

PB173 Domain specific development: side-channel analysis



Course organization

Łukasz Chmielewski
chmiel@fi.muni.cz,

Consultation: A406 Friday 9:00-11:00



Course info

- First seminar of this type
- Practical focus (hands-on):
 1. Learning what side-channel analysis is
 2. Working with ready tools and libraries
 3. Implementing your own tooling/scripts
- Style of seminars is usually:
 - small intro at the beginning of every seminar with materials and tasks
 - individual (Step 1-2)/team work (Step 3)
- Discussion:
 - ask (me) when stucked (within the seminar),
 - IS discussion group if everybody might be interested

Course info cont'd

- Today is different, lecture called:

 “Introduction to side-channel analysis”
- Look at one trace set (if we do not manage to do it today – look at that at home and give me an answer on the next seminar)
- We have to start somewhere

Seminars overview (12 seminars)

- First 1-3/4 seminars: “Introduction to side-channel analysis”:
 - Lecture
 - Inspecting Traces
 - Exercises with ChipWhisperer Acquisition
 - Implementing CPA and DPA
 - Inspecting More Traces
- Seminar 4/5 – choosing project topic and the team
 - Which kind of side-channel tool you would like to implement?
- Seminar 5/6-12 – implementing tooling
- Seminars 11-12 - utilization

Project

- Second part of the semester
 - 3 people, 5 teams
- Implementing on your own or using existing tools (+10 points)
 - Present your tool script and its usefulness (+2 points)
- For your code:
 - Github repository + individual commits
- Trace sets:
 - From me or
 - Find on your own
- Possible Topics:
 - Trace Alignment
 - Manual Analysis of Traces: displaying, zooming, etc.
 - Implementing Classical Attacks: Differential/Correlation Power Analysis, Mutual Information Analysis, etc.
 - Filtering techniques: bandpass filters, etc.
 - Compression Techniques: windowed compression, frequency-based compression
 - More difficult, dimension reductions: Linear Regression and Principal Component Analysis
 - ...

Assignments

- Homeworks/assignments
 - 10 points maximum
 - 10 assignments (100 points)
 - There will be some extra points
 - 65 % required (i.e. 65 points or 50 points)
 - Submit files into is.muni.cz:
 - code + write-ups (word, pdf, or txt with markups)
 - Points for your HW within one week in is.muni.cz
 - **Deadline:** usually until the next seminar (approx. 1 week)
 - **plagiarism is strictly forbidden:**
 - The source of the copied code must be cited

Colloquium

- To get the colloquium
 - You must be present at seminars (2 absences OK)
 - You must be active at seminars (+2 points given by me at the end)
 - You must submit and get:
 - 50%: 7 points in total
(projects + presentation + activity = 14 points)

People

- Main contact: Łukasz Chmielewski (CRoCS@FI MU)
 - Office hours (consultation): Friday 9:00-11:00, A406
 - ✉ chmiel@fi.muni.cz,
 - 👤 <https://keybase.io/grasshopper>

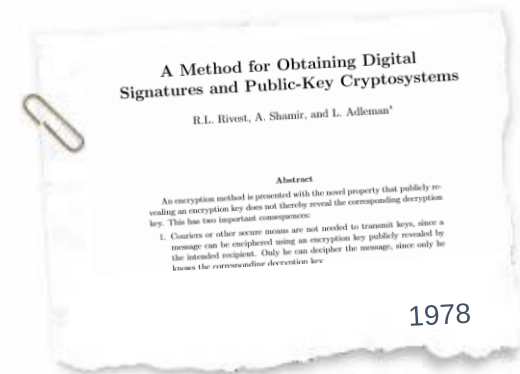
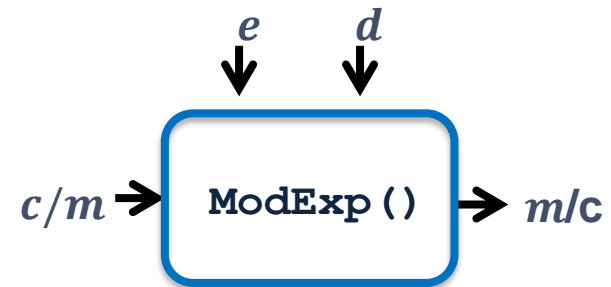
Exercise: SPA on RSA

RSA

- Two primes p and q
- $N = pq$
- $\varphi(N) = (p - 1)(q - 1)$
- $e = 3, 5, 7, 17, 257, 65537 \rightarrow \gcd(e, \varphi(N)) = 1$
- $d = e^{-1} \bmod \varphi(N)$

Modular Exponentiation:

- Encryption / Verification: $c = m^e \bmod N$
- Decryption / Signature: $m = c^d \bmod N$



RSA Exponentiation (1)

```

ModExp (c) {
    A = 1
    for ( i = n-1; i ≥ 0; i--)
        A = A2 mod N
        if (di = 1)
            A = A*c mod N
        end if
    end for
    return A = cd mod N
}

```

$d = (101)_2 = 5$
 $A = 1,$
 $d_2 = 1$
 $A = A^2 \text{ mod } N = 1$
 $A = A * c \text{ mod } N = c$
 $d_1 = 0$
 $A = A^2 \text{ mod } N = c^2$
 $d_0 = 1$
 $A = A^2 \text{ mod } N = c^4$
 $A = A * c \text{ mod } N = c^5$

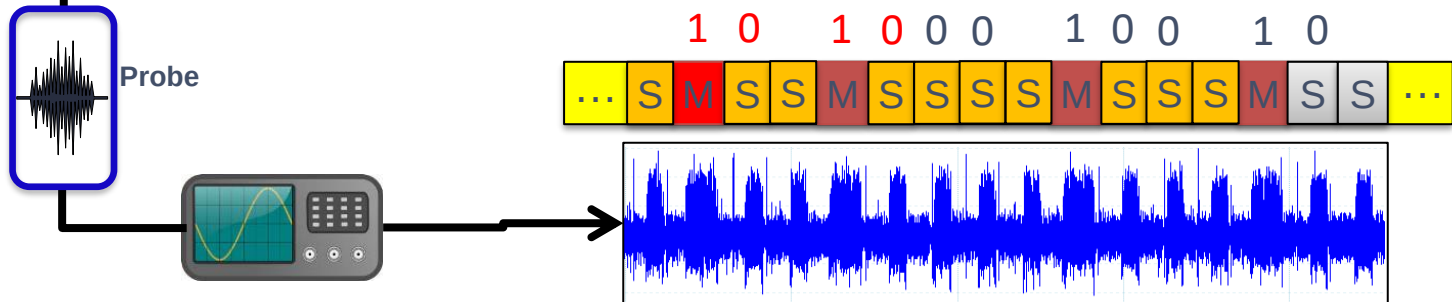
Simple Power Analysis on RSA

```

ModExp (c) {
  A = 1
  for (i = n-1; i ≥ 0; i--)
    A = A2 mod N
    if (di = 1)
      A = A*c mod N
    end if
  end for
  return A = cd mod N
}
    
```



“By carefully measuring the *amount of time* required to perform private key operations, attackers may be able to find [...] RSA keys.”



Simple Power Analysis on RSA

```
ModExp (c) {  
  A = 1  
  for (i = n-1; i ≥ 0; i--)  
    A = A2 mod N S  
    if (di = 1) M  
      A = A*c mod N  
    end if  
  end for  
  return A = cd mod N  
}
```



This SPA matching does not always need to look this way!
One pattern might correspond multiple operations etc.

RSA Exponentiation (2)

```
ModExp (c) {
```

```

  A = c
  j=-1
  for (i = n-1; i ≥ 0; i--)
    if (di == 1):
      j = i
      break
    end if
  if j == -1:
    return 1
  end if
  ...

```

```

  ...
  for (i = j-1; i ≥ 0; i--)
    A = A2 mod N
    if (di == 1):
      A = A*c mod N
    end if
  end for
  return A = cd mod N

```

```
}
```

$d = (0101) = 5$

$j-1 = 1$

$A = c$

$d_1 = 0$

$A = A^2 \bmod N = c^2$

$d_0 = 1$

$A = A^2 \bmod N = c^4$

$A = A * c \bmod N = c^5$

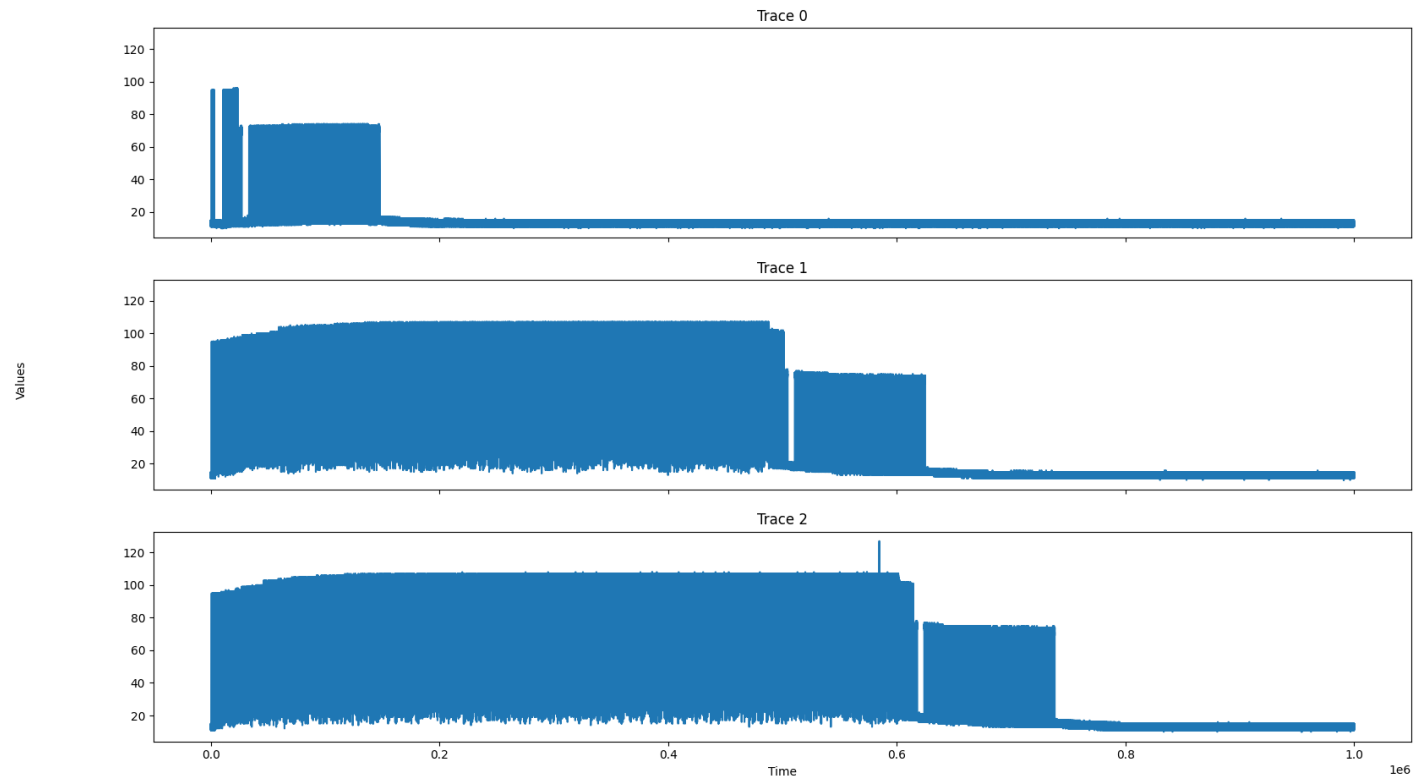
Excercise

- RSA_unprotected.trs
- visualize.py
 - python3
 - Install matplotlib (e.g., pip)
 - Install trsfile (available on pip)
 - Feel free to modify the code and ask me questions about that.
- Three different traces
 - Tell me first 20 most significant bits of each exponent.
- Take your time, good luck!
 - I will give some hints during the exercise 😊

Exercise

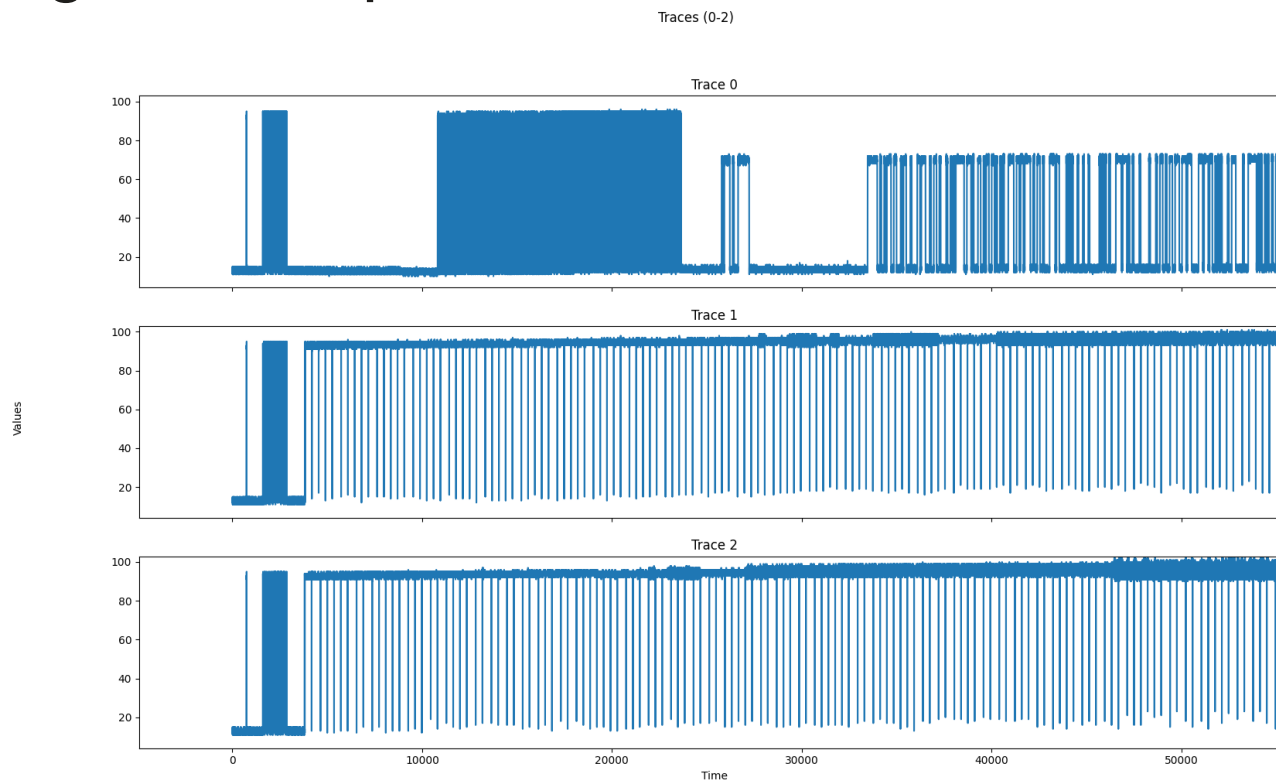
- SPA with operation leakage

Traces (0-2)



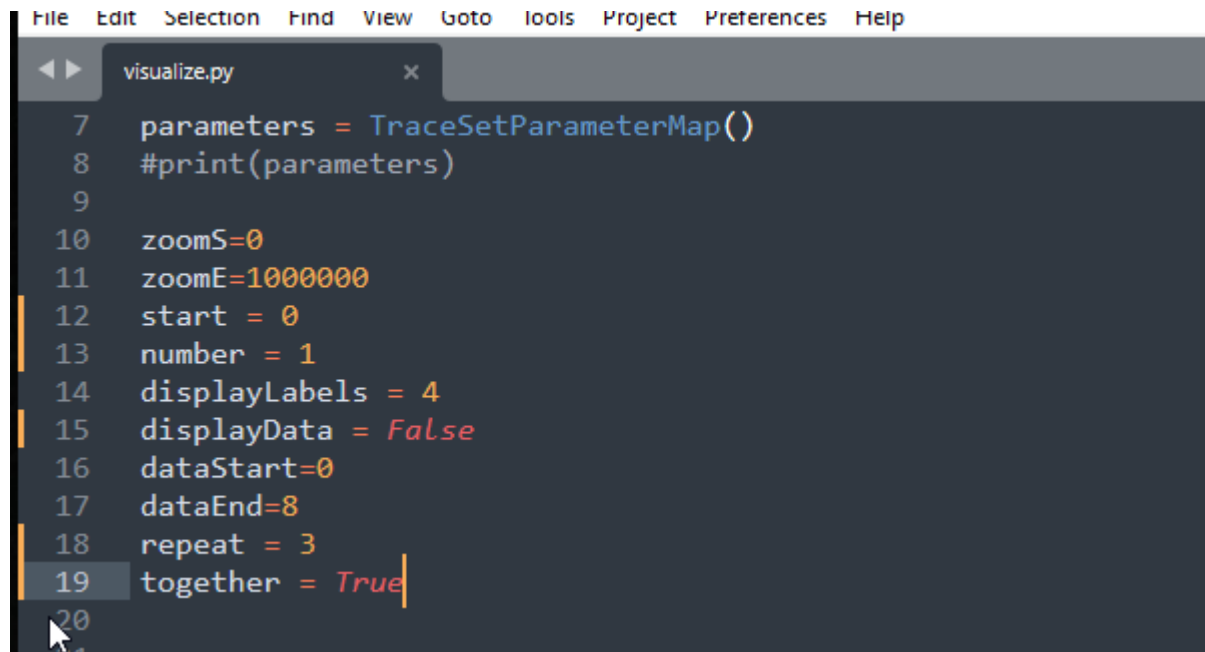
Exercise

- Try to zoom in and find the RSA exponentiation and then get the exponent!



Exercise

- How the visualization script works?



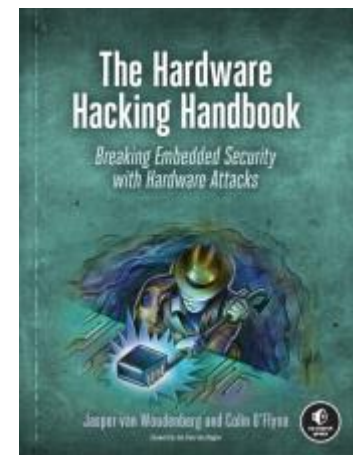
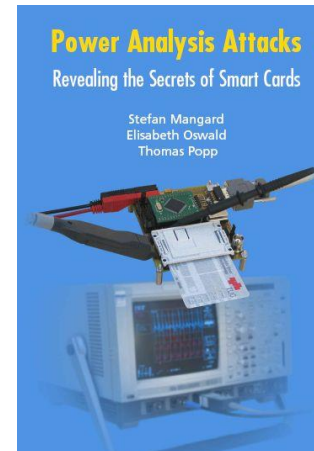
```
File Edit Selection Find View Goto Tools Project Preferences Help
visualize.py x
7 parameters = TraceSetParameterMap()
8 #print(parameters)
9
10 zoomS=0
11 zoomE=1000000
12 start = 0
13 number = 1
14 displayLabels = 4
15 displayData = False
16 dataStart=0
17 dataEnd=8
18 repeat = 3
19 together = True
20
21
```

Homework

- TODOs before the next seminar:
 - Install ChipWhisperer:
<https://chipwhisperer.readthedocs.io/en/latest/linux-install.html>
 - Read the website in general. I am using CW in a linux VM under Windows but do as you prefer 😊
- Watch
 - “PV204 Security technologies: Trust, trusted element, usage scenarios, side-channel attacks”
 - I will provide you with a link in a separate email in the coming days.

Reading

- For interested people
- Side-Channel Analysis – blue book:
 - <http://dpabook.iaik.tugraz.at/>
 - The books is available at the uni.
 - Look online
- The Hardware Hacking Handbook:
 - <https://nostarch.com/hardwarehacking>
 - I have an epub version.



Questions?

