Deriving cryptographic keys via power consumption

Roman Korkikian
Запустите виртуальную машину, вы должны увидеть терминал с тремя вкладками и редактор (тоже с несколькими вкладками).

Перейдите в редактор и откройте вкладку Task1 она нам потребуется в дальнейшем (если у вас нет распечатки).

Все слайды есть на флешках. Откройте, если вам не видно на проекторе.
What this workshop about?

Рома

Ты

Questions during/after and instead of workshop.
Who am I?

Roman Korkikian
What this workshop about?

The workshop agenda:
1. Hands-on theory (you will execute couple of commands). During this part I will not come to help you. I will help you after theory.
2. Theory (1-2 hours).
3. Practice (1-2 hours) so you may leave if you don’t want it to do.
What this workshop about?

The workshop goal:

Atract you interest with side-channel attacks.
The workshop is about side-channel attacks:

**how to extract the cryptographic key using physical data**
What this workshop about?

The workshop is about side-channel attacks:

how to extract the cryptographic key using physical data

Sounds crazy?
PART 0. Power trace acquisition
Each electronic device require power to perform computations.

Typical power supplies are 0.95 – 1.8V depending on the technology.

During the work electronic device drains current to the ground, transforms energy and etc, i.e. device consume power.
Power traces acquisition

https://github.com/kokke/tiny-AES128-C/blob/master/aes.c
Power trace plotting

AES algorithm
Power trace explanation

Изменение входного напряжения STM8 при работе алгоритма AES
Start Virtual Machine and open folder:

Desktop/DPA_Workshop/AES_STM8_Example

There should be file Task1 – open the file and follow all the steps (7-13) to plot power curves.
Power traces acquisition
• AES is a particular algorithm:
  • 11 Key mixing operations;
  • 10 Sbox and Shift rows operations;
  • 9 MixColumn operations;

• Hence from power trace we can understand where each operation took place.
Power trace explanation

Изменение входного напряжения STM8 при работе алгоритма AES
• AES engine acquisition:
  • 10,000 plaintext/ciphertext pairs and corresponding power trace during encryption are available in folder data.
• We clearly see that AES algorithm reveals its operation via power consumption.
• What we will do with all of that previous information?! EXTRACT THE KEY!
• Key extraction:
  • We build simple power models that depend on the key byte and know information and then we try all the bytes and among them we will choose the correct one.

• Let's come back to Virtual Machine and continue Task 1 (items 14 to 17).
Power trace explanation
Power trace explanation
Power trace explanation

Изменение входного напряжения STM8 при работе алгоритма AES
Steps 14 to 17 computes relationship between power traces and the first byte of the last round state:

\[ S_{10} = InvSbox[C \ xor K_{10}] \]

- \( S_{10} \) is used twice in a program –
  - first time \( S_{10} \) is obtained after AddRoundKey
  - second time \( S_{10} \) is read from the memory to compute \( Sbox[S_{10}] \).
• We were correlating first byte of the key. Now I want you to rewrite two numbers in the code so you will correlate another key byte.
• Do the Task1 from lines 18 till 25.
• Check the position of the pike – it shall move.
Power trace explanation

- "pcc_lr_realsec_n10000_hw.d"
- "pcc_lr_realkey_n10000_hw_wr.d"
- "powTrace10.d" using 0:2
So in this workshop I will try to explain:

- Why and how power consumption leak binary information.
- How to build simple power consumption models based on binary data.
- How to search for a key.
PART 1. The truth is out there…*  

* This part is boring, don’t not fall asleep
Intuition lies

- R. Pacalet
Examples of side-channels

Examples of side-channel techniques that YOU KNOW FROM SCHOOL
Examples of side channels: model of the atom
Examples of side channels: volume definition
Examples of side-channels

• Side channel techniques – are the methods that allow characterize object’s properties by observing reaction and feedback of other objects.

• For cryptography – side channel attacks are the attacks that use physical information to extract binary data.
How binary and physical data are linked?
Algorithms are just physical signals

Computing machinery

Computing is a physical process

To perform computations energy has to be spent irreversibly
CMOS (electronic) devices consume electrical power, but also transform energy to other observable types of side-channel.
Side channel leakages
Power consumption
Power consumption

- Hardware works from frequencies from several MHz till several GHz.
- Power consumption shall be measured accordingly (sampling rate may be smaller than the actual frequency).
- Use fast digital oscilloscopes.
- In our case the bandwidth was 250 MHz with microcontroller running at 16 MHz.
Power consumption

- Home setup.
- Bandwidth up to 250 MHz, sampling 10 GHz – can attack up to 500 MHz devices.
  - 1.8K $

- Industrial setup.
- All type of devices
  - >30K $
• Roughly speaking power consumption is a measure of current/voltage needed for the correct device work – at different moments of time current that flows through the device will be different.

• We consider CMOS systems – they consume power only on transaction.
Let's keep it simple:
each hardware is based on **registers** (and logic), registers consume a lot of power on transaction when 0 overwrites 1 or 1 overwrites 0.
Power consumption: D flip flop

- D flip flop consumes power on clock’s edge.

- Lets see small gif
Power consumption: D flip flop

- Flip flop power consumption on D input transaction
Power consumption in microcontroller
Power consumption

Different instructions – different impedance/path/power consumption
Power consumption
Power consumption

• Well... registers consume power but the rest of the circuit also consumes a lot (even more than one register).

• What to do?
Mathematics behind side channel attacks
• Consider a small example:
  • Two asset values 2 and 1.
  • Each time asset value is returned a significant noise is added:
Mathematics

We know asset values, but we don’t know its appearance

Guess 1: sequence of two asset values
Red is 2
Blue is 1

Guess 2: sequence of two asset values
• Take all, average and extract:
  • Mean(red bars) – mean(blue bars) approximately 1

• For guess 1 this difference is equal to 1.042
• For guess 2 this difference is equal to -0.297
• Why?
• Law of large numbers (check wiki): the average of the results obtained from a large number of trials should be close to the expected value, and will tend to become closer as more trials are performed.
Mathematics

- Asset values 0 and 1
- Noise is Gaussian with mean 128 and variance of 78
- Average for asset value 1 will converge to 128 + 1, and for asset value 0 the average converges to 128 + 0
• Asset values 0 and 1

• Noise is Gaussian with mean 128 and variance of 78

• Average for asset value 1 will converge to 128 + 1, and for asset value 0 the average converges to 128 + 0
• Law of large numbers for our case:
• Correct guess:
  \[ \text{mean}(n_{21}+2, n_{22}+2, n_{23}+2 \ldots n_{2i}+2) = \text{mean}(\text{noise}) + 2 \]
  \[ \text{mean}(n_{11}+1, n_{12}+1, n_{13}+1 \ldots n_{1i}+1) = \text{mean}(\text{noise}) + 1 \]
• Wrong guess:
  \[ \text{mean}(n_{21}+2, n_{22}+1, n_{23}+2 \ldots n_{2i}+1) = \text{mean}(\text{noise}) + 1.5 \]
  \[ \text{mean}(n_{11}+1, n_{12}+2, n_{13}+1 \ldots n_{1i}+1) = \text{mean}(\text{noise}) + 1.5 \]
Mathematics

Difference = 1.042

Guess 1: sequence of two asset values

Difference = -0.297

Guess 2: sequence of two asset values
That was for an arbitrary data, but what happens in reality for an arbitrary instruction:

\[ R = f(x,y) \]
Mathematics

\[ R = \text{func}(x,y) \]

Averaged power consumption vs. Number of averages for different HW values:

- HW = 8
- HW = 7
- HW = 6
- HW = 5
- HW = 4
- HW = 3
- HW = 2
- HW = 1
- HW = 0
Mathematics

• Mathematics is simple – average will show the difference in power consumption thus revealing Hamming weight only for the correct model.

• Due to noise we need a lot of acquisitions.

• Let's finally go to side channel attacks.
PART 2. Side channel attacks
• **Power consumption** does depend on **number of bits set to 1**

• An 8bit operation (Sbox[C xor K]) happened during the measurement

• You know C (10,000 values) but you don’t know K.

• You know power consumption trace (lets assume for simplicity that you know time of the operation).
1. Create power model for each key value: $S = \text{Sbox}[C \text{ xor } K]$
Power consumption: D flip flop

- Flip flop power consumption on D input transaction
Mathematics

\[ R = \text{func}(x,y) \]

Averaged power consumption

Number of averages
Side channel preliminaries

<table>
<thead>
<tr>
<th>Шифротекст</th>
<th>Первый байт</th>
<th>Ключ 0x00</th>
<th>Ключ 0x01</th>
<th>Ключ 0xFF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>S</td>
<td>HW(S)</td>
<td>S</td>
</tr>
<tr>
<td>9cb4cad1a9b4031c678e5afc997dd75a</td>
<td>9C</td>
<td>1C</td>
<td>3</td>
<td>75</td>
</tr>
<tr>
<td>505d4db951930c707c8ef4bbe52f25ea</td>
<td>50</td>
<td>6C</td>
<td>4</td>
<td>70</td>
</tr>
<tr>
<td>a3a1e523d7c2d1b17c0da136d0be1559</td>
<td>A3</td>
<td>71</td>
<td>4</td>
<td>1A</td>
</tr>
<tr>
<td>0f8164f091690deff2e3f326c9877c1f</td>
<td>0F</td>
<td>FB</td>
<td>7</td>
<td>D7</td>
</tr>
<tr>
<td>9c4df2500df0f92cd6f6baaff1f765b5</td>
<td>9C</td>
<td>1C</td>
<td>3</td>
<td>75</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>ad38d78c2590807ac3a8b992056b6c3a</td>
<td>AD</td>
<td>18</td>
<td>2</td>
<td>AA</td>
</tr>
<tr>
<td>c766e6776c7d80e1acd68dd825591595</td>
<td>C7</td>
<td>31</td>
<td>3</td>
<td>C7</td>
</tr>
<tr>
<td>fd3d63130367d08e31fe96dd2b5d49ca</td>
<td>FD</td>
<td>21</td>
<td>2</td>
<td>55</td>
</tr>
<tr>
<td>368d5ad4525dce11c9a7c63afe4bf2b2</td>
<td>36</td>
<td>24</td>
<td>2</td>
<td>B2</td>
</tr>
</tbody>
</table>
1. Create power model for each key value: $S = \text{Sbox}[C \text{ xor} \ K]$
2. Distribute power measurements according to the model.
Side channel preliminaries

\[ S = \text{Sbox}[C \oplus K] \]
Side channel preliminaries

\[ S = S_{\text{box}}[C \text{ xor } K] \]
Side channel preliminaries

\[ S = \text{Sbox}[C \oplus K] \]
\[ S = \text{Sbox}[C \oplus K] \]
Side channel preliminaries

\[ S = \text{Sbox}[C \oplus K] \]
1. Create power model for each key value: $S = Sbox[C \text{xor} K]$
2. Distribute power measurements according to the model.
3. Among all distributions get the key with the best dependency.
Side channel preliminaries
1. By eyes this is not comfortable to observe these results, instead use coefficients of mutual dependence as correlation coefficient.
Side channel preliminaries

Let's do a small demo and then you will try to develop your own first side-channel attack.

Do steps 26-27 of the Task1.
• Steps 14 to 17 computes relationship between power traces and the first byte of the last round state:
  \[ S_{10} = InvSbox[C \text{ xor } K_{10}] \]
• \( S_{10} \) is used twice in a program –
  • first time \( S_{10} \) is obtained after \( \text{AddRndKey} \)
  • second time \( S_{10} \) is read from the memory to compute \( Sbox[S_{10}] \)
Side channel preliminaries
PART 2. Practice 1-2 hours
If you did not finish Task1 and still you want to do it – I will help you after small explanation
• AES algorithm can be also implemented in hardware (faster, more reliable, protected against timing attacks etc.).
• You will develop and attack the algorithm in two ways.
• Firstly short explanation how algorithm is done.
Practice

128 bits register

Shift Rows / Sbox → MixColumn → Add round key
• Assume that the only thing that consumes power is 128 bit register so you need to correlate its values.

• AES is executed in 11 clock cycles.

• You need to identify register value that you can compute and correlate. Follow description of the Task2.
• What to read:
  • Scholar.google.com (side channel attacks, power analysis, correlation power analysis and etc.)
  • COSADE, CARDIS, CHES and other academic conferences.
  • Журнал Хакер – я пишу туда серию статей по аппаратным атакам (не только по второстепенным каналам). Пока раз в два месяца.
• This is just the beginning of Side Channel Attacks. Nowadays there are methods that allow:
  • Extract the key without plaintexts and ciphertexts information.
  • Attack protected algorithms.
  • Reverse the code using side channel techniques.
  • Reverse the circuit (approximate IP location).
  • Use side-channels to communicate.
  • Possible other applications.

• Definitely side-channels are not dead and there are enormous place to improve.
Roman Korkikian
Roman.korkikian@yandex.com