feistel network structure. This structure can be implemented compactly in both in hardware and software. CLEFIA consists of Diffusion Switching Mechanism, which ensures immunity against major attacks. Moreover, the similarity of functions between the data processing part and the key scheduling part of CLEFIA reduces the gate size.

Side channel attack mainly Differential Power Analysis attack(DPA) of CLEFIA is one of the major challenge for crypto groups as data and key generation functions share same structure Thus complicates the power attack specially in FPGA hardware implementation. Differential Fault Analysis (DFA) is also possible when fault is introduced into hardware. We are proposing a DPA on CLEFIA with 128 bit key on FPGA based hardware with selection function to analyze and extract the key bits. Attack requirements, method, setup and process are discussed in details.

Considering its application potential of CLEFIA, as many hardware devices are being produced using it, so it is important to mount DPA attack on hardware including FPGA implementations of CLEFIA.

Table of Contents

List of Tables

1.0 Introduction

Side channel analysis is a branch of cryptology using which sensitive information obtained by capturing and analyzing physical elements (like power, EM radiation, Sound etc.) of system rather than using computational weakness or mathematical consistency of cipher algorithm. Current practice to use many functions and round key during formation of cipher algorithms as well as using increased key bits size to resist computational attack. So it is more difficult to break cipher by computational analysis. Best alternate way is to break the algorithm, that is, Side Channel Analysis as shown in fig 1.

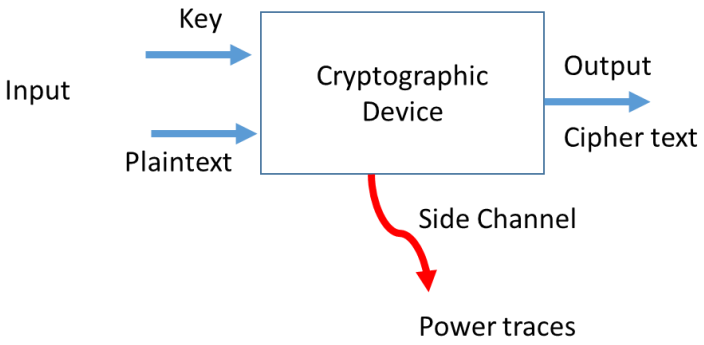


Figure 1 : Cryptographic process

Side channel attacks are two types 1. Active 2. Passive. Under active attack, in the cryptographic device, its inputs, its environment are manipulated so that device behaves abnormally. By exploiting this behavior of device attacker may get the key information. Here, attacker tries to induce errors in the computation through fault-induction and then calculate the required keys by analysis of those induced faults. Here problem is gaining the access to device and inducing the required faults at desired rounds. Passive attacks like differential power analysis, where the attack is done on the information obtained from the power consumption pattern during execution of cipher. Here difficulty is several process are running in the hardware at a given time.

They become the noise source for the cipher power trace capturing. Here Differential Side Channel Analysis will help to mount the attack .It is required to know the beginning of

cipher rounds, synchronizing the traces with functions .Complex setup is required to record minute power variation corresponding to the cipher rounds. Differential Side Channel Analysis involves

- Identifies the differences in side channel measurements which are not directly visible in measurement traces.
- Customized statistical methods are to be applied.
- Targeting one specific intermediate result, which is in a specific part of the measurement traces.
- A typical approach is to choose a selection function, which gives an intermediate result at the beginning or end of the algorithm.
- The outcome of the selection function depends on the known plaintext or cipher text and a small hypotheses made on the key bit value.
- The result of the selection function enables to partition of overall measurement data for each hypothesis made.
- If key hypothesis is correct, different statistical properties are shown on the two partitioning sets for given bits and traces in time which depend on the outcome of the selection function

Several research groups have been working on CLEFIA [1], about analyses of its security, performance evaluations and attacks. But no one claimed the successful Differential Power Analysis (DPA) attacks of CLEFIA so far. Differential Fault Analysis [4] on CLEFIA is recently published and we have also implemented the same.

Yizhi Xu from UST, China [2] presented a concept of application of DPA introduced by the Kocher [3] to CLEFIA supported by simulation of experiments but not the practical attack where key bits are fully recovered.

1.1 Study:

Differential power analysis is one kind of side-channel attacks, it was introduced by Kocher et al [3]. This technique applied to extract secret keys by capturing, measuring and analyzing the power consumption of the cryptographic devices. DPA is proved to be an efficient method to attack the different types of implementations of specially block ciphers.

DPA is where power traces corresponding the crypto operation are captured and analyzed. I have studied the theoretical aspects of DPA and its implementation on DES. In DPA, Statistical methods used for segregation of samples into different sets and signal processing methods are used for finding the correlation and extracting the key bits. Interestingly, DPA methods used for standard hardware implantation on Microcontrollers, Smartcards and Embedded processors are not effective if same is used for FPGA based hardware.

Towards this different type of DPA methods including hamming weight model are also studied which are suitable for the FPGA based hardware implementations, which are widely used now a days. I also studied setup and instruments required for the implementation of CLEFIA in hardware, capturing the power traces and analysis of samples.

2.0 CLEFIA Design

CLEFIA, it is a 128 bit block cipher with three different key sizes (128/192/256 bits) .It was proposed by Sony corporation. CLEFIA consists of two main parts: 1. data processing part and 2. Key scheduling part. CLEFIA consists of generalized Feistel structure with 4 data lines, and the width of each data line is 32 bits. In addition in, there are key whitening parts at the beginning and at the end of the structure. For key generation, numbers of rounds for 128-bit is 18, 192-bit is 22 and 256-bit is 26.

CLEFIA has mainly two processing parts one is for processing the data for encryption and decryption, second one for key generation part where round keys and whitening keys are generated from the main key.

2.1 Data Processing Part

CLEFIA [1] is based on the four branch generalized Feistel network structure as shown in figure 2 given by SONY, Width of each data line(branch) is 32 bits. Additionally, key whitening functions present at the beginning and at the end of the data processing part. The number of rounds are depends on the key length.

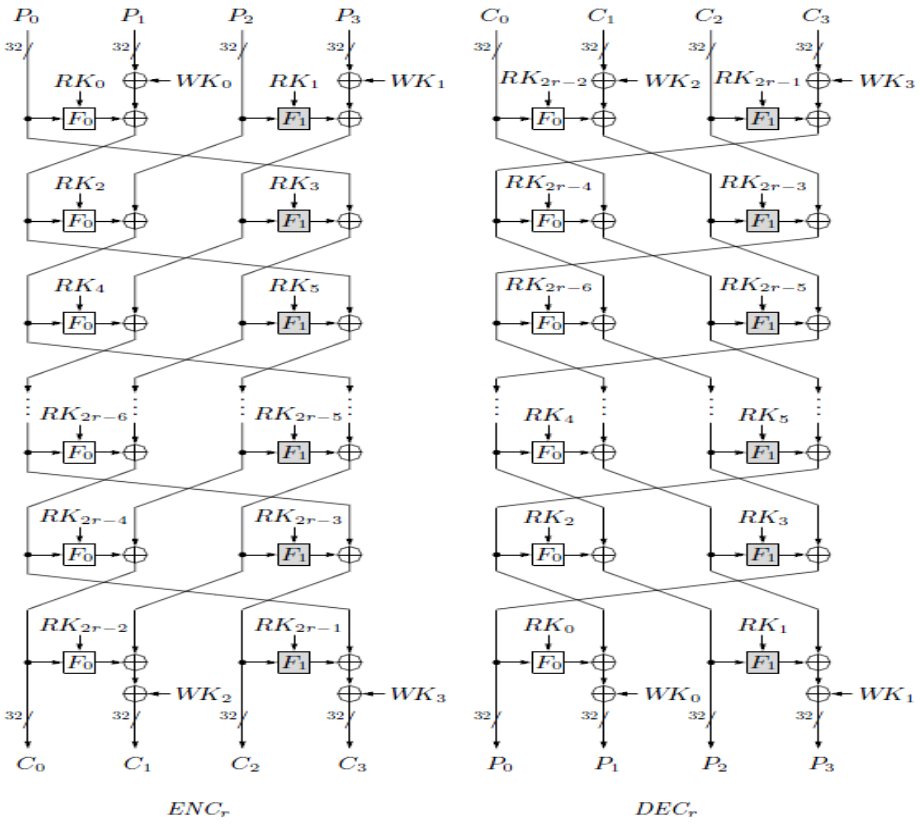


Figure 2 : Structure of data processing part

The r-round operation of encryption function defined as:

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

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

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

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

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

And

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

Typival Feistal function is like Byte wise round key mixing ,then S-Box lookup and finally Diffusion matrix multiplication.

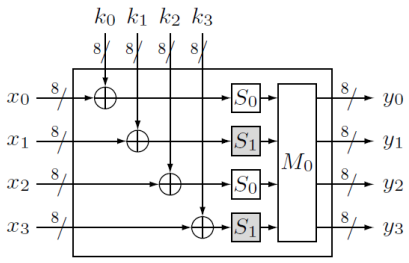


Figure 3 : Feistal function structure

Where F_0 and F_1 is as given below with matrix values

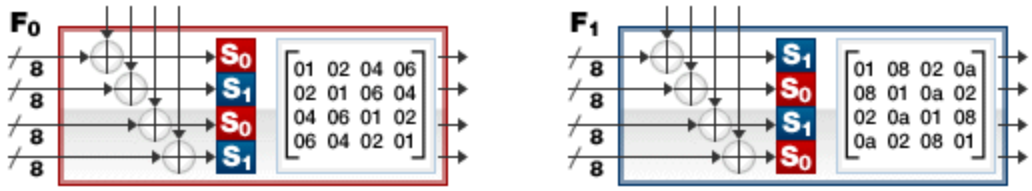


Figure 4 : Fo and F1 functions

Two F-functions F0 and F1 used by $GFN_{d;r}$ are defined as follows:

F0: (RK (32), x (32)) ↔ y (32)

Step 1. T← RK ⊕ x

Step 2. Let T = T_0 |T1 | T2 | T3, Ti ∈ $\{0,1\}^8$

S-Box look up

T0 ←S_0 (T_0);

T1← S_1 (T_1);

T2 ←S_0 (T_2);

T3← S_1 (T_3)

Step 3. Let y = y_0 | y_1| y_2| y_3, y_i ∈ $\{0,1\}^8$

Finally diffusion matrix multiplication

$\mathbf{t_{(y0;\ y1;\ y2;\ y3)} = M_0\ t_{(T0;\ T1;\ T2;\ T3)}}$

Similarly For F_1

F0: (RK (32), x (32)) ↔ y (32)

Step 1. T← RK ⊕ x

Step 2. Let T = T0 |T1 | T2 | T3, Ti ∈ $\{0,1\}^8$

S-Box look up

T0 ←S_1 (T0);

T1← S_0 (T1);

T2 ←S_1 (T2);

T3← S_0 (T3)

Step 3. Let y = y0 | y1| y2| y3, yi ∈ $\{0,1\}^8$

Finally diffusion matrix multiplication

$t_{(y0; y1; y2; y3)}$ = M1 $t_{(T0; T1; T2; T3)}$

Here S box 0 and 1 are 4 bit input output tables constructed using GF polynomial, Diffusion matrixes M0, M1 are 4*4 matrixes.

2.2 Key Scheduling Part

The key scheduling part of CLEFIA basically three types viz. 128, 192 and 256 bits and has the whitening keys $WKi,\ 0 \le i \le 3$ and number of round keys $RKi,\ 0 \le i < 2r$ required for the data processing part. Assume **K** as main key and **L** as intermediate key.

The key scheduling part mainly contains of two modules, 1. Generating L from K, and 2. Expanding K and L for generation of WKi and RKi. **L** is generated by mixing the constant values CONi and **K** using the general feistel network structure. These constants values are given by SONY. WKi is generated directly from K, and RKi is generated directly from ExOR operation of K, CONi, Land Σi (L), where Σ denotes bit-wise permutation function called **Double Swap**.

Round key generation can be summarized in the below given figure.

WK_0	WK_1	WK_2	WK_3	$\leftarrow K$
RK_0	RK_1	RK_2	RK_3	$\leftarrow L \oplus (CON_{24}^{(128)} \mid CON_{25}^{(128)} \mid CON_{26}^{(128)} \mid CON_{27}^{(128)})$
RK_4	RK_5	RK_6	RK_7	$\leftarrow \Sigma(L) \oplus K \oplus (CON_{28}^{(128)} \mid CON_{29}^{(128)} \mid CON_{30}^{(128)} \mid CON_{31}^{(128)})$
RK_8	RK_9	RK_{10}	RK_{11}	$\leftarrow \Sigma^2(L) \oplus (CON_{32}^{(128)} \mid CON_{33}^{(128)} \mid CON_{34}^{(128)} \mid CON_{35}^{(128)})$
RK_{12}	RK_{13}	RK_{14}	RK_{15}	$\leftarrow \Sigma^3(L) \oplus K \oplus (CON_{36}^{(128)} \mid CON_{37}^{(128)} \mid CON_{38}^{(128)} \mid CON_{39}^{(128)})$
RK_{16}	RK_{17}	RK_{18}	RK_{19}	$\leftarrow \Sigma^4(L) \oplus (CON_{40}^{(128)} \mid CON_{41}^{(128)} \mid CON_{42}^{(128)} \mid CON_{43}^{(128)})$
RK_{20}	RK_{21}	RK_{22}	RK_{23}	$\leftarrow \Sigma^5(L) \oplus K \oplus (CON_{44}^{(128)} \mid CON_{45}^{(128)} \mid CON_{46}^{(128)} \mid CON_{47}^{(128)})$
RK_{24}	RK_{25}	RK_{26}	RK_{27}	$\leftarrow \Sigma^6(L) \oplus (CON_{48}^{(128)} \mid CON_{49}^{(128)} \mid CON_{50}^{(128)} \mid CON_{51}^{(128)})$
RK_{28}	RK_{29}	RK_{30}	RK_{31}	$\leftarrow \Sigma^7(L) \oplus K \oplus (CON_{52}^{(128)} \mid CON_{53}^{(128)} \mid CON_{54}^{(128)} \mid CON_{55}^{(128)})$
RK_{32}	RK_{33}	RK_{34}	RK_{35}	$\leftarrow \Sigma^8(L) \oplus (CON_{56}^{(128)} \mid CON_{57}^{(128)} \mid CON_{58}^{(128)} \mid CON_{59}^{(128)})$

Figure 5 : Round key generation function

Double swap function which does bit-wise permutation as given below.

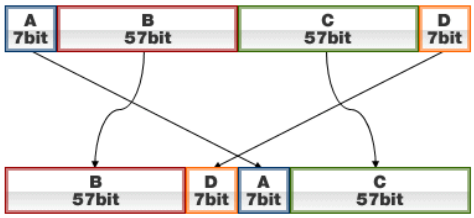


Figure 6 : Double swap function

3.0 Differential power analysis attack

DPA is basically depends on the power consumed by the FPGA or any Hardware on the intermediate data values. Following steps are involved in attack procedure.

- Selection of FPGA hardware with Power monitoring port.
- HDL implantation of Cipher.
- Trace capture setup including current probe with amplifier and oscilloscope.
- SMA Cable setup for interconnectivity.
- Development of Signal analysis algorithm to filter and implement selection function.
- Trace capture and key bits extraction.

3.1 DPA attack procedure:

For implementation of DPA attack, Frist M encryption operations have to be performed using M plaintexts P(m),m ∈ {1, ...,M} with same key, and capturing the power traces T(P(m), t), t ∈ {1, ..., k}, where k denotes the number of a sample. Cipher texts C (m) are recorded for M operations. Let RK_i represent the round key targeted for attack.

As per CLEFIA cipher structure, RK_i is separated into four bytes, represented by $RK_{i,b}$, where $0 \leq b \leq 3$. There are two types of models exists for the relation between power trace and values of intermediate data. They are the 1. Hamming weight model 2. Hamming distance model. The definition and tuning of the DPA selection function purely depends on the structure of algorithm and the specific implementation on FPGA hardware.

For this attack Hamming weight model is used, here output of the S-box corresponding to $RK_{i,b}$ is selected as the intermediate data, represented by $S(P(m), b, RK_{i,b,s})$, where P(m) is cipher text, b is the byte number of round key RK_i, $RK_{i,b,s} \in \{0, ..., 255\}$ is our hypothesis for $RK_{i,b}$. Let W (.) represent the Hamming weight of a variable.

For this selection function defined as

$D(P(m), b, RK_{i,b,s}) = 0$, If $W(S(P(m), b, RK_i, b, s)) < 4$

1, If $W(S(P(m), b, RK_i, b, s)) > 4$

For every key round hypothesis $RK_{i,b,s}$, the power traces T(P(m), t) are classified into two sets they are defined as

T0 = $\{T(P(m), t) \mid D(P(m), b, RK_{i,b,s}) = 0\}$

T1 = $\{T(P(m), t) \mid D(P(m), b, RK_{i,b,s}) = 1\}$

Then, calculating a differential trace as defined below

$$\Delta D(t, b, RK_{i,b,s}) = \frac{1}{|\mathbf{T_1}|} \sum_{T \in \mathbf{T_1}} T(P(m), t) - \frac{1}{|\mathbf{T_0}|} \sum_{T \in \mathbf{T_0}} T(P(m), t)$$

Using a selection function, where |**T1**| and |**T0**| are the numbers of elements present in **T1** and **T1**.

If round key hypothesis $RK_{i,b,s}$ is the correct value of $RK_{i,b}$, then there would be an clear peak in $\Delta D(t, b, RK_{i,b,s})$. If $RK_{i,b,s}$ is incorrect, this no peak would be found.

Here RK_0 and RK_1 can be obtained from C_0^0 and C_0^2,, that is, P_0 and P_2, which are known by attackers. As described above, main key calculated using DPA method.

As per the definition of F_0, we get

$$F_0(C_0^1, RK_2)$$
$$= F_0(C_1^0 \oplus WK_0 \oplus F_0(C_0^0, RK_0), RK_2)$$
$$= F_0(C_1^0 \oplus F_0(C_0^0, RK_0), RK_2 \oplus WK_0)$$

Where know the value of C_0^1 and C_0^0 and RK_0 can be obtained using DPA on the first round.

So ($RK_2 \oplus WK_0$) can be obtained using DPA attack.

Similar way ($RK_3 \oplus WK_1$) also be obtained. Step by step process, using the DPA method, we will get RK_{4i}, $RK_{4i+1} \oplus WK_0$, RK_{4i+2}, $RK_{4i+3} \oplus WK_1$, $0 \leq i < r/2$.

On other side, we get RK_{2r-2} and RK_{2r-1} from C_{r-1}^0 and C_{r-1}^2,, that is, C_0 and C_2, which are already known.

From the above obtained values, all round keys can be calculated RKi, $0 \leq i < 2r$ and also the whitening keys WKi, $0 \leq i \leq 3$. As per key scheduling algorithm, using round keys main key K can be calculated. Pictorial representation of attack procedure given below.

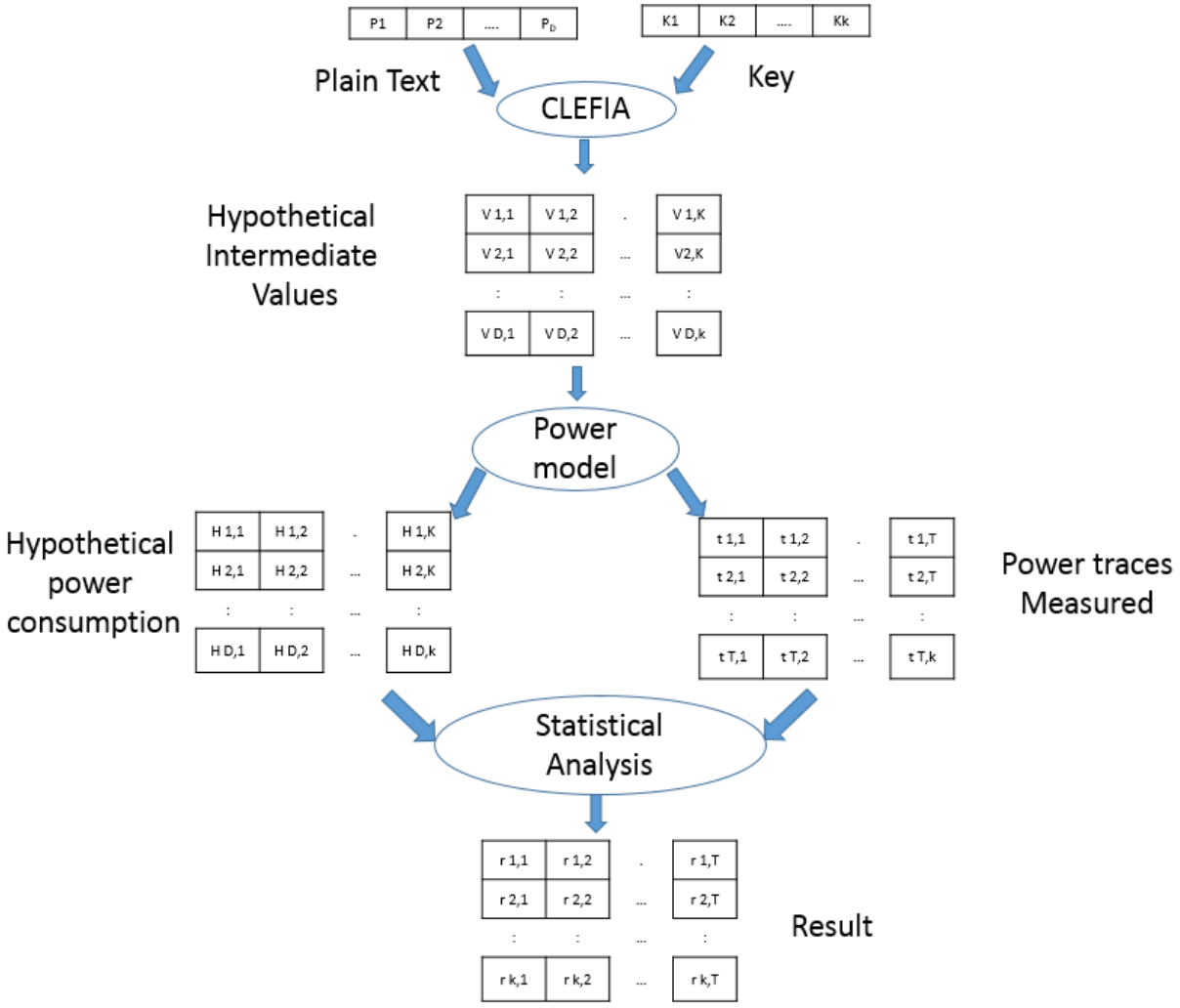


Figure 7 : DPA Process representation

3.0 Implementation of CLEFIA:

For hardware implementation of CLEFIA, I have selected 128 bit input plain text and key with four branch feistal structure consists of 18 round for data processing part including four whitening keys and 36 round keys. Its key generated using GFN structure with 12 rounds .Using Xilinx ISE 14.2 tool, CLEFIA hardware implementation in VHDL is completed. After Synthesis targeting to the Xilinx vettex-5 FPGA the following resources are consumed.

3.1 CLEFIA Implementation Results

Selected Device: Virtex-5 FX 200-T

Slice Logic Utilization:

Slice Registers:	4969 out of 97280	5%
Slice LUTs:	6245 out of 97280	6%
Logic:	4872 out of 97280	5%
Memory (Kb):	1373 out of 26240	5%

Timing Summary:

Speed Grade: -1

Minimum period: 7.537ns (Max Frequency: 132.679 MHz)

Maximum combinational path delay: 5.607ns

Specific Feature Utilization:

Block RAM/FIFO:	15 out of	212	7%
BUFG/BUFGCTRLs:	1 out of	32	3%
DSP48Es:	90 out of	128	70%

It is consuming the resources more than the optimum implementation as round wise implementation enable clear demarcation and synchronization in traces for capture for power analysis.

With the high density and lower core voltage FPGAs, DPA complexity is increasing multifold. Here we discuss the approach to capture the power traces when any block cipher running on a FPGA board. Generic FPGA boards have EMI filter, LVDOs, POLA devices in their power distribution network.

4.0 DPA Setup and Process:

Differential power analysis attack requires a very special setup including Target crypto device, Probes to monitor power, Amplifier to amplify the very minute variations emanate during crypto operations. This also improves the signals SNR for further processing .Amplified traces are fed to high sampling rate oscilloscope with low band width .Complete setup is shown below. In order to capture power traces general practice is to insert a 50 ohm resistor in the power line for general hardware or to monitor current through a current probe.

4.1 Setup diagram:

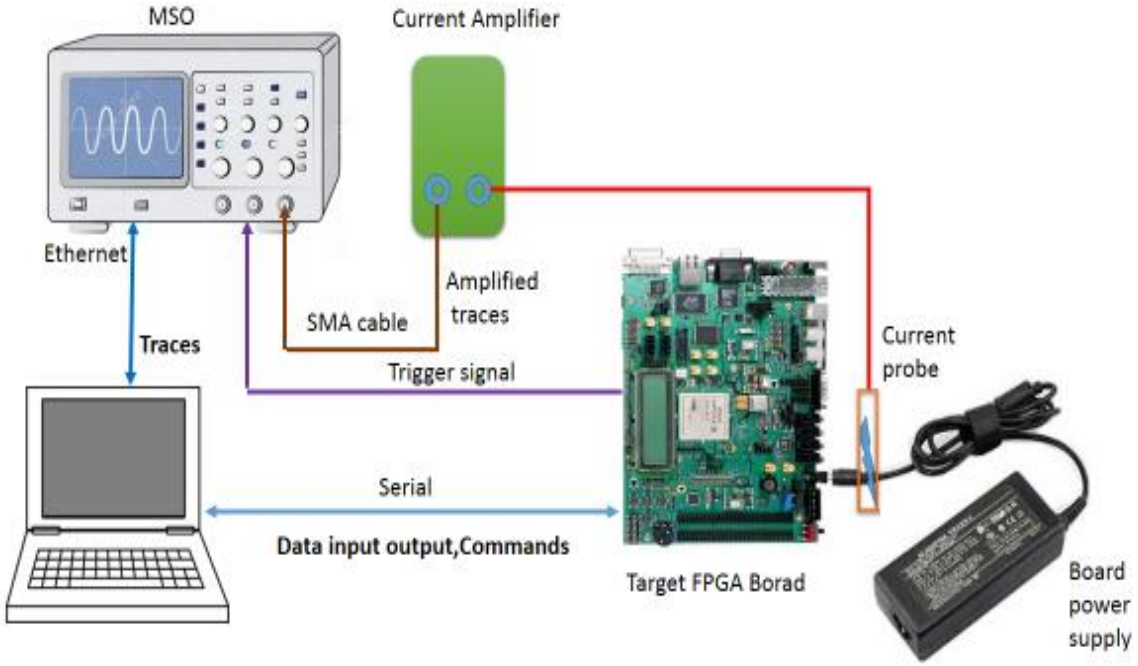


Figure 8 : DPA setup diagram

4.2 Actual setup @ Lab:

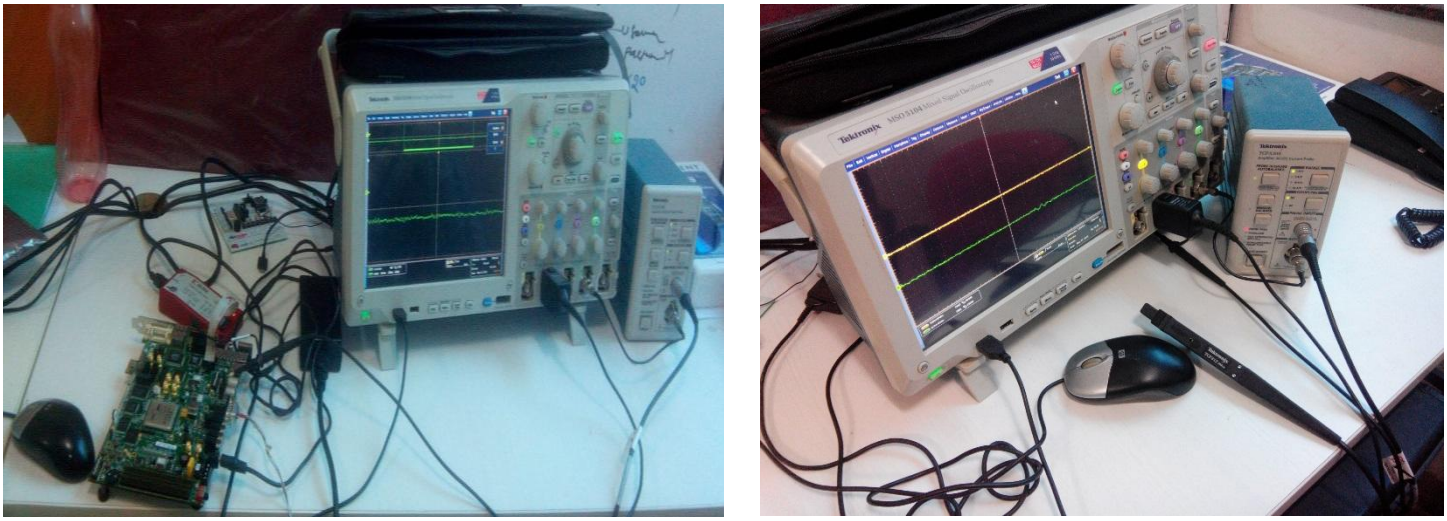


Figure 9 : DPA lab setup diagram

4.3 Requirements:

1. MSO – Tektronix 5104
2. Current amplifier – Tektronix TCP A300
3. Current probe
4. FPGA Hardware – Xilinx ML 507 with power supply
5. SMA, Ethernet, Serial cables
6. PC with Xilinx ISE, EDK, Chip Scope Pro, Mat lab, with required toolbox loaded.

All these are connected as shown in setup diagram. Hardware which is essential for capturing and analysis of wave forms. Here is the list of Components with their functionality:

1. Field Programmable Gate Array (FPGA): It is a Virtex-5 FX-200-T chip in which hardware code, that is, CLEFIA is dumped. It works on core voltage VCCINT of 1.0 V. Its I/O voltage with DCI is from +1.8 to 3.3 V.
2. Adapter: It is used to step down convert alternative current (AC) to direct current (DC). Output of this adapter is +5V which is suitable for FPGA board.
3. Computer System: This the medium to synthesize the hardware code with the help of software Xilinx ISE/EDK. The input is given/output read to FPGA with this system software only.
4. Sensor probe: This is a current probe which is useful to record at a particular point of FPGA board preferably power port before filtering. Which is directly analyses in the oscilloscope.
5. Amplifier: This is a current amplifier which is used to amplify the signal which is coming from FPGA board to oscilloscope. This can amplify the signal by increase in the scale of amplitude by 15 times more. This helps in analysis of coming signal in the oscilloscope resolution range.
6. Oscilloscope: This is a digital oscilloscope (1GHz) used for actual storing waveform coming from FPGA board in the form of digital signal. This will also help in capture and save waveform in hardware on synchronization from FPGA board. It can intake 4 input waveform simultaneously and also interface with Computer system.

4.4 Attack Process:

1. HDL code developed for given block cipher.
2. Through EDK, Module with software registers to give input and take output and UART interface developed
3. Module to raise a trigger when encryption starts and lower when finished also developed.
4. All the above three are fused into FPGA board.
5. MSO Interface to read trace files developed.

6. Matlab code for Analysis of traces using filters, Selection function will be developed.
7. Finally a DPA module to interface all devices, Control all modules, generate input to board, capture traces and analyze key will be developed.

4.5 Steps involved in capturing process:

1. The flow starts with the PC sends inputs to the FPGA device and initializing MSO.
2. PC sends input data and a command to start encryption to the FPGA device.
3. The FPGA device receives the data and the command, raises a trigger signal and starts the encryption in FPGA.
4. MSO acquires traces upon detecting the trigger edge and stop when trigger goes low.
5. MSO reports the PC that acquisition is finished.
6. Meanwhile, the target reports the PC that encryption is finished and returns the encryption result.
7. MSO sends the traces to the PC.
8. PC receives the trace, saves it and proceeds to the next capture cycle. After acquiring given number of traces,
9. After completion of multiple acquitions of traces for several crypto operations PC starts analysis of Traces using statistical methods which are implemented in Mat lab.
10. Based on the processing of data key bits are obtained.

5.0 DPA on ML507 platform.

5.1 Capture process

Capture the large signal traces of probe (in the order of mV) and stored in MSO in CSV or other format. These values can be read and replayed in Malab as shown below. Having captured the multiple sets of power traces correlation between capture two sets calculated and plotted. However actual traces for CLEFIA operation are of very less magnitude, that is, in the order of micro amps, can only be captured using current probe along with a current amplifier.

FPGA board or Device which supports power trace capturing over SMA connector is required as this current probe supports Lowest measurable current of 1 milli Amp (at ± 2% accuracy at DC) where Scope set to 1 mV/div and at a limited band width of 20 MHz only.

To mount the attack on Xilinx ML507evaluation board, power traces be captured before the filter after voltage regulators. But this provision is not available in ML507. FPGA core Vcc INT and device I/O VccO voltages are different, correlation of traces is different for these voltages.

At this point we are unable to measure the power consumption (traces) of the device. For these attacks side channel evaluation boards (SASEBO) are required as capacitors are not mounted on them (FPGA board to power supply) to allow monitoring of small fluctuations in power consumption. For attack we have all the information you need except the secret key. Here using differential power analysis to extract the secret key using captured traces, plaintext, cipher text and the knowledge of the encryption algorithm by creating the

hypothesis of the power consumption and after that correlating it with the measured traces. Here though useful traces are not captured, procedure for the entire processes is developed.

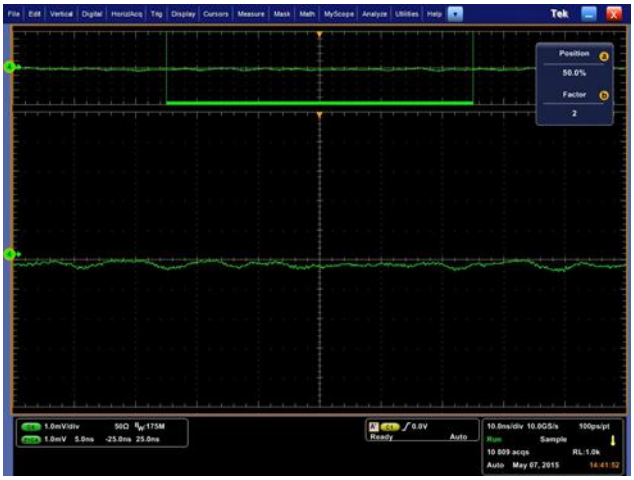


Figure 10: Power traces diagram

5.2 Synchronization

In the process of generating trigger from FPGA board to run cipher module and initiate the capture, signals may be misaligned and synchronization may be lost. In that case identifying the specific round traces and removal of noise becomes difficult. For that proper synchronization must be ensured to record traces with respect to each functionality. Following steps would ensure the same.

After generating trigger from FPGA board.

- Plot one trace of one operation, check that it is complete.
- Check the alignment of traces, ensure they overlay correctly to confirm that triggering works.
- Select the appropriate part of the traces (e.g. containing the first round). Record the required number of traces.

- Depending on measurements, Traces are required to be corrected over mean value. It can done by subtracting each trace from its mean value. Then recover the secret key using the DPA with correlation coefficients. Some of traces captured for CLEFIA are shown below.

Figure 10: Trigger diagram

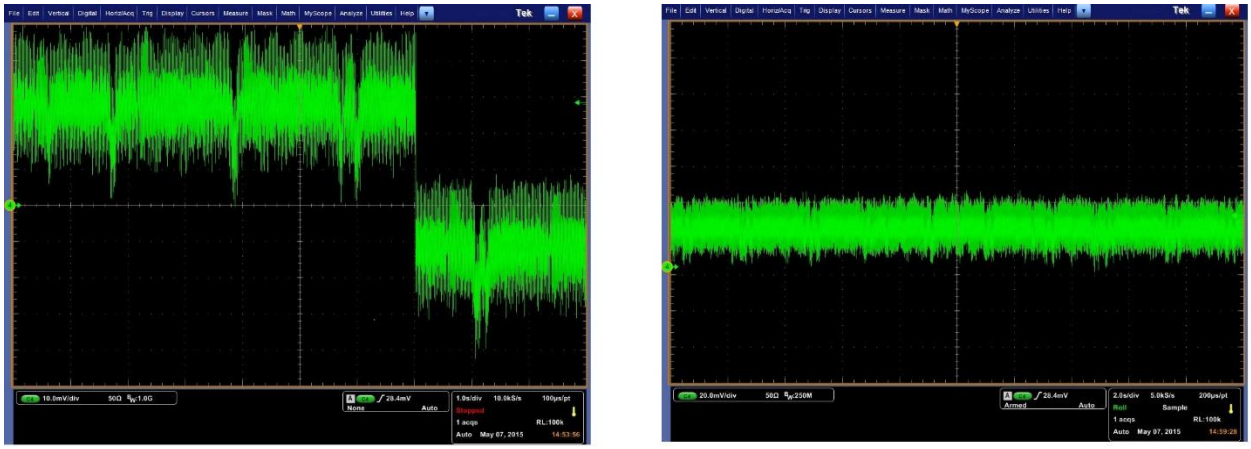


Figure 11: Power trace diagram (zoomed)

5.3 Trace Analysis

Set of 200 plaintexts using same key we obtain 200 cipher texts. During encryptions we measured power traces. Each trace has a length of 320000 samples (Typically). Each sample is represented by 8 bit unsigned value (Then length of the file is 320000 * 8 bits * 200 traces = 64 MB). These trace files will be analyzed trough the script of selection function. If proper alignment for capturing is done then the samples will be processed into sets then the selection function will be applied to get the correlation coefficients for each key bit.

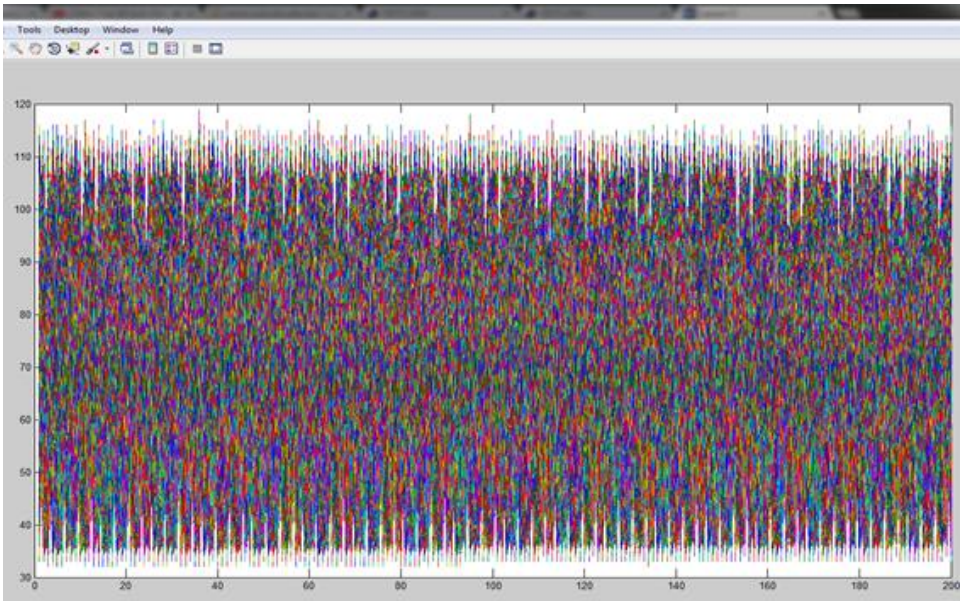


Figure 12: Plotting of power traces

6.0. Conclusion

Study of CLEFIA Implementation of CLEFIA in VHDL and porting on to the Xilinx evaluation board is completed. Required DPA setup is completed with Xilinx Evaluation board .Complete Power analysis procedure has been established.

Suitable FPGA hardware platform like SASEBO board has to be obtained so as to capture the measurable traces. Any FPGA board with proper power monitoring port with SMA connectivity is required to capture the traces in oscilloscope even at low band width. Thus the setup for mounting the attack on CLEFIA will be completed. After tuning the selection function to suit the trace properties viz. order of magnitude of amplitude/current, noise level present in traces and importantly synchronization with CLEFIA internal operation (data processing or round key generation) all the key bits will be obtained.

DPA based attacks can perform much useful when other techniques are not useful to break cipher it is also faster than other techniques. However, this type of attacks requires physical access to the hardware power ports in order to get the traces required for its execution and special setup.

7.0 References

[1] Sony Corporation. (2007) The 128-bit block cipher CLEFIA algorithm specification (Revision 1.0). [Online]. Available: http://www.sony.net/Products/cryptography/clefia/technical/data/clefia-spec-1.0.pdf

[2] Differential Power Analysis Attack on CLEFIA Block Cipher --Xuefei Bai, Lu Huang, Yao Wang, Yizhi Xu University of Science and Technology of China

[3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology – 19th Annual International Cryptology Conference, CRYPTO 1999, Proceedings, LNCS 1666*, Santa Barbara, CA, USA, Aug.1999, pp. 388–397.

[4] H. Chen, W. Wu, and D. Feng, "Differential fault analysis on CLEFIA,"in *Information and Communications Security – 9th International Conference,ICICS 2007, Proceedings, LNCS 4861*, Zhengzhou, China, Dec.2007, pp. 284–295.

[5] S.B.Ors, E.Oswald, B.Preneel, Power-Analysis Attacks on an FPGA - First Experimental Results, in the proceedings of CHES 2003, Lecture Notes in Computer Science, vol 2279, pp 35-50, Springer-Verlag.

[6] Post Acquisition analysis, "DPA script", Graz University of Technology, April 2007.