black hat®

USA 2018

AUGUST 4-9, 2018

MANDALAY BAY / LAS VEGAS

#BHUSA / @BLACK HAT EVENTS

Screaming Channels

When Electromagnetic Side Channels Meet Radio Transceivers

Giovanni Camurati, Sebastian Poeplau, Marius Muench,

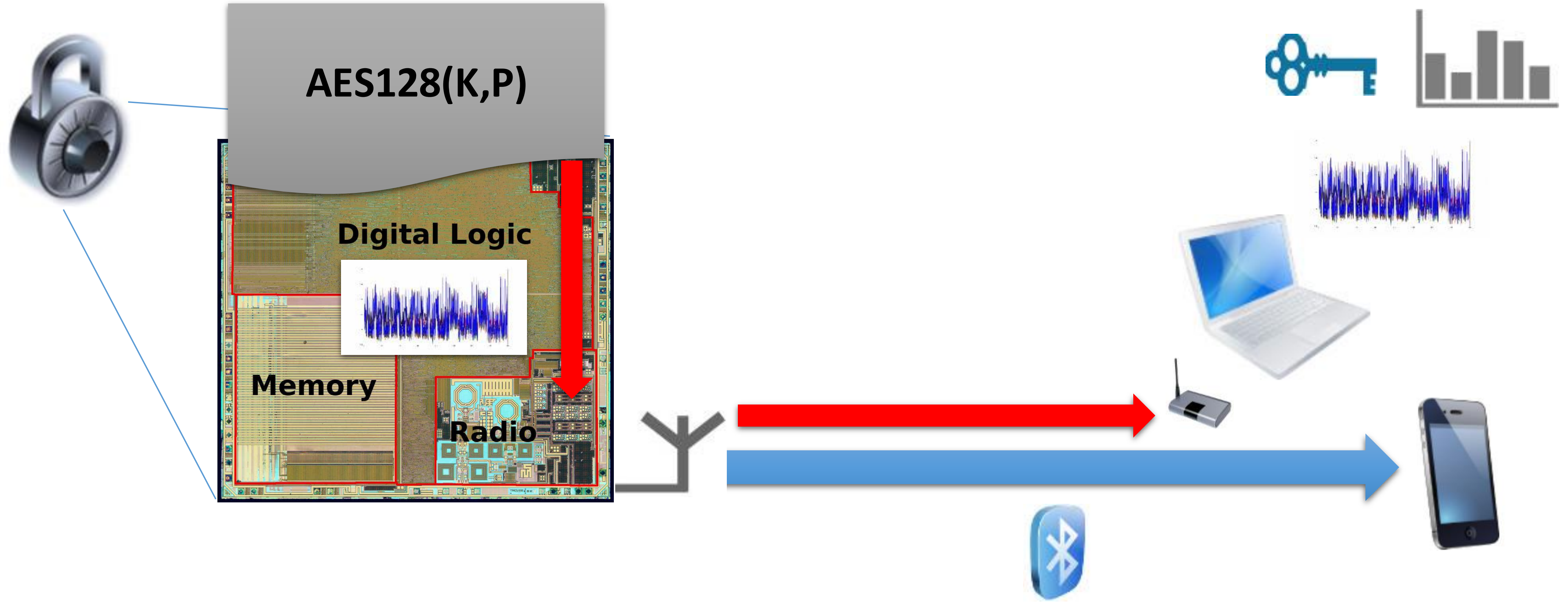
Tom Hayes, Aurélien Francillon

What’s this all about?

- A novel attack exploiting EM side channels from a distance
- A PoC implementation up to 10m distance (with demo!)
- Where to go from here?

Let’s start from the beginning

Leaks in radio signals



Agenda

From the state of the art to a novel attack

Agenda

Introduction		
Part I	Part II	Part III
Background - EM Side-Channels - RF communications 101 - Noise in mixed-signal ICs	*Our Story* - Discovery of the leak - Explanation	*Towards an attack* - Building the attack - Demo
Conclusion		

Agenda

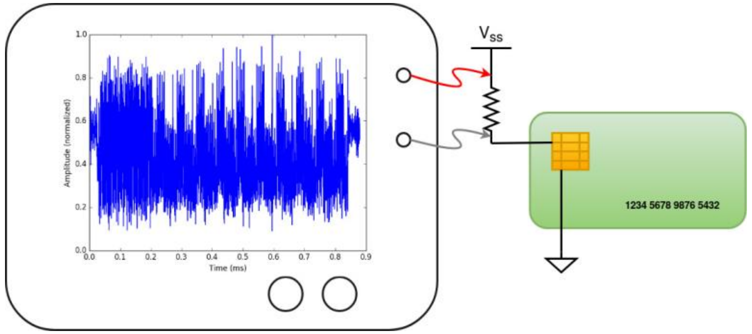
Introduction

Part I	Part II	Part III
Background	*Our Story*	*Towards an attack*
- EM Side-Channels	- Discovery of the leak	- Building the attack
- RF communications 101	- Explanation	- Demo
- Noise in mixed-signal ICs		

Conclusion

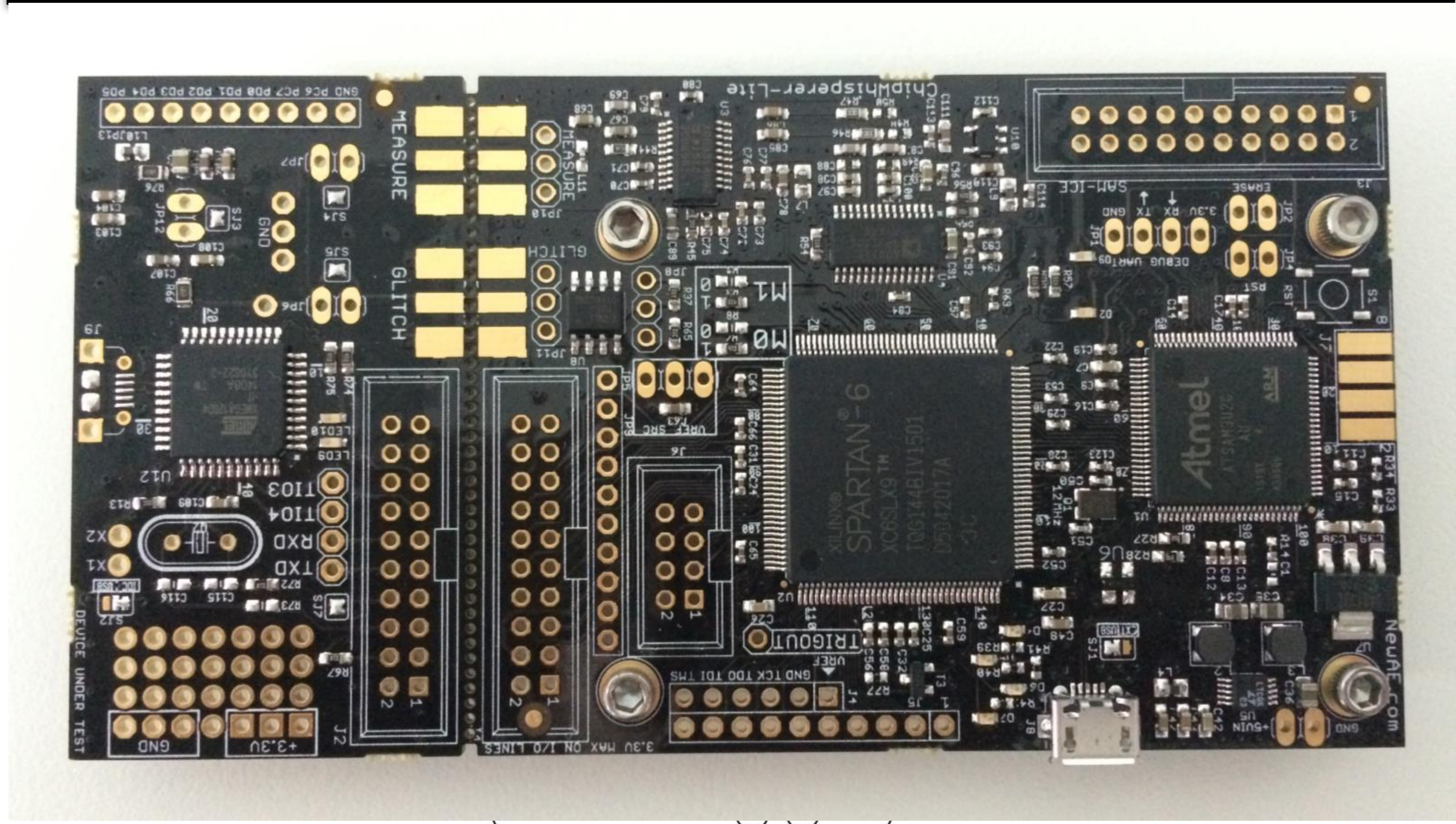
Side channel basics

- Even provably secure cryptography may be broken if some intermediate computations are visible
- Physical implementations may leak intermediate data
- Attackers observe the leaks and reconstruct cryptographic secrets



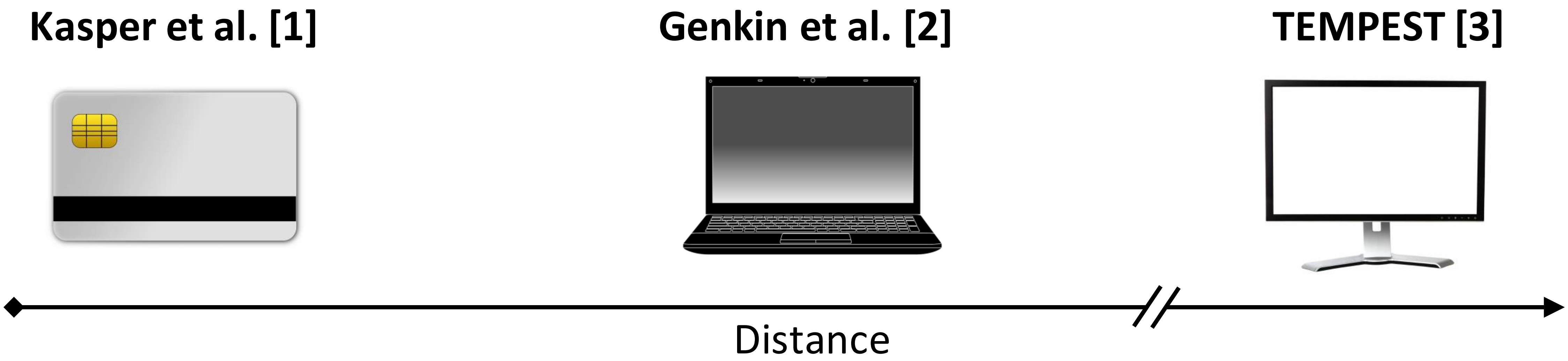
Side channel basics

ChipWhisperer!



Electromagnetic Side-Channels

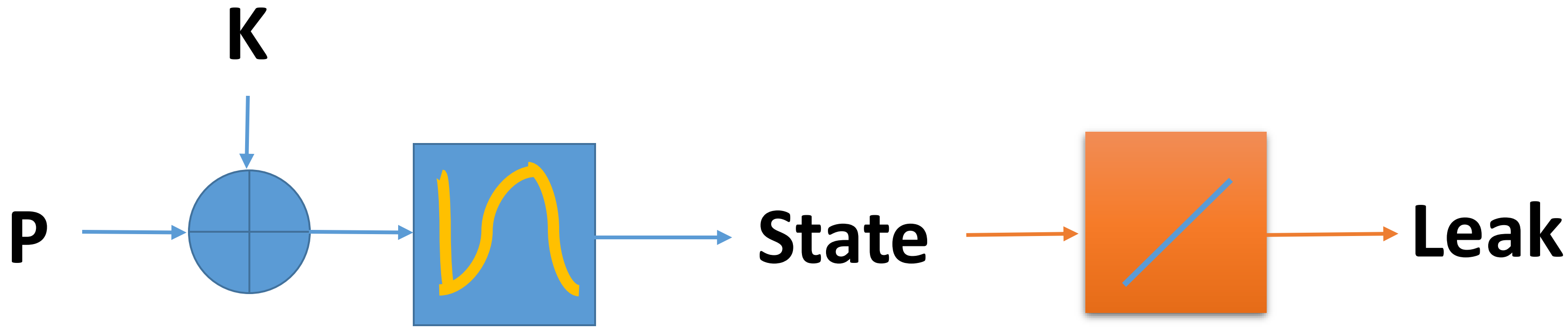
- Data-dependent EM leaks occur because:
  - Digital logic consumes current when switching
  - Current variations generate EM emissions
  - Similar to power side-channels
- Known attacks:



Correlation attack basics

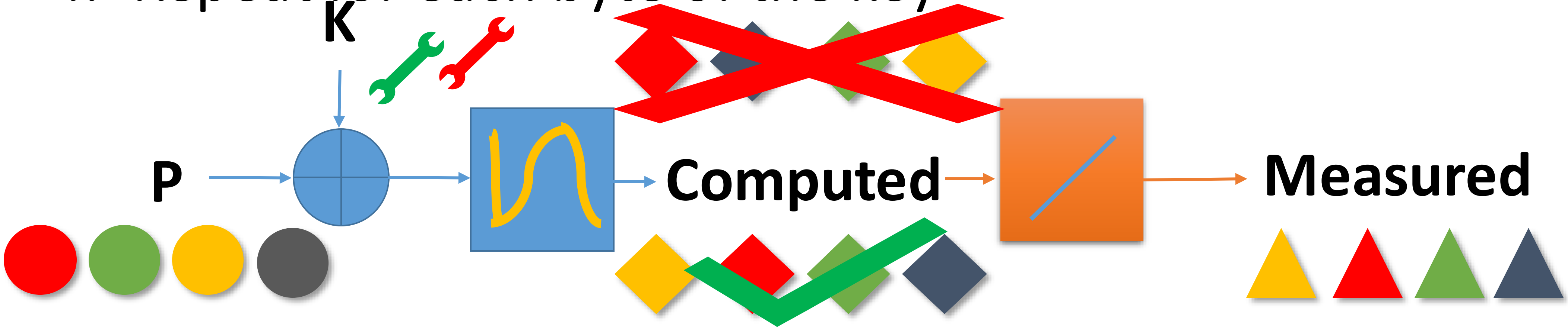
- An intuitive attack, there are many more
- Ingredients:
  - Known Plaintext
  - State non-linear in Plaintext and Key
  - Leak linear in the State

Leak model



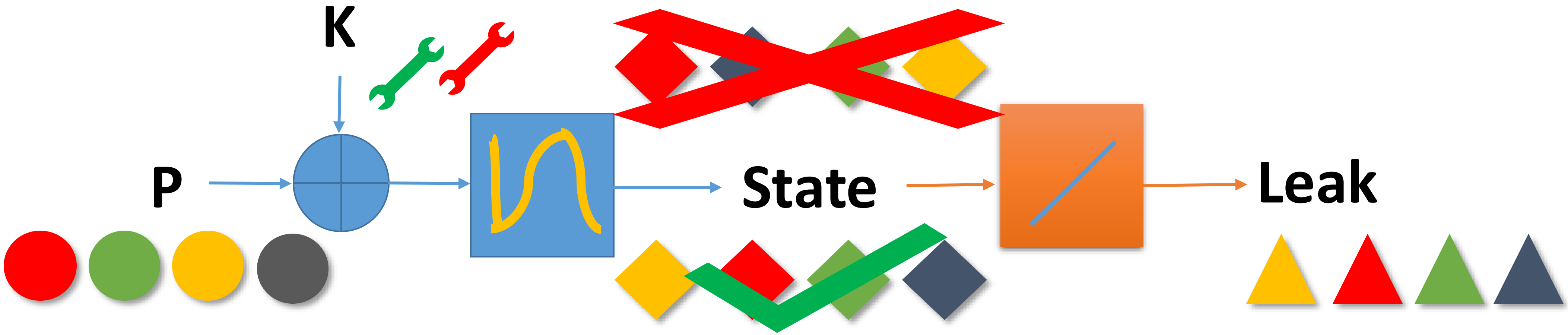
Correlation attack basics

- Recipe:
  1. Encrypt many times and measure the Leaks
  2. Guess a byte of the Key and compute the States
  3. Check if the **Measurements** correlate with the **Computations**
  4. Repeat for each byte of the key



Correlation attack basics

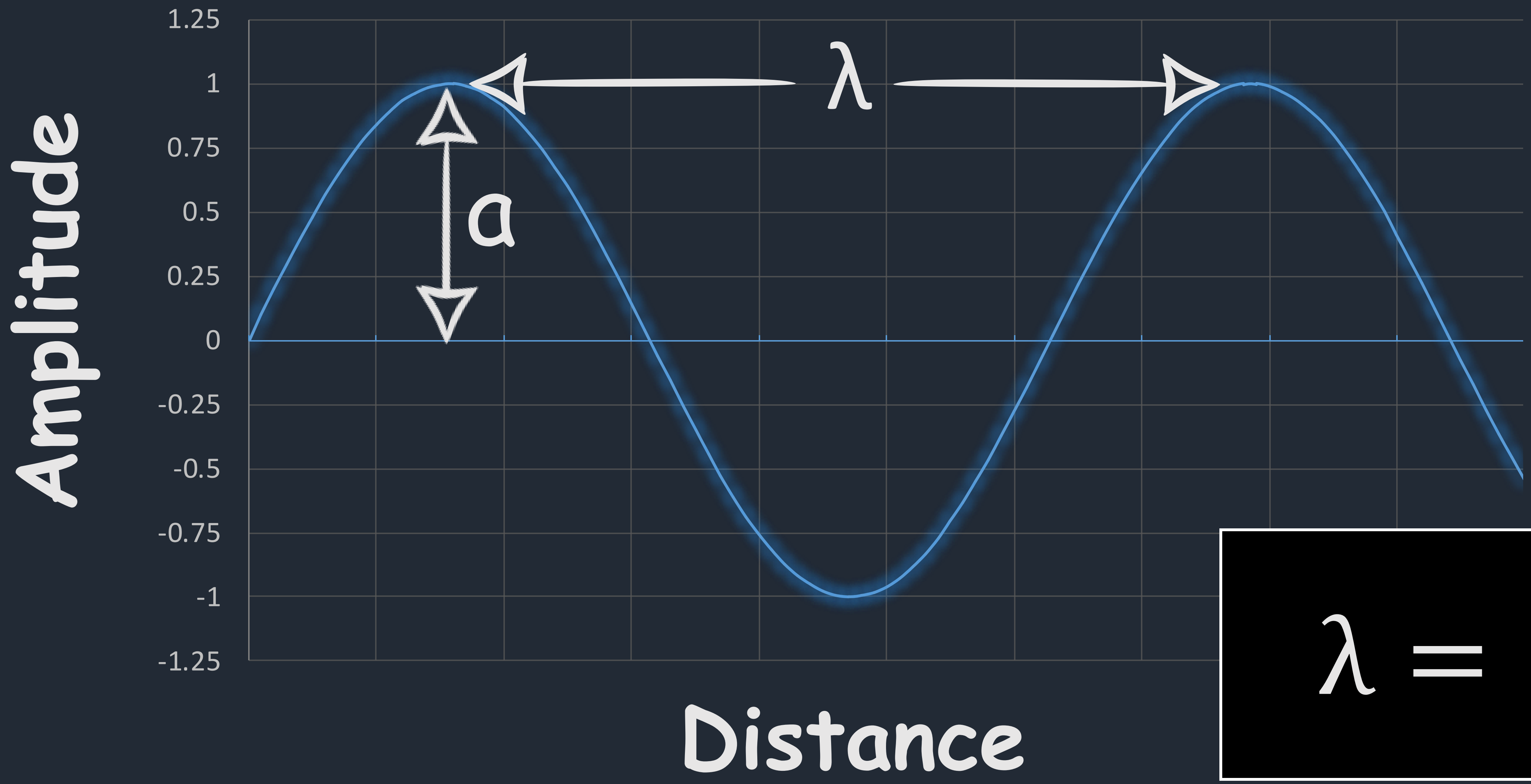
$$
\begin{aligned}
&for\ \mathbf{byte}\ in\ \mathbf{key}:\\
&\quad for\ \mathbf{guess}\ in\ \mathbf{0}\ to\ \mathbf{255}:\\
&\quad\quad ranks[guess] = correlation(leak, guess)\\
&\quad guess_{best}[byte] = argmax(ranks)
\end{aligned}
$$



Agenda

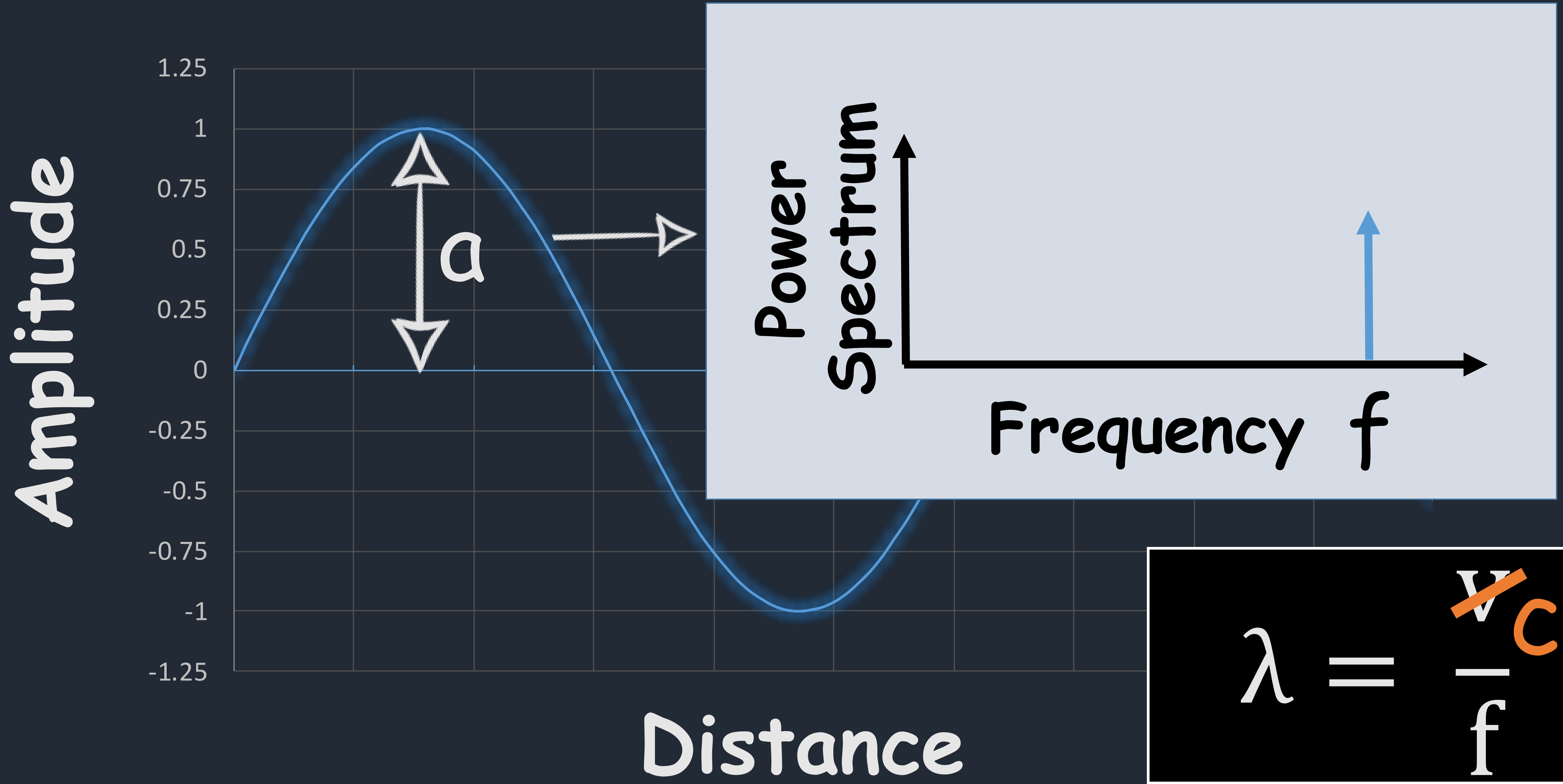
Introduction		
Part I	Part II	Part III
Background	*Our Story*	*Towards an attack*
- EM Side-Channels - RF communications 101 - Noise in mixed-signal ICs	- The Hypothesis - Explanation	- Building the attack - Demo
Conclusion		

A Simple Wave



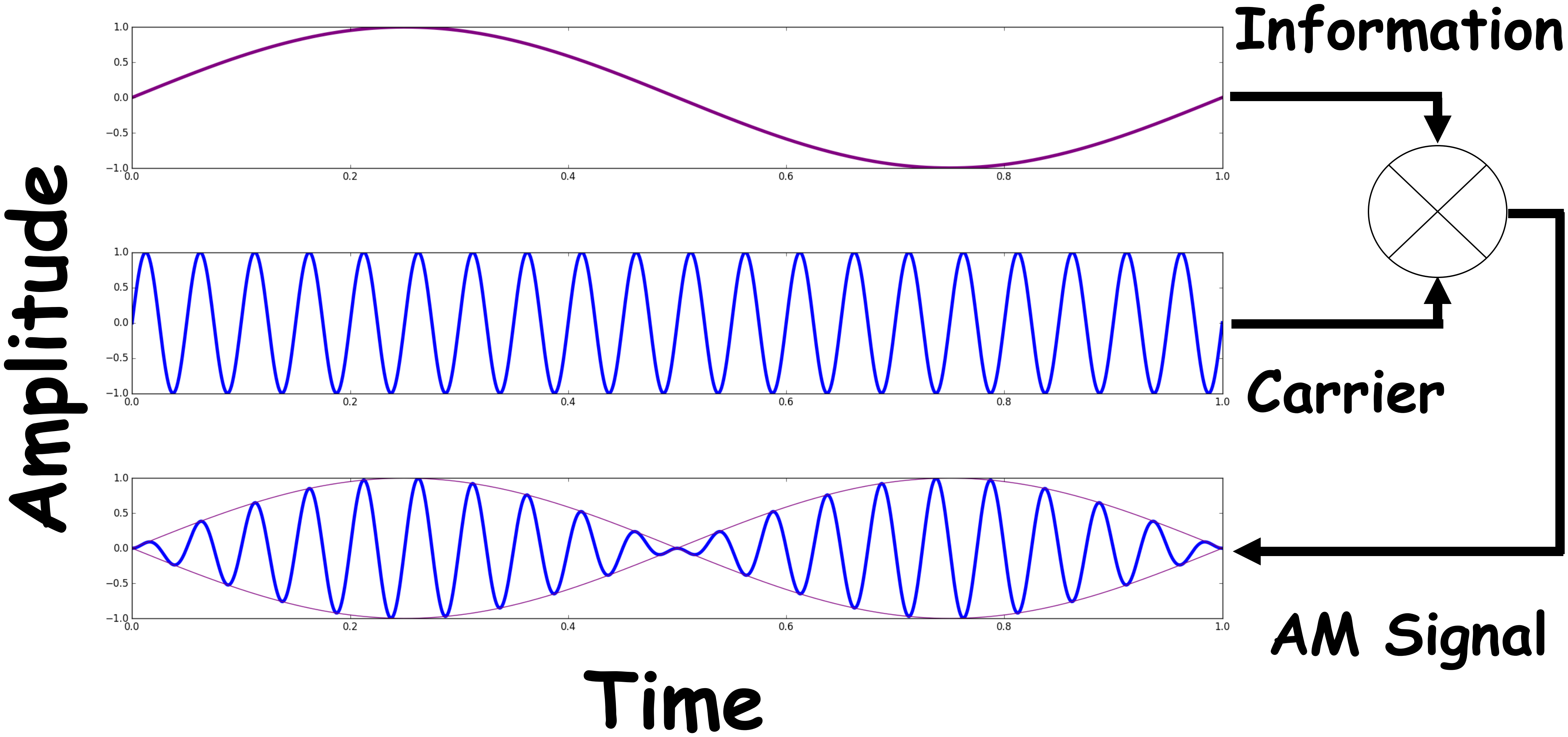
$$\lambda = \frac{\cancel{v}\,c}{f}$$

A Simple Wave

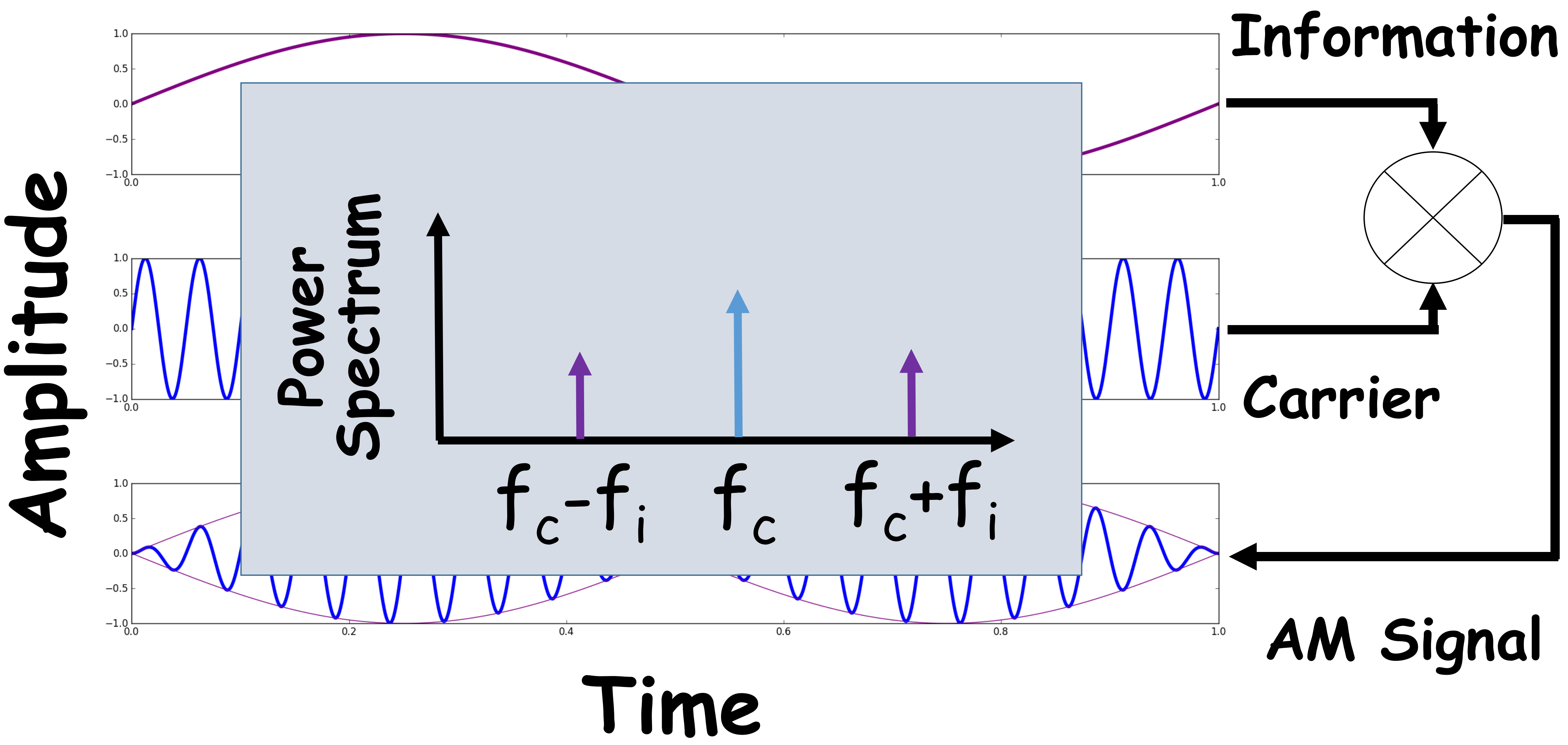


$$\lambda = \frac{\cancel{v}\,c}{f}$$

Modulation Basics



Modulation Basics



Agenda

Introduction

Part I	Part II	Part III
Background	*Our Story*	*Towards an attack*
- EM Side-Channels	- Discovery of the leak	- Building the attack
- RF communications 101	- Explanation	- Demo
- Noise in mixed-signal ICs		

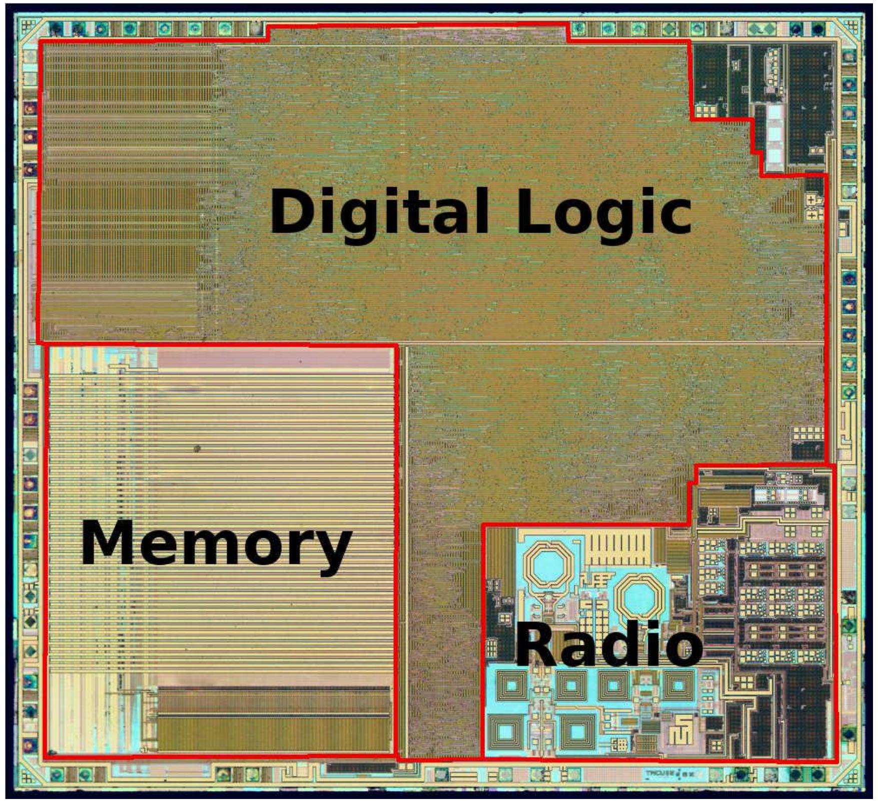
Conclusion

Mixed-signal chips

- Examples
  - Look around…
  - BT, WiFi, GPS, etc.
- Idea
  - Combine digital processor and analog radio on a single chip
  - Integrate the two and provide an easy interface to the outside
- Benefits
  - Cheap
  - Small
  - Power efficient
  - Nice for developers

A big problem: Noise

- Digital logic produces noise
- Close physical proximity facilitates noise propagation
- Analog radio is sensitive to noise
- Designers care about functionality



What if digital noise with sensitive information leaks into the radio signal?

Agenda

Introduction		
Part I	Part II	Part III
Background	*Our Story*	*Towards an attack*
- EM Side-Channels	- Discovery of the leak	- Building the attack
- RF communications 101	- Explanation	- Demo
- Noise in mixed-signal ICs		
Conclusion		

So the journey begins…

Phase
Cable
Firmware
Wifi
Chip
Frequency
Implementation
Bluetooth
Hardware
Amplitude
Antenna
Radio
Distance

Discovery of a leak

- After months of trying:
    - Multiple chips
    - Custom firmware
- One day:
    - Accidental tuning on "wrong" frequency
    - A leak dependent on our computations
- So the investigation started

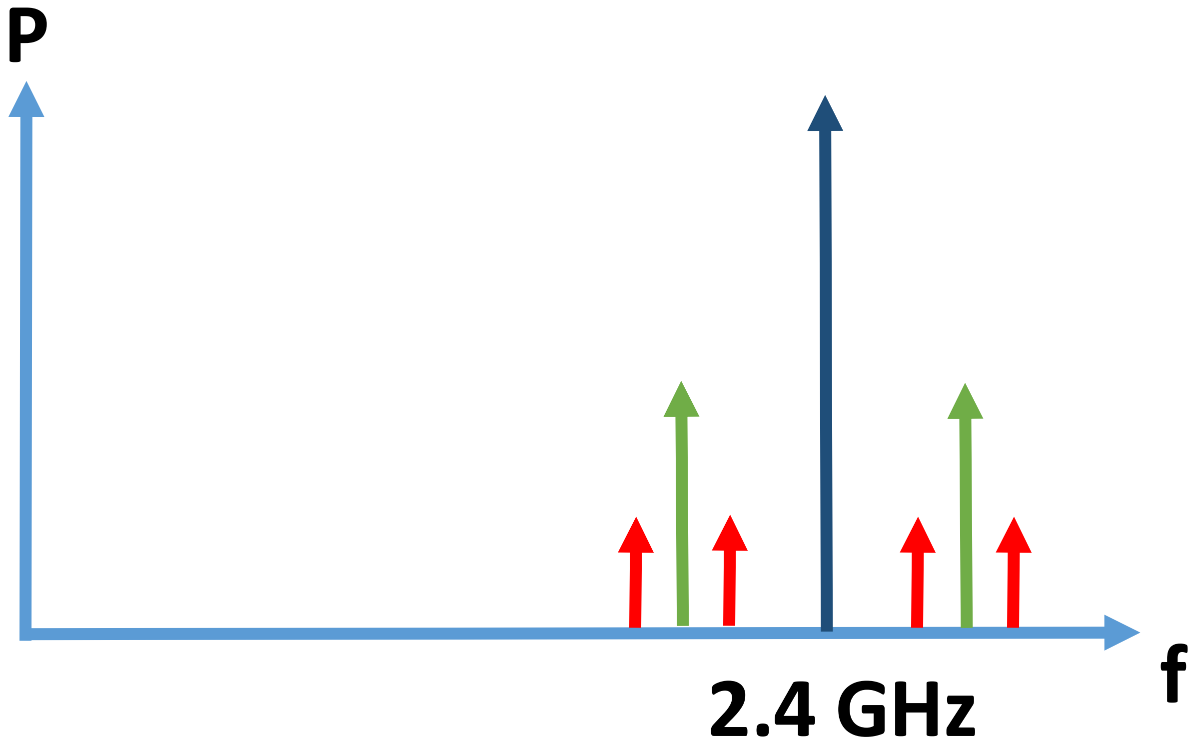
Discovery of a leak

Simple Firmware:

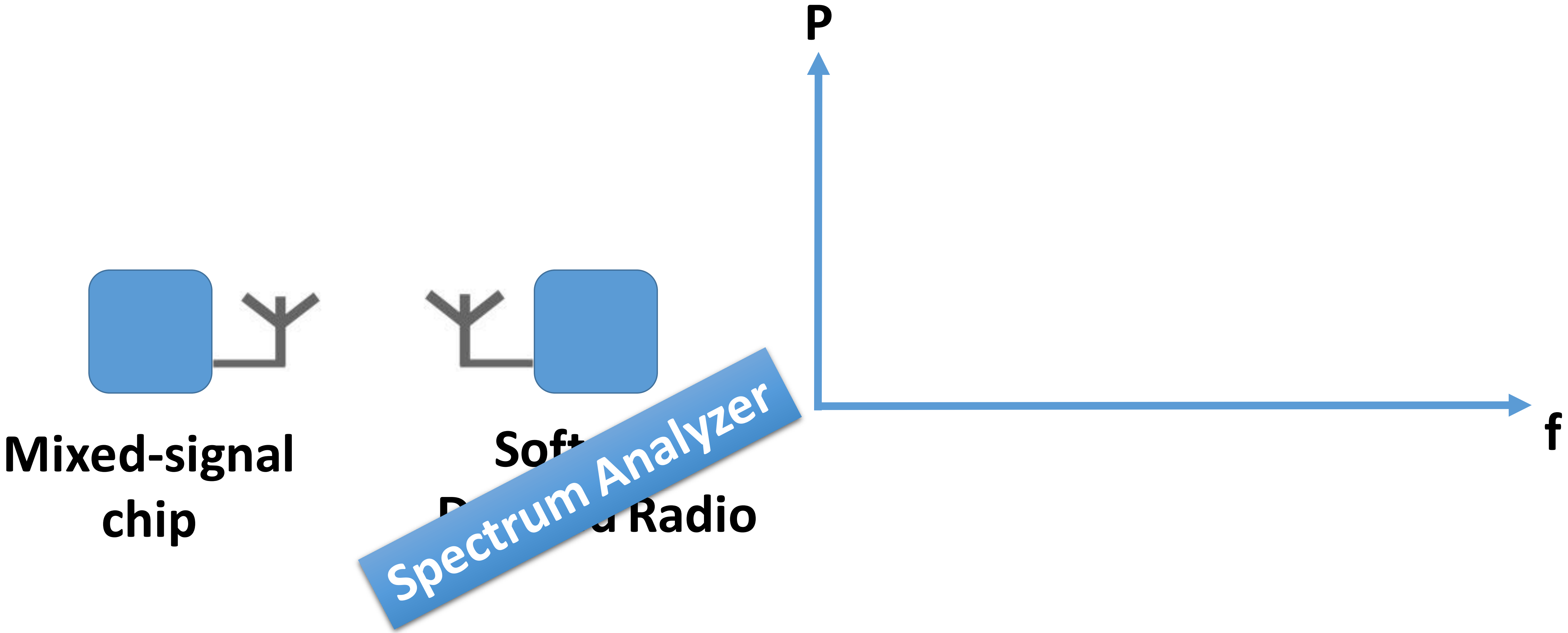
- TX off/on (CW)
- Slow loop/fast loop
- Controlled via UART

Mixed-signal chip

Software Defined Radio

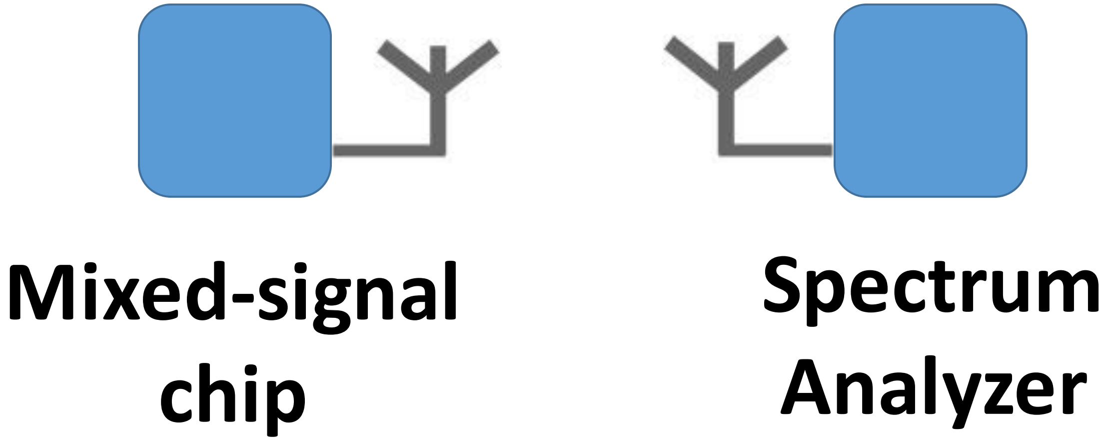


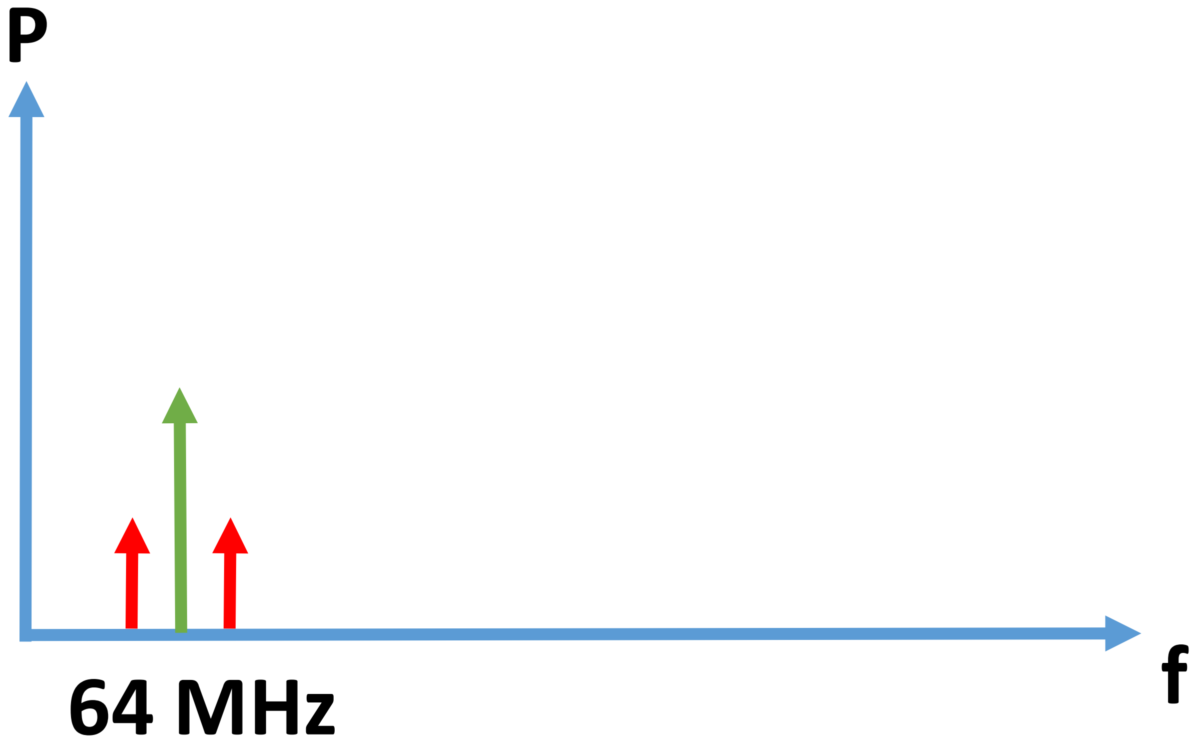
Discovery of a leak



Discovery of a leak

- Slow loop
- TX off
- Close distance



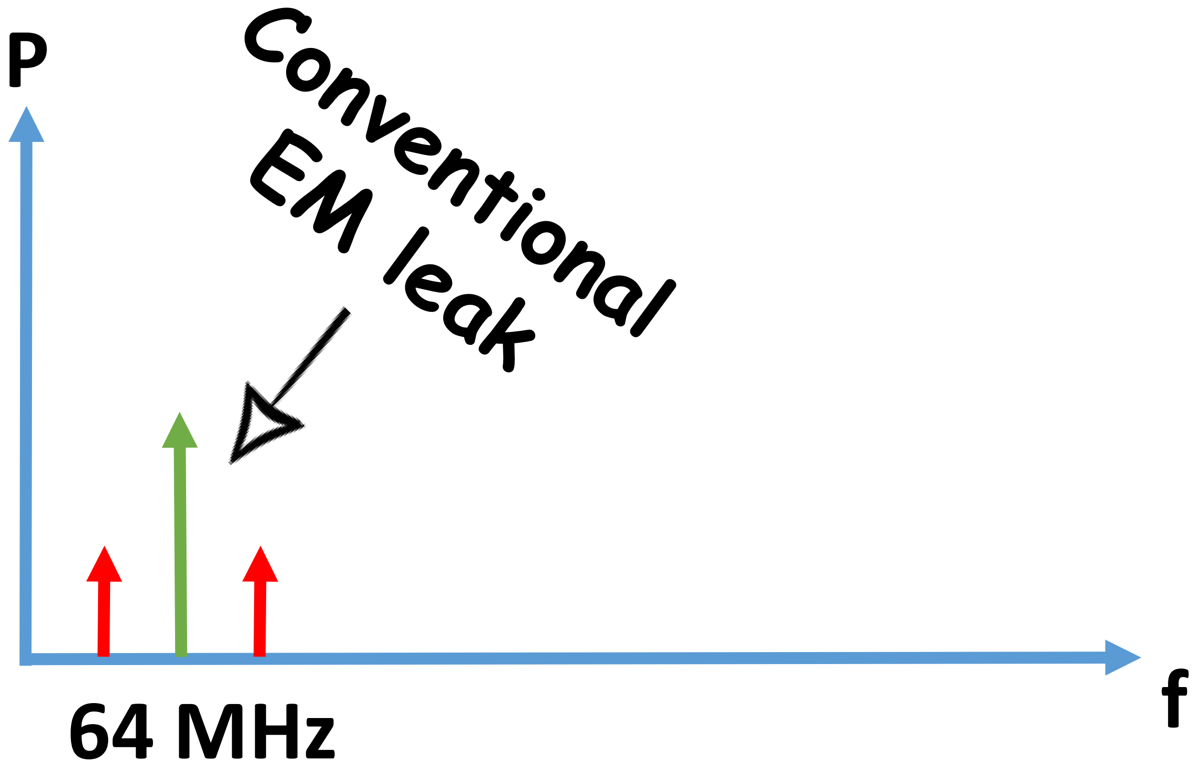


Discovery of a leak

- Fast loop
- TX off
- Close distance

Mixed-signal chip

Spectrum Analyzer

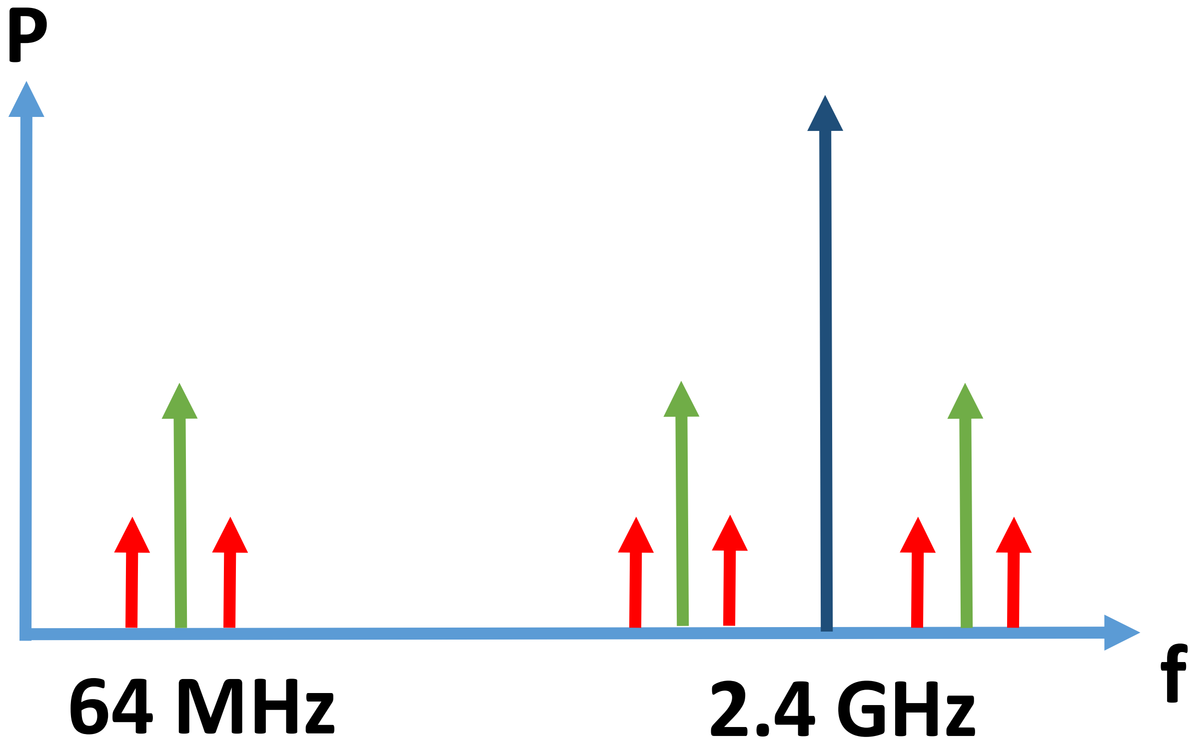


Discovery of a leak

- Slow loop
- TX on

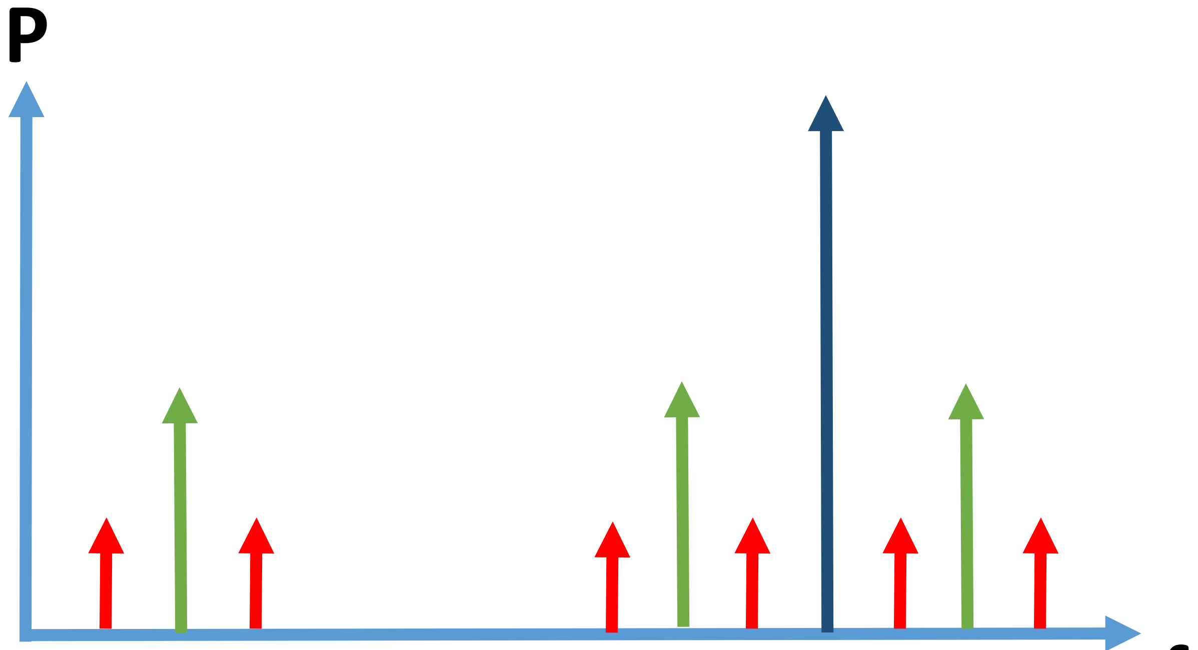
Mixed-signal chip

Spectrum Analyzer



Discovery of a leak

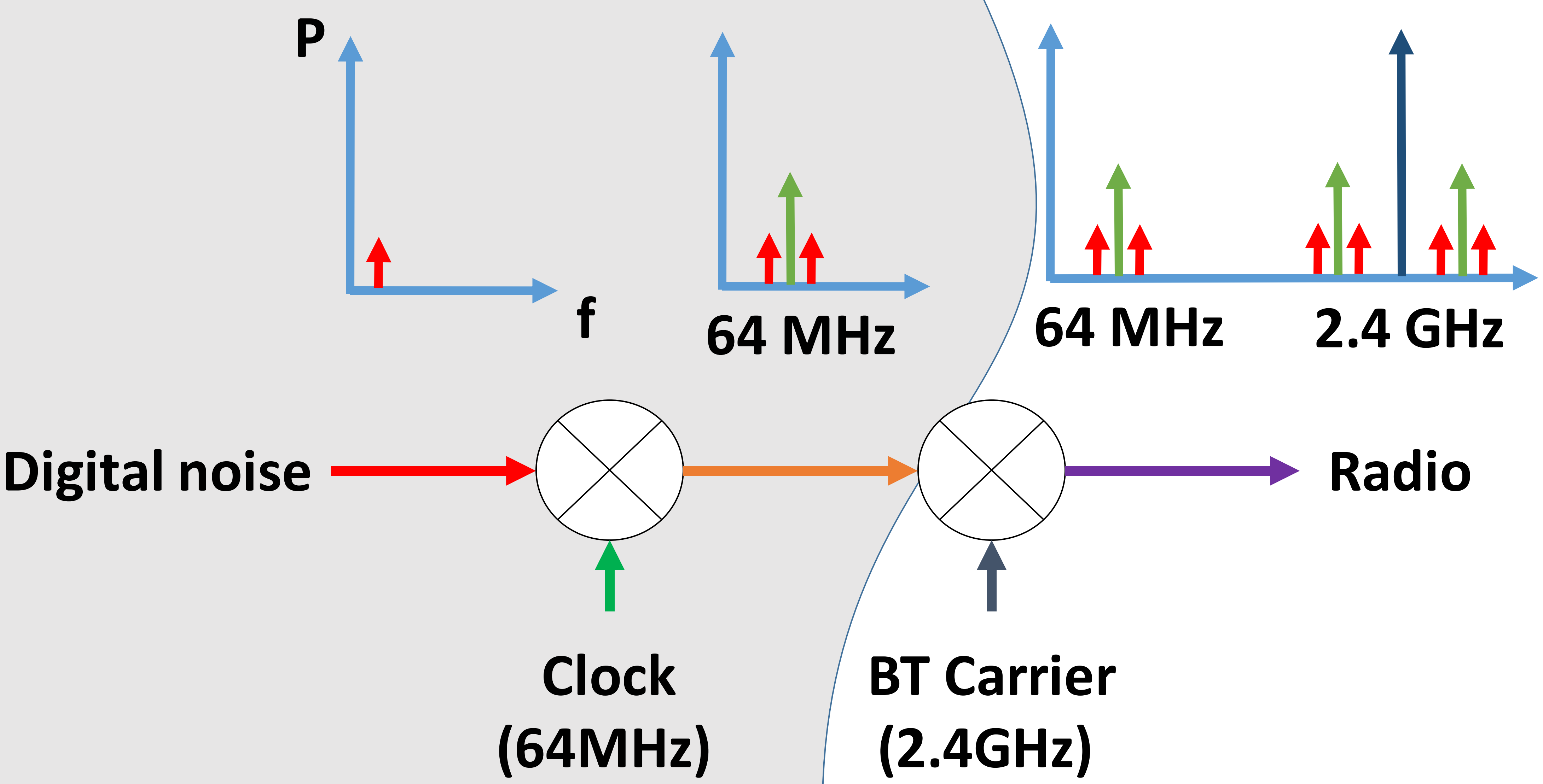
- Fast loop
- TX on



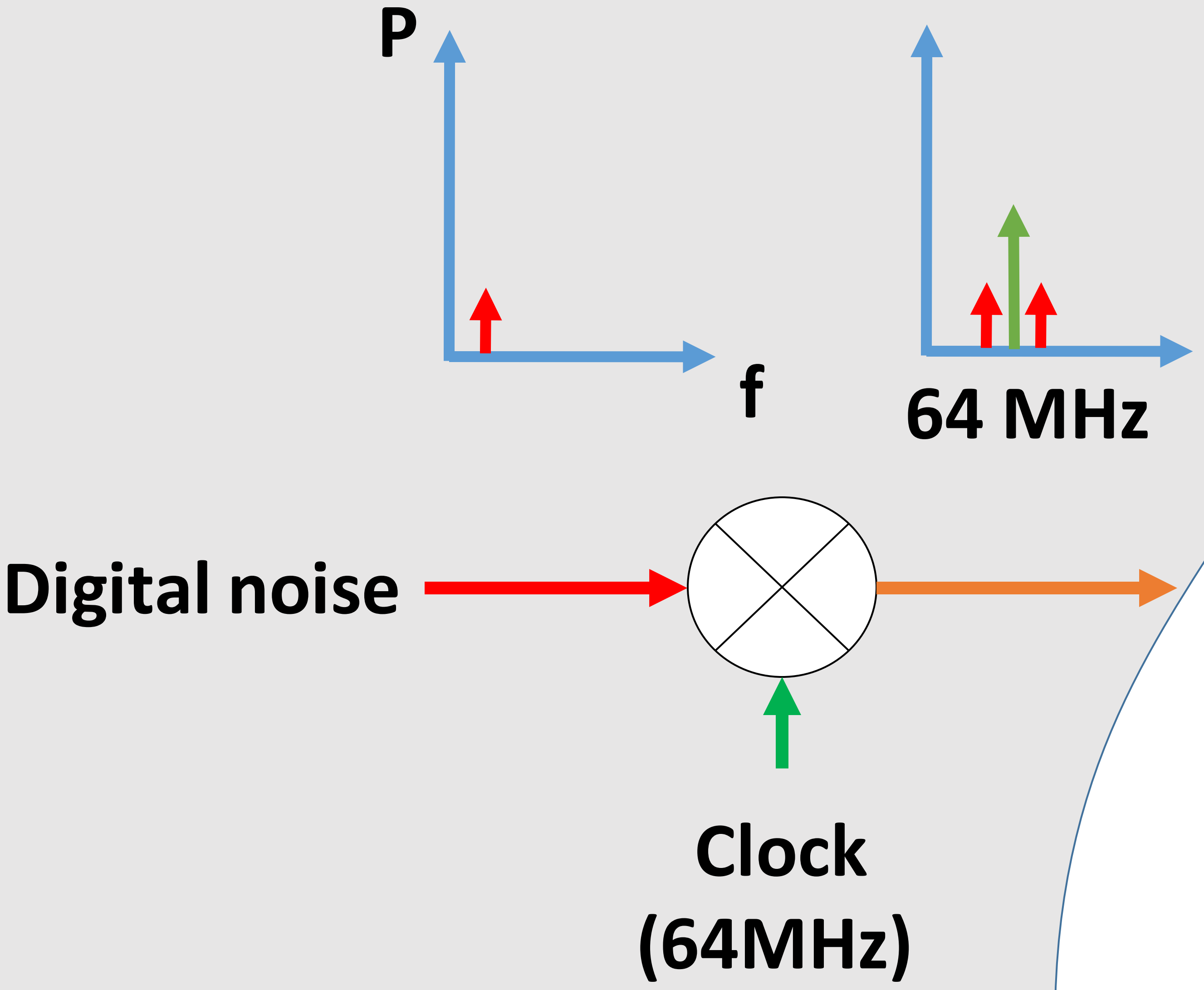
Agenda

Introduction		
Part I	Part II	Part III
Background	*Our Story*	*Towards an attack*
- EM Side-Channels - RF communications 101 - Noise in mixed-signal ICs	- Discovery of the leak - Explanation	- Building the attack - Demo
Conclusion		

Logic Transmission Scheme

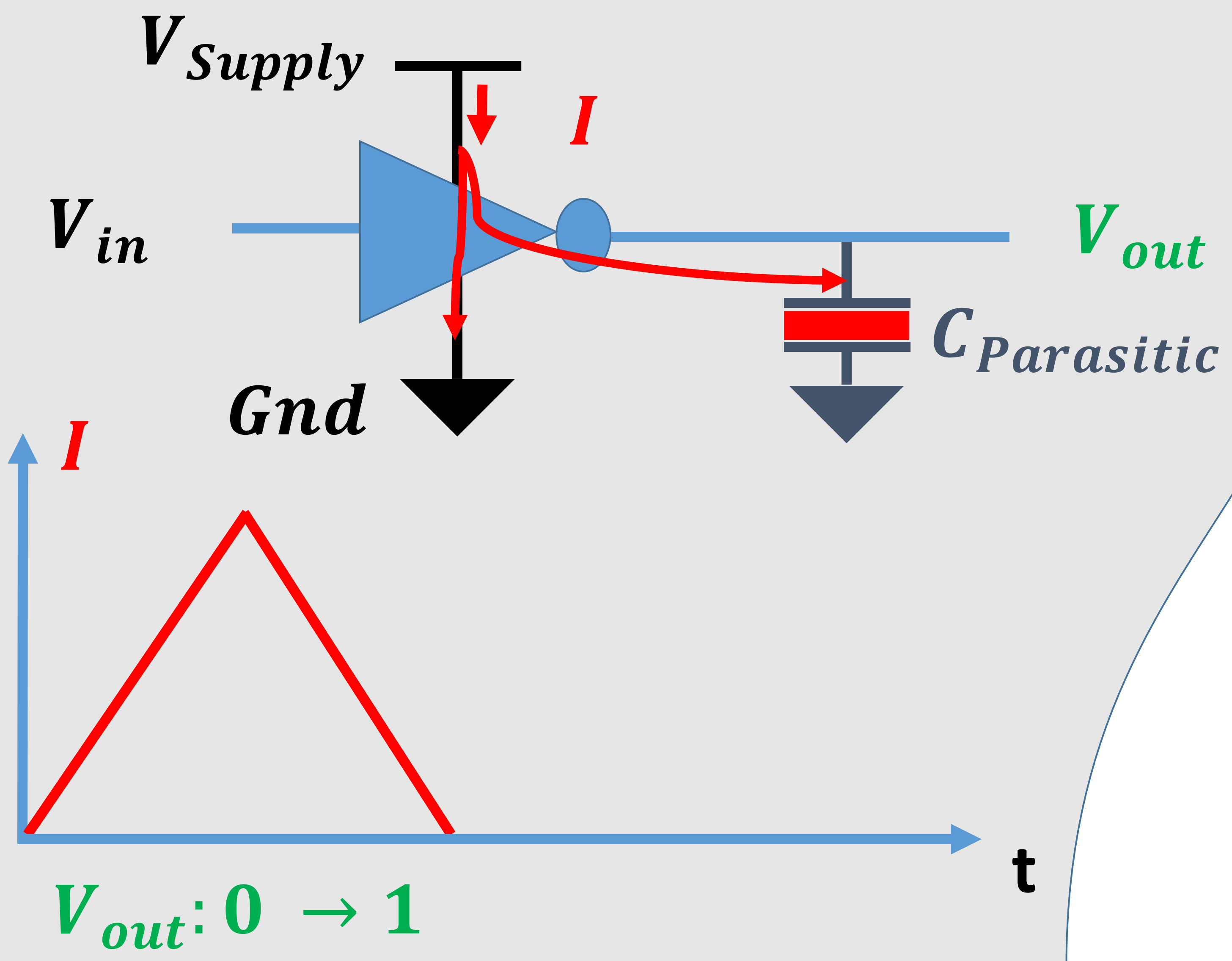


Conventional



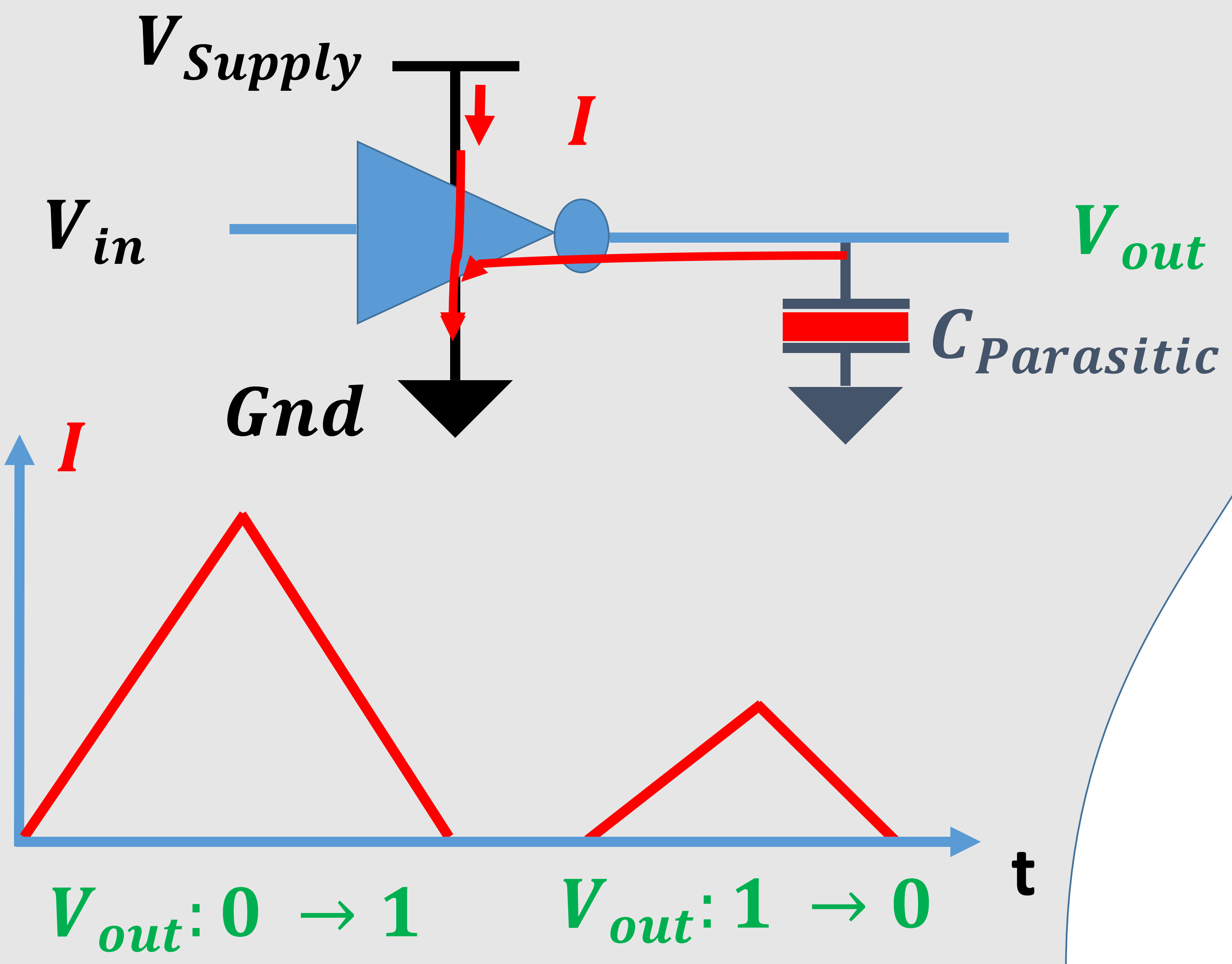
- Current consumption
- Mixing

Conventional



- **Current consumption**
  - **Dependent on transitions of logic values**
- **Mixing**

Conventional

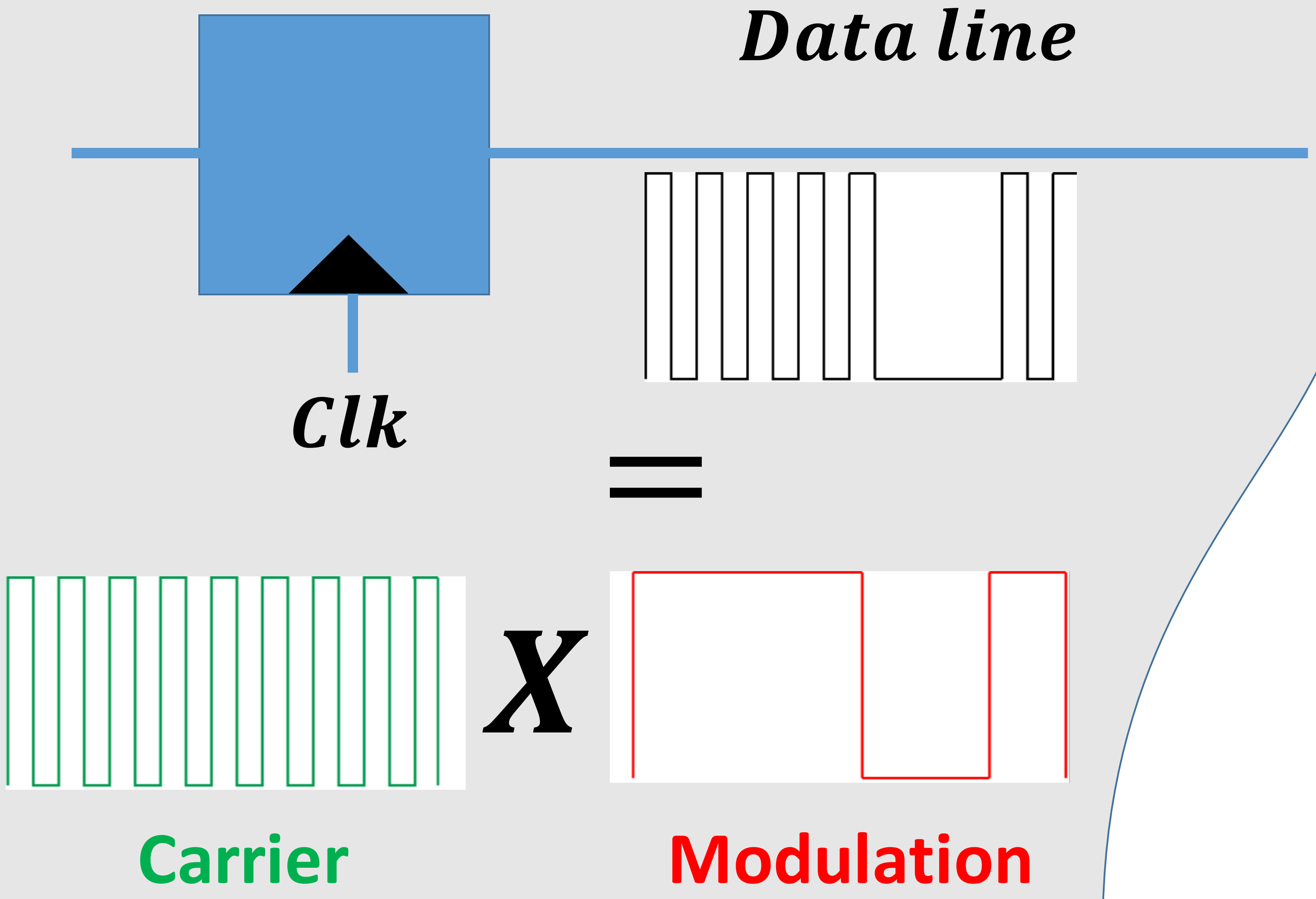


- Current consumption
  - Dependent on transitions of logic values
- Mixing

blackhat USA 2018

Conventional

#BHUSA



- Current consumption
  - Dependent on transitions of logic values
- Mixing
  - Clock
  - 1: “direct”

Conventional

$V_1 + V_2$

$$\downarrow I_{sat} = \alpha(V_1 + V_2 - V_{th})^2 =$$

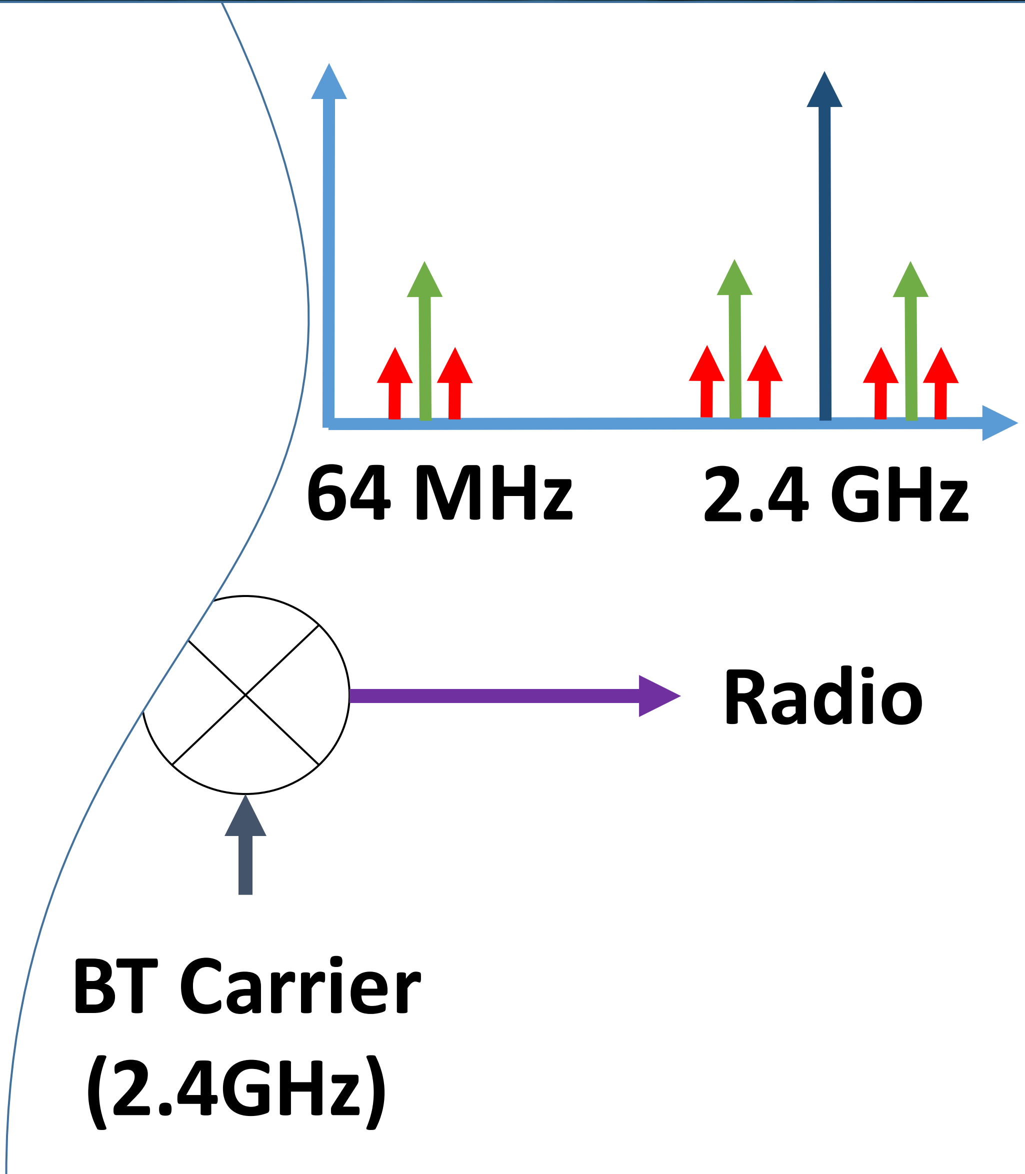
$$= 2\,V_1 \times V_2 + etc.$$

nMOS transistor
in saturation

- Current consumption
  - Dependent on transitions of logic values
- Mixing
  - Clock
  - 1: “direct”
  - 2: non-linear components

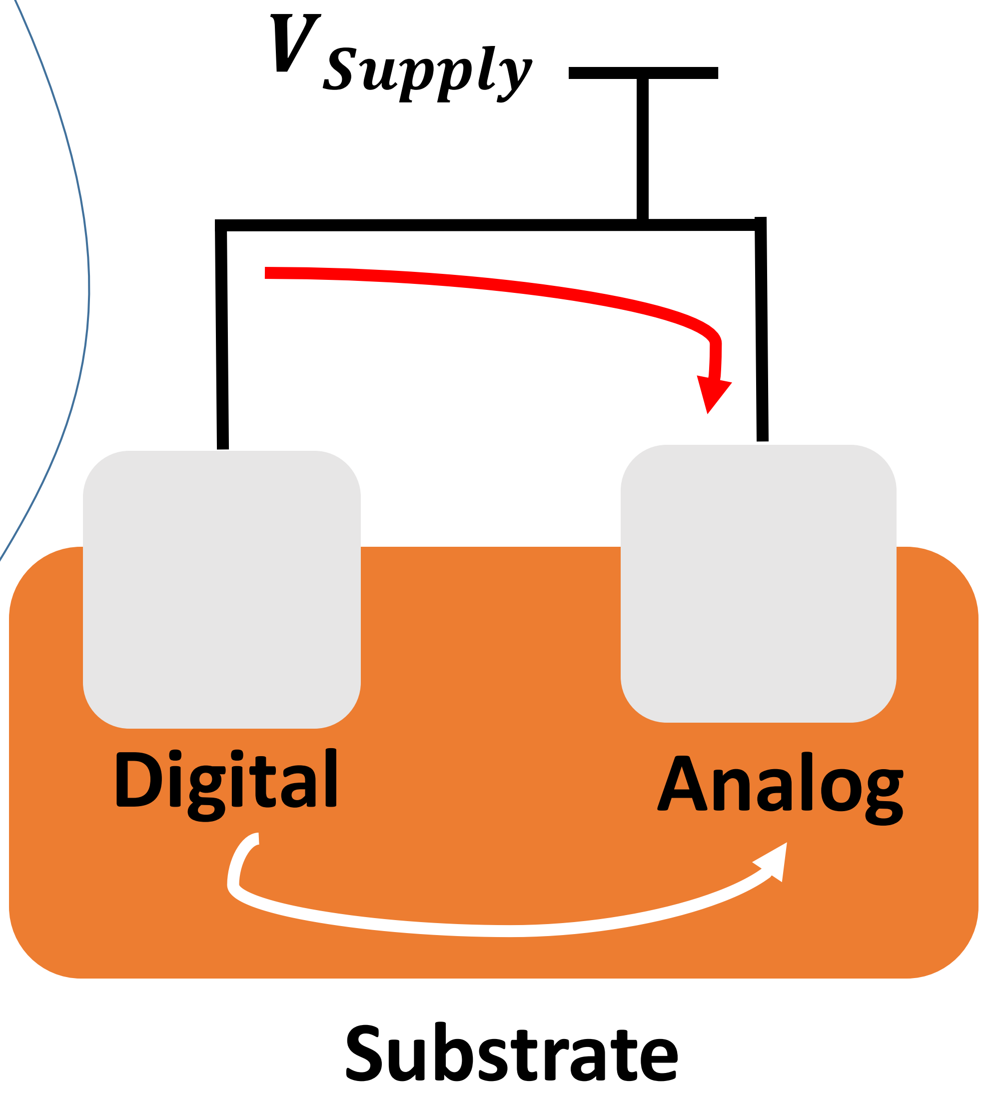
Screaming Channels

- **Digital to Analog propagation**
- **Mixing**



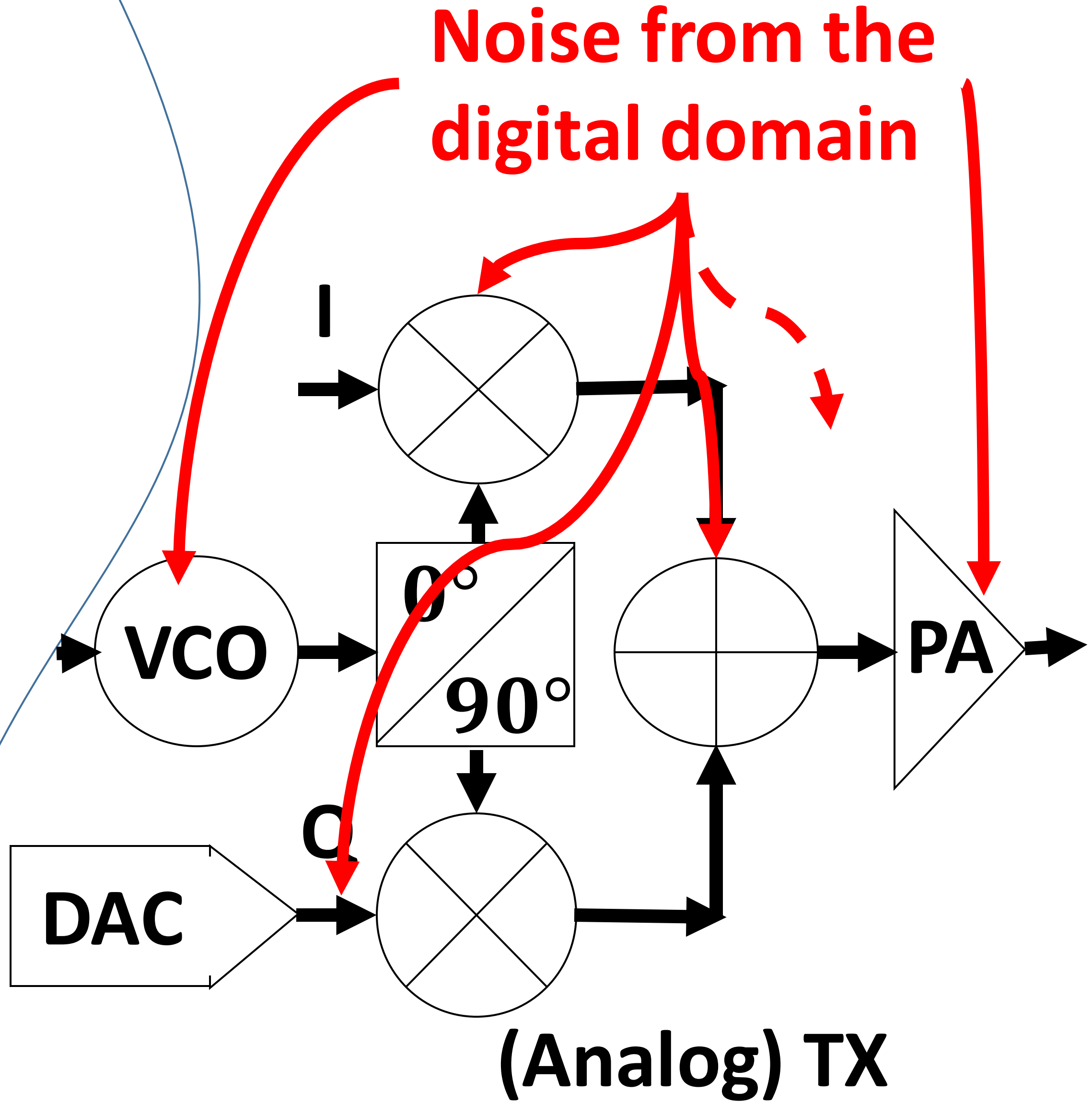
Screaming Channels

- Digital to Analog propagation
  - 1: Substrate Coupling
    - Same silicon die
  - 2: Power Supply Coupling
    - Same power supply
- Mixing

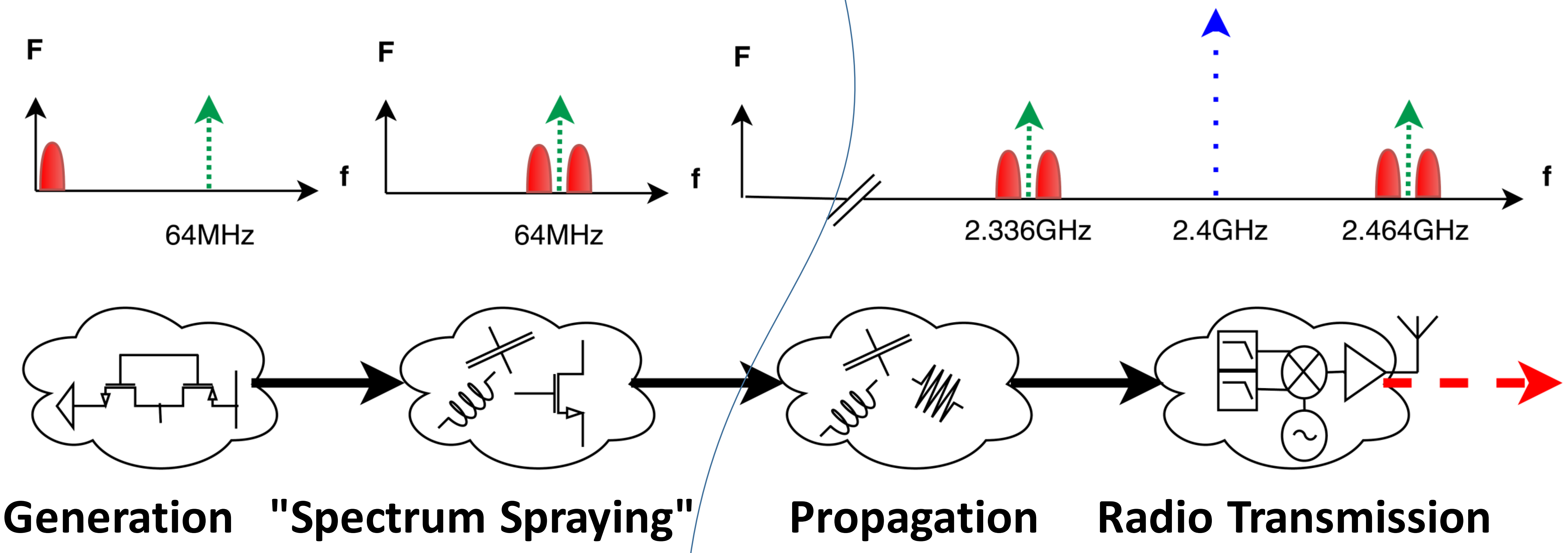


Screaming Channels

- Digital to Analog propagation
  1. Substrate Coupling
     - Same silicon die
  2. Power Supply Coupling
     - Same power supply
- Mixing
  1. Voltage Controlled Oscillator
  2. Power Amplifier
  3. etc.



Summing Up

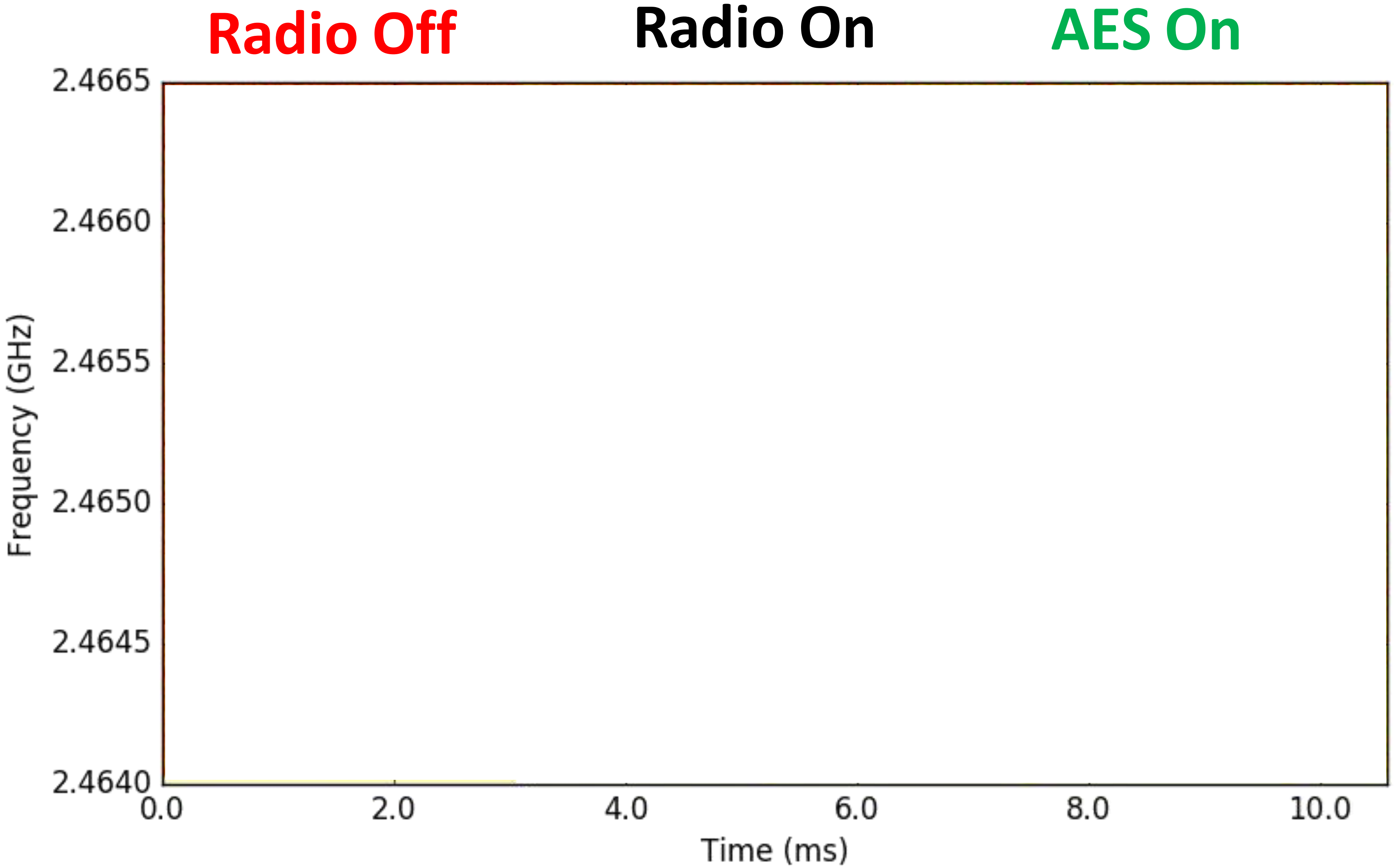


F
f
64MHz
F
f
64MHz
F
f
2.336GHz
2.4GHz
2.464GHz
Generation
"Spectrum Spraying"
Propagation
Radio Transmission

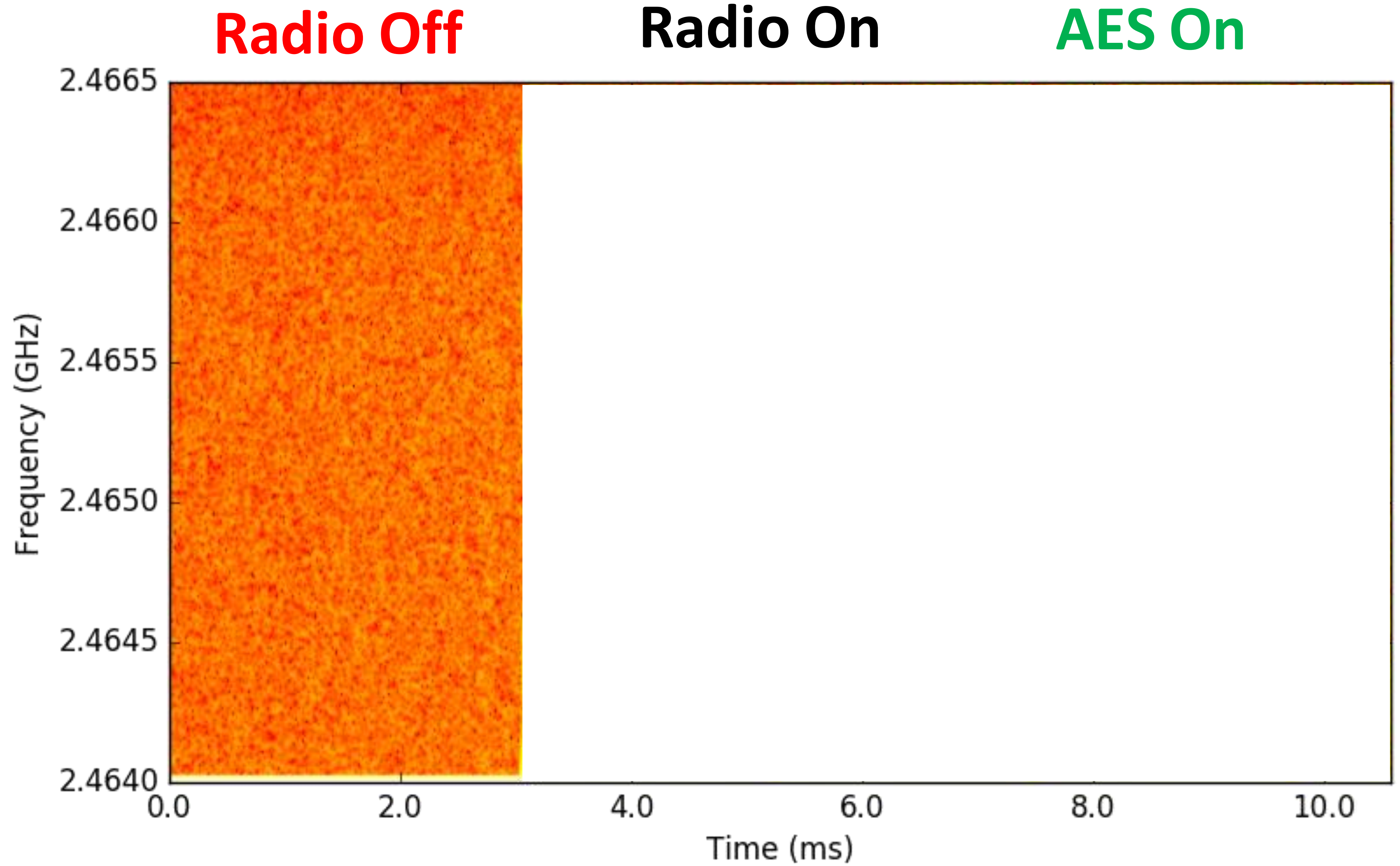
Agenda

Introduction		
Part I	Part II	Part III
Background	*Our Story*	*Towards an attack*
- EM Side-Channels - RF communications 101 - Noise in mixed-signal ICs	- Discovery of the leak - Explanation	- Building the attack - Demo
Conclusion		

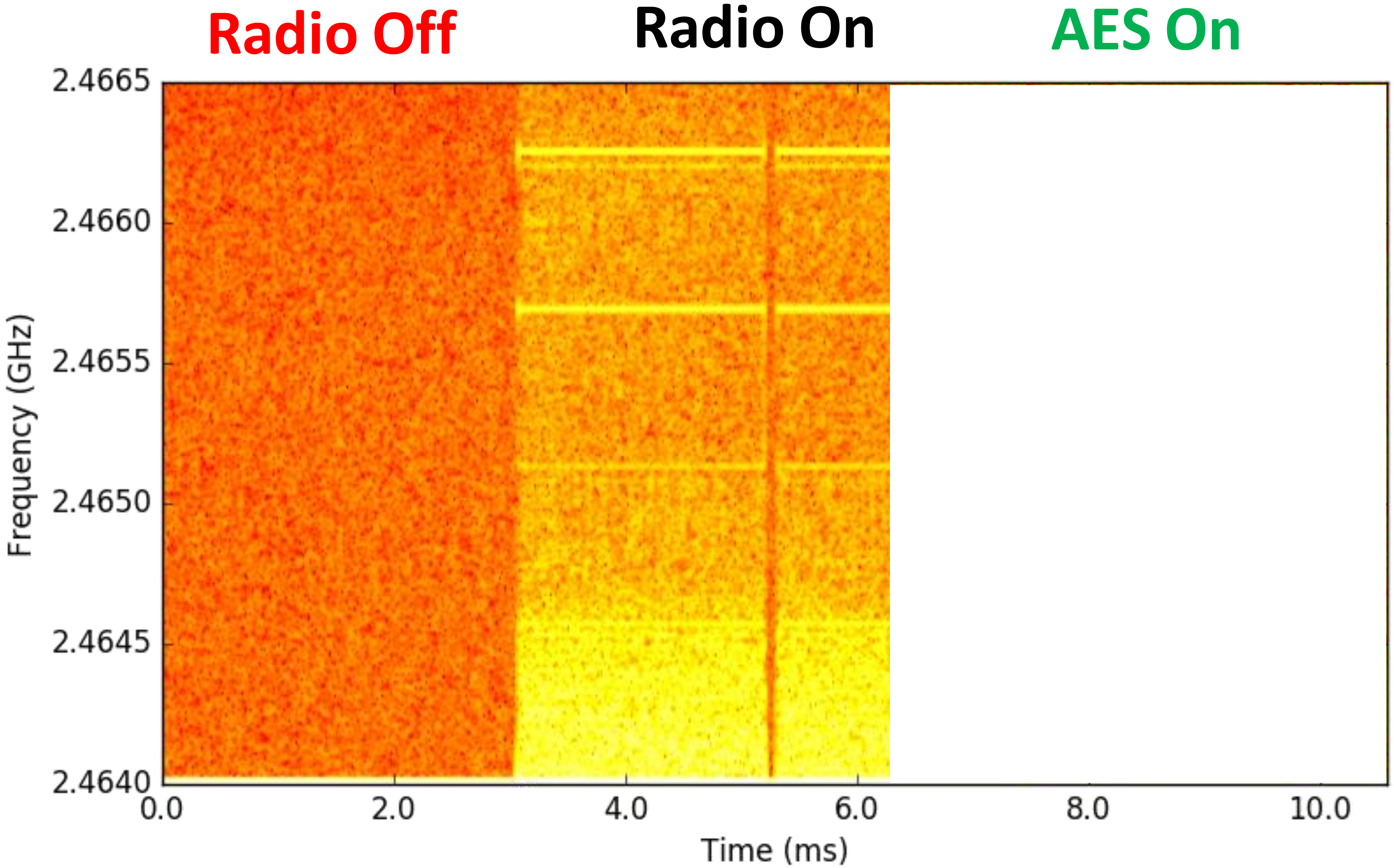
AES in the spectrogram



AES in the spectrogram

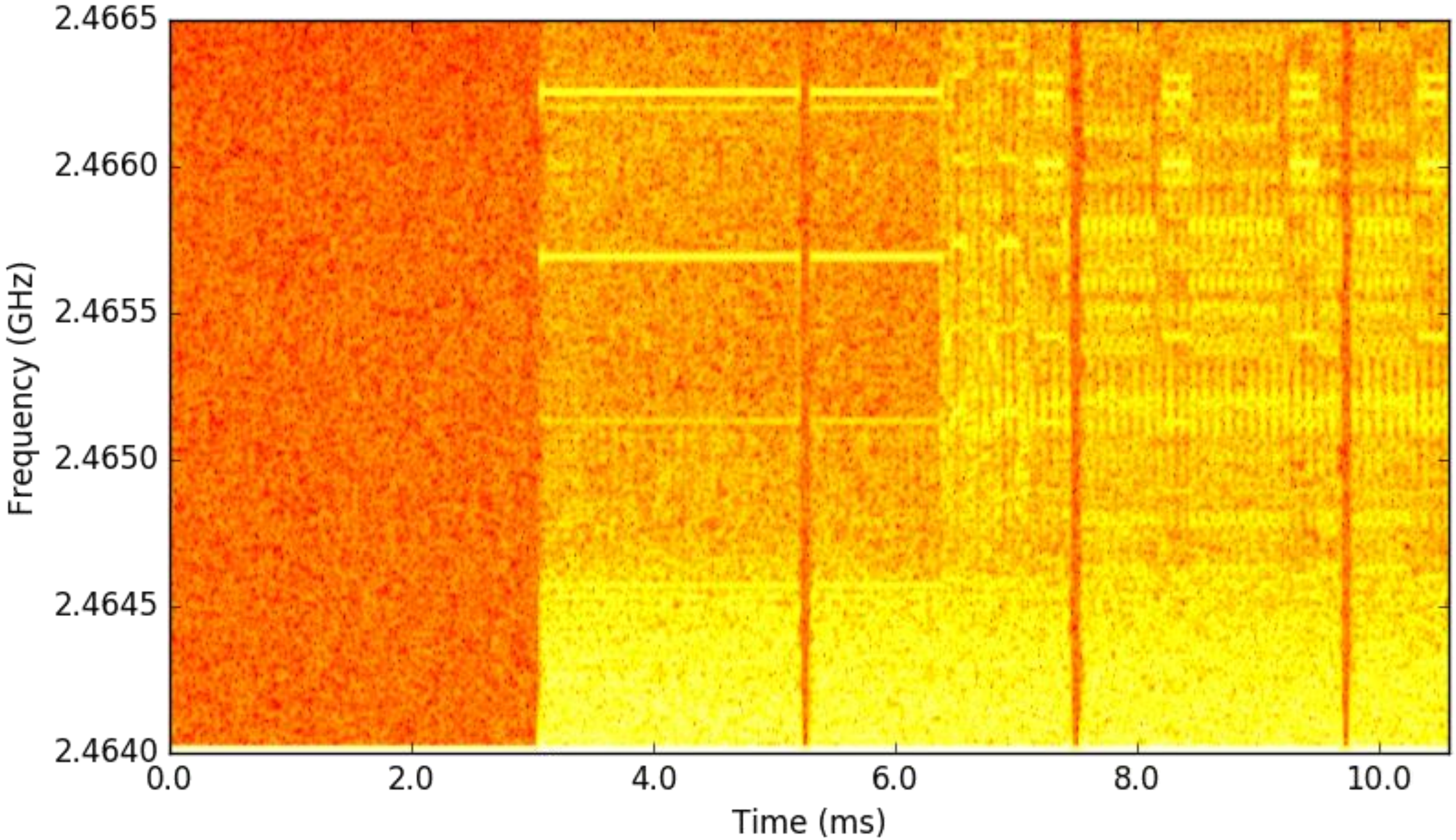


AES in the spectrogram

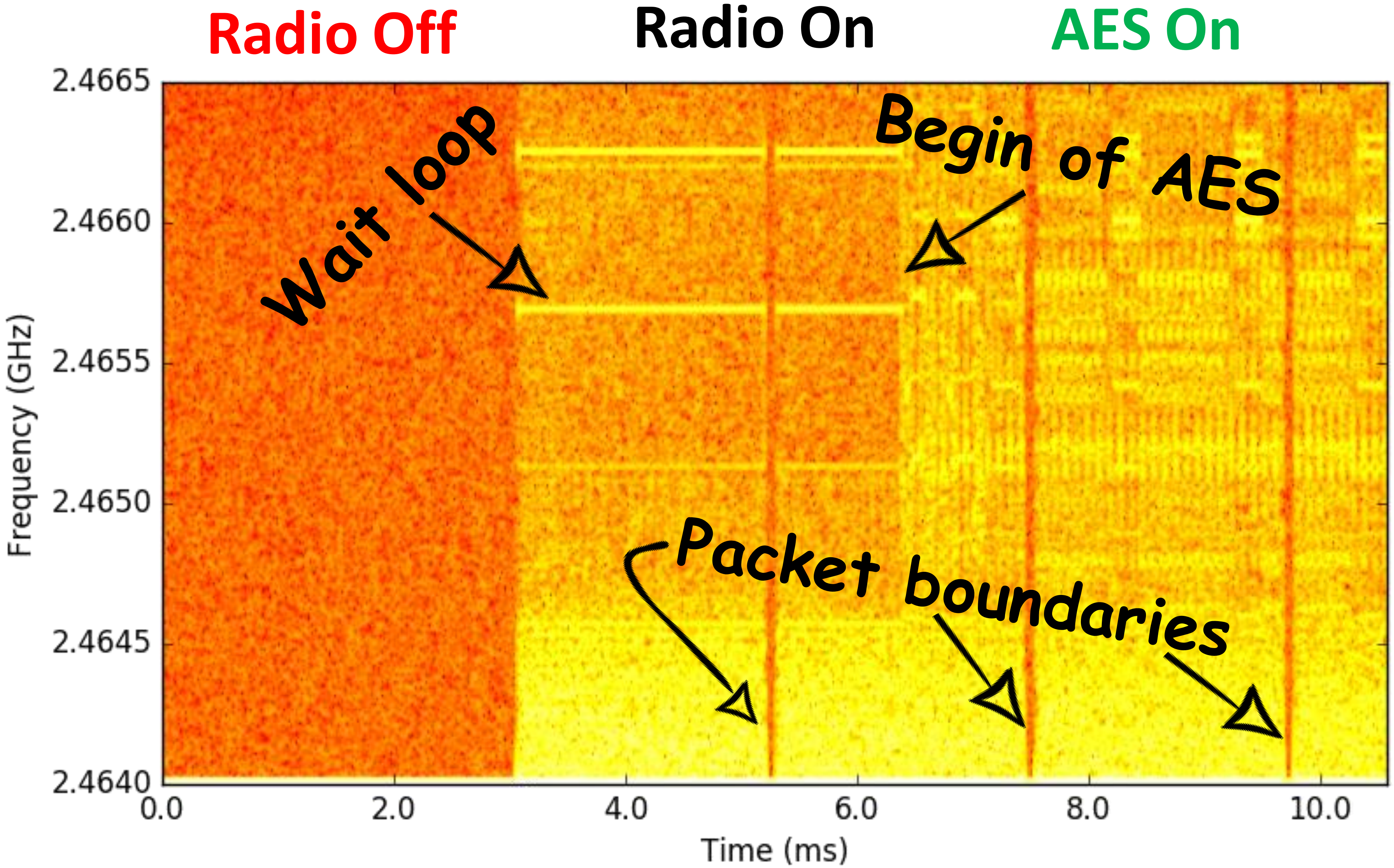


AES in the spectrogram

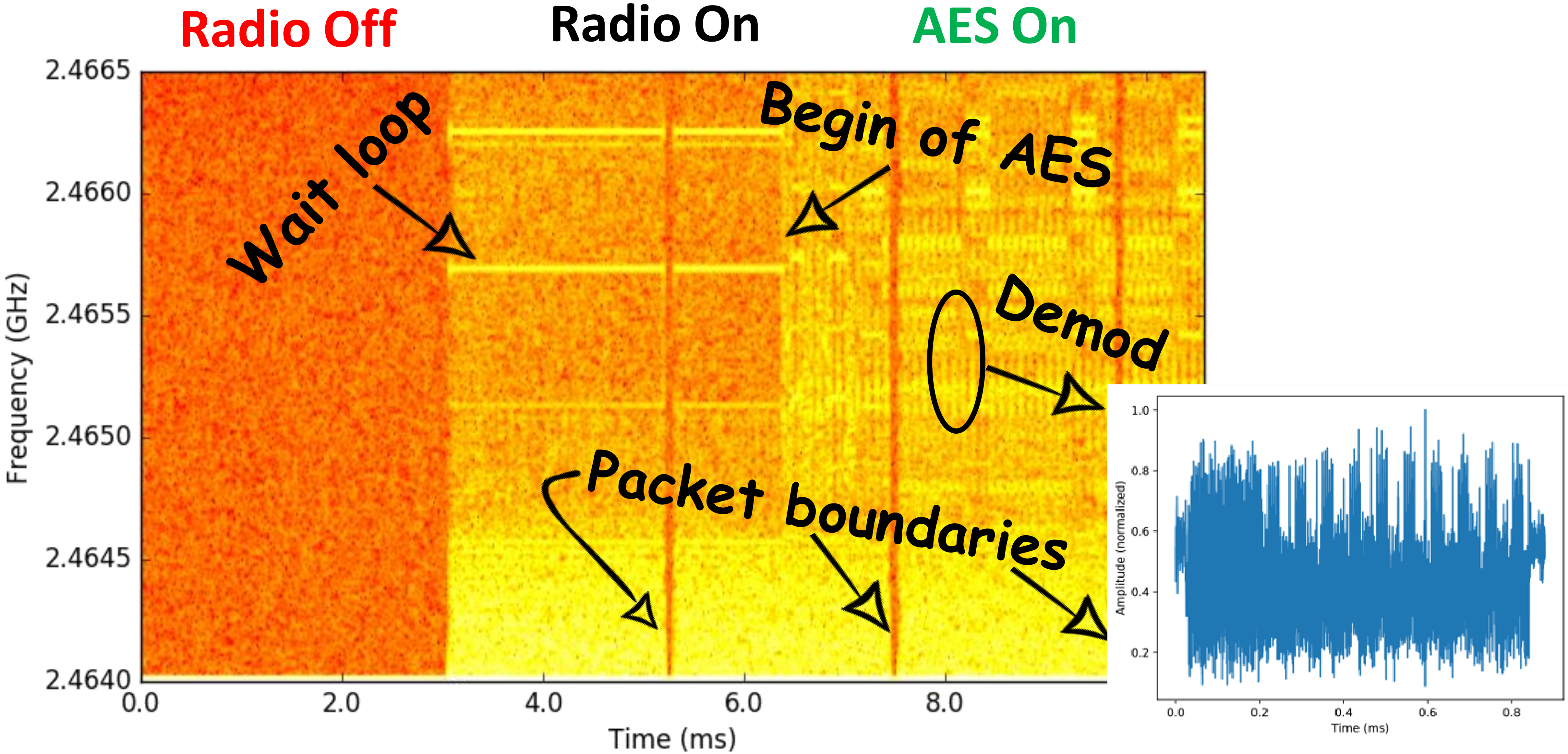
Radio Off | Radio On | AES On



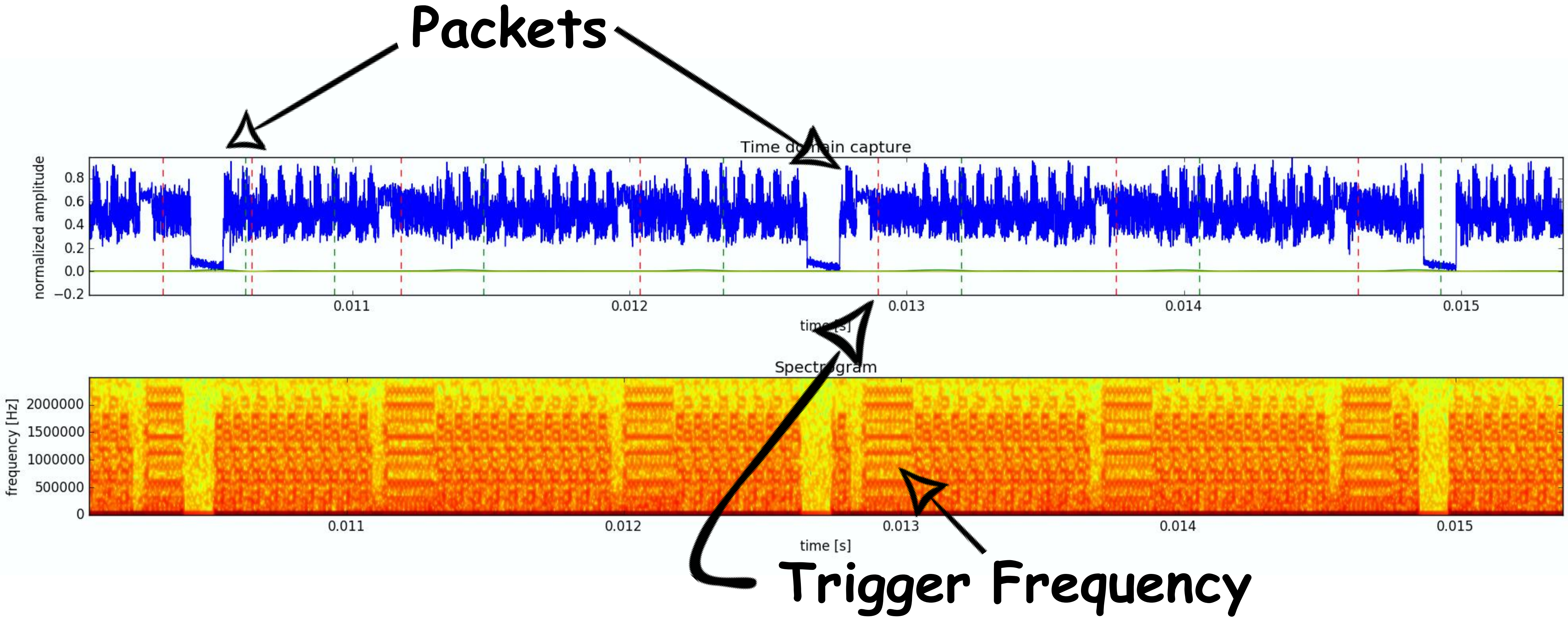
AES in the spectrogram



AES in the spectrogram

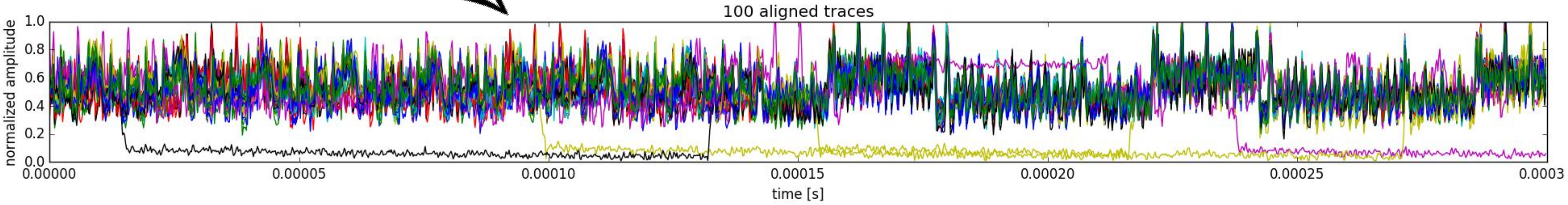


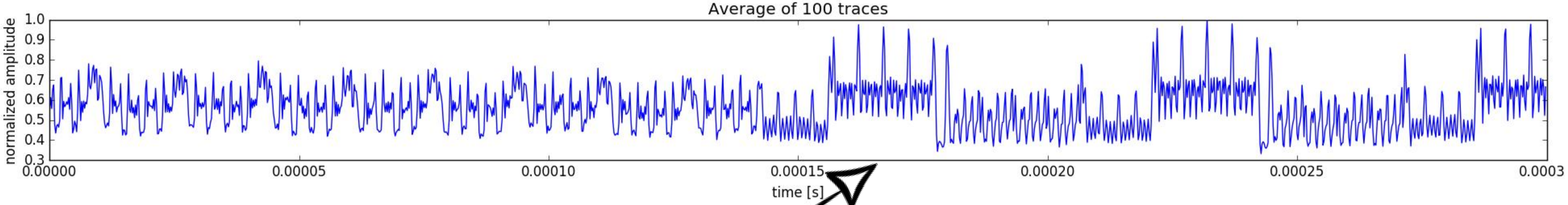
Extraction and alignment



Extraction and alignment

Self-correlation alignment





Average

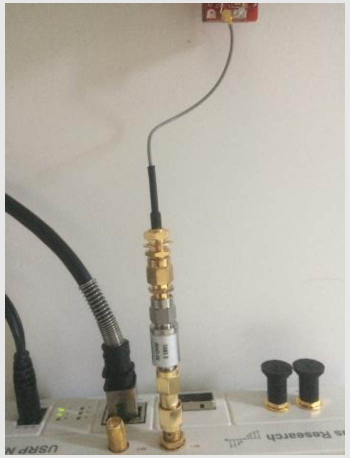
Attacking

- Extraction of clean traces

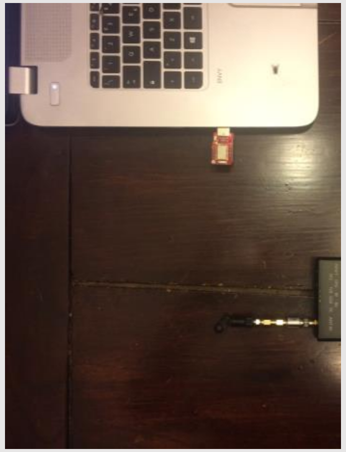
- Some attacks
  - Correlation attack
  - Template attack
  - Built upon ChipWhisperer's implementations

- Attacked implementations
  - mbedTLS
  - TinyAES

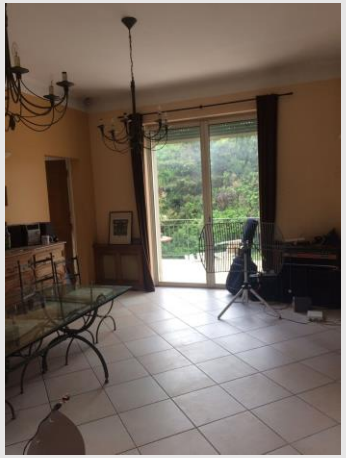
Evolution of the attack



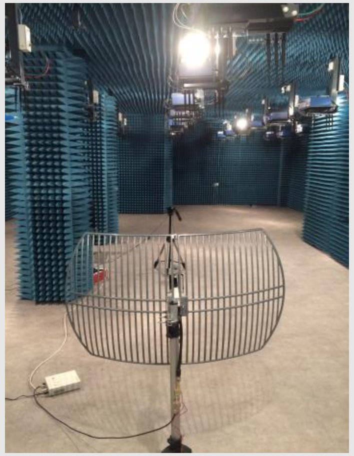
Cable



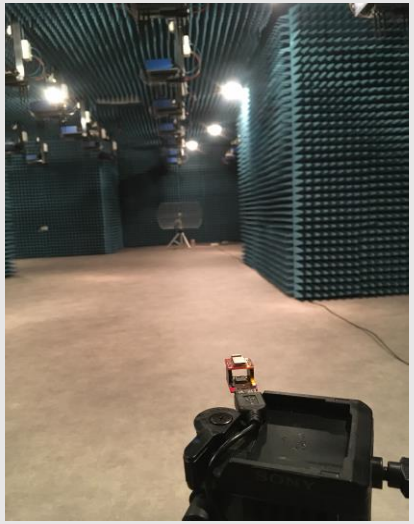
15 cm



2 m



3 m



10 m

5 m

Agenda

Introduction		
Part I	Part II	Part III
Background	*Our Story*	*Towards an attack*
- EM Side-Channels - RF communications 101 - Noise in mixed-signal ICs	- Discovery of the leak - Explanation	- Building the attack - Demo
Conclusion		

Demo time!

Agenda

Introduction

Part I	Part II	Part III
Background	*Our Story*	*Towards an attack*
- EM Side-Channels	- Discovery of the leak	- Building the attack
- Noise in mixed-signal ICs	- Explanation	- Demo results

Conclusion

Impact

Impact

- General Problem
- Potential to affect any radio transmitter close to digital logic
- Not limited to IC designs

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.]

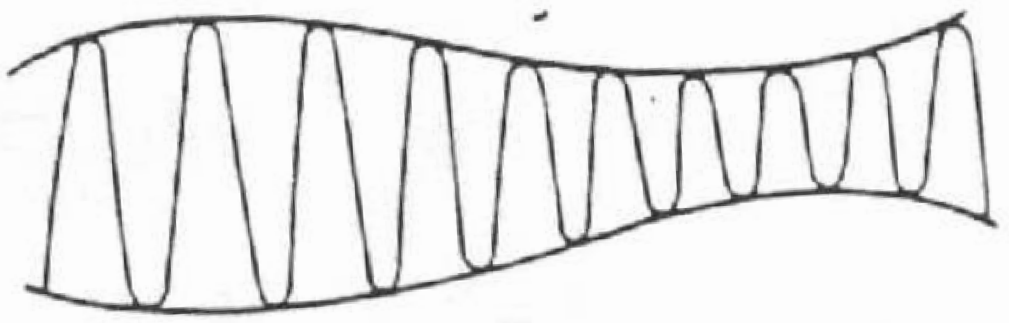


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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.

Just a PoC?

- Attacks on real-world targets will follow
- Simple attack, we can do much better
  - Collection: get more data in less time
  - Processing: make better use of the information we have
  - Abusing protocol weaknesses
- Share early, mitigate faster

Responsible Disclosure

- Contacted major vendors & multiple CERTs
- Multiple acknowledgments of the problem’s generality
- 2 vendors are replicating our results
- 1 vendor looks actively into short- and long-term countermeasures

Countermeasures

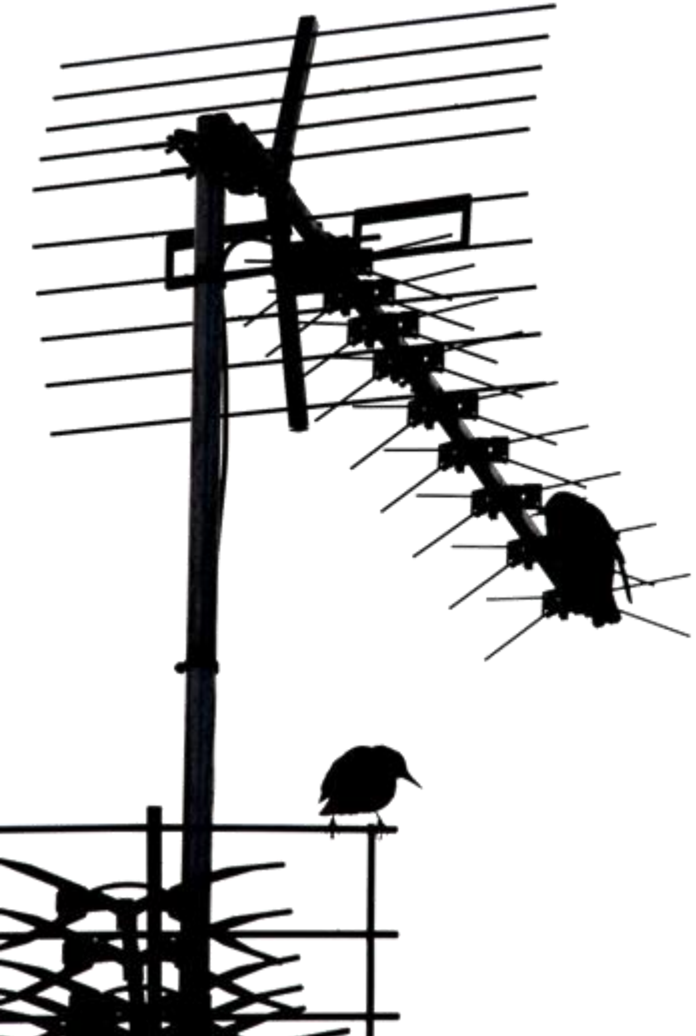
Countermeasures

- Classic (SW/HW)
  - Masking, Noise, good protocols, etc.
  - "Easy" but may be expensive to buy license for low-cost chips
  - A classic arms race can start
- Software-specific
  - Turn off the radio during sensitive computations
  - Not so easy if there are real-time requirements
  - Turns off the channel completely
- Hardware-specific
  - Consider security impact of noise coupling during design and testing
  - Will it increase the cost too much?

Black Hat Sound Bytes

What will you take home?

Screaming Channels: The Sound Bytes



Everything is analog

Digital noise can leak into RF circuitry

EM side-channel attacks from a distance

Thank you!

Code: https://www.github.com/eurecom-s3/screaming_channels
More Info: https://s3.eurecom.fr/tools/screaming_channels

<camurati@eurecom.fr>
@GioCamurati

<muench@eurecom.fr>
@nSinusR

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] Kasper, Timo, et al. "EM side-channel attacks on commercial contactless smartcards using low-cost equipment." *International Workshop on Information Security Applications*. Springer, Berlin, Heidelberg, 2009.

[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] 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

- "Github ribbon" - MIT – mojombo
https://blog.github.com/2008-12-19-github-ribbons/

- “Television Antenna" - CC0 – George Hodan
https://www.publicdomainpictures.net/en/view-image.php?image=239649

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