EURECOM
Sophia Antipolis

Screaming Channels

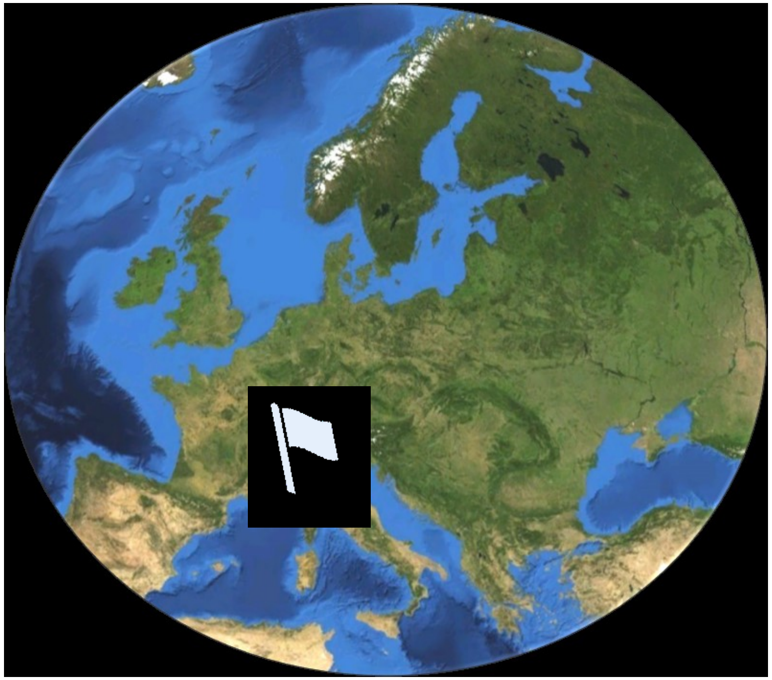
When Electromagnetic Side Channels Meet Radio Transceivers

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"

Side Channels, The Idea

Theory

Secure lock is impossible to open

Side Channels, The Idea

Theory

Secure lock is impossible to open

Side Channels, The Idea

Theory

Secure lock is impossible to open

Implementation

Different sound if we make a partial correct guess

Side Channels, The Idea

Theory

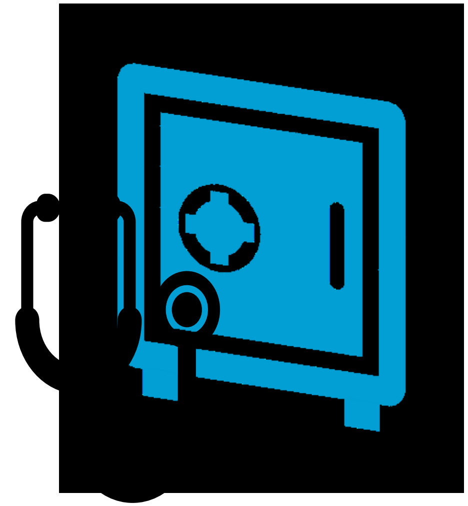
Secure lock is impossible to open

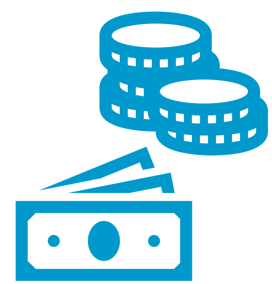
Implementation

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, ...

Embedded Devices and Side Channels

Secure systems: E-Passport, Smartcard, …

Crypto against stealing, cloning, tampering, …

Embedded Devices and Side Channels

Secure systems: E-Passport, Smartcard, …

Crypto against stealing, cloning, tampering, …

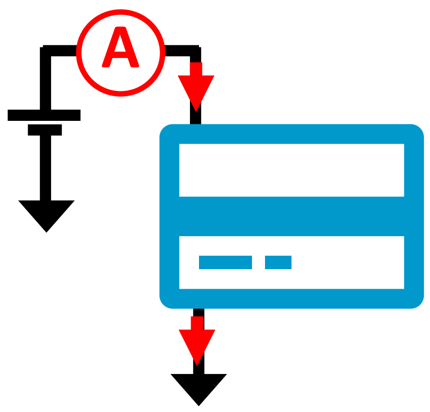
Generally protected against attacks which require physical access

Conventional Side Channels

Physical activity depends on logic data

Conventional Side Channels

Power (current)

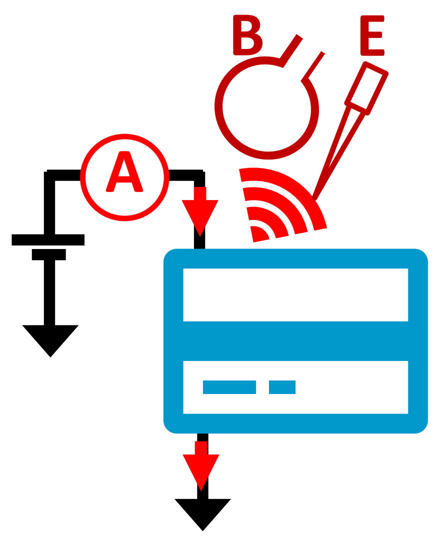


Physical activity depends on logic data

Conventional Side Channels

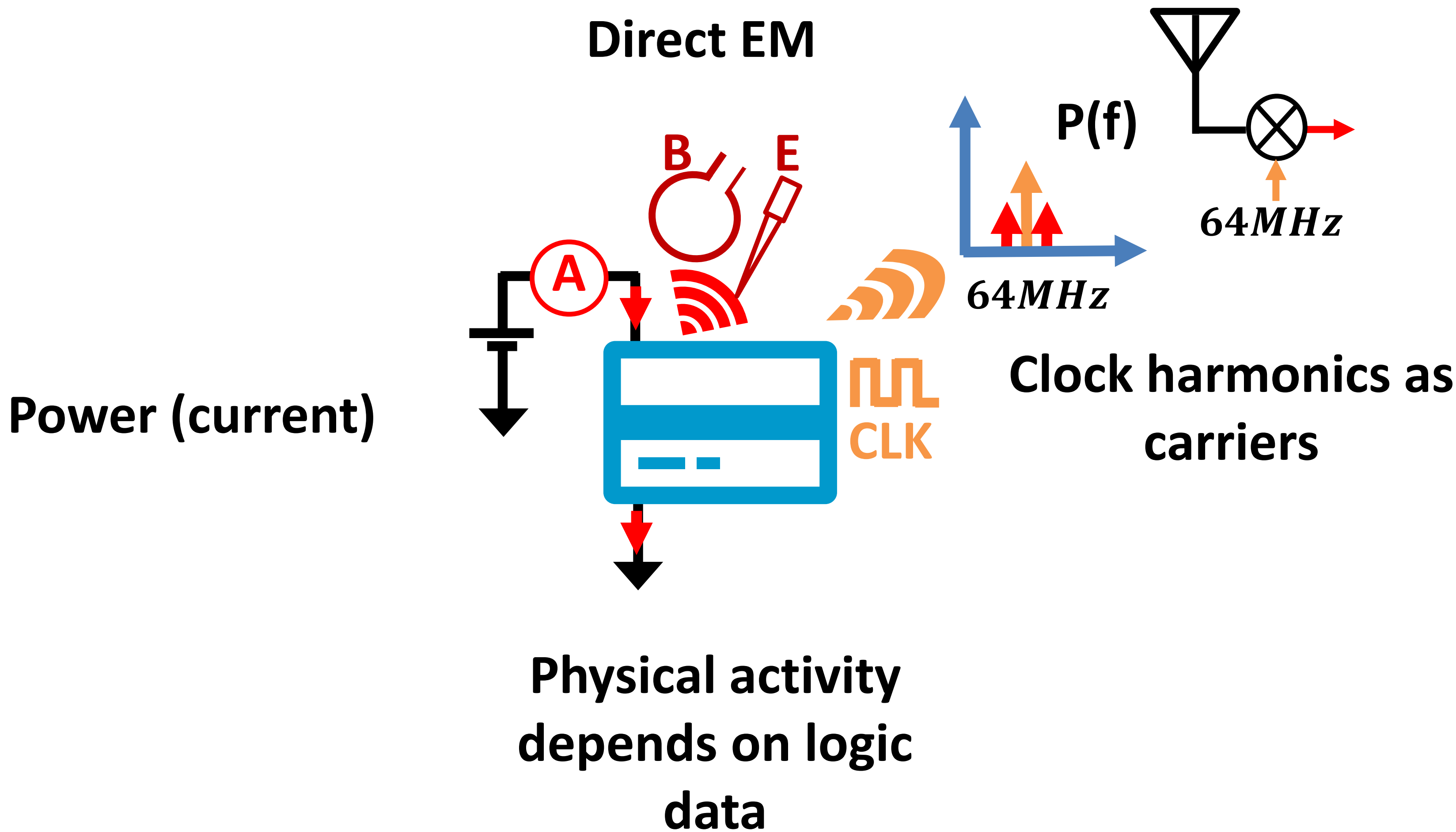
Direct EM

Power (current)

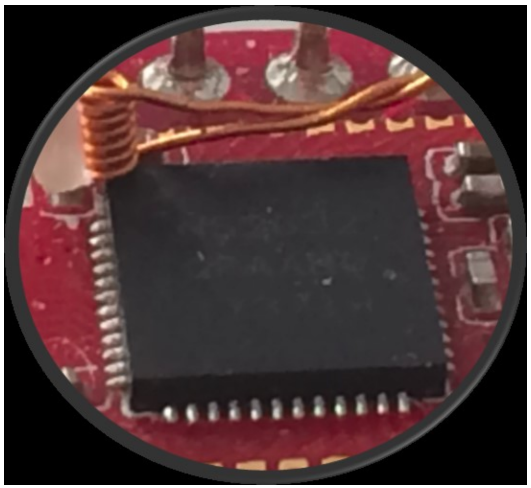


Physical activity depends on logic data

Conventional Side Channels



In Practice

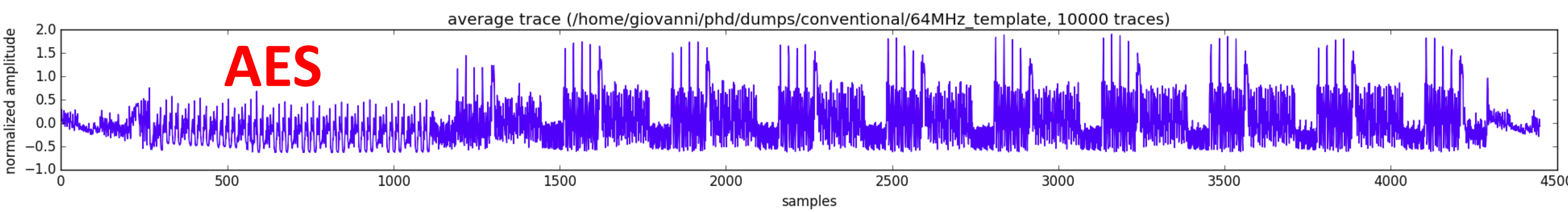


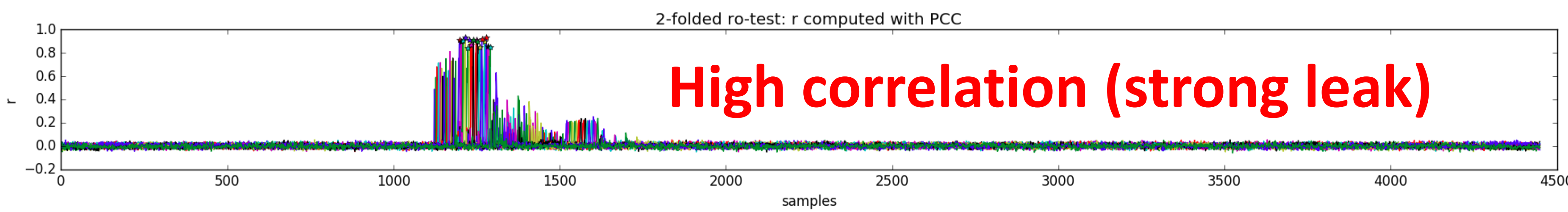
Collection

E.g. loop probe
+ oscilloscope

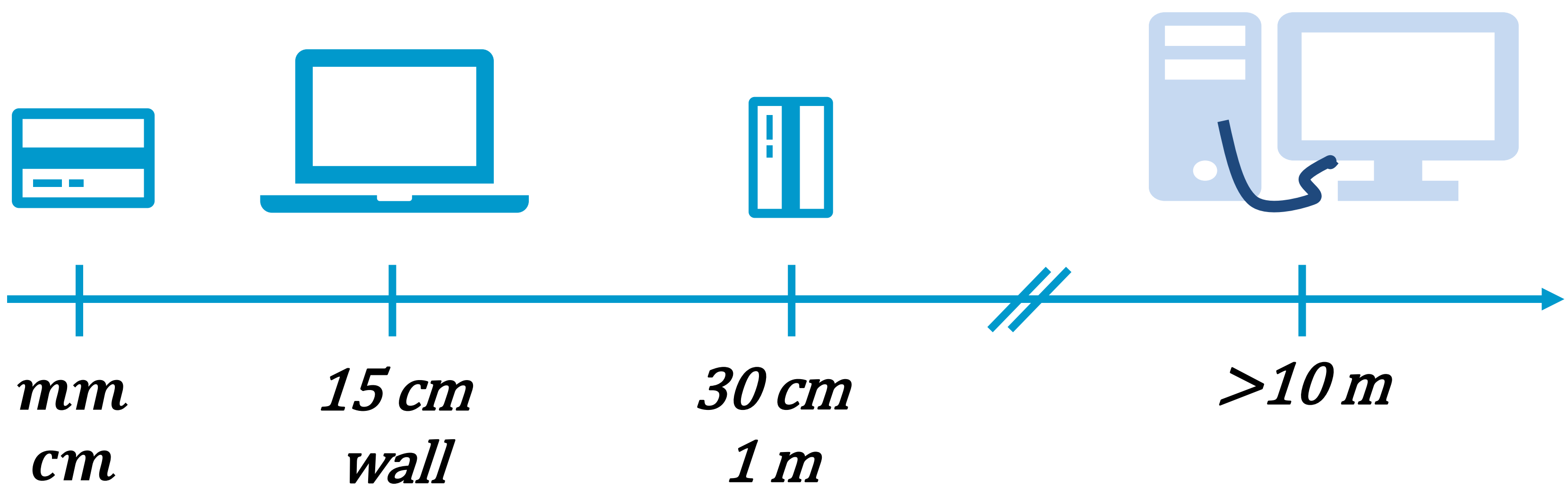
Many Analyses/Attacks

SPA, CPA, TPA, …
SEMA, CEMA, TEMA, …

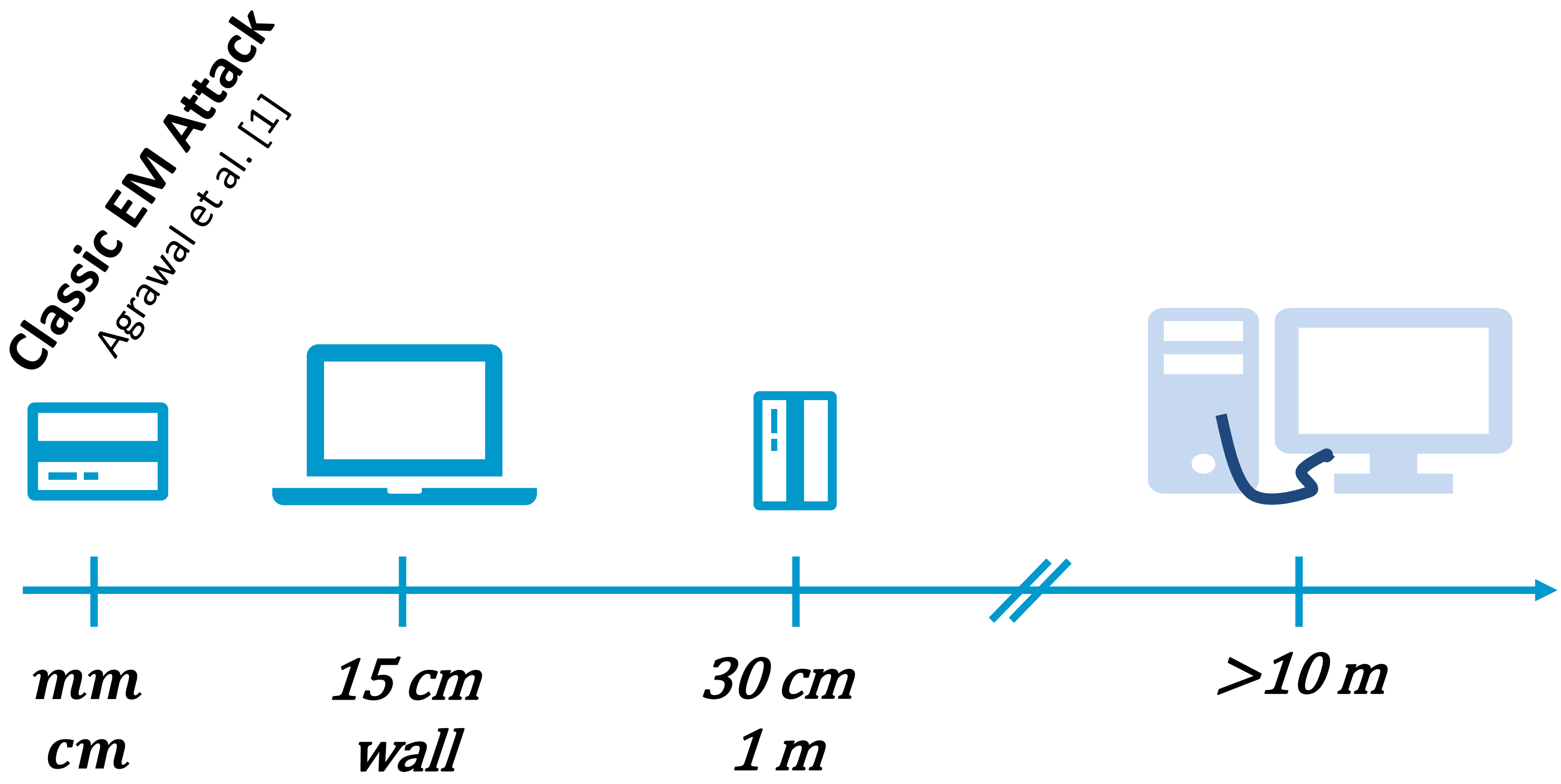




Many Side Channels Involving EM



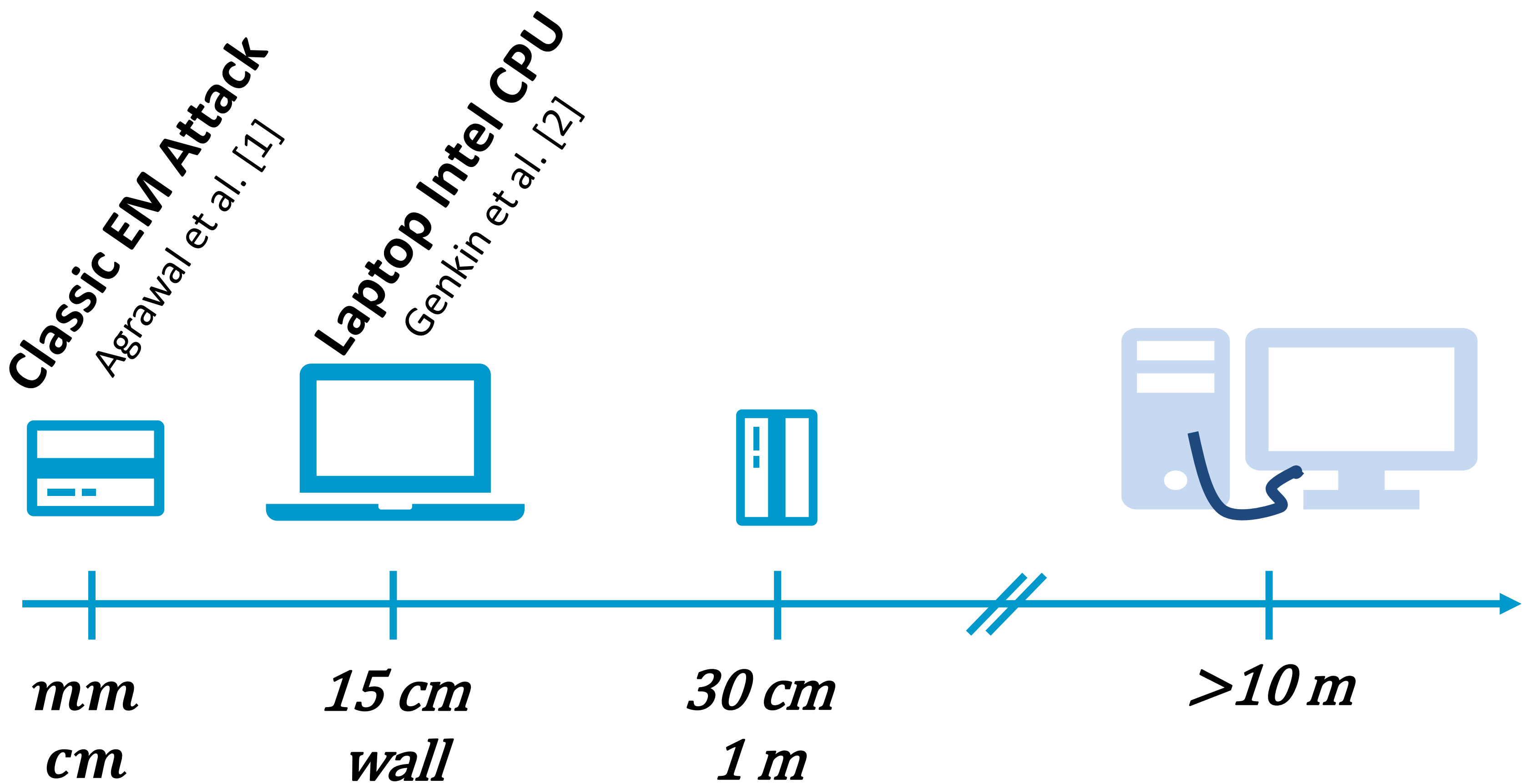
Many Side Channels Involving EM



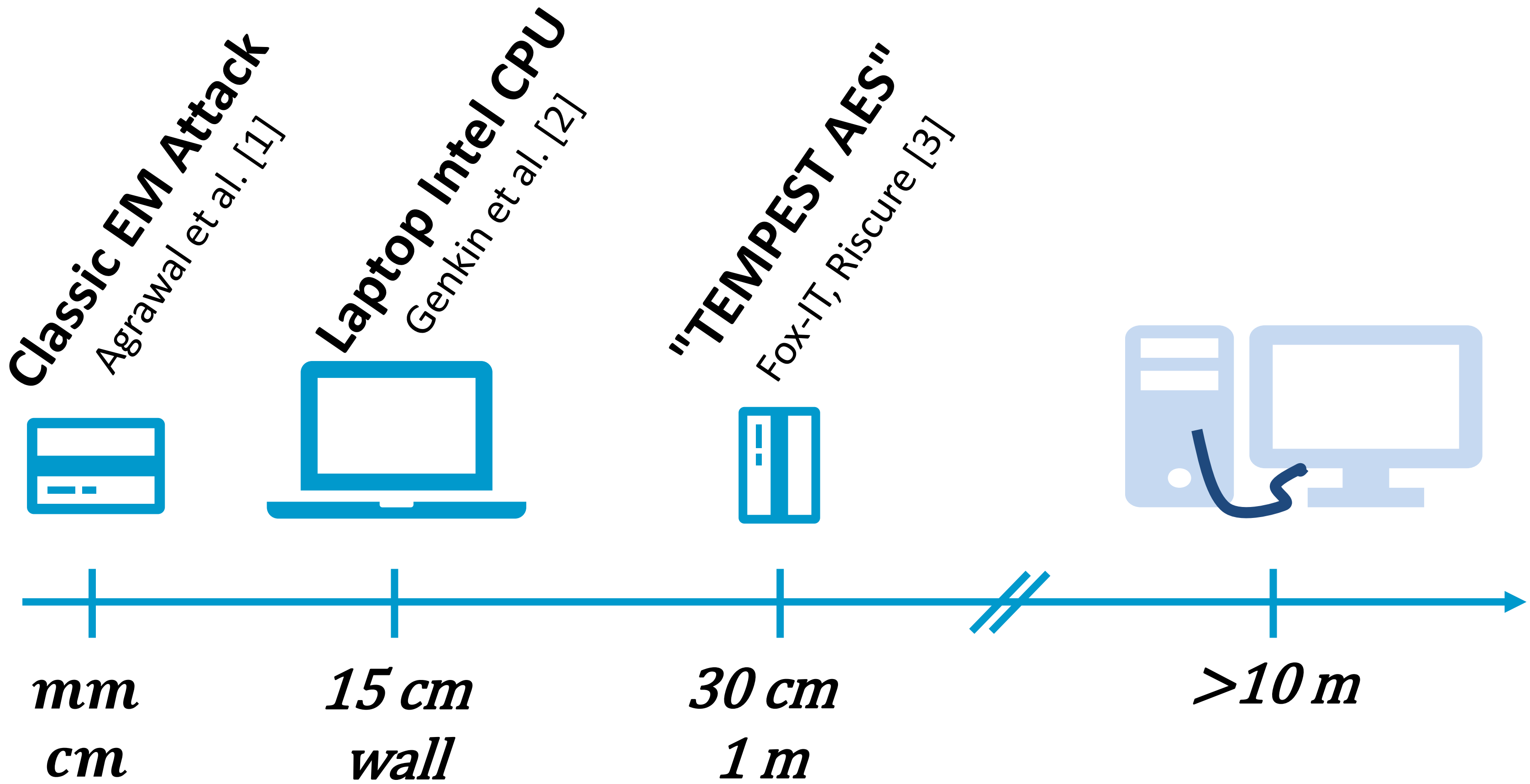
INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

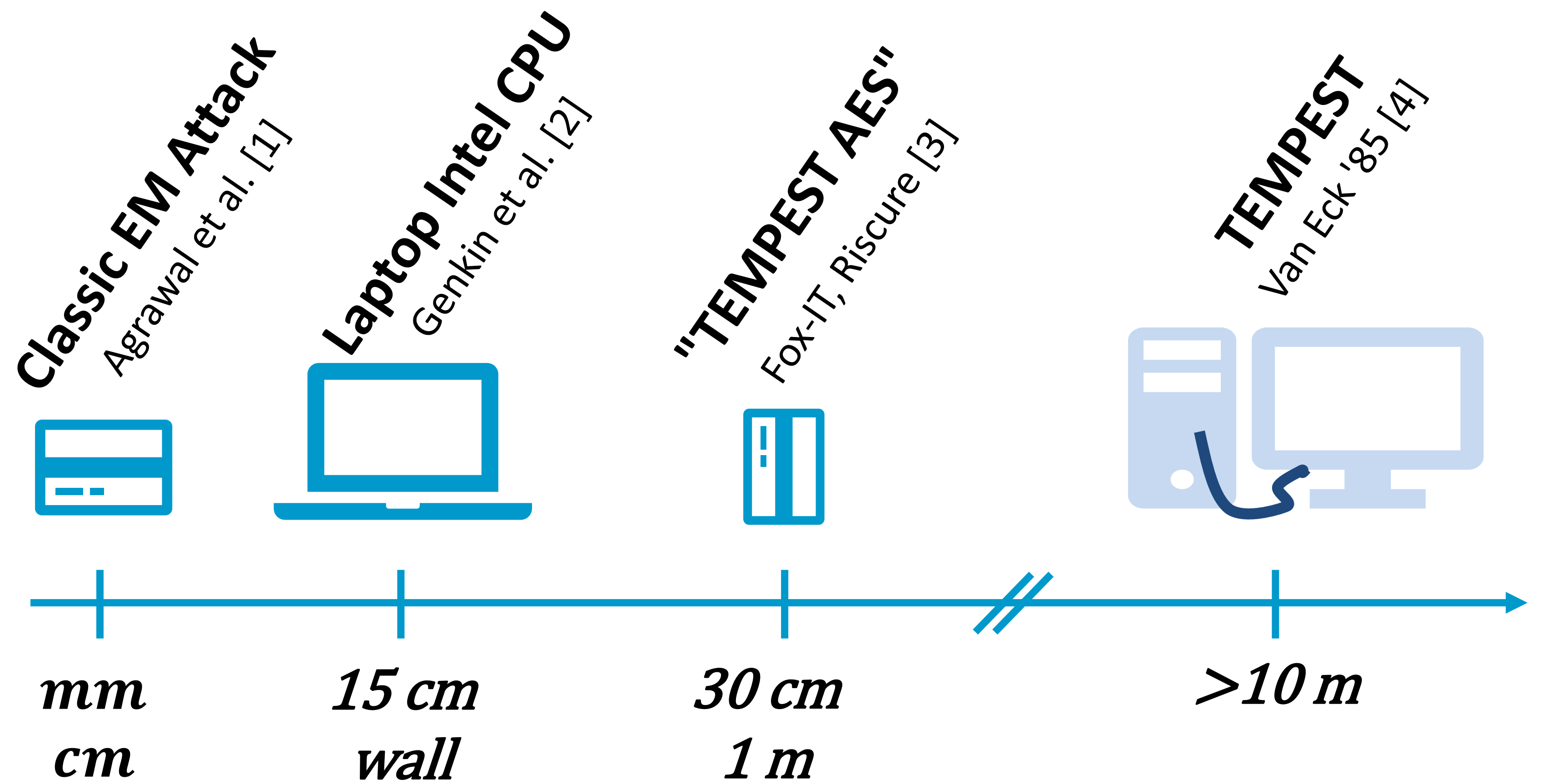
Many Side Channels Involving EM



Many Side Channels Involving EM



Many Side Channels Involving EM



Many Side Channels Involving EM

Classic EM Attack
Agrawal et al. [1]

Laptop Intel CPU
Genkin et al. [2]

"TEMPEST AES"
Fox-IT, Riscure [3]

TEMPEST
...n Eck '85 [4]

mm
cm

15 cm
wall

30 cm
1 m

Many Side Channels In

Classic EM Attack
Agrawal et al. [1]

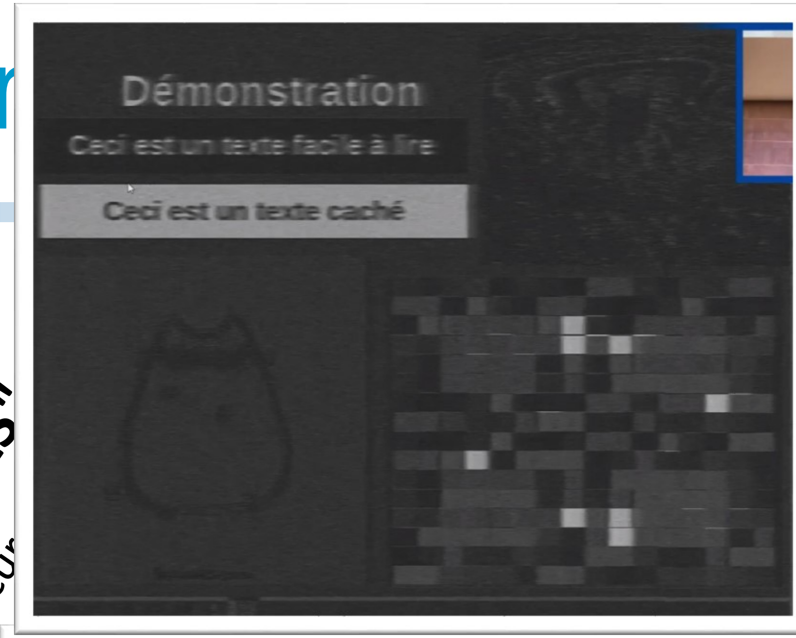
Laptop Intel CPU
Genkin et al. [2]

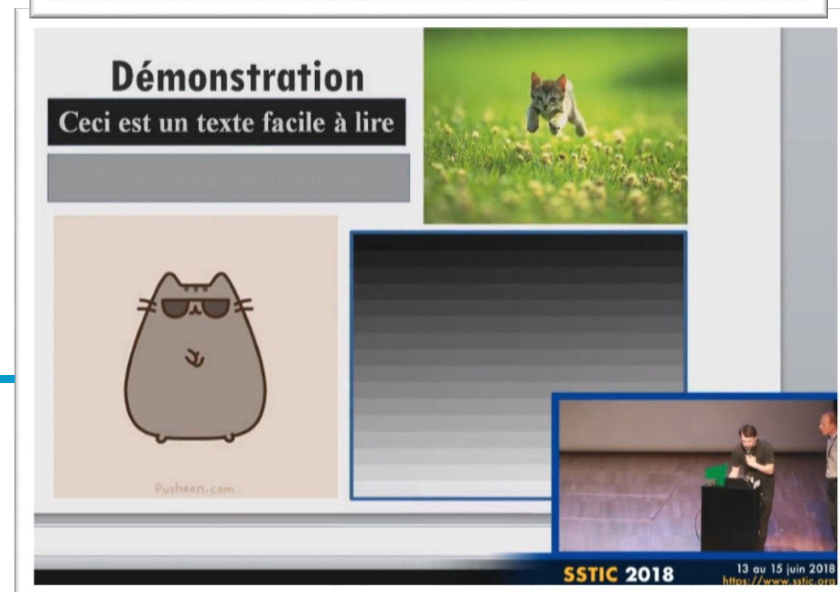
"TEMPEST AES"
Fox-IT, Riscu

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

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, …

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

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

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

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

Remote Side Channels

Remote Timing

Non constant time

Caches

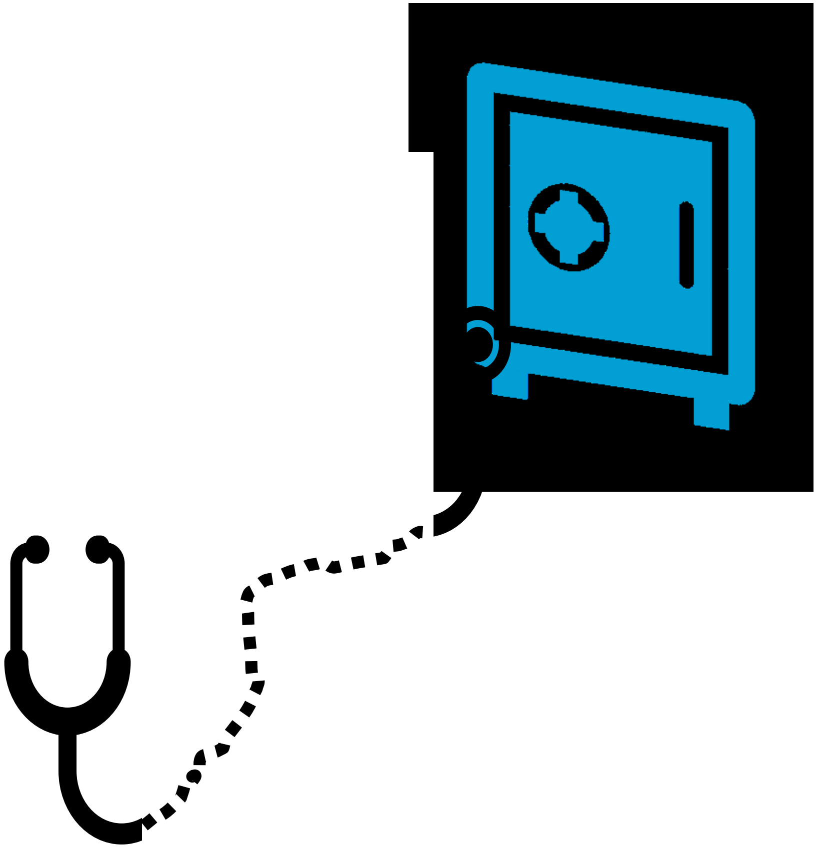
AES, TLS, …

WPA3 (Dragonblood)

EM?

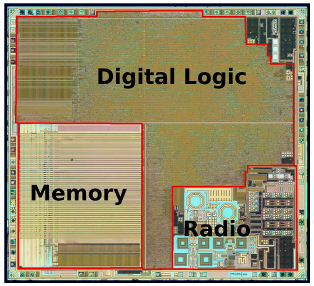
Physical access

Local



Problems When Adding Wireless Capabilities

Implementation: Mixed-signal Chips

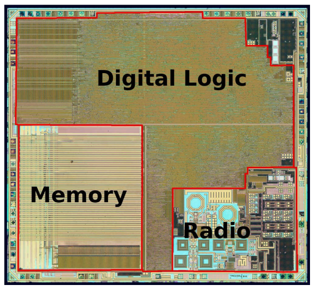


Idea:

CPU + Crypto + Radio

Same chip

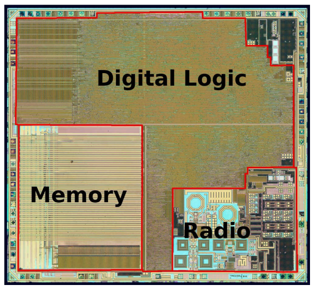
Implementation: Mixed-signal Chips



Idea:
CPU + Crypto + Radio
Same chip

Benefits:
Low Power, Cheap, Small
Easy to integrate

Implementation: Mixed-signal Chips



Idea:
CPU + Crypto + Radio
Same chip

Benefits:
Low Power, Cheap, Small
Easy to integrate

Examples:
BT, BLE, WiFi, GPS, etc

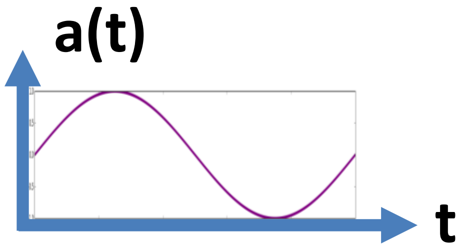
Issues

Reminder

Time vs. Frequency

Up-conversion

Issues



Reminder

Time vs. Frequency

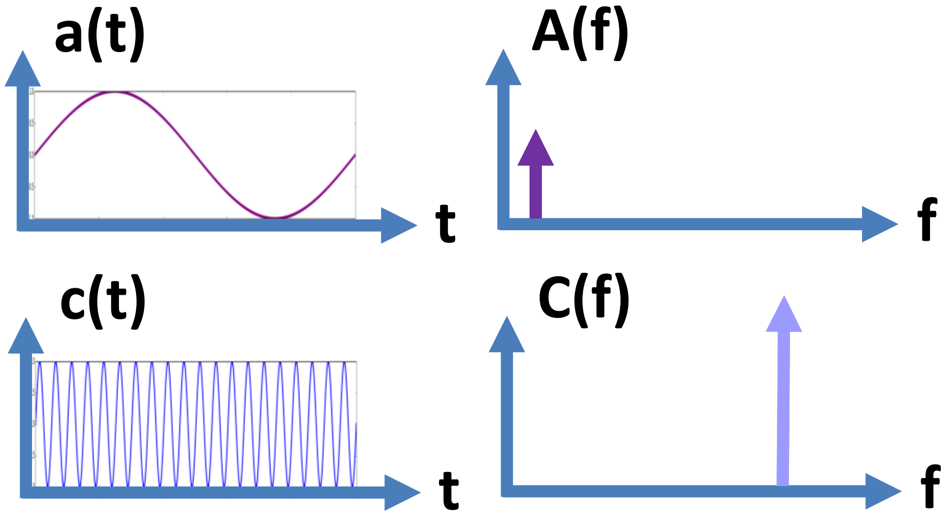
Up-conversion

Issues

Reminder

Time vs. Frequency

Up-conversion



INSTITUT CARNOT Télécom & Société numérique

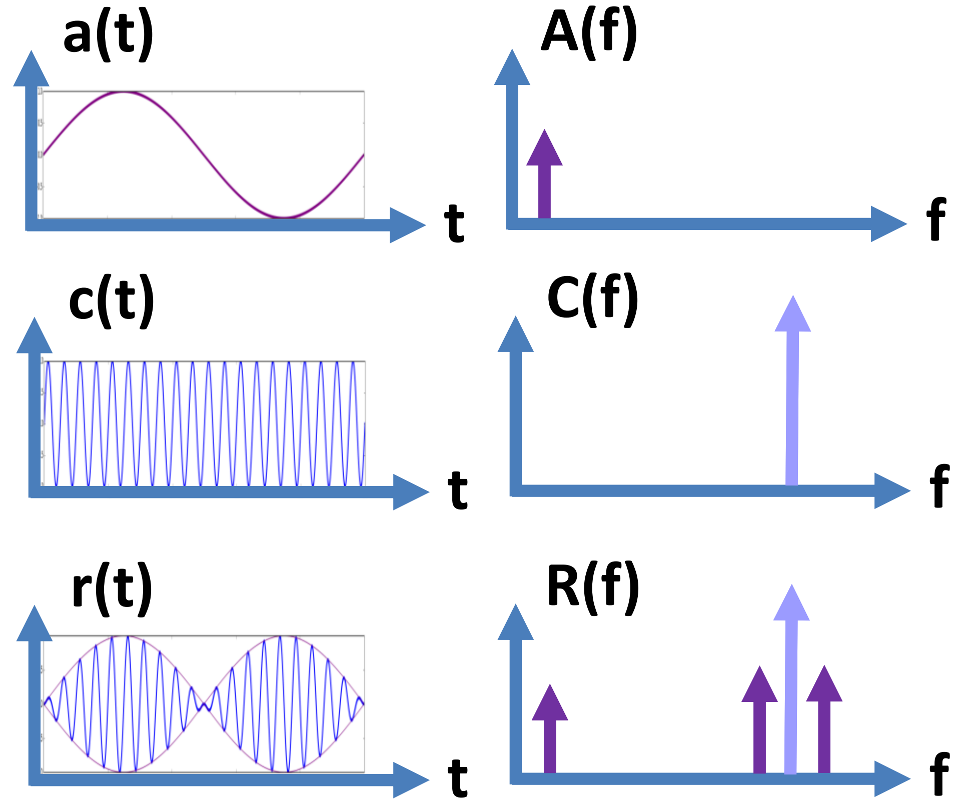
EUREKOM Sophia Antipolis

Issues

Reminder

Time vs. Frequency

Up-conversion



INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

Issues

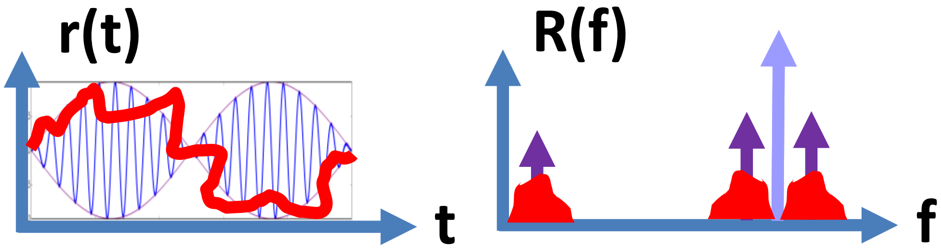
Institut Carnot Télécom & Société numérique

EURECOM Sophia Antipolis

Issues

Analog/RF

Noise Sensitive



Issues

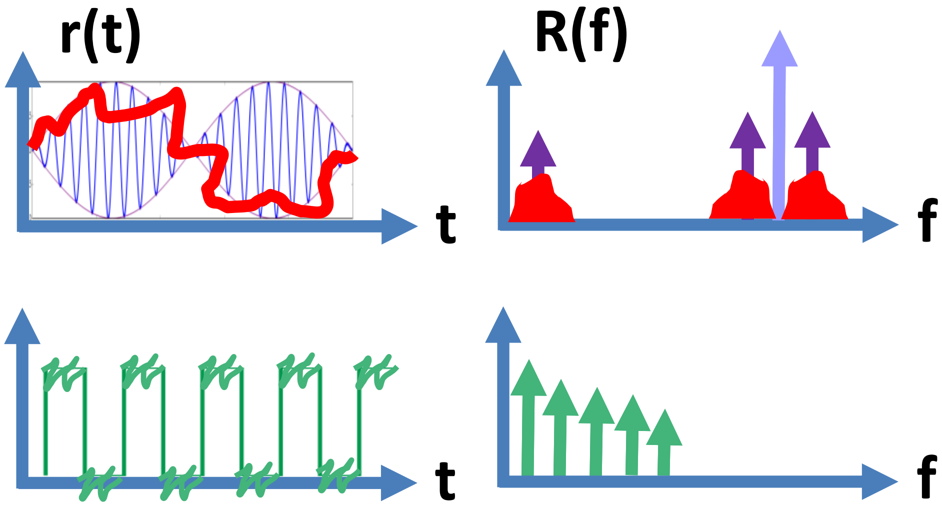
Analog/RF

Noise Sensitive

Digital

Noise resilient

Noise Source

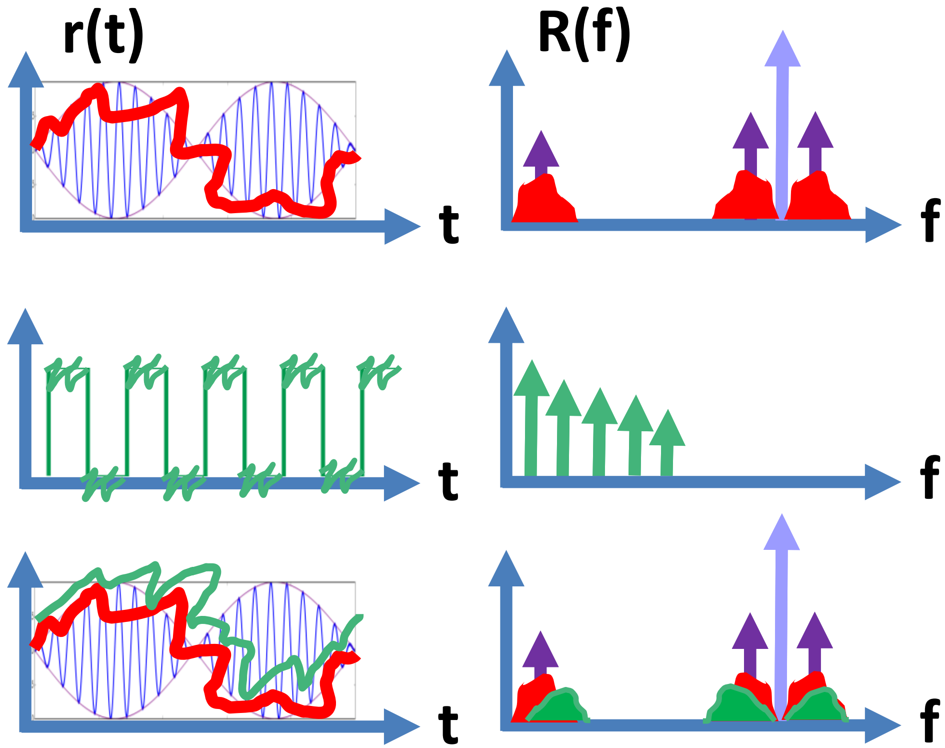


Issues

Analog/RF
Noise Sensitive

Digital
Noise resilient
Noise Source

Same Chip
Noise Coupling



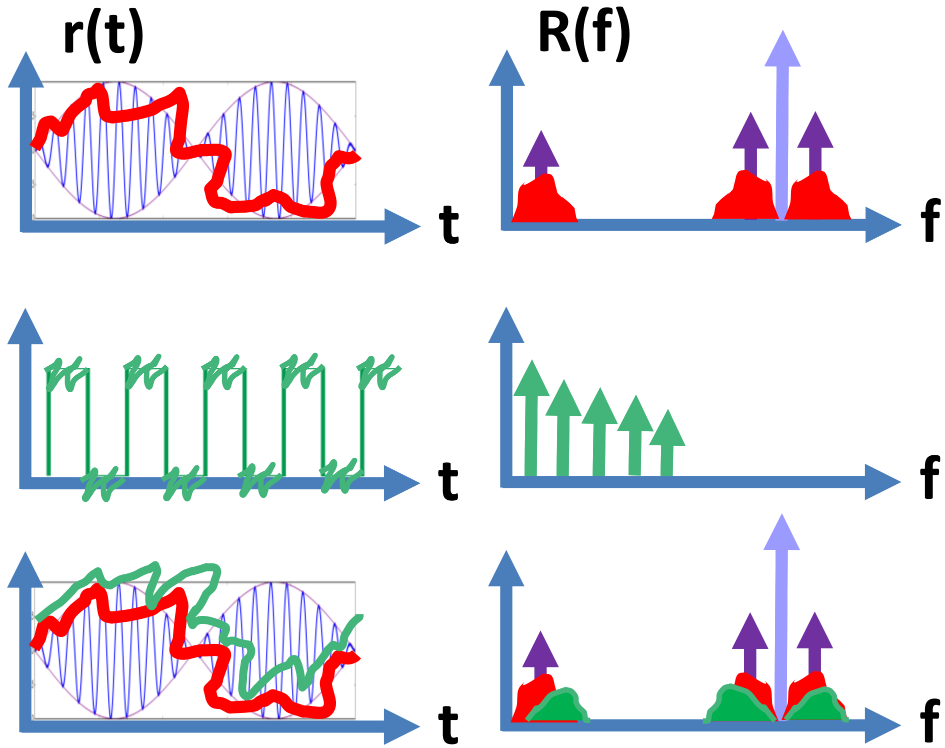
Issues

Analog/RF
Noise Sensitive

Digital
Noise resilient
Noise Source

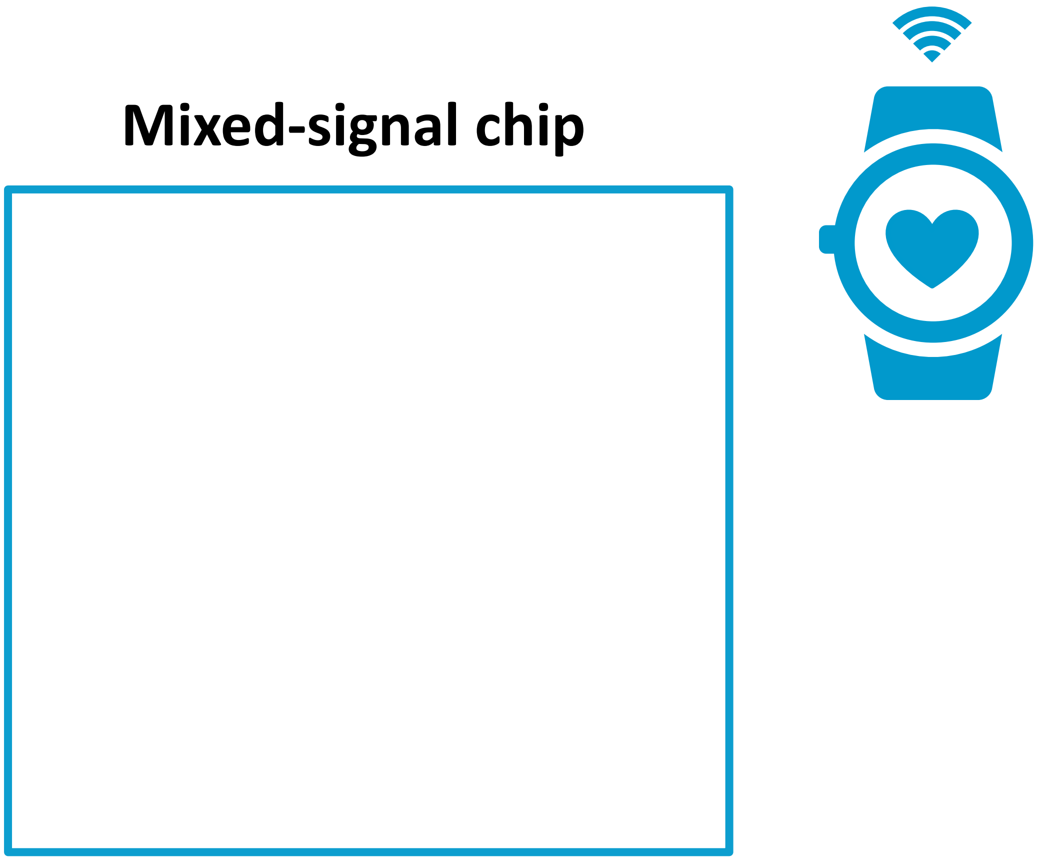
Same Chip
Noise Coupling

Careful Design
Radio Still Works



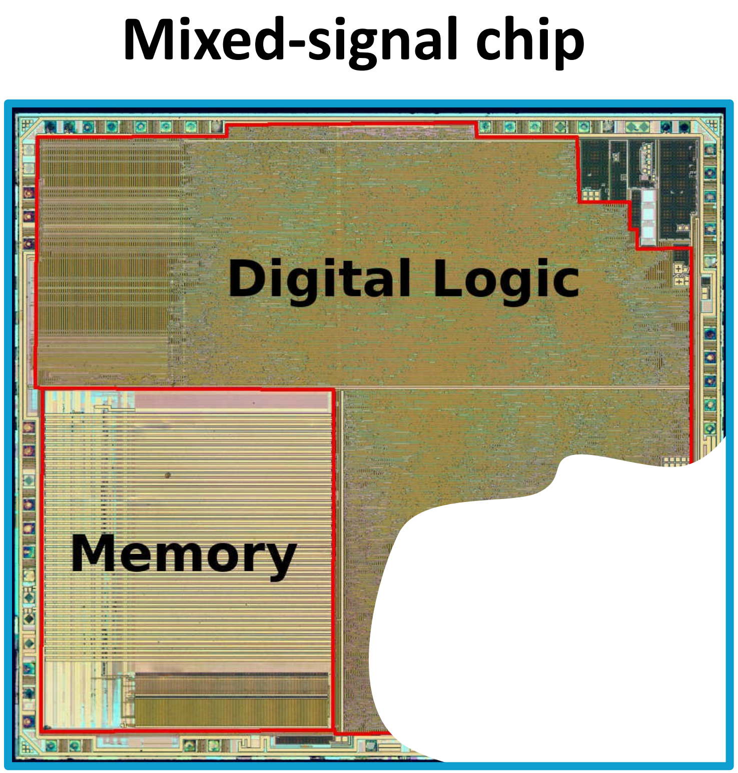
Problems, the global view

Mixed-signal chip



Problems, the global view

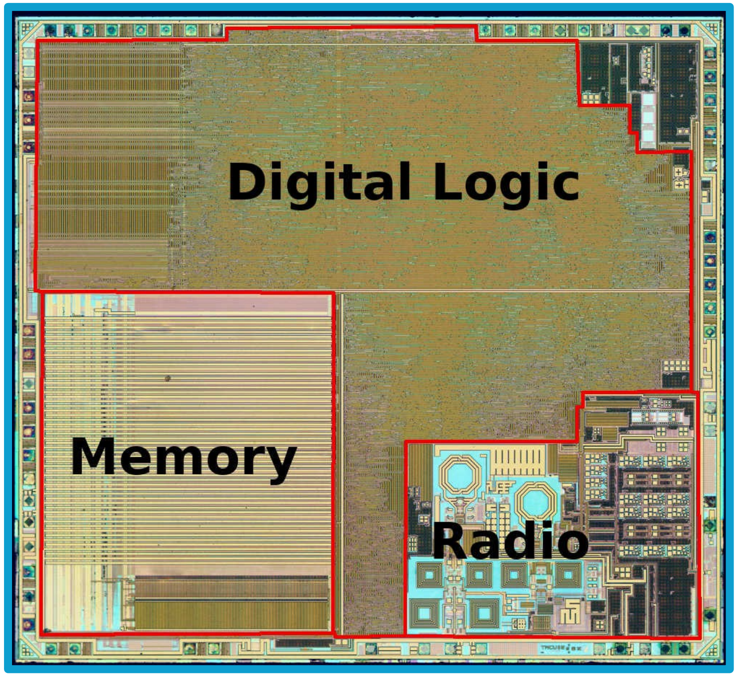
Strong noise source



Problems, the global view

Strong noise source

Mixed-signal chip

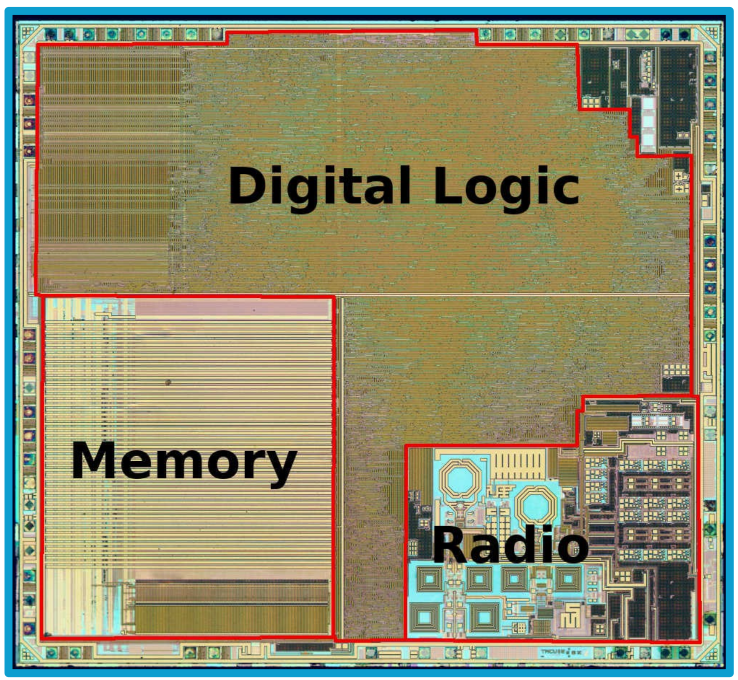


Noise sensitive transmitter

Problems, the global view

Mixed-signal chip

Strong noise source



Easy propagation

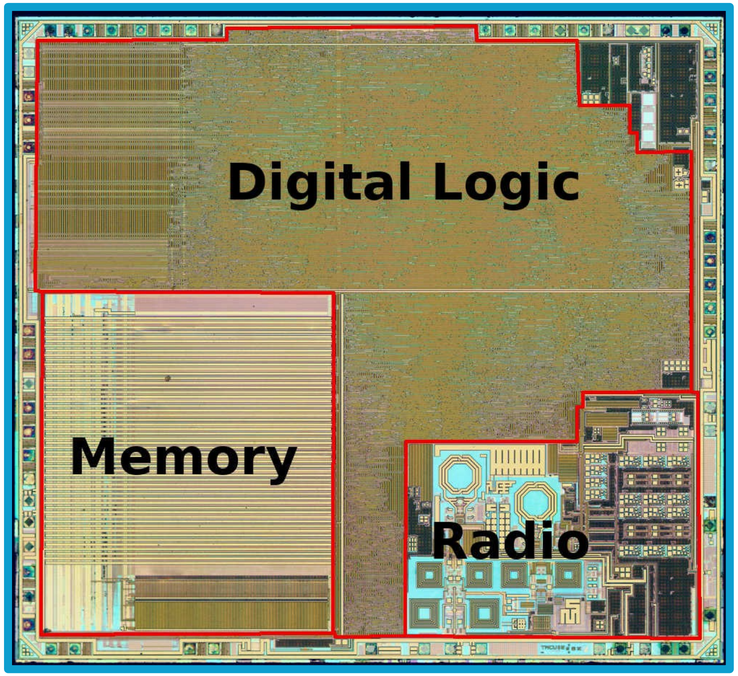
Noise sensitive transmitter

Screaming Channels
The Idea

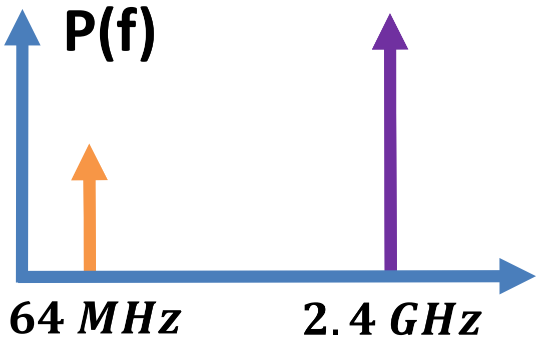
Screaming Channels Idea

Mixed-signal chip

Strong noise source



Easy propagation



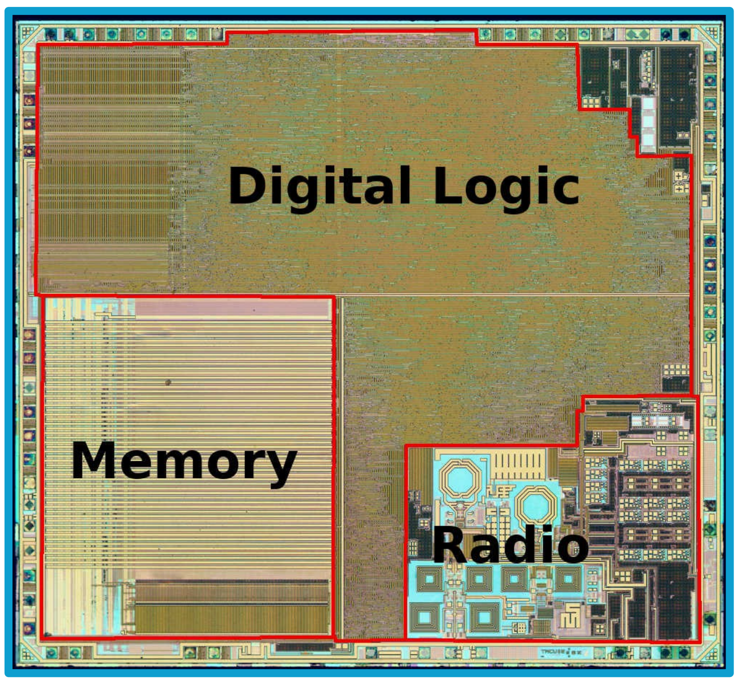
Noise sensitive transmitter

Screaming Channels Idea

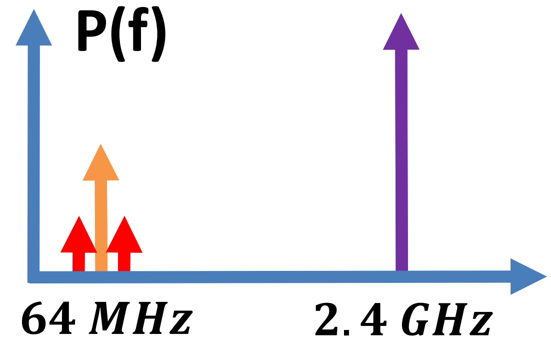
Conventional Side Channel Leak

Mixed-signal chip

Strong noise source



Easy propagation



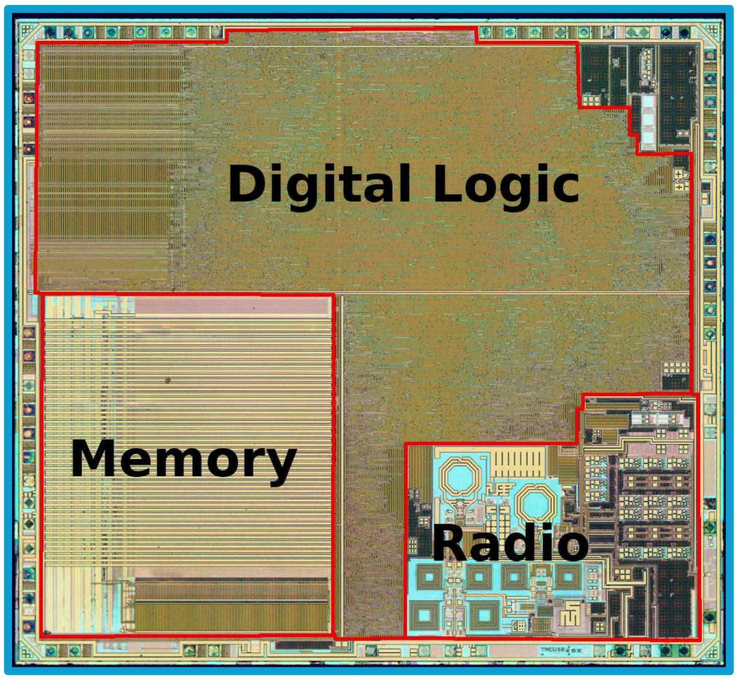
Noise sensitive transmitter

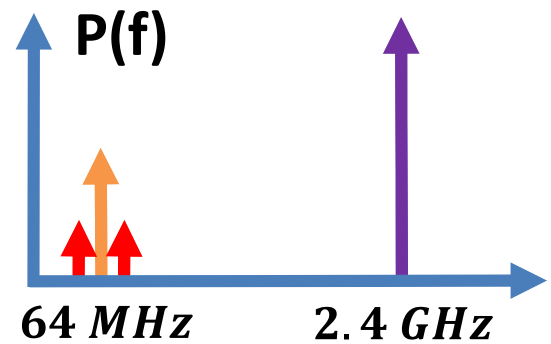
Screaming Channels Idea

Conventional Side Channel Leak

Mixed-signal chip

Strong noise source



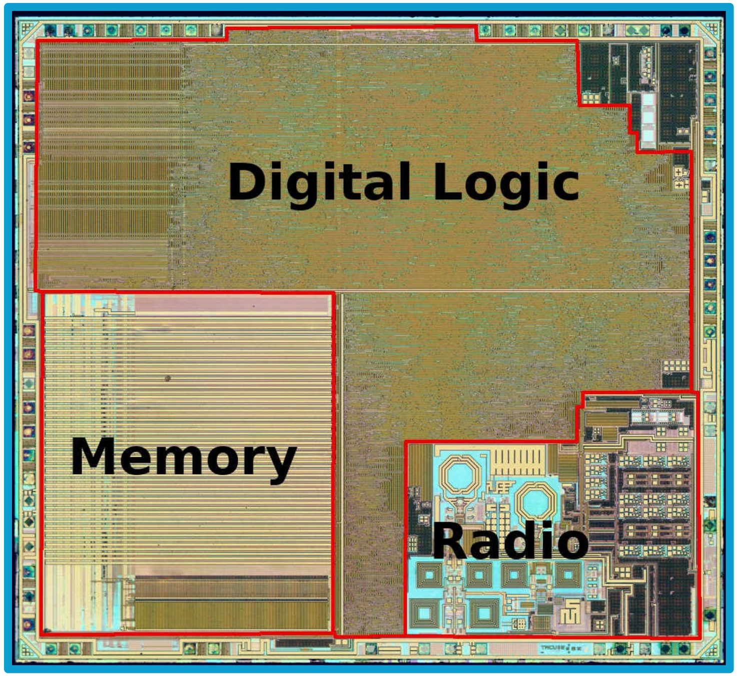


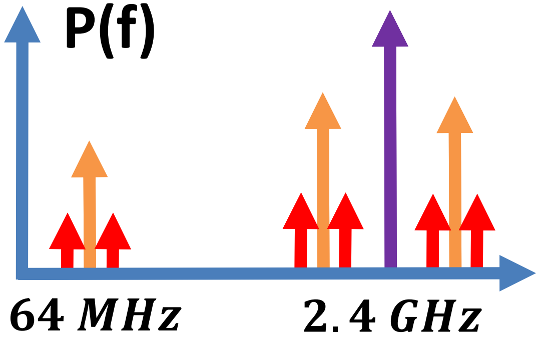
Noise sensitive transmitter

Easy propagation

Leak Propagation

Screaming Channels Idea





Noise sensitive transmitter

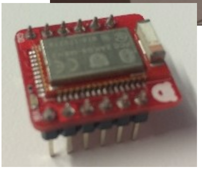
Leak Is Broadcast

Easy propagation

Leak Propagation

Screaming Channels in Action

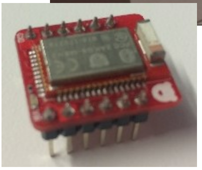
Antenna + SDR RX



Cortex-M4
+ BT TX

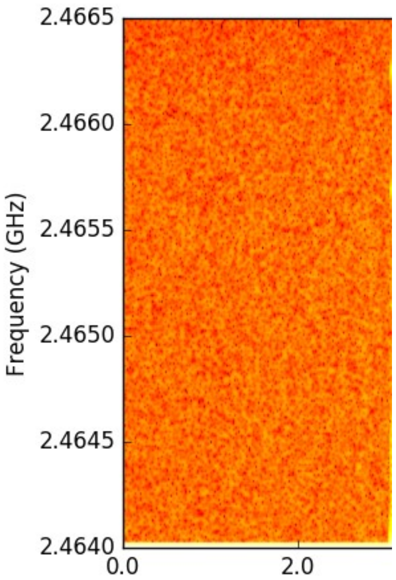
Screaming Channels in Action

Antenna + SDR RX



Cortex-M4 + BT TX

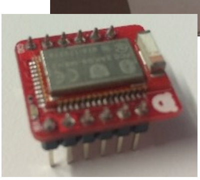
Radio Off



Noise

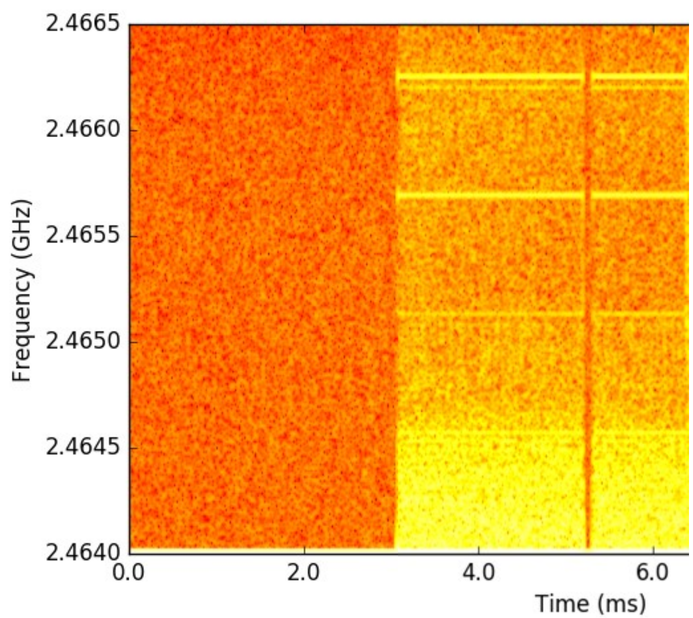
Screaming Channels in Action

Antenna + SDR RX



Cortex-M4 + BT TX

Radio Off **Radio TX**



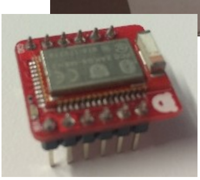
Noise **Packet**

INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

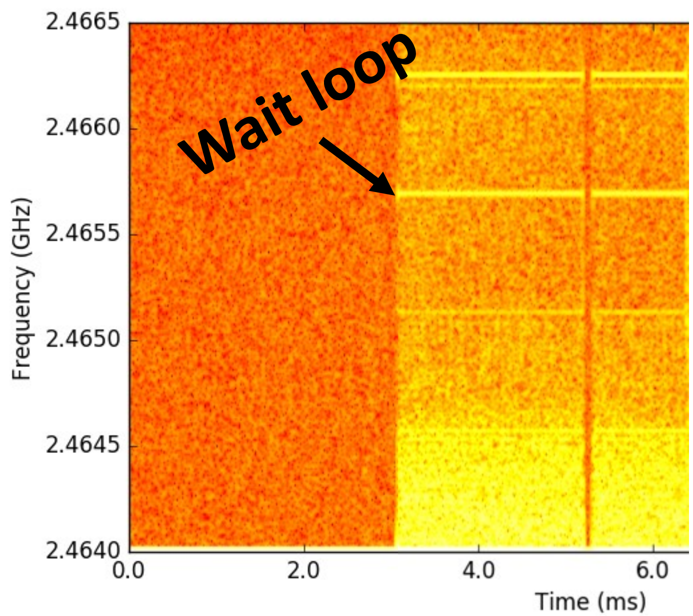
Screaming Channels in Action

Antenna + SDR RX



Cortex-M4
+ BT TX

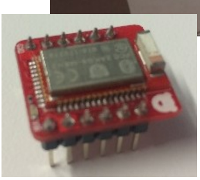
Radio Off **Radio TX**



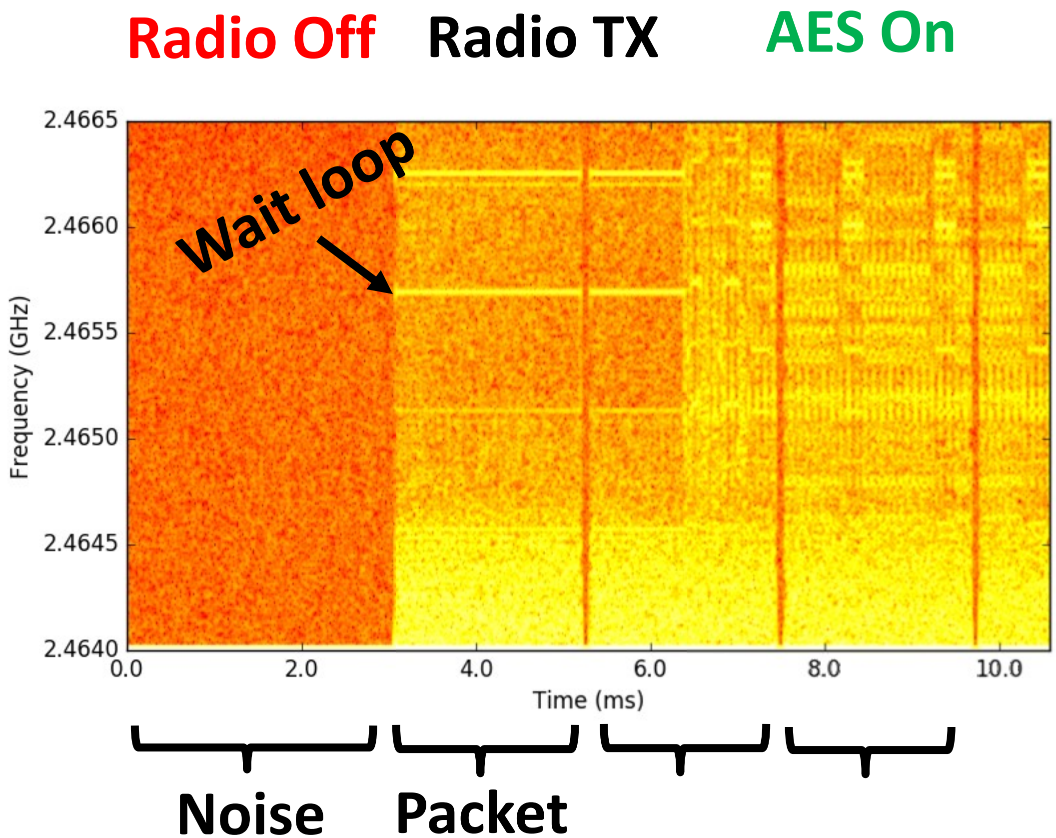
Noise **Packet**

Screaming Channels in Action

Antenna + SDR RX

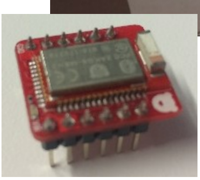


Cortex-M4 + BT TX



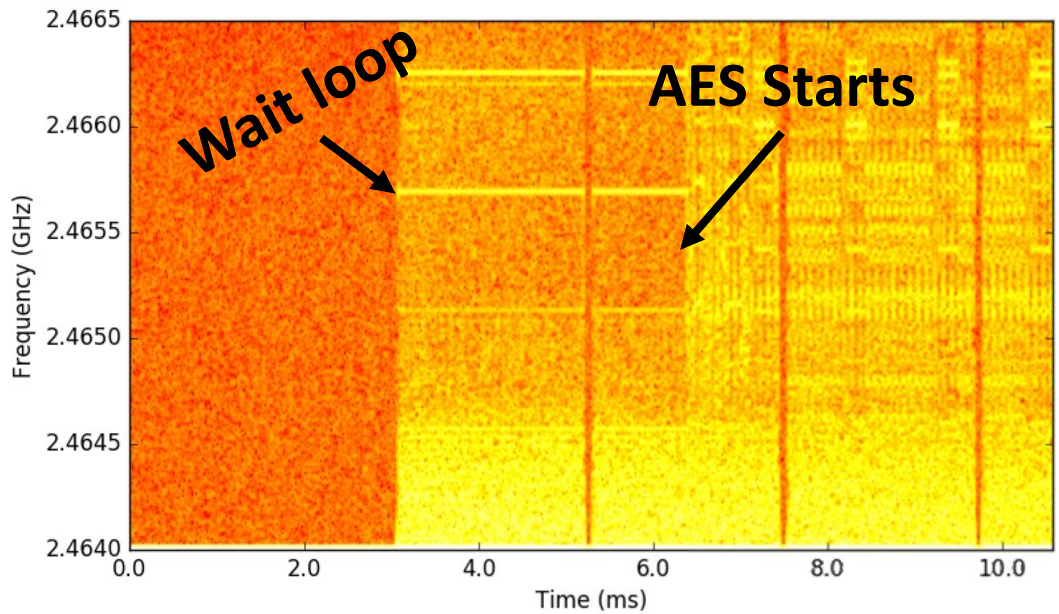
Screaming Channels in Action

Antenna + SDR RX



Cortex-M4 + BT TX

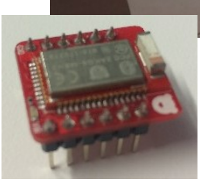
Radio Off **Radio TX** **AES On**



Noise **Packet**

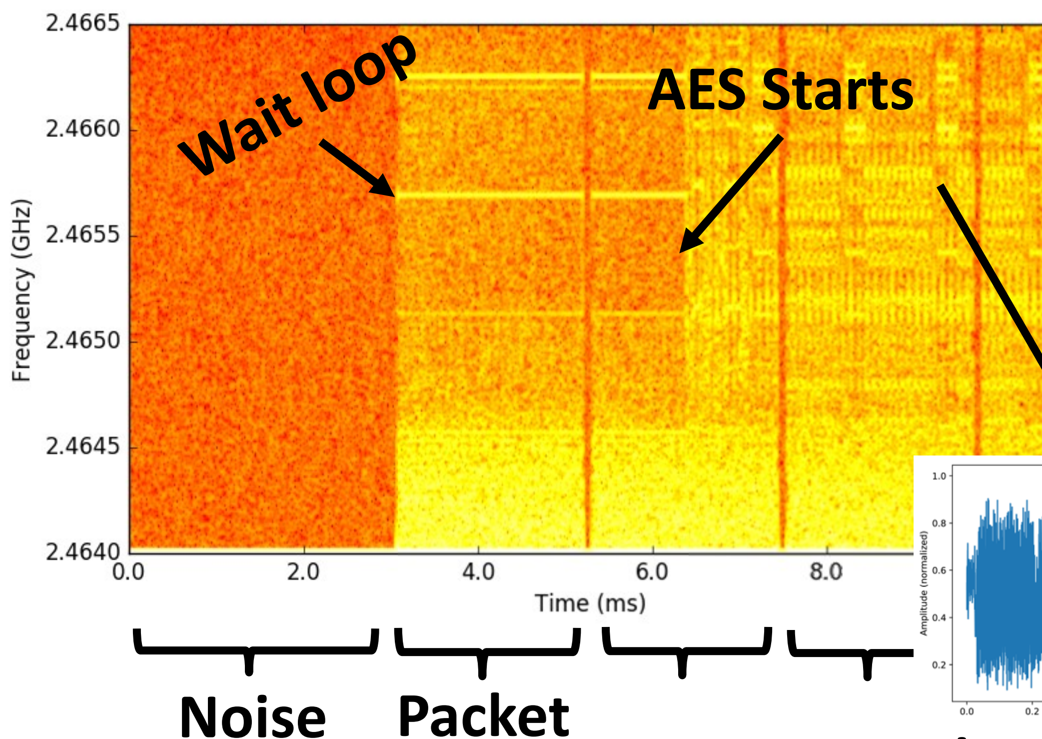
Screaming Channels in Action

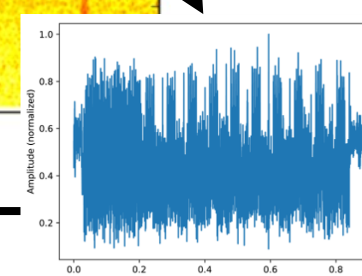
Antenna + SDR RX



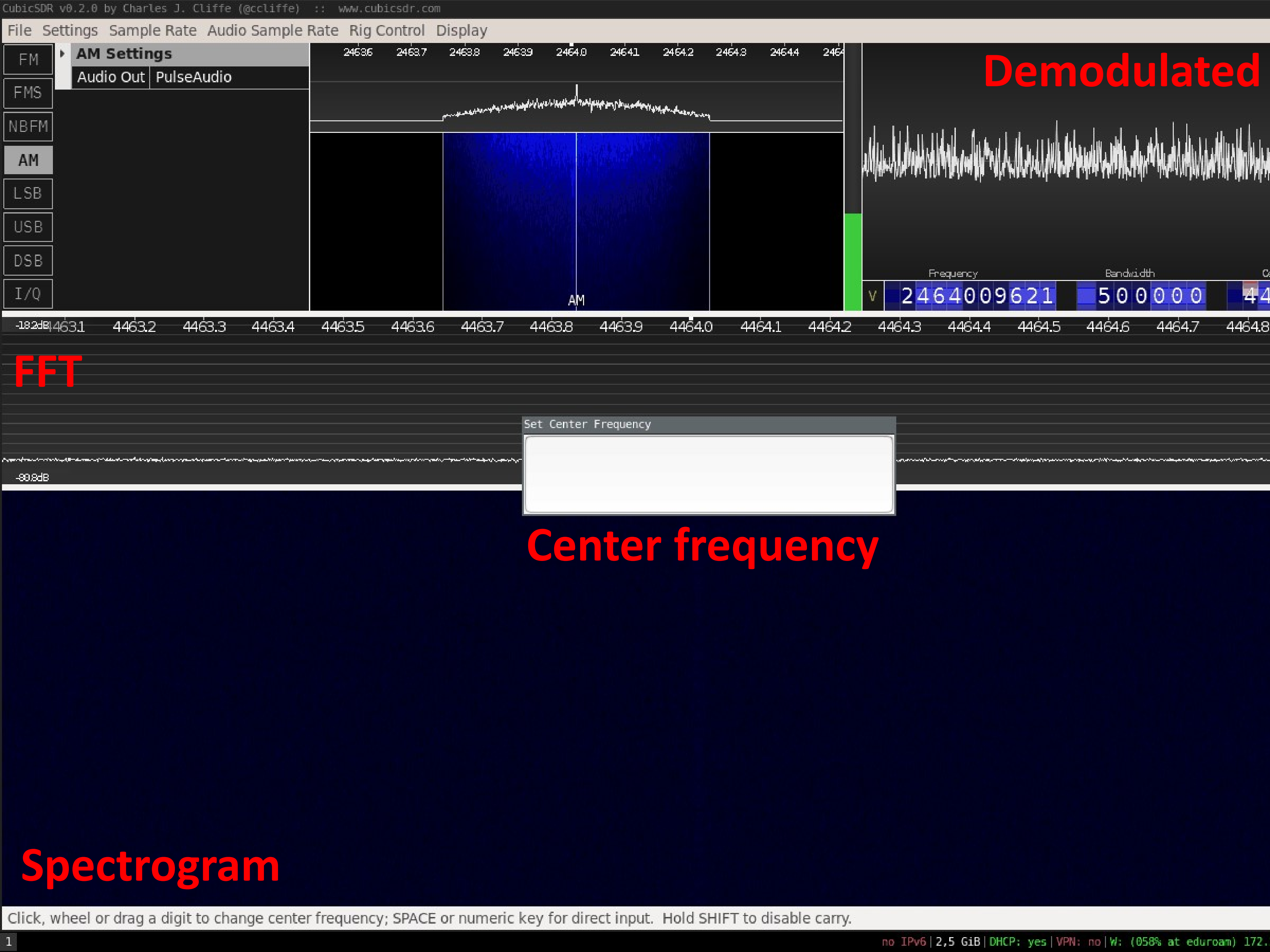
Cortex-M4
+ BT TX

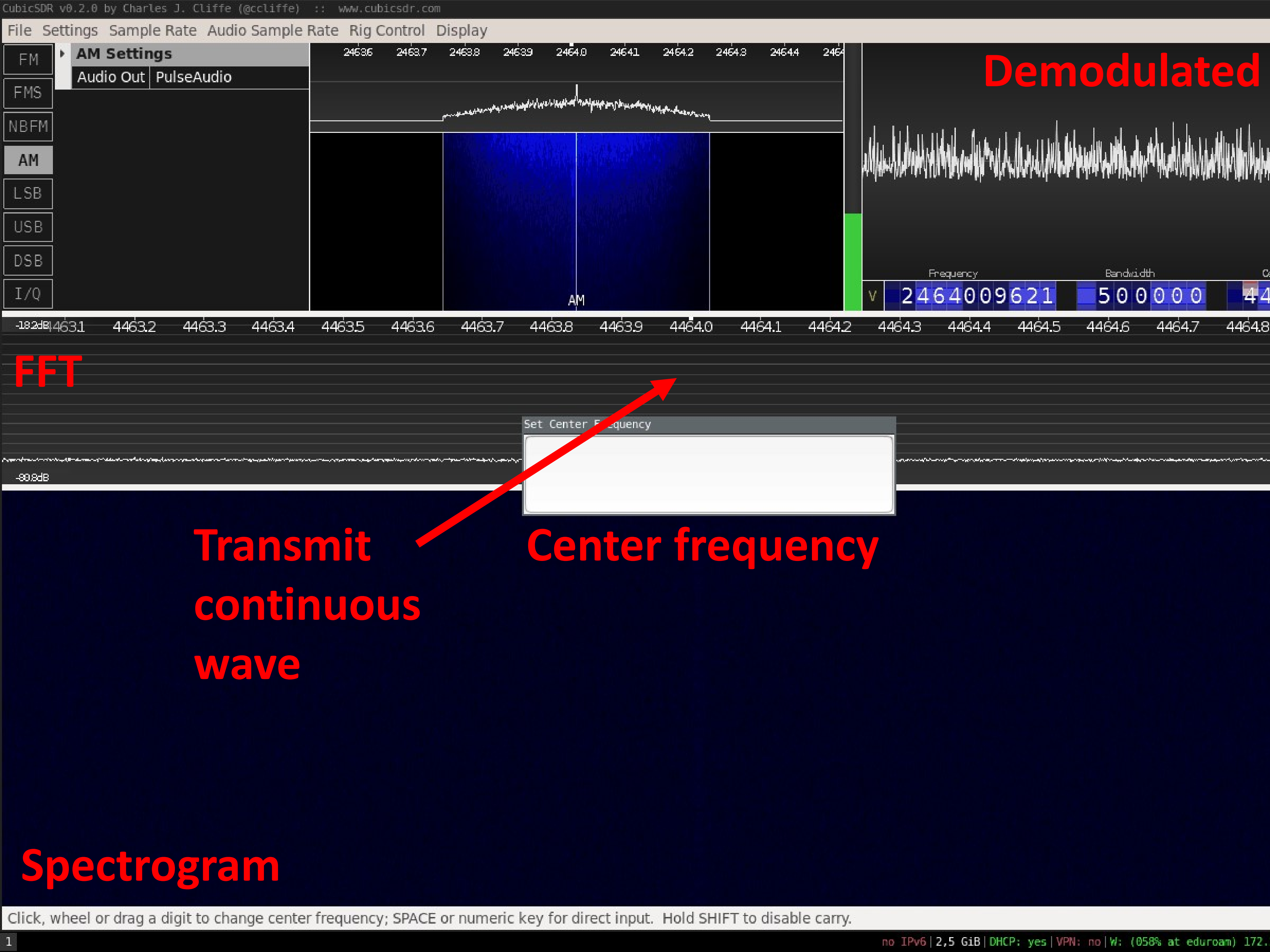
Radio Off **Radio TX** **AES On**

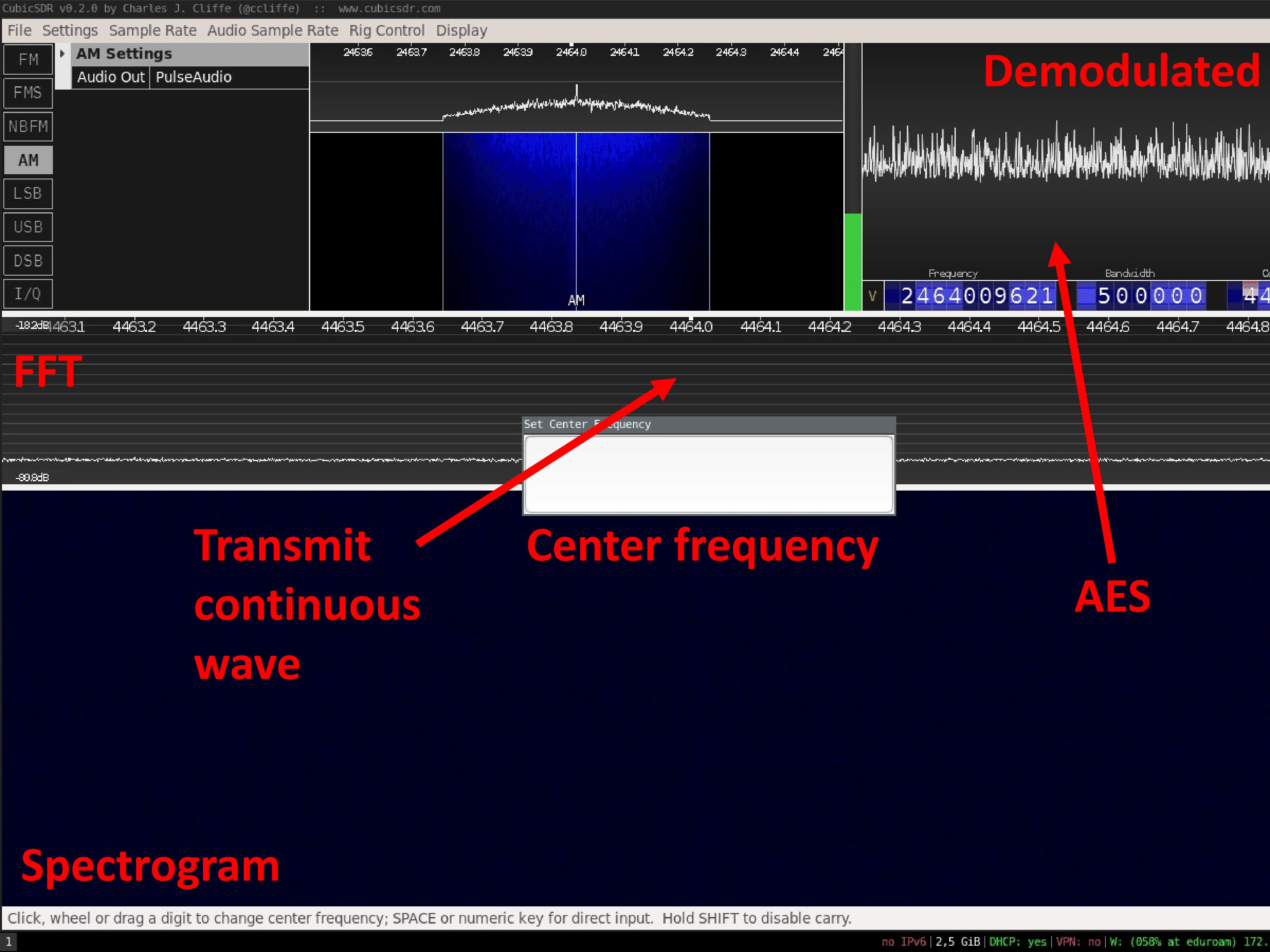




Time domain

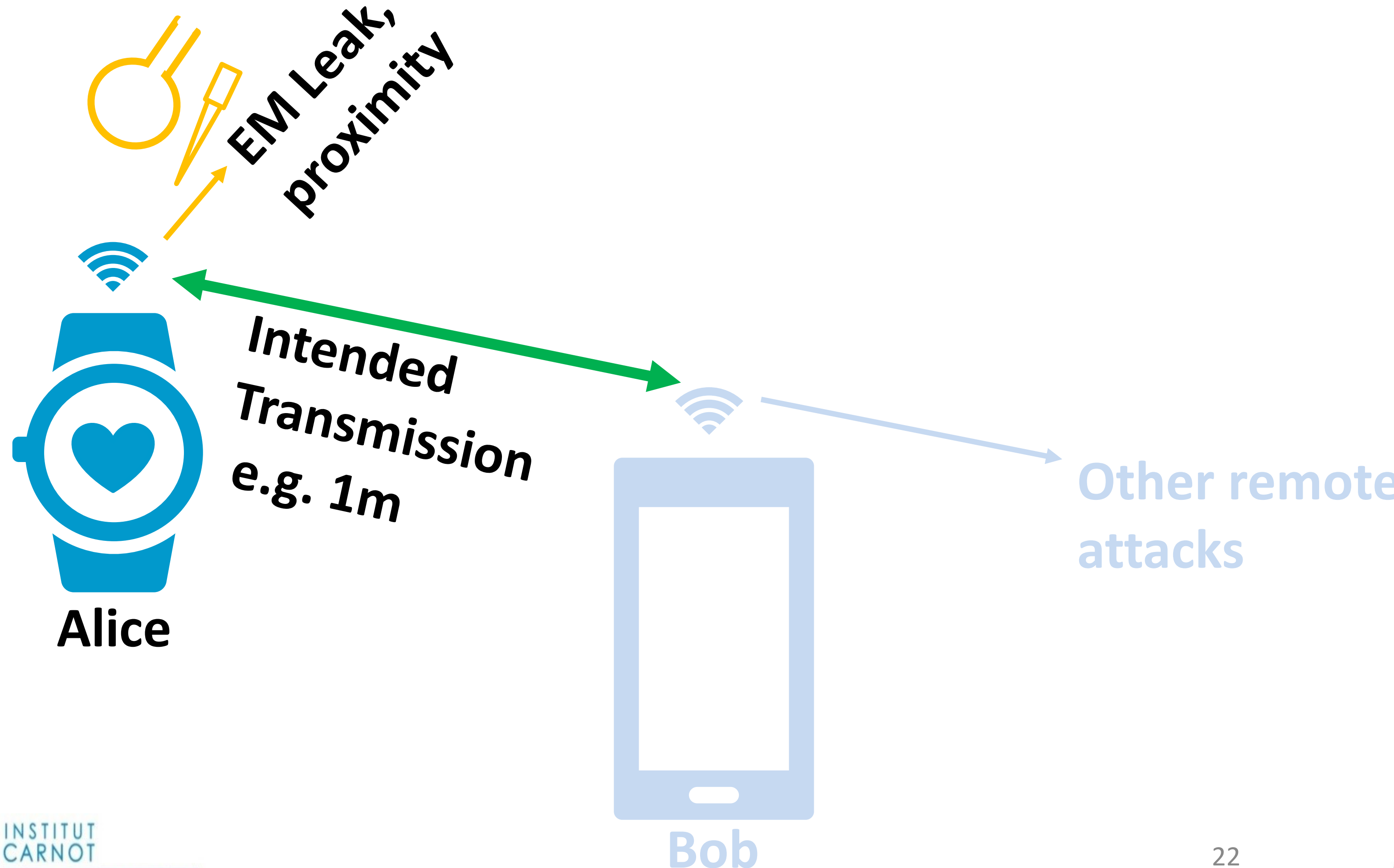

CubicSDR v0.2.0 by Charles J. Cliffe (@ccliffe) :: www.cubicsdr.com
File Settings Sample Rate Audio Sample Rate Rig Control Display
FM
FMS
NBFM
AM
LSB
USB
DSB
I/Q
AM Settings
Audio Out PulseAudio
AM
Demodulated
Frequency
Bandwidth
2464009621
500000
FFT
Set Center Frequency
Center frequency
Spectrogram
Click, wheel or drag a digit to change center frequency; SPACE or numeric key for direct input. Hold SHIFT to disable carry.


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
Demodulated
Frequency
Bandwidth
2464009621
500000
FFT
Set Center Frequency
Transmit continuous wave
Center frequency
Spectrogram
Click, wheel or drag a digit to change center frequency; SPACE or numeric key for direct input. Hold SHIFT to disable carry.

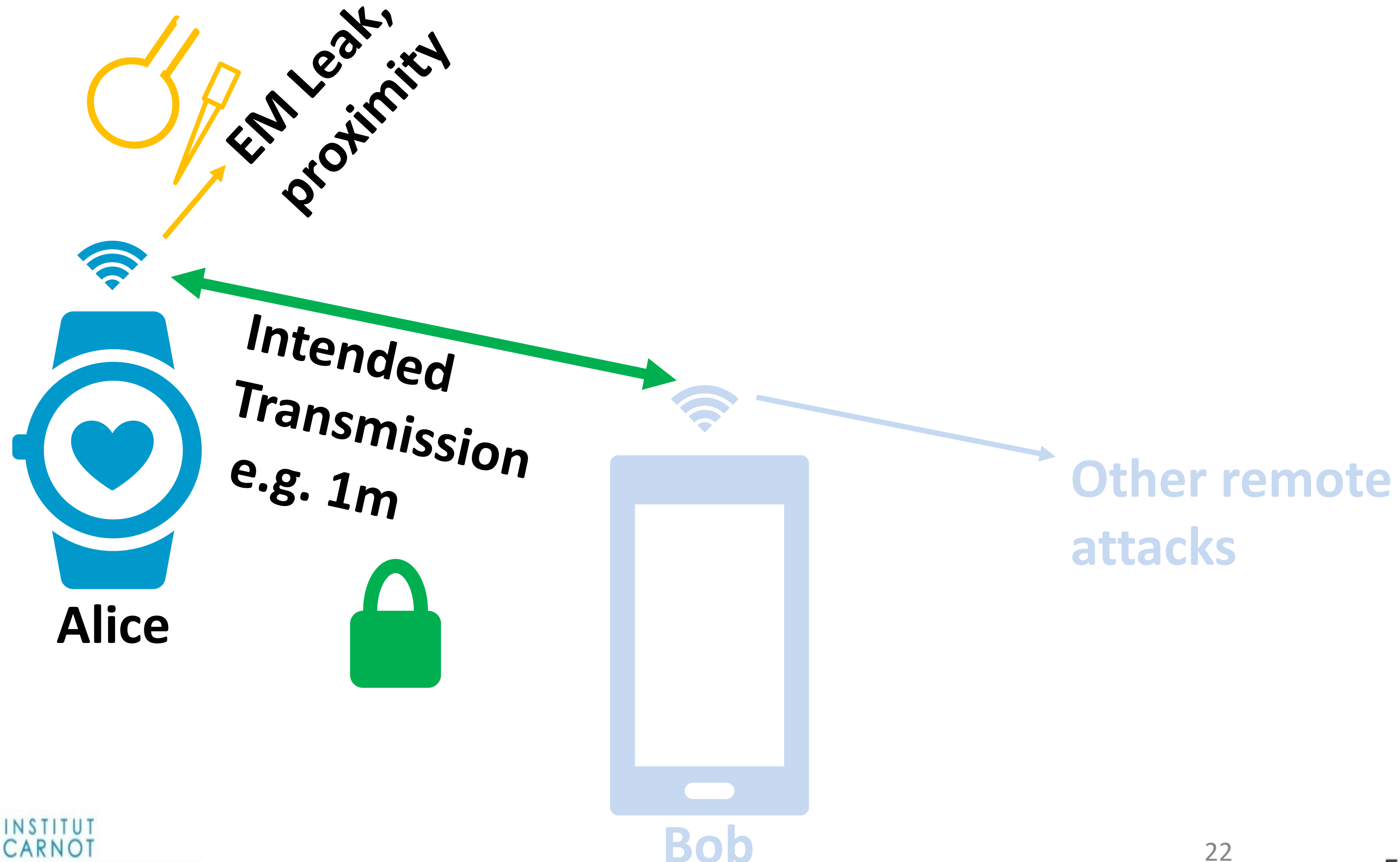


CubicSDR v0.2.0 by Charles J. Cliffe (@ccliffe) :: www.cubicsdr.com
File Settings Sample Rate Audio Sample Rate Rig Control Display
FM
FMS
NBFM
AM
LSB
USB
DSB
I/Q
AM Settings
Audio Out PulseAudio
Demodulated
Frequency
Bandwidth
2464009621
500000
AM
FFT
Set Center Frequency
Transmit continuous wave
Center frequency
AES
Spectrogram
Click, wheel or drag a digit to change center frequency; SPACE or numeric key for direct input. Hold SHIFT to disable carry.

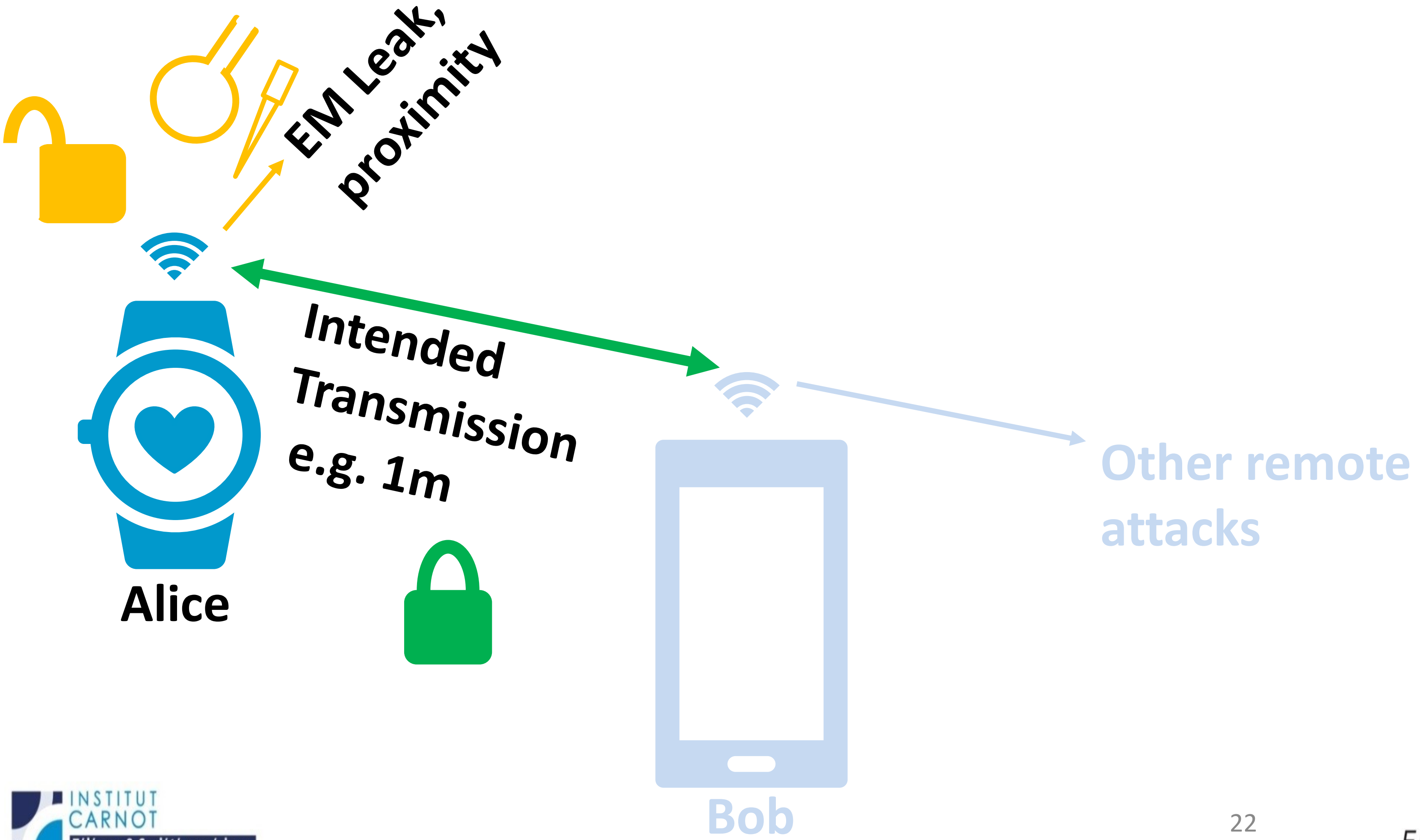
Screaming Channels: Leak Broadcast



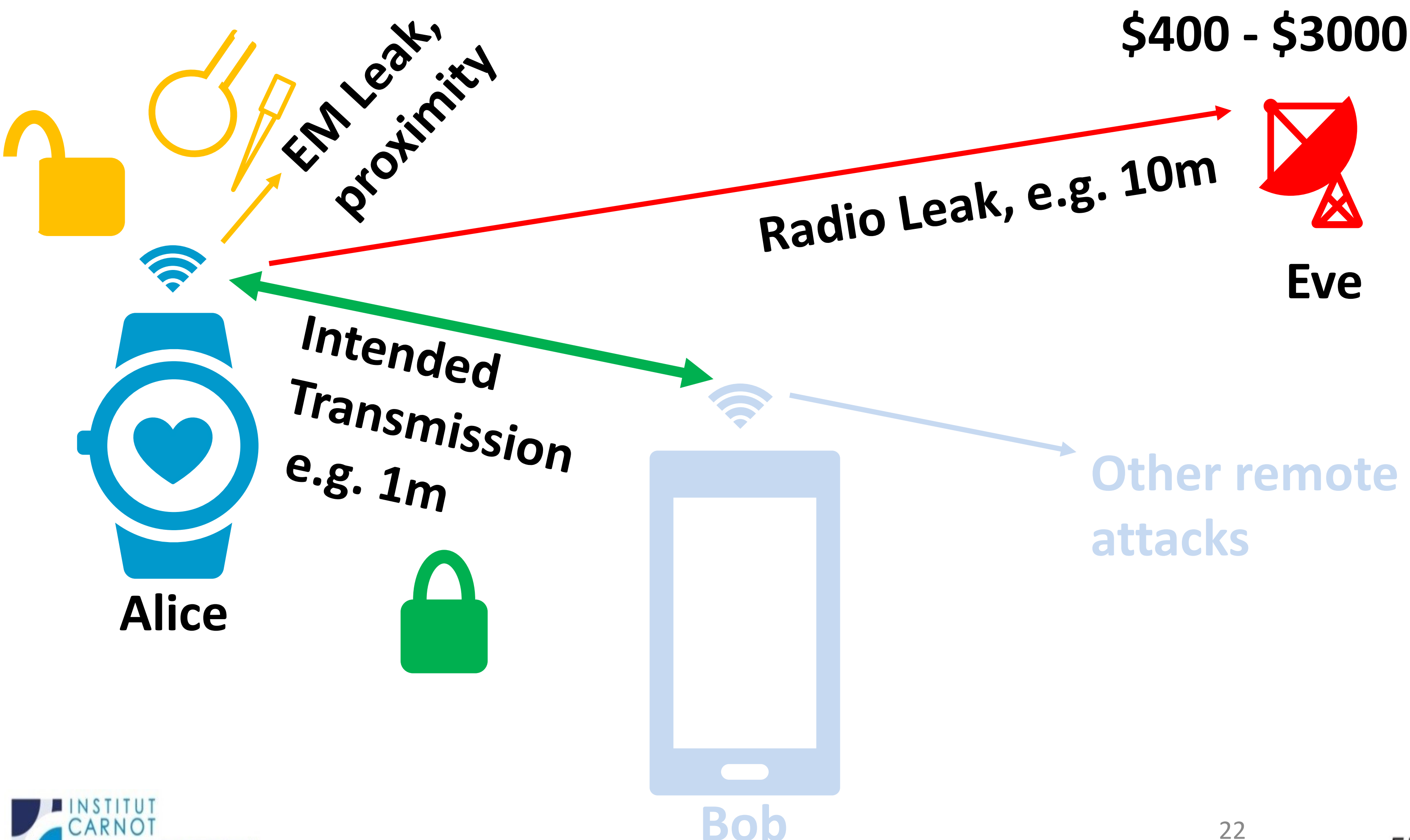
Screaming Channels: Leak Broadcast



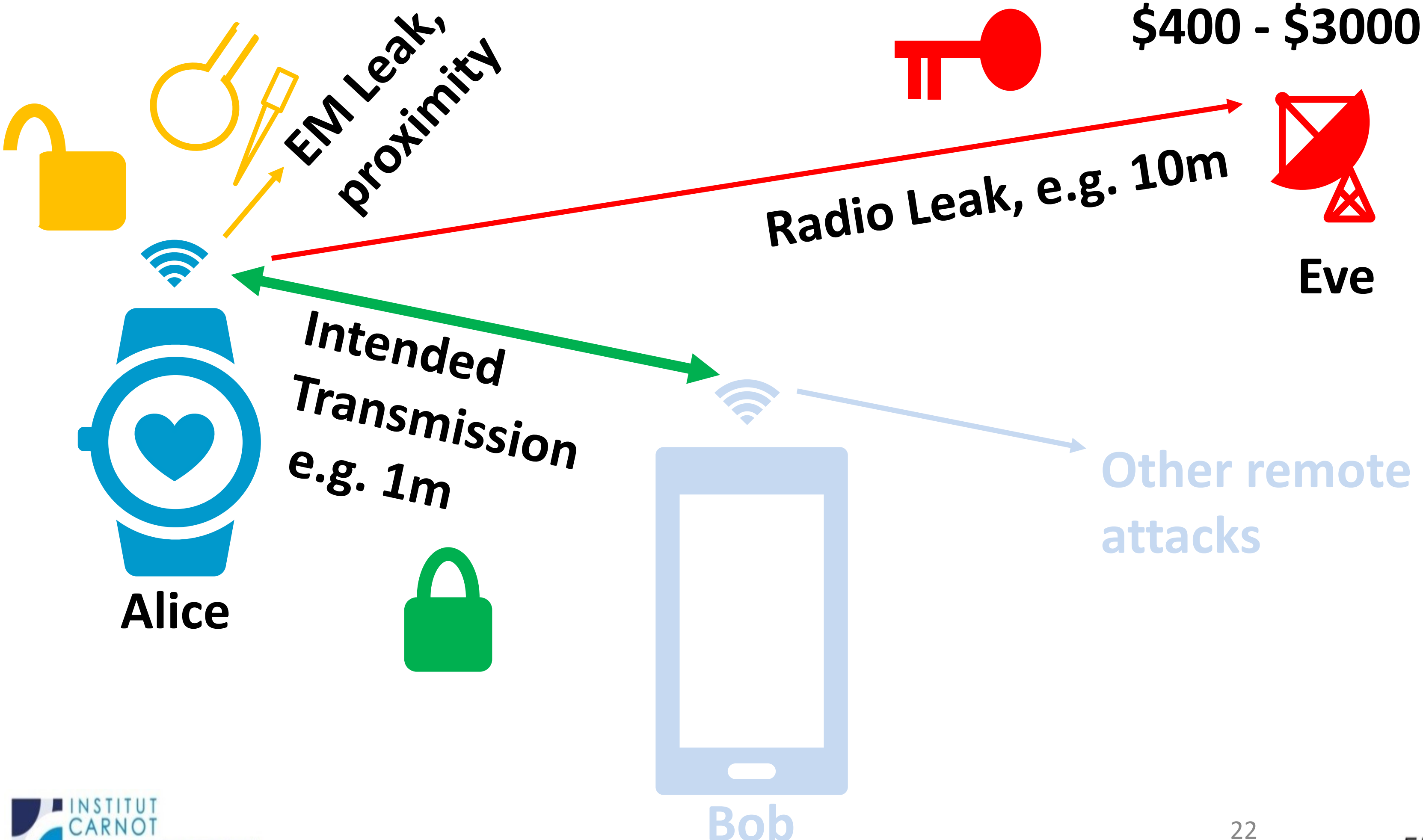
Screaming Channels: Leak Broadcast



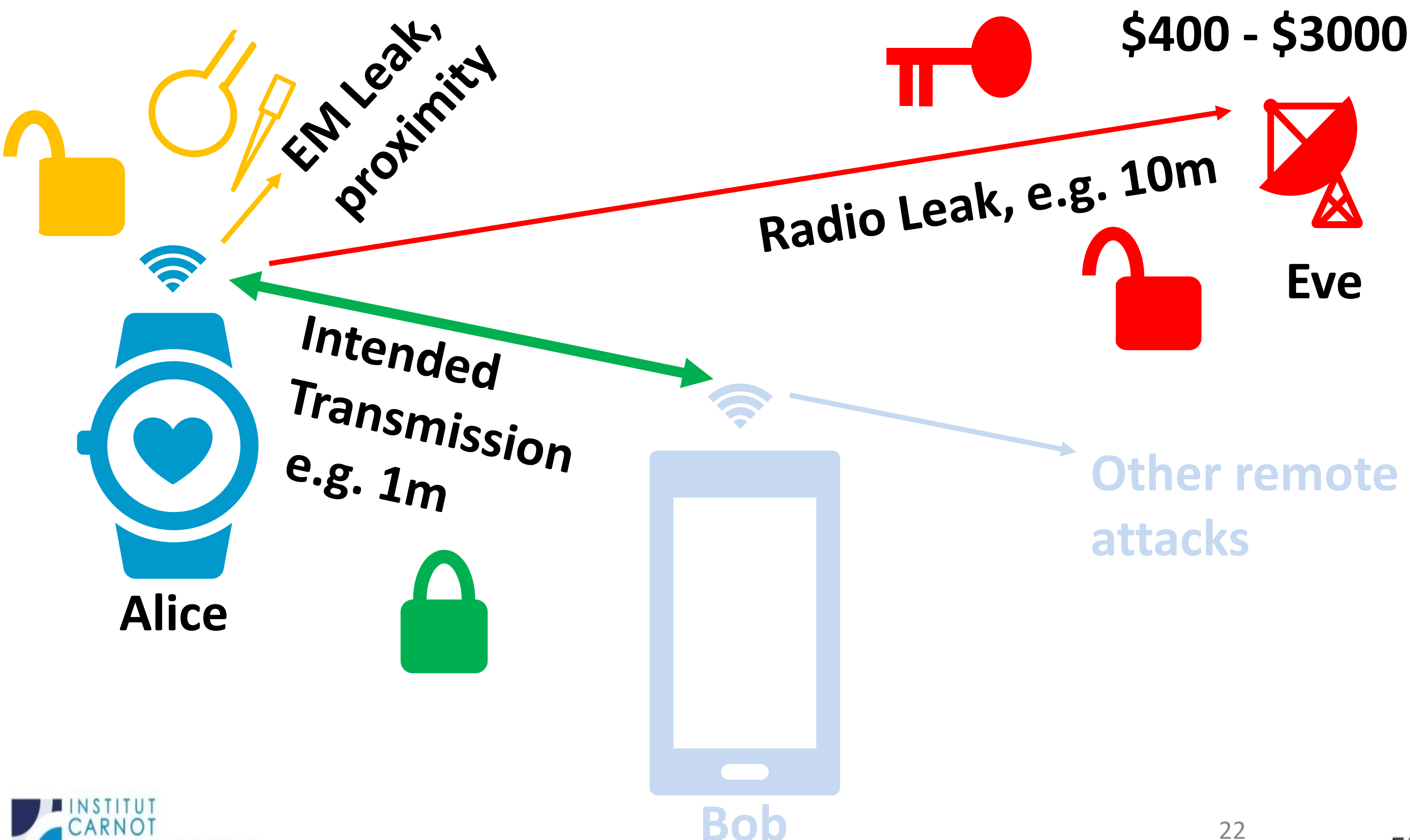
Screaming Channels: Leak Broadcast



Screaming Channels: Leak Broadcast

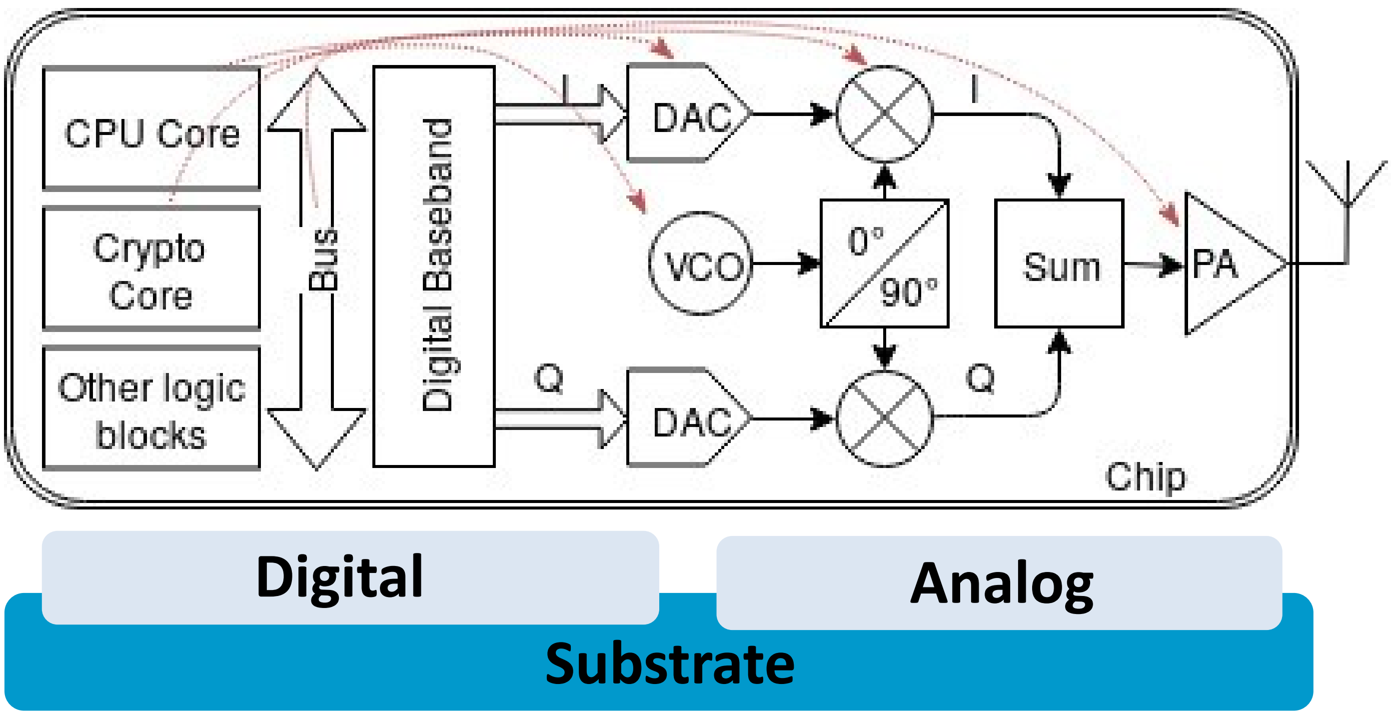


Screaming Channels: Leak Broadcast



From Digital Noise
To Noise On The Radio Signal

Possible Impact on Radio Transmission

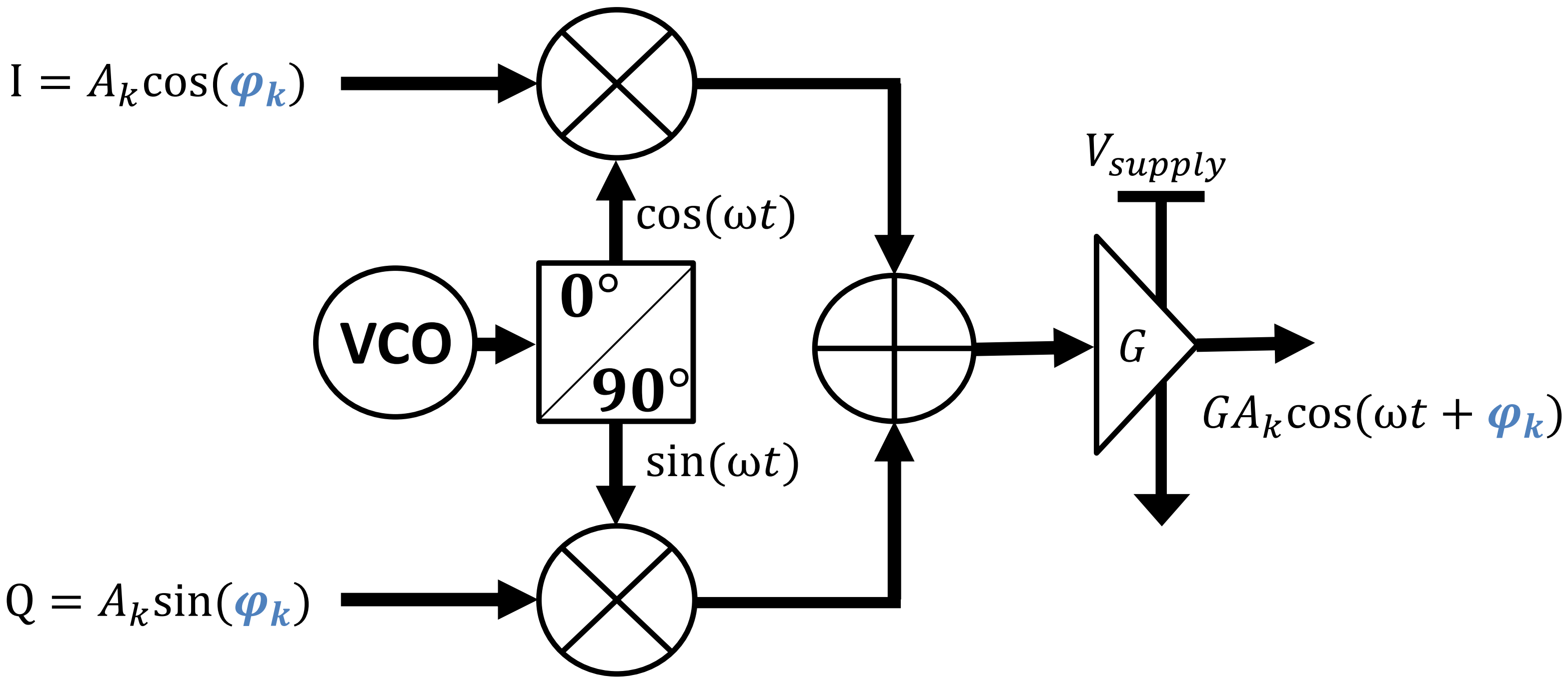


Digital: Inherently noisy

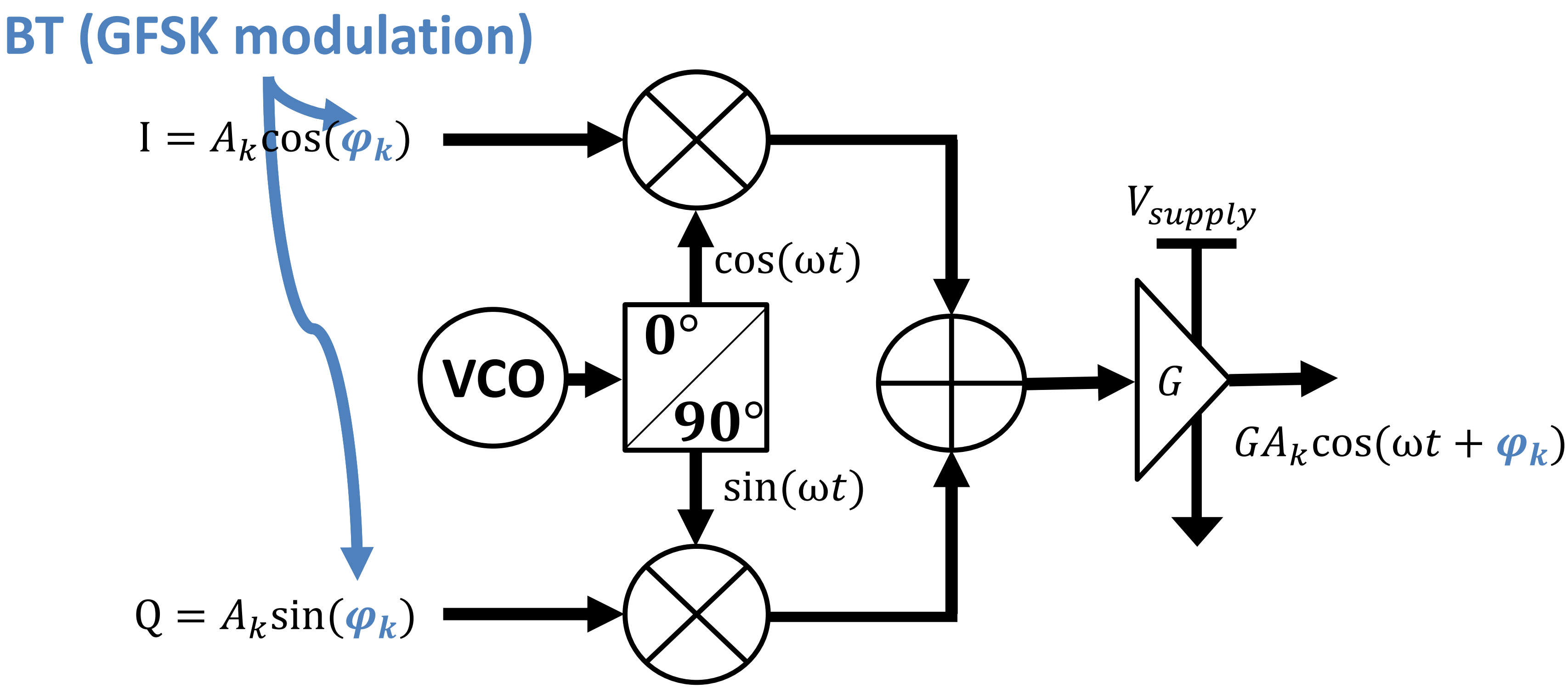
Propagation: Substrate coupling, Power supply/Gnd

Analog: Noise sensitive

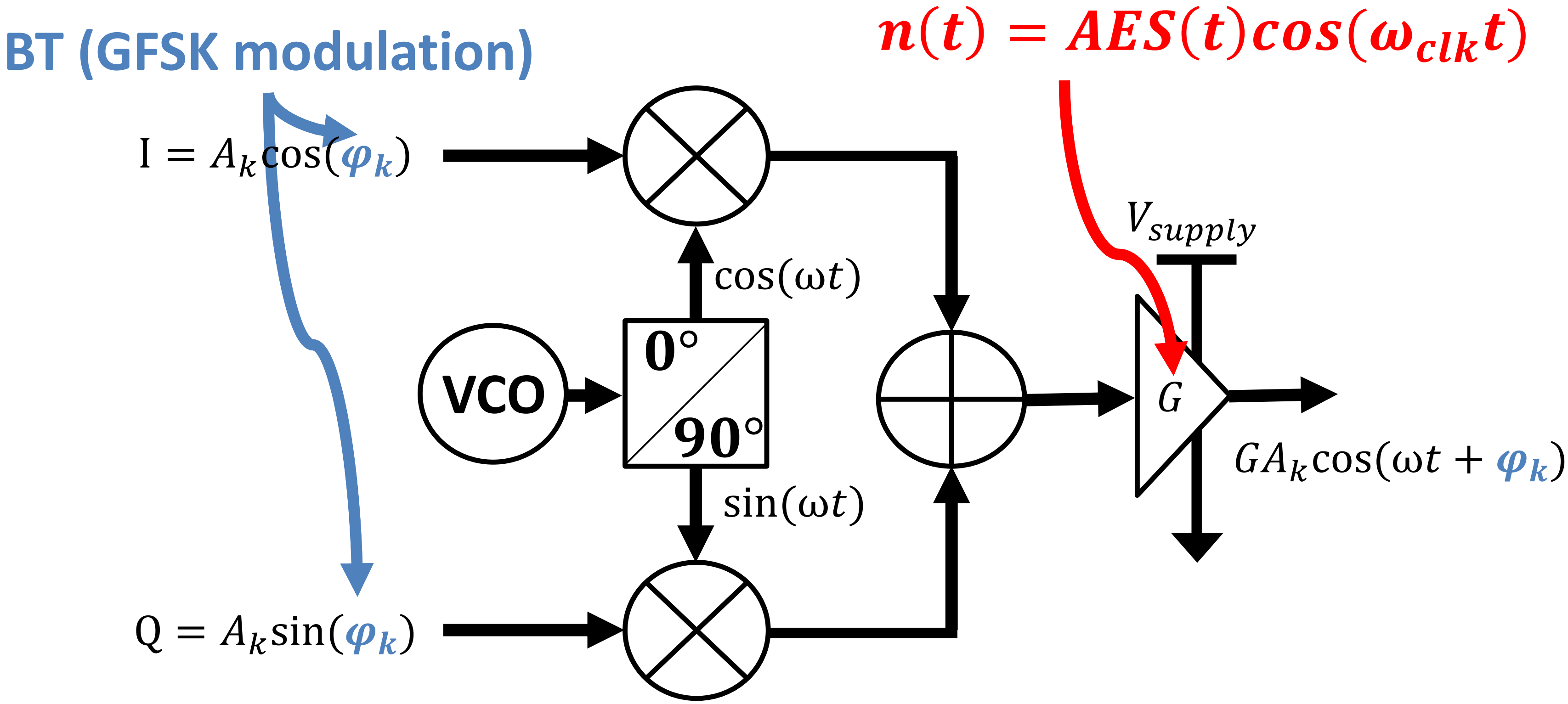
Practical Case We Observed



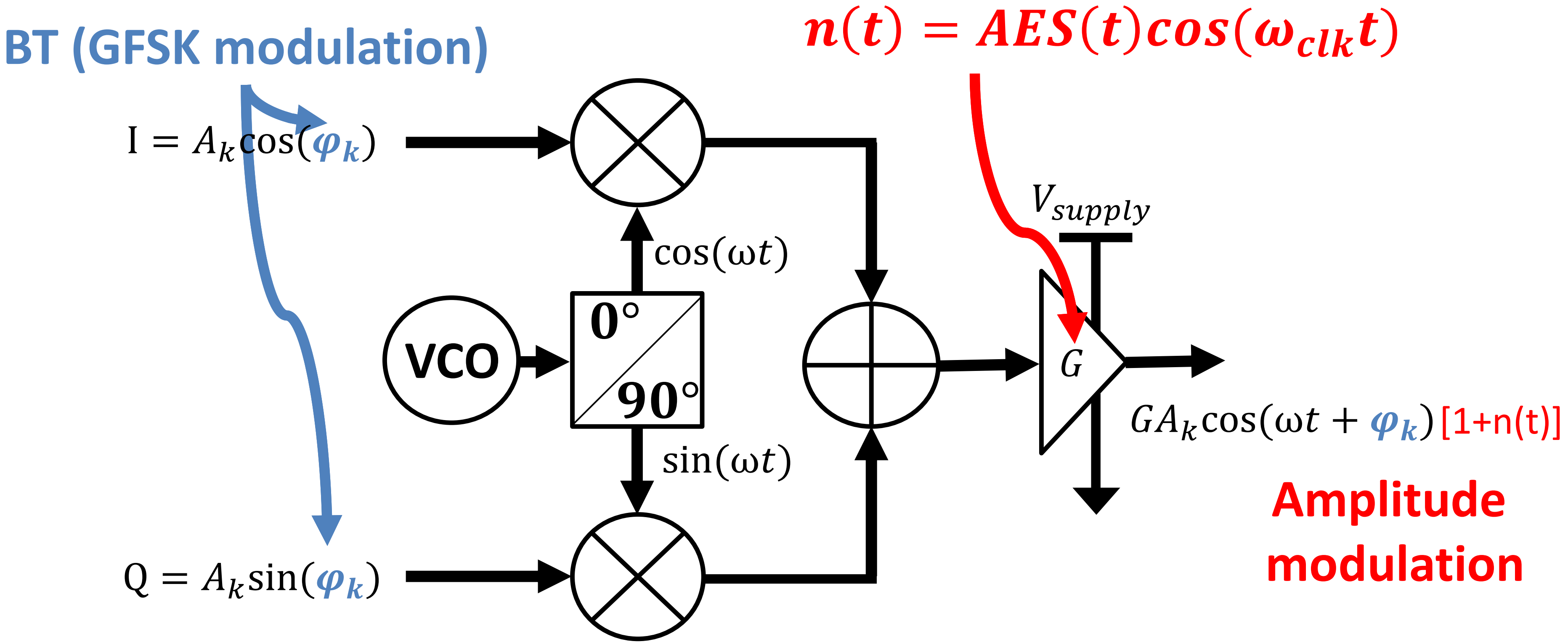
Practical Case We Observed



Practical Case We Observed



Practical Case We Observed



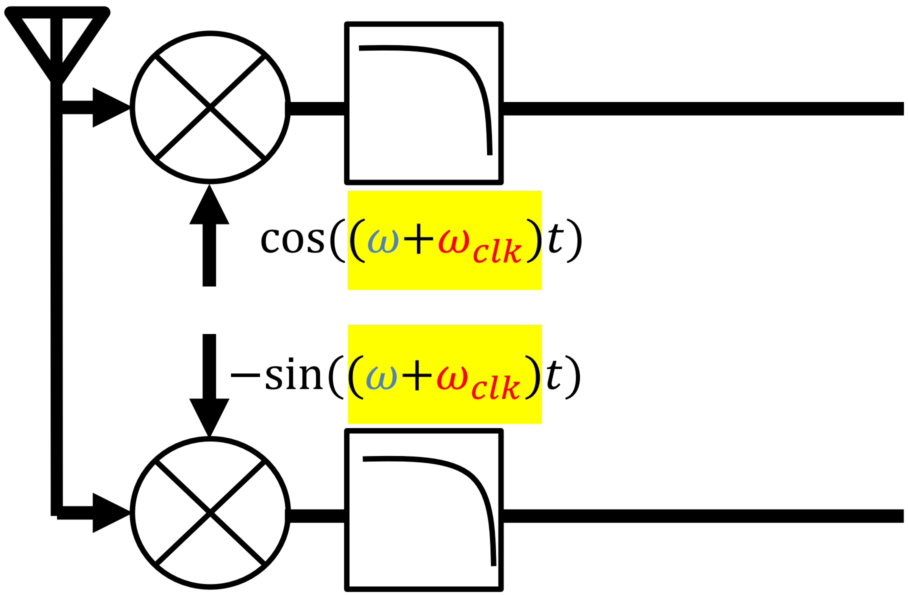
Extraction

Quadrature Amplitude Demodulation

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

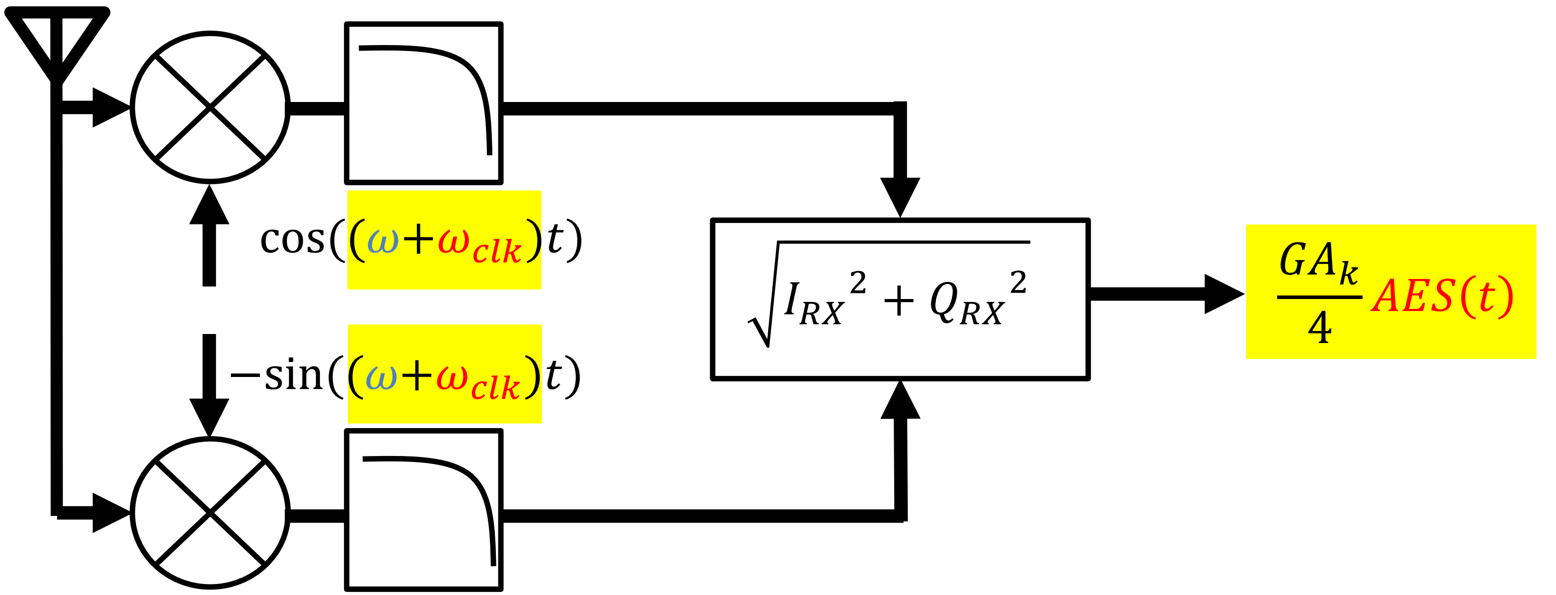
Quadrature Amplitude Demodulation

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



Quadrature Amplitude Demodulation

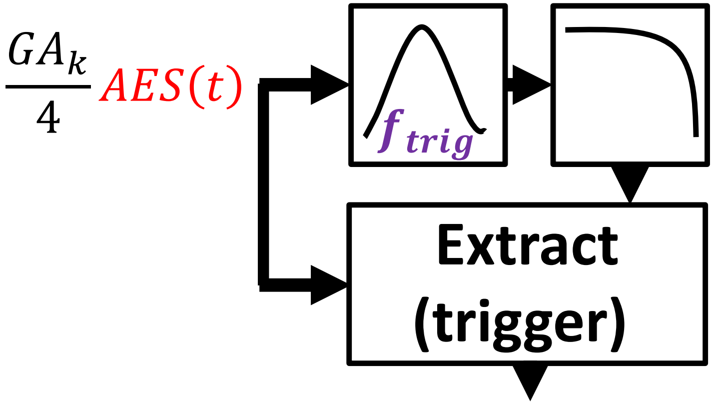
$$\frac{GA_k}{2} AES(t) \cos((\omega + \omega_{clk})t + \varphi_k)$$



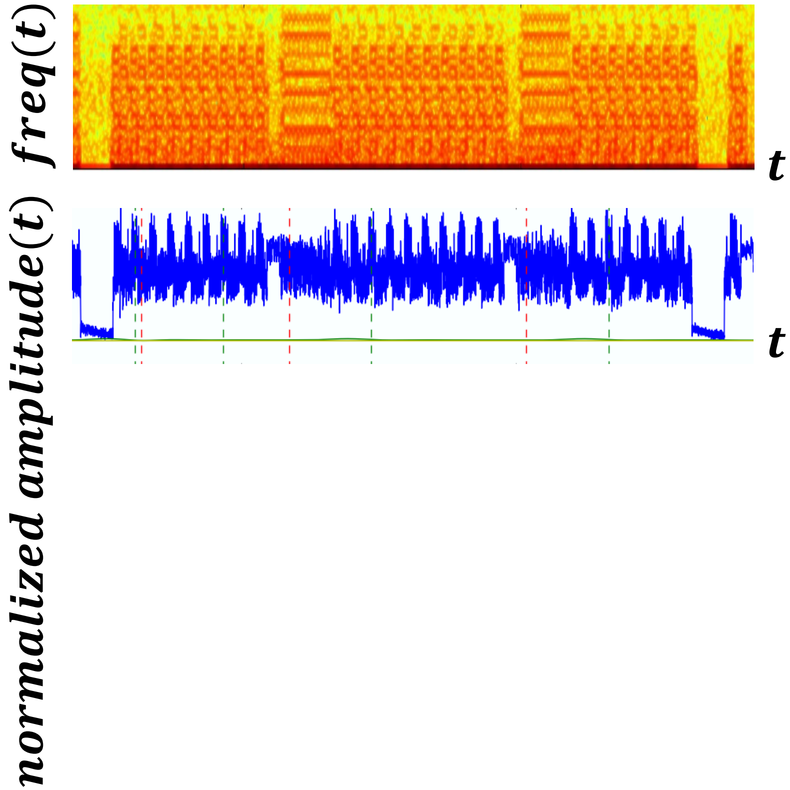
INSTITUT CARNOT Télécom & Société numérique

EURECOM Sophia Antipolis

Extraction

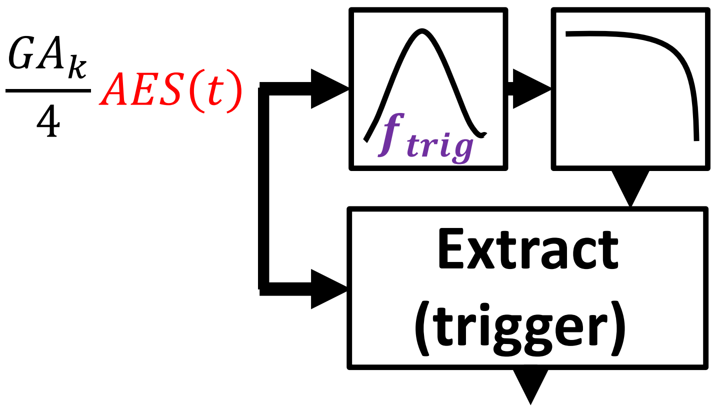


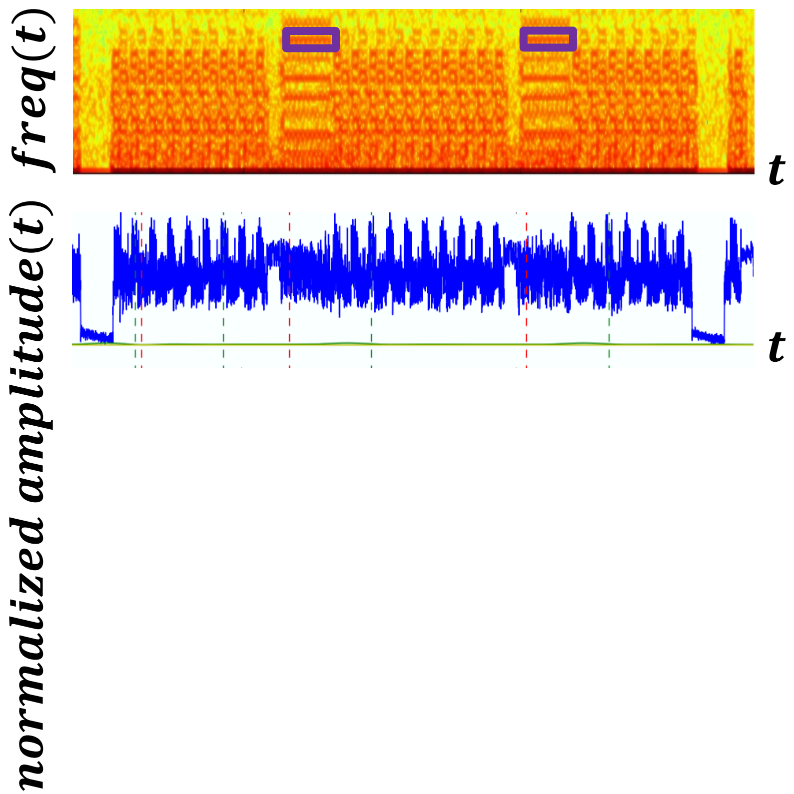
$\frac{GA_k}{4}AES(t)$
f_{trig}
Extract
(trigger)



$freq(t)$
t
$normalized\ amplitude(t)$
t

Extraction

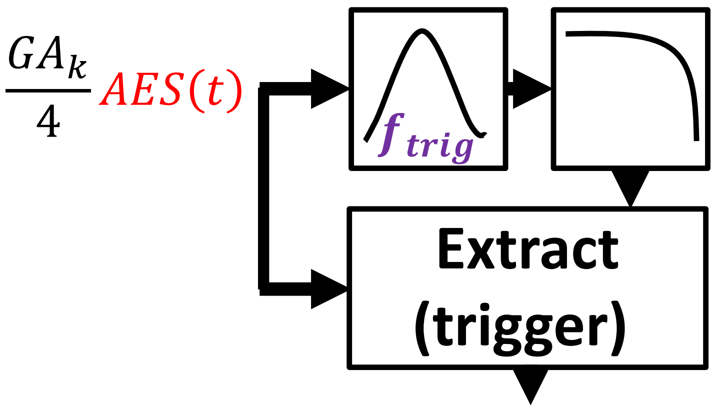


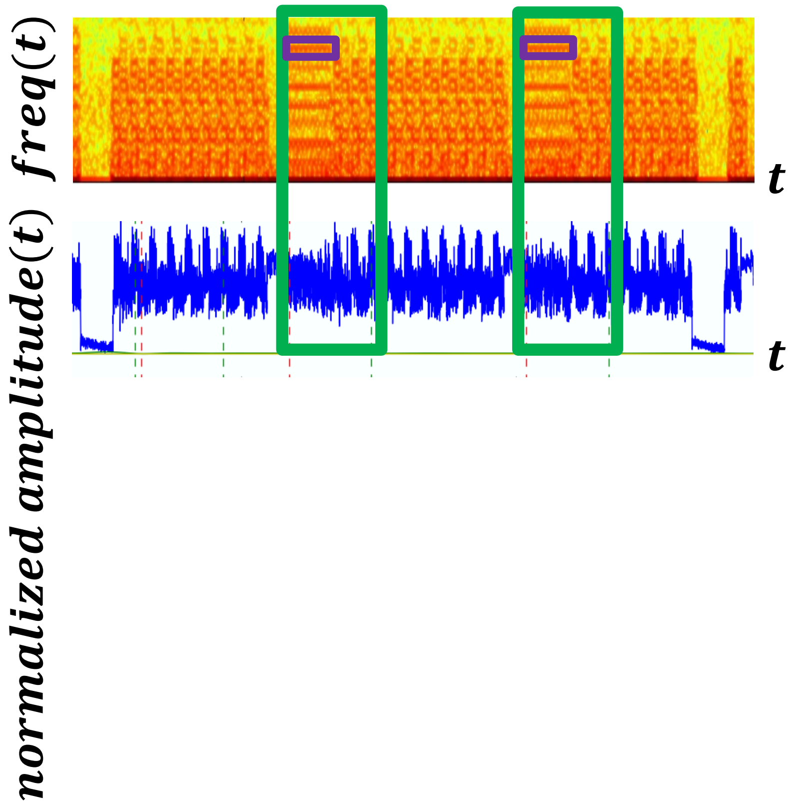


INSTITUT CARNOT Télécom & Société numérique

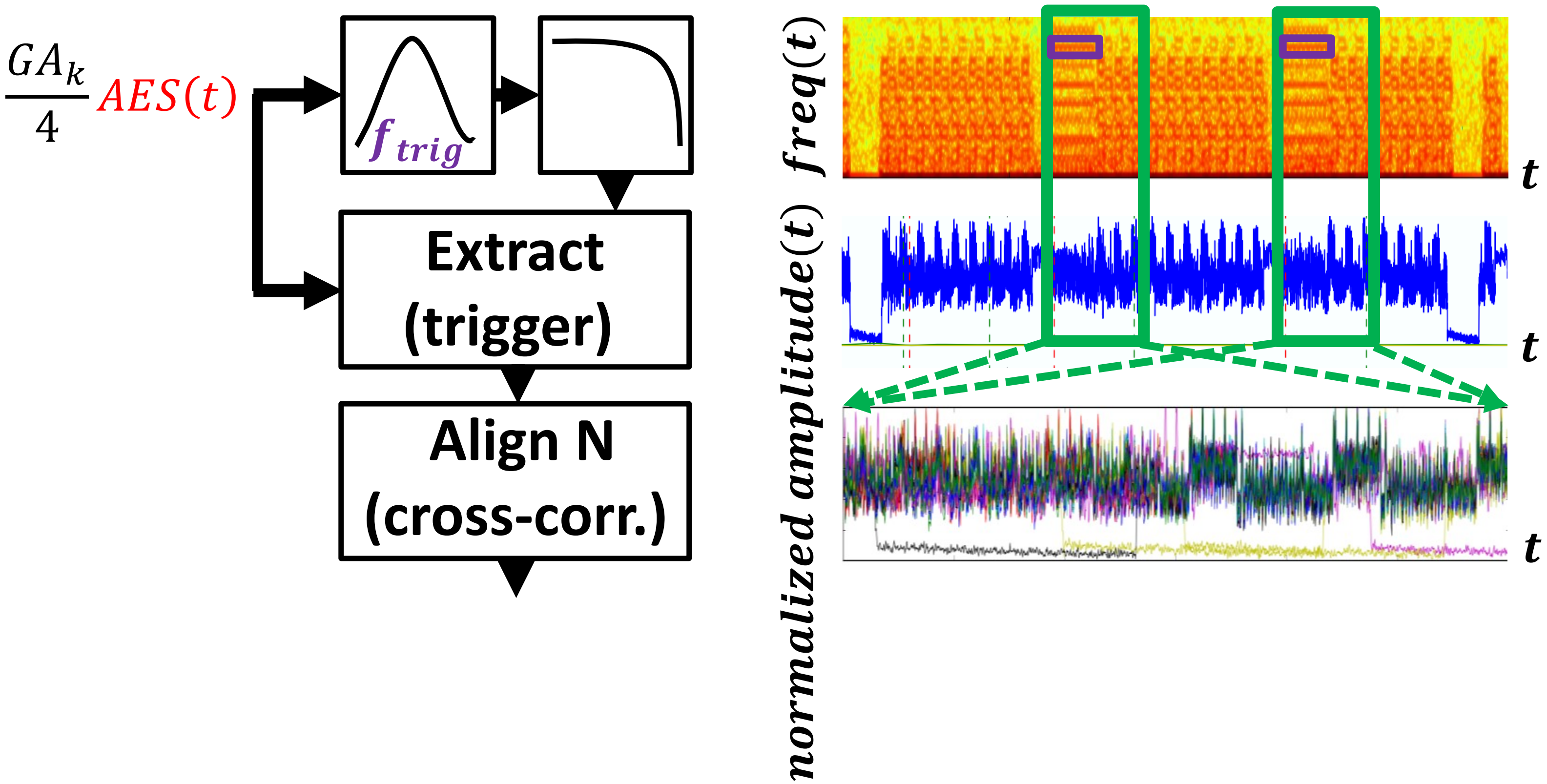
EURECOM Sophia Antipolis

Extraction


$\frac{GA_k}{4}AES(t)$
f_{trig}
Extract
(trigger)

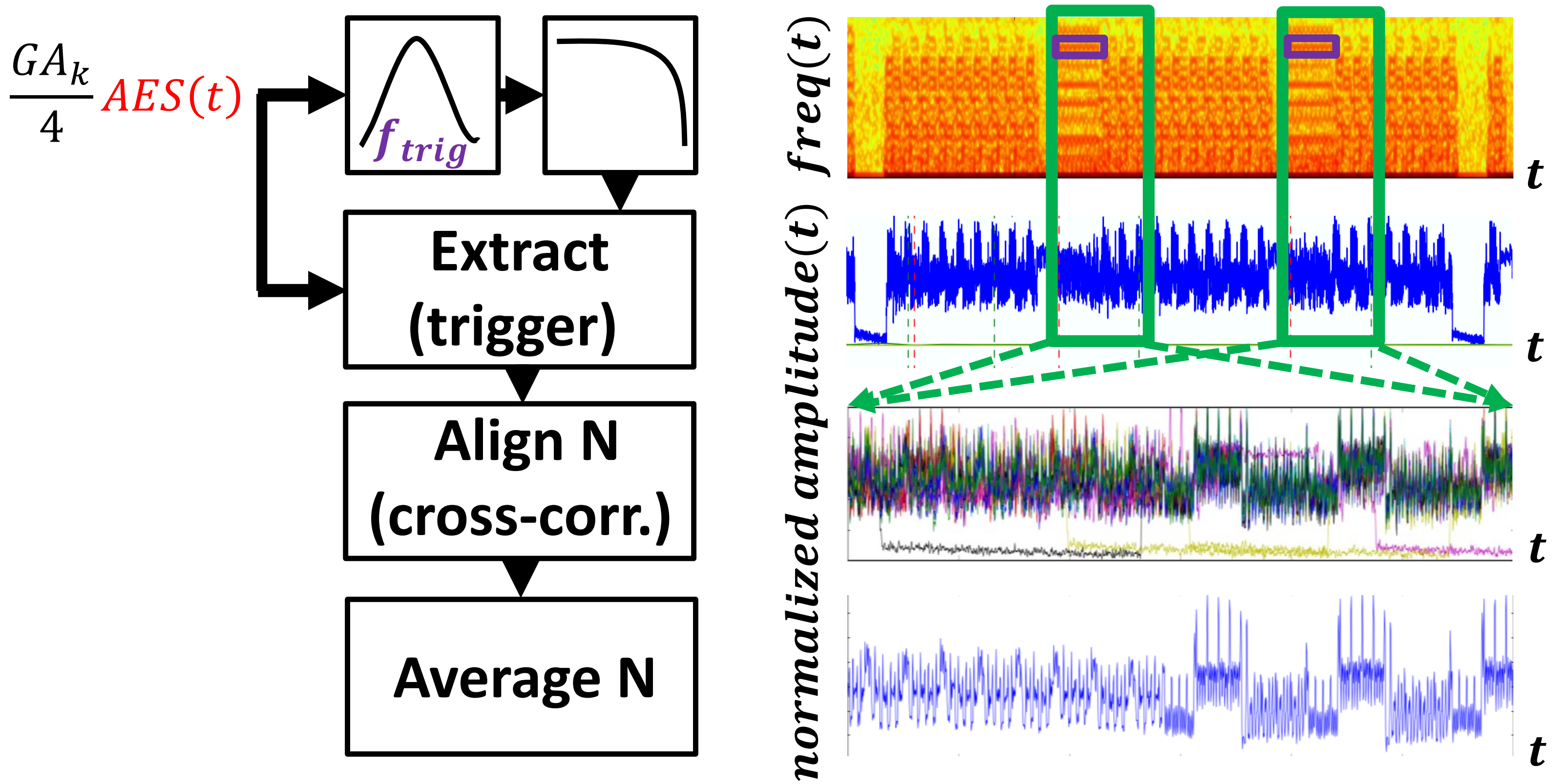

$freq(t)$
t
$normalized\ amplitude(t)$
t

Extraction



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

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

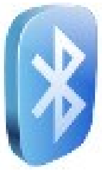
Attack

Attacking

Targets:
Cortex-M4 + BT TX
TinyAES, mbedTLS

Attacking

Targets:
Cortex-M4 + BT TX
TinyAES, mbedTLS



Extraction:
Automated via radio
Known plaintext

Attacking

Targets:
Cortex-M4 + BT TX
TinyAES, mbedTLS

Extraction:
Automated via radio
Known plaintext

Attacks:
Correlation, Template
Code based on
ChipWhisperer

Attacking

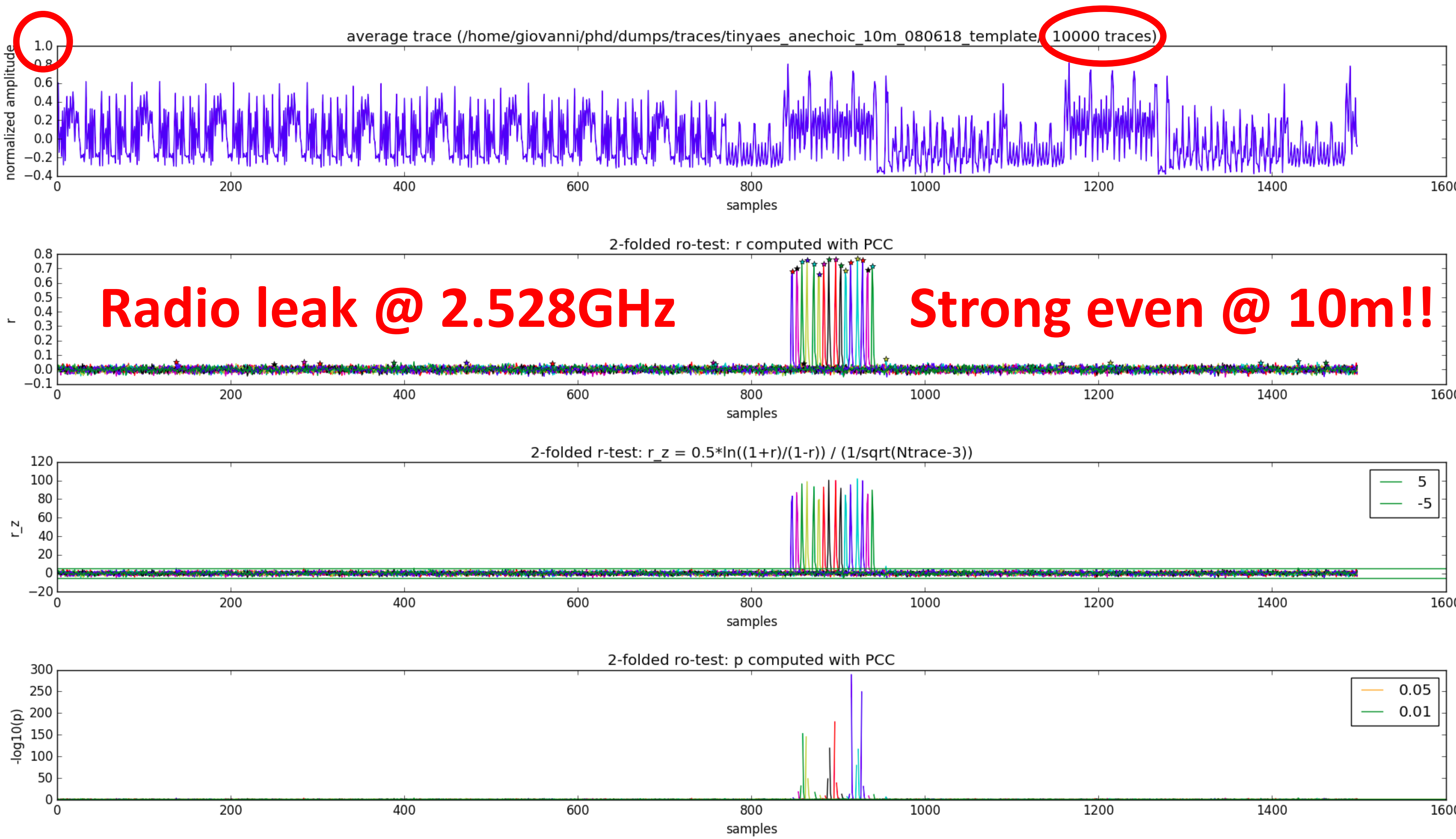
Targets:
Cortex-M4 + BT TX
TinyAES, mbedTLS

Extraction:
Automated via radio
Known plaintext

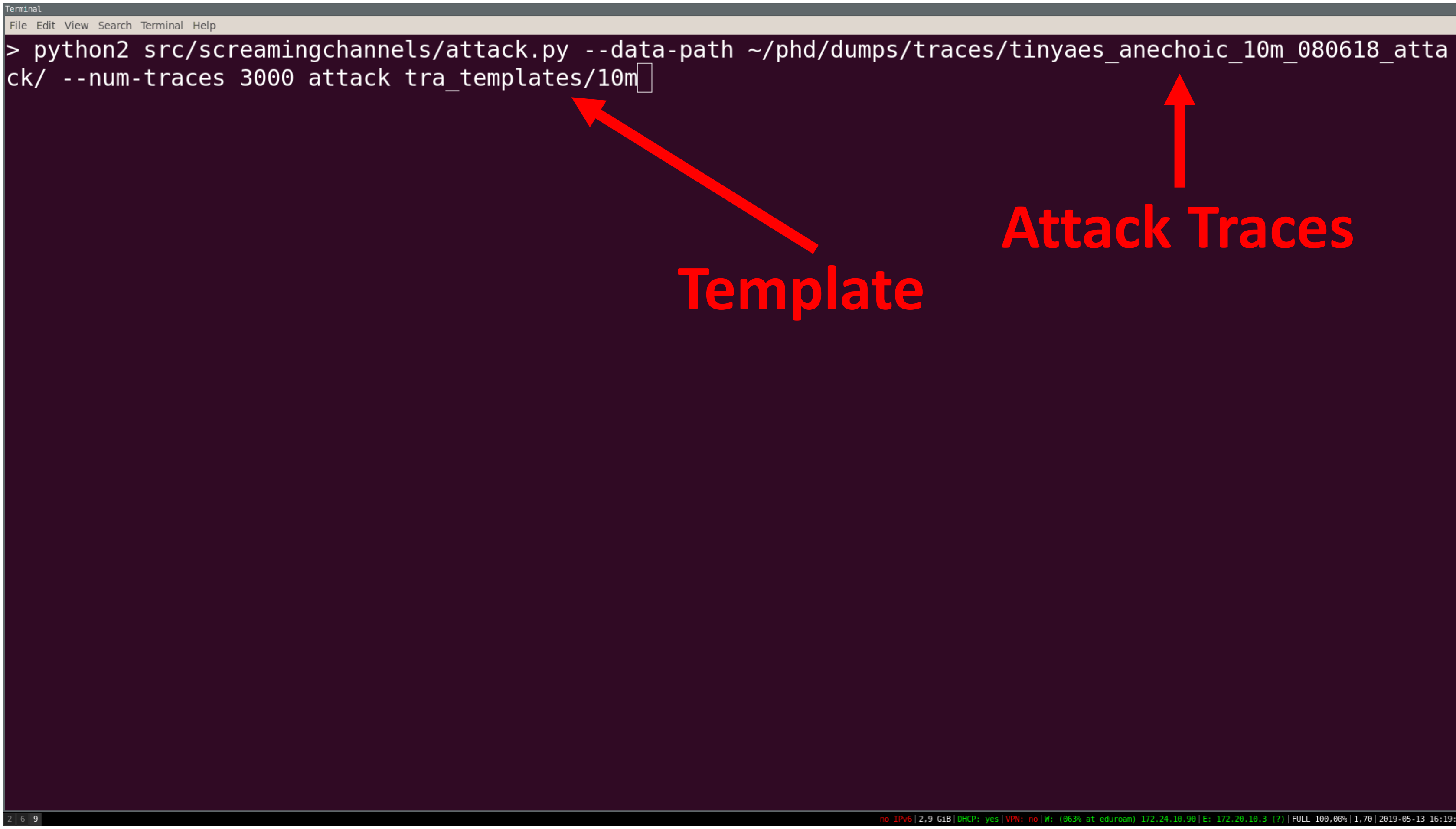
Attacks:
Correlation, Template
Code based on
ChipWhisperer

Much more advanced attacks exist

Correlation @ 10m



Quick Demo


Terminal
File Edit View Search Terminal Help
> python2 src/screamingchannels/attack.py --data-path ~/phd/dumps/traces/tinyaes_anechoic_10m_080618_attack/ --num-traces 3000 attack tra_templates/10m
Attack Traces
Template

Quick Demo

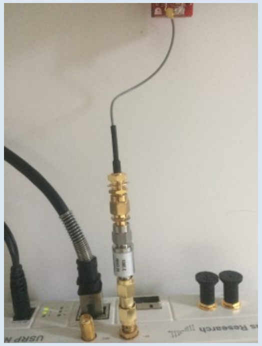
Terminal
File Edit View Search Terminal Help
> python2 src/screamingchannels/attack.py --data-path ~/phd/dumps/traces/tinyaes_anechoic_10m_080618_attack/ --num-traces 3000 attack tra_templates/10m
Attack Traces
Template
Attack one byte
at a time

Quick Demo


Terminal
File Edit View Search Terminal Help
> python2 src/screamingchannels/attack.py --data-path ~/phd/dumps/traces/tinyaes_anechoic_10m_080618_attack/ --num-traces 3000 attack tra_templates/10m
Attack Traces
Template
Attack one byte at a time
SUCCESS!

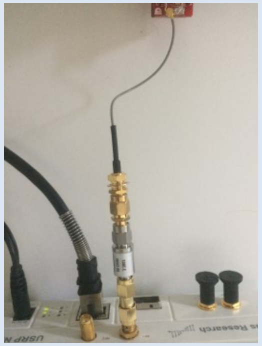
Evolution of the attack

Evolution of the attack

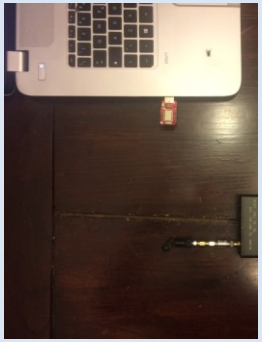


Cable

Evolution of the attack

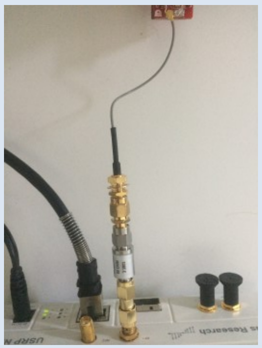


$\boldsymbol{Cable}$

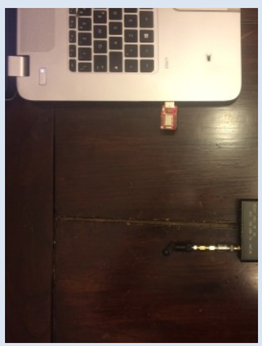


$\boldsymbol{15\ cm}$

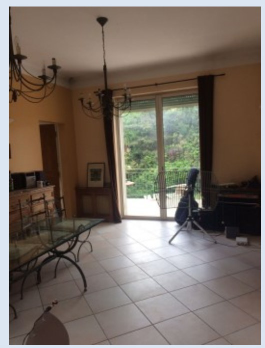
Evolution of the attack



$\boldsymbol{Cable}$

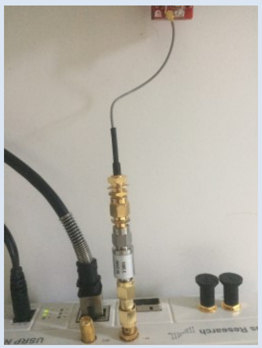


$\boldsymbol{15\ cm}$

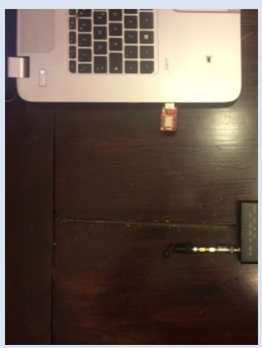


$\boldsymbol{2\ m}$

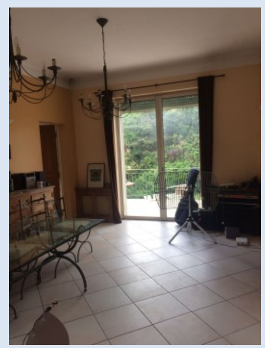
Evolution of the attack



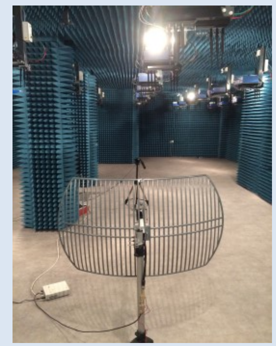
Cable



15 ***cm***

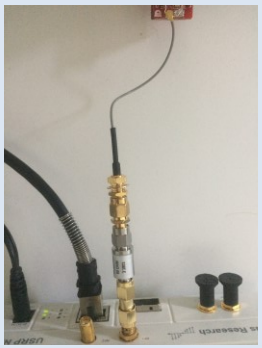


2 ***m***

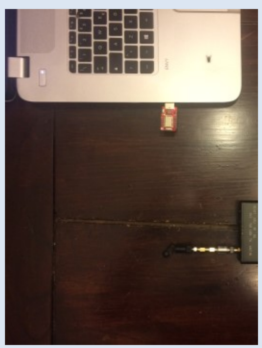


3 ***m***

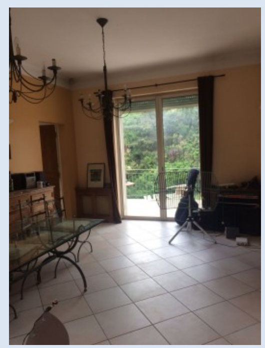
Evolution of the attack



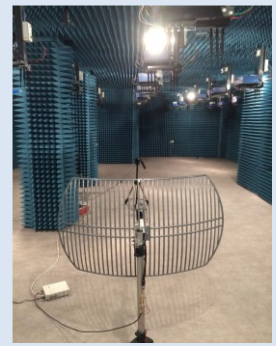
Cable



15 *cm*



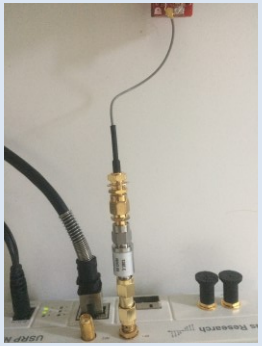
2 *m*



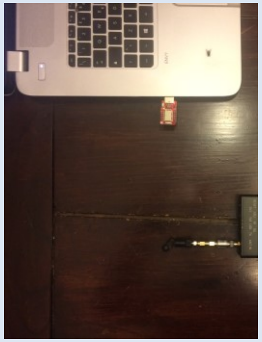
3 *m*

5 *m*

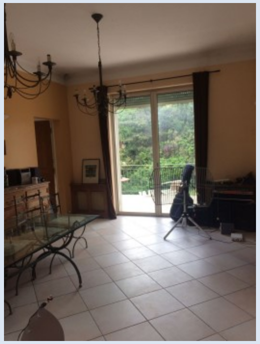
Evolution of the attack



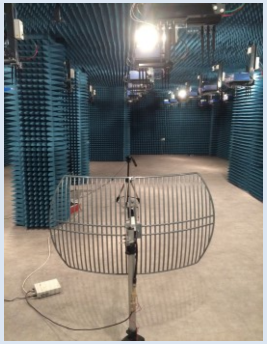
Cable



15 cm

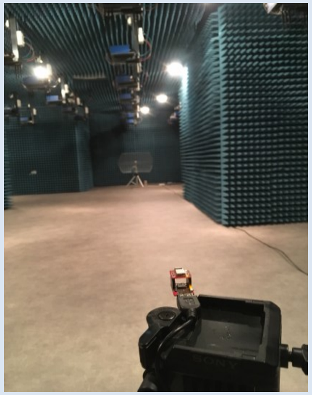


2 m



3 m

5 m



10 m

Protection

Countermeasures

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

Countermeasures

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

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

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)

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)

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.]

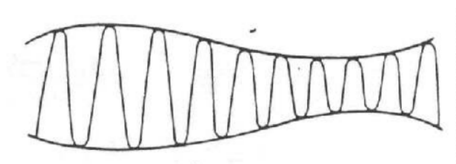


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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:

Tempest Fundamentals [5]
From ‘80s
Declassified 2000

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.]

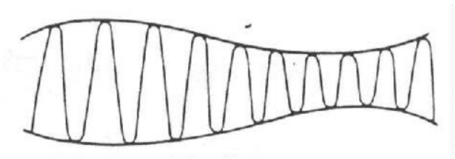


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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

Tempest Fundamentals [5]
From ‘80s
Declassified 2000

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.]

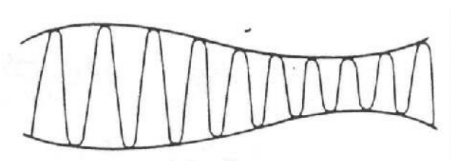


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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**

Tempest Fundamentals [5]
From '80s
Declassified 2000

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.]

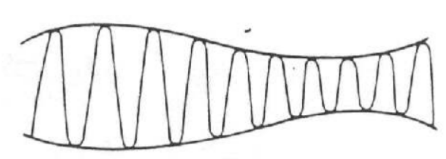


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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**

1. **Acoustic**

Tempest Fundamentals [5]

From ‘80s

Declassified 2000

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.]

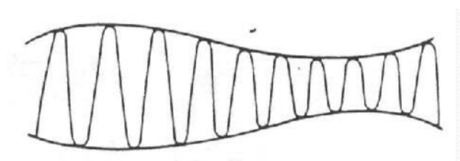


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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

Conclusion

General problem if sensitive processing and wireless tx

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

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**

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)**

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**

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.

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

GRADUATE SCHOOL & RESEARCH CENTER IN DIGITAL SCIENCE

Institut Mines-Télécom

EURECOM
Sophia Antipolis

Academia

Institut Mines-Télécom

Politecnico di Torino 1859 1906

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