GRADUATE SCHOOL AND RESEARCH CENTER AT THE HEART OF THE DIGITAL SOCIETY

EURECOM
Sophia Antipolis

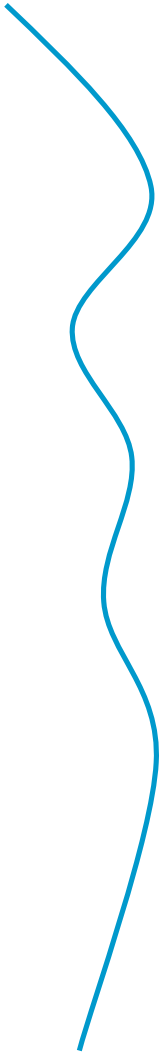
Screaming Channels

When Electromagnetic Side Channels Meet Radio Transceivers

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

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, …

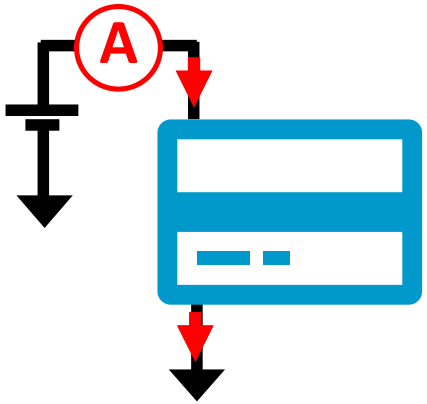
Generally protected against attacks which require physical access

Conventional Side Channels

Physical activity depends on logic data

Conventional Side Channels

Power (current)

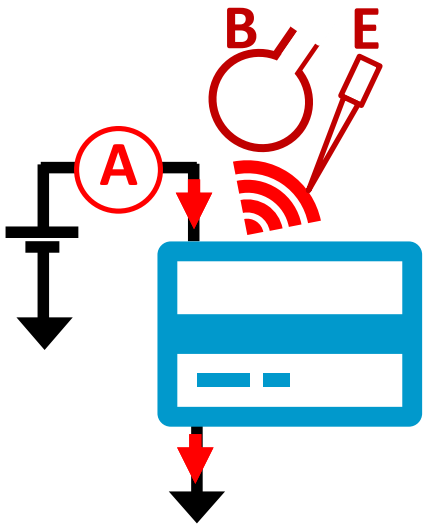


Physical activity depends on logic data

Conventional Side Channels

Direct EM

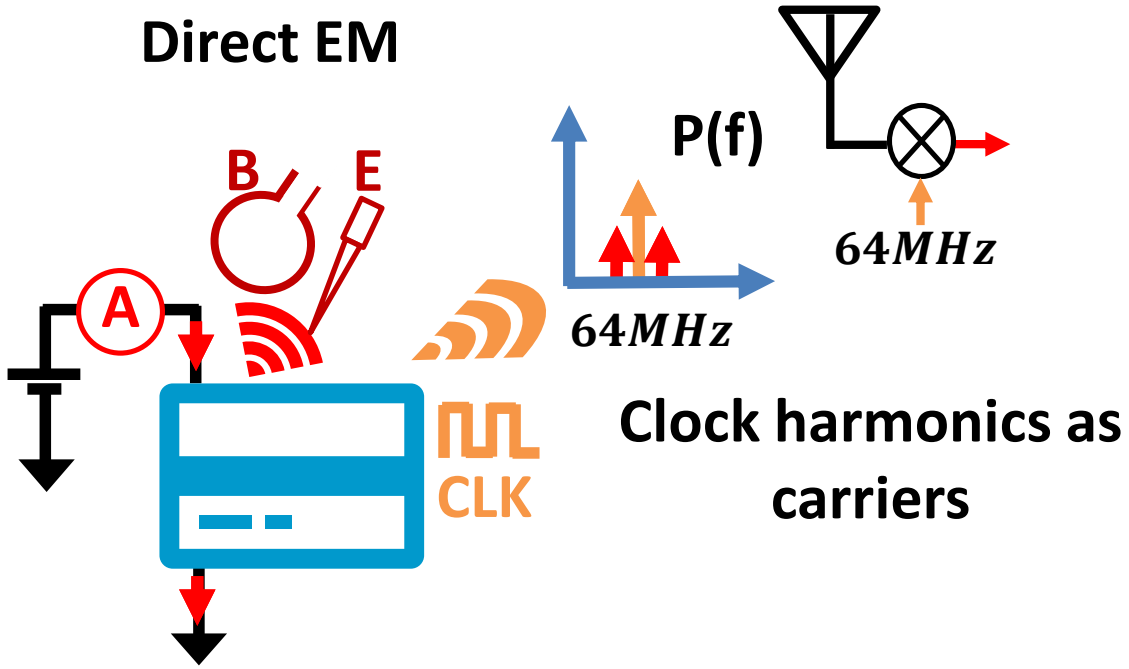
Power (current)



Physical activity depends on logic data

Conventional Side Channels

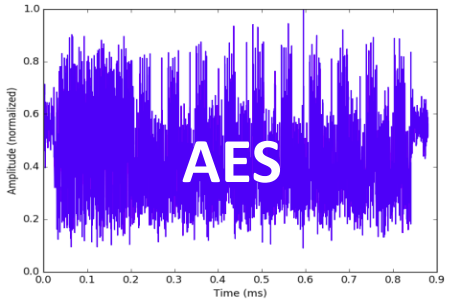
Power (current)



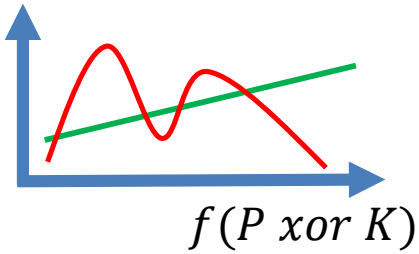
Clock harmonics as carriers

Physical activity depends on logic data

Conventional Side Channels



$AESLeak$

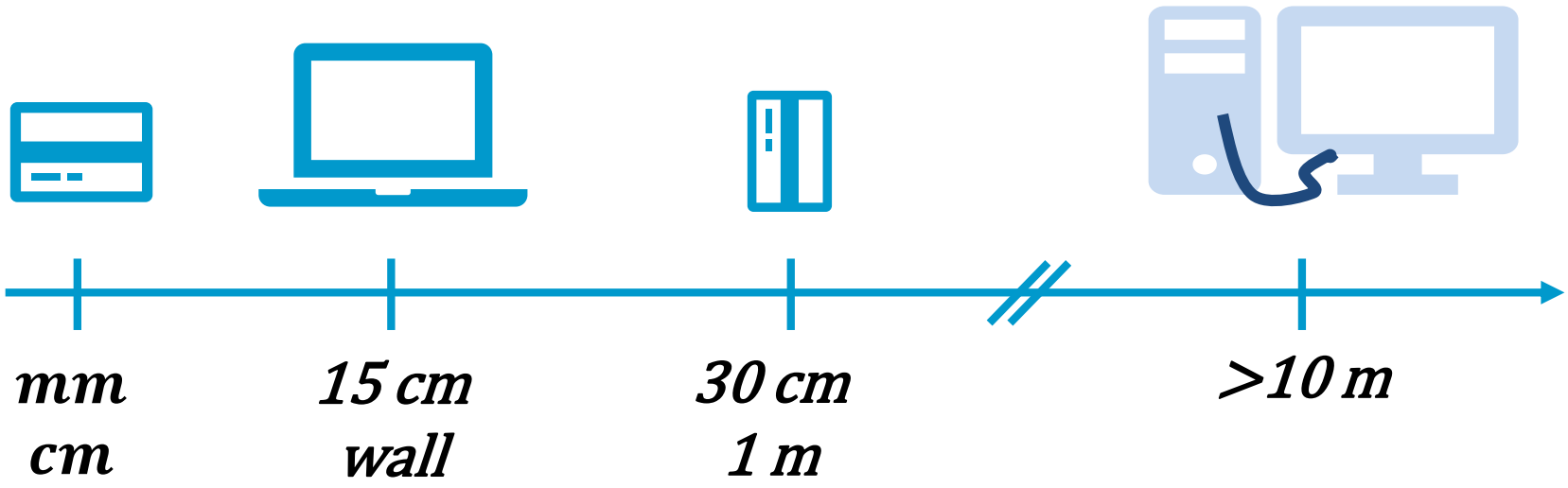


Retrieve traces

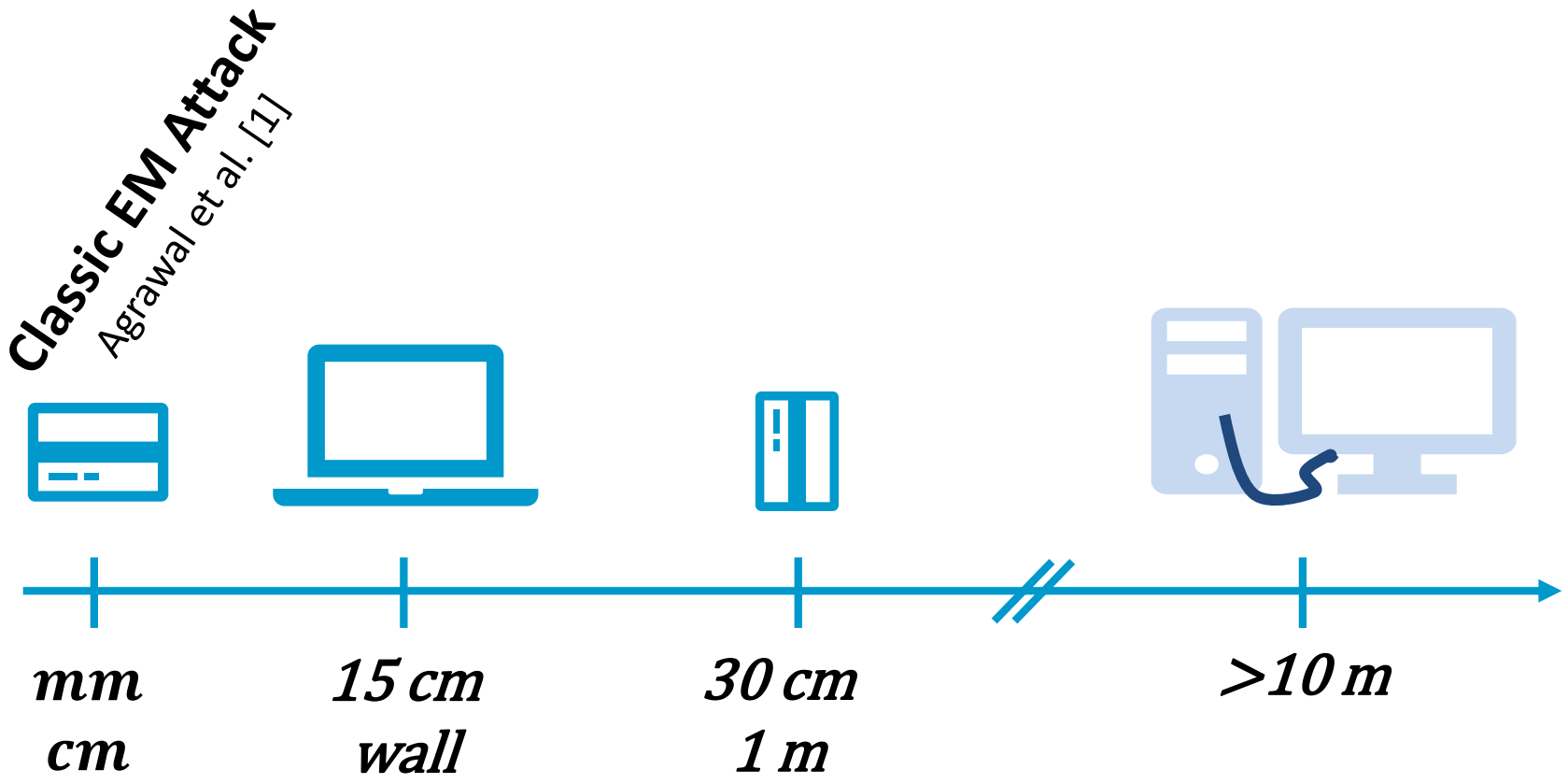
Attack

- **SPA, CPA, TPA, …**
- **SEMA, CEMA, TEMA, …**

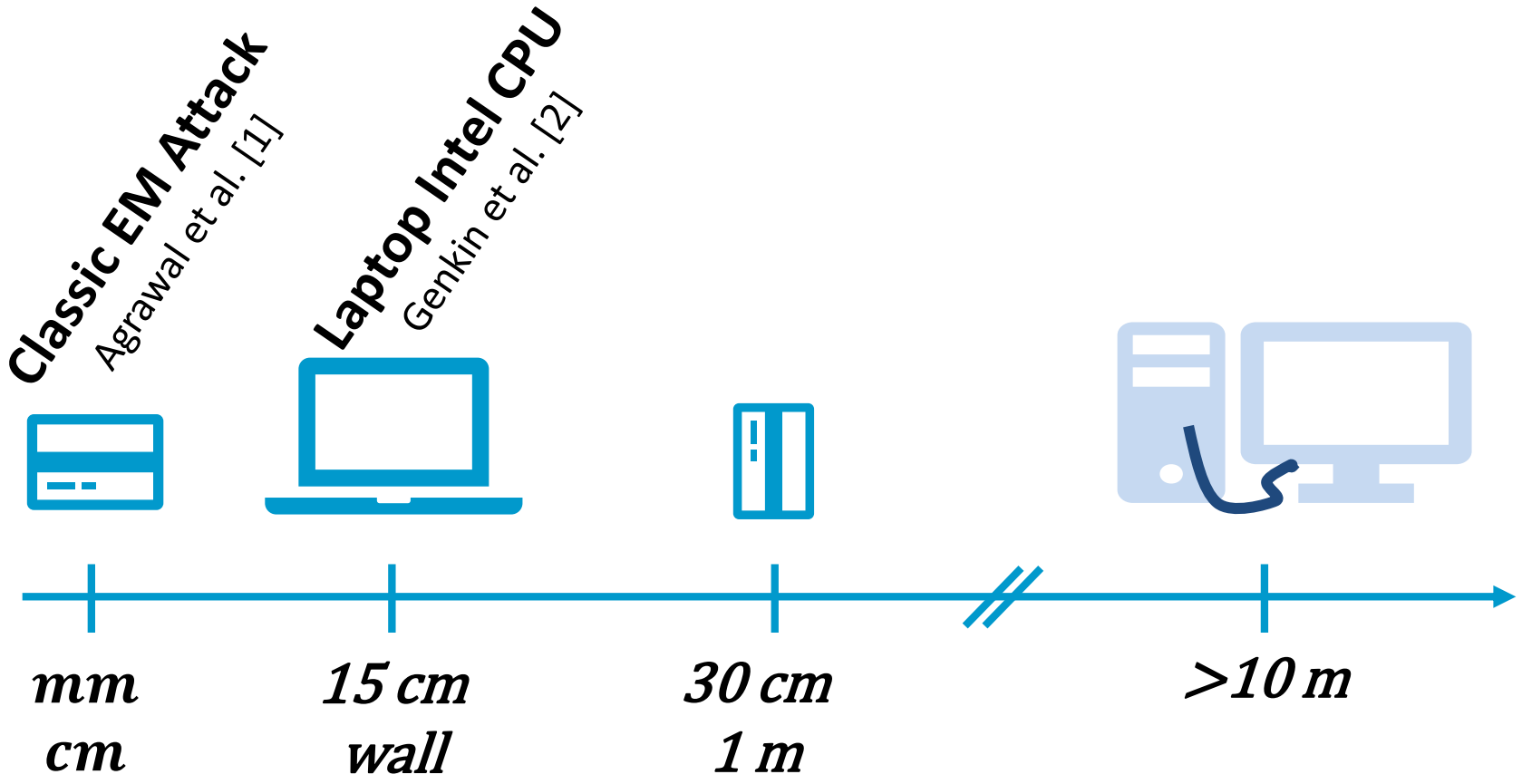
Many Side Channels Involving EM



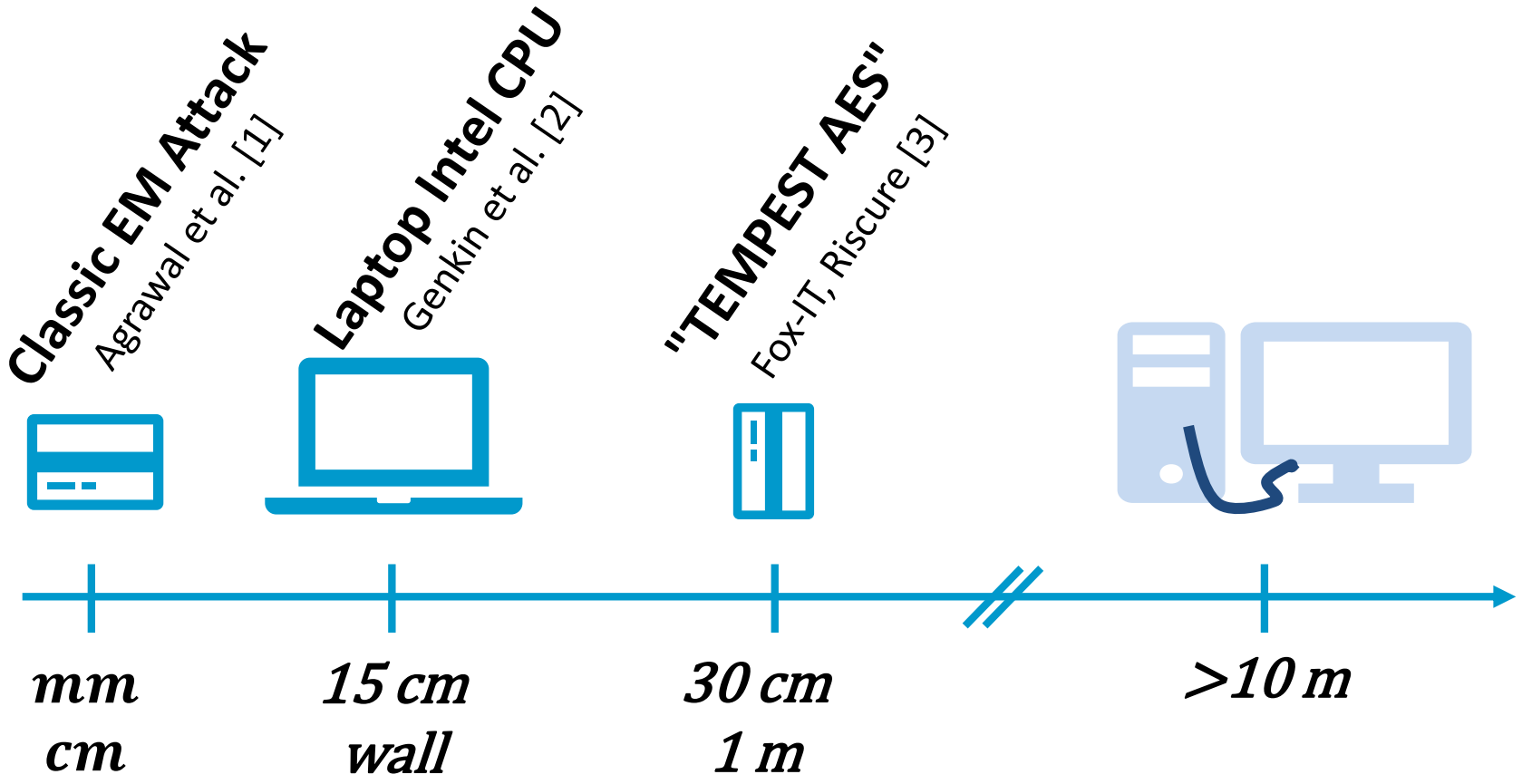
Many Side Channels Involving EM



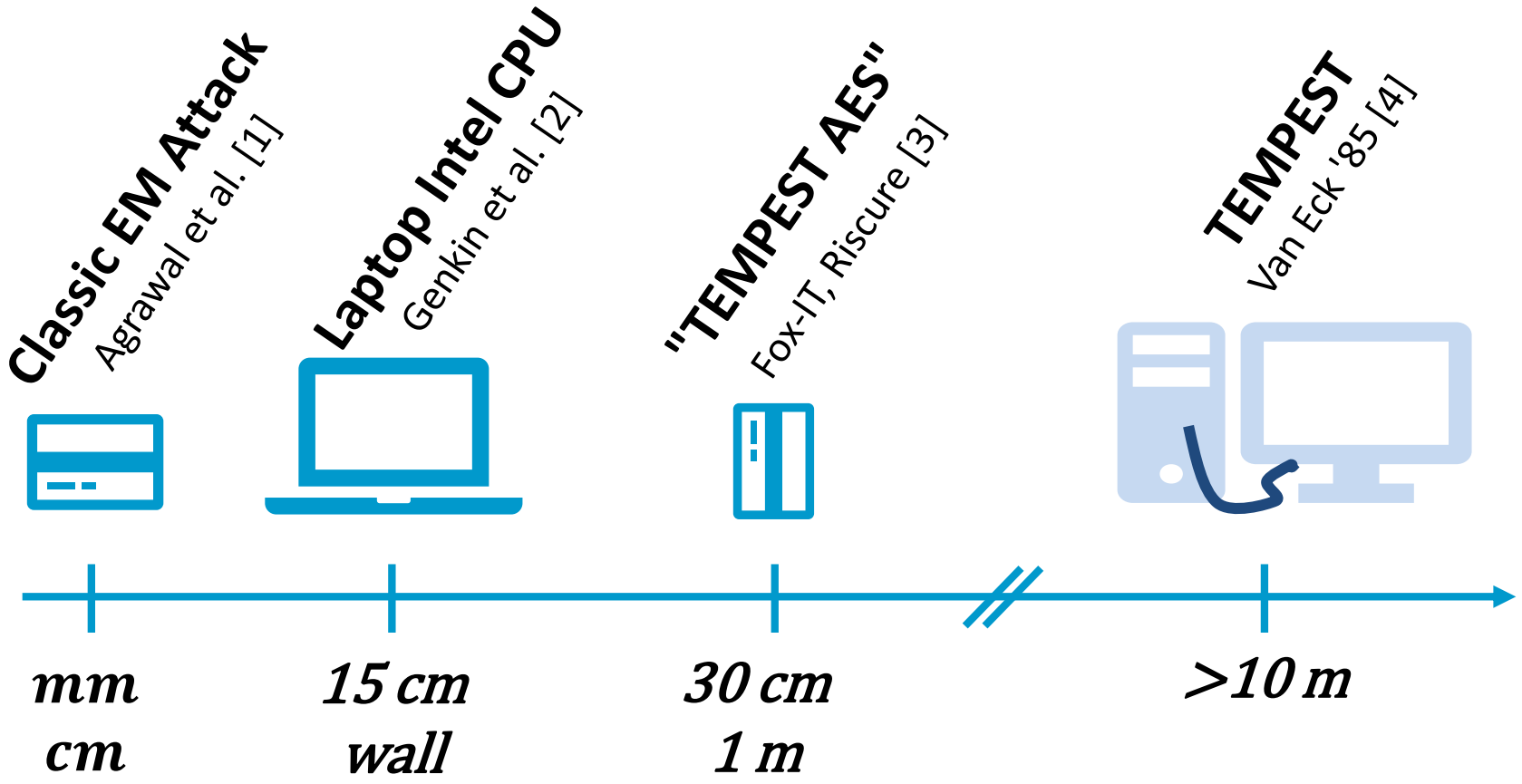
Many Side Channels Involving EM



Many Side Channels Involving EM



Many Side Channels Involving EM



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, …

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

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

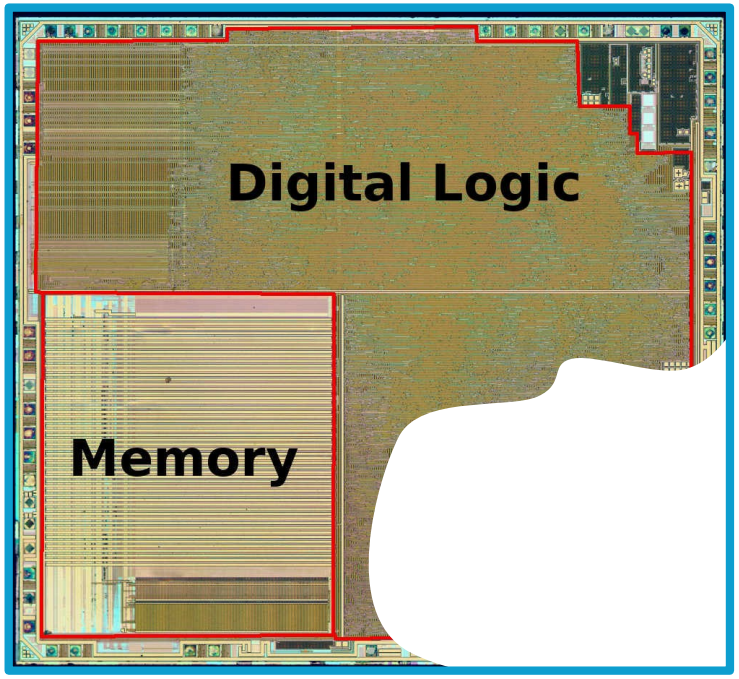
Only remote attacks are considered

Extra Problems When Adding a Radio

Mixed-signal chip

Extra Problems When Adding a Radio

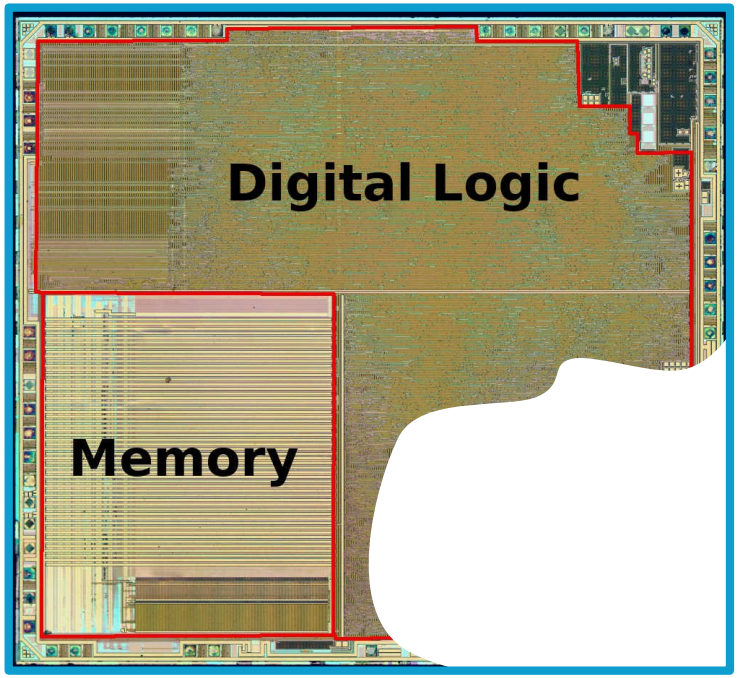
Mixed-signal chip



Extra Problems When Adding a Radio

Data dependent noise

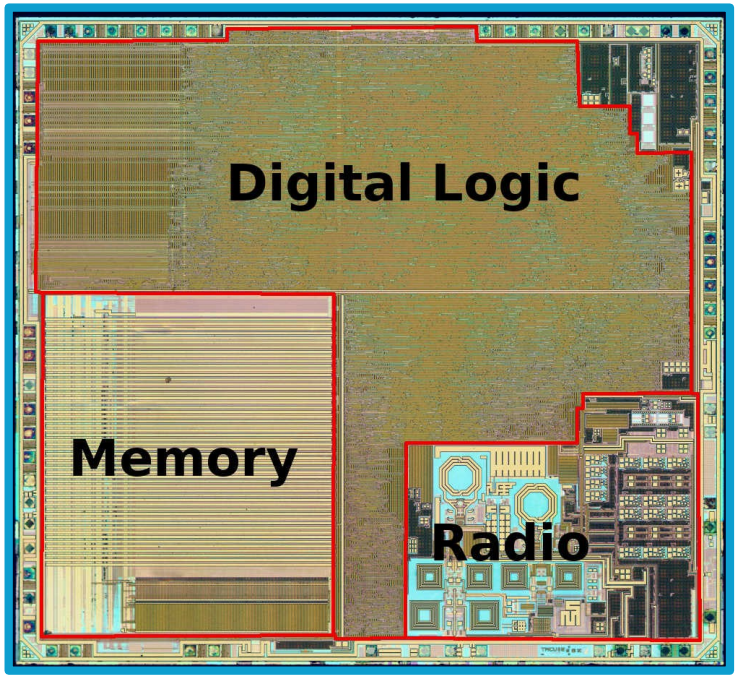
Mixed-signal chip



Extra Problems When Adding a Radio

Data dependent noise

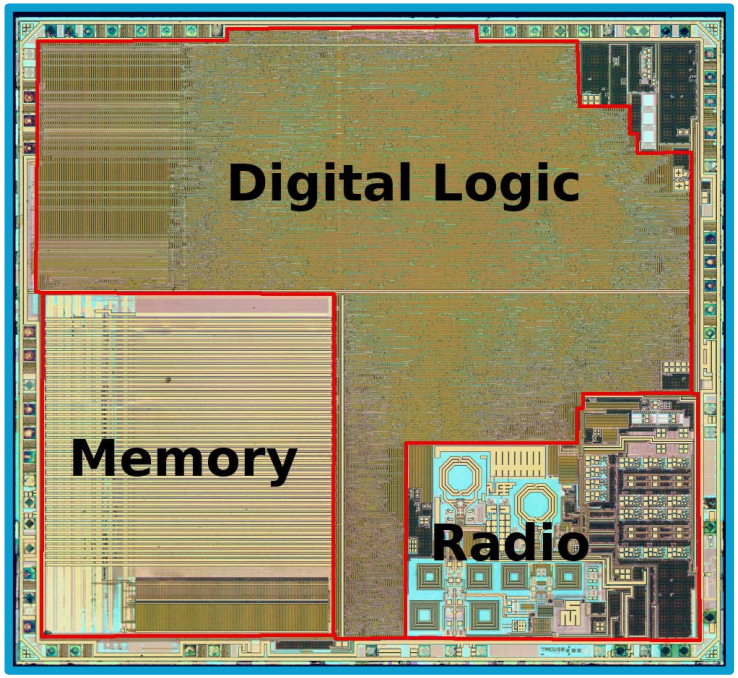
Mixed-signal chip



Extra Problems When Adding a Radio

Mixed-signal chip

Data dependent noise

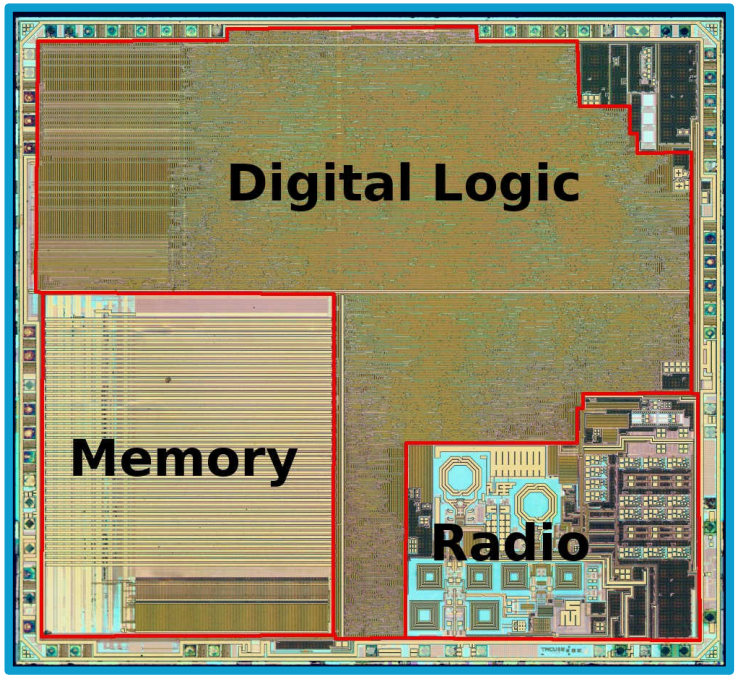


Noise sensitive transmitter

Extra Problems When Adding a Radio

Mixed-signal chip

Data dependent noise



Noise sensitive transmitter

Easy propagation

Screaming Channels

What if … the leak is broadcast? Can we exploit it?

Screaming Channels in Action

Antenna + SDR RX

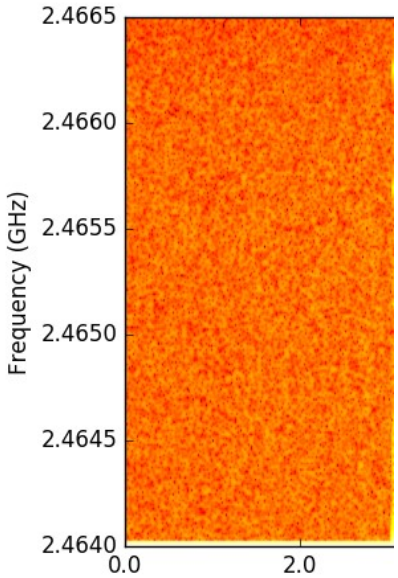
Cortex-M4
+ BT TX

Screaming Channels in Action

Antenna + SDR RX

Cortex-M4
+ BT TX

Radio Off



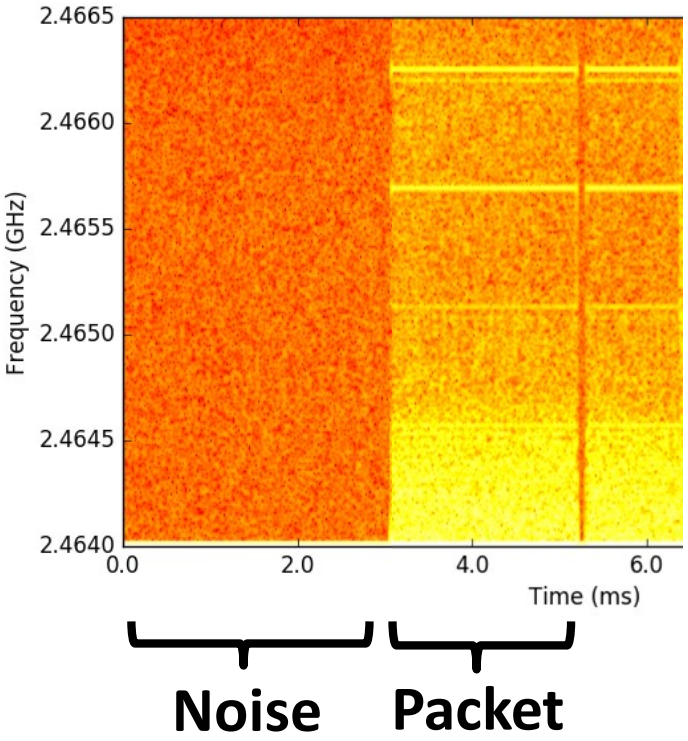
Noise

Screaming Channels in Action

Antenna + SDR RX

Cortex-M4 + BT TX

Radio Off **Radio TX**

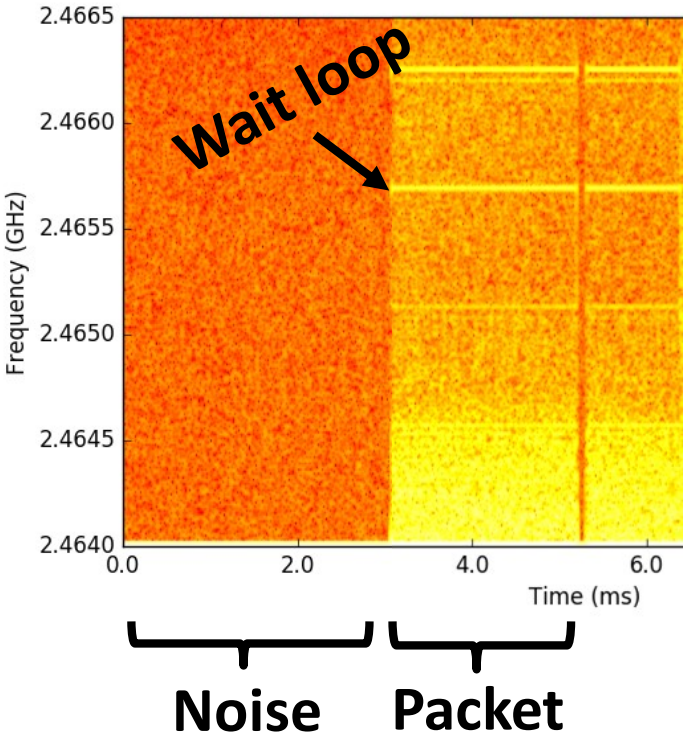


Screaming Channels in Action

Antenna + SDR RX

Cortex-M4
+ BT TX

Radio Off **Radio TX**

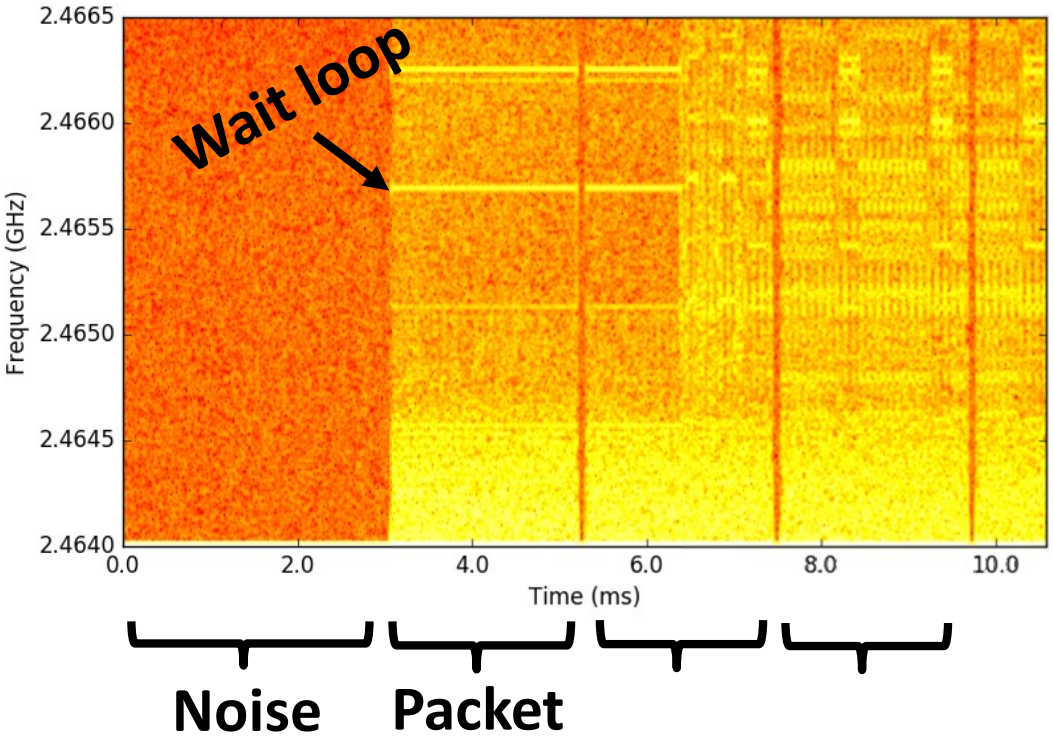


Screaming Channels in Action

Antenna + SDR RX

Cortex-M4 + BT TX

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

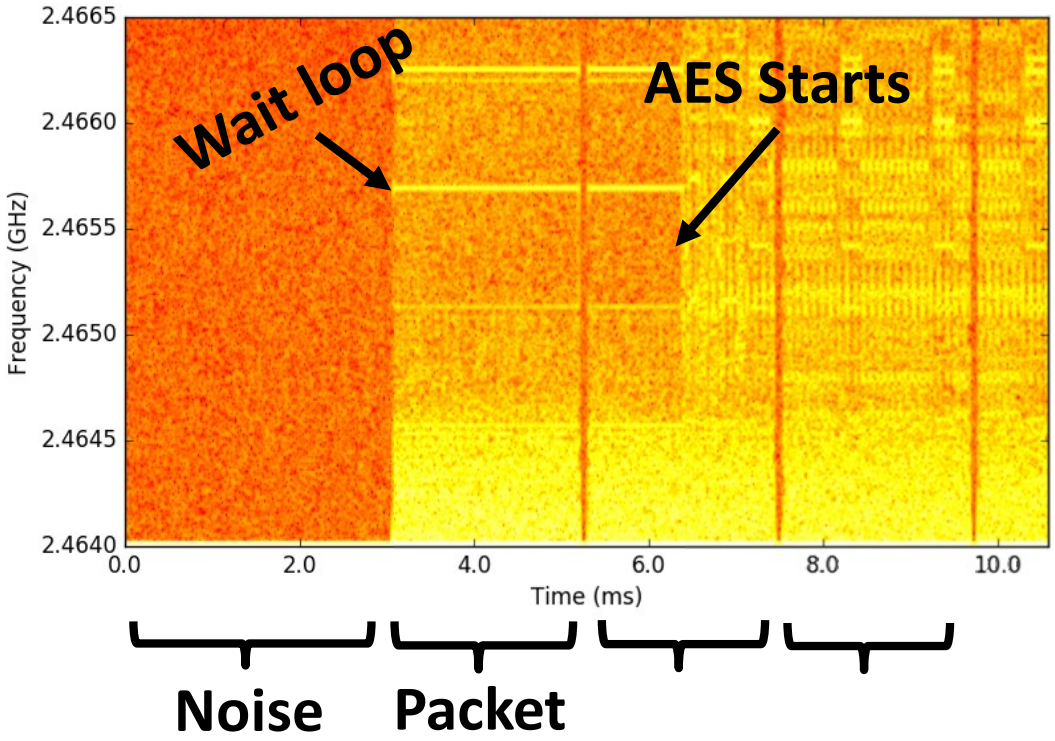


Screaming Channels in Action

Antenna + SDR RX

Cortex-M4 + BT TX

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

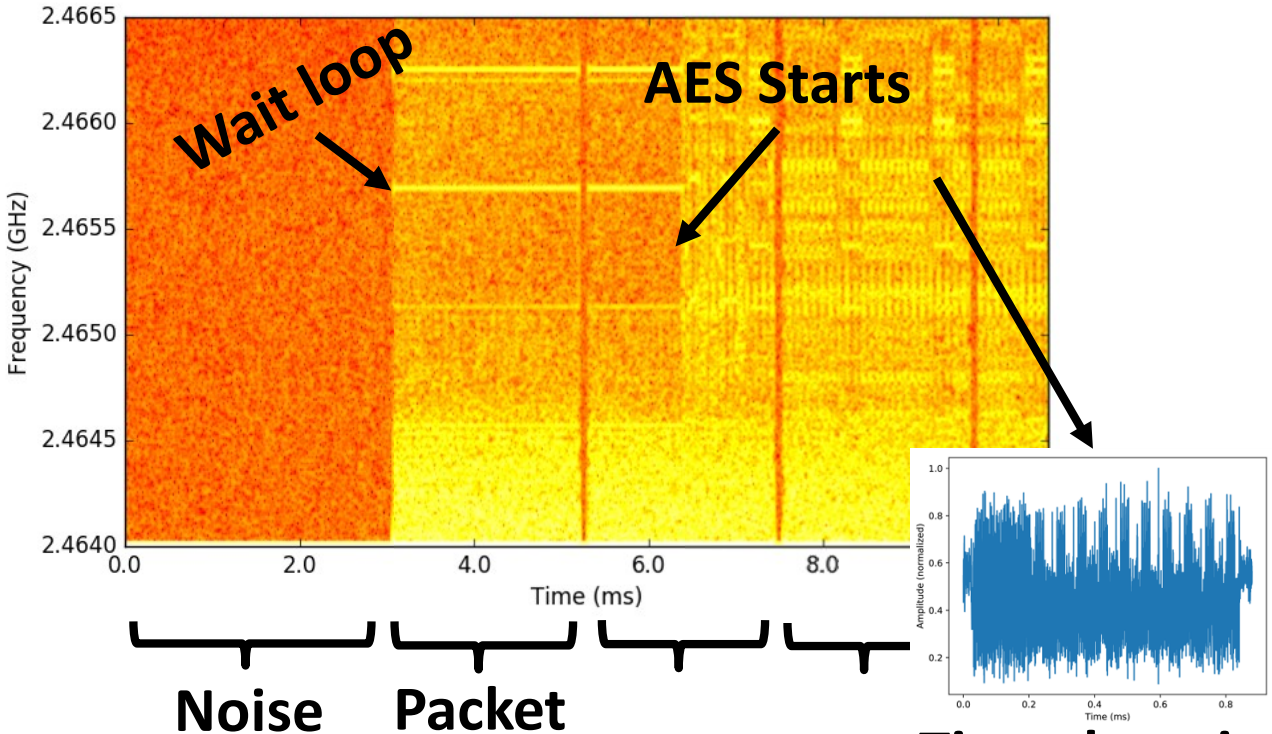


Screaming Channels in Action

Antenna + SDR RX

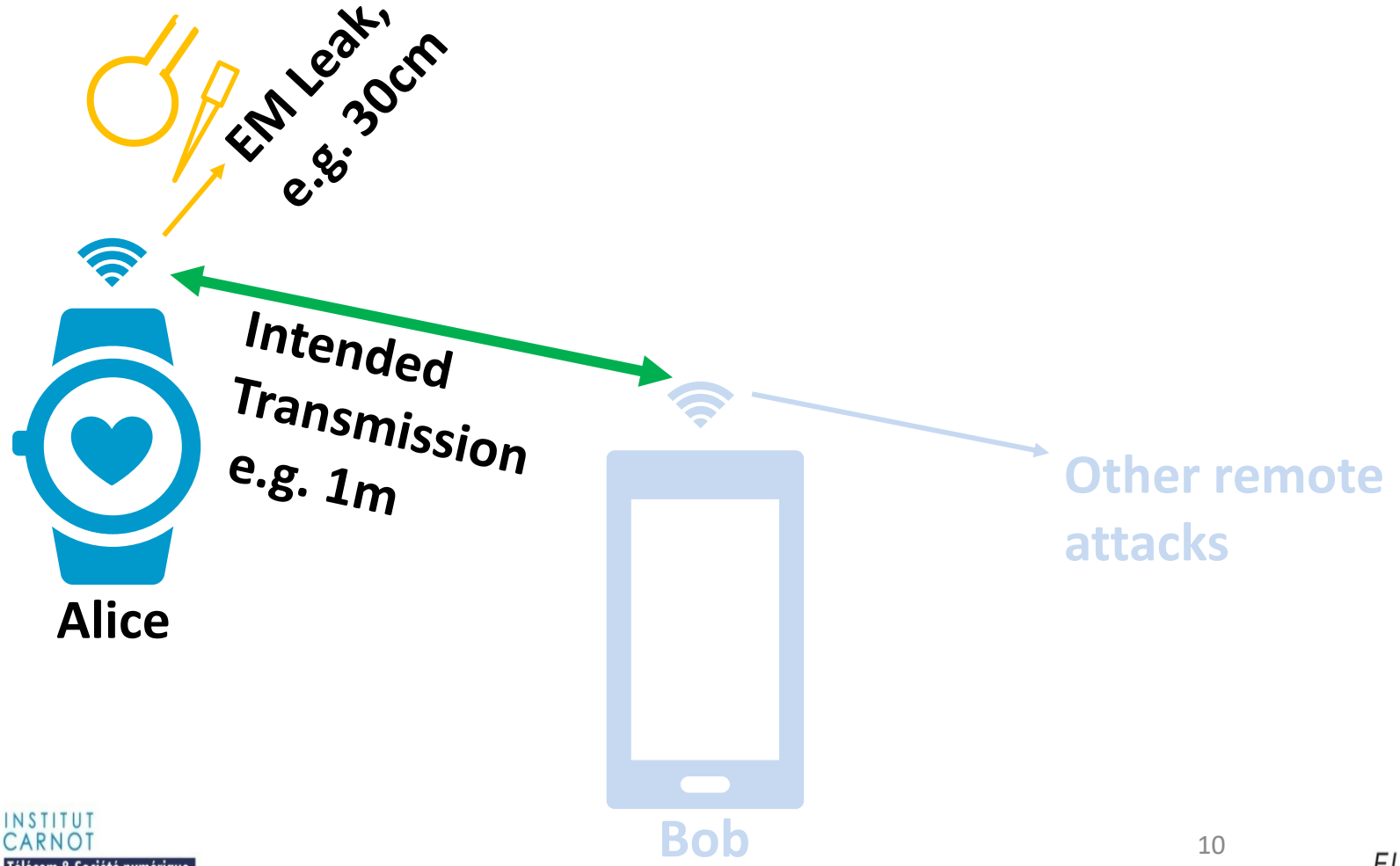
Cortex-M4 + BT TX

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

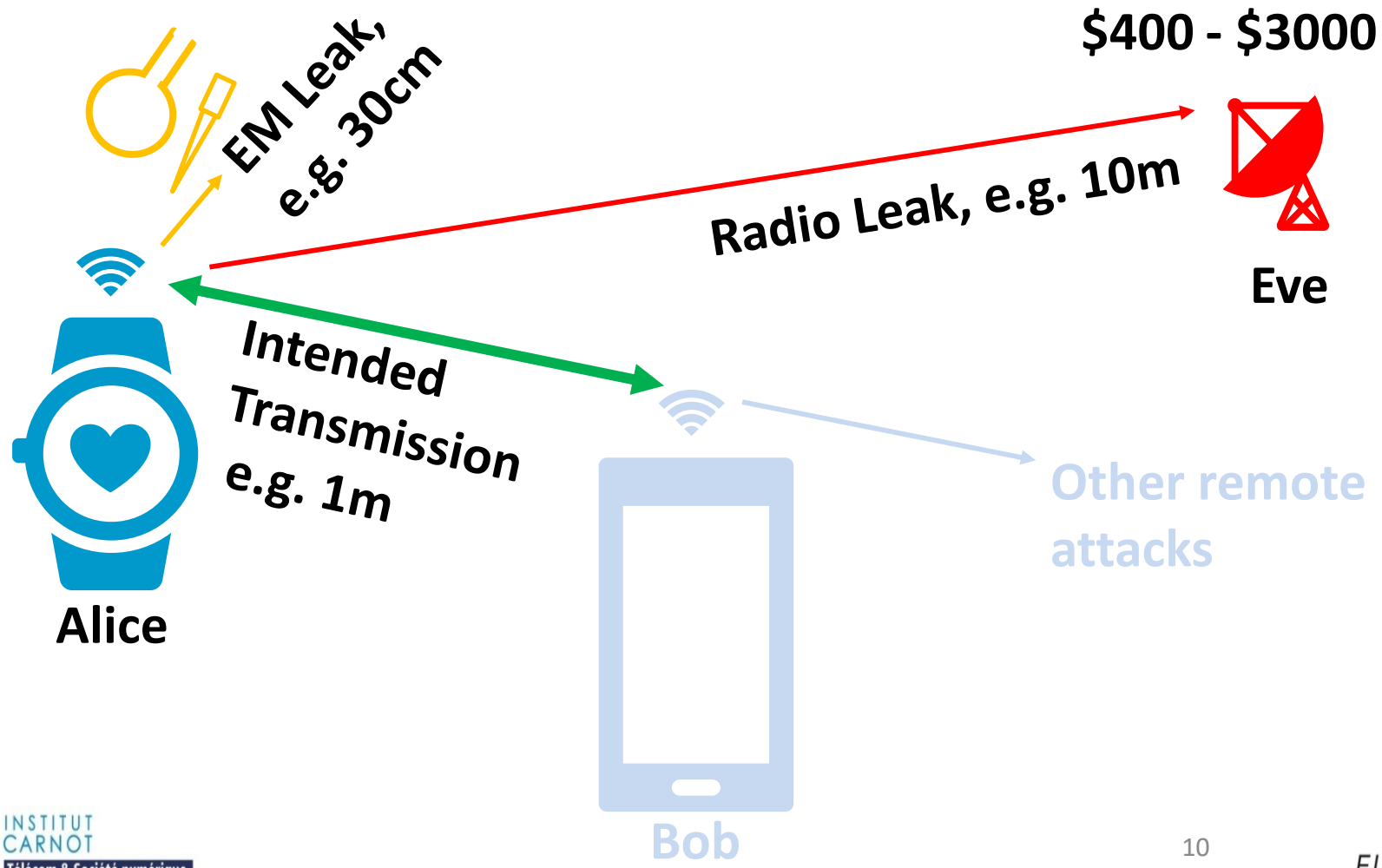


Time domain

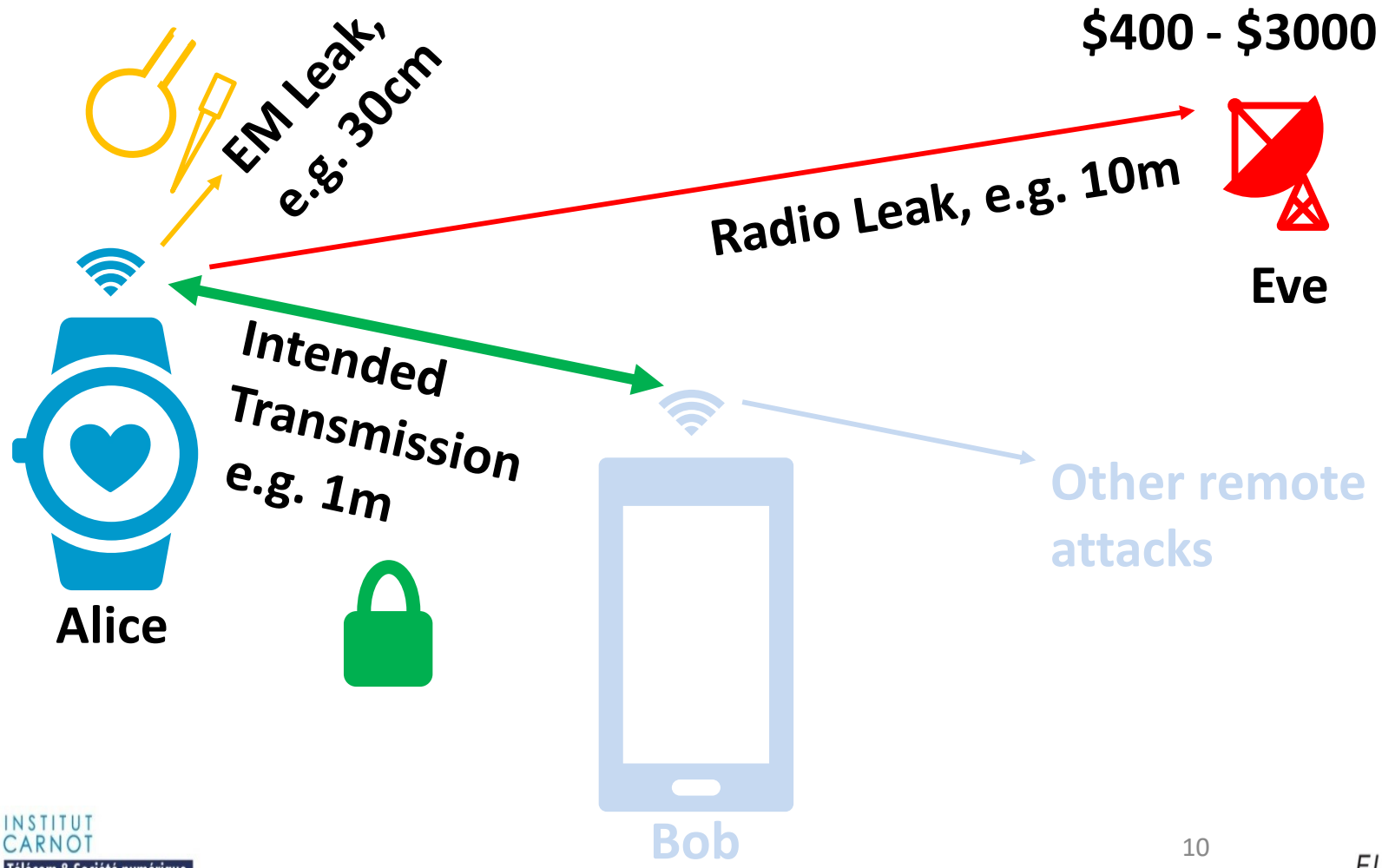
Screaming Channels: Leak Broadcast



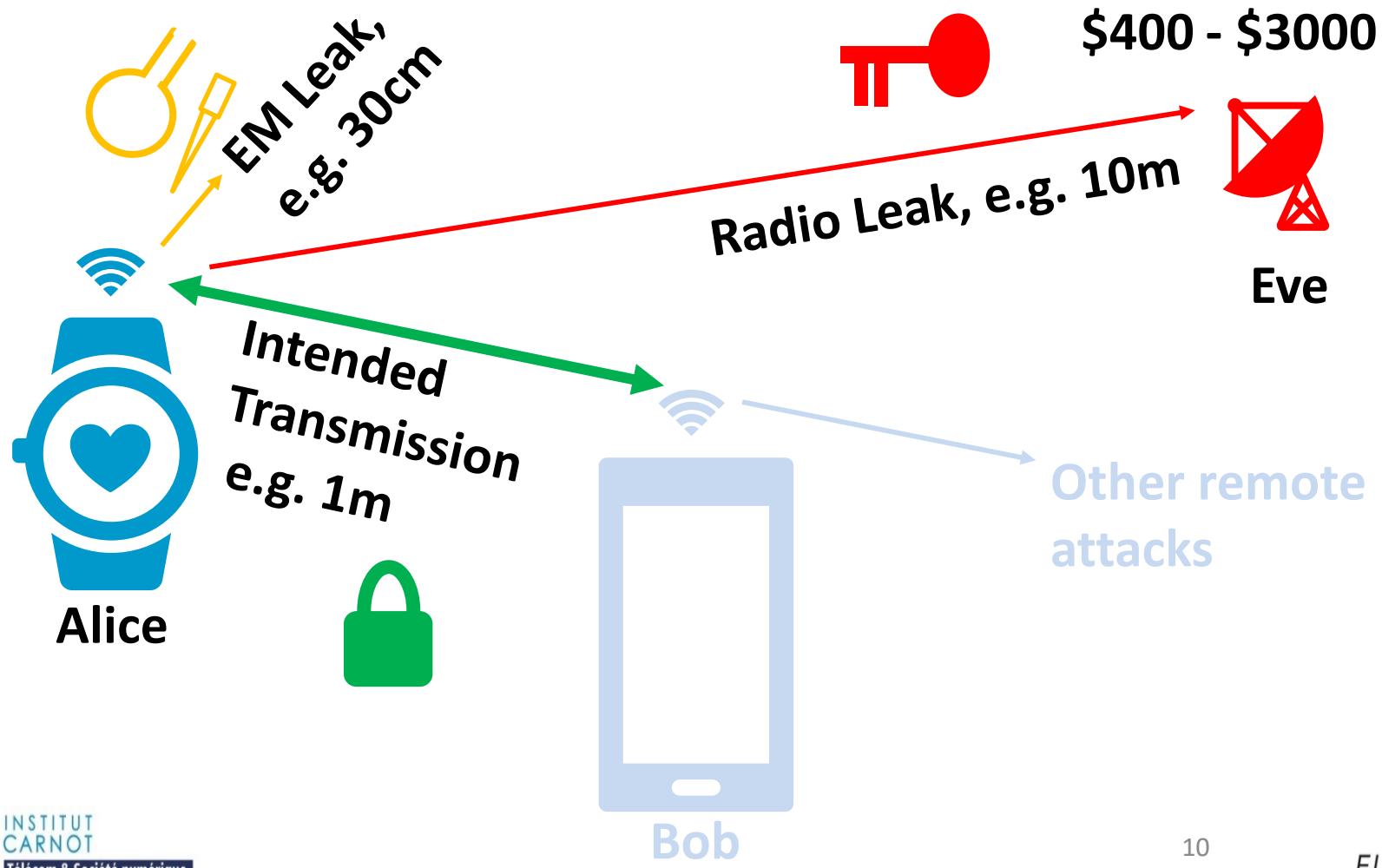
Screaming Channels: Leak Broadcast



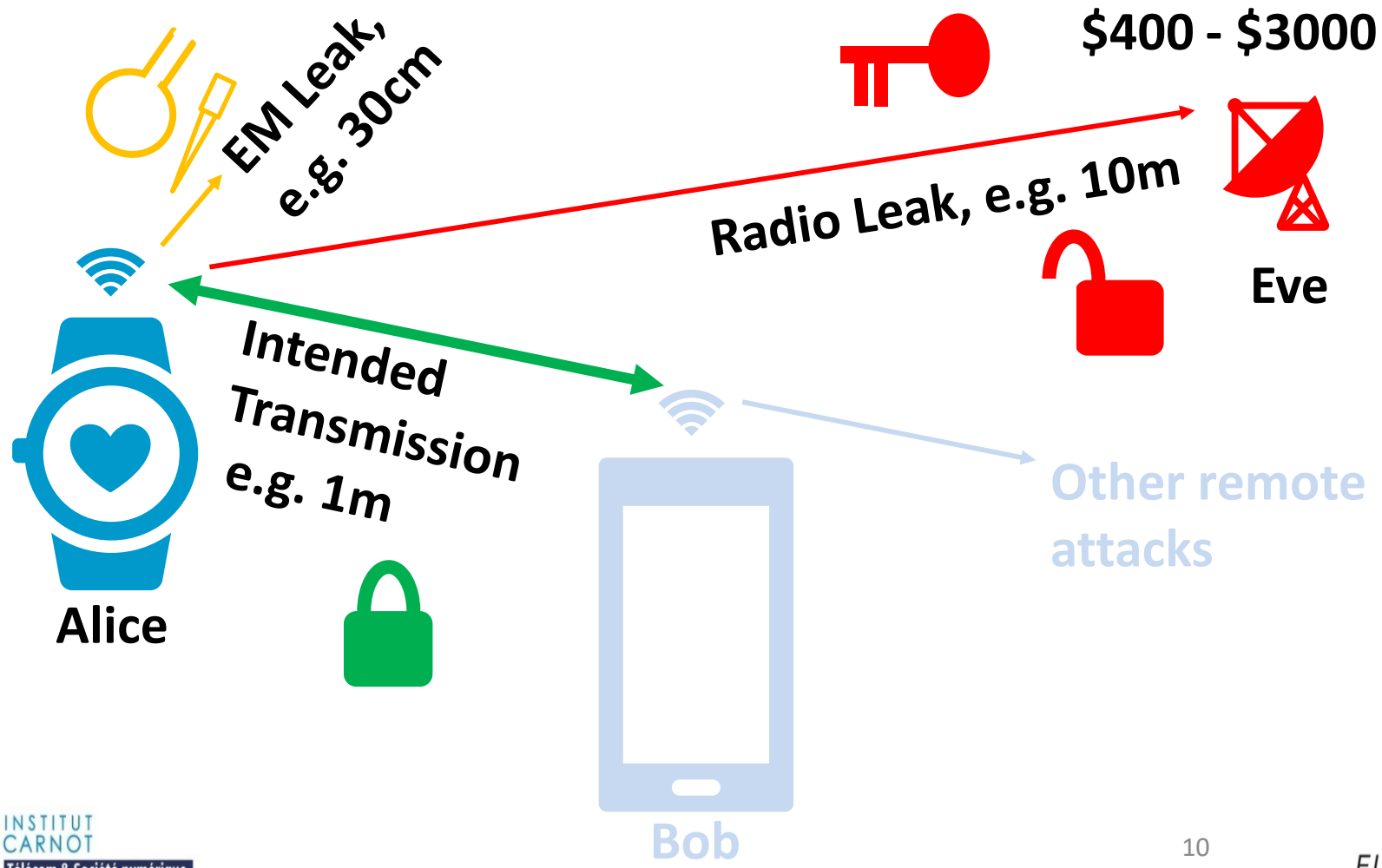
Screaming Channels: Leak Broadcast



Screaming Channels: Leak Broadcast

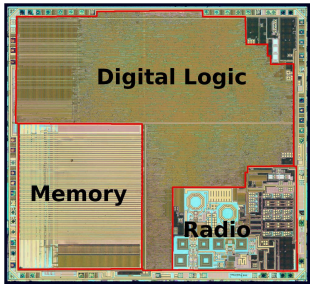


Screaming Channels: Leak Broadcast



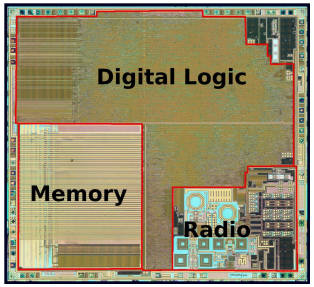
From digital noise to noise on the radio signal

Mixed-signal chips

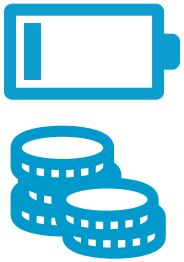


Idea:
CPU + Crypto + Radio
Same chip

Mixed-signal chips

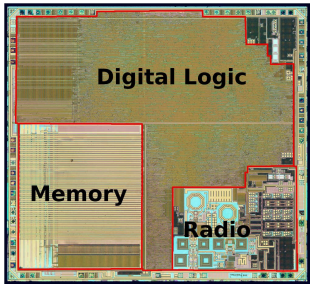


Idea:
CPU + Crypto + Radio
Same chip

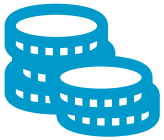


Benefits:
Low Power, Cheap, Small
Easy to integrate

Mixed-signal chips



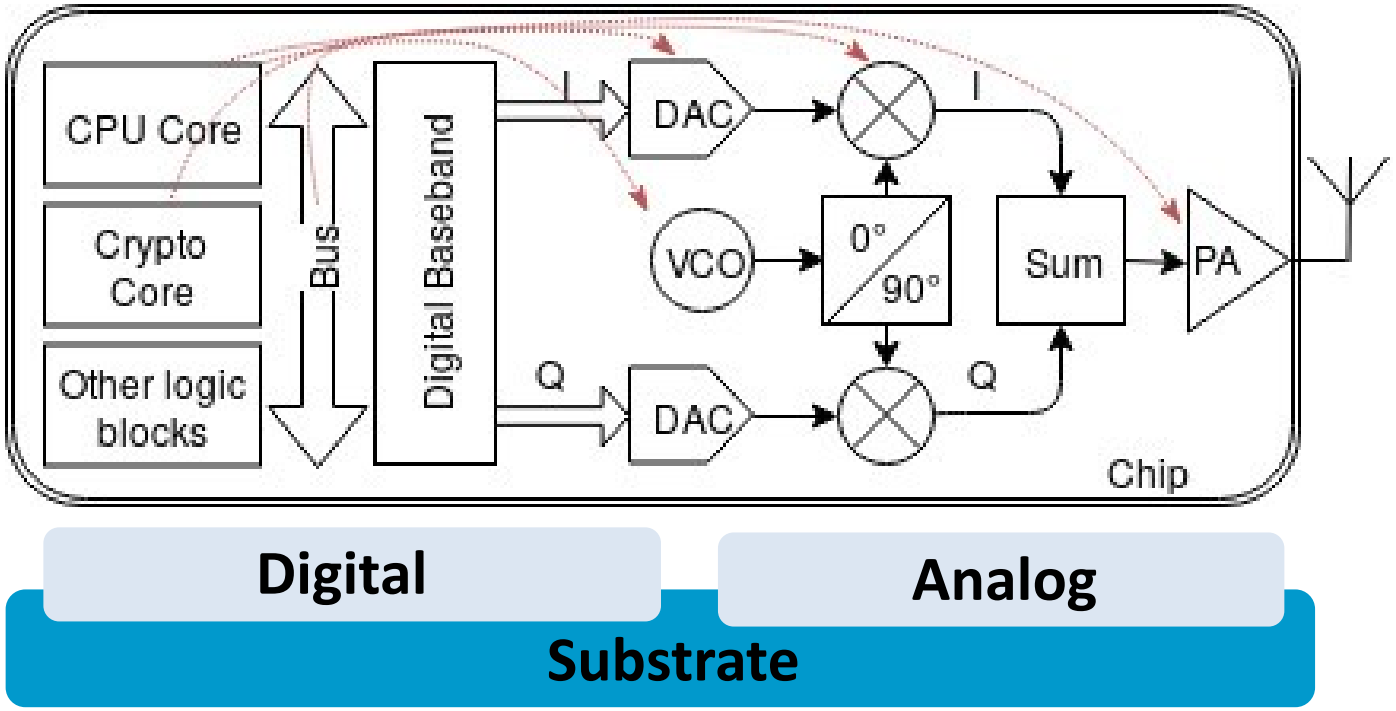
Idea:
CPU + Crypto + Radio
Same chip



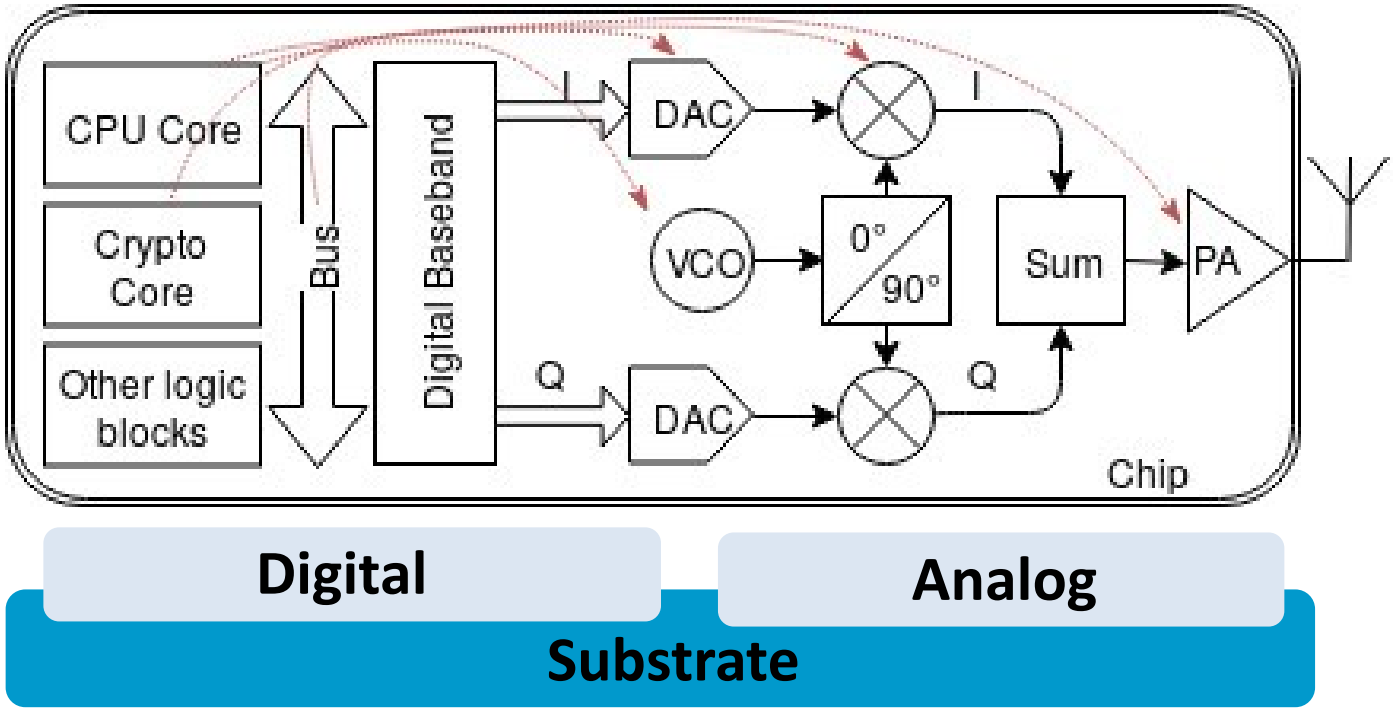
Benefits:
Low Power, Cheap, Small
Easy to integrate

Examples:
BT, BLE, WiFi, GPS, etc

Noise: Functionality vs. Side Channels

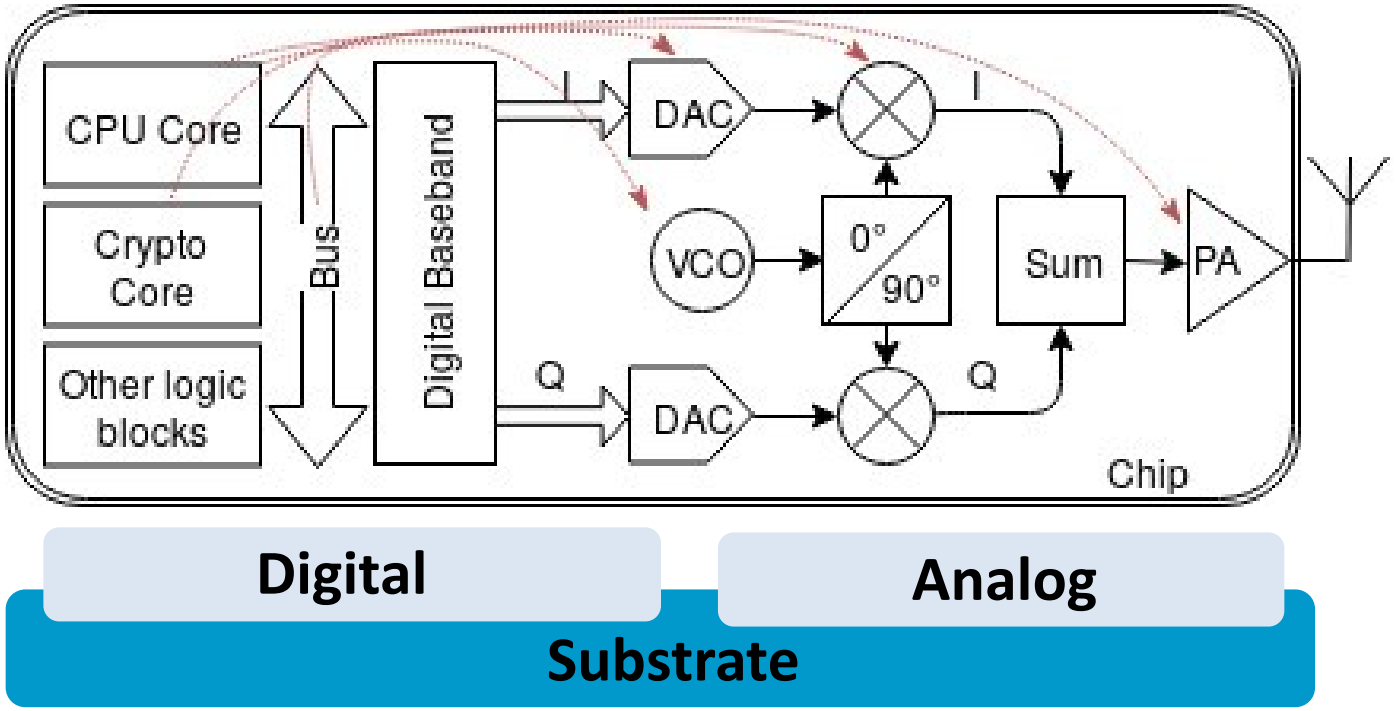


Noise: Functionality vs. Side Channels



Digital:
Inherently noisy

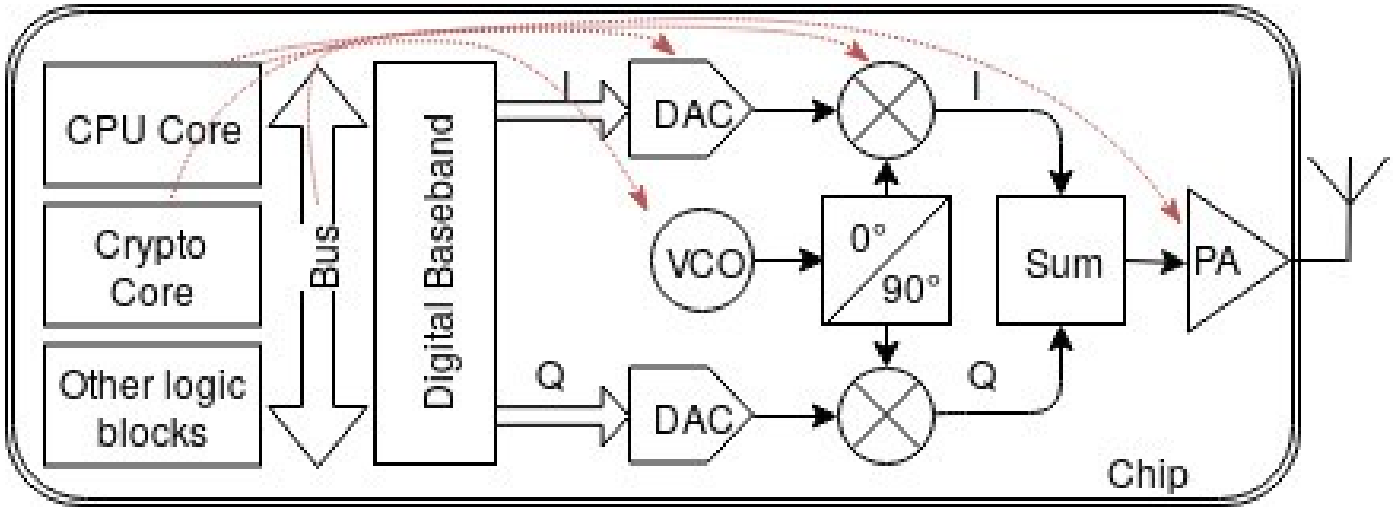
Noise: Functionality vs. Side Channels



Digital:
Inherently noisy

Propagation:
Substrate coupling
Power supply/Gnd

Noise: Functionality vs. Side Channels

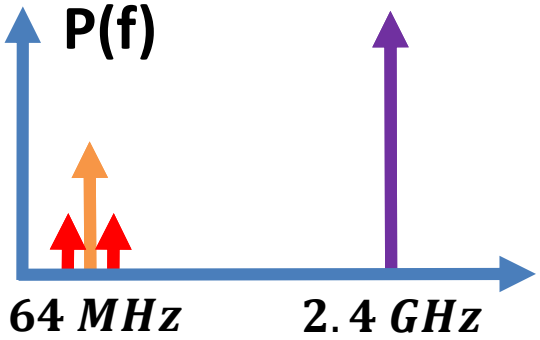


Digital:
Inherently noisy

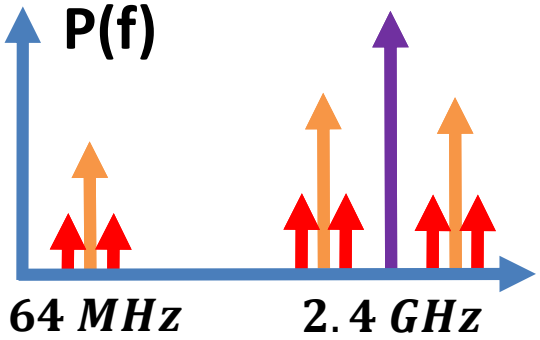
Propagation:
Substrate coupling
Power supply/Gnd

Analog:
Noise sensitive

Screaming Channels

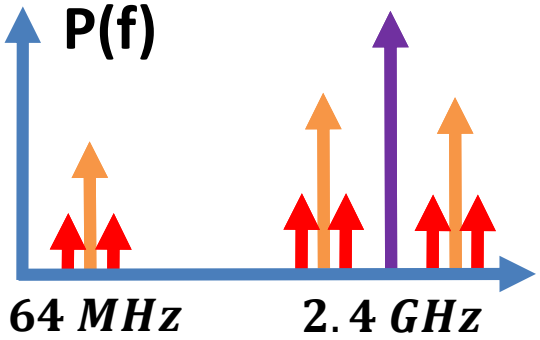


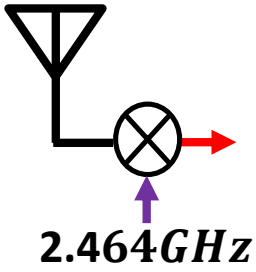
Screaming Channels



Upconverted and amplified leak

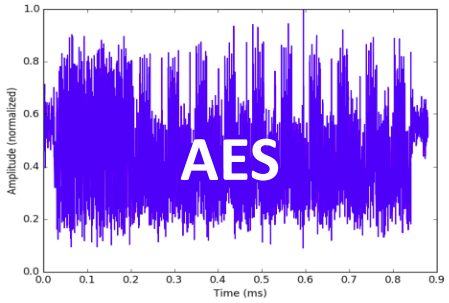
Screaming Channels





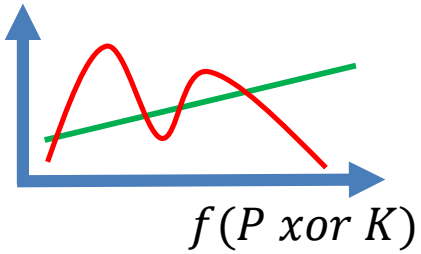
Upconverted and amplified leak

Screaming Channels



Retrieve traces

$AESLeak$



Attack

- **Correlation (Template) Radio Analysis, …**
- **Up to 2m – 10m**

Extraction

Impact on Radio Transmission

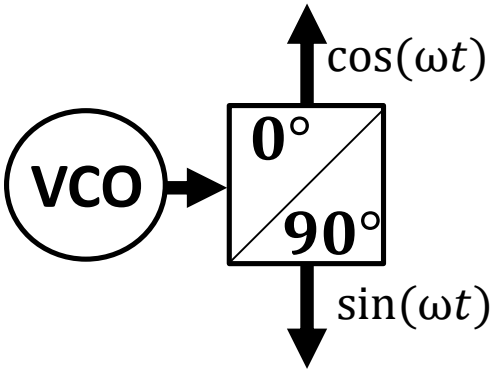
Impact on Radio Transmission

$$\mathrm{I} = A_k \cos(\varphi_k) \longrightarrow$$

$$\mathrm{Q} = A_k \sin(\varphi_k) \longrightarrow$$

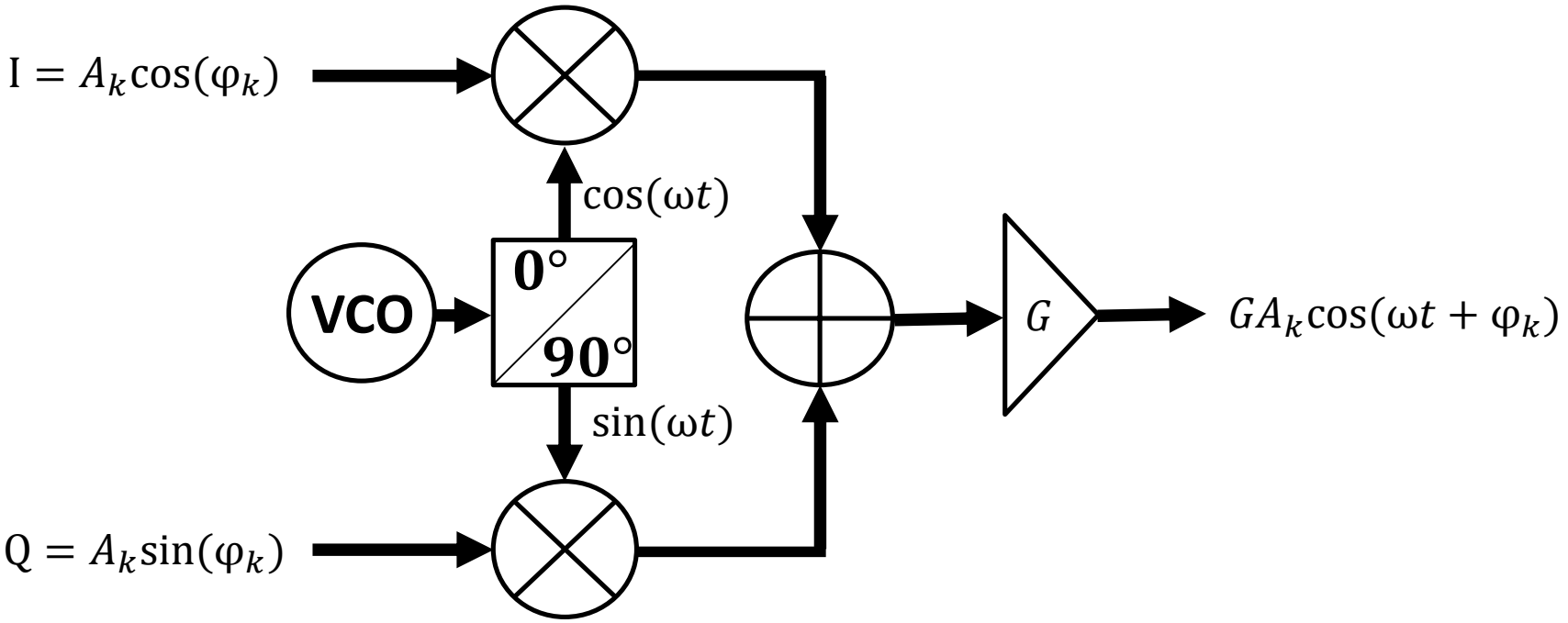
Impact on Radio Transmission

$\mathrm{I} = A_k \cos(\varphi_k)$ ⟶

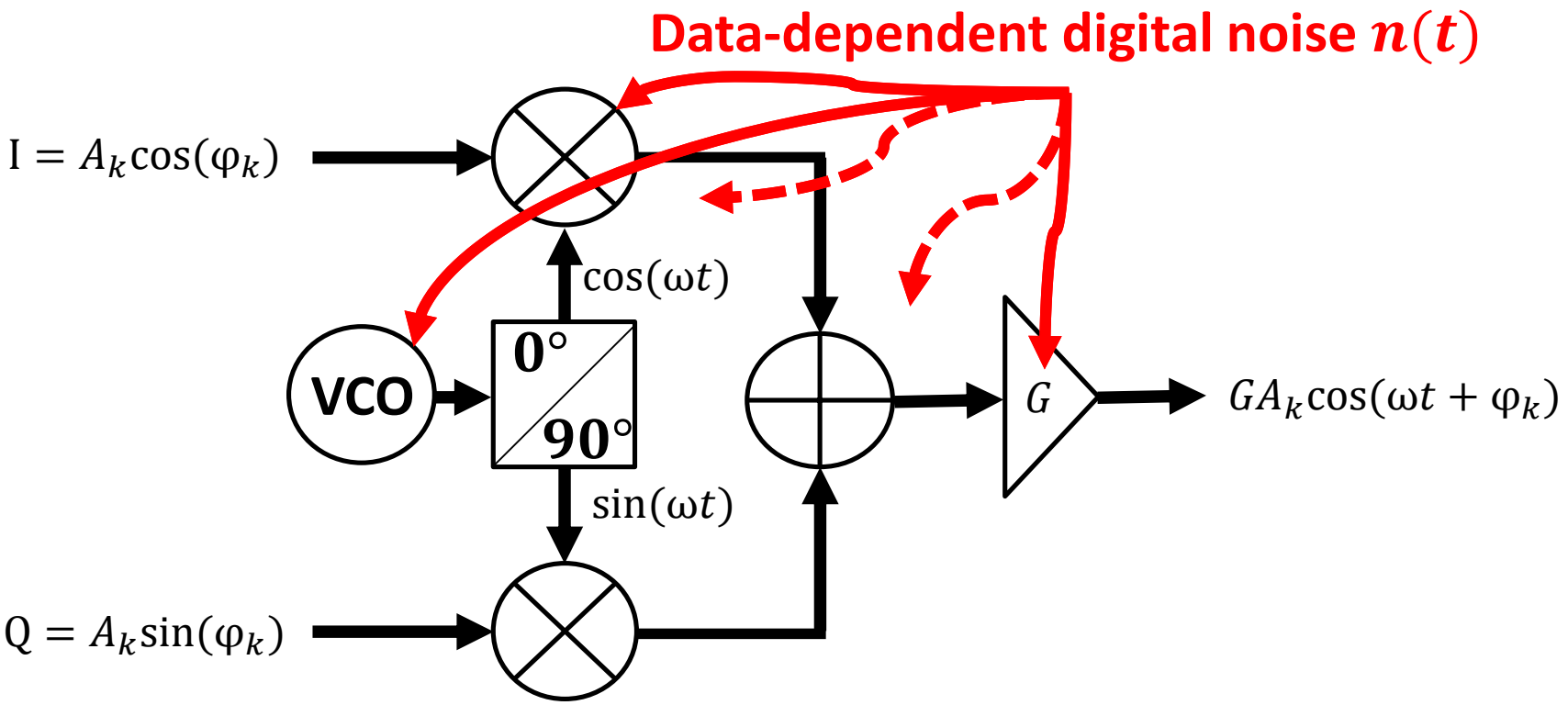


$\mathrm{Q} = A_k \sin(\varphi_k)$ ⟶

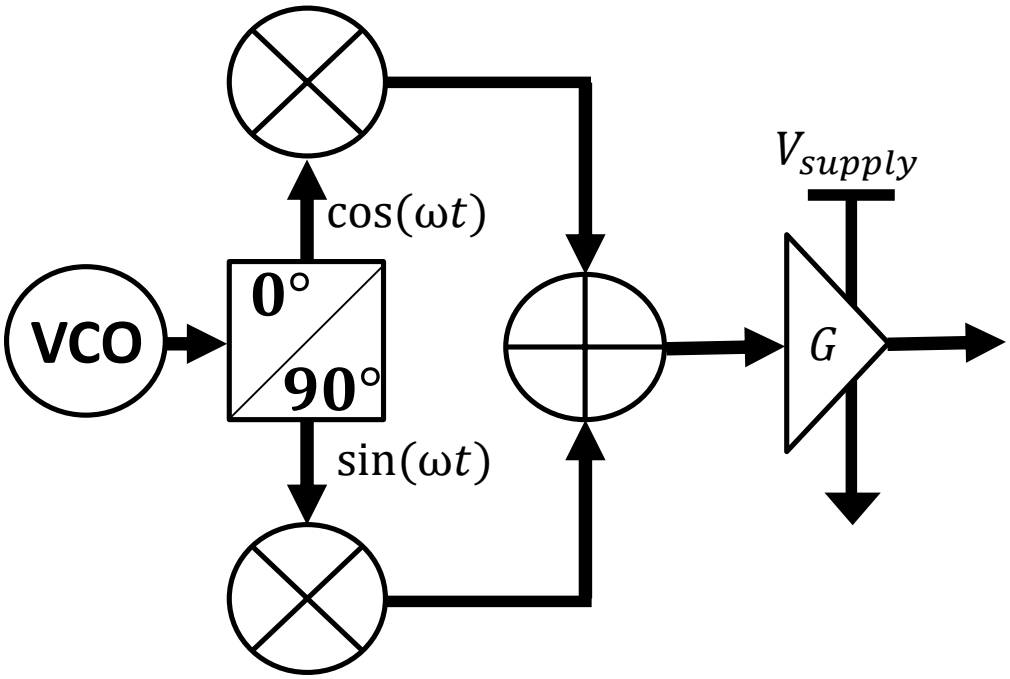
Impact on Radio Transmission



Impact on Radio Transmission

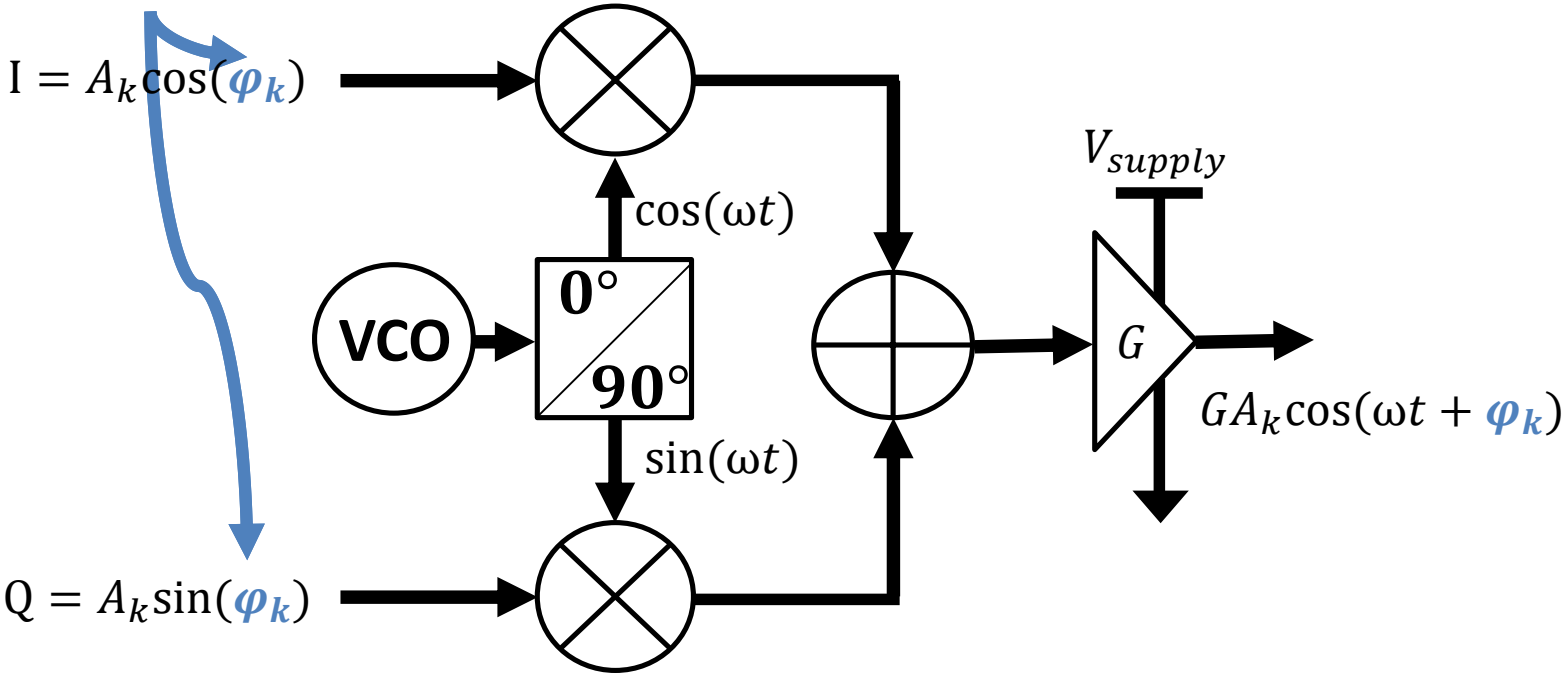


Example of Screaming Channel

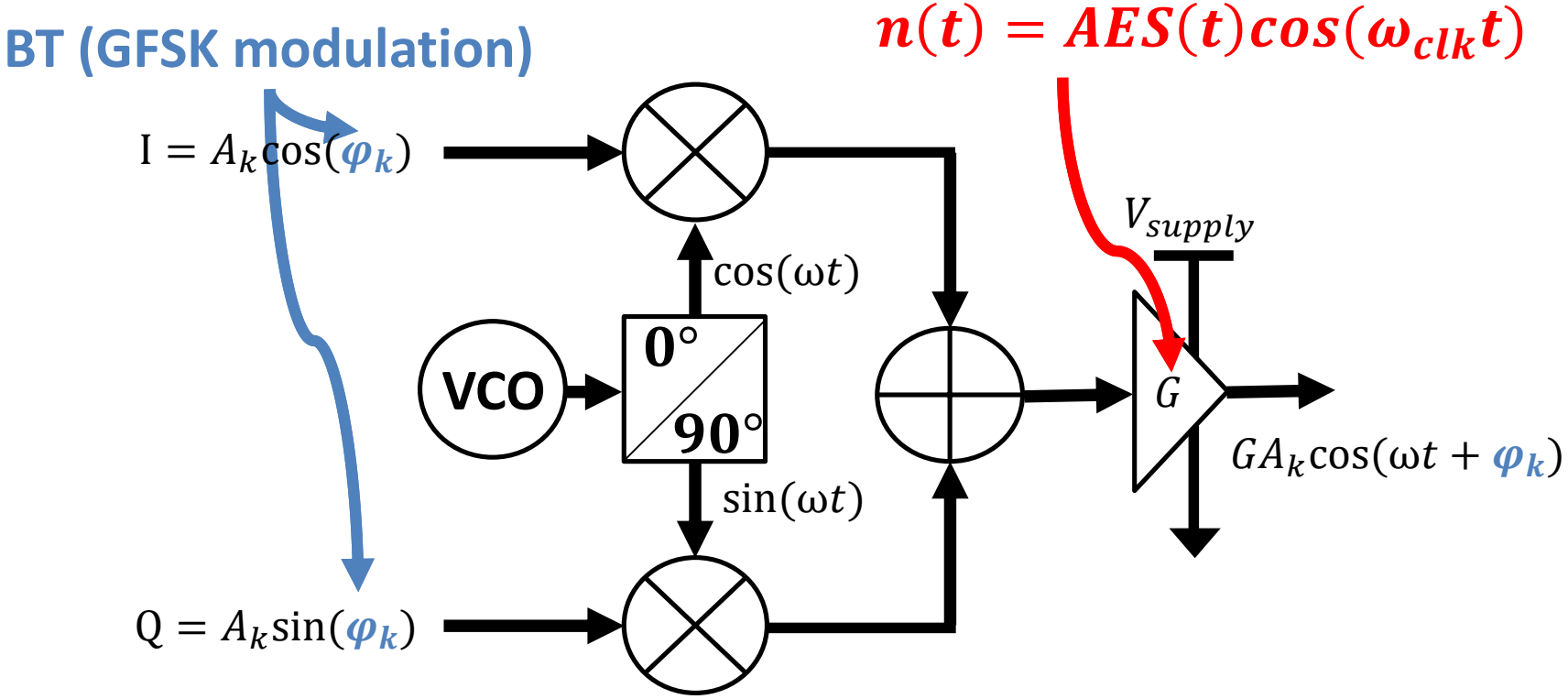


Example of Screaming Channel

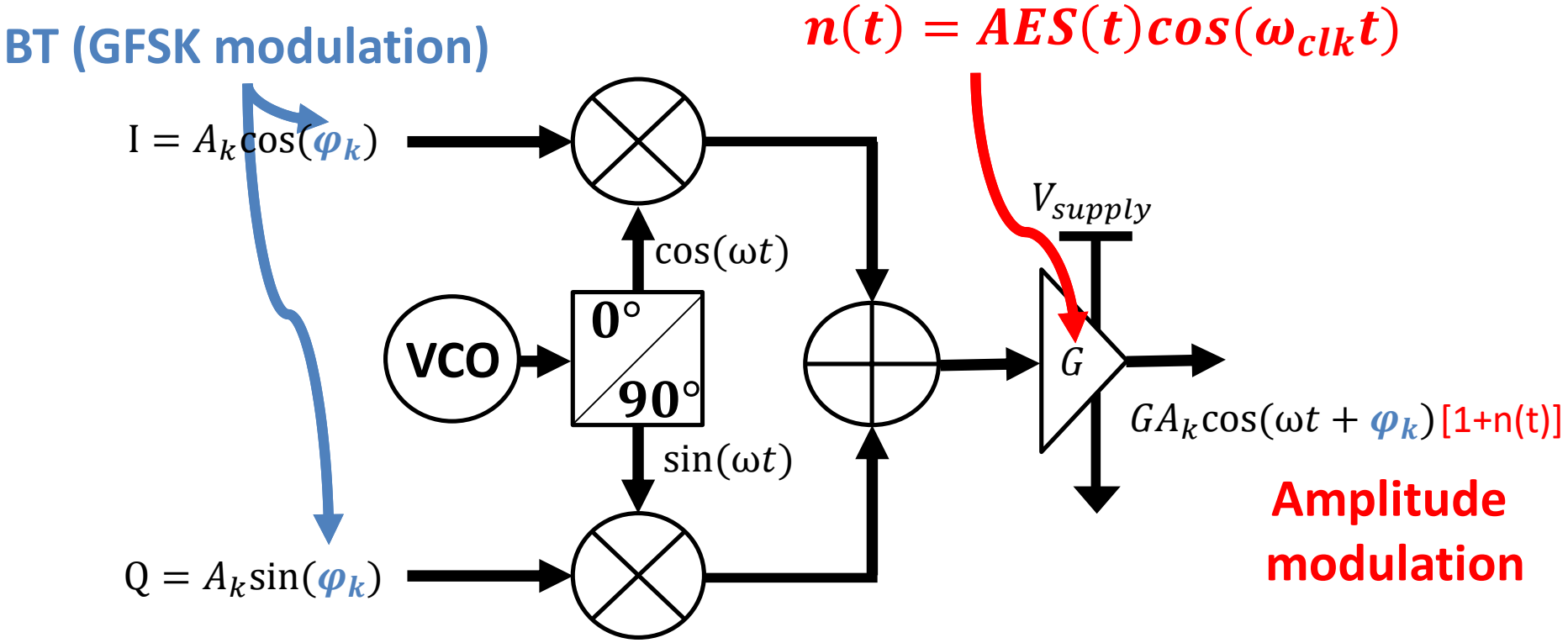
BT (GFSK modulation)



Example of Screaming Channel



Example of Screaming Channel

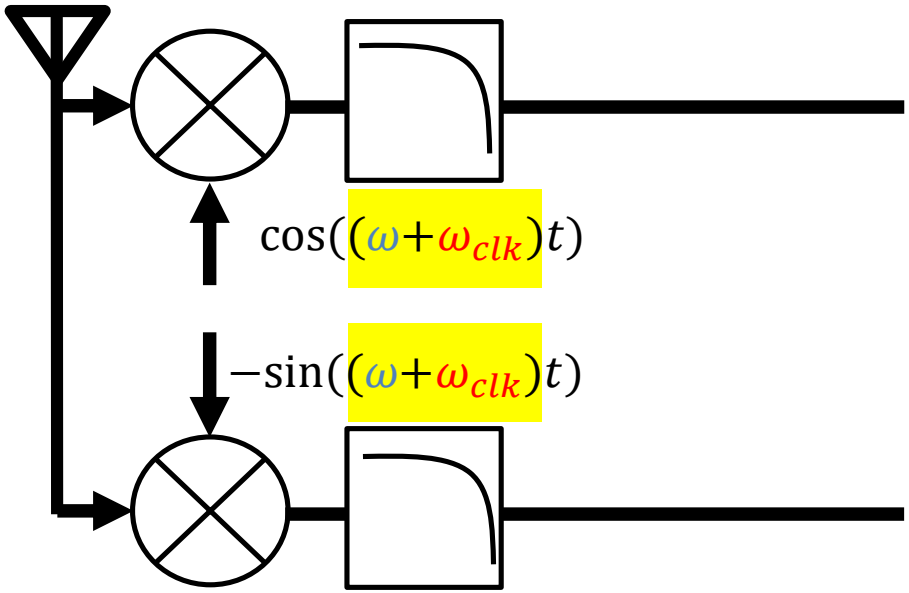


RX (quadrature ampl. demod.)

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

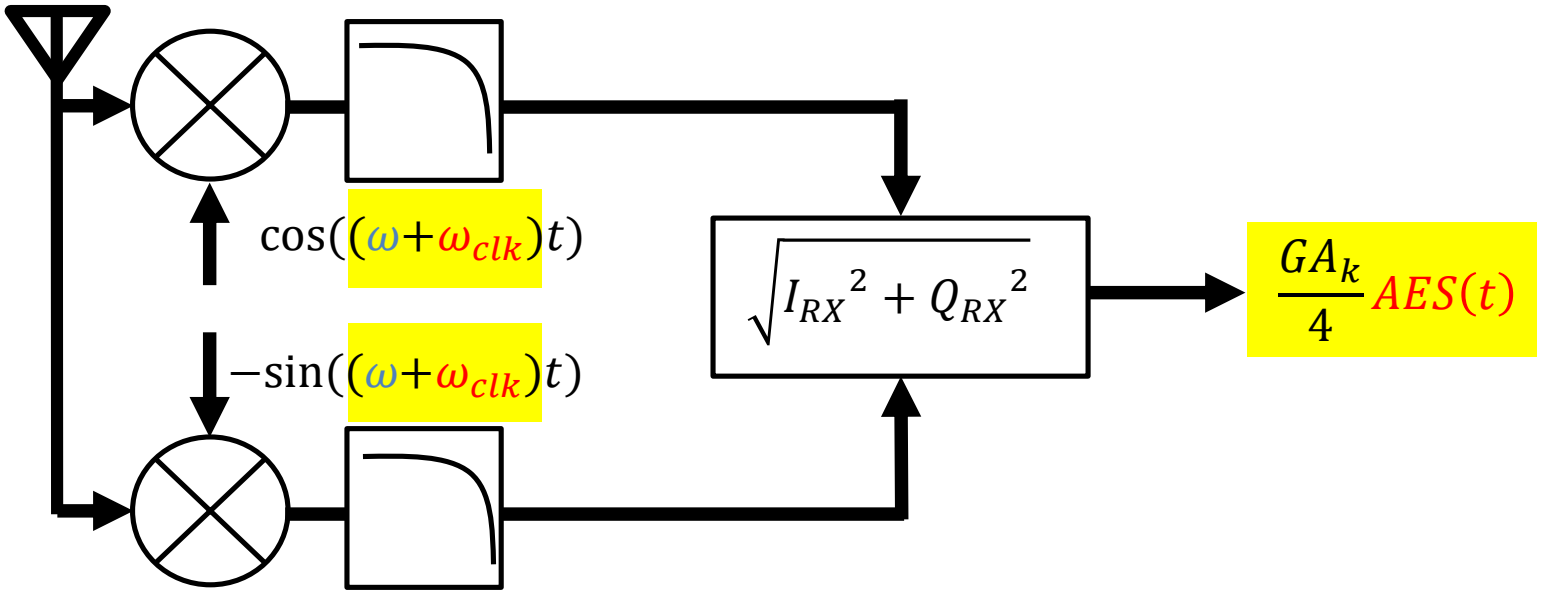
RX (quadrature ampl. demod.)

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

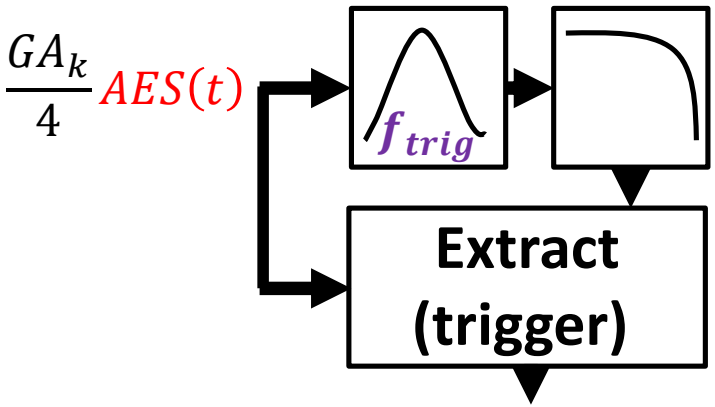


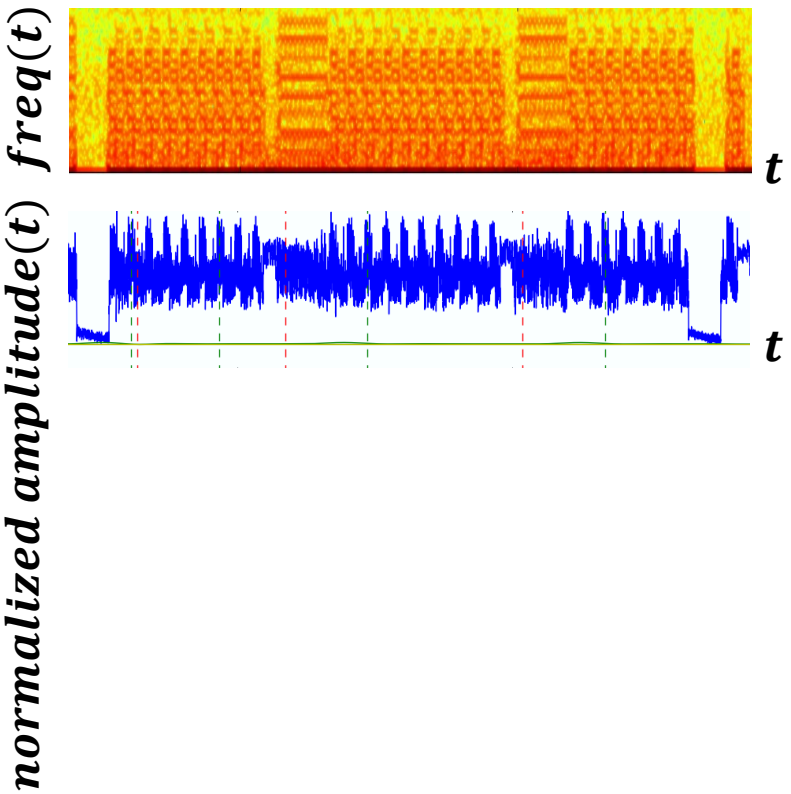
RX (quadrature ampl. demod.)

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

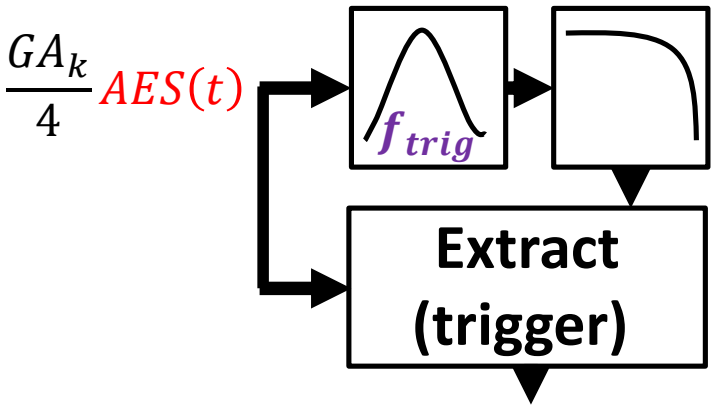


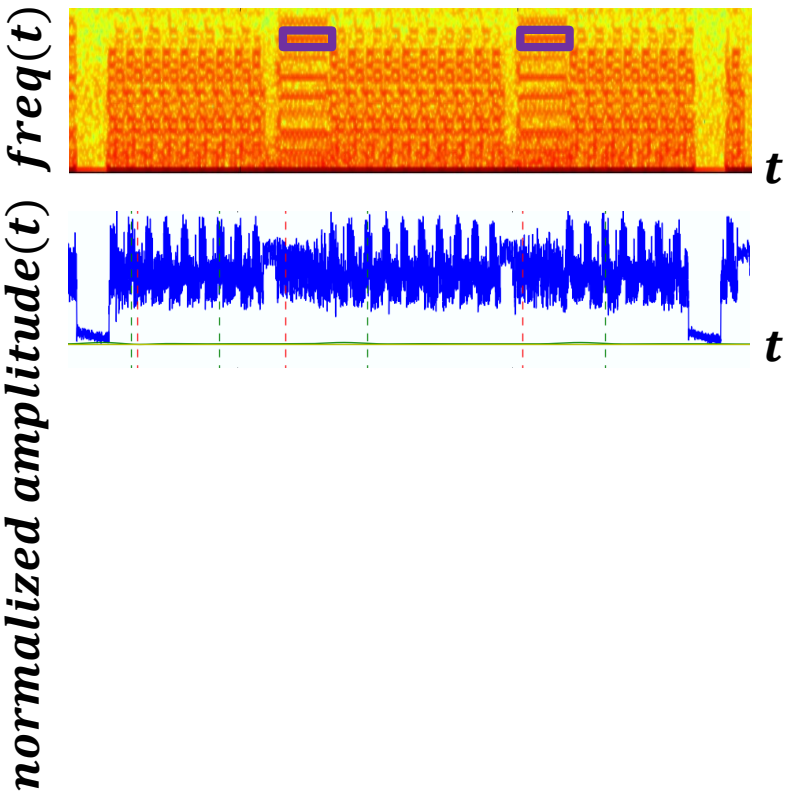
Extraction


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

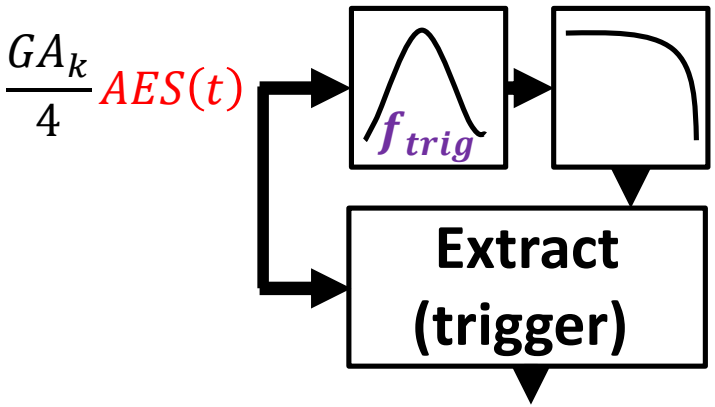

$freq(t)$
t
$normalized\ amplitude(t)$
t

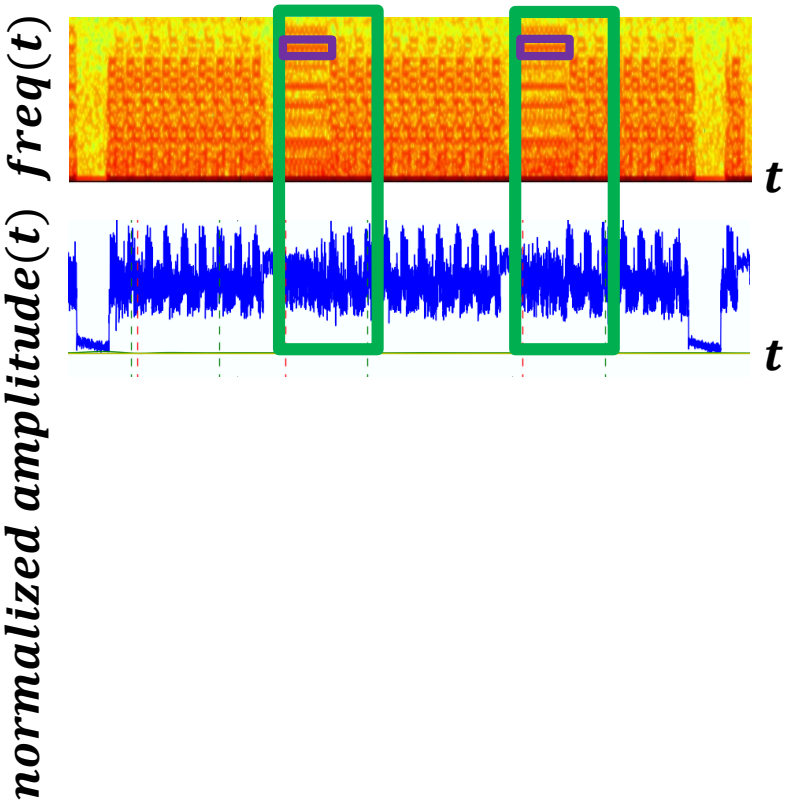
Extraction


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

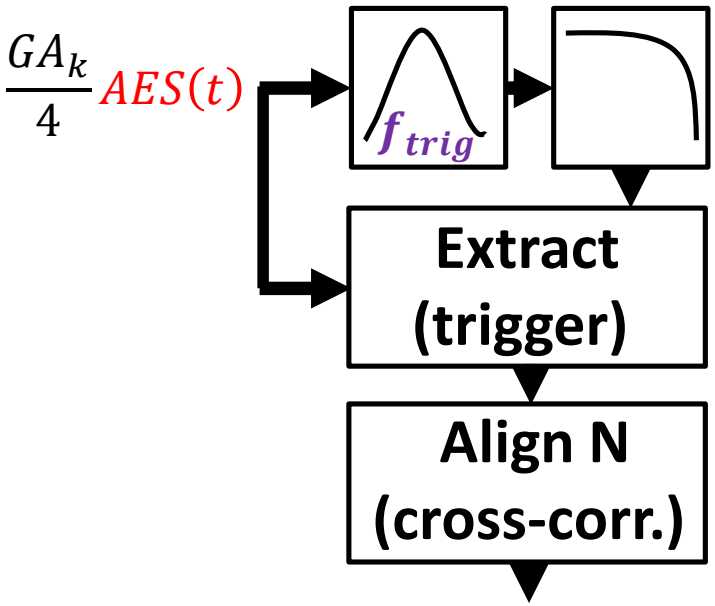

$freq(t)$
t
$normalized\ amplitude(t)$
t

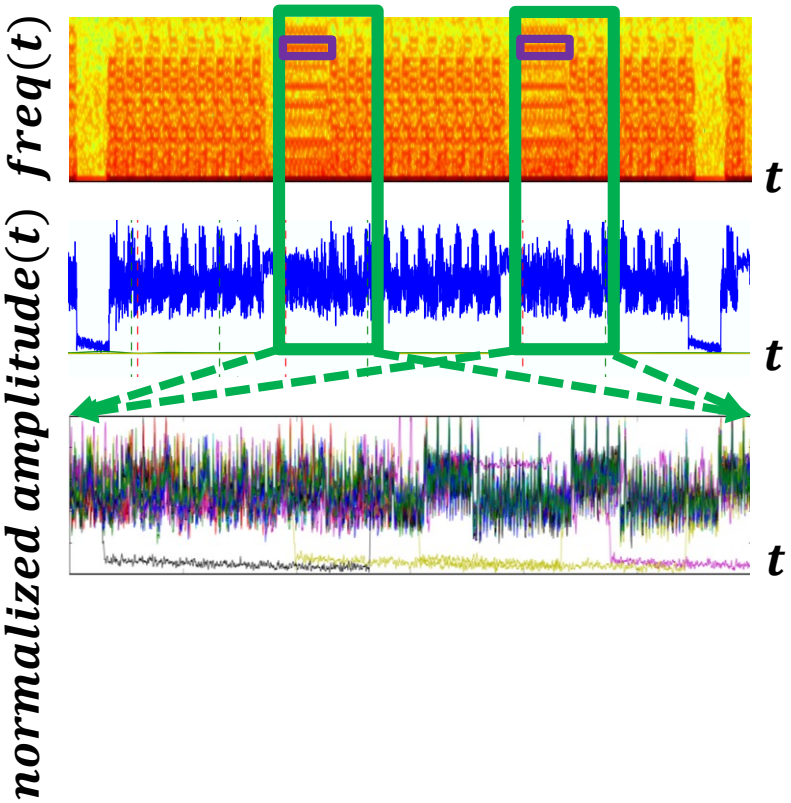
Extraction


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

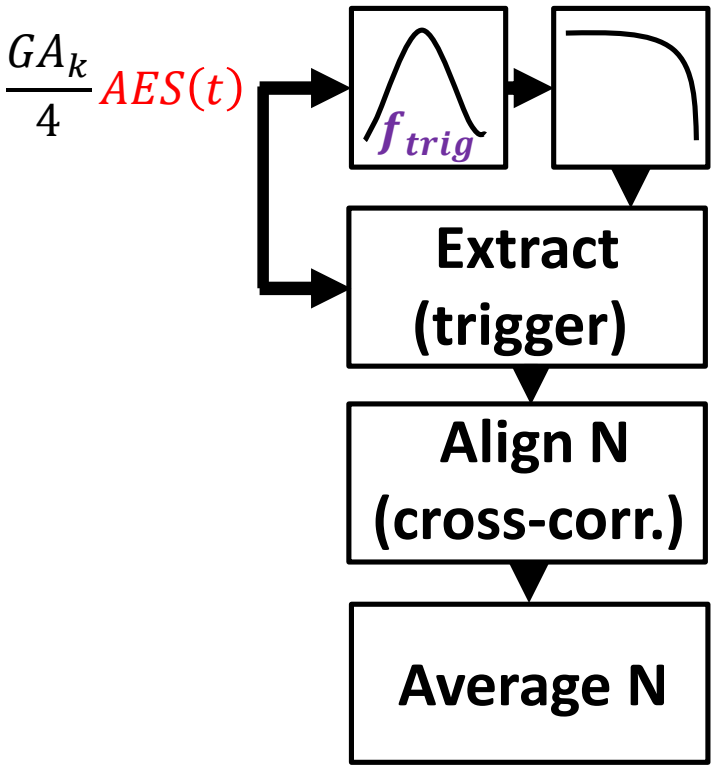

$freq(t)$
t
$normalized\ amplitude(t)$
t

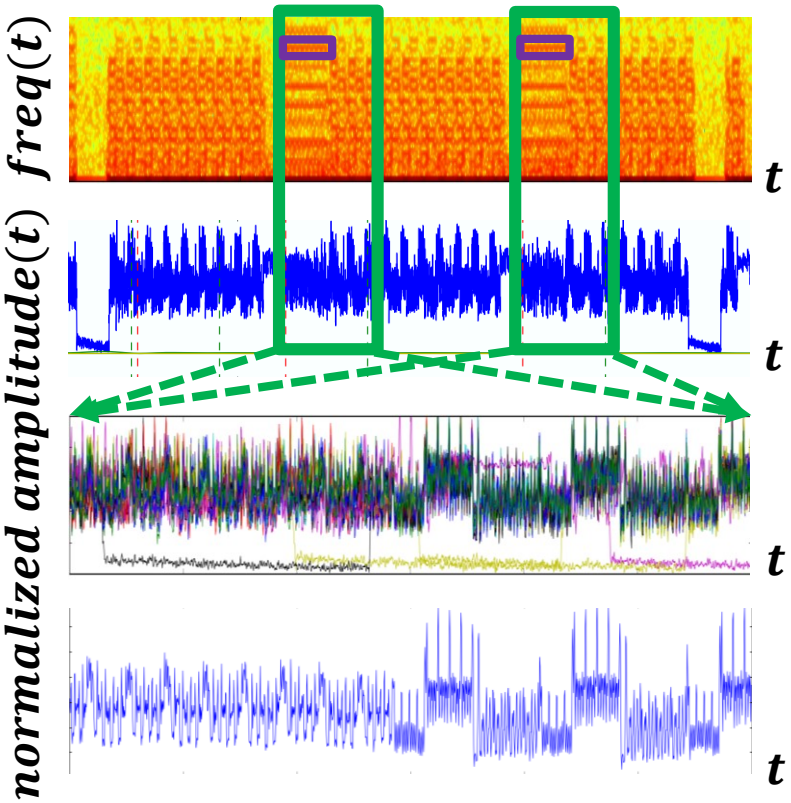
Extraction


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


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

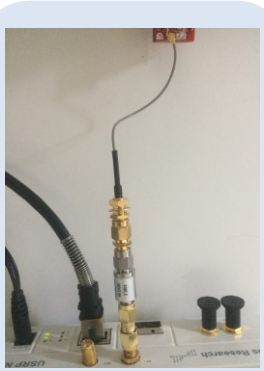
Extraction:
Automated via radio
Known plaintext

Attacks:
Correlation, Template
Code based on ChipWhisperer

Much more advanced attacks exist

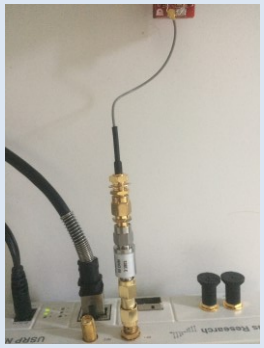
Evolution of the attack

Evolution of the attack

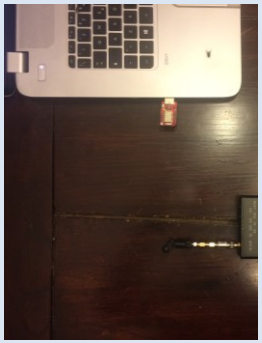


Cable

Evolution of the attack

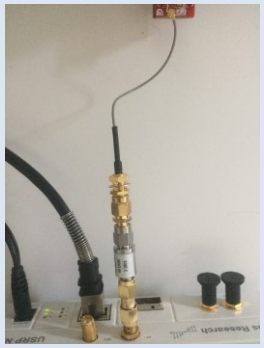


$\boldsymbol{Cable}$

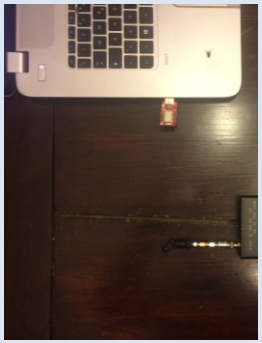


$\boldsymbol{15\ cm}$

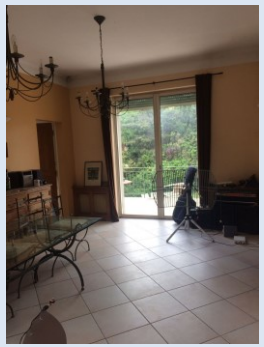
Evolution of the attack



$\boldsymbol{Cable}$

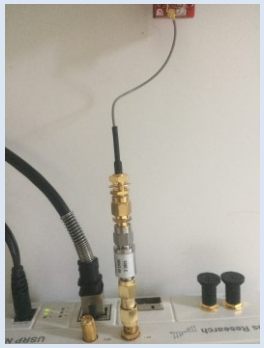


$\boldsymbol{15\ cm}$

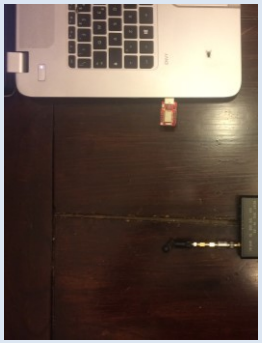


$\boldsymbol{2\ m}$

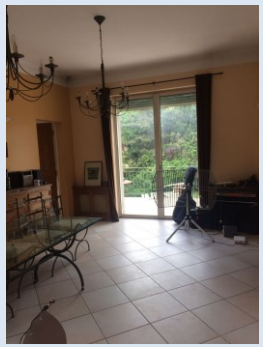
Evolution of the attack



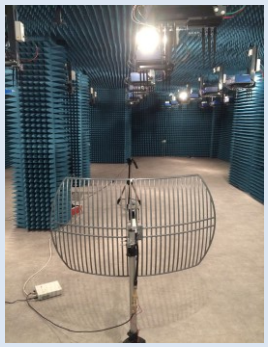
$\boldsymbol{Cable}$



$\boldsymbol{15\ cm}$

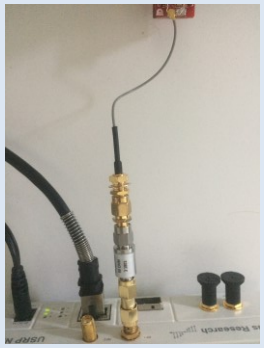


$\boldsymbol{2\ m}$

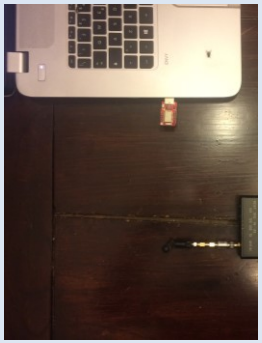


$\boldsymbol{3\ m}$

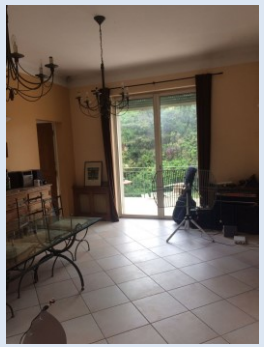
Evolution of the attack



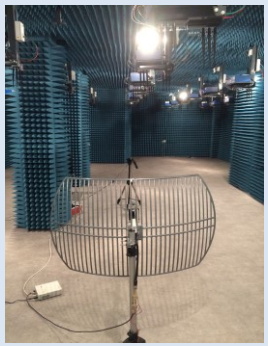
$Cable$



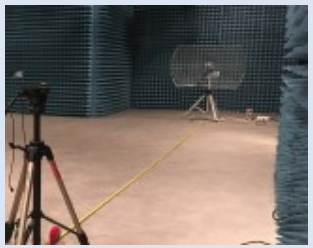
$15\ cm$



$2\ m$

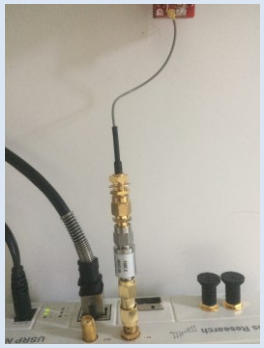


$3\ m$

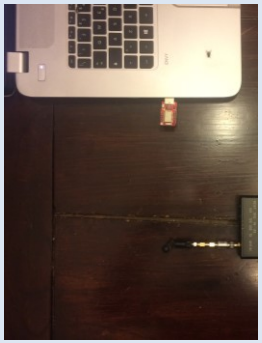


$5\ m$

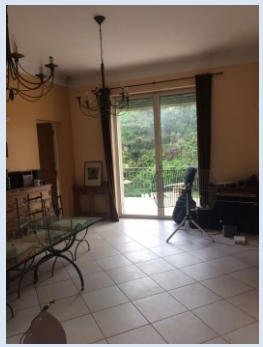
Evolution of the attack



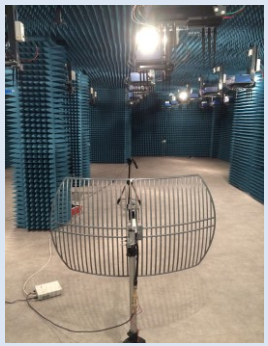
$Cable$



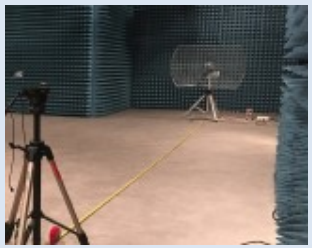
$15\ cm$



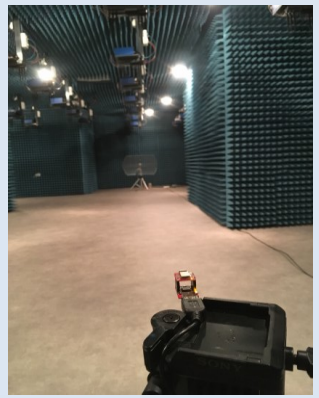
$2\ m$



$3\ m$



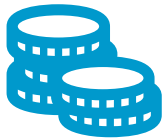
$5\ m$



$10\ m$

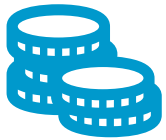
Protection

Countermeasures



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

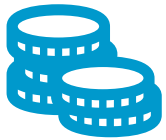
Countermeasures



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

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

Countermeasures

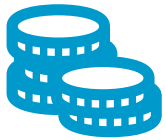


Resource constraint devices:
Cost, power, time to market,
etc.

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

d. (Ⓒ) [Six lines redacted.]

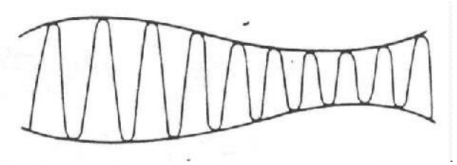


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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

d. (Ⓒ) [Six lines redacted.]

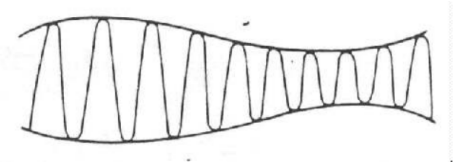


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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

d. (U) [Six lines redacted.]

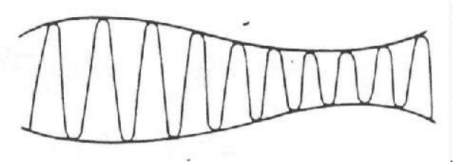


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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

d. (Ⓒ) [Six lines redacted.]

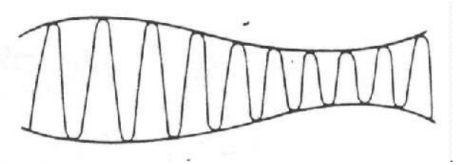


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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

d. (Ⓒ) [Six lines redacted.]

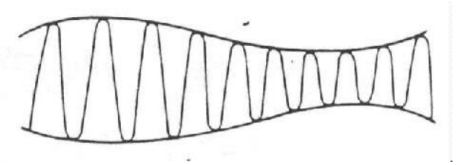


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

e. (Ⓒ) 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

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

Backup slides

Which devices?

- We do not want to blame a specific vendor
  - Especially because the problem is general
  - But you can find all names and details in the paper and on our website
- The problem is general
  - Ack by vendors
  - Attack on several BLE devices of the same vendor
  - Signs of leaks on other (Wi-Fi) devices
  - Also different types of leaks
  - Still need more investigations (time…)

What about hopping?

- Real BT communications use frequency hopping
  - The carrier changes values (in a given set) following a pseudo-random sequence
  - The frequency of the leak changes too
- We can still attack
  - We can listen to multiple frequencies, or with a large bandwidth
  - Actually, we already plan to exploit more replicas of the leak
  - Tom Hayes, Sebastian Poeplau, and Aurélien Francillon worked on an IEEE 802.15.4 sniffer that concurrently listens to all channels, we could reuse the same ideas

What about Wi-Fi?

- The problem is in the mixed-signal design, not in the protocol
- We ended up on a BT chip by chance, and then decided to go deeper (increasing the distance)
- We have signs of (different) leaks in 2 Wi-Fi chips
- But for sure now we have to try more chips

What about Hardware AES?

- 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

Threat model?

- For these devices, side channels were not in the threat model
  - Close physical proximity/access not too realistic
  - Low cost, low impact
- But now attacks could be mounted from a large distance
  - EM side channels become important
  - Indeed remote timing side channels (cache) are already considered

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

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