PB173 Domain specific development: side-channel analysis

Seminar 2: Finishing Seminar 1, ChipWhisperer, & SPA Exercise

Łukasz Chmielewski (chmiel@fi.muni.cz),

Consultation: in A406 on Fridays 9:30-11:00
(please email Łukasz before coming)

CROCS
Centre for Research on Cryptography and Security

People

- Łukasz Chmielewski (CRoCS@FI MU)
  - Office hours (consultation): Friday 9:30-11:00, A406
  - Contact me first ↓

  chmiel@fi.muni.cz

  https://keybase.io/grasshoppper

  @chmiel:fi.muni.cz
- Milan Šorf (CRoCS@FI MU)
  - Office hours (consultation): Friday 16:00-18:00, A403
  - Contact me first ↓

  xsorf@fi.muni.cz,

  https://keybase.io/milan_s

  @xsorf:fi.muni.cz

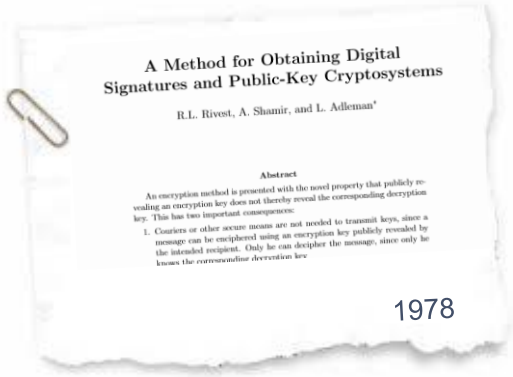
Finish the previous lecture

Chip Whisperer Fast Run

Exercise: SPA on RSA

RSA

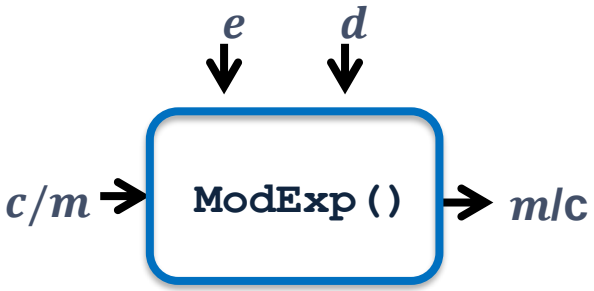
- Two primes p and q



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

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 = A^2 mod N
        if (d_i = =1)
            A = A*c mod N
        end if
    end for
    return A = c^d mod N
}
```

$d=(101)=5$

$A = 1,$

$d_2=1$

$A = A^2 \bmod N=1$

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

$d_1=0$

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

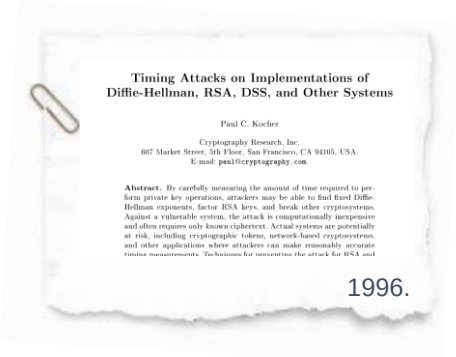
$d_0=1$

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

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

Simple Power Analysis on RSA

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


Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems

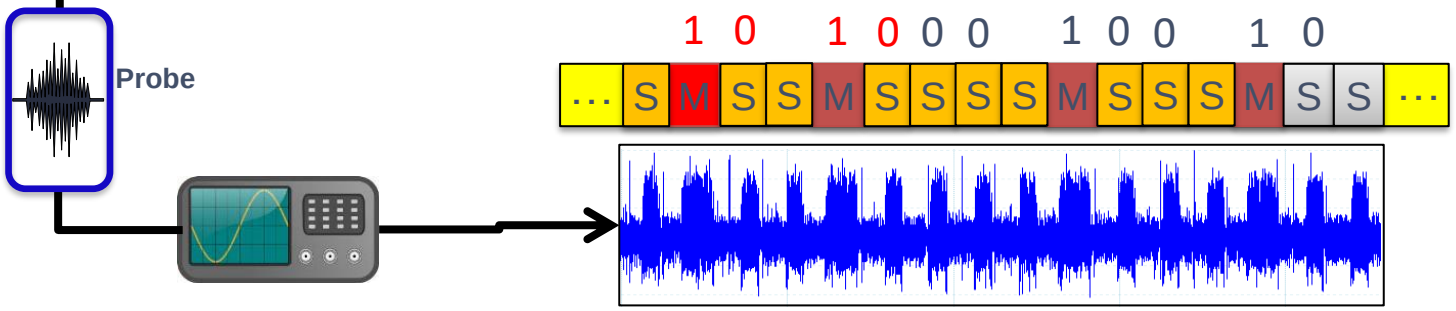
Paul C. Kocher

Cryptography Research, Inc.
607 Market Street, 5th Floor, San Francisco, CA 94105, USA.
E-mail: paul@cryptography.com

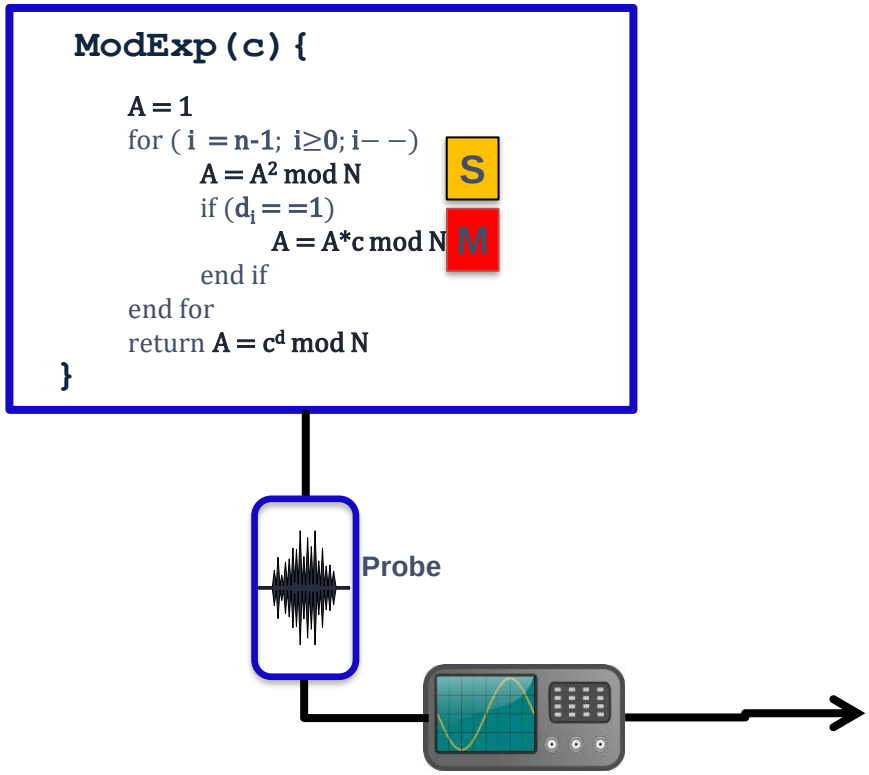
Abstract. By carefully measuring the amount of time required to perform private key operations, attackers may be able to find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems. Against a vulnerable system, the attack is computationally inexpensive and often requires only known ciphertext. Actual systems are potentially at risk, including cryptographic tokens, network-based cryptosystems, and other applications where attackers can make reasonably accurate

1996.

"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



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 (d_i ==1):
                        j = i
                        break
                end if
        if j==-1:
                return 1
        end if
        ...

        ...
        for ( i = j-1; i≥0; i--)
                A = A^2 mod N
                if (d_i = =1):
                        A = A*c mod N
                end if
        end for
        return A = c^d mod N

}
```

$d=(0101)=5$

$j-1=1$

$A=c$

$d_1=0$

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

$d_0=1$

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

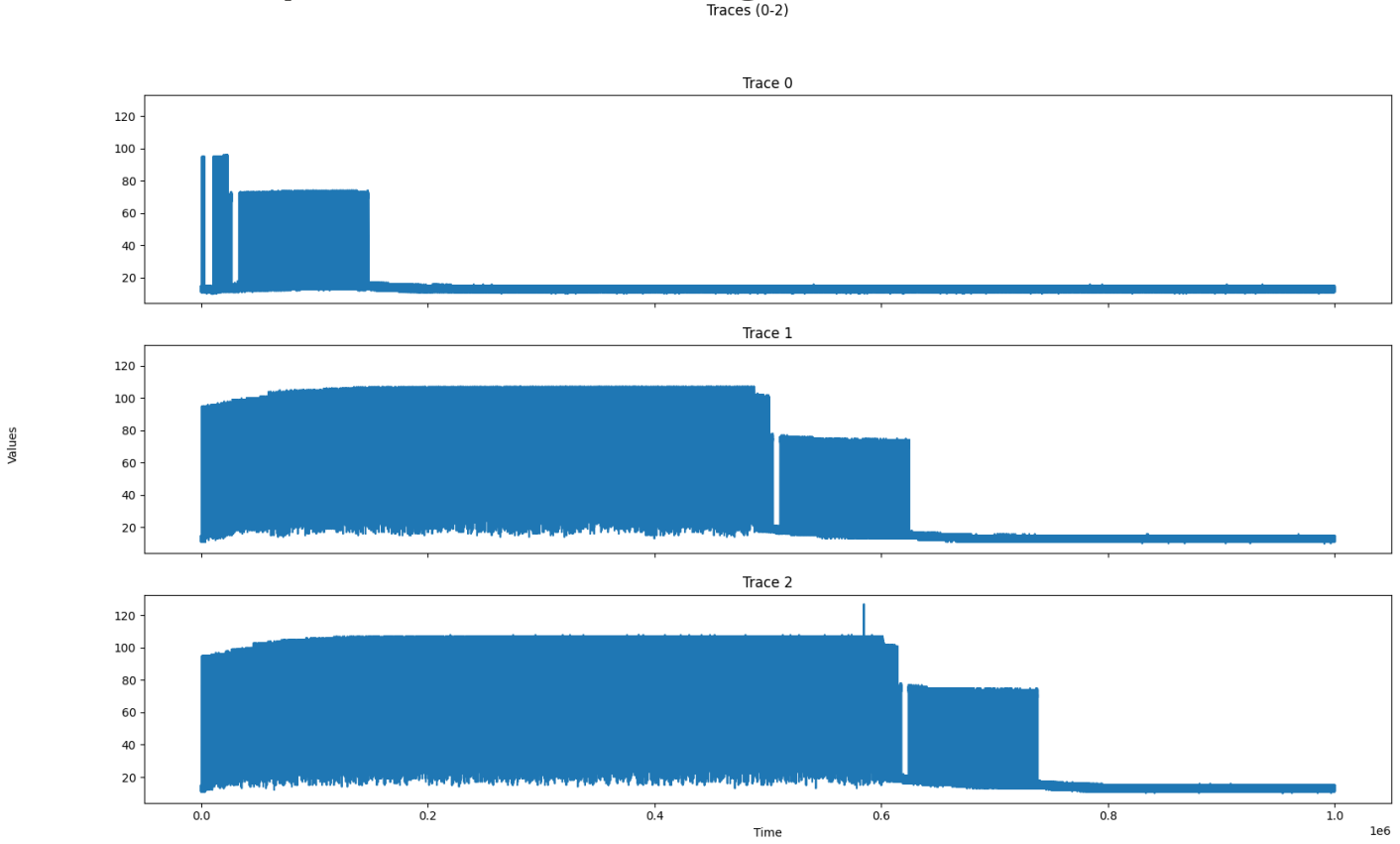
$A=A*c \bmod N=c^5$

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 ☺

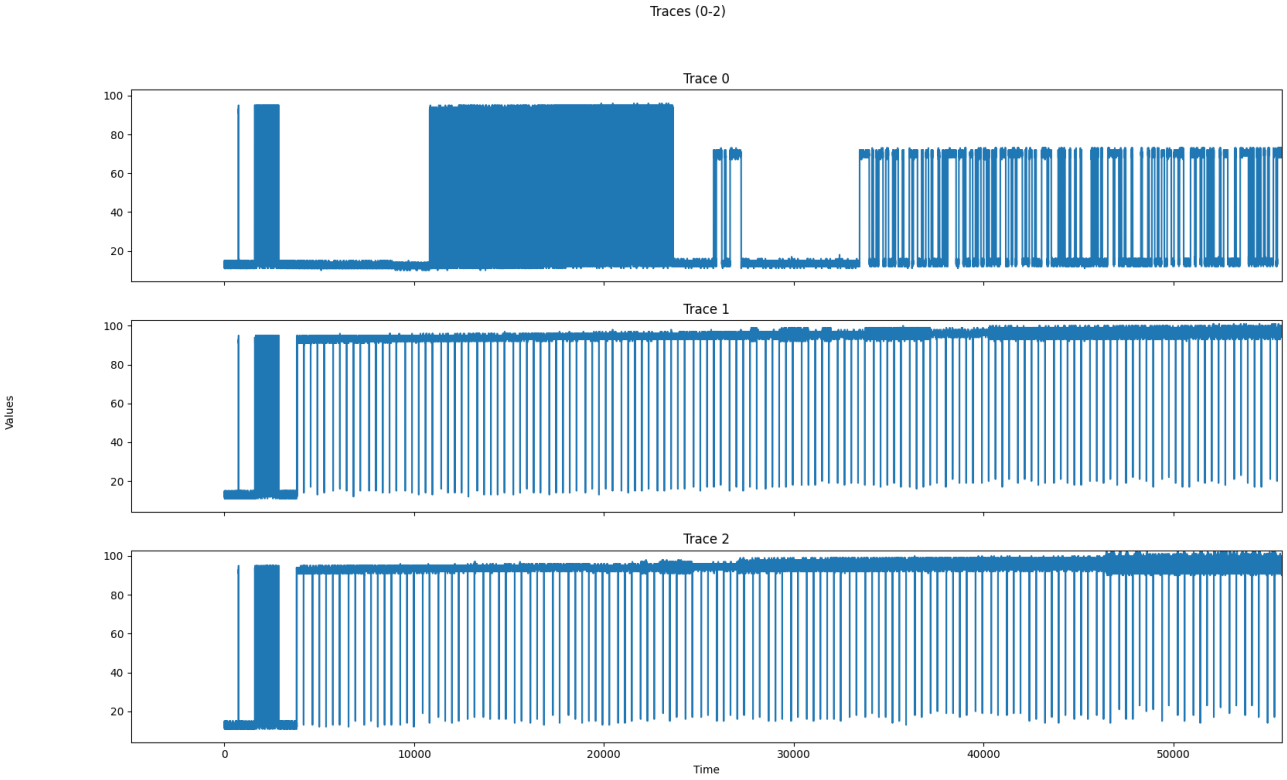
Exercise

- SPA with operation leakage



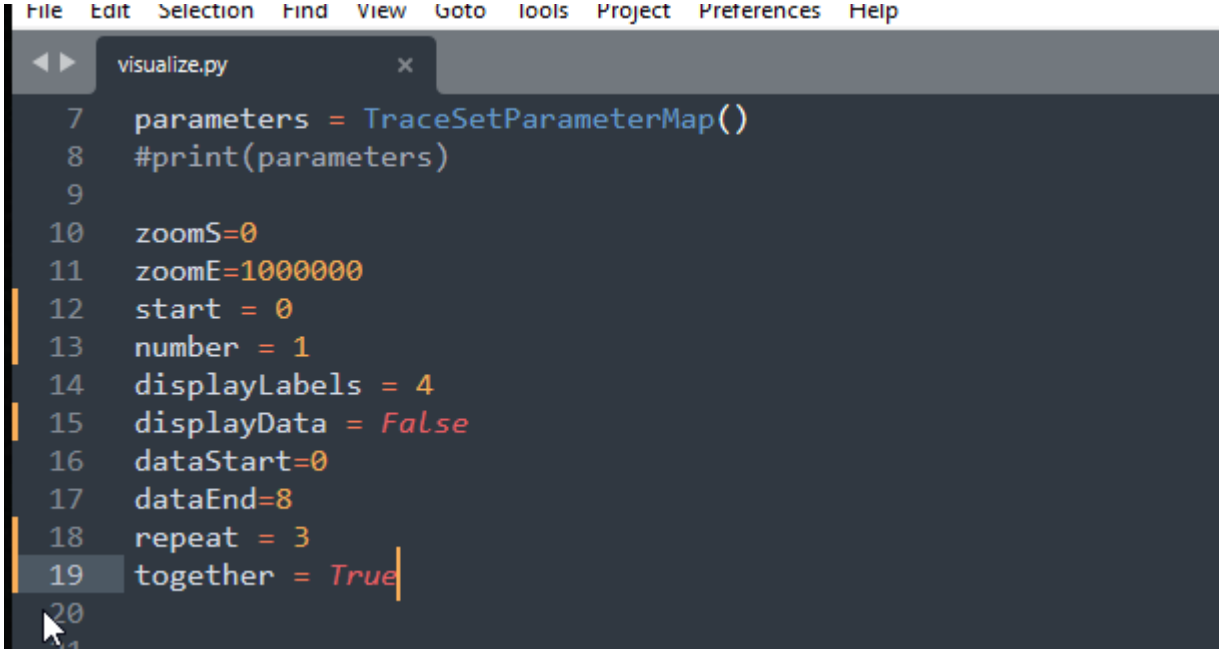
Exercise

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



Exercise

- How the visualization script works?

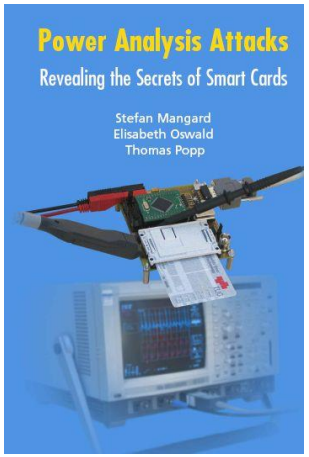


Homework

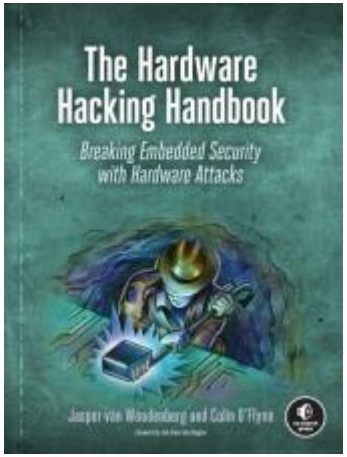
- TODOs before the next seminar:
  - (REALLY) Install ChipWhisperer: https://chipwhisperer.readthedocs.io/en/latest/virtual-box-inst.html
  - Copy Excercise_CPA_DPA.ipynb to ./chipwhisperer/jupyter/courses/sca101
  - Run the first two cells from Excercise_CPA_DPA.ipynb with:
    - PLATFORM = 'CWNANO'
    - %run "../../Setup_Scripts/Setup_Generic.ipynb“
      Result:
      INFO: Found ChipWhisperer😍

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