EURECOM
Sophia Antipolis

Screaming Channels

When Electromagnetic Side Channels Meet Radio Transceivers

Giovanni Camurati, Sebastian Poeplau, Marius Muench,
Tom Hayes, Aurélien Francillon

RESSI

15-05-2019

Who are we?

System and Software Security Group at EURECOM
s3.eurecom.fr

I am a PhD student "on radio side channels"

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

Side Channels, The Idea

Theory

Secure lock is impossible to open

Implementation

Different sound if we make a partial correct guess

Attack

Open it with a few attempts

Embedded Devices and Side Channels

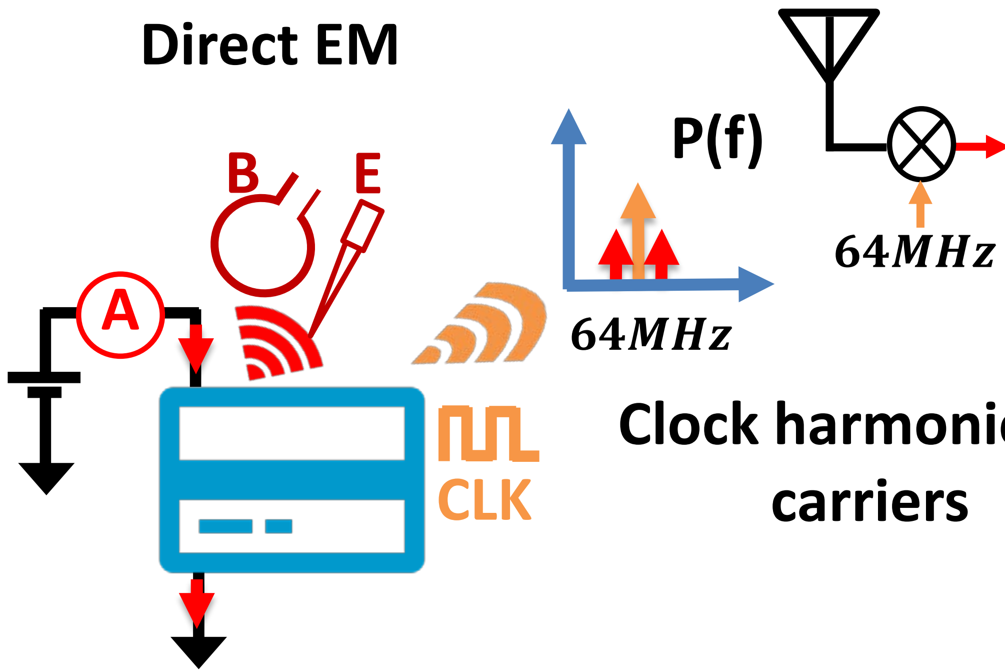
Secure systems: E-Passport, Smartcard, …

Crypto against stealing, cloning, tampering, …

Generally protected against attacks which require physical access

Conventional Side Channels

Direct EM

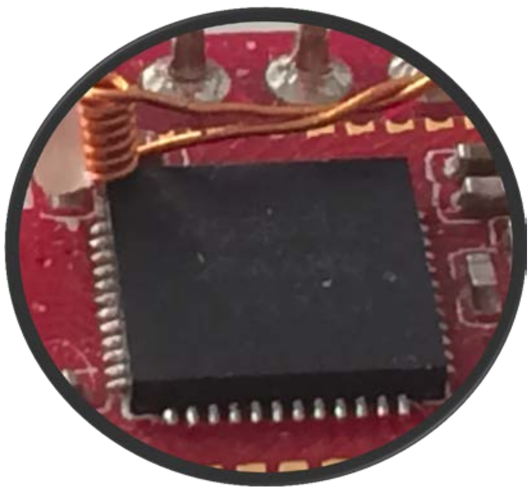


Power (current)

Clock harmonics as carriers

Physical activity depends on logic data

In Practice



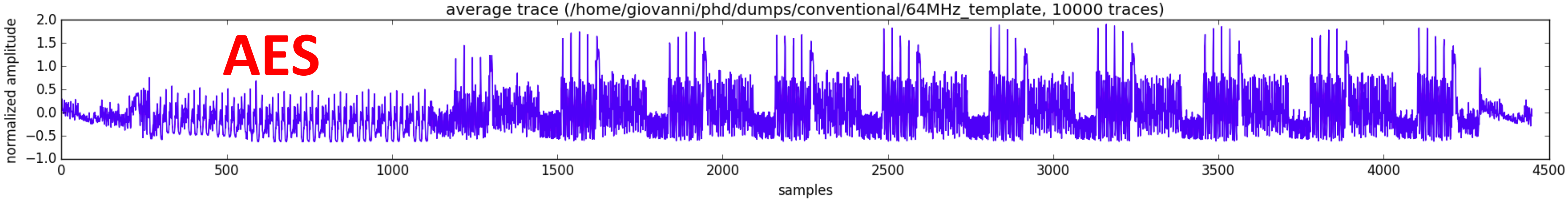
Collection

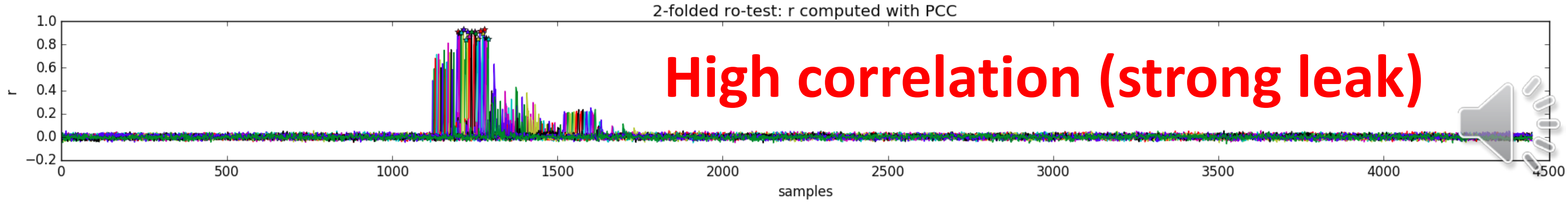
E.g. loop probe + oscilloscope

Many Analyses/Attacks

SPA, CPA, TPA, …

SEMA, CEMA, TEMA, …





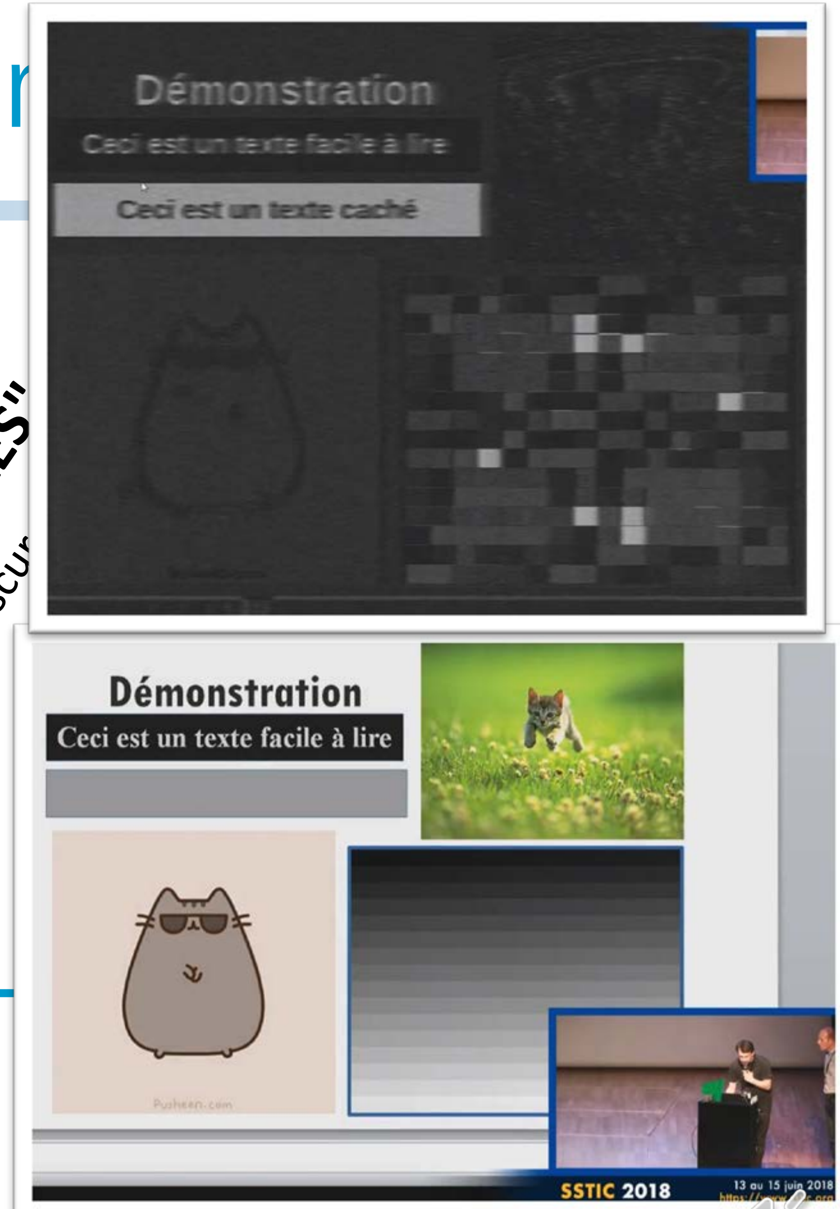
Many Side Channels Ir

Classic EM Attack
Agrawal et al. [1]

Laptop Intel CPU
Genkin et al. [2]

"TEMPEST AES"
Fox-IT, Riscu

mm cm	15 cm wall	30 cm 1 m



Embedded Devices and Side Channels

Secure systems:
E-Passport,
Smartcard, …

Crypto against stealing, cloning, tampering, …

Generally protected against attacks which require physical access

Connected devices:
Smart watch,
camera, …

Crypto protects the communication channel

Only remote attacks are considered

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

Remote Side Channels

Remote Timing

Non constant time

Caches

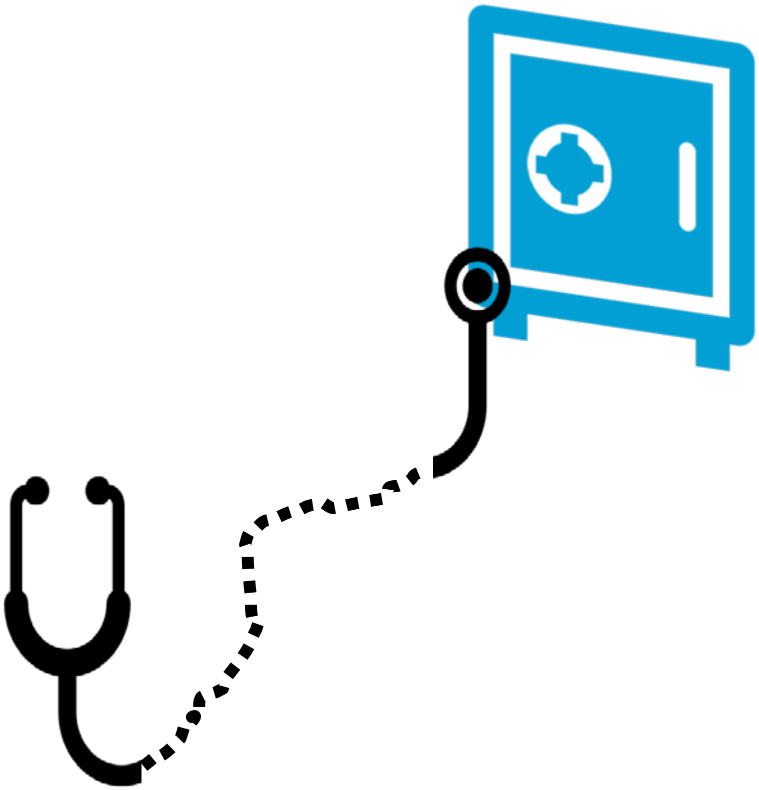
AES, TLS, …

WPA3 (Dragonblood)

EM?

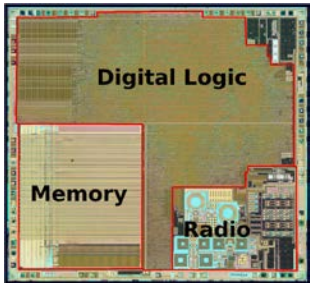
Physical access

Local



Problems When Adding Wireless Capabilities

Implementation: Mixed-signal Chips



Idea:
CPU + Crypto + Radio
Same chip

Benefits:
Low Power, Cheap, Small
Easy to integrate

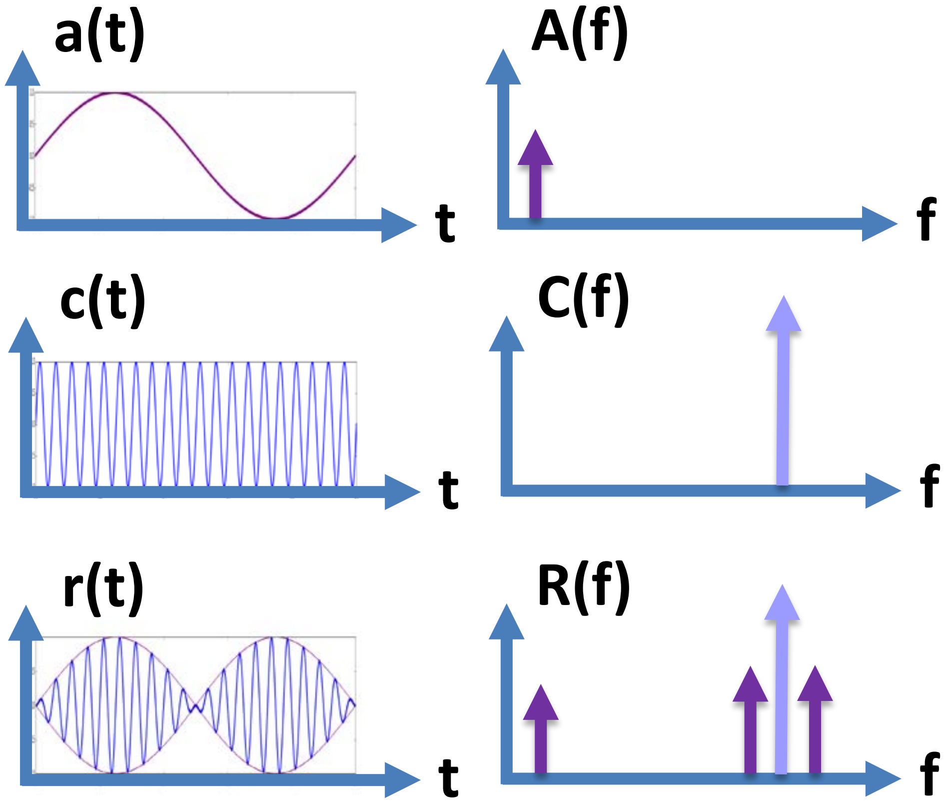
Examples:
BT, BLE, WiFi, GPS, etc

Issues

Reminder

Time vs. Frequency

Up-conversion



Issues

Analog/RF

Noise Sensitive

Digital

Noise resilient

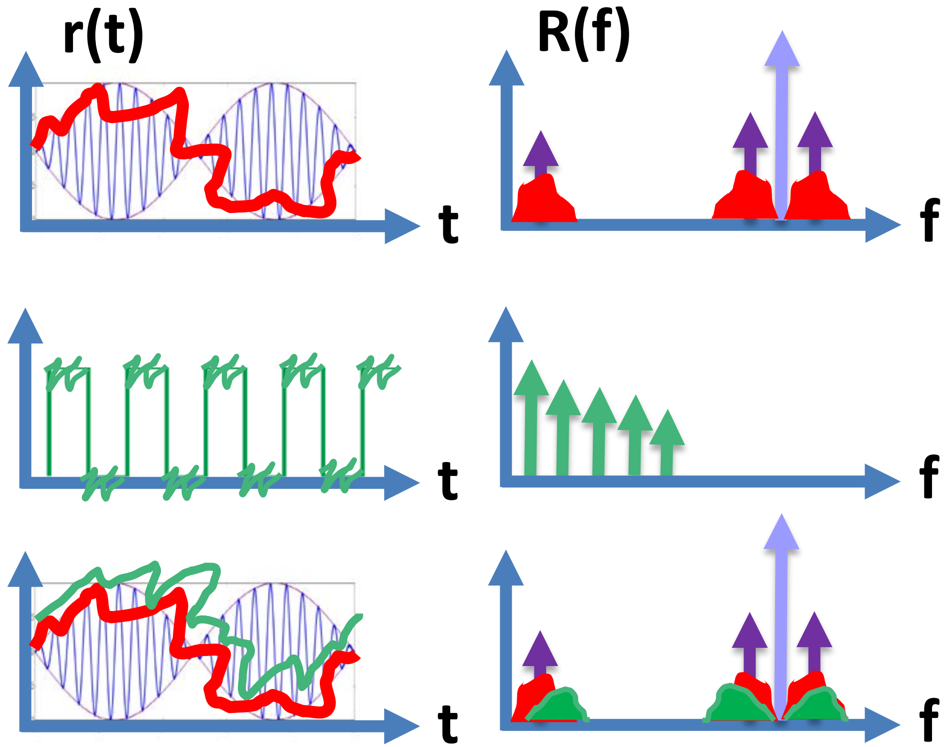
Noise Source

Same Chip

Noise Coupling

Careful Design

Radio Still Works



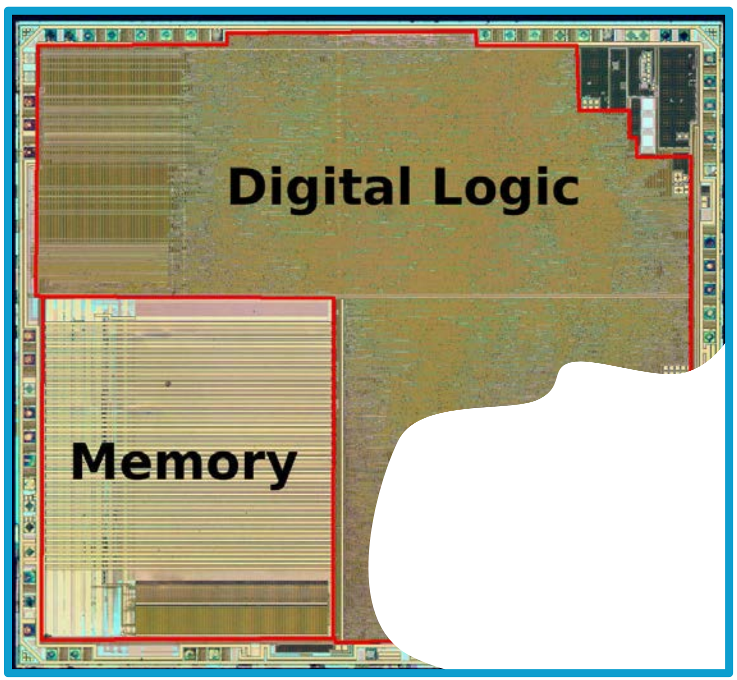
INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

Problems, the global view

Mixed-signal chip

Strong
noise
source



Easy propagation

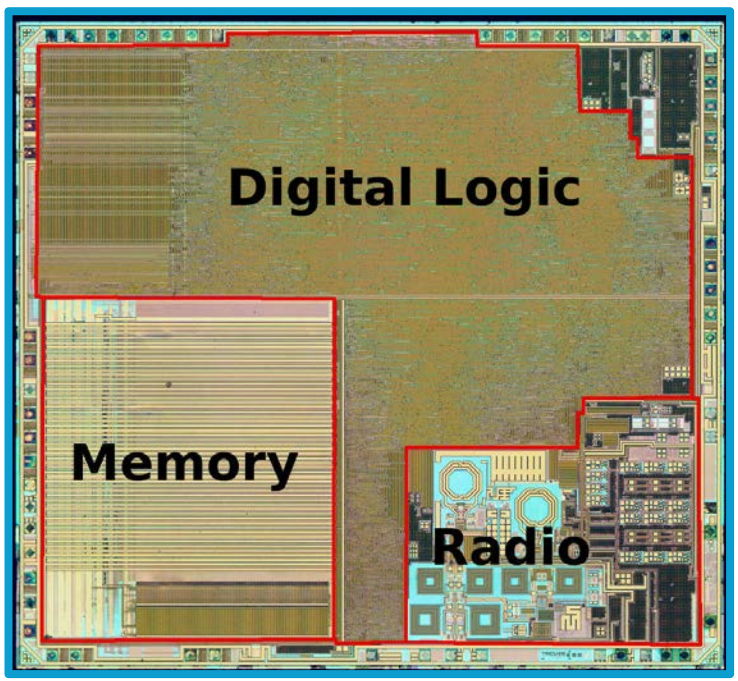
Screaming Channels
The Idea

Screaming Channels Idea

Conventional Side Channel Leak

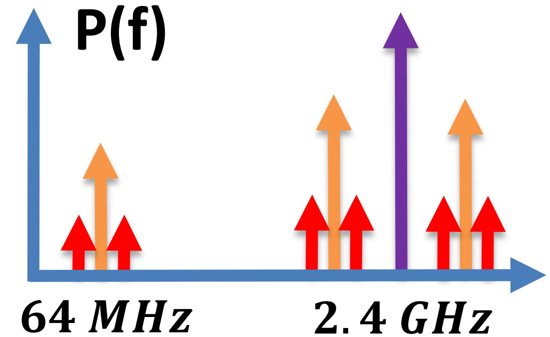
Strong noise source

Mixed-signal chip



Easy propagation

Leak Propagation



Noise sensitive transmitter

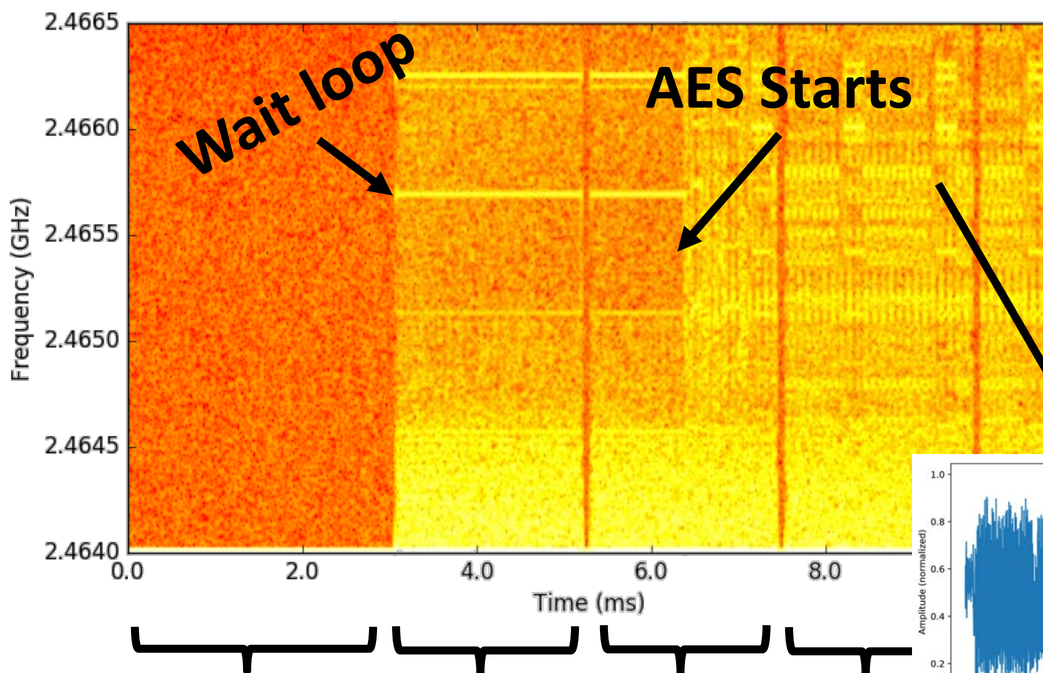
Leak Is Broadcast

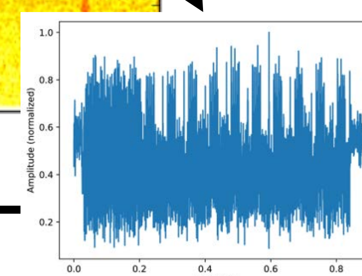
Screaming Channels in Action

Antenna + SDR RX

Cortex-M4
+ BT TX

Radio Off **Radio TX** **AES On**

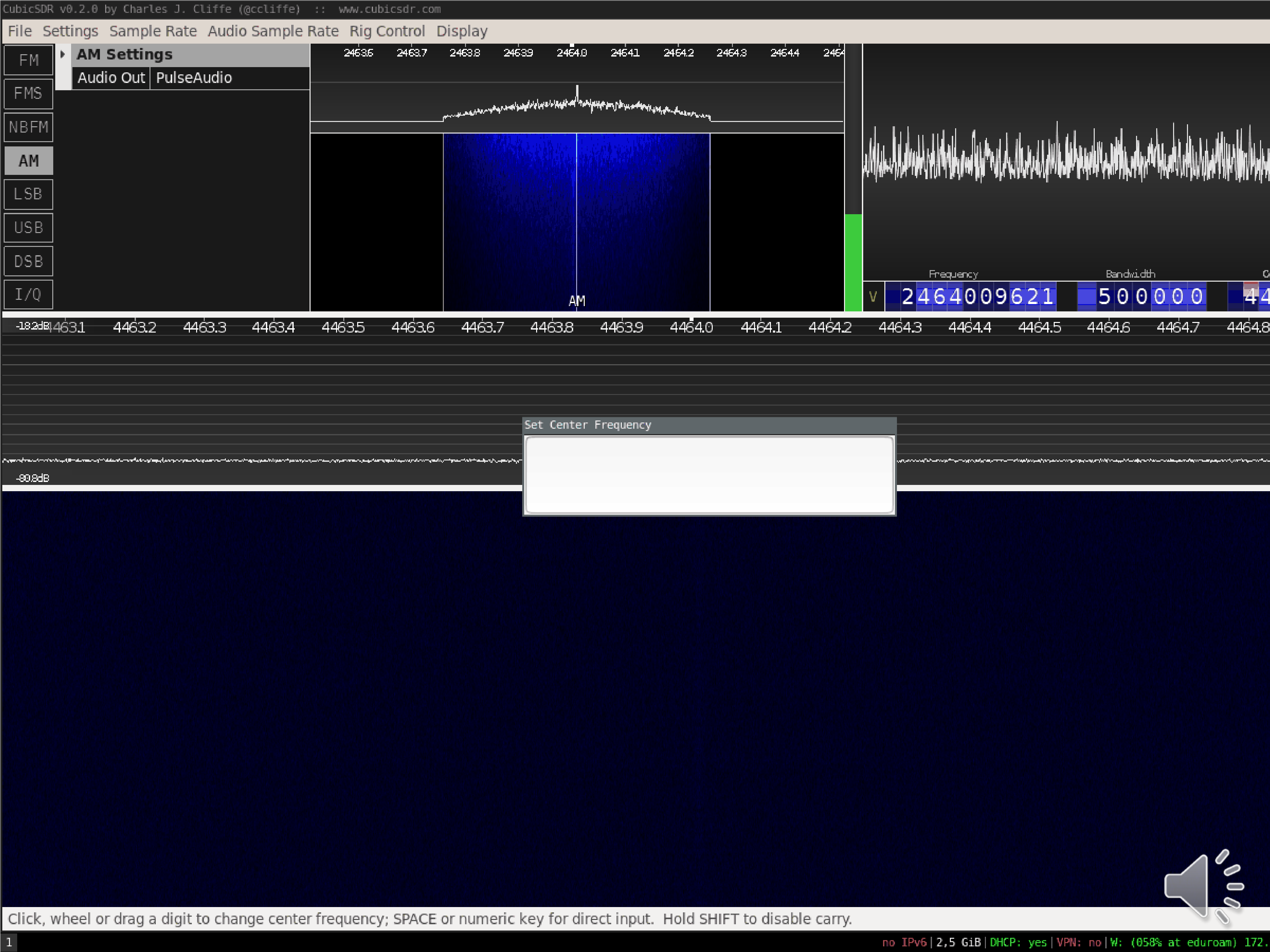




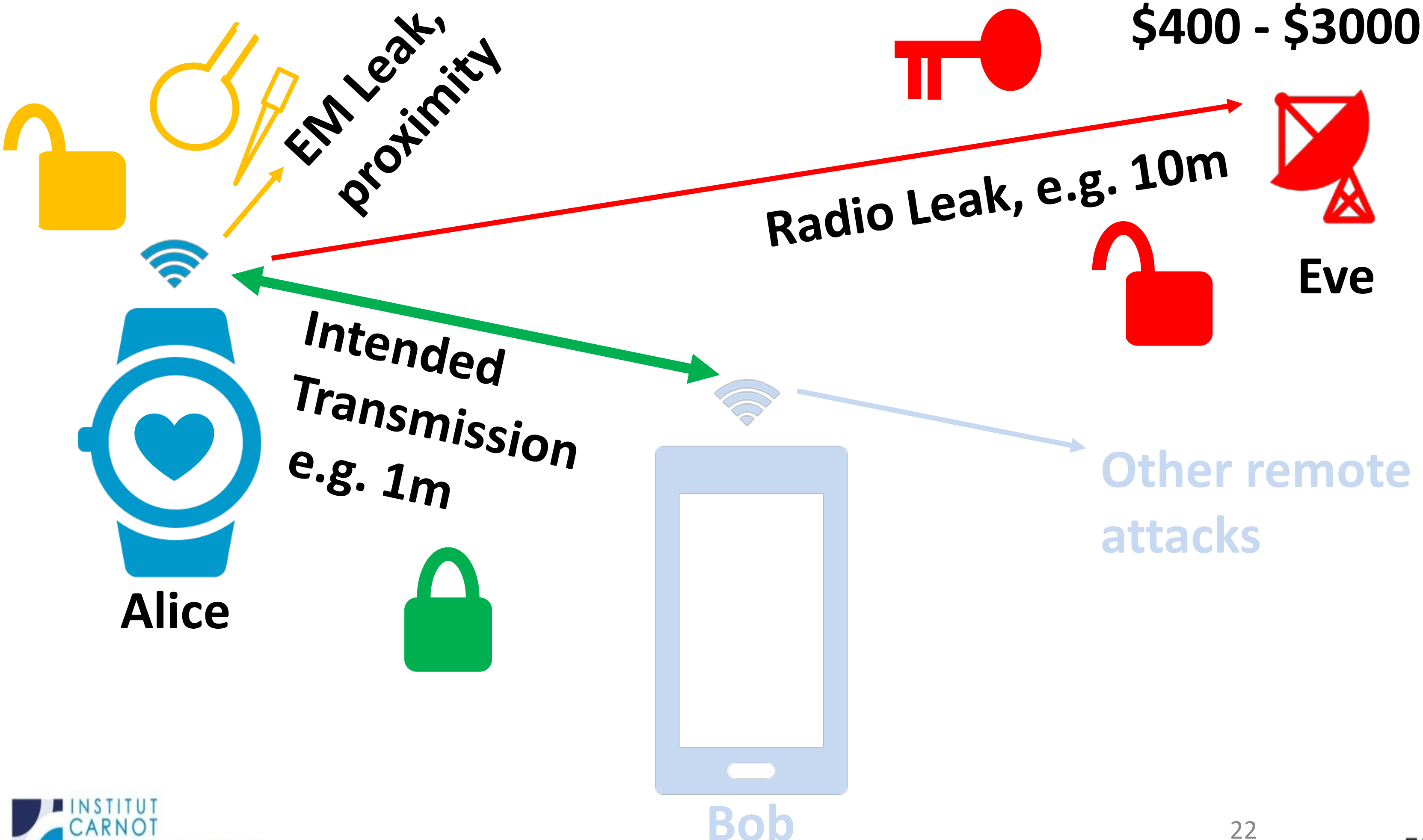
Time domain

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

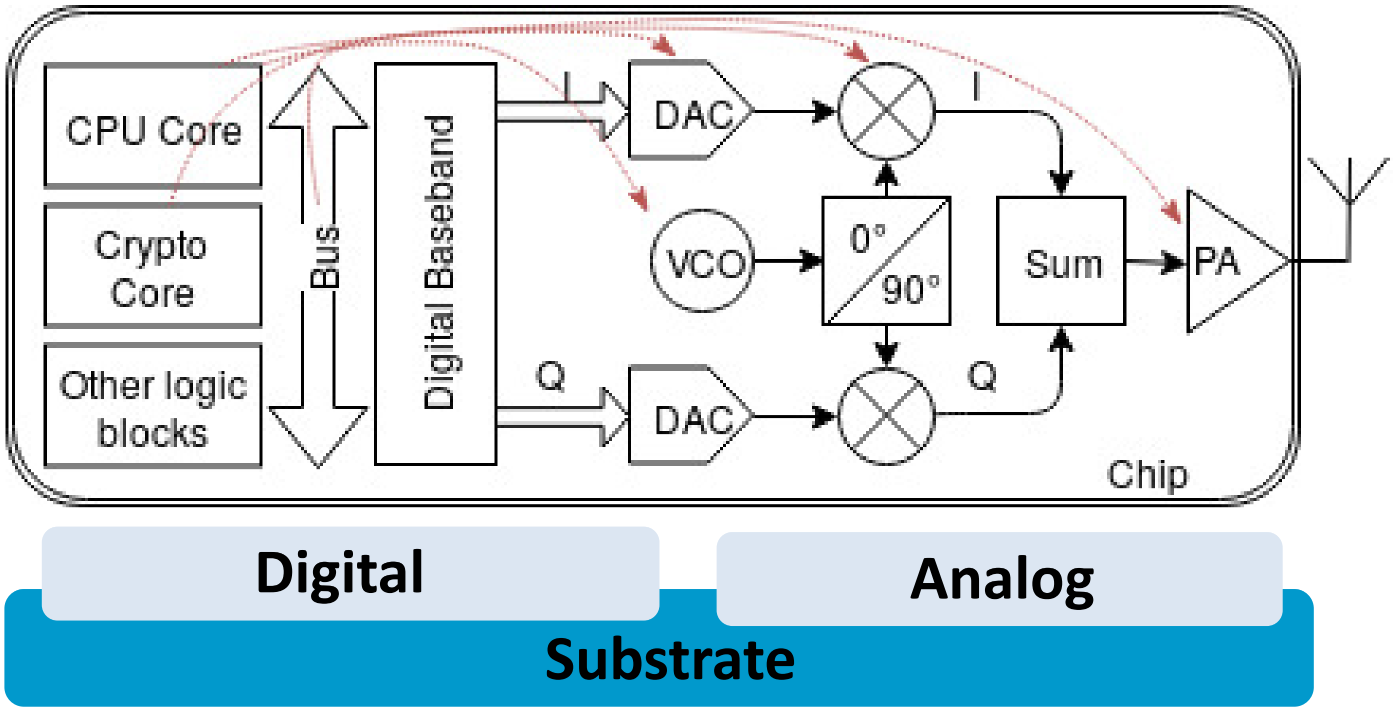

CubicSDR v0.2.0 by Charles J. Cliffe (@ccliffe) :: www.cubicsdr.com
File
Settings
Sample Rate
Audio Sample Rate
Rig Control
Display
FM
FMS
NBFM
AM
LSB
USB
DSB
I/Q
AM Settings
Audio Out
PulseAudio
AM
Frequency
Bandwidth
V
2464009621
500000
-182dB
-80.8dB
Set Center Frequency
Click, wheel or drag a digit to change center frequency; SPACE or numeric key for direct input. Hold SHIFT to disable carry.
no IPv6 | 2,5 GiB | DHCP: yes | VPN: no | W: (058% at eduroam) 172.

Screaming Channels: Leak Broadcast



From Digital Noise
To Noise On The Radio Signal

Possible Impact on Radio Transmission

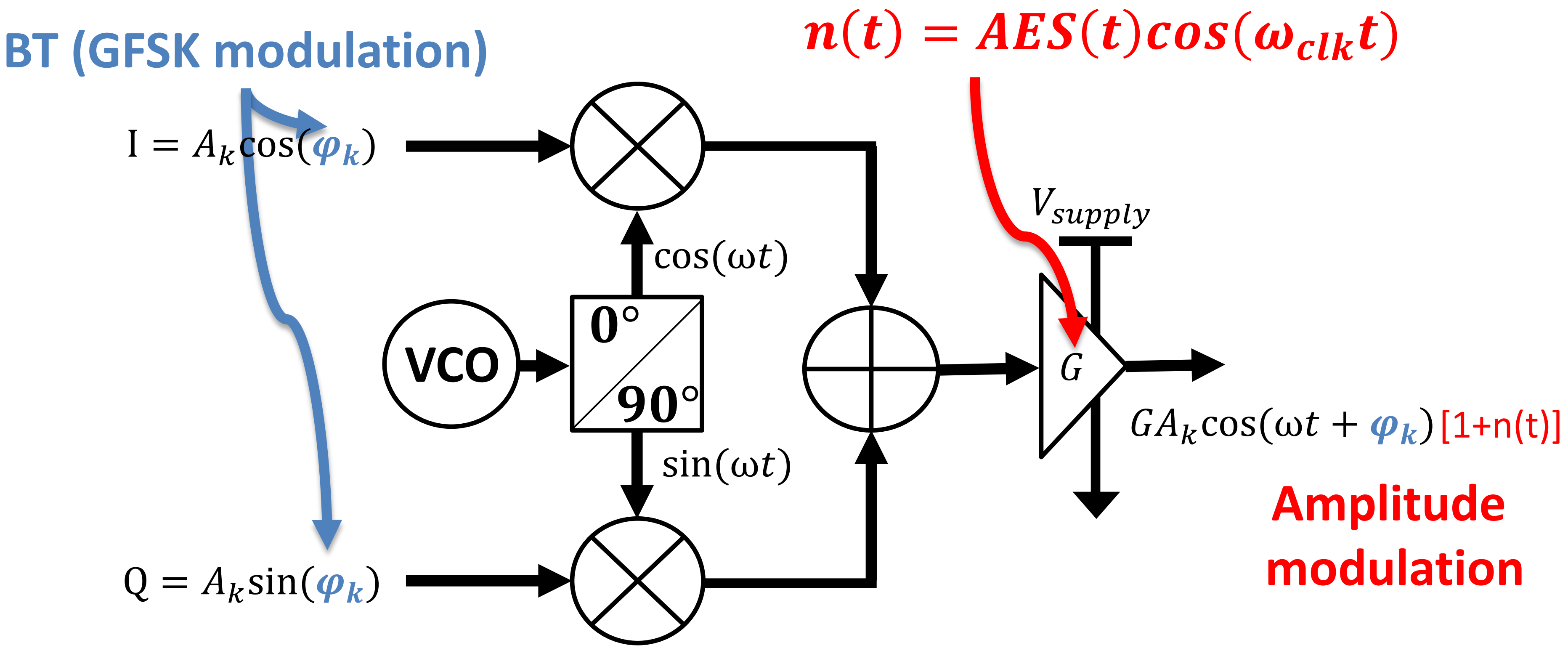


Digital: Inherently noisy

Propagation: Substrate coupling, Power supply/Gnd

Analog: Noise sensitive

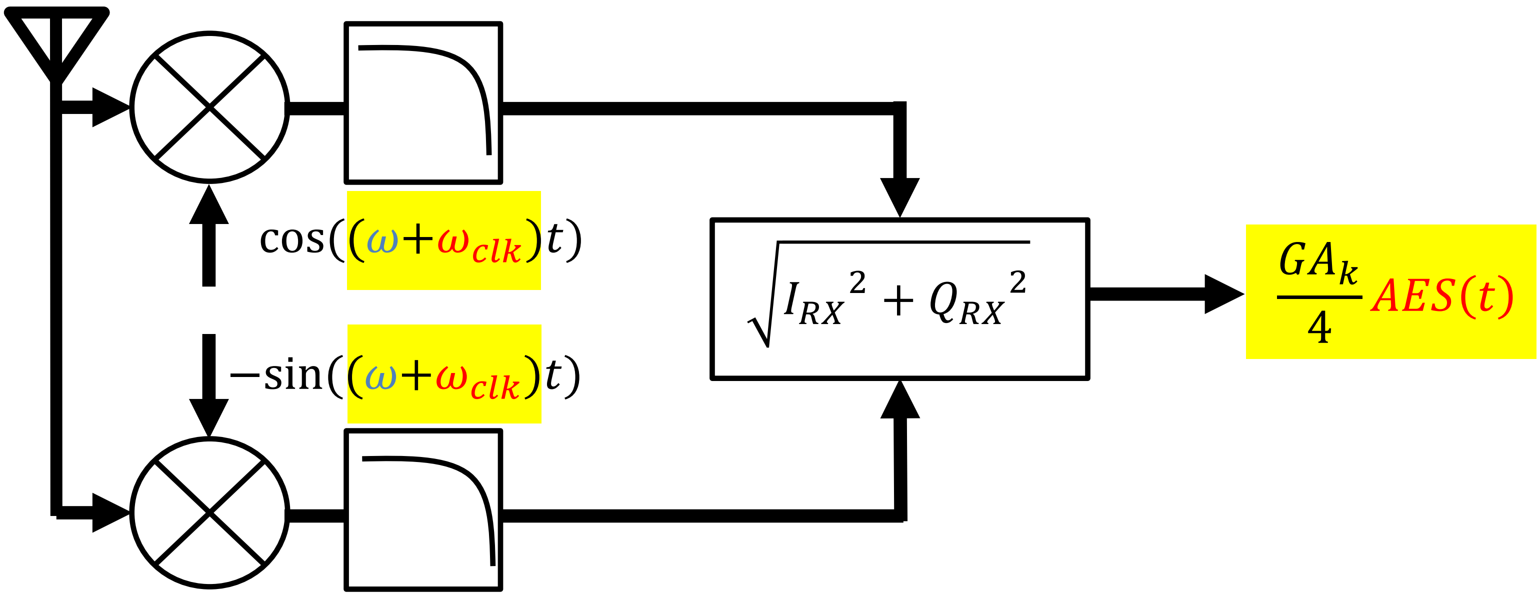
Practical Case We Observed



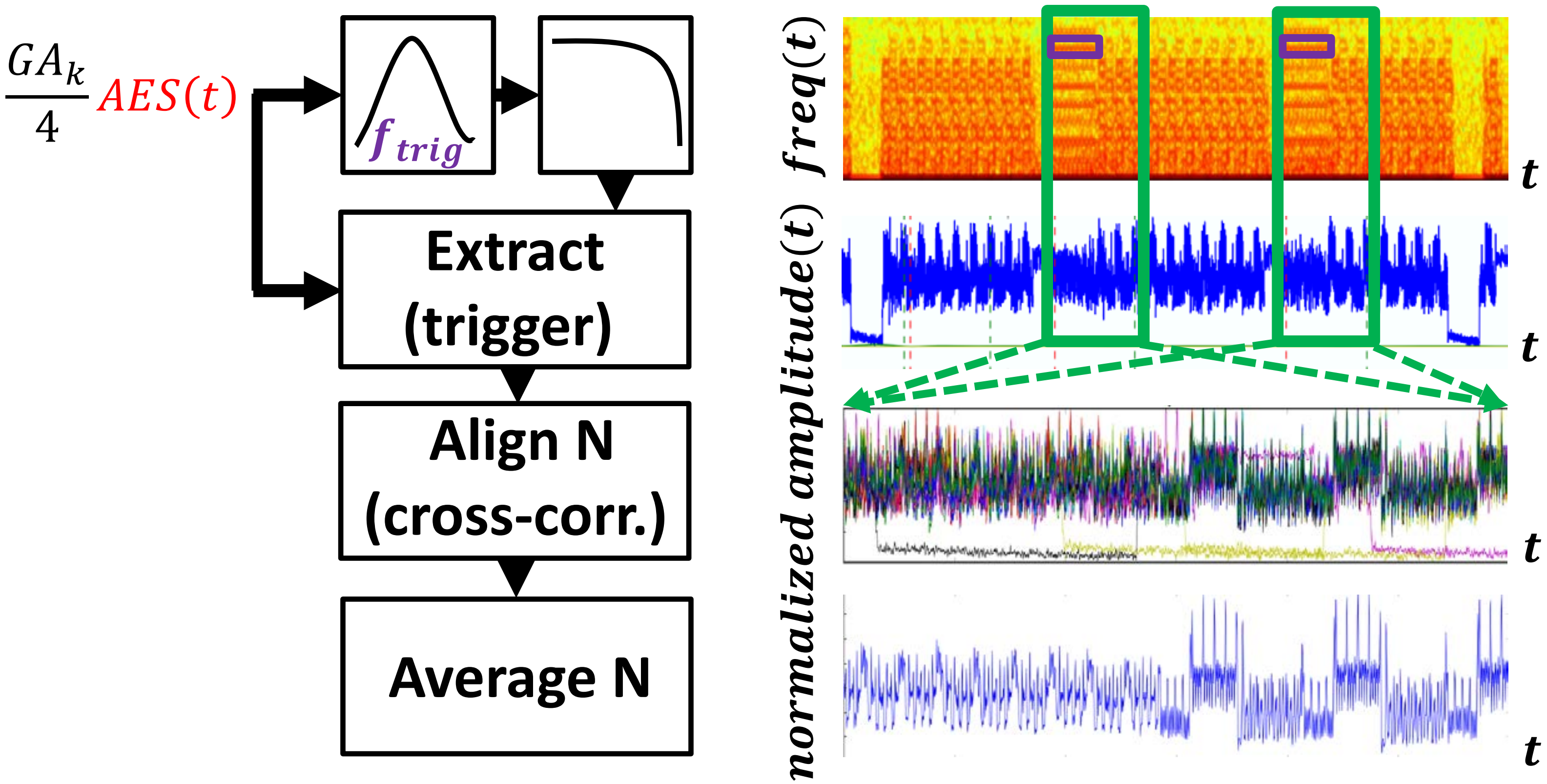
Extraction

Quadrature Amplitude Demodulation

$$\frac{GA_k}{2} AES(t)\cos((\omega+\omega_{clk})t+\varphi_k)$$



Extraction


$\frac{GA_k}{4} AES(t)$
f_{trig}
Extract (trigger)
Align N (cross-corr.)
Average N
$freq(t)$
$normalized\ amplitude(t)$
t
t
t
t

Attack

Attacking

Targets:
Cortex-M4 + BT TX
TinyAES, mbedTLS

Extraction:
Automated via radio
Known plaintext

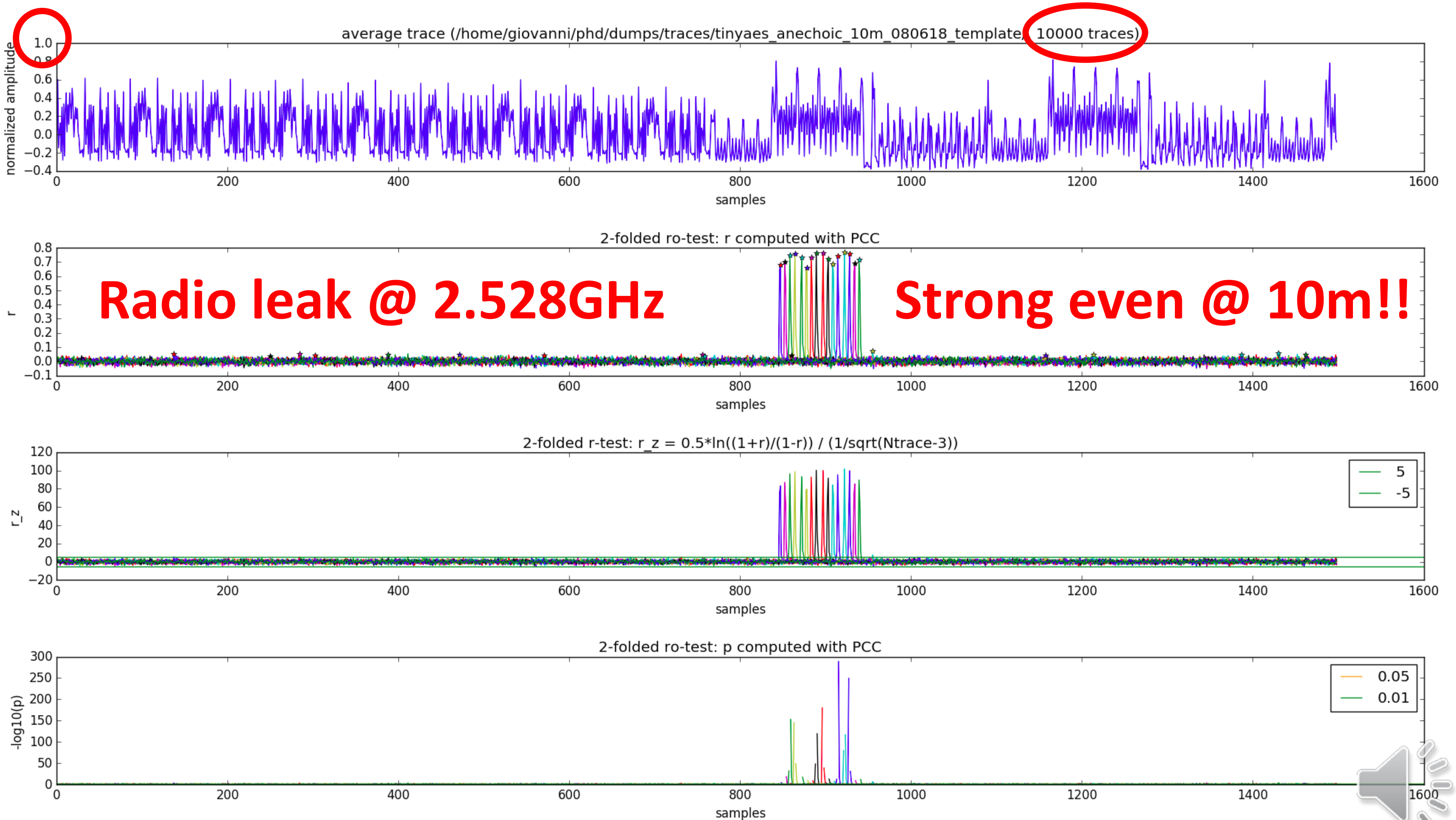
Attacks:
Correlation, Template
Code based on
ChipWhisperer

Much more advanced attacks exist

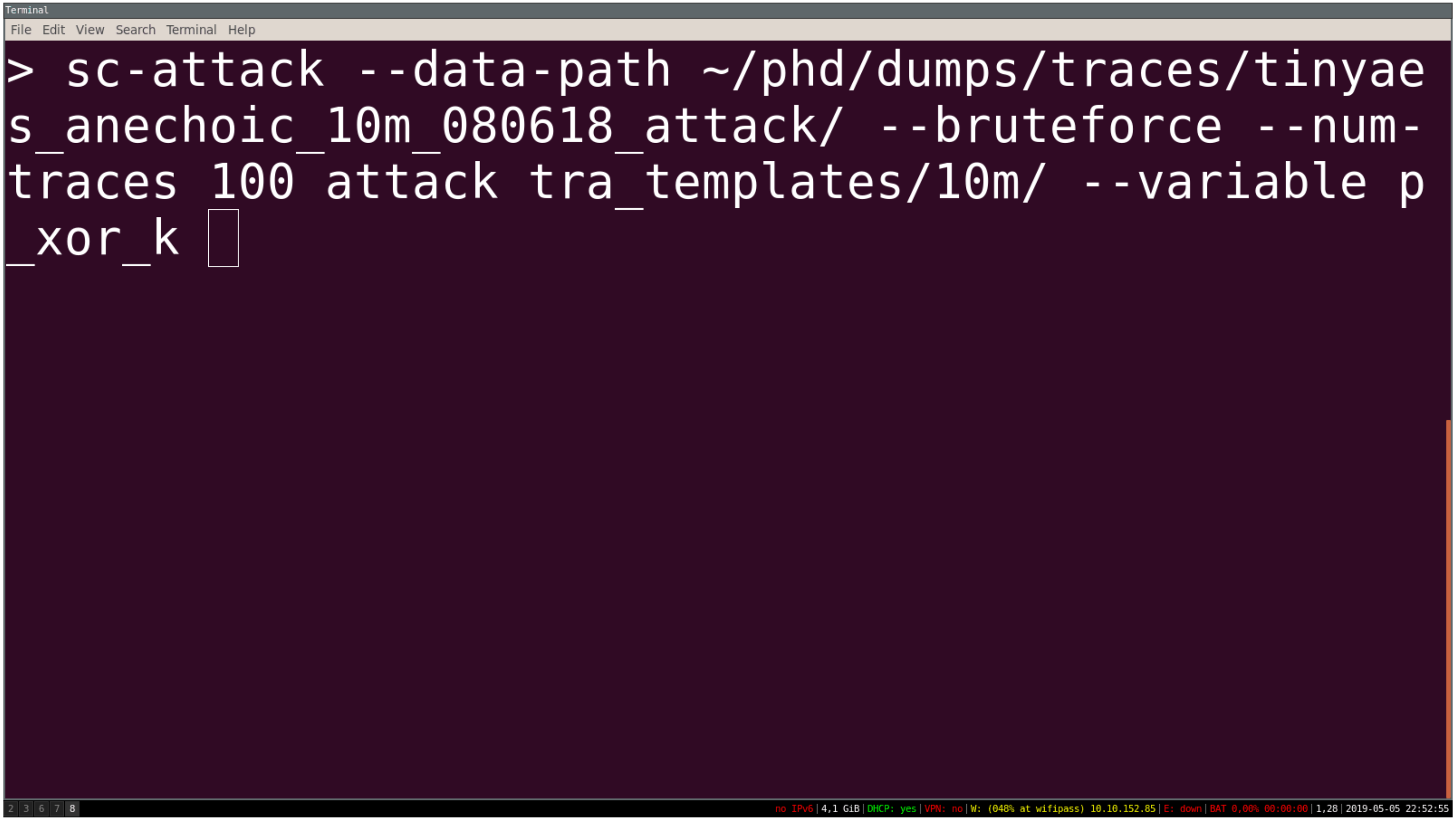
INSTITUT CARNOT
Télécom & Société numérique

EURECOM
Sophia Antipolis

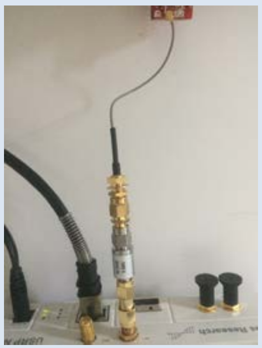
Correlation @ 10m



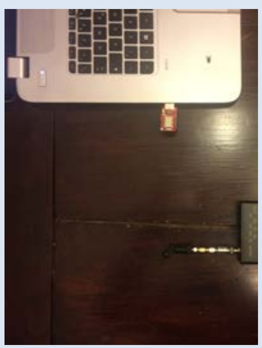
Quick Demo


Terminal
File Edit View Search Terminal Help
> sc-attack --data-path ~/phd/dumps/traces/tinyaes_anechoic_10m_080618_attack/ --bruteforce --num-traces 100 attack tra_templates/10m/ --variable p_xor_k
2019-05-05 22:52:55

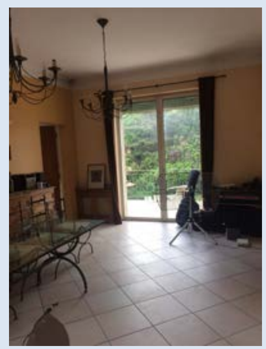
Evolution of the attack



$Cable$



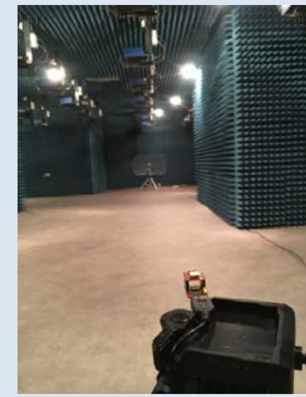
$15\ cm$



$2\ m$

$3\ m$

$5\ m$



$10\ m$

Protection

Countermeasures

Resource constraint devices:
Cost, power, time to market, etc.

Classic HW/SW:
Masking, noise, key refresh (expensive, not complete)

Specific (SW):
Radio off during sensitive computations (real time constraints)

Specific (HW):
Consider impact of coupling on security during design and test (hard, expensive)

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

Final remarks

Reference to a Similar Effect

1-5. (~~C~~) **Propagation of TEMPEST Signals (U).** - There are four basic means by which compromising emanations may be propagated. They are: electromagnetic radiation; conduction; modulation of an intended signal; and acoustics. A brief explanation of each follows.

a. (~~C~~) Electromagnetic Radiation (U). - Whenever a RED signal is generated or processed in an equipment, an electric, magnetic or electromagnetic field is generated. If this electromagnetic field is permitted to exist outside of an equipment, a twofold problem is created; first the electromagnetic field may be detected outside the Controlled Space (CS); second the electromagnetic field may couple onto BLACK lines connected to or located near the equipments, which exit the CS of the installation.

b. (~~C~~) Line Conduction. - Line Conduction is defined as the emanations produced on any external or interface line of an equipment, which, in any way, alters the signal on the external or interface lines. The external lines include signal lines, control and indicator lines, and a.c. and d.c. powerlines.

c. (~~C~~) Fortuitous Conduction. - Emanations in the form of signals propagated along any unintended conductor such as pipes, beams, wires, cables, conduits, ducts, etc.

d. (~~C~~) [Six lines redacted.]

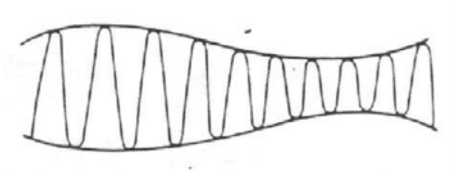


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

e. (~~C~~) Acoustics (U) - Characteristically plaintext processing systems are primarily electrical in function. However, other sources of CE exist where mechanical operations occur and sound is produced. Keyboards, printers, relays -- these produce sound. and consequently can be sources of compromise.

Propagation of leaks:

1. **Radiation**
2. **Conduction**
3. **Modulation of an intended signal (redacted)**
4. **Acoustic**

Tempest Fundamentals [5]
From ‘80s
Declassified 2000

Responsible Disclosure

Major vendors & multiple CERTS

Multiple acknowledgements of the relevance and generality of the problem

2 vendors are reproducing our results
1 vendor is actively looking at short/long-term countermeasures

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

Conclusion

General problem if sensitive processing and wireless tx

- **HW AES, WiFi, other chips**
- **any device with radio?**

A new point in the threat model space

- **Remote EM attacks**

Must be considered

- **Design and test of new devices**
- **Smart countermeasures (specific)**

Many open directions for future research

- **More distant, less traces**
- **Different crypto and wireless technologies**
- **Attack the protocol**

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

Questions?

Code

https://www.github.com/eurecom-s3/screaming_channels

More Info

https://s3.eurecom.fr/tools/screaming_channels

Giovanni Camurati

@GioCamurati

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

Acknowledgements

- The authors acknowledge the support of SeCiF project within the French-German Academy for the Industry of the future, as well as the support by the DAPCODS/IOTics ANR 2016 project (ANR-16-CE25-0015).
- We would like to thank the FIT R2lab team from Inria, Sophia Antipolis, for their help in using the R2lab testbed.

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

References

- [1] Agrawal, Dakshi, et al. “The EM Side-Channel(s)” CHES '02
- [2] Genkin, Daniel, et al. "ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs." Cryptographers’ Track at the RSA Conference. Springer, Cham, 2016.
- [3]Tempest attacks against AES: https://www.fox-it.com/en/wp-content/uploads/sites/11/Tempest_attacks_against_AES.pdf
- [4] Van Eck Phreaking

https://en.wikipedia.org/wiki/Van_Eck_phreaking

- [5] NSA. “NACSIM 5000, Tempest fundamentals.” Technical Report. 1982. Document declassified in 2000 and available at https://cryptome.org/jya/nacsim-5000/nacsim-5000.htm

Third-Party Images

- "nRF51822 - Bluetooth LE SoC : weekend die-shot" - CC-BY– Modified with annotations. Original by zeptobars https://zeptobars.com/en/read/nRF51822-Bluetooth-LE-SoC-Cortex-M0

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

GRADUATE SCHOOL & RESEARCH CENTER IN DIGITAL SCIENCE

Institut Mines-Télécom

EURECOM
Sophia Antipolis

Academia

Institut Mines-Télécom

Politecnico di Torino

Aalto University

Technische Universität München

NTNU
Norwegian University of Science and Technology

CHALMERS
UNIVERSITY OF TECHNOLOGY

CZECH TECHNICAL UNIVERSITY IN PRAGUE

Industry and Institutions

orange

SAP

BMW GROUP THE NEXT 100 YEARS

IABG

Symantec.

monaco telecom

Gouvernement Princier
PRINCIPAUTÉ DE MONACO

www.eurecom.fr

Backup Slides

Some Attack Data

Distance	Environment	Implementation	# Attack Traces	# Template Traces
1 m	Office	tinyAES	52589 x 500	70000 x 500
3 m	Anechoic Room	tinyAES	718 x 500	70000 x 500
5m	Anechoic Room	tinyAES	428 x 500	70000 x 500
10 m	Anechoic Room	tinyAES	1428 x 500	130000 x 500

Attack on Hardware AES, possible?

- Hardware AES implementations are used for link layer encryption

- Attacking turns out to be more difficult than software AES
  - Faster calculation, higher radio resolution is needed
  - Most of the time blackbox implementations

- We ran some experiments
  - 4/16 bytes recovered