Side Channel Attacks

COM-402: Information Security and Privacy

(slide credits: Nicolas Gailly)

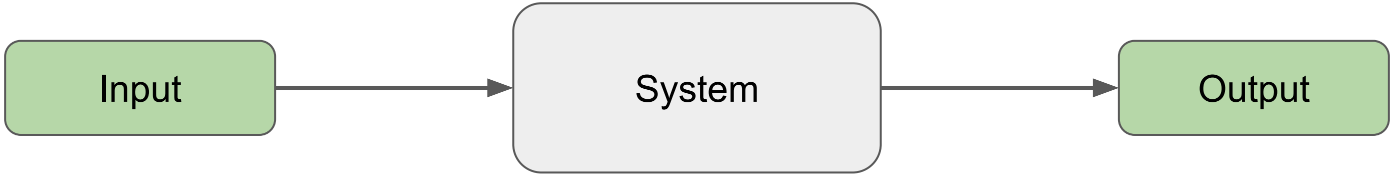
Side Channel: Why bother?

- Many fast growing fields for embedded applications: RFID, sensor networks, “Internet of Things”
- Areas of interest: public transportation, communication, health care, car industry, banking sector, military, etc.
- Drastic increase in the importance of hardware security and the demand for secure chips
- Hardware implementing cryptographic functions (including smartcards) often show severe vulnerabilities

https://zerobyteio/talks/2013-01-28-ieeepdf

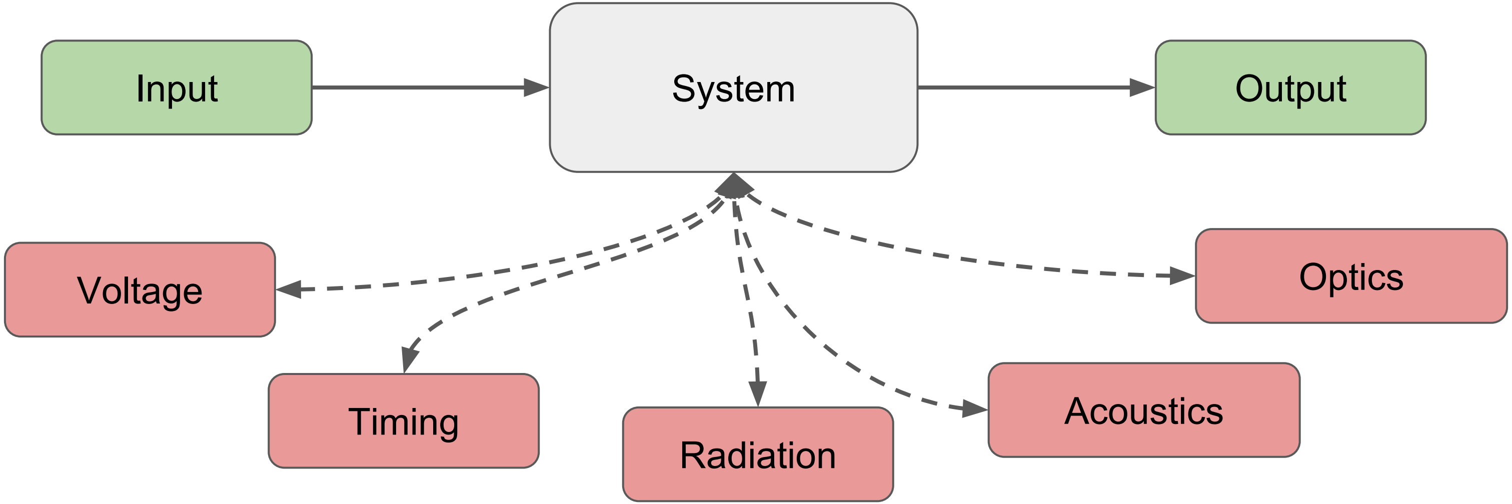
Side Channel: Definition

Before side channel cryptanalysis, a cryptographic system was only conceived as:



Side Channel: Definition

- Starting mid-90s, a new broader definition
- Attacks target the system device itself without relying on input/output pair



Examples of Side Channels

- How much power the computer uses when it does something
- How long it takes the computer to do something
- Which areas of the computer’s memory have been accessed
- Unintentional electromagnetic radiation emanating from the system
- Sounds coming from the system (beeps, hard drives working, etc.)
- The time that network packets get sent out of the system

Side Channel: Timing Attacks

- Cryptosystems take slightly different amounts of time depending on the **input data** (i.e., secret key)
- Feed the timing measurements to a statistical model
- Model can guess key with some degree of certainty
- Attack is **non-invasive** and **passive**

- RSA: Square and multiply algorithm:
  - If the i^{th} bit of secret key is 1, do a modular reduction
  - If the i^{th} bit of secret key is 0, continue to next bit
- Time difference is enough to guess the i^{th} bit

```
x = C
for j = 1 to n
    x = mod(x^2, N)
    if d_j == 1 then
        x = mod(xC, N)
    end if
next j
return x
```

Timing Attack: SSH Keystrokes

- SSH (interactive) sends one packet for each key pressed
- Infer key typed by correlation with timing information!

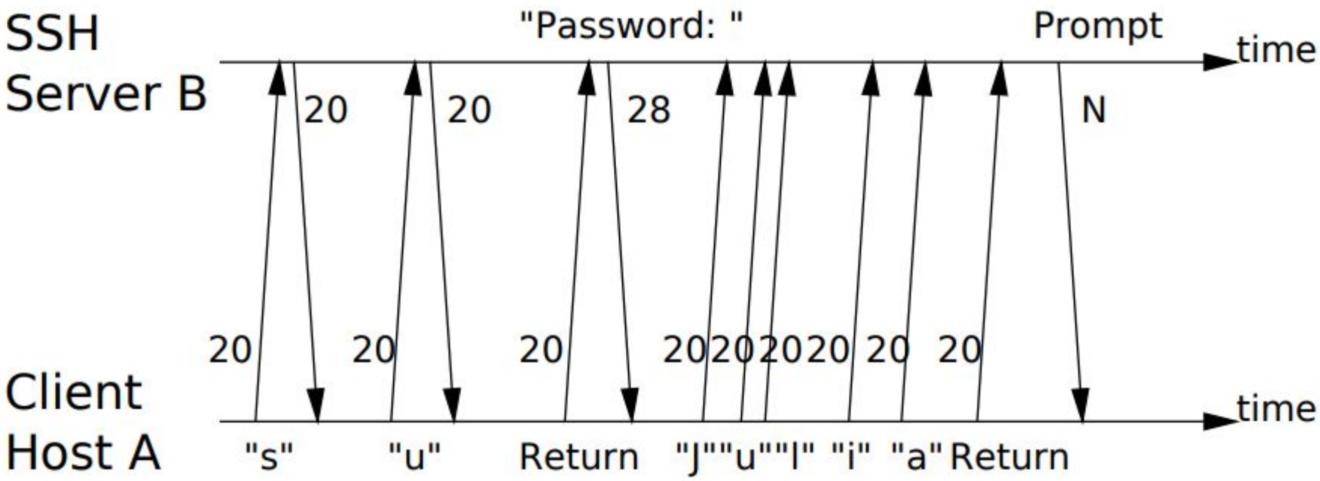


Figure 1: The traffic signature associated with running SU in a SSH session. The numbers in the figure are the size (in bytes) of the corresponding packet payloads.

https://peopleeecsberkeleyedu/~daw/papers/ssh-use01pdf

Timing Attacks: AES Cipher

- AES rounds use table lookup for fast implementations
- Access depends on secret key
- Tables are in the **cache**
- <u>Assumptions:</u> AES and attacker share the same CPU

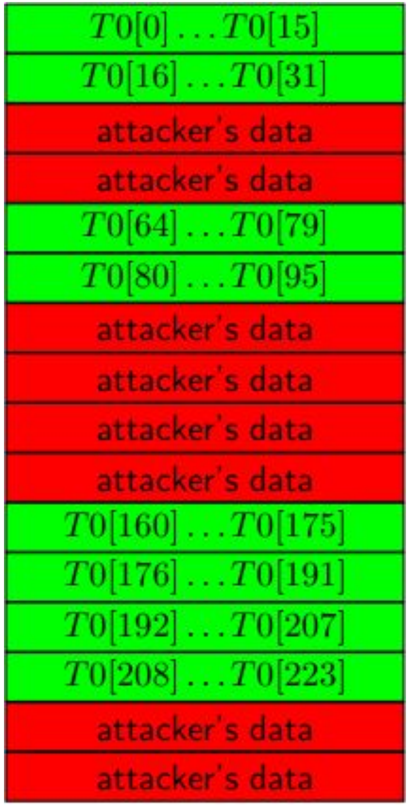
  (assumption can be relaxed)

$T0[0] \dots T0[15]$
$T0[16] \dots T0[31]$
$T0[32] \dots T0[47]$
$T0[48] \dots T0[63]$
$T0[64] \dots T0[79]$
$T0[80] \dots T0[95]$
$T0[96] \dots T0[111]$
$T0[112] \dots T0[127]$
$T0[128] \dots T0[143]$
$T0[144] \dots T0[159]$
$T0[160] \dots T0[175]$
$T0[176] \dots T0[191]$
$T0[192] \dots T0[207]$
$T0[208] \dots T0[223]$
$T0[224] \dots T0[239]$
$T0[240] \dots T0[255]$

https://cryptojediorg/peter/data/croatia-20160610pdf

Timing Attacks: AES Cipher

- AES rounds use table lookup for fast implementations
- Access depends on secret key
- Tables are in **cache**
- AES and attacker share the same CPU
- Attacker **evicts** some entries

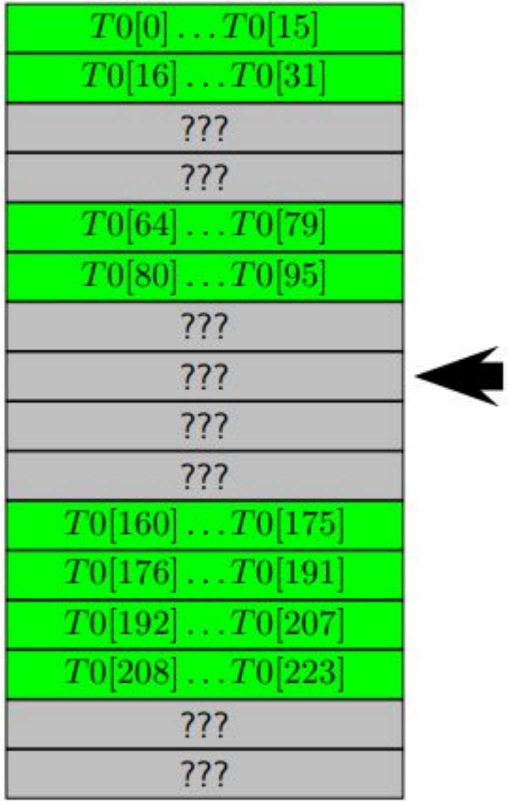


https://cryptojediorg/peter/data/croatia-20160610pdf

Timing Attacks: AES Cipher

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

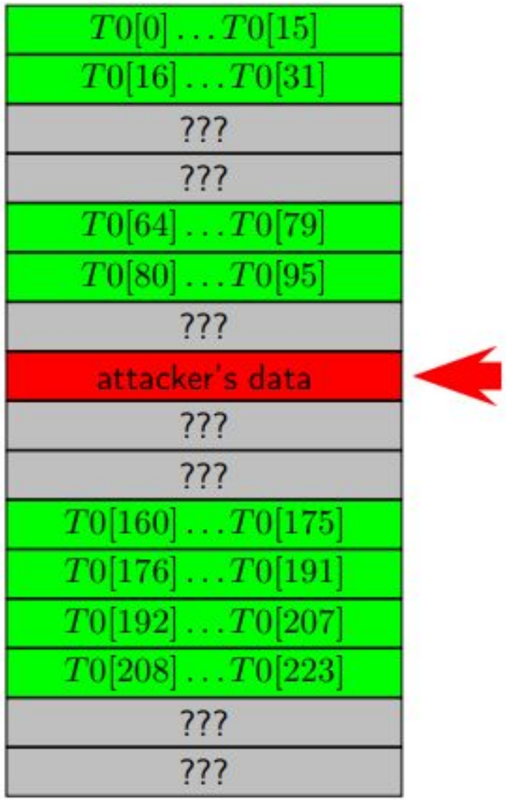
- AES rounds use table lookup for fast implementations
- Access depends on secret key
- Tables are in **cache**
- AES and attacker share the same CPU
- Attacker **evicts** some entries
- AES **<u>loads</u>** the data from table



https://cryptojediorg/peter/data/croatia-20160610pdf

Timing Attacks: AES Cipher

- AES rounds use table lookup for fast implementations
- Access depends on secret key
- Tables are in cache
- AES and attacker share the same CPU
- Attacker **evicts** some entries
- AES **loads** the data from table
- Attacker **loads** same entry
  - Fast lookup→AES did **not** load from this line
  - Slow→AES loaded from this line
- **Leaks** secret key bits!



https://cryptojediorg/peter/data/croatia-20160610pdf

Timing Attacks: Flush + Reload

- Extract RSA private key from cache access timing information
- Attacker process flushes the cache, waits, then loads same information
- Time to fetch from the cache depends on the victim process's activity
- Works even on different VMs on same host !

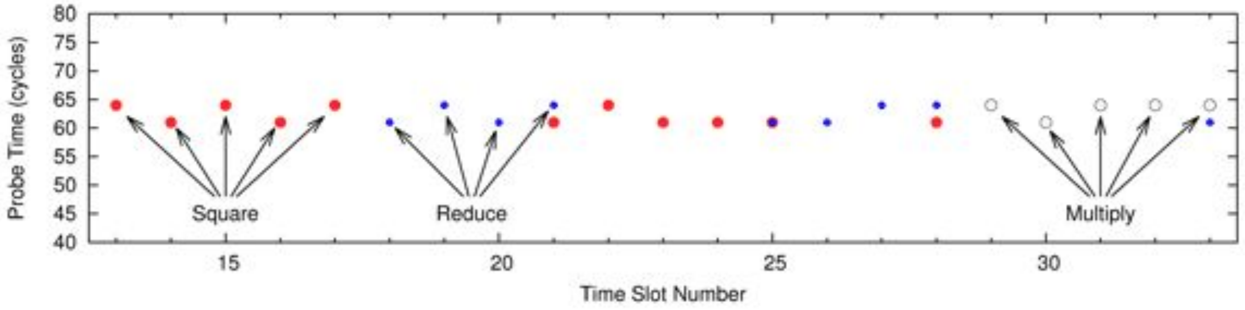


Figure 7: Time measurements of probes

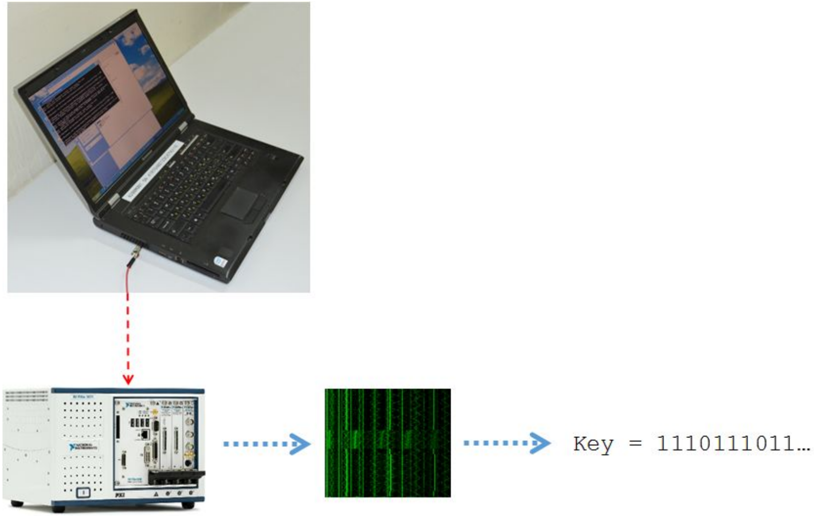
https://eprintiacrorg/2013/448pdf

Timing Attacks: Defenses

- General data-independent calculations:
  - Same time for any computations
  - Or at least same number of **clock cycle** if computation done using input data
- Avoid conditional branch and secret intermediates
  - Using XOR, OR etc operations instead of IF / ELSE
  - Takes the same amount of time *and* power
- Introduce random delays of a few milliseconds
  - Closes fine-grained but not coarse-grained timing channels
- **Most of the time** reasonable defenses are available if used properly!

Side Channel: Power Analysis Attacks

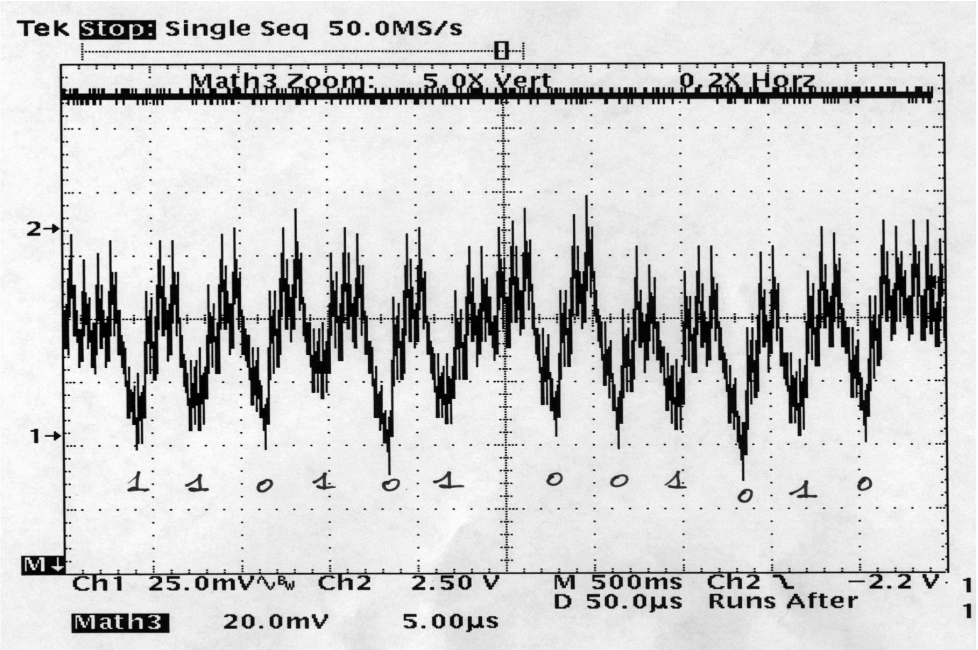
- Every circuit with transistors consume power (smartcards, mobile phone, etc.)
- Monitoring the power consumption reveals informations stored in the circuit
- The attack is cheap and **non-invasive** (USB sound card, some wires and a probe)
- Very successful in practice: Can recover ECDSA private key during signature



https://wwwtauacil/~tromer/handsoff/

Side Channel: Simple Power Analysis

- Often requires detailed knowledge about device + implementation
- Triple-DES power analysis reveal key easily



http://wwwnicolascourtoiscom/papers/sc/sidech_attackspdf

Side Channel: Simpler Power Analysis RSA

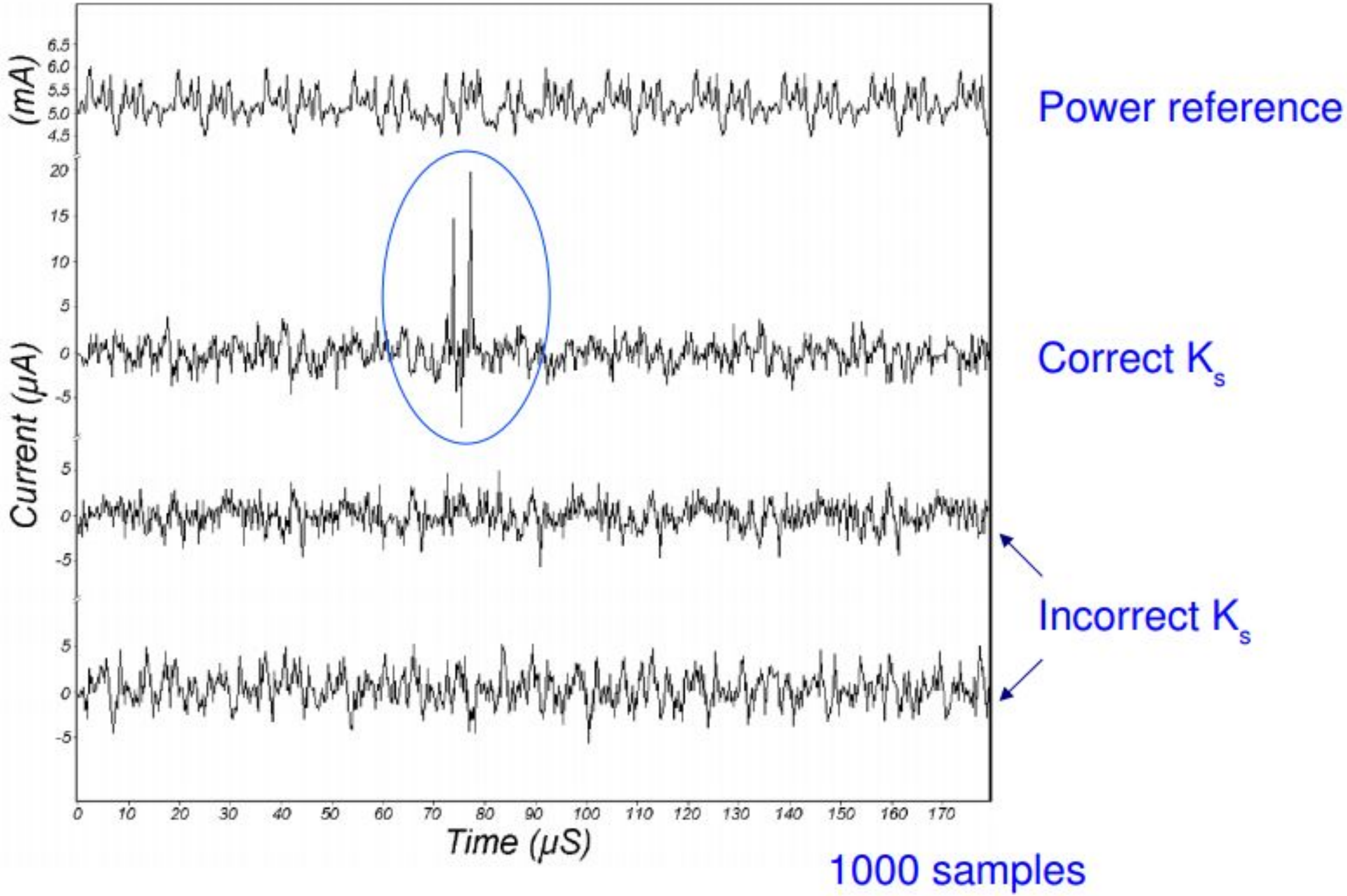
- RSA uses **Square-and-Multiply**:
  - Loop over each bits of the secret key
  - If bit is 1 => multiply then square => more power consumption
  - If bit is 0 => square directly
- Leaks the secret key entirely!

x = *C*
  for *j* = 1 to *n*
    x = mod(x^2, *N*)
    if d_j == 1 **then**
      x = mod(*xC*, *N*)
    end if
  next *j*
  return *x*

http://wwwcryptofailscom/post/70097430253/crypto-noobs-2-side-channel-attacks

Side Channel: Differential Power Analysis

- Use of advanced statistical techniques including error correction, noise filtering methods, etc.
- General technique:
  - Observe ***m*** encryption operations: ciphertext and power traces
  - Choose a selection function ***S***: it's a **guess** over the key ***K***
  - Run ***k*** sample differential traces
  - If the guess is good, it will show



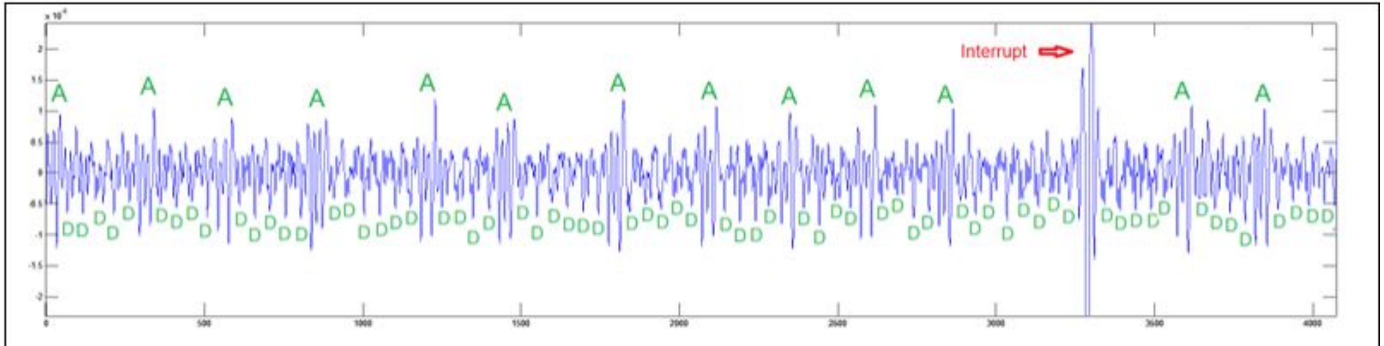
(mA)
6.5
6.0
5.5
5.0
4.5
Current (µA)
20
15
10
5
0
-5
5
0
-5
5
0
-5
0
10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
Time (µS)
Power reference
Correct K$_s$
Incorrect K$_s$
1000 samples

Side Channel: Differential Power Analysis

- DPA can be used to break any algorithm in principle
- DPA can also be used to reverse engineer closed-source protocols
- **Defenses**:
  - Reduce signal size
  - Introduce noise
  - Design cryptosystems with realistic assumptions about the underlying hardware

Side Channel: Electromagnetics

- Electromagnetic signal measured with a magnetic probe + digital card: works **through a wall**
- Detect DOUBLE and ADD operations of ECDSA signatures
- Much harder than RSA because much faster (more advanced signal processing techniques)



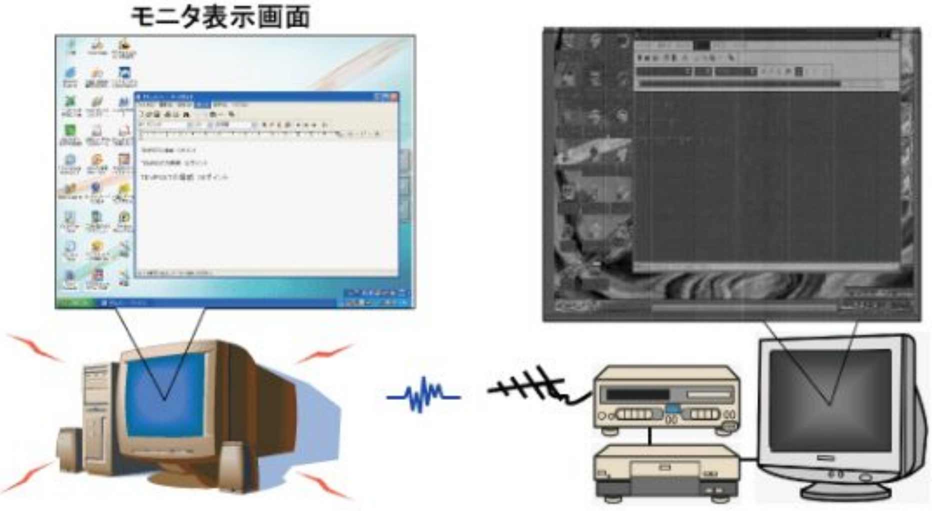
A segment of the electromagnetic signal, after singular spectrum analysis.

https://wwwcstauacil/~tromer/mobilesc/

Electromagnetics: A Long History Reality

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

- Every electrical device generates magnetic radiations:
    - **Screens**, laptops, mobiles, etc.
- Exploited by NSA TEMPEST program since 1943 !
- First public knowledge in 1972



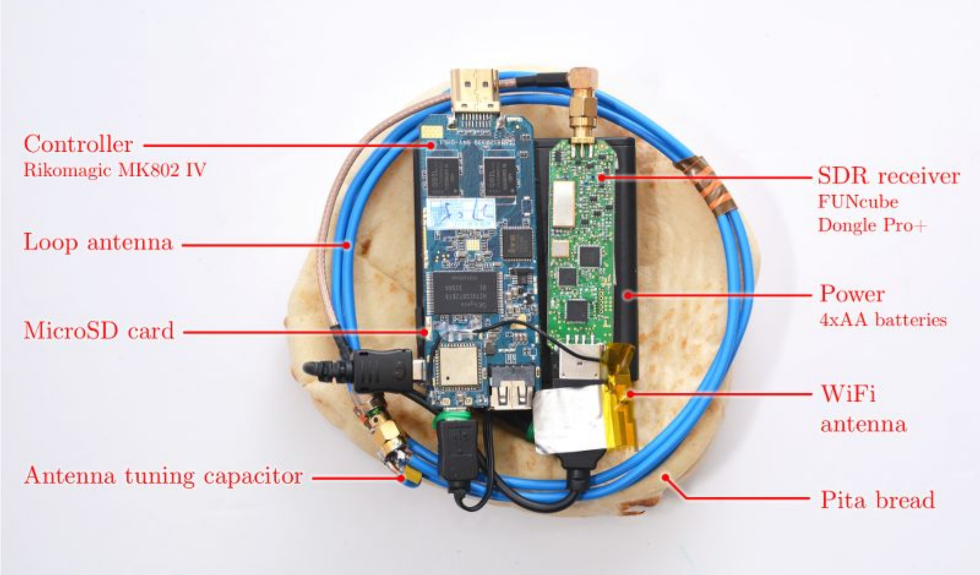
TV. If you think that's scary, the National Security Agency can view your cellphone screen from over a kilometer away, listen to signals from your monitor cable, and use your computer's power supply to snoop on you. This

https://wwwwiredcom/2008/04/nsa-releases-se/

https://climateviewercom/

Side Channel: Electromagnetics

- Attack possible with consumer grade radio receiver or even with handmade receiver!

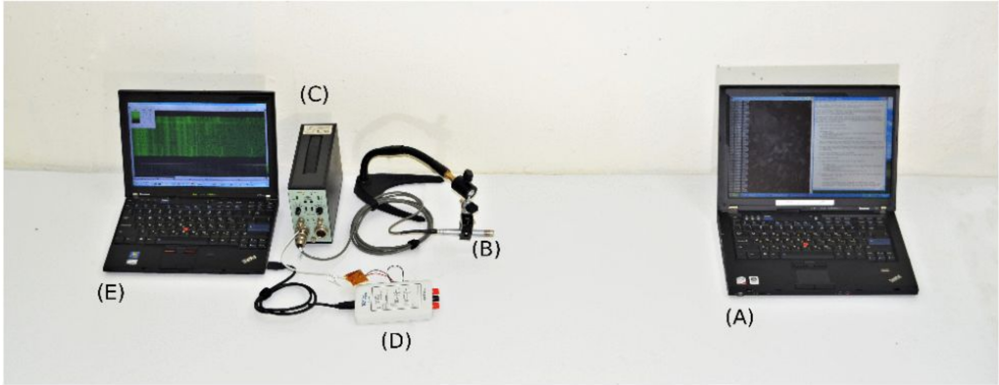


https://wwwcstauacil/~tromer/radioexp/

Side Channel: Acoustic Cryptanalysis

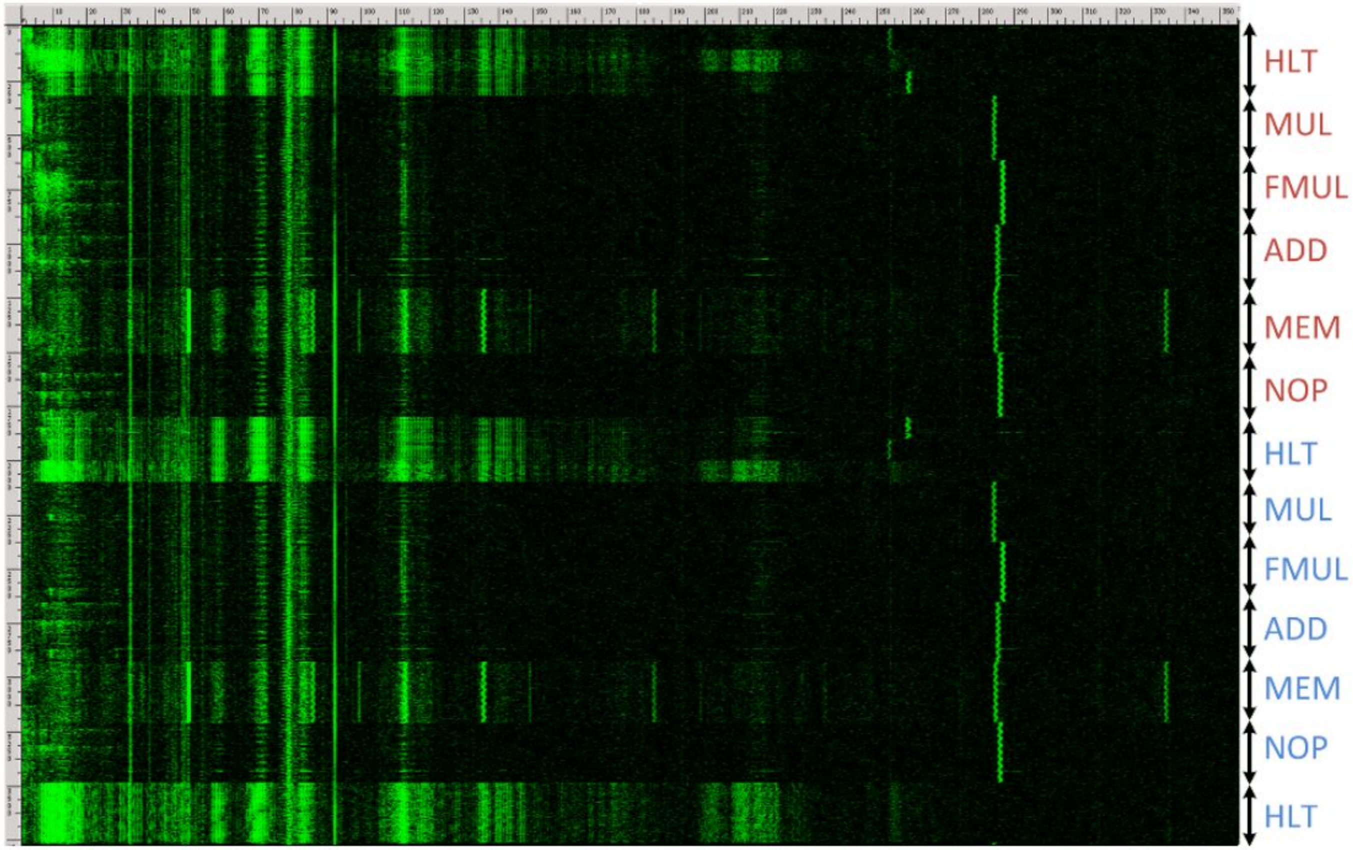
ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

- Recover information from acoustic sounds of the **voltage regulator** inside the PC (“whining” sound)
    - Goal: recovery of a 4096-bit private key used in RSA encryption
    - Requires at least 2048 decryptions, bit-by-bit key recovery
    - Attack vector: Enigmail with Thunderbird GPG plugin, automatic decryption when receiving email



https://wwwslidesharenet/dusanklinec1/accoustic-crypto-33236263?from_action=save

Acoustic Cryptanalysis



Acoustic Cryptanalysis: RSA - CRT

Textbook RSA encryption:

```
c  = m^e mod n
m: message
e: public key exponent
n: public key modulus n = p*q
```

Textbook RSA decryption:

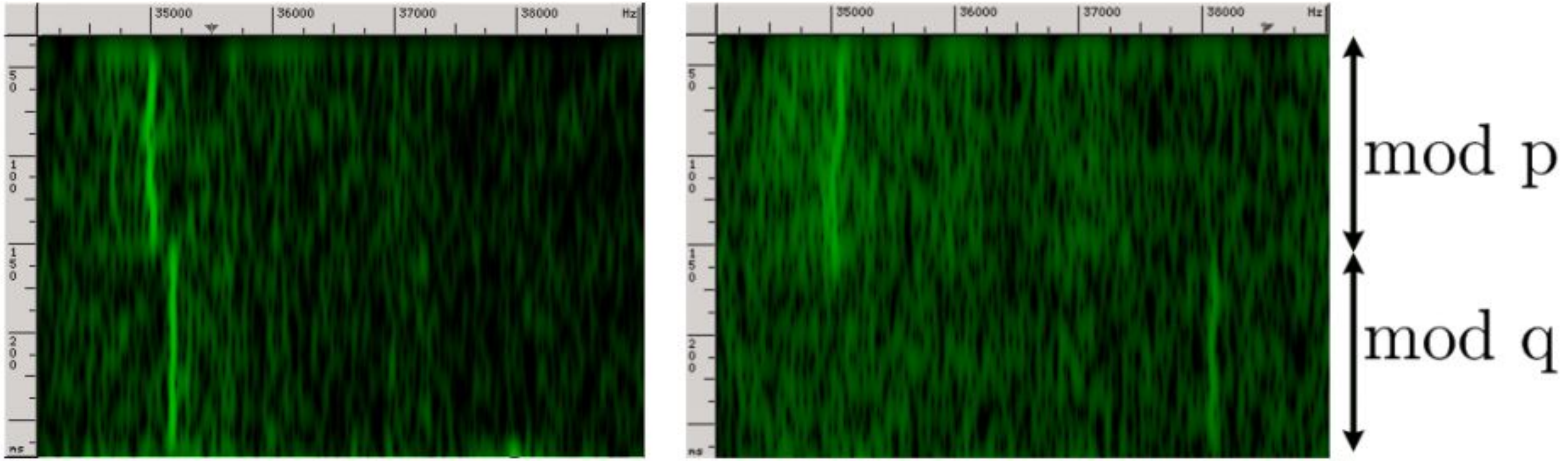
```
m  = c^d mod n
m: message
d: private key exponent
n: public key modulus n = p*q
```

Chinese Remainder Theorem (CRT) optimization:

```
Precompute:

d_p = d mod p-1
d_q = d mod q-1
q_inv = q^-1 mod p

Decryption:

m1 = c^(d_p) mod p
m2 = c^(d_q) mod q
h = q_inv * (m1 - m2) mod p
m = m2 + h * q
```

Acoustic Cryptanalysis: RSA

- General algorithm:
  - Guess ith bit of the key→1 or 0
  - Submit to decryption (decryption oracle)
  - Observe difference between the mod p and mod q operations



(a) attacking 0 bit (b) attacking 1 bit

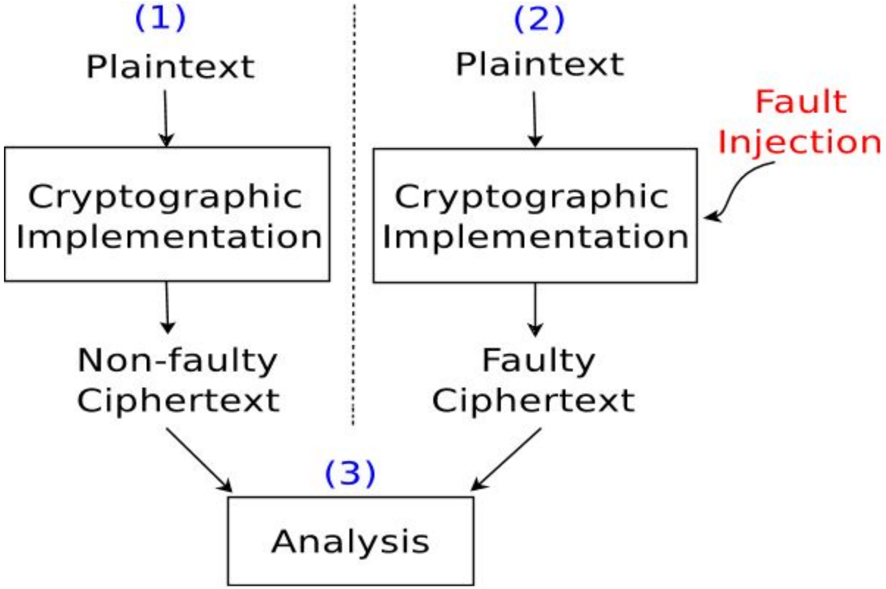
Side Channel: Fault Attacks

- **Inject** faults into the system
  - Change voltage, tamper the clock, etc.
- Smartcard hacking is a huge business
  - Paid TV content
  - ATMs
  - Laundry machines!!

http://fortune.com/2016/11/21/cybercrime-bank-atm-buhtrap/
http://inforippleshotcom/blog/the-brief-history-of-chip-card-hacking

Side Channel: Differential Fault Analysis

- **Inject** faults into the system
  - Change voltage, tamper the clock, etc.
- Encrypt data twice and compare results
  - One bit difference indicates a fault in one operation
- Able to attack RSA, DES, etc.



RowHammer

- Memory access rapidly activating same memory rows
- Accesses modify contents of nearby memory rows
- Attack can:
  - Gain root access
  - Escape sand boxes
  - Make apps with higher privileges, etc.

Side Channel: Optical Covert Channel

- Exfiltrate data from air-gapped computers
- Data exfiltration through the drive LEDs’ blink frequency
- LED blinks encode a QR-code encoded data
- Analyzed by remote camera (e.g., mounted on drone!)

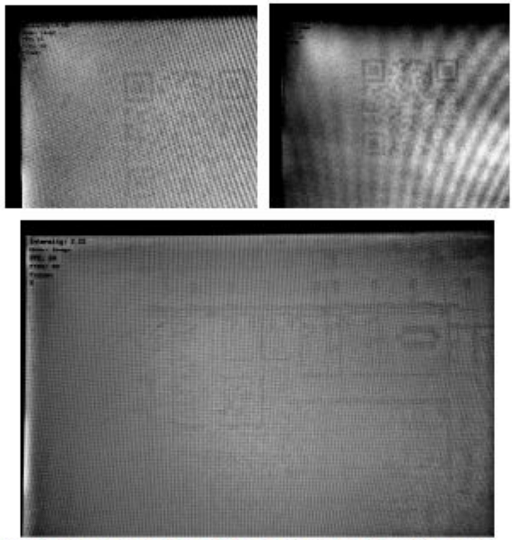
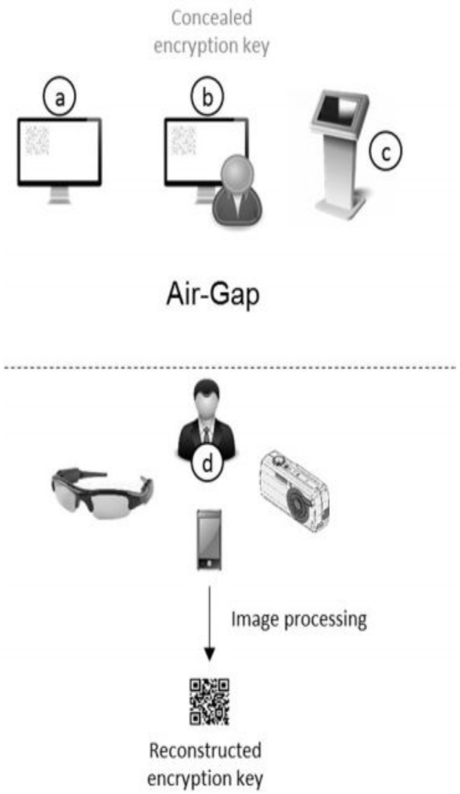


Figure 6. Sample of photos taken during testing, following basic image processing.



https://arxivorg/pdf/160703946pdf

Conclusion

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

- Side-channel risks come in many shapes and sizes
  - Timing, power, visual, acoustic, faults, …
  - Can be exploited to exfiltrate secrets, fingerprint systems or users, …
- Important to develop defensively with awareness of side-channel risks
  - Example: constant-time implementations of code handling sensitive secrets
  - No all-purpose, general defense exists (yet), unfortunately