

Current Analysis Attacks on various of-the-shelf Emerging Memory Technologies

Final Project A REPORT

PROJECT NO.: 4786

AUTHORS: KARAM GHANAYEM & NOOR KORDI

SUPERVISOR: ERIC HERBELIN

ASIC2 – VLSI LABS, TECHNION

WINTER 2018/2019

FORWARD

Final Project Report for project no. 4786, the project research title is:

Current Analysis Attacks on various of-the-shelf Emerging Memory Technologies.

The report contains:

- Documentations for an advanced Side-channel attack setup.
- Suggestions for Current Analysis Attacks on Emerging Memory Technologies.

The report attached with project GitHub link:

<https://github.com/CurrentAnalysis/Project.git>

.....

AUTHORS:

KARAM GHANAYEM – karam5@campus.technion.ac.il

NOOR KORDI - noorkordi@campus.technion.ac.il

SUPERVISOR:

ERIC HERBELIN - ericherbelin@ee.technion.ac.il

ABSTRACT

As the first phase of our project, we build a side-channel setup in order to test emerging memory technologies resistance to current analysis attacks, since current analysis is a practical type of attack in order to do any research, a current analysis side-channel setup is the first requirement.

Our setup includes KEYSIGHT CX3300 Device Current Waveform Analyzer, KEYSIGHT DC Power Supply, APPLIED MATERIALS Logic Analyzer, RASPBERRY PI Smart Card 3 b+, FUJITSU RERAM memory chip, CYPRESS FRAM memory chip and MICROCHIP SRAM memory chip in the hardware side, in the software side our setup includes algorithms running on the smart card in order to communicate with the memory chips, oscilloscope automation scripts and MATLAB Signal Processing and Analyzing libraries.

We verify the functionality of the setup by performing 3 different current analysis attacks on the setup outcome current traces, since building a setup is a complicated process that includes a long process of debugging and testing, having a pre-built setup would save the time of future researchers.

The second phase of our project is to attack the memory chips technologies which have widely use on electronic devices in order to create current consumption profiles for their supported operations that allow us to exploit the stored and transmitted bits, we introduce novel approaches to exploit stored information by the time the computing device access those memory chip in its system, Therefore, we practically show that even though the algorithm is very new still it is vulnerable to current analysis.

The third phase of the project is to work on countermeasures, after getting familiar with the current state of art, we select few already introduced countermeasures and practically attack them on our setup to do a comparative analysis, Meanwhile, we try to form our own countermeasures and to improve existing countermeasures, under circuit-based countermeasures, the existing idea of implementing software decoding algorithm is practically implemented and tested, we show that it is not safe enough we try few of our own circuit-based ideas as well, to evaluate how good they are as countermeasures, but unfortunately, none of them are good enough.

TABLE OF CONTENTS

FORWARD	2
ABSTRACT	3
1. PROJECT BACKGROUND	6
1.1 INTRODUCTION TO SIDE CHANNEL ATTACKS	6
1.2 INTRODUCTION TO CURRENT ANALYSIS ATTACKS	7
1.3 EMERGING MEMORY TECHNOLOGIES.....	8
1.4 PROJECT GOAL	9
2. CURRENT ANALYSIS ATTACKS TARGETS	10
2.1 MEMORY CHIPS TECHNOLOGY	10
2.2 SERIAL PARALLEL INTERFACE (SPI).....	15
2.3 MEMORY CHIPS CARD.....	16
3. CURRENT ANALYSIS SETUP EQUIPMENT.....	18
3.1 CURRENT ANALYSIS SETUP REQUIREMENTS	18
3.2 KEYSIGHT CX3300 Device Current Waveform Analyzer.....	20
3.3 KEYSIGHT DC POWER SUPPLY.....	21
3.4 APPLIED MATERIALS LOGIC ANALYZER	21
3.5 COMPONENT 3 – SPI MASTER RASPBERRY PI	22
3.5 MANUAL MEASURING PROCESS	23
4. CURRENT ANALYSIS SETUP AUTOMATION.....	25
4.1 COMMUNICATION SCRIPTS.....	25
4.3 CURRENT MEASUREMENTS DATABASES	27
5. SIMPLE CURRENT ANALYSIS ATTACK	29
5.1 BACKGROUND.....	29
5.2 ATTACK GOAL.....	29
5.3 ATTACK STEPS EXPLANATIONS.....	30
5.4 CONCLUSION.....	32
6. CORRELATION CURRENT ANALYSIS ATTACK	33
7.1 BACKGROUND.....	33
7.2 ATTACK GOAL.....	34
7.3 ATTACK STEPS EXPLANATIONS.....	35
7. PREVENTING CURRENT ANALYSIS ATTACKS	44
7.1 BACKGROUND.....	44

7.2	DECODING METHOD	46
7.3	ENCRYPTION ALGORITHMS	48

1. PROJECT BACKGROUND

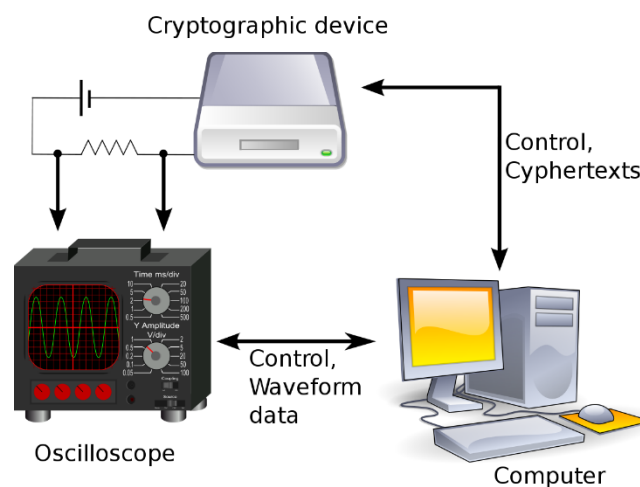
1.1 INTRODUCTION TO SIDE CHANNEL ATTACKS

In computer security, a side-channel attack is a security exploit based on collecting information about what a computing device does when it is performing its supported operations and information gained from the implementation of a computer system in order to use that information to reverse engineer the device's system, these attacks are carried out passively.

In computing, a side channel is any communication channel that is incidental to another communication channel, thus, side-channel attacks rely on the relationship between information emitted (leaked) through a side channel and the secret data in a computing device, rather than weaknesses in the implemented algorithm itself.

Timing information, power consumption, electromagnetic fields or even sound can provide an extra source of information, which can be exploited.

This research focuses on current consumption of computing chips as source of information that indicates which operation and parameters the computing chip is performing by its current consumption profile.



1.2 INTRODUCTION TO CURRENT ANALYSIS ATTACKS

Power analysis is a branch of side channel attacks in which power consumption data is used as the side channel to attack the system.

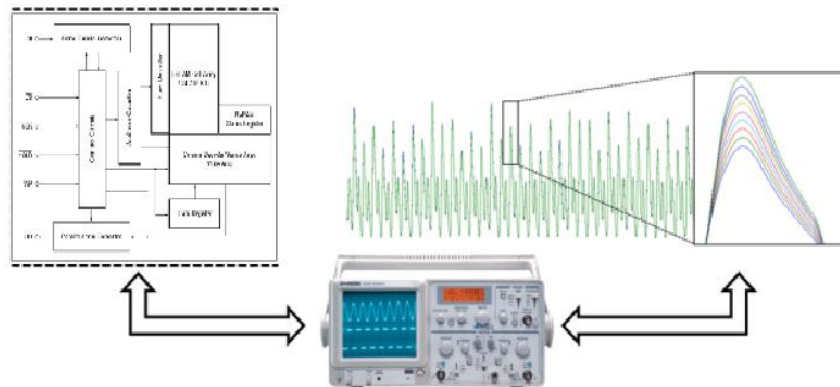
Current analysis attacks are a form of power analysis and side channel attacks in which studying the current consumption of a hardware computing device can lead to formulating information which can exploit secrets about the hardware computing device.

First using a current measuring device such as an oscilloscope, current traces are collected when the hardware computing device is performing operations, then those traces are statistically analyzed using signal processing techniques to derive the secrets of the system.

Many Power Analysis Attack and similar techniques have been developed, making Side-Channel Attack a real threat to commercial hardware and software, unfortunately, there is no sufficient awareness of the subject

This research report suggests and researches 3 techniques of Power analysis and adjust them to current analysis:

- Simple Power analysis (section 5).
- Differential Power analysis (section 6).
- Correlation Power Analysis (section 7).

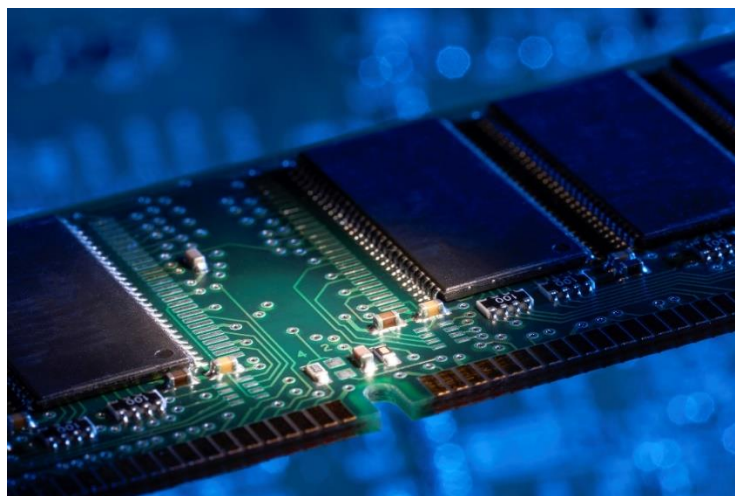


1.3 EMERGING MEMORY TECHNOLOGIES

Semiconductor memory chip is a digital electronic semiconductor device used for digital data storage, such as computer memory, made out of millions of capacitors and transistors that can store data or can be used to process code.

Semiconductor memory also has much faster access times than other types of data storage; a byte of data can be written to or read from semiconductor memory within a few nanoseconds, while access time for rotating storage such as hard disks is in the range of milliseconds. For these reasons it is used for main computer memory (primary storage), to hold data the computer is currently working on, among other uses.

Memory chips can hold memory either temporarily through random access memory (RAM), or permanently through read only memory (ROM). Read only memory contains permanently stored data that a processor can read but cannot modify. Memory chips comes in different sizes and shapes. Some can be connected directly while some need special drives. Memory chips are essential components in computer and electronic devices in which memory storage plays a key role.



1.4 PROJECT GOAL

PROJECT MOTIVATION:

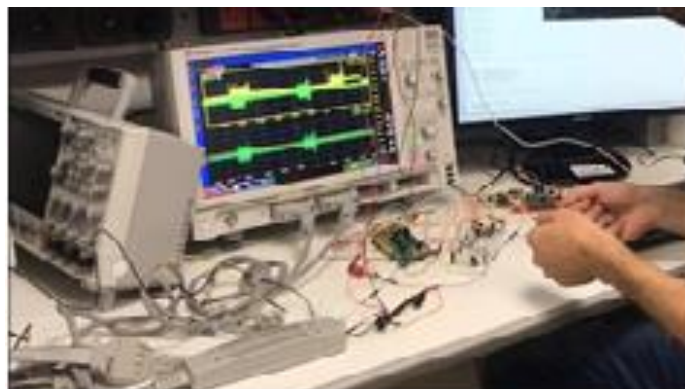
We frequently assume that secrets will be manipulated in closed, reliable computing environments, Unfortunately, actual hardware devices leak information about the operations they process.



PROJECT GOAL:

Side channel attacks setups are known as relatively low-cost setups and easy to implement, our project goal develop Current Analysis setup contains advanced equipment and combine various comminution and control protocols in order to suit the targeted hardware, we use this setup in order to:

- Test emerging memory technologies resistance to current analysis attacks, advanced setup examines these attacks in higher resolution and extract more detailed attacks reports.
- Testing common methodology using Current analysis attacks in order to Evaluate the vulnerabilities and introduce countermeasures to prevent tested Current analysis attacks



2. CURRENT ANALYSIS ATTACKS TARGETS

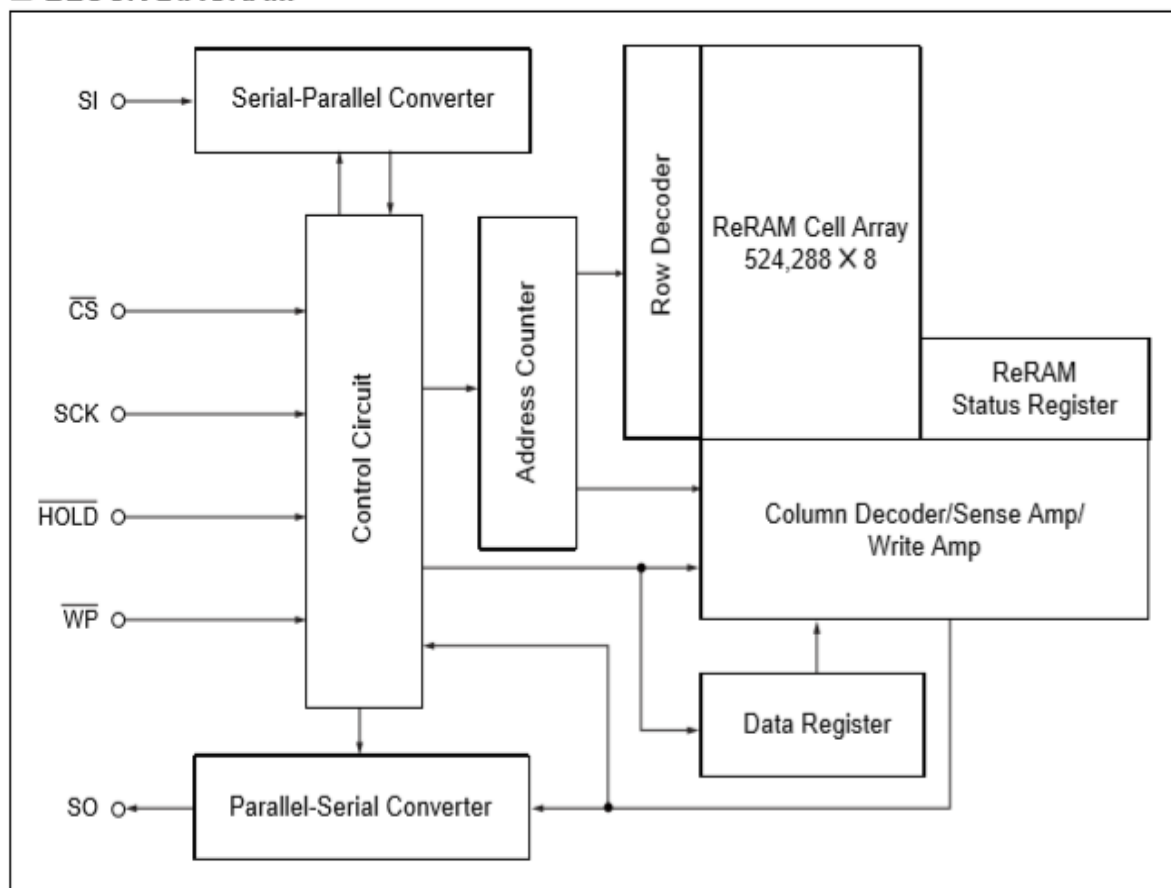
2.1 MEMORY CHIPS TECHNOLOGY

There are many different types of implementations using various technologies, during our research phases we tested various memory technologies, in this report section we will mention 3 main Emerging Memory Technologies in order to test their current analysis resistance, compare and analysis:

- Resistive random-access memory (ReRAM):
ReRAM is a type of non-volatile (NV) random-access (RAM) computer memory that works by changing the resistance across a dielectric solid-state material, ReRAM involves generating defects in a thin oxide layer, known as oxygen vacancies (oxide bond locations where the oxygen has been removed), which can subsequently charge and drift under an electric field. The motion of oxygen ions and vacancies in the oxide would be analogous to the motion of electrons and holes in a semiconductor.
- Static random-access memory (SRAM):
SRAM is a type of semiconductor random-access memory (RAM) that uses bistable latching circuitry (flip-flop) to store each bit, SRAM exhibits data remanence, but it is still volatile in the conventional sense that data is eventually lost when the memory is not powered, must be periodically refreshed, SRAM is considered faster and more expensive than other memory technologies, it is typically used for CPU cache.
- Ferroelectric RAM (FRAM):
FRAM is a random-access memory using a ferroelectric to achieve non-volatility, FRAM is one of a growing number of alternative non-volatile random-access memory technologies that offer the same functionality as flash memory, FRAM's advantages over Flash include: lower power usage, faster write performance. and a much greater maximum read/write endurance.

The previous memory chips use SPI communication protocol, therefore they have some common components, the Figure below describes the block diagram of RERAM, this Figure attached to the providers documentation of RERAM chip, in our research we managed to split this block diagram into 2 main parts in order to get deep understanding of those chips systems and be able to attack them with current analysis attacks, the first part includes: Serial Parallel converter and Parallel Serial converter, the second part includes: memory chip Cell Array and the logic functions which maintain the cell array.

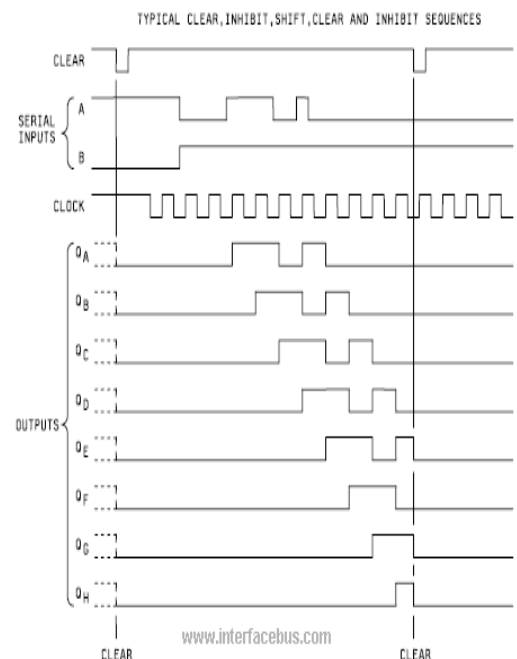
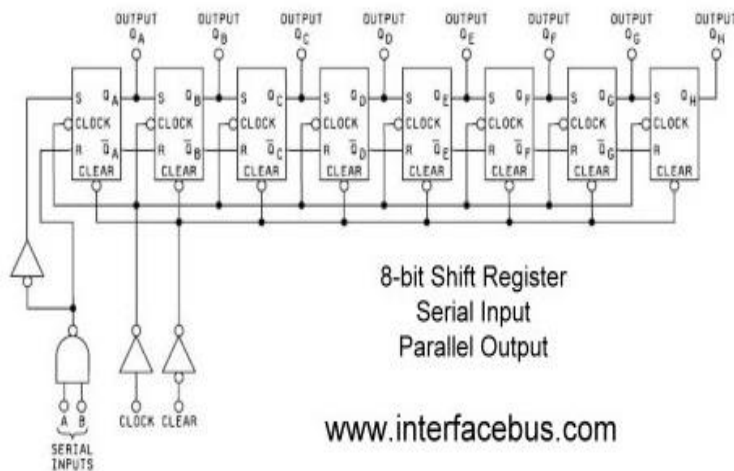
■ BLOCK DIAGRAM



Common principles and components:

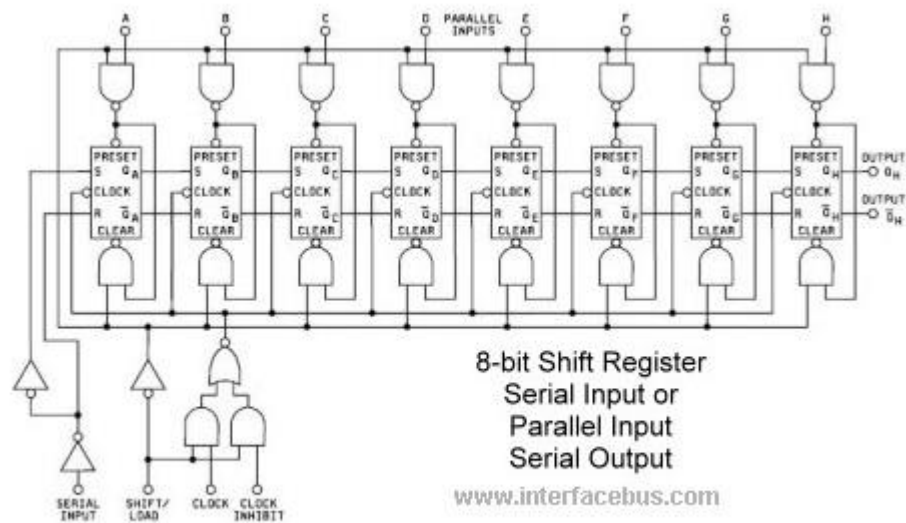
- Serial to parallel converter interface:

Serial data transmission from one digital system to another is commonly used to reduce the number of wires in the transmission line, microprocessor-based system commonly requires incoming data to be in parallel format, thus the requirement for serial-to-parallel conversion, serial parallel converters implementation include shift registers, a shift register works by shifting data to the right with each clock pulse. Regardless of if the data is loaded in all at once via parallel load or one bit at a time via serial input. Each clock pulse shifts data into the first flip flop, the data that was in the 1st flip flop shifts to the 2nd flip flop and so on. In a serial load shift register each flip flop begins with a 0 loaded. A parallel load shift register may contain whatever is loaded into the register when the load pin is activated. Regardless of what is pre-loaded, the data is shifted to the right with each clock pulse.



- Parallel to serial converter output:

In this converter all parallel data is loaded (stored) simultaneously into the D-type flip-flops. Once this is achieved, with the help of the clock, data is shifted one bit a time from the last flip-flop. This two-step process is schematically illustrated in the accompanying figure. In an actual converter, more circuitry is needed. Simply, the parallel data is multiplexed in order to convert it into serial data. The multiplexer will force the parallel data to be shifted one bit at a time through the last (most significant bit) flip-flop.



8-Bit Shift Register IC

Different principles and components:- Cell array

The memory cell is the fundamental building block of memory. It can be implemented using different technologies, such as bipolar, MOS, and other semiconductor devices. It can also be built from magnetic material such as ferrite cores or magnetic bubbles. Regardless of the implementation technology used, the purpose of the binary memory cell is always the same. It stores one bit of binary information that can be accessed by reading the cell and it must be set to store a 1 and reset to store a 0.

Memory type	Max freq	Read current	Write current	Write Buffer	endurance
RERAM	5Mhz	0.2mA	1.3mA	yes	1.2e6
SRAM	20Mhz	3mA	3mA	no	~inf
FRAM	20Mhz	250uA	250uA	no	~inf

2.2 SERIAL PARALLEL INTERFACE (SPI)

The Serial Peripheral Interface (SPI) is a synchronous serial communication interface specification used for short-distance communication, typical applications include Secure Digital cards and liquid crystal displays.

SPI devices communicate in full duplex mode using a master-slave architecture with a single master. The master device originates the frame for reading and writing. Multiple slave-devices are supported through selection with individual chip select (CS) line.

The SPI bus specifies four logic signals:

- SCLK: Serial Clock (output from master)
- MOSI: Master Output Slave Input (data output from master)
- MISO: Master Input Slave Output (data output from slave)
- CS: Chip Select (active low, output from master)

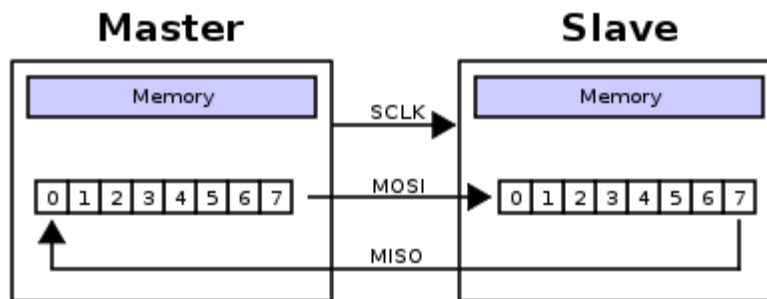


Figure: A typical hardware setup using two shift registers to form an inter-chip circular buffer

Data transmission:

To begin communication, the bus master configures the clock, using a frequency supported by the slave device, typically up to a few MHz's. The master then selects the slave device with a logic level 0 on the select line. During each SPI clock cycle, a full-duplex data transmission occurs. The master sends a bit on the MOSI line and the slave reads it, while the slave sends a bit on the MISO line and the master reads it. This sequence is maintained even when only one-directional data transfer is intended.

Data is usually shifted out with the most significant bit first. On the clock edge, both master and slave shift out a bit and output it on the transmission line to the counterpart. On the next clock edge, at each receiver the bit is sampled from the transmission line and set as a new least-significant bit of the shift register. After the register bits have been shifted out and in, the master and slave have exchanged register values. If more data needs to be exchanged, the shift registers are reloaded and the process repeats. Transmission may continue for any number of clock cycles. When complete, the master stops toggling the clock signal, and typically deselects the slave.

2.3 MEMORY CHIPS CARD

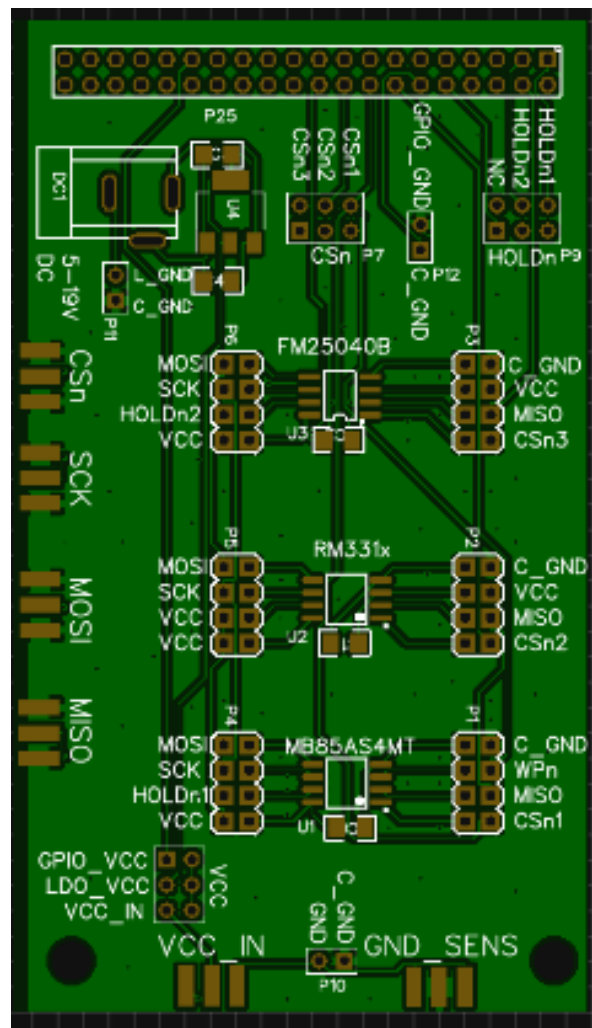
First equipment in the Current analysis Setup is the memory chips card, this card is the target of the current analysis attacks, we attached the scheme as it was provided, the card designed to support 3 memory chips which work with SPI.

The Datasheet for memory chips we tested in the research can be found in the project report GitHub link.

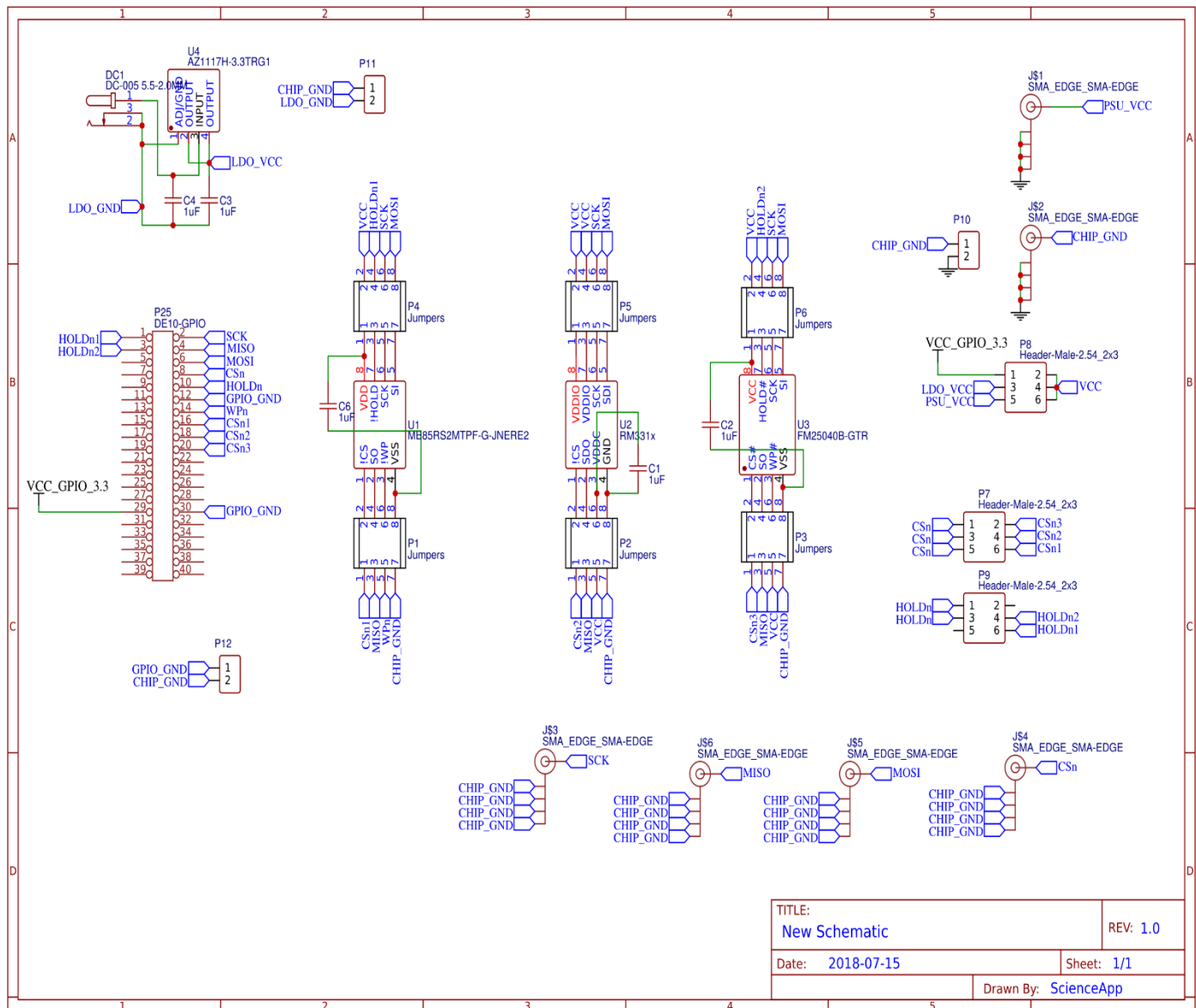
FUJITSU

MICROCHIP

CYPRESS
EMBEDDED IN TOMORROW™



Current Analysis Attacks on various of-the-shelf Emerging Memory Technologies



3. CURRENT ANALYSIS SETUP EQUIPMENT

3.1 CURRENT ANALYSIS SETUP REQUIREMENTS

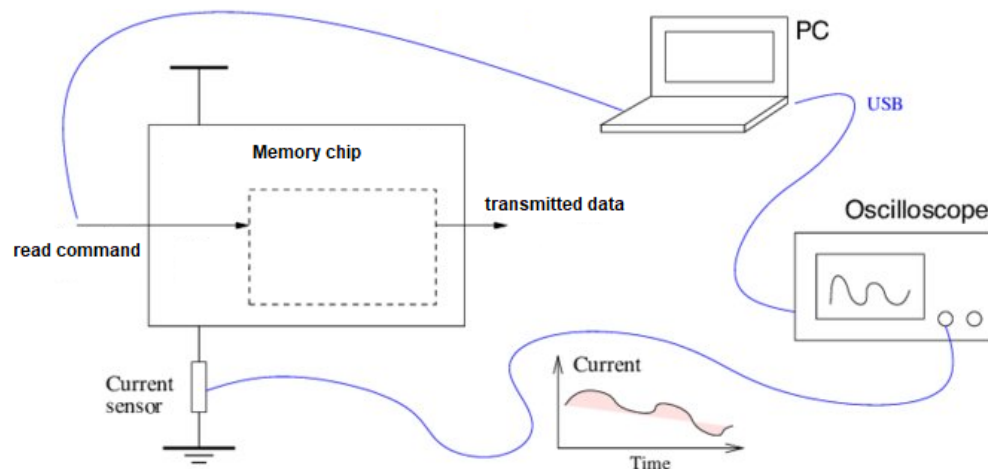
Motivation: characterizing advanced devices and evaluating low-power devices are challenging tasks; ones that require engineers to measure high-speed (over 1MHz) and low-level dynamic current (below 1 μ A)

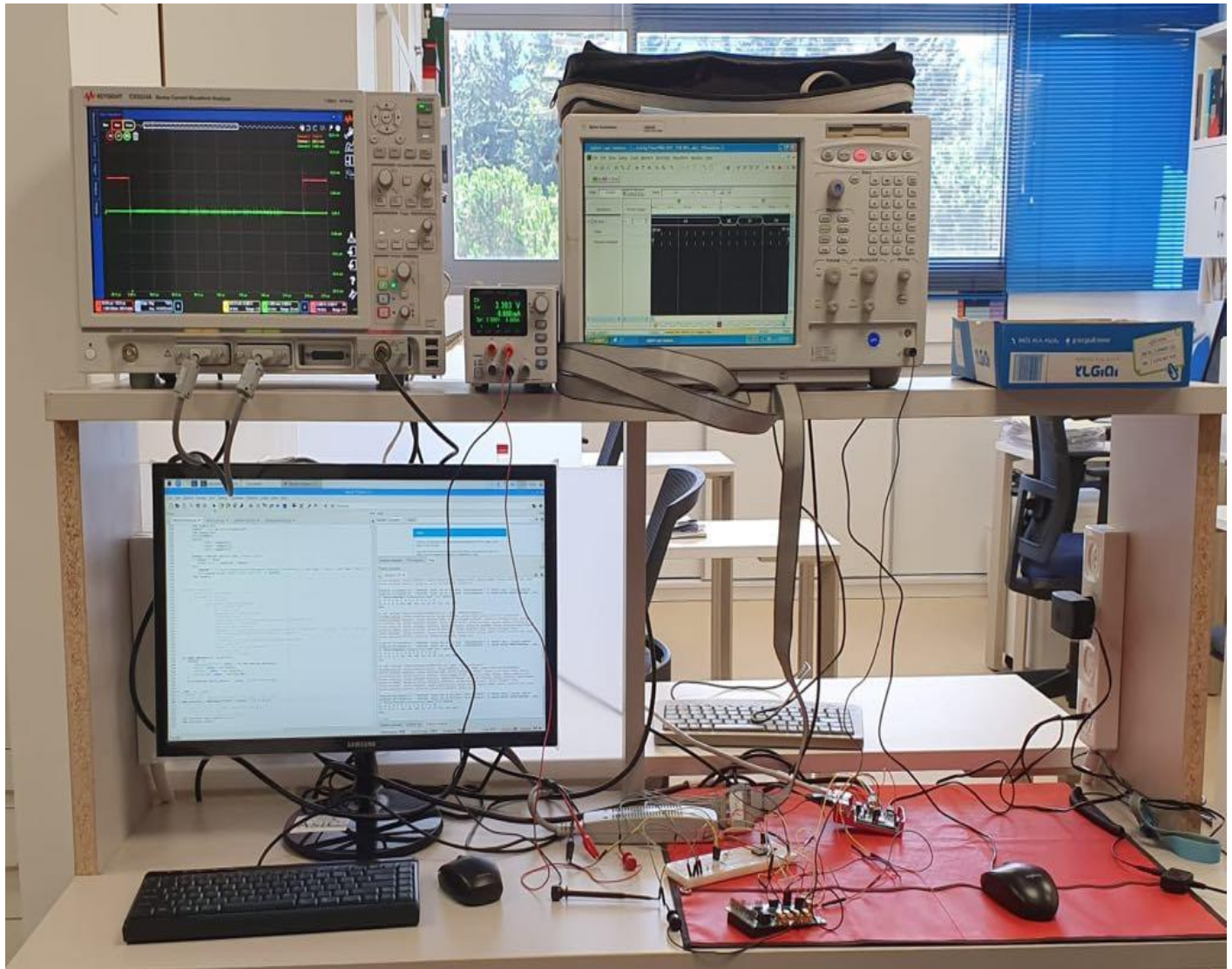
Setup requirements:

- High resolution sampling
- Free Noise
- Programmable trigger
- Support various memory chips
- Debugging and verifying
- Collecting large number of traces
- Power analysis tools

Open issues and solutions:

- SPI communication.
- Debugging combined communication.
- Debugging setup circuits.
- Supporting different input voltage levels.
- Verifying traces.
- Traces denoising.
- Advanced Triggering in order to sample targeted intervals.





3.2 KEYSIGHT CX3300 Device Current Waveform Analyzer

The Keysight CX3300A series is an all-in-one measurement and analysis solution to solve your power rail, power delivery network, and power integrity challenges. The CX3300A series integrates an oscilloscope's bandwidth and sampling rate, a DMM's sensitivity, and data logger's extended duration measurement recording to reveal accurate current and voltage waveforms. The CX3300A's Waveform Analytics feature accelerates characterization, validation, and debugging on mainframe and PC.

Important Features for the research:

- Supports a minimum of 100pA level dynamic current measurements with a maximum of 200 MHz bandwidth, 1GSa/s sampling rate and 14 - or 16-bit wide dynamic range.
- Waveform analytics, current profiler and more efficient analysis functions on mainframe and PC
- Supports a Lan port for local network communication.
- Supports Aux-trig-in for external triggering.
- Supports up to 4 probe connecting slots.
- Long-duration measurement capabilities up to 100 hours maximum

Aside from using this Device we took time to determine which probe should be connected, our understanding of the requirements led us to choose **the probe CX1102A with sensor head CX1205A**

Key features of the probe:

- Supports a minimum of 40nA level dynamic current measurements with a maximum of 100 MHz bandwidth
- Supports up to 12 voltage.

For further info about choosing the right probe please refer to:

<http://literature.cdn.keysight.com/litweb/pdf/5992-1434EN.pdf>

3.3 KEYSIGHT DC POWER SUPPLY

A power supply is an electrical device that supplies electric power to an electrical load. The primary function of a power supply is to convert electric current from a source to the correct voltage, current, and frequency to power the load.

Our main purpose of using power supply is to separate the supply of the power input to the chip, in order to keep a clean, low noise as possible.

Level shifter - TXS0108E 8-Bit Bi-directional

A level shifter in digital electronics, also called logic-level shifter or voltage level translation, is a circuit used to translate signals from one logic level or voltage domain to another, allowing compatibility between ICs with different voltage requirements, such as TTL and CMOS. Many modern full featured systems use level shifters to bridge domains between processors, logic, sensors, and other circuits. In recent years, the three most common logic levels are 1.8V, 3.3V, 5V, though other levels exist above and below these voltages too.

The memory chips operate at different logic levels, we use this device in order to level shift to the appropriate required level.

3.4 APPLIED MATERIALS LOGIC ANALYZER

A logic analyzer is an electronic instrument that captures and displays multiple signals from a digital system or digital circuit. A logic analyzer may convert the captured data into timing diagrams, protocol decodes, state machine traces. Logic analyzers have advanced triggering capabilities and are useful when a user needs to see the timing relationships between many signals in a digital system.

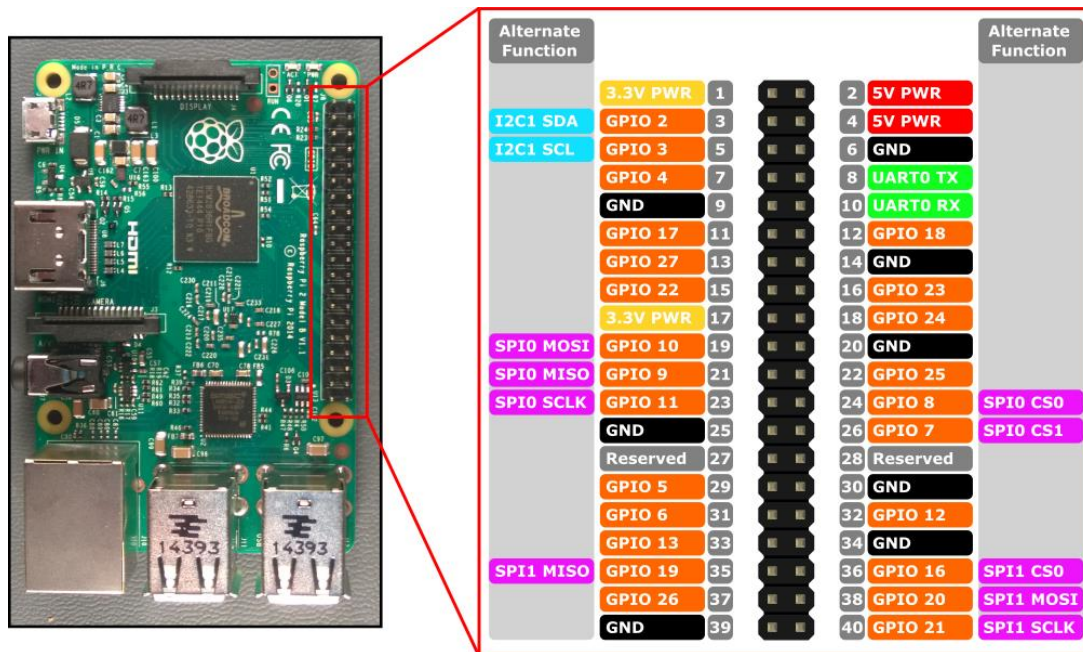
We have used this device for debugging/validating the setup, checking connectivity and for its Triggering capabilities as we will explain in the next sections.

3.5 COMPONENT 3 – SPI MASTER RASPBERRY PI

The Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor and uses a standard keyboard and mouse. It is a capable little device that enables people to program in languages like Python. It's capable of doing everything you'd expect a desktop computer to do, from browsing the internet to making spreadsheets and programming.

Key features:

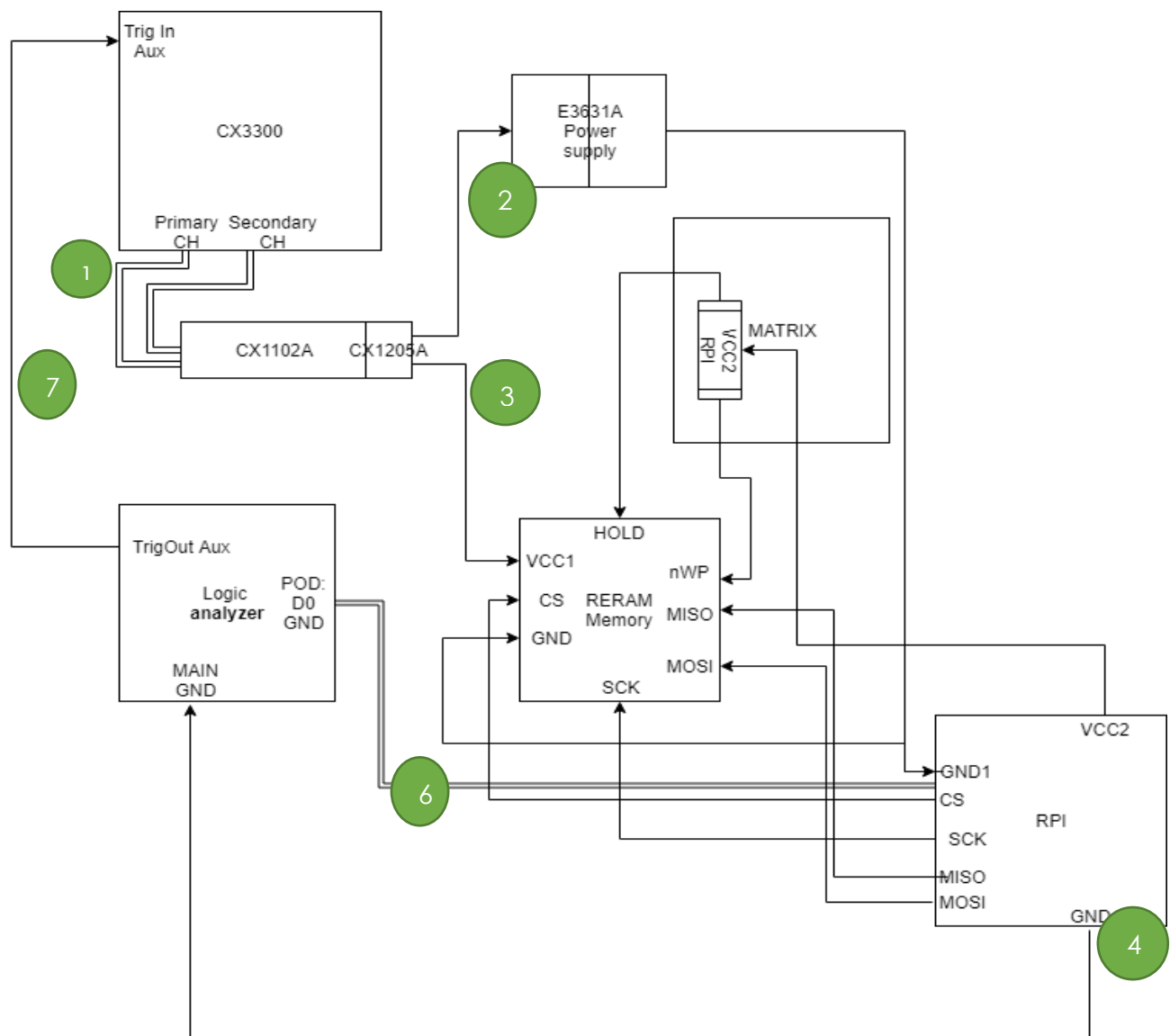
- Supports free open source linux as OS.
- Supports lan Port.
- Supports Direct GPIO interface which supplies the SPI communication.
- Fully supports python 2.7/3.
- Supplise 5V, 3.3V
-



The role of this device is as an SPI master which will initiate the communication with the memory chip, and for Controlling the CX3300A remotely via TCP.

3.5 MANUAL MEASURING PROCESS

RERAM Connecting Diagram:



MANUAL MEASURING PROCESS:

1. Connecting the probe to the CX3300 with both the primary and secondary channel.
2. On one end of the probe we will connect the power supply.
3. On the other end of the probe we will connect to the VCC of the memory chip.
4. Notice that the common GND is the RPI's GND all device should reference to it.
5. Connect wires from the appropriate GPIO pins and into the Memory chip (referee to RPI overview).
6. The CS signal is acting as trigger for logic analyzer to capture the signal and to send external aux trig.
7. The External aux trig out is connected into the Aux trig-in in CX3300.
8. When Hold and write protected function aren't used it's preferable to be connected to VCC.

4. CURRENT ANALYSIS SETUP AUTOMATION

4.1 COMMUNICATION SCRIPTS

Automatic control is the use of various control systems for operating equipment in order to collect and verify large number of traces.

Automation goal:

First step in most of Current analysis techniques is to build large current consumption Databases, in order to use those databases in statistical analyzing.

Databases need to contain all values combinations and various hardware operation, traces need to be verified, sampled at various frequencies.

The main component of the automation process are: CX3300 control libraries, logic analyzer trigger, raspi python automation scripts.

Automation algorithm

1. Preparing Step: filling the memory chip array with all transmitted data combinations.
2. Reading from targeted address + triggering via the Digital Analyzer and getting snapshot.
3. Saving the labeled snapshot.

- “the best documented code is a simple code”
- Object-oriented

Automation Instructions & Libraries – Python

- Python script combine communication protocols
- Serial Peripheral Interface: transmitting and receiving data – memory chips communication.
- LAN communication via VISA: setting commands for current measurement equipment CX3324.

Linux Python Libraries: spidev, time, VISA and TCP/IP.

Python scripts combine RPI built in SPI commands and cx3300 providers libraries:

```
if __name__ == '__main__':
    mem_controller = MemConnect("RERAM", "500000", "132.68.59.9")
    while pattern is not "exit":
        pattern = input("Lets Dance, What pattern You want: ")
        if pattern is not "exit":
            mem_controller.apply_pattern(pattern)
    mem_controller.apply_pattern("OneWrite")
    mem_controller.close()
```

CX3324 control library:

```
class MemConnect:

    def modify4Mem(self, initProtoVal, memSiz):
        self.memSize = memSiz
        self.initWrite = initProtoVal
        print(np.size(self.initWrite))

    def __init__(self, memtype, freq, ip):
        # initiate CX
        self.rm = visa.ResourceManager()
        self.CX3324A = self.rm.open_resource('TCPIP0::' + ip + '::inst0::INSTR')
        self.CX3324A.write(':TRIGger:SEQuence:SLOPe %s' % ('NEGative'))
        self.CX3324A.write(':TRIGger:SEQuence:SOURce %s' % ('EXternal'))
        self.CX3324A.write(':TRIGger:SEQuence:TYPE %s' % ('EDGE'))
        self.CX3324A.write(':TRIGger:SEQuence:ATRigger:STATE %d' % (0))
        self.CX3324A.write(':FORMat:DATA %s,%d' % ('REAL', 32))
        self.CX3324A.write(':FORMat:SORDER %s' % ('COLUMN'))
        self.CX3324A.write(':FORMat:ELEMENTs:TRACE %s%s%s' % ('X', 'Y', 'X,Y'))
        # initiate SPI
        self.spi = spidev.SpiDev()
        self.spi.open(0, 0)
        self.spi.mode = 0b00
        self.spi.max_speed_hz = int(freq)
```

4.3 CURRENT MEASUREMENTS DATABASES

We use the automation process to create a large database of current consumption while the chip performs reading commands, it was important to cover all the data combination of 8 bits (256 combination) each combination the process read from different random 10 memory cells in order to cover all the section of the array memory cells.

We share in the project GitHub link 3 main databases for REAM, SRAM and FRAM.

This database labeled with the suitable label and easy to use for future researches, current analysis attacks or even signal processing tutorials.

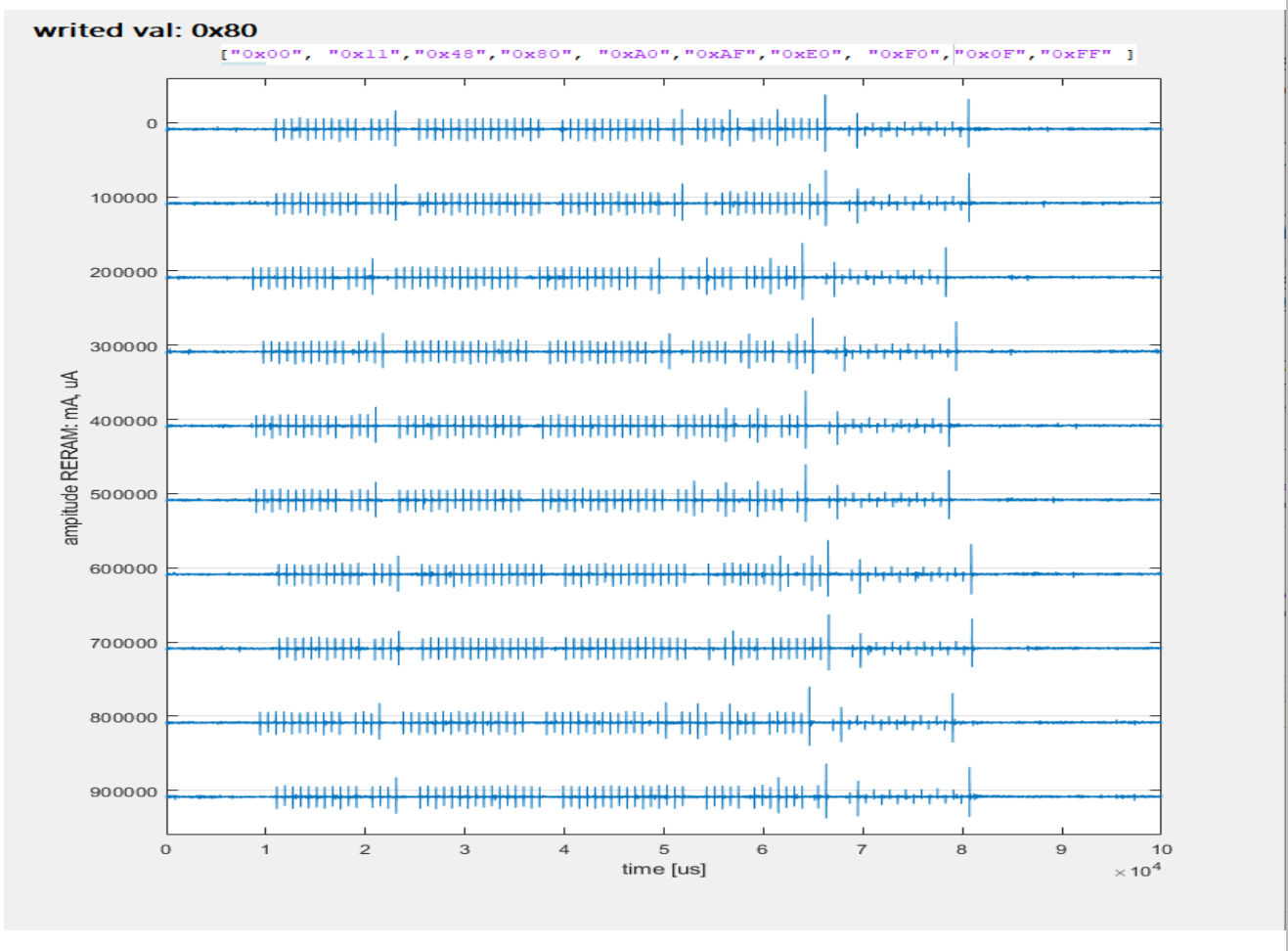
memoryTechnology_transmittedData_Date.csv
example: ReRam_11_17-4.csv

Benefits:

- Understanding: this DB would help better understand the functionality of the chip
- Time Saving: one of the main usages of this DB is to save time for other researches regarding the RERAM
- Verified Contents: Each value was Verified inside the Python script
- Versatile: this DB contains Large number of the RD/WR Traces

Main features:

- Collecting Current supply current traces (Data patterns) and building Data bases
- Verified current measurement traces.
- Traces Sampled at various frequencies.
- Few plots contain voltage measurements for SPI signals.
- Full read Databases for advanced memory chips (data combinations 2^8).
- Full write Databases for advanced memory chips (data combinations 2^8).
- Full write Databases including previous data stored in the target cell.
- Data Bases organization



5. SIMPLE CURRENT ANALYSIS ATTACK

5.1 BACKGROUND

Simple power analysis (SPA) is a side-channel attack which involves visual examination of graphs of the current used by a device over time, variations in power consumption occur as the device performs different operations, for example, different instructions performed by a hardware device will have differing power consumption profiles, often attackers are able to determine what type of function is being performed at a given time.

As a result, in a current trace from a memory chip using Serial Peripheral Interface as communication interface card, we can tell clearly that the chip is selected and receiving data bits. Similarly, the byte of the operation code, bytes of the address and the transmitted value can often be distinguished, enabling an adversary to exploit transmitted and stored data.

Even if the magnitude of the variations in power consumption are small, standard digital oscilloscopes can easily show the data-induced variations. Frequency filters and averaging functions (such as those built into oscilloscopes) are often used to filter out high-frequency components.

5.2 ATTACK GOAL

Simple power analysis considered as first power analysis step which lay the groundwork for more advanced power analysis attacks, as the attacker examines the current traces and build current consumption profiles for the hardware device supported operation, the attacker solidifies deep understanding for the correlation between the device system and its current consumption over time.

5.3 ATTACK STEPS EXPLANATIONS

The attack requires timing and understanding of the operations given for instance writing, reading and Enabling a write. Such understanding would help us close in on the region we want to further investigate. In the picture below, one can notice the four regions as labeled, such conclusion and observation were made after deep understanding of the SPI protocol and reviewing hundreds of measurements.

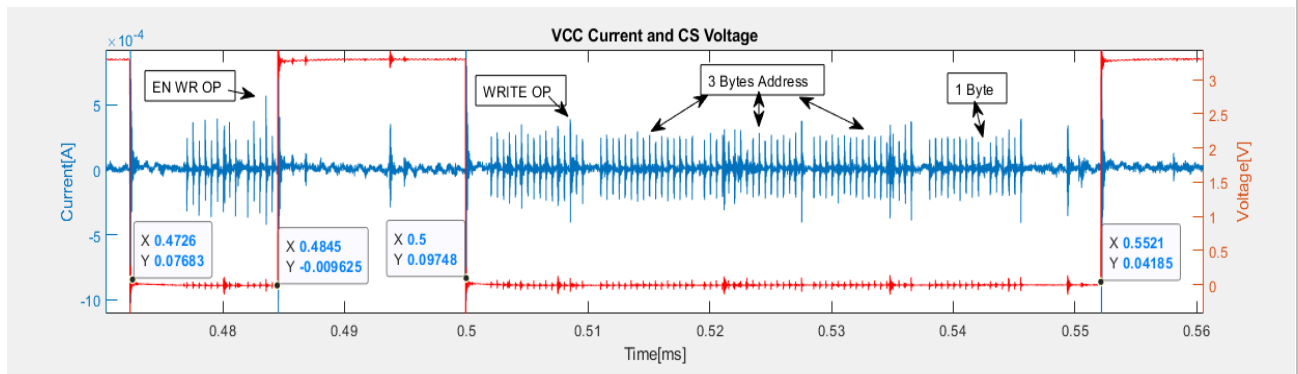


Figure 1 writing 1 byte on RERAM

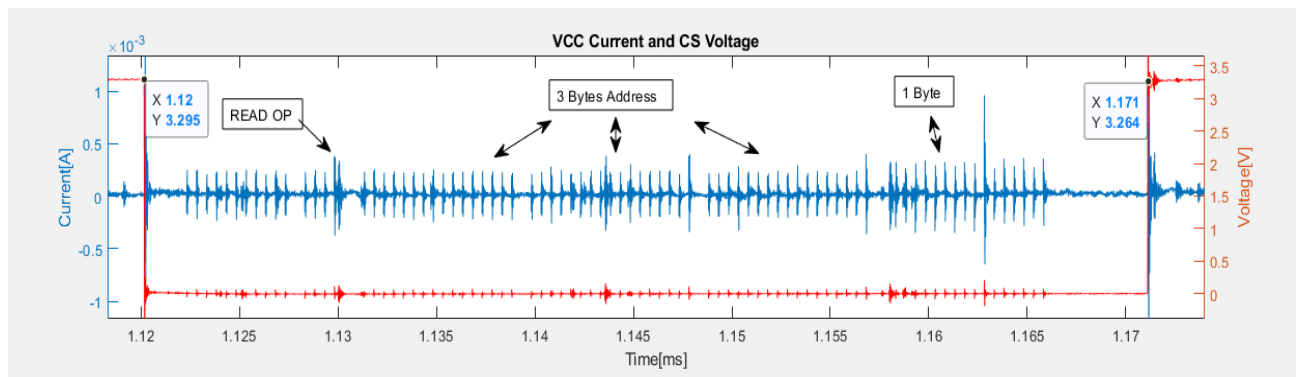
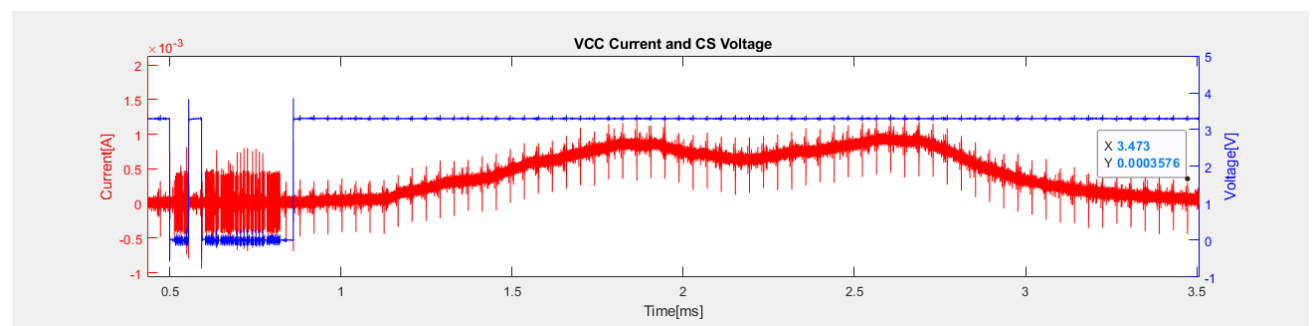


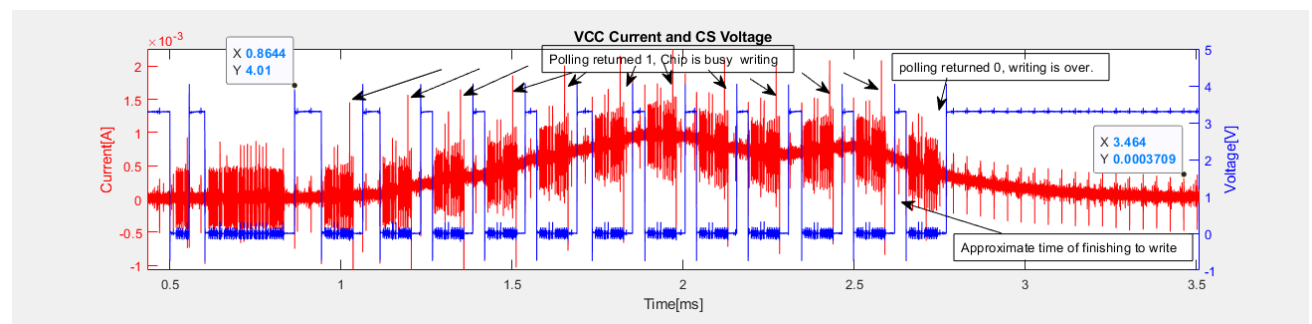
Figure 2 Reading 1 byte from RERAM

Another observation was made on ReRam was the curve that followed the writing op,

Such curve was observed every time we sent a writing op, crossing that with the fact that RERAM uses a writing buffer which adds a delay to writing op, led us to suspect that this is where the writing happens and referred to it as writing in progress area (WIP).



In order to approximate the time took for WIP we have executed a repetitive polling on the writing status in the memory chip itself, As shown below it is clear that the last polling gave in that the writing is over.



5.4 CONCLUSION

Results summaries in a table as conclusion:

memType/op	RERAM	Starts	~Ends
read op	56.94us	trigger by falling CS	stops at raising CS
write op 1B	59.62us	trigger by falling CS	stops at raising CS
WIP 1-byte	588.95us	trigger by falling CS	approximation of WIP polli
enable op	18us	trigger by falling CS	stops at raising CS

Above summary shows that by only giving the op time one could determine the type of the op and how many bytes is it.

6. CORRELATION CURRENT ANALYSIS ATTACK

7.1 BACKGROUND

Electronic devices have two components to their power consumption. First, static power consumption is the power required to keep the device running. This static power depends on things like the number of transistors inside the device. Secondly, and more importantly, dynamic power consumption depends on the data moving around inside the device. Every time a bit is changed from a 0 to a 1 (or vice versa), some current is required to (dis)charge the data lines. The dynamic power is the part that we're interested in - it can tell us what's happening inside. One power model which may be used is the Hamming Weight Power Model. Traditionally, the Hamming weight of a value is the number of non-zeroes. For example, in the binary number 1100 0010 the Hamming weight would be 3. The assumption in using the Hamming Weight Power Model in power analysis attacks is that the number of bits set to 0 or 1 of an output is correlated with the power consumption of a device. The Hamming weight itself is then used as an arbitrary unit to model the consumption of power in a device. Hamming weight units can then be compared to the actual current levels of power traces captured when a device was performing storing operations. This act of comparison is the process of finding correlation between the modelled power unit values and the actual power consumed.

One technique to calculate correlation between the power model and the actual power consumption is to use Pearson correlation coefficient equation. In essence, this equation will take two sets data (W and P) and calculate whether there is a linear (positive or negative) correlation between the two sets of values. We may use this equation to find significance in our power traces since the assumption with the Hamming Weight Power Model is that as the number of 1's increase in our predicted output, so too does the power consumption increase in the actual output (and vice versa).

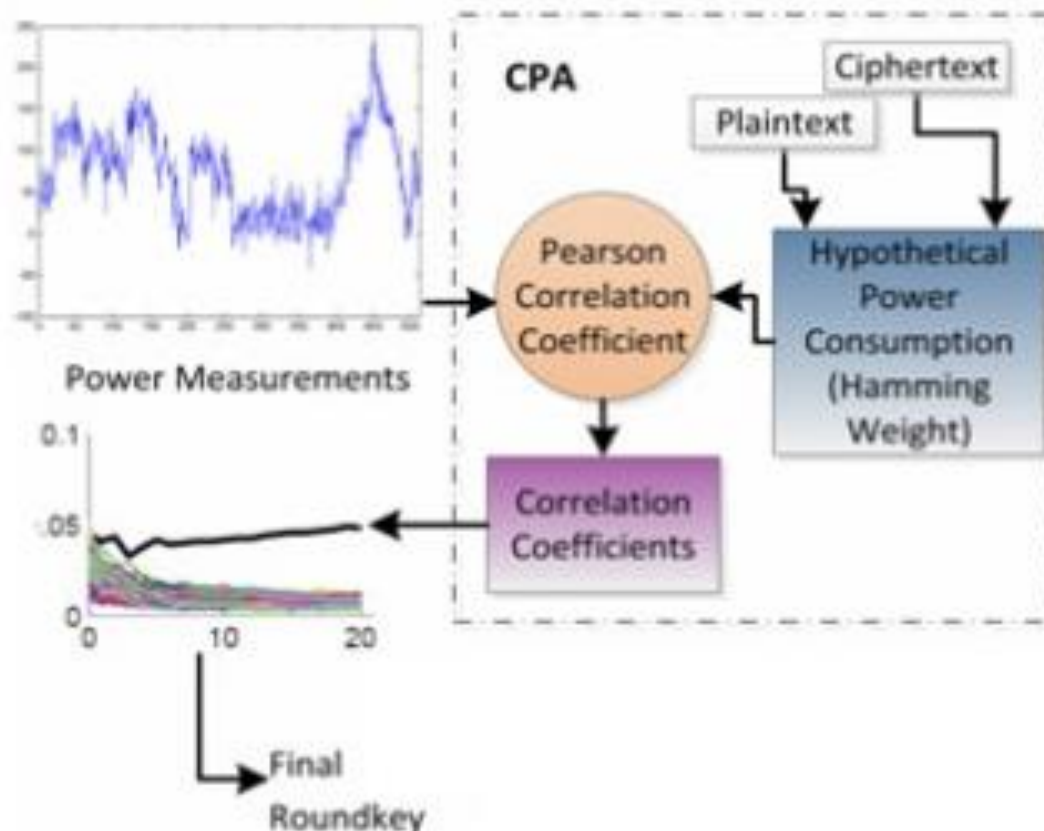
Equation: Pearson's correlation coefficient

$$r_{i,j} = \frac{D \sum_{d=1}^D h_{d,i} t_{d,j} - \sum_{d=1}^D h_{d,i} \sum_{d=1}^D t_{d,j}}{\sqrt{\left(\left(\sum_{d=1}^D h_{d,i} \right)^2 - D \sum_{d=1}^D h_{d,i}^2 \right) \left(\left(\sum_{d=1}^D t_{d,j} \right)^2 - D \sum_{d=1}^D t_{d,j}^2 \right)}}$$

7.2 ATTACK GOAL

In CPA, the goal is to accurately produce a power model of the device under attack. During an attack, the aim is to find correlation between a predicted output and the actual power output of a device. If the power model is accurate then a strong correlation should be demonstrated between the predicted output and actual output. If this correlation is found then, similar to DPA, gathering a large number of traces will enable one to show that the correctly predicted cipher key will demonstrate the highest level of correlation.

For this section the main goal is to exploit the “Hello World!” string that has been stored in RERAM memory chip by performing correlation current analysis on the current consumption while reading the string bytes one by one.



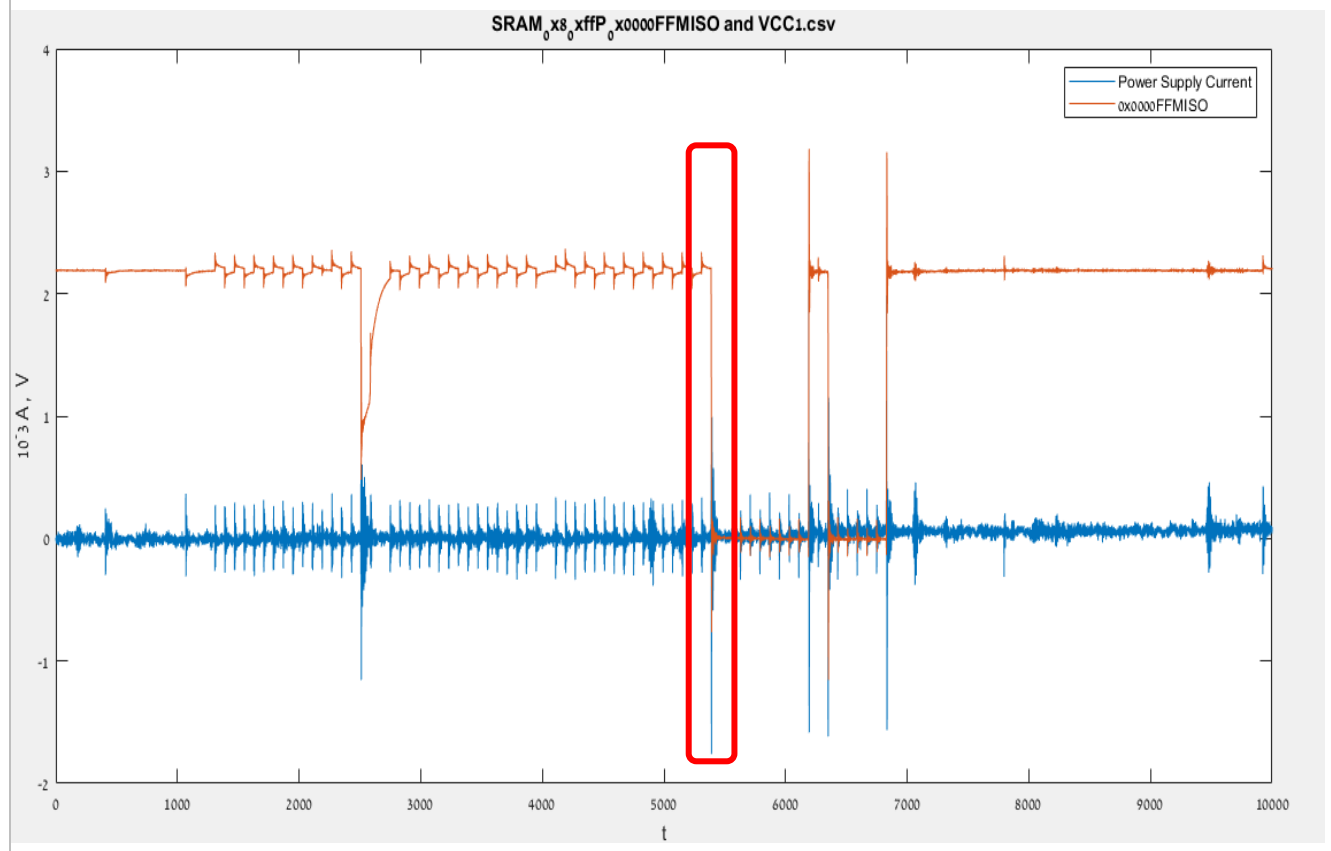
7.3 ATTACK STEPS EXPLANATIONS

As first, we explain why correlation current analysis is the suitable technique to the task we are trying to attack and why would this technique allow us to obtain stored values:

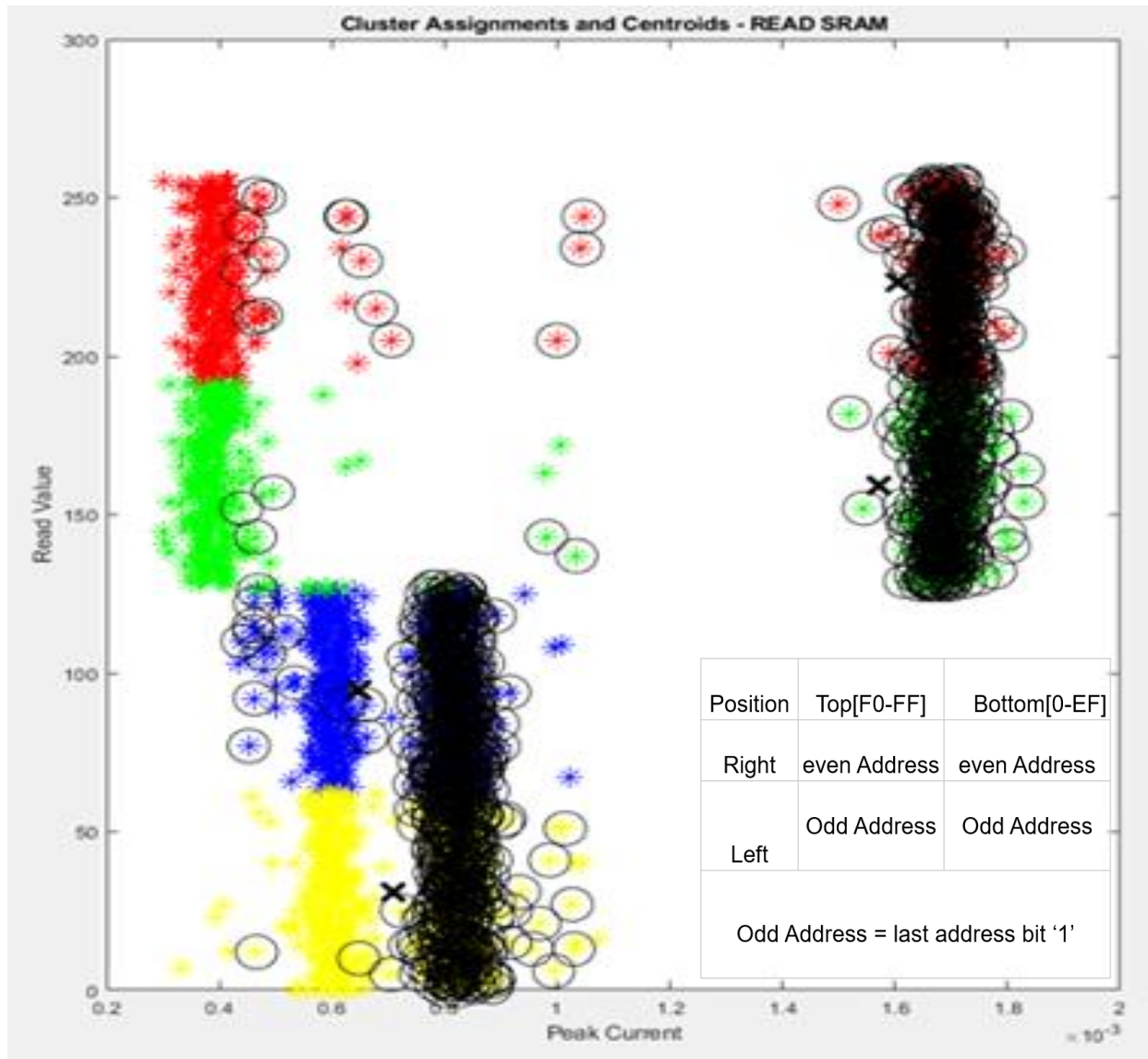
To prove that we suggest the following, the aim is to find correlation between a predicted output and the actual current consumption of the device, we sample all the database which we suggest in the automation section at a very specific point of time:

Point of Time between: receiving last address bit and outputting the transmitted value.

In the figure below the orange signal is the Master In Slave Out Voltage and in blue is the current overall consumption of the chip over time.



We sampled all the database traces at this point of time and fill an array with the current overall consumption, we use KNN clustering algorithms to visualizes and analysis the outcome, we see an interesting result in the figure below:



Y-axis: transmitted value (0X00 - 0XFF), X-axis: current consumption.

Conclusion:

The current measurement at the point of time which we indicated the parallel data access is indicating an accumulation of:

- Processing last bit of Address.
- Accessing the suitable memory cells.
- **Rising/failing the output in order to output the MSB (first bit) of the data.**

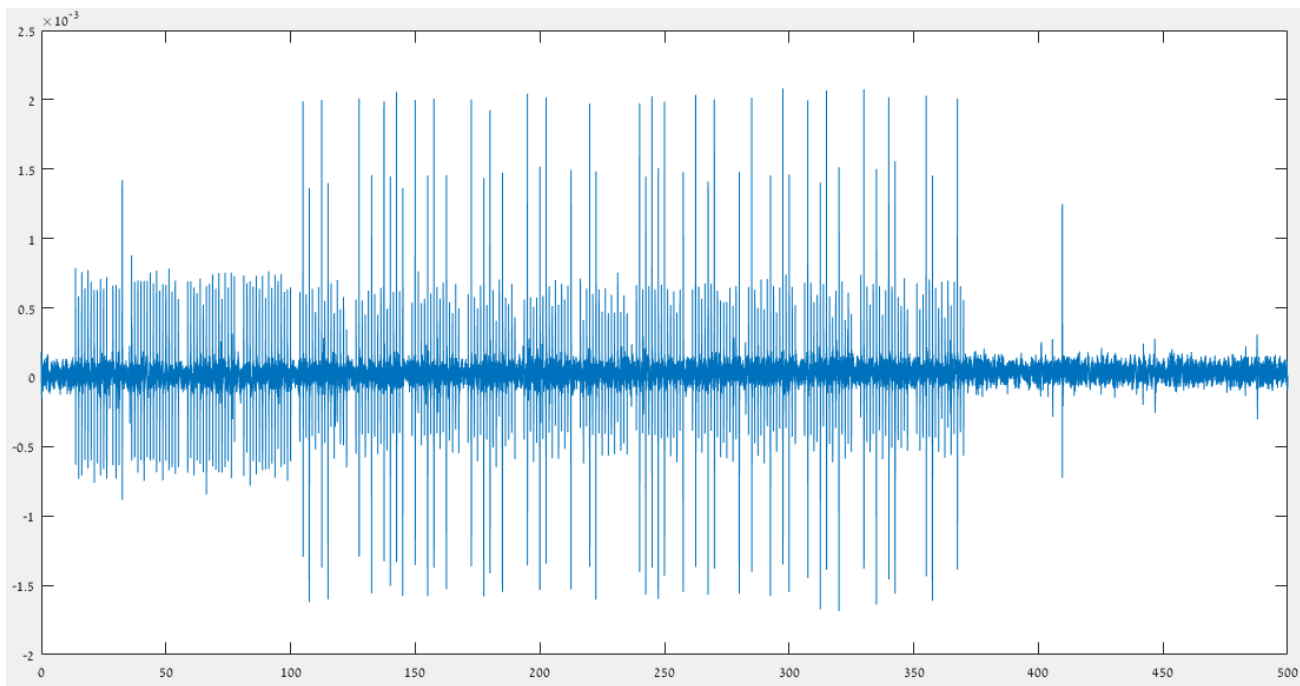
In other words, we find correlation between the predicted MSB bit of the output and the actual current consumption and we find correlation between the sampled bits in the input interface of the chip and the actual current consumption, therefore we are able to perform an attack of correlation current analysis.

Now we can start the attack, first step is extracting the feature we interested in from the large database, this pre proccing saves time in the actual passive attack, the feature we interested in is as we explained above is the 16 spices of current consumption of the chip while outputting the transmitted data to the master.

We get after the pre proccing an array with 2560 rows and 16 columns We search for max correlation and this array is our reference.

FIRST STEP

In the figure below, we can see the current consumption of the chip while performing read command from 12 memory cells, again the first 16 current spikes are for the command next 24 * 16 spikes are the address and each 16 spikes after that are for one byte, technologies we gain from the simple power analysis, the transmitted string is: Hello World!



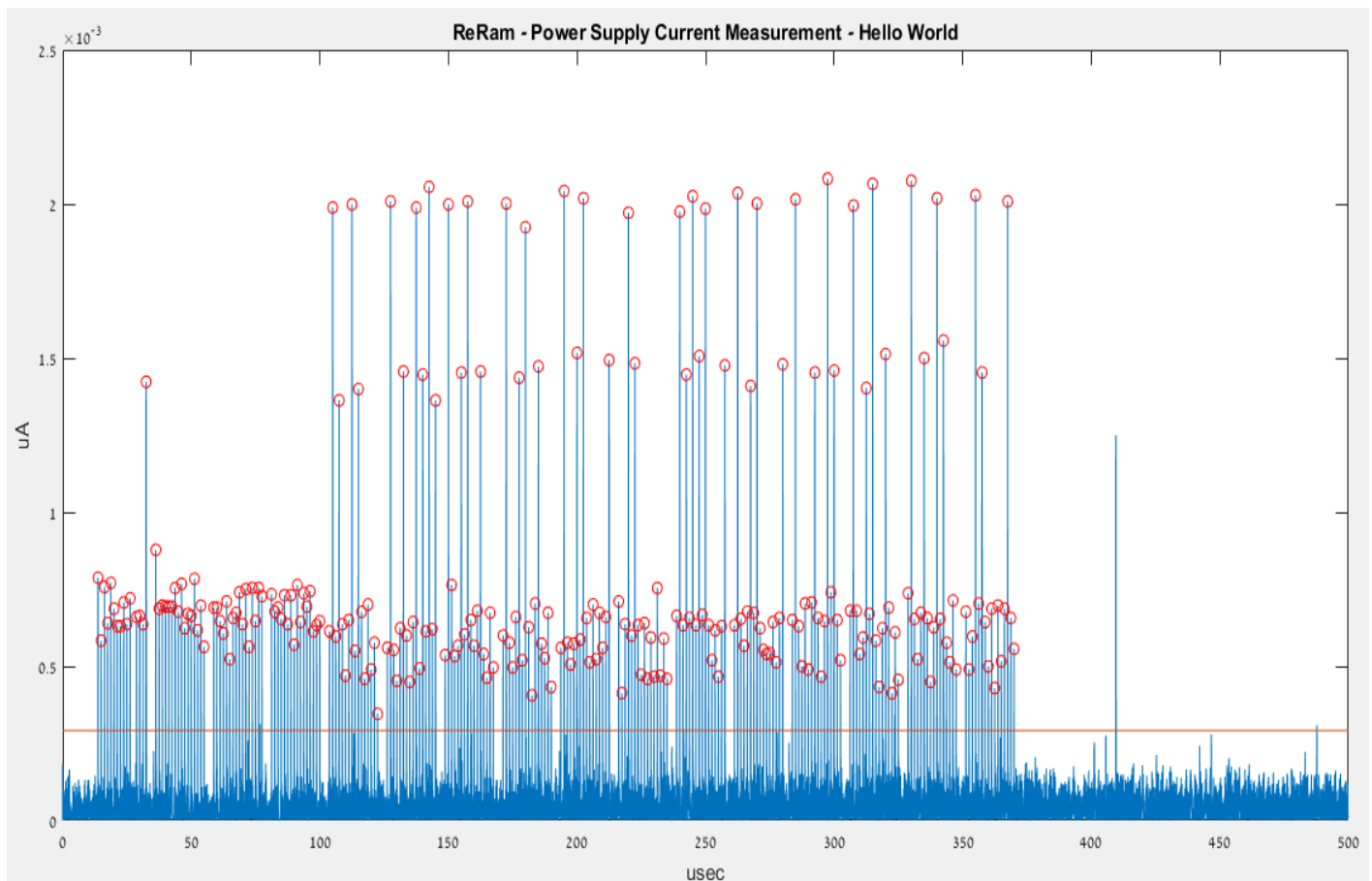
```

3  %%
4  % Reading data %
5  Array_Reram=csvread('RERAM_HelloWorld.csv',1);
6  x=linspace(0,500,length(Array_Reram));
7  figure;
8  plot(x,Array_Reram);
9
10 %%
11 %sample the postive values
12 x_pos = x(find(Array_Reram>0));
13 Array_Reram_postive = Array_Reram(find(Array_Reram > 0));
14
15 %%
16 %find signal peaks
17 [Array_Reram_pks,locs] = findpeaks(Array_Reram_postive,'MinPeakDistance',100);
18 mean_peaks = mean(Array_Reram_pks);
19 figure;
20 plot(x_pos,Array_Reram_postive,x_pos(locs), Array_Reram_pks,'or');
21

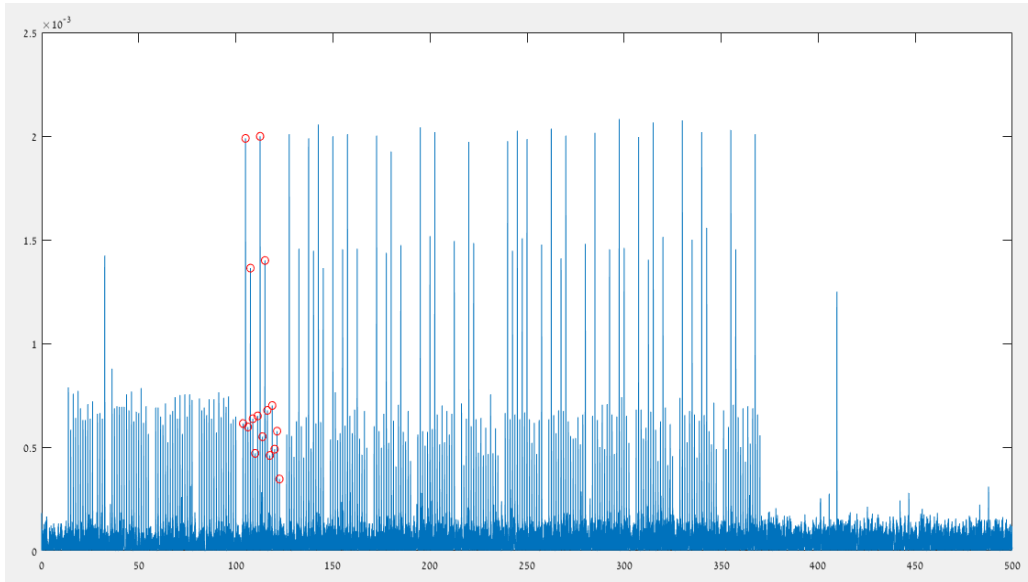
```

SECOND STEP

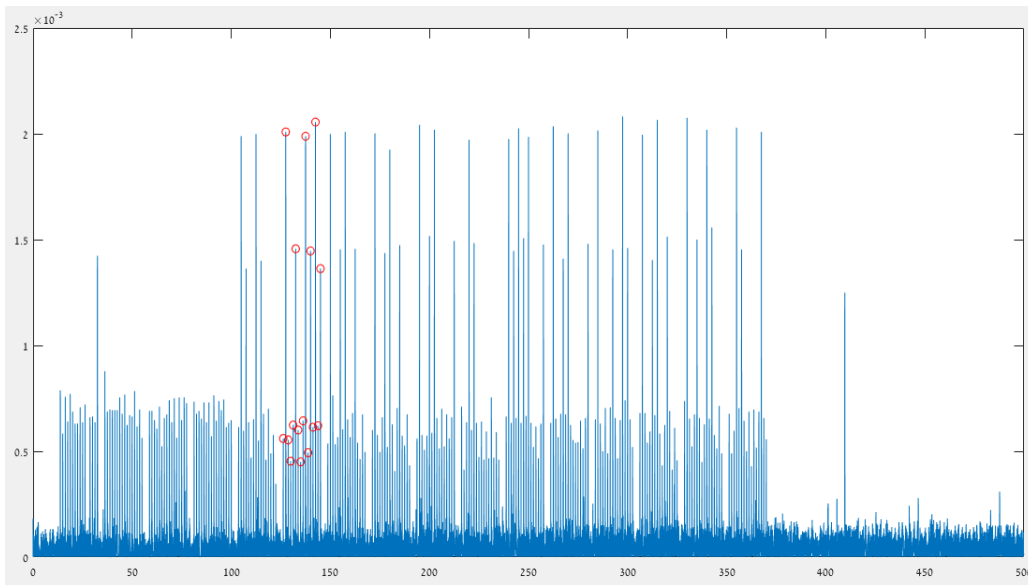
We run the MATLAB script above on the current consumption trace, the main function are get positive and get peaks, in the figure below we can see that we filtered the signal to the wanted data only and we manage to circle with read the current spices we search for, the next step will be to split each 16 current spices of 1 byte in order to compare them with the database features array and search for max correlation.



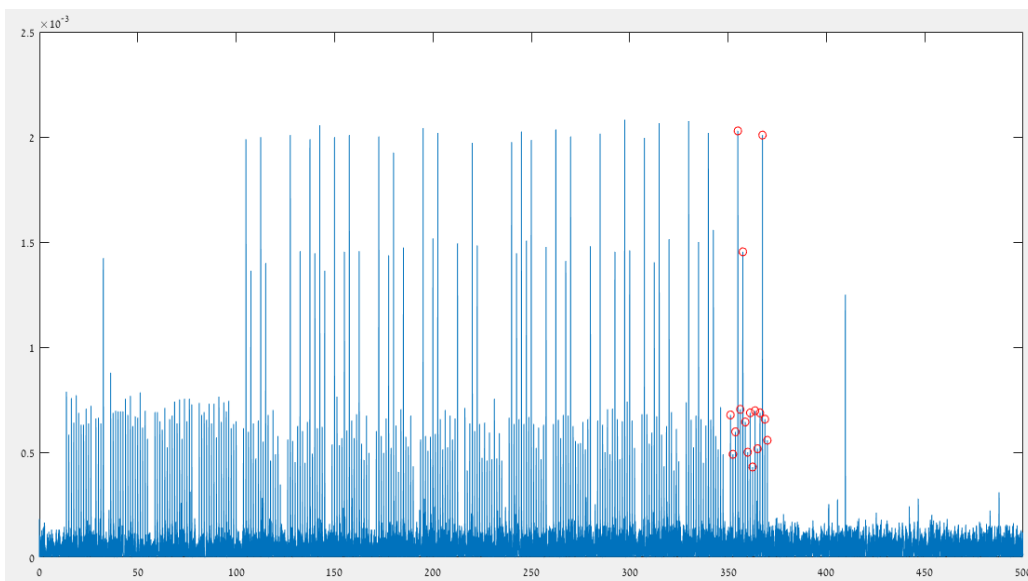
Current Analysis Attacks on various of-the-shelf Emerging Memory Technologies



In the first figure we can see how we manage to circle with red the first 16 current spices of the first data byte, this byte as we already know is the latter H.



In the next figure we can see how the MATLAB script move to next data bytes and split and save the current consumption spices till the 12th byte.



THIRD STEP

At this point of the attack we got to main arrays:

- Array [2560X16] the feature extracted from the current consumption database
- Array [12X16] the feature extracted from the current consumption of the target string

We run the below MATLAB script which manage to perform Pearson formula of correlation between each row of the two arrays, the output of this script is an array [12X2560], in other words for each byte of data in the string we have the outputted correlation with all the rows of the database.

We search of the 10 max correlation for each byte and we predict that the target byte is the most repeated letter among those 10 results.

```
51 %% find max corr between target signal and database peaks
52 %
53 - for target_index = 1 : 12
54     % find corr between target signal and database peaks
55 -     for n = 1 : 2560
56         tmp_pattren_peaks = Array_database_peaks(:,n);
57         rho = corr(target_peaks(1:end-1,target_index),tmp_pattren_peaks(1:end-1));
58         corr_array_results(n) = rho;
59     end
60
61     %find hypothesis target string by finding max corr
62 -     [max_values,max_indexes] = sort(corr_array_results','descend');
63     hypo = max_indexes(1:10);
64 - end
65
```

LAST STEP – THE PREDICTED STRING

```
>> corr_find_reram
```

```
ans =
```

```
'!!!!!!!!!!'
```

```
ans =
```

```
'dddddddddd'
```

```
ans =
```

```
'|||||'
```

```
ans =
```

```
'rrrrrrrr'
```

```
ans =
```

```
'oooooooooooo'
```

```
ans =
```

```
'WWWWWWWWWWWW'
```

```
ans =
```

```
'      '
```

```
ans =
```

```
'oooooooooooo'
```

```
ans =
```

```
'|||||'
```

```
ans =
```

```
'|||||'
```

```
ans =
```

```
'eeeeeeeeeeee'
```

```
ans =
```

```
'HHHHHHHHHHH'
```

```
target_hypo_data =
```

```
12×1 string array
```

```
"H"
```

```
"e"
```

```
"l"
```

```
"l"
```

```
"o"
```

```
" "
```

```
"W"
```

```
"o"
```

```
"r"
```

```
"l"
```

```
"d"
```

```
"l"
```

7. PREVENTING CURRENT ANALYSIS ATTACKS

7.1 BACKGROUND

Many techniques to prevent SPA and DPA attacks have been proposed in the academic literature making power analysis attacks a real threat on commercial hardware, and software.

Power analysis attacks cannot generally be detected by a device, since the adversary's monitoring is normally passive. In addition, the attack is non-invasive. As a result, physical enclosures, auditing capabilities, and attack detectors are ineffective. Instead, hardware system engineers must ensure that devices' power variations do not reveal information usable by adversaries.

Simple power analysis can easily distinguish the outcome of conditional branches in the execution of hardware system, since a device does different things (consuming different power) depending on whether the conditional branch is taken. For this reason, care should be taken to ensure there are no secret values which affect the conditional branches within hardware system implementations. Other sources of variation, current consumption variations in the serial and parallel converters in the input on the output pins of the memory chips, in this manner we can suggest technique to prevent simple power analysis on this kinds of converters which we introduced earlier, the idea of the technique is to consume the same current consumption I case sampling logic one and logic zero in the input interface.

Differential power analysis is more difficult to prevent, since even small biases in the power consumption can lead to exploitable weaknesses. Some countermeasure strategies involve algorithmic modifications such that the hardware system operations occur on data that is related to the actual value by some mathematical relationship that survives the system operation. One approach involves blinding parameters to randomize their value. Other countermeasure strategies to reduce the effectiveness of DPA attacks involve hardware modifications: varying the chip internal clock frequency has been considered to desynchronize electric signals, which lead in return to algorithmic enhancements of traditional DPA.

In our research we showed that the hardware system is consuming large current consumption that mask the biases in the power consumption that we searched for, therefore we are not able to suggest a countermeasure to DPA.

In next section we introduce and suggest countermeasures to prevent Correlation Power Analysis.

7.2 DECODING METHOD

To prevent side-channel attacks, we have two choices: we must either reduce the release of current consumption information that could be used to launch an attack, or we must make it impossible for an attacker to link information about what the chip is doing with specific compute operations. For example, a computer engineer may want to change the order of operations used on data within the system by using a process called randomization to make it more difficult for an attacker to launch a side-channel attack.

Another preventative technique we may use is to increase the amount of noise in a channel. An increase in noise means an attacker will have to collect more measurements than is needed and not all the information will be relevant. Faraday cages can also be used to reduce current leaks.

In the research we suggest in addition to those steps a decoding method to decode the transmitted data, decoding the data will make it impossible for the attacker to obtain the decoded value even when the attacker perform an successful current analysis attack.

The decoding method rely on decoding each value with the value that give the most correlation result in the previse attack for example:

Letter H:

```
= char_hypo
```

```
' ^ ^ HHHHHHHHHHOOPOOOOOO '
```

```
= char_decode_near
```

```
' O '
```

We also are able to explain why letter H and 0 have max correlation, this because the output component raises the voltage almost in the same time.

We suggest this decoding method because attacker with an average current analysis side channel setups won't notices the similitude between those values and our advanced setup we suggested earlier has a wide dynamic range and is able to notice this high correlations.

This method isn't recommended in cyber security manners and it is consider as weak cyber defense because the method don't contains random keys or other cyber feature.


7.3 ENCRYPTION ALGORITHMS

In addition to the decoding method we suggest above we suggest for computer engineers which design their systems and add memory chips that use serial to parallel interface, to use an encryption software algorithms in the master unit in the system, encryption software algorithm will make it impossible for the attacker to obtain the decoded value even when the attacker perform an successful current analysis attack.

We suggest AES-128.

This countermeasure considered as strong cyber security method because AES-128 is very hard to break.

Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)

Owen Lo , William J. Buchanan & Douglas Carson

Pages 88-107 | Received 29 Aug 2016, Accepted 30 Aug 2016, Published online: 19 Sep 2016

Although there are large number of researches today which suggest different techniques of power analysis attacks to break AES, our method still safe because all the researches rely on attacking the unit which compute, generate the random keys and encrypt with it, and is not our case we suggest in advanced CPU unit and not in the memory chips that we consider as targets.

The report attached with project GitHub link:

<https://github.com/CurrentAnalysis/Project.git>

For more code and documentation.