PhaseSCA

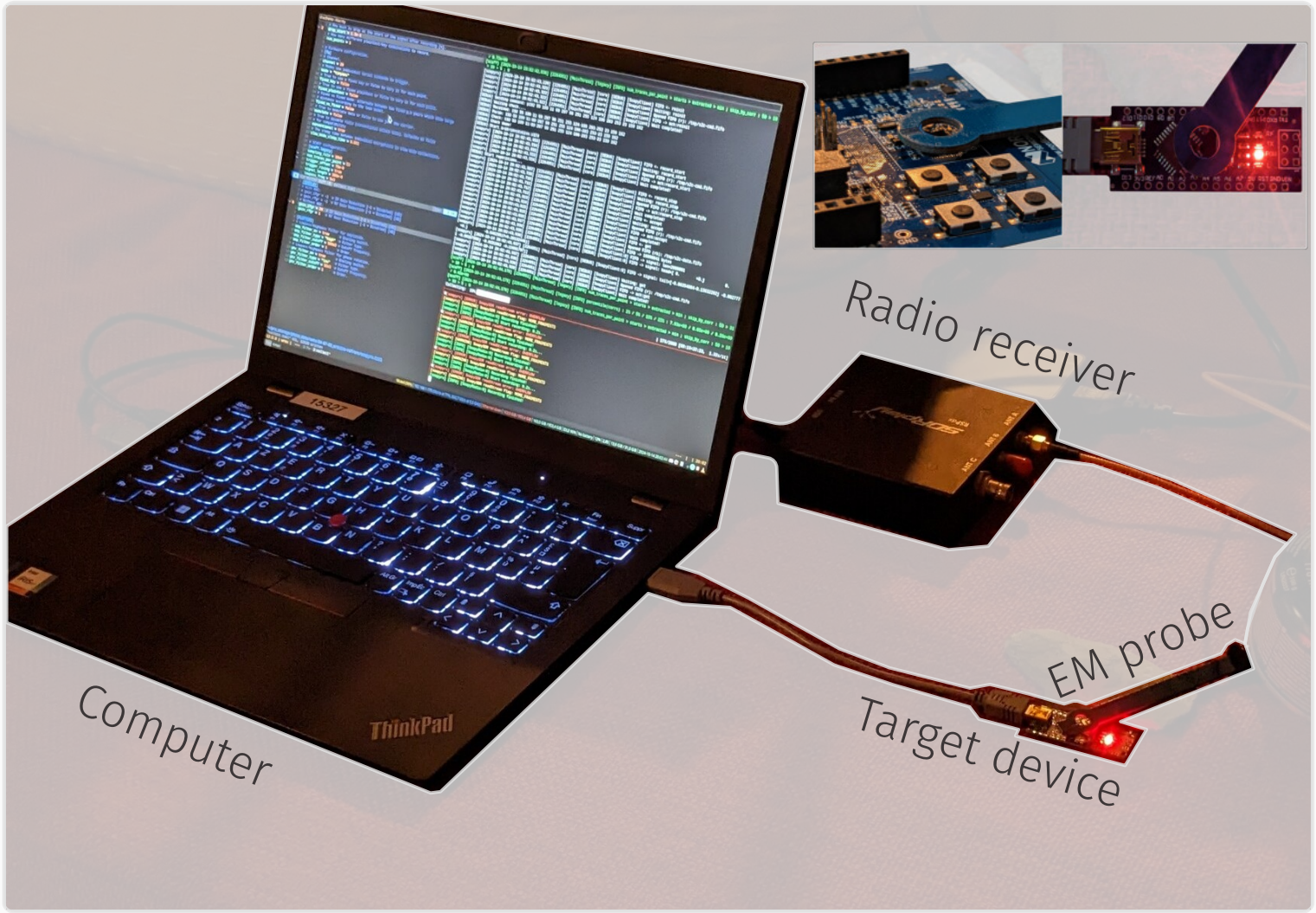
Exploiting Phase-Modulated Emanations in Side Channels

Toulouse Hacking Convention (THCon) April 10, 2025

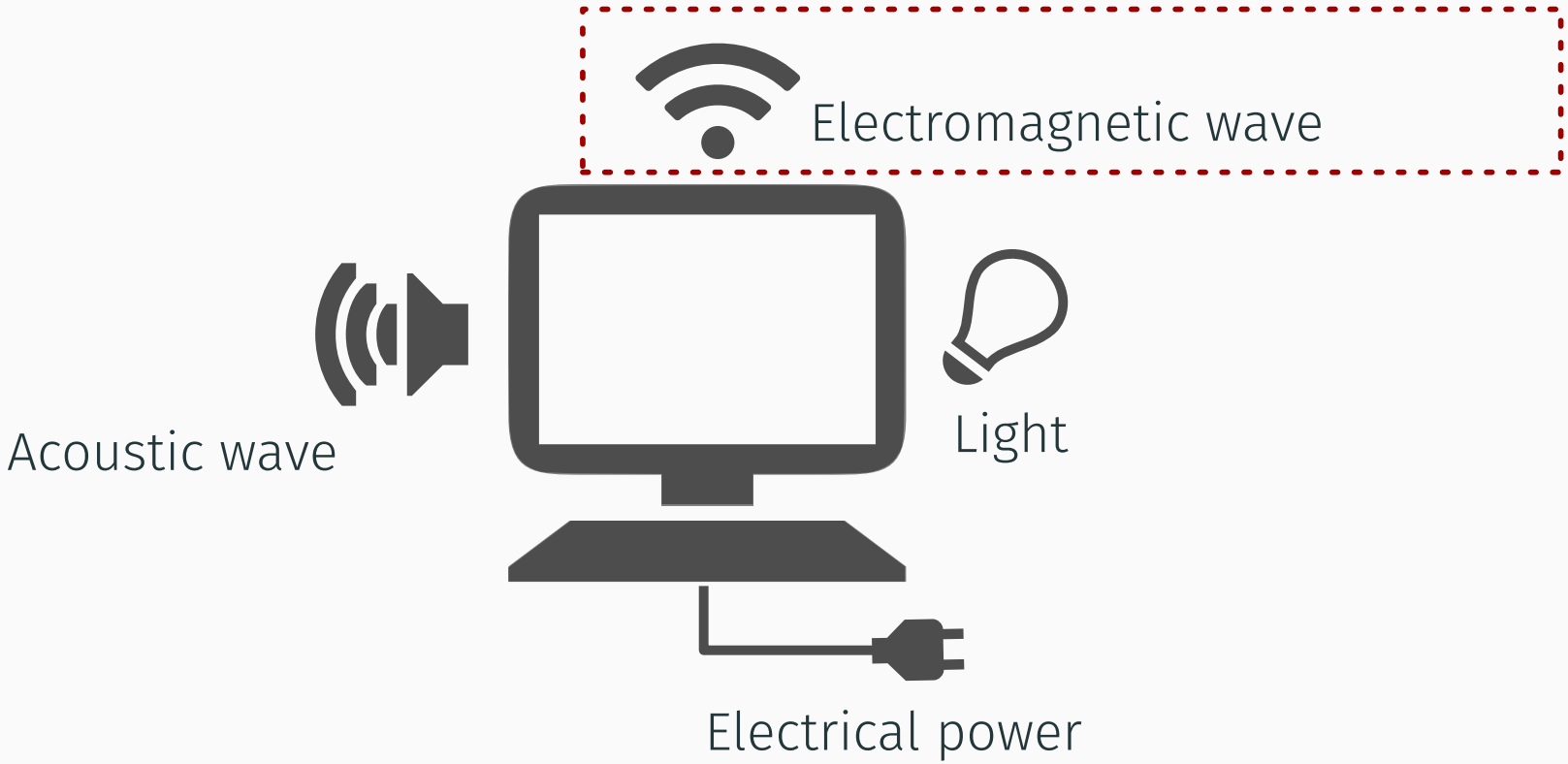
- ***Pierre Ayoub***
  LAAS-CNRS / EURECOM – Toulouse
- ***Aurélien Hernandez***
  EURECOM – Biot
- *Romain Cayre*
  LAAS-CNRS / EURECOM – Toulouse
- *Aurélien Francillon*
  EURECOM – Biot
- *Clémentine Maurice*
  Univ. Lille, CNRS, Inria – Lille

Introduction

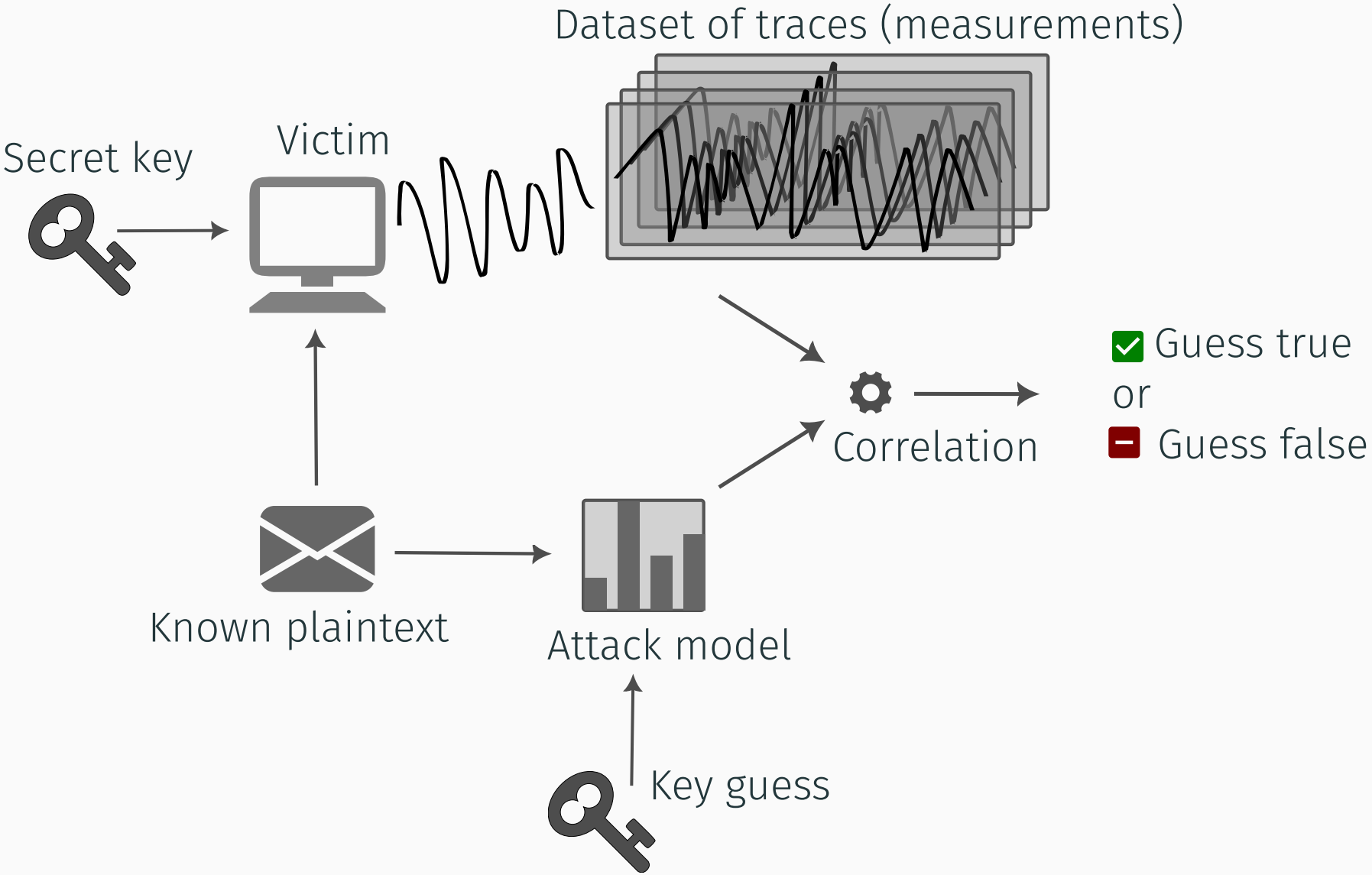
EM side-channel attack



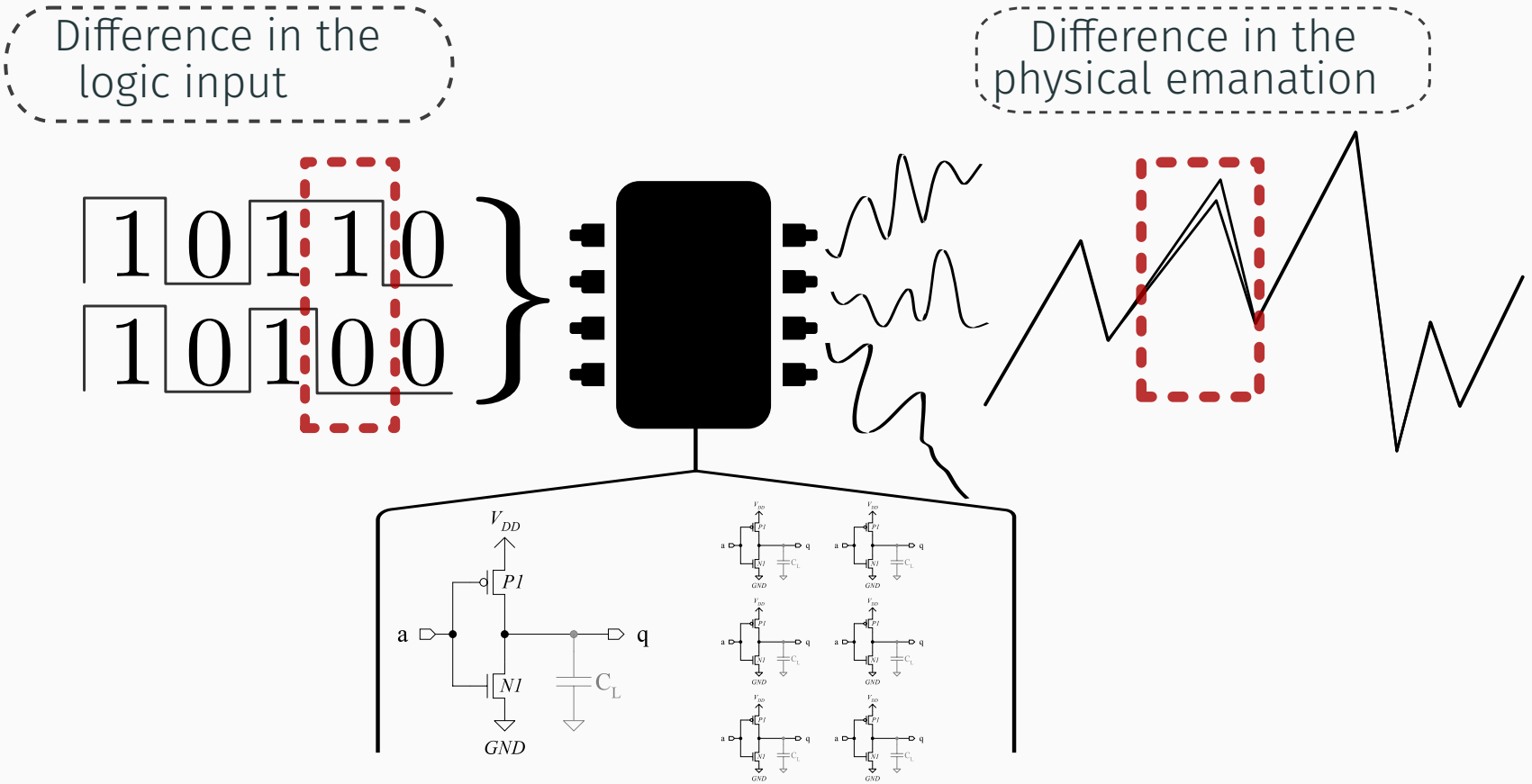
Unintentional Emanations



Example of a Side-Channel Attack



Compromising Emanations



Overview

Contribution

Demonstrating a novel side-channel leakage source through unintended phase modulation of electromagnetic signal

Outline

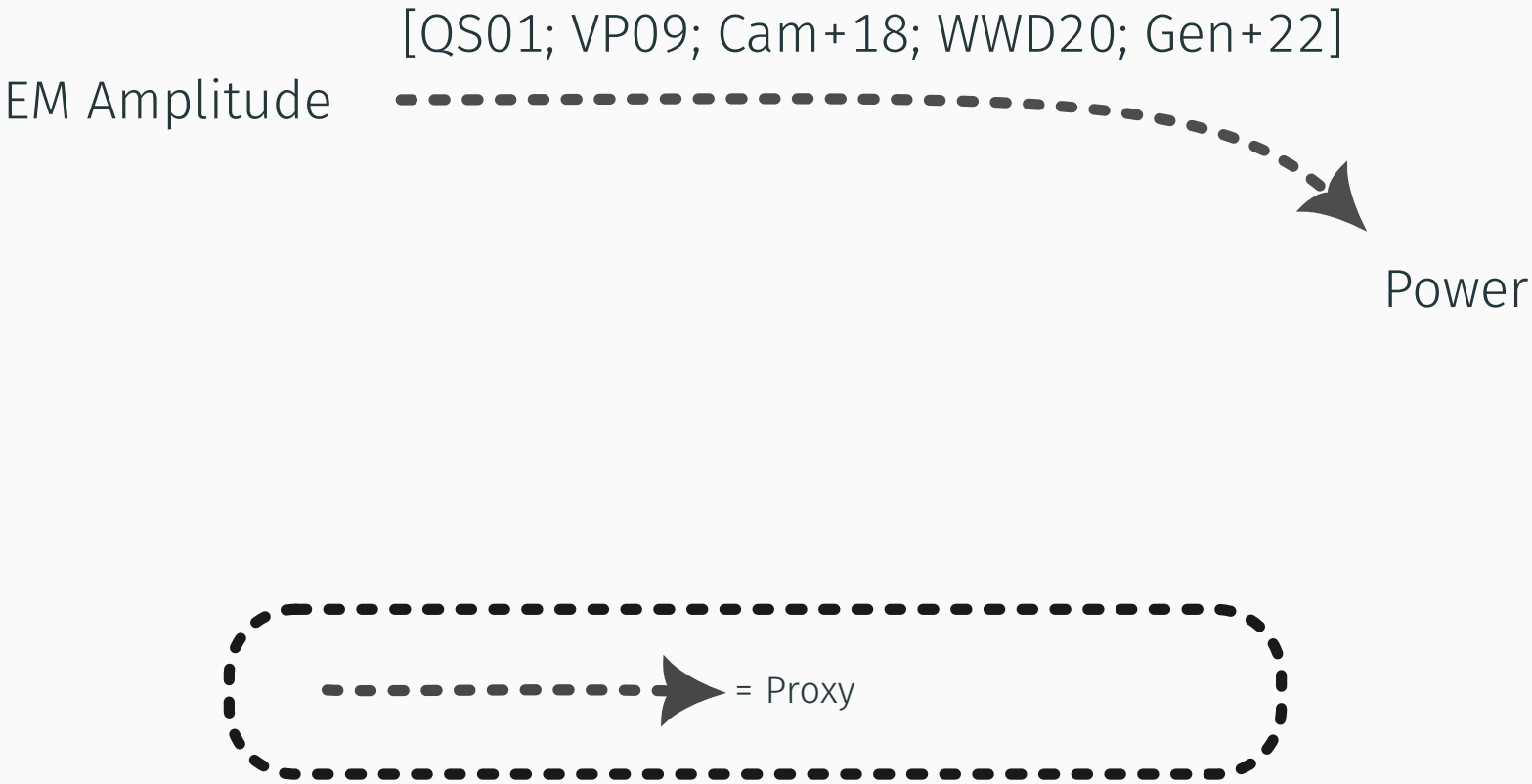
1. Exploitation of phase in side channels
2. Analysis of the root cause phenomenon

Exploitation of Phase-modulated Side Channels

Exploitation of Phase-modulated Side Channels

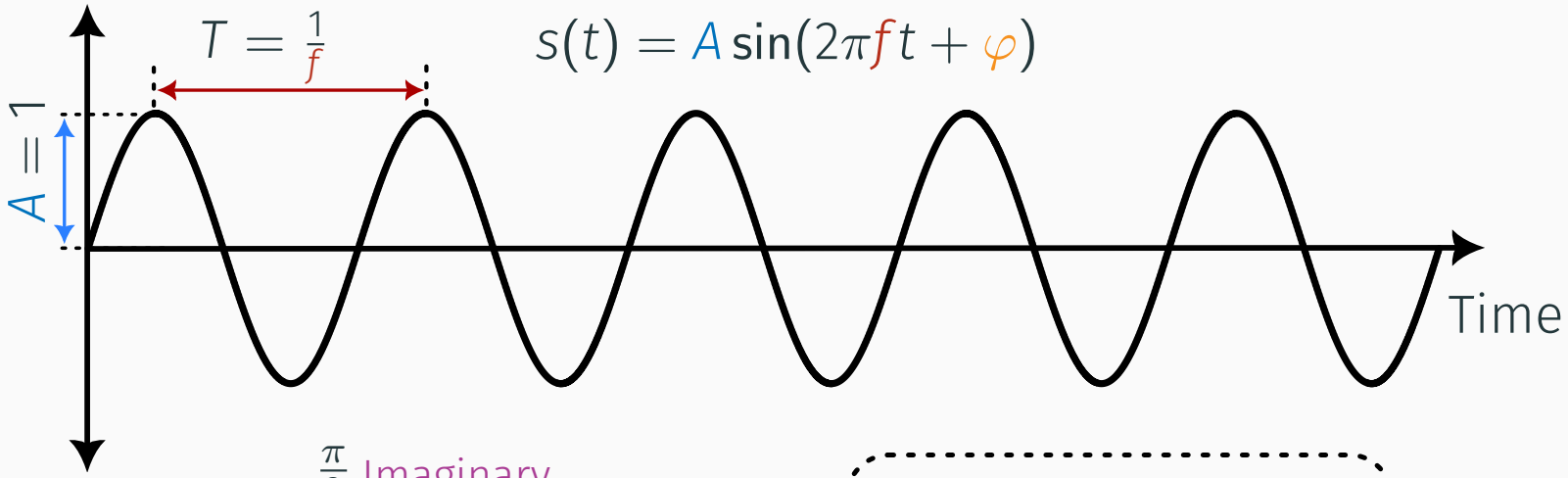
Amplitude-modulated Emanations to Side-channel Trace

Proxy Traces – From Amplitude to Power



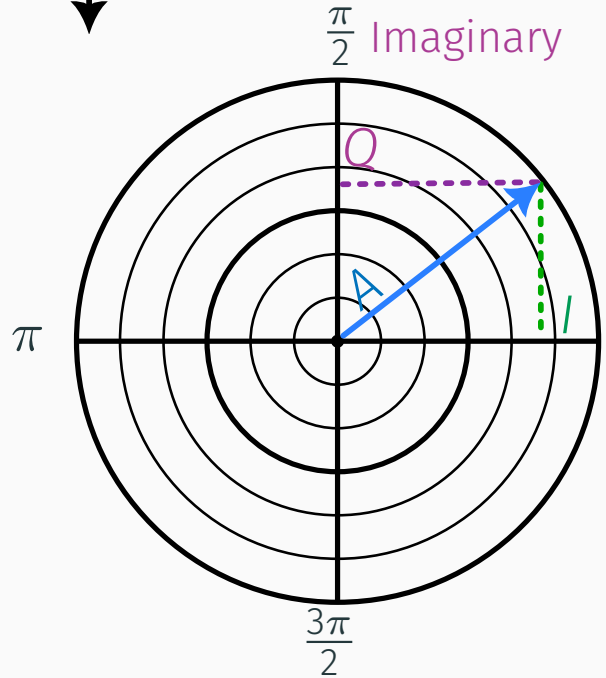
Amplitude in Signal Representation

Real-valued signal



Complex-valued signal

(analytic representation)



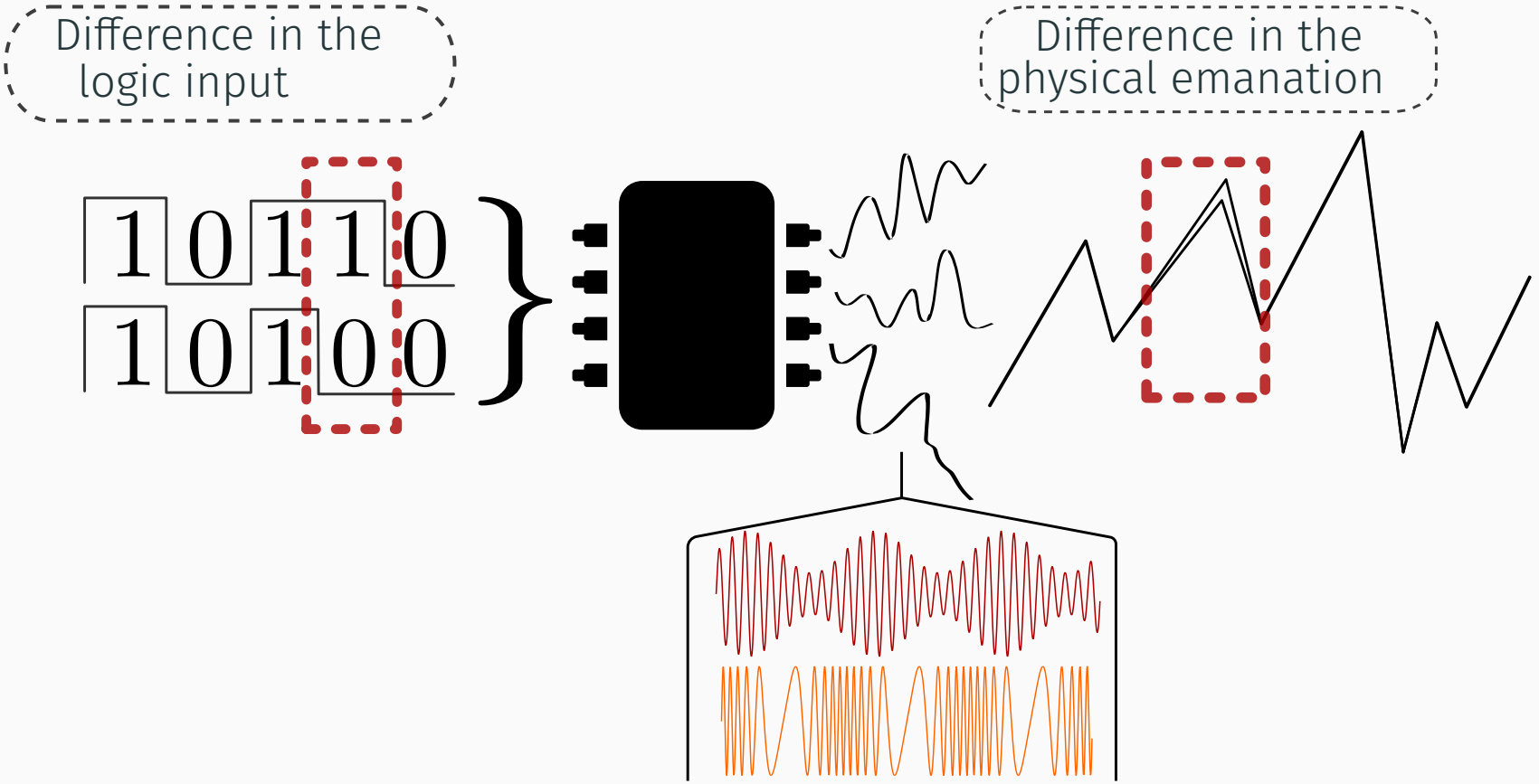
$$s(t) = I\cos(2\pi f t) + Q\sin(2\pi f t)$$
$$x_i = I + jQ$$

Simple SDR receiver Architecture

Various Software-Defined Radios (from 20$ to 1000$)

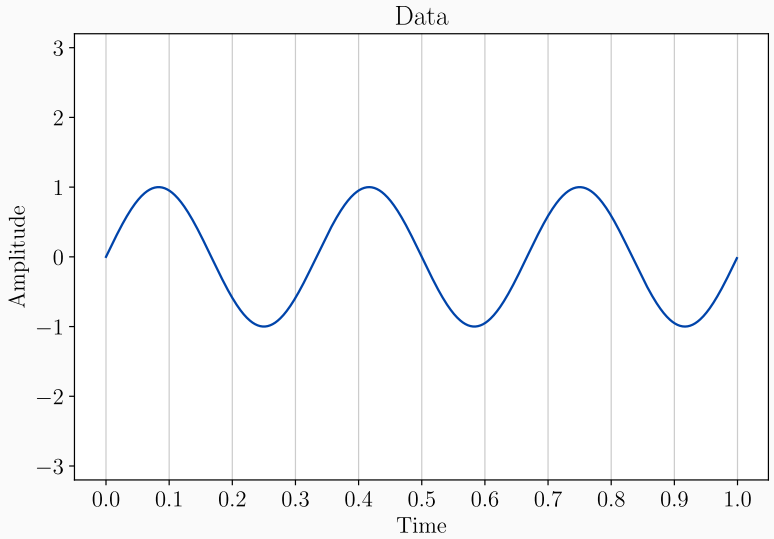
Simple SDR receiver Architecture

Modulations in Compromising Emanations



In EM side channels, **message** is related to the **secret**, **carrier** can be a **digital clock** for example

Amplitude Modulation (AM)

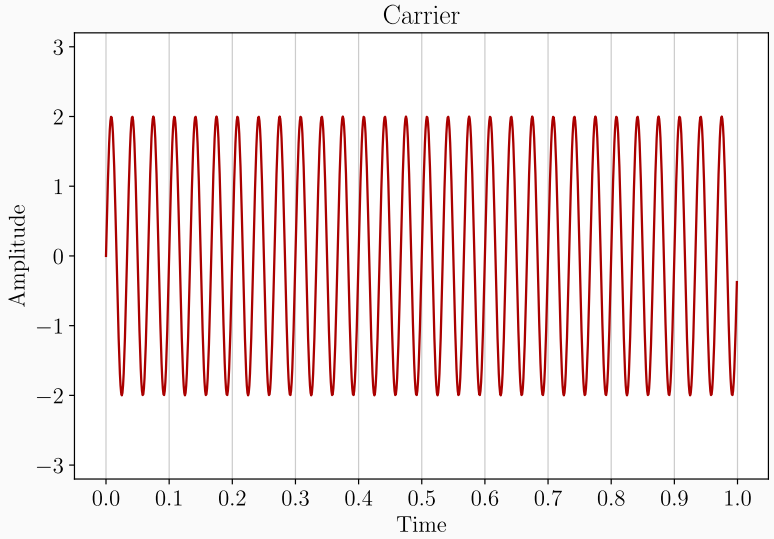


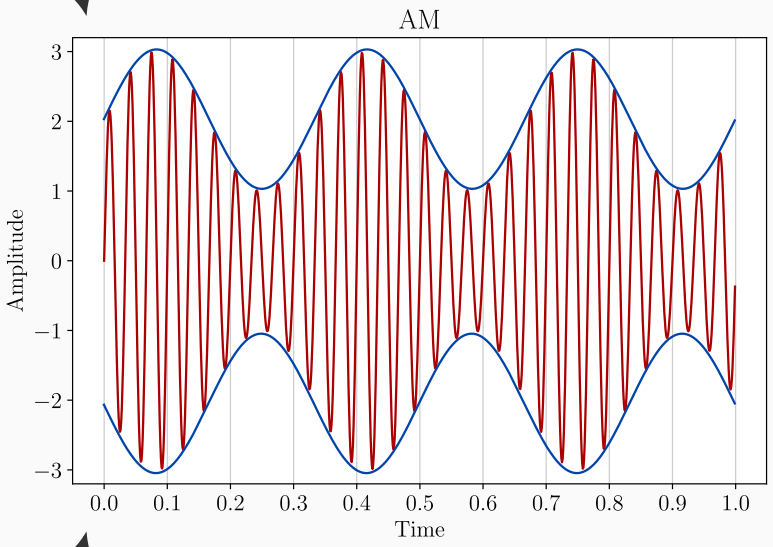
Message (Baseband):

$m(t) = A_m \sin(2\pi f_m t + \varphi_m)$

Amplitude-modulated carrier (Bandpass):

$y(t) = [A_c + m(t)]\sin(2\pi f_c t + \varphi_c)$





Carrier (Bandpass):

$c(t) = A_c \sin(2\pi f_c t + \varphi_c)$

Summarizing

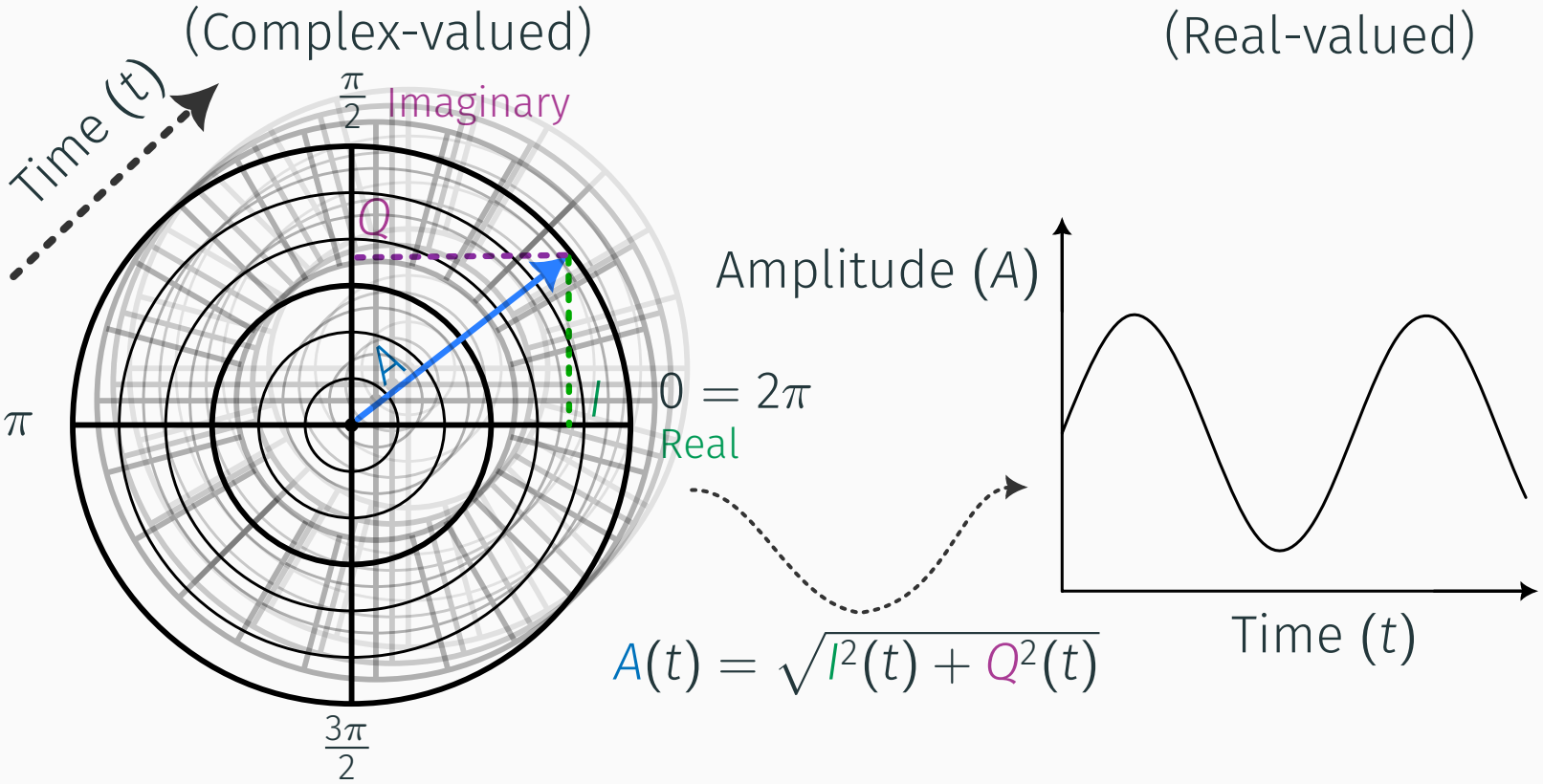
We know...

- How to represent a signal
- How to measure a signal
- How information is embedded inside a signal

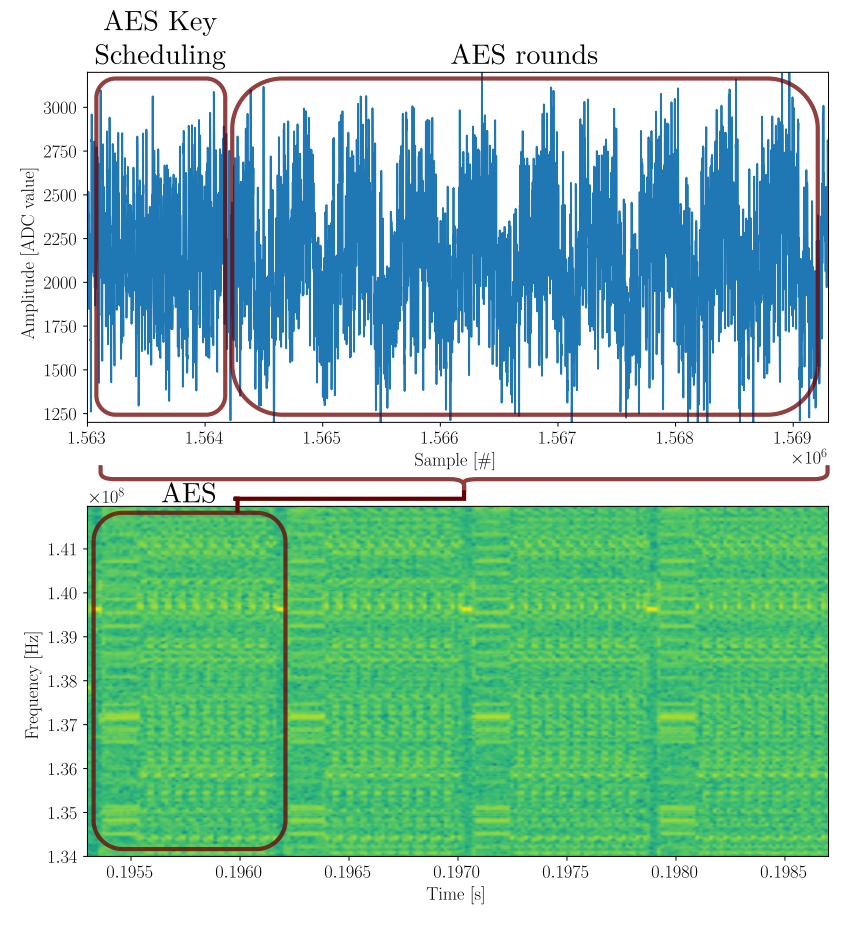
We can now...

1. Acquire our signals
2. Demodulate them
3. Perform a side-channel attack

Amplitude Trace Computation



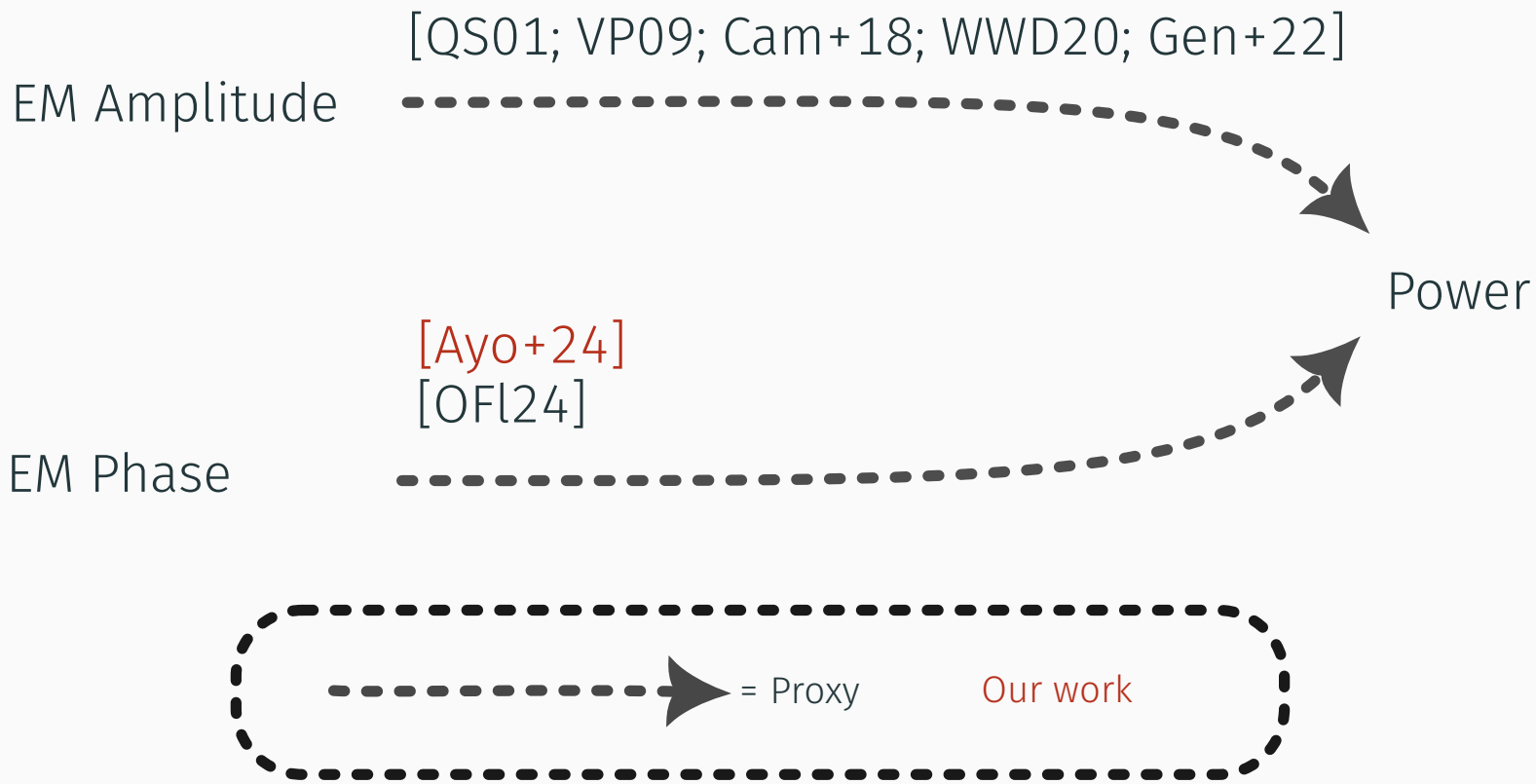
Visualizing AES in Amplitude Trace



Exploitation of Phase-modulated Side Channels

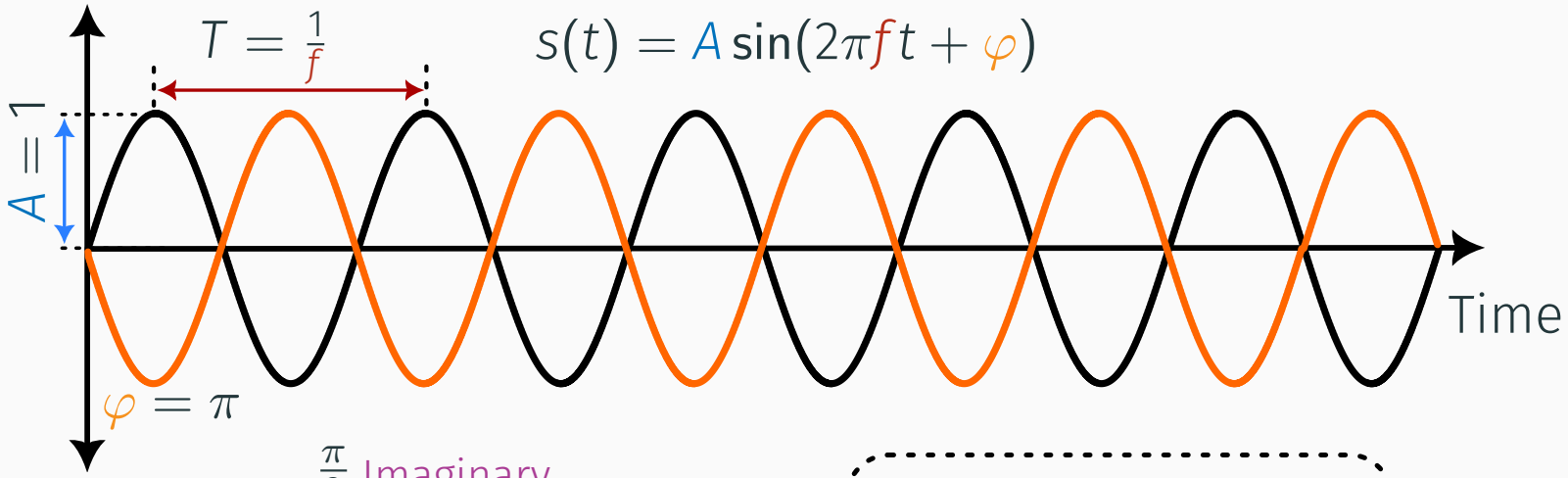
Phase-modulated Emanations to Side-channel Trace

Proxy Traces – From Phase to Power



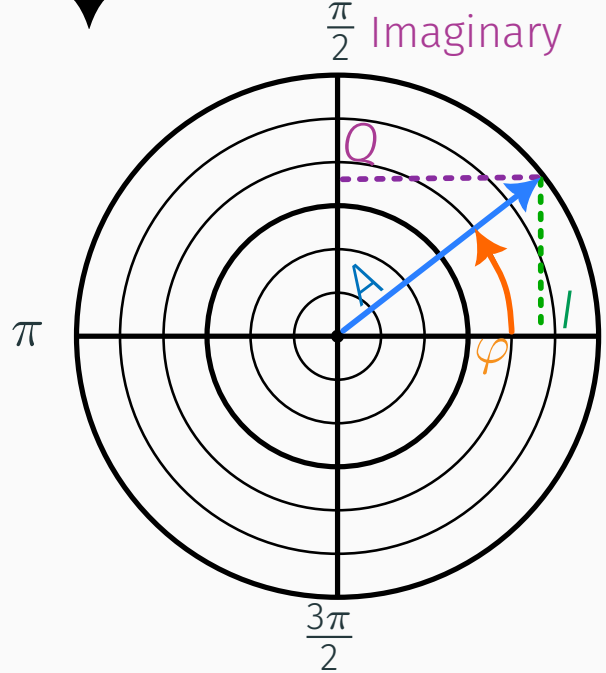
Phase in Signal Representation

Real-valued signal



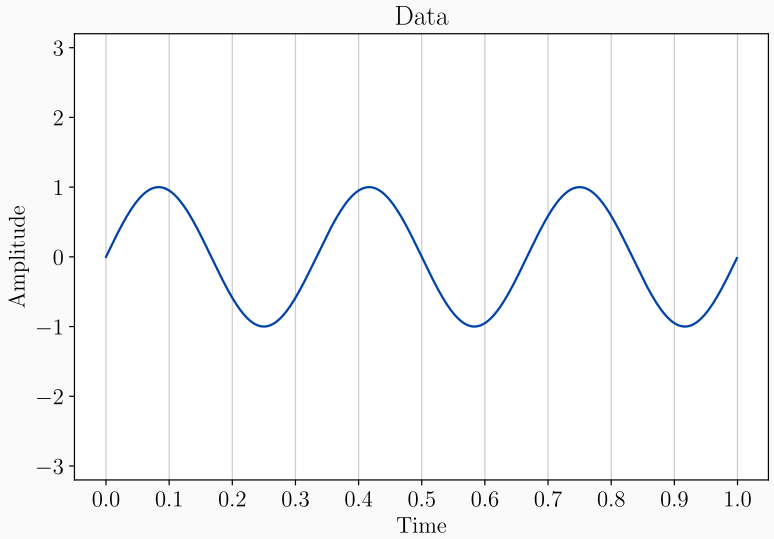
Complex-valued signal

(analytic representation)



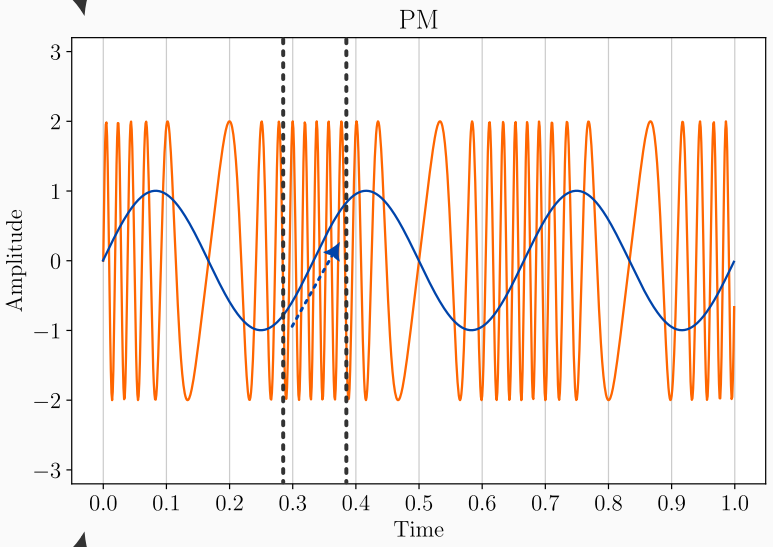
$$s(t) = I\cos(2\pi f t) + Q\sin(2\pi f t)$$
$$x_i = I + jQ$$

Phase Modulation (PM)



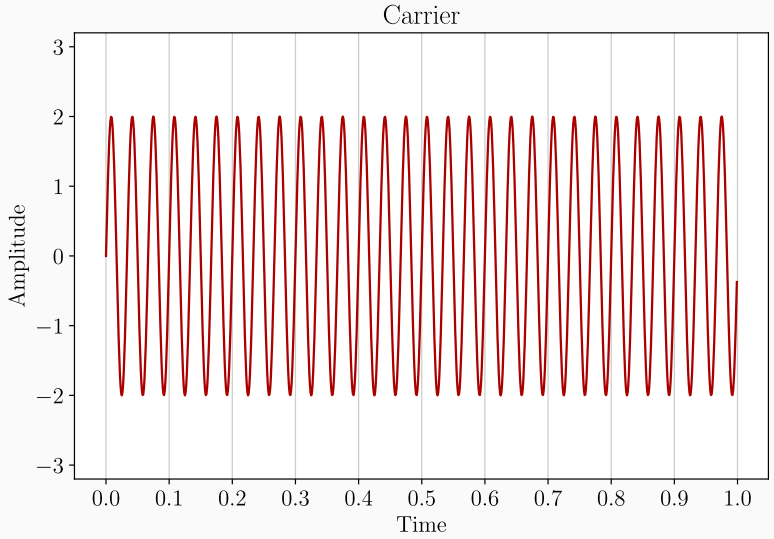
Message (Baseband):

$m(t) = A_m \sin(2\pi f_m t + \varphi_m)$



Phase-modulated carrier (Bandpass):

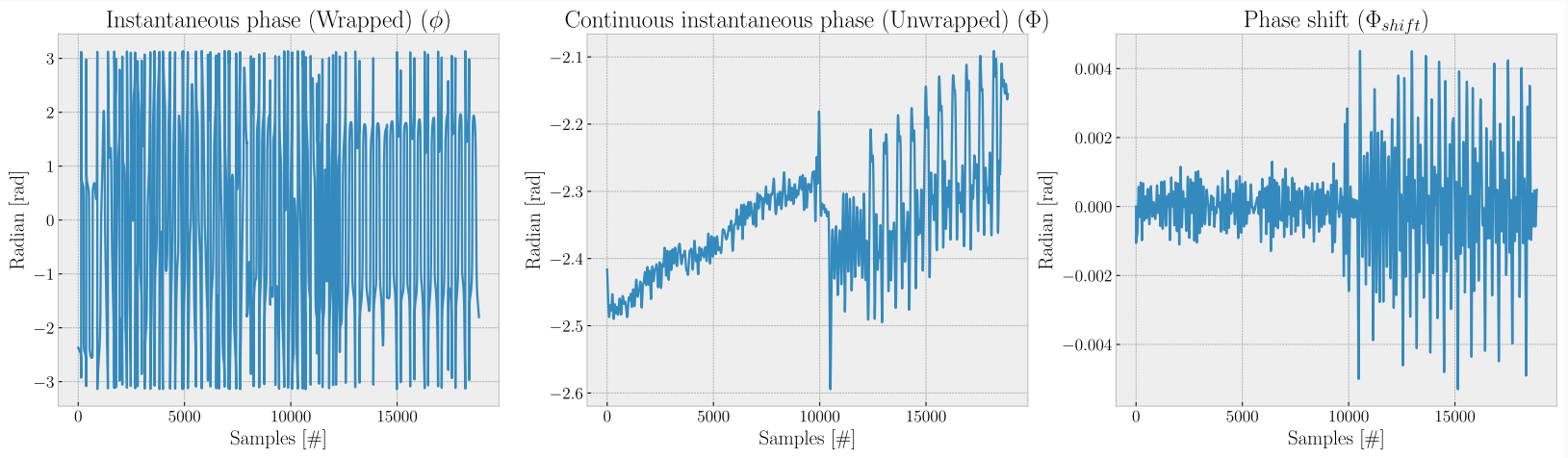
$y(t) = A_c \sin(2\pi f_c t + \varphi_c + m(t))$



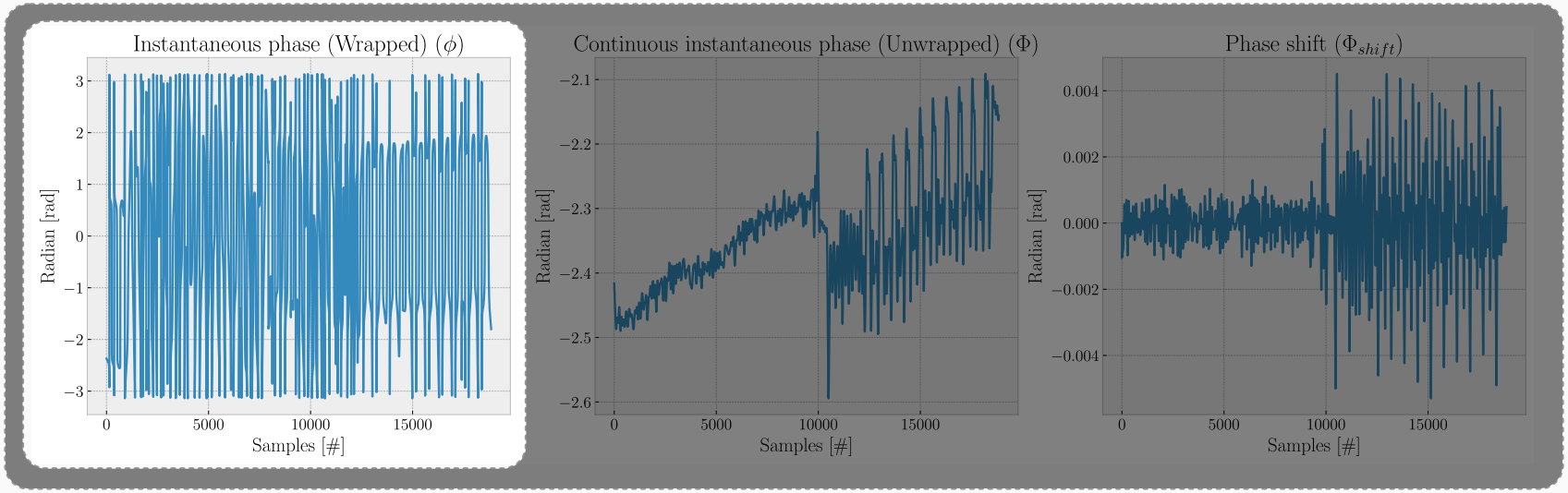
Carrier (Bandpass):

$c(t) = A_c \sin(2\pi f_c t + \varphi_c)$

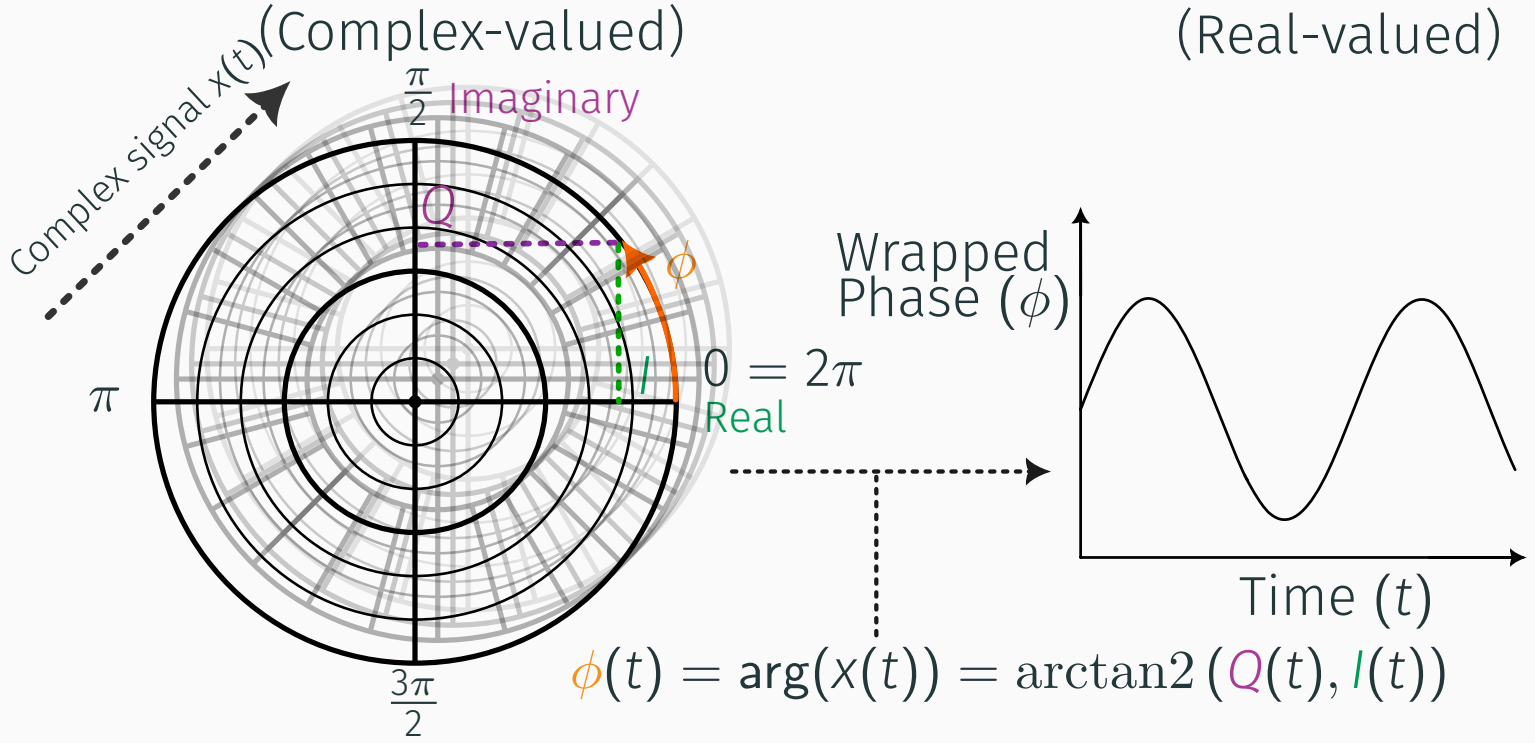
Phase Trace Computation: Step 1



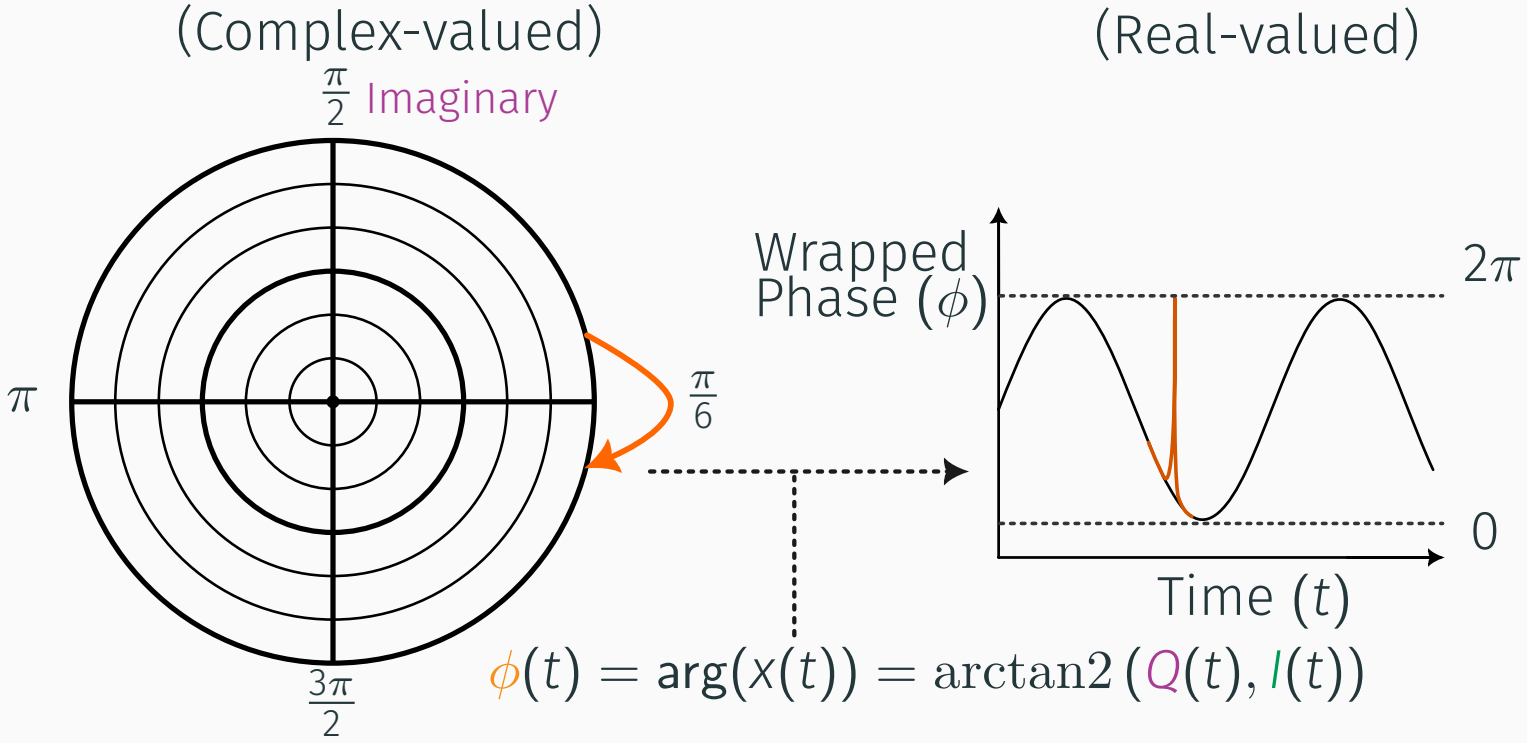
Phase Trace Computation: Step 1



Step 1: Instantaneous Phase



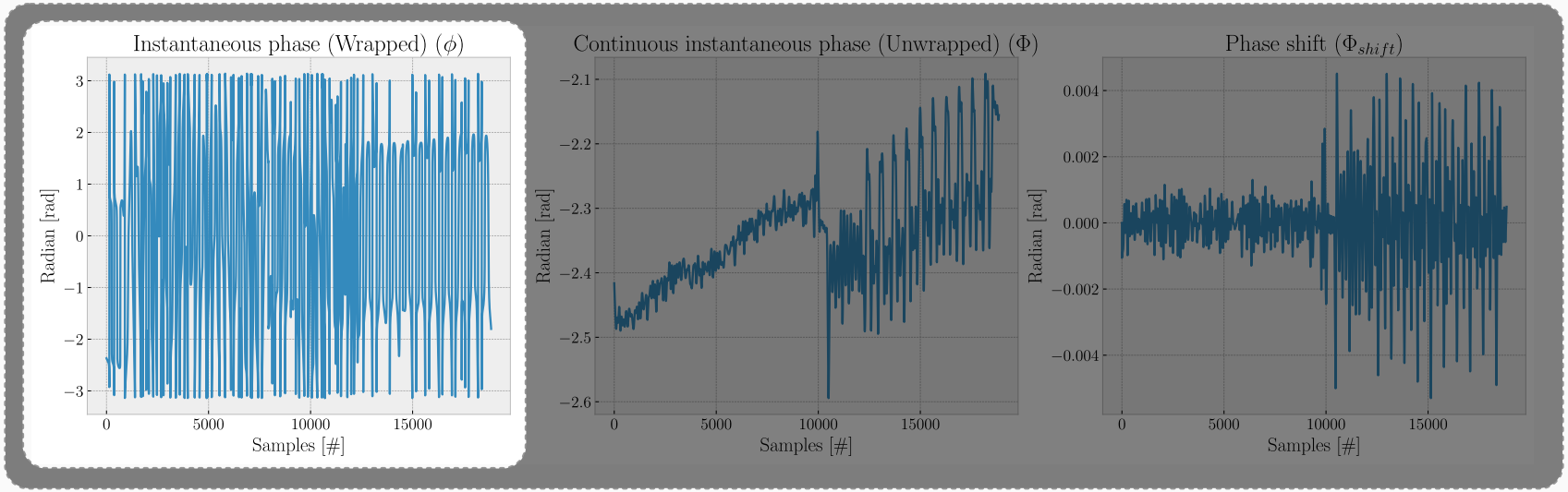
Step 1: Instantaneous Phase

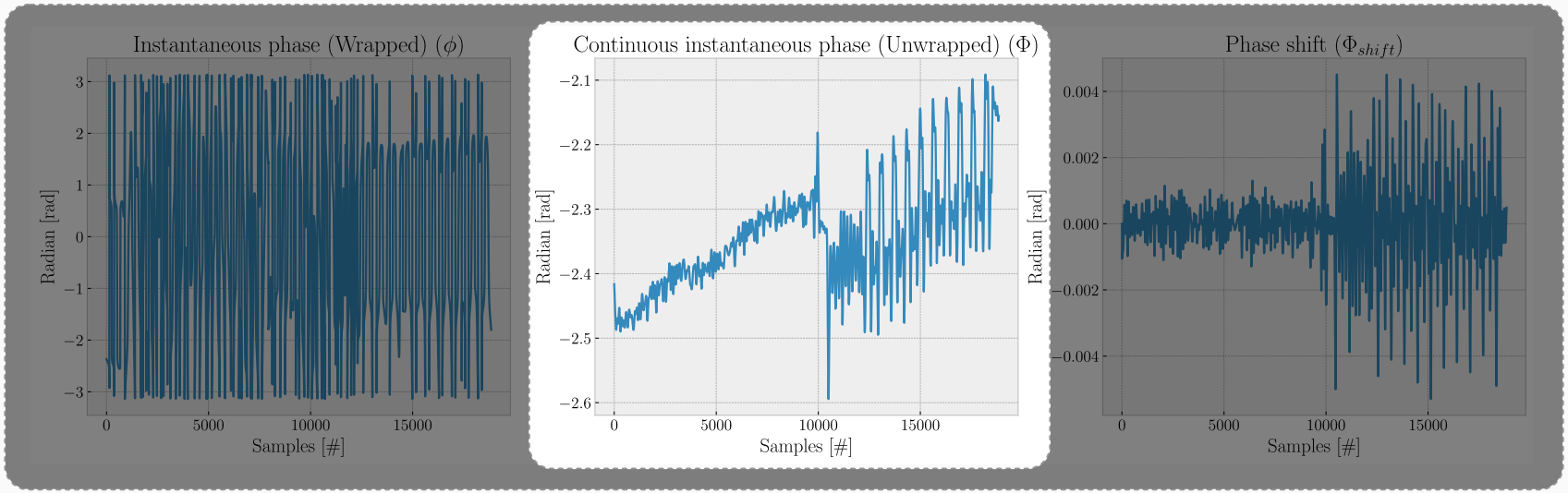


Problem

- Due to cyclic nature of phase measurement, discontinuities happens in the real-valued trace
- Not comparable across measurement

Phase Trace Computation: Step 2



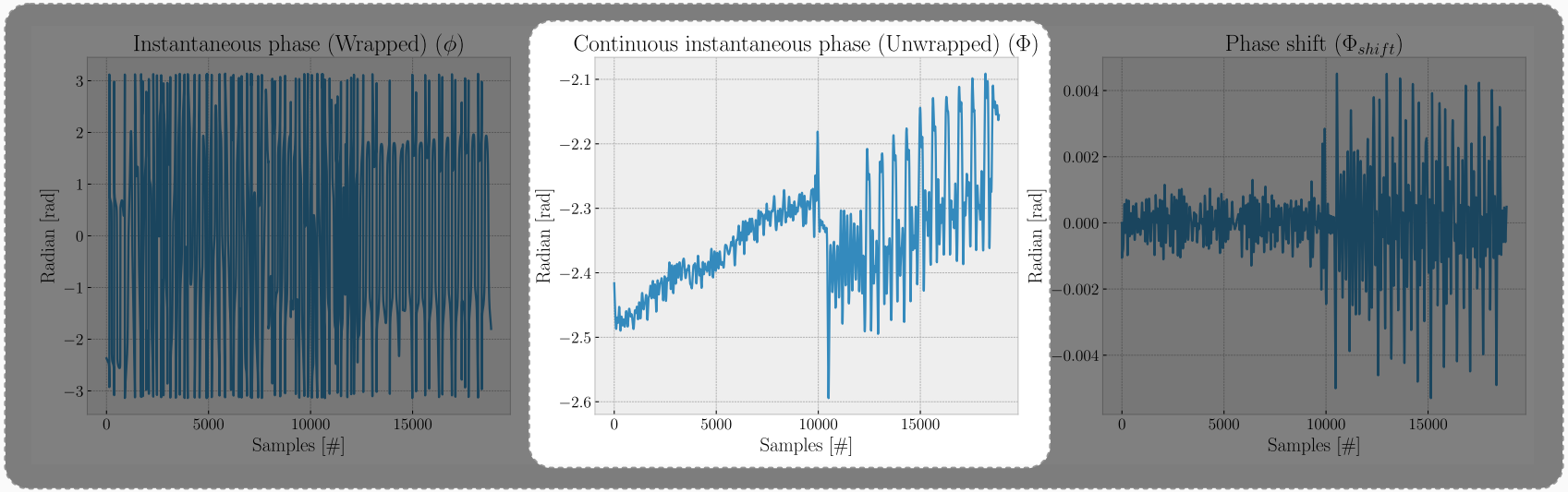


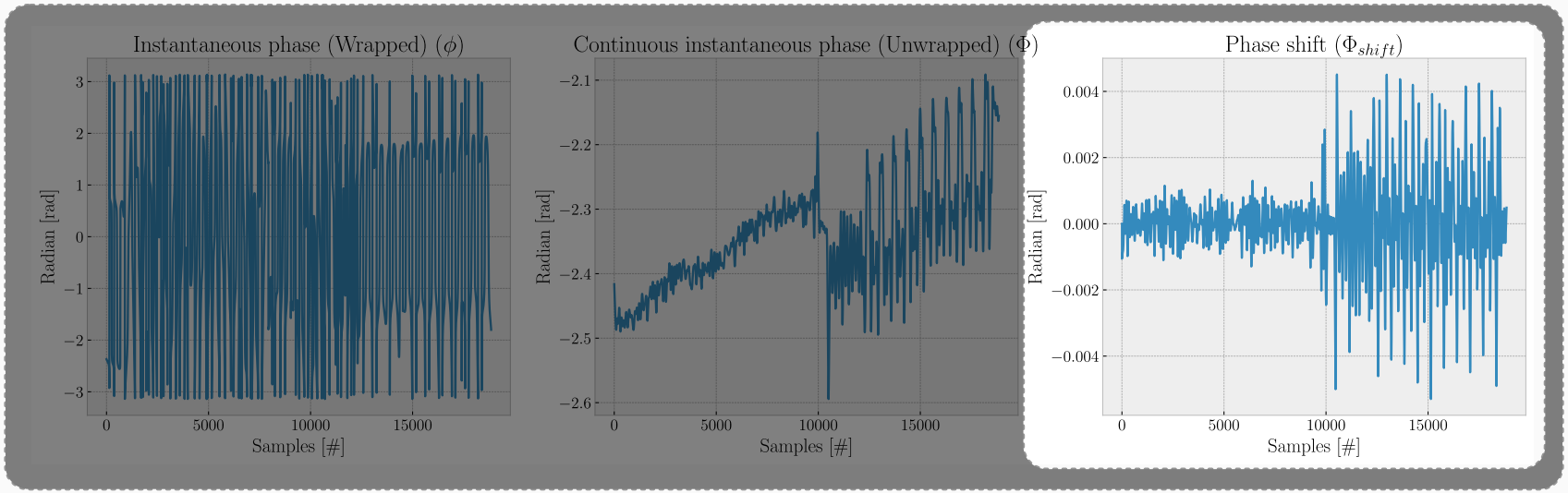
Step 2: Continuous Instantaneous Phase

$$\Phi(t) = \phi(t) + k(t)2\pi$$

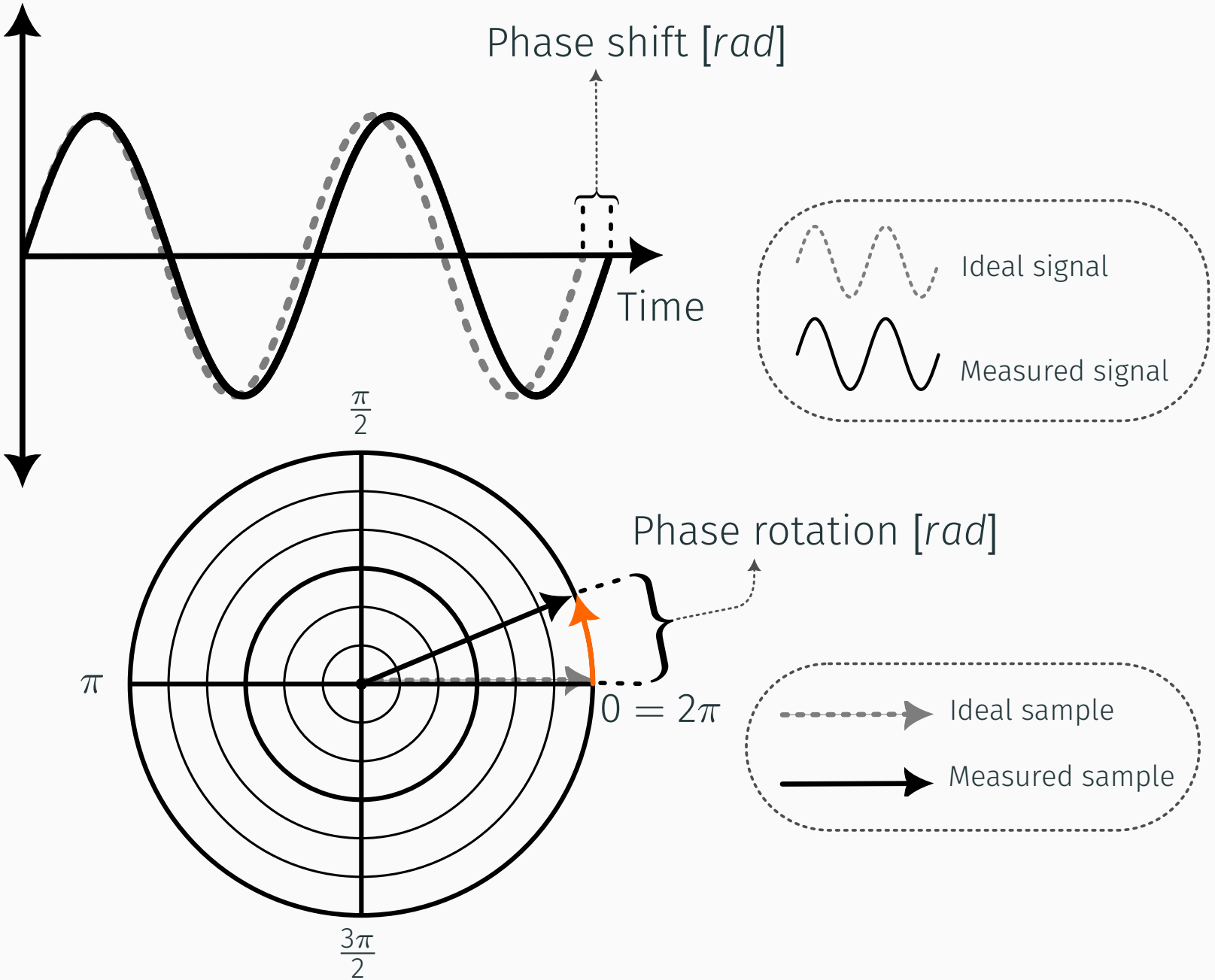
- $k \in \{0, 1, 2, ...\}$ increased for each 2π discontinuity
- $\Phi(t)$ cumulative function (not constrained to the 2π principal-values)

Phase Trace Computation: Step 3





Phase Shift and Phase Rotation

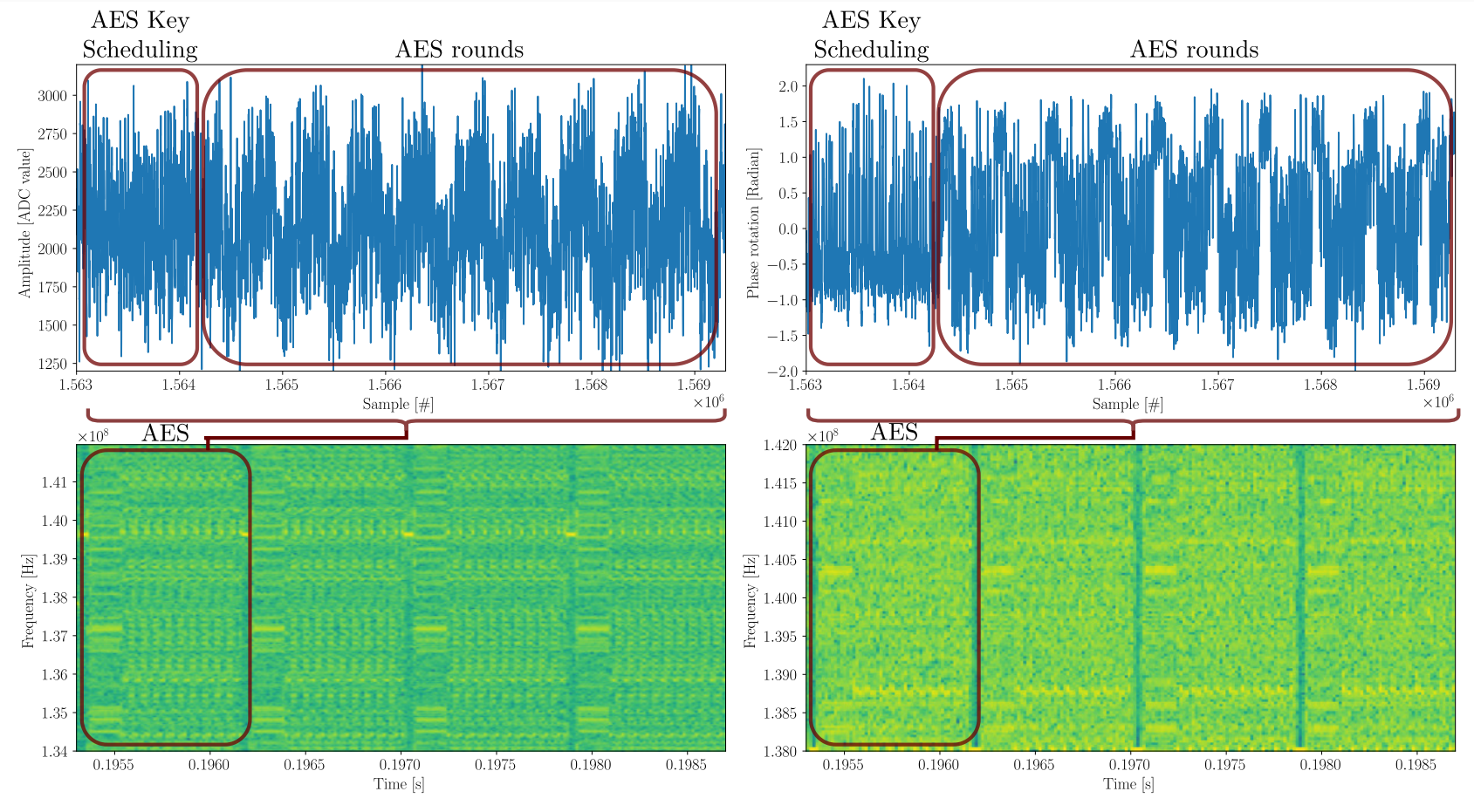


Step 3: Phase Shift Analysis

$$\Phi_{shift}(t) = \frac{d\Phi}{dt}(t) = \begin{cases} 0, & \text{if } t = 0 \\ \Phi(t) - \Phi(t-1), & \text{otherwise} \end{cases}$$

- Compute the **first derivative** (numerical differentiation)
- $\rightarrow$ Phase shift between two samples

Visualizing AES in a Phase Shift Trace



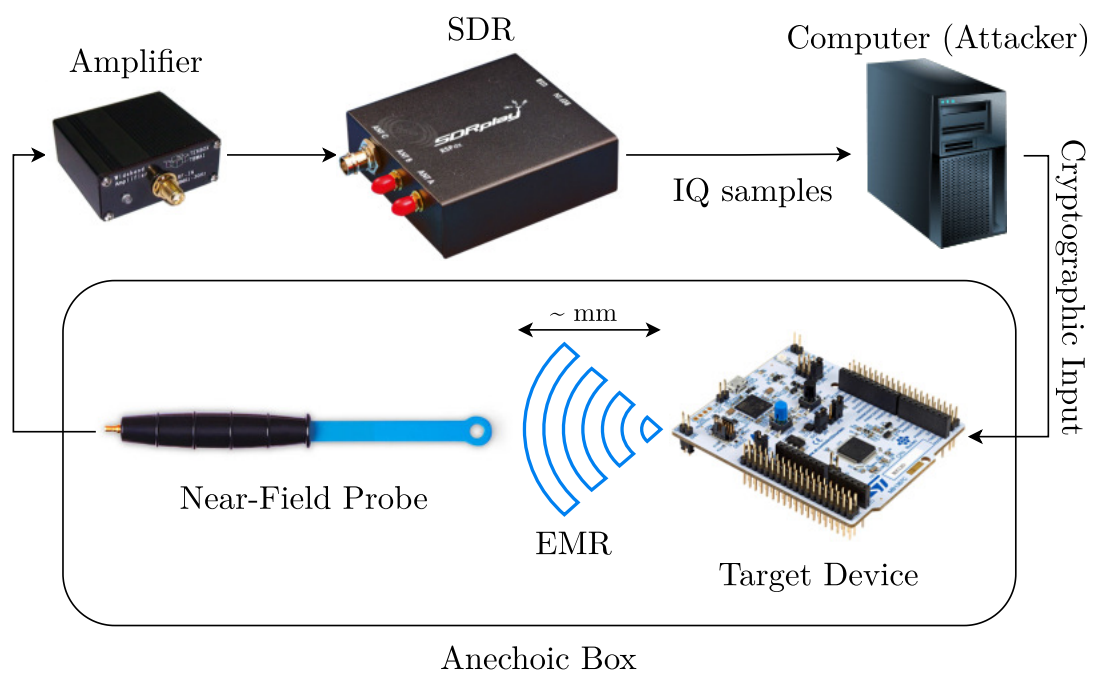
AES trace in amplitude (left) and phase shift (right)

Captured from an nRF52832 using a near-field probe connected to an SDR tuned at 2nd clock harmonic

Exploitation of Phase-modulated Side Channels

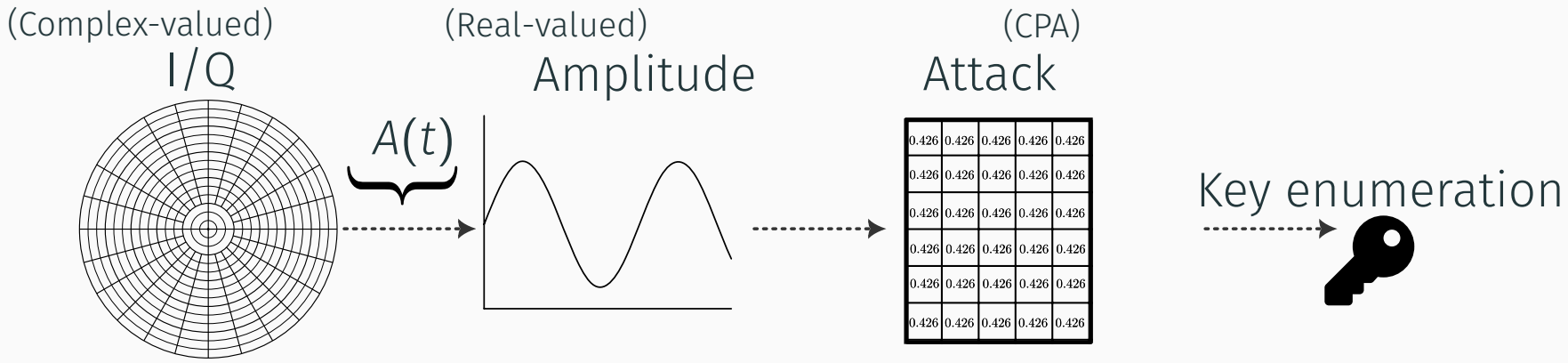
Exploitation

Experimental Setup for Side-Channel Attack

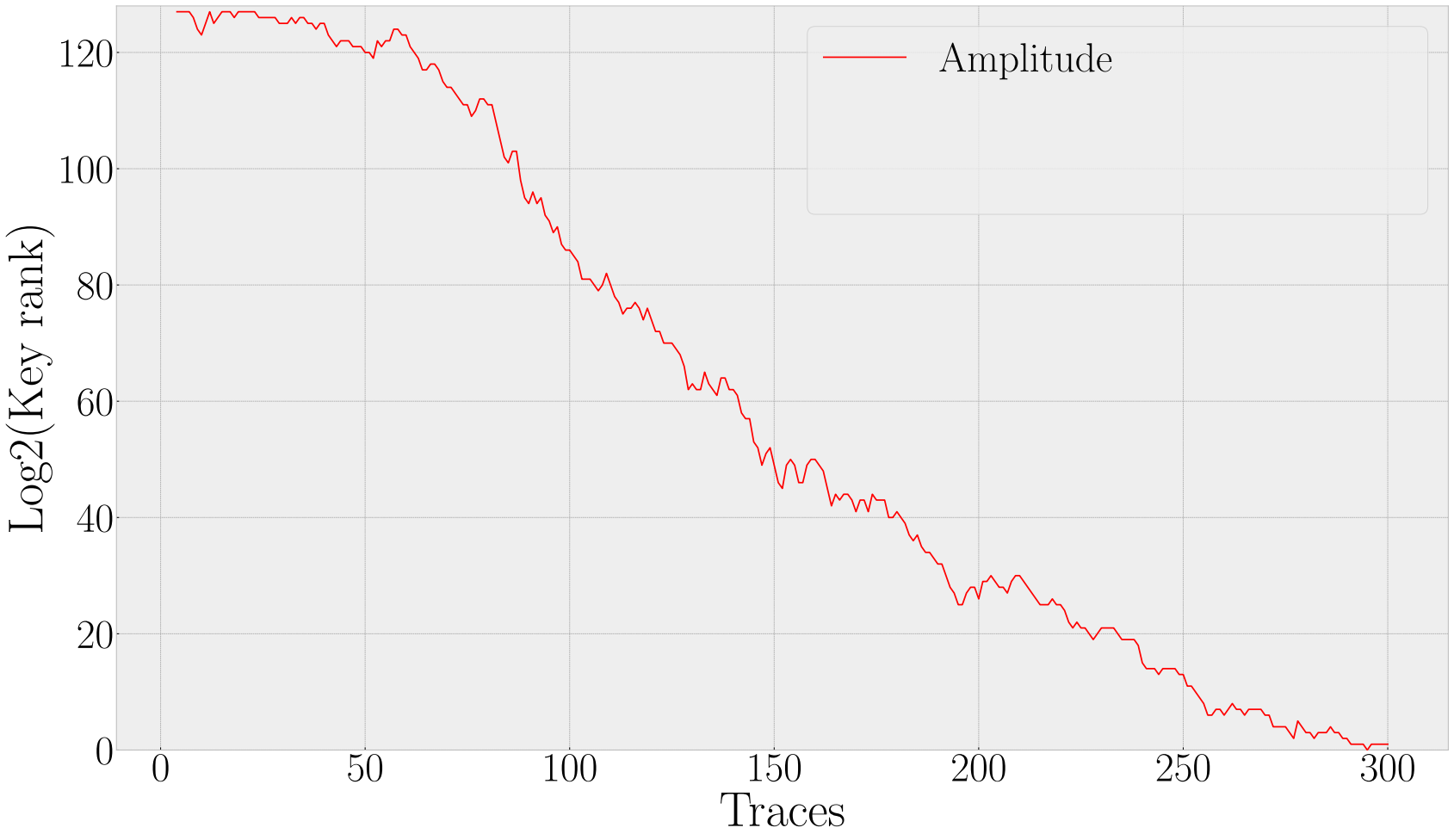


SoC	Board
STM32L1	NUCLEO-L152RE
nRF52832	PCA10040
nRF51422	PCA10028
ATmega328	Arduino Nano
RP2040	Raspberry Pi Pico

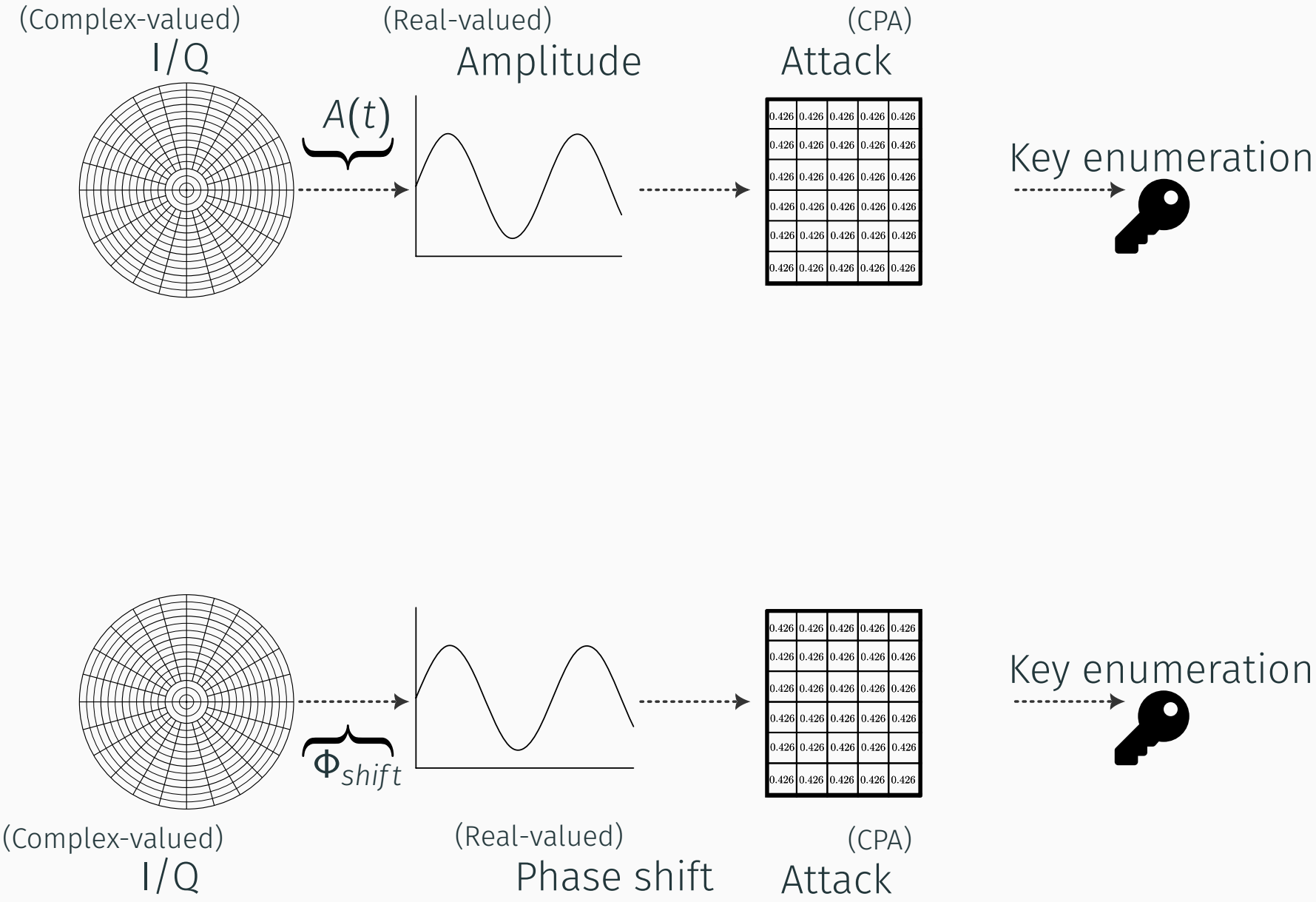
Mono-Channel Attack using Amplitude



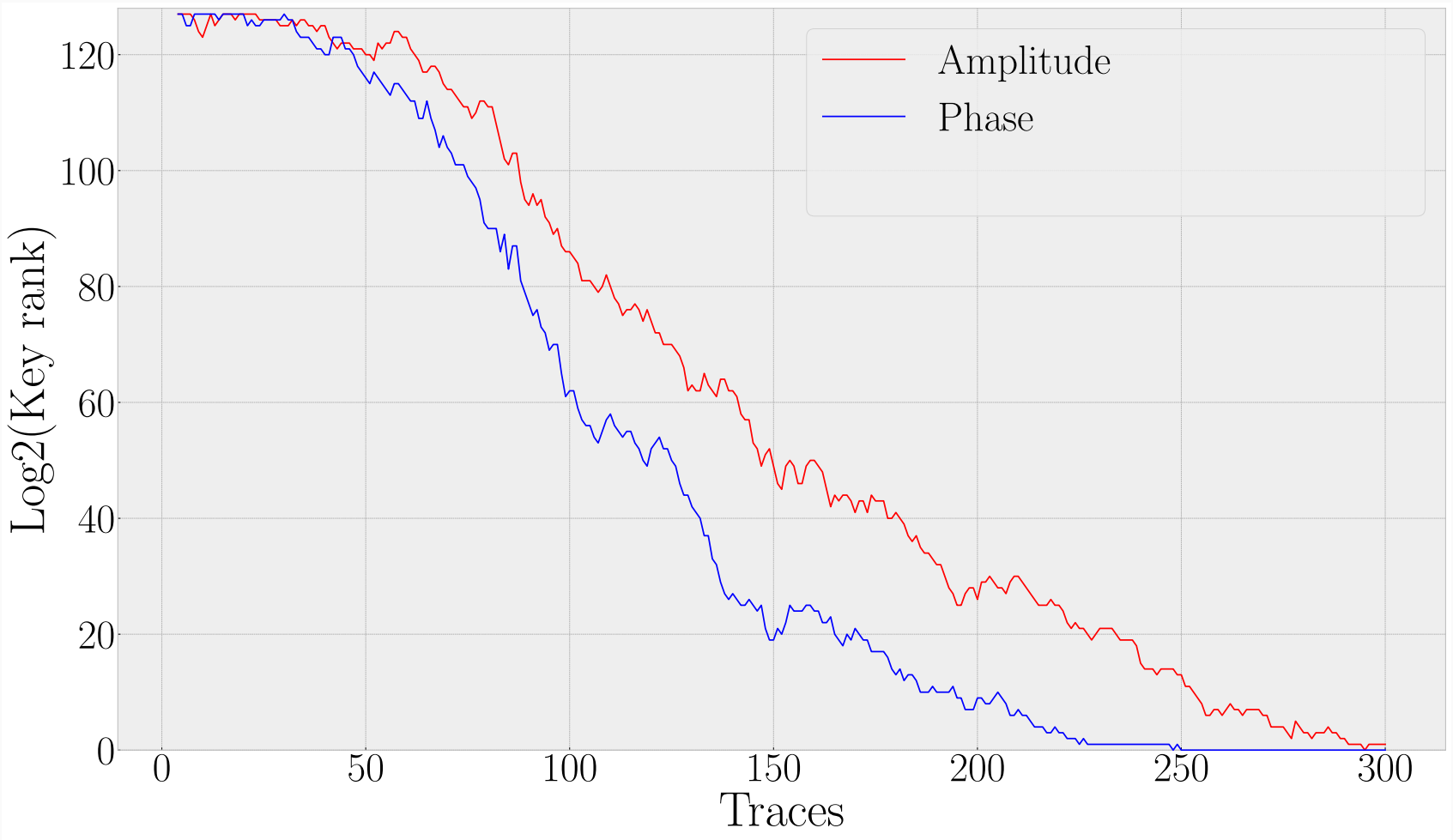
Non-Profiled Side-Channel Attack on nRF52



Mono-Channel Attack using Phase Shift



Non-Profiled Side-Channel Attack on nRF52



Multi-Channel Attack

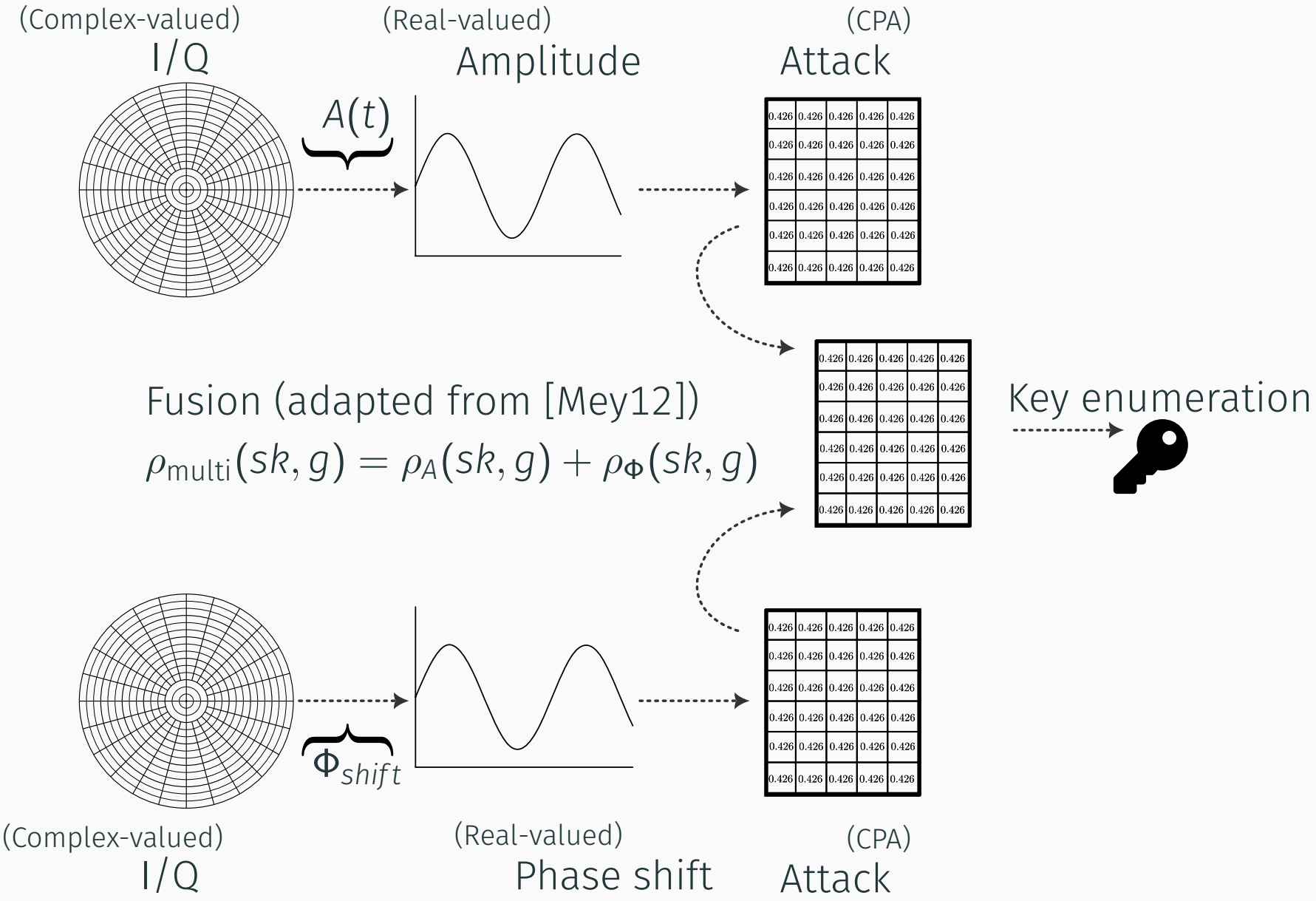
Questions

1. Are the **information** on amplitude and the phase identical?
2. If not, could we recombine it?

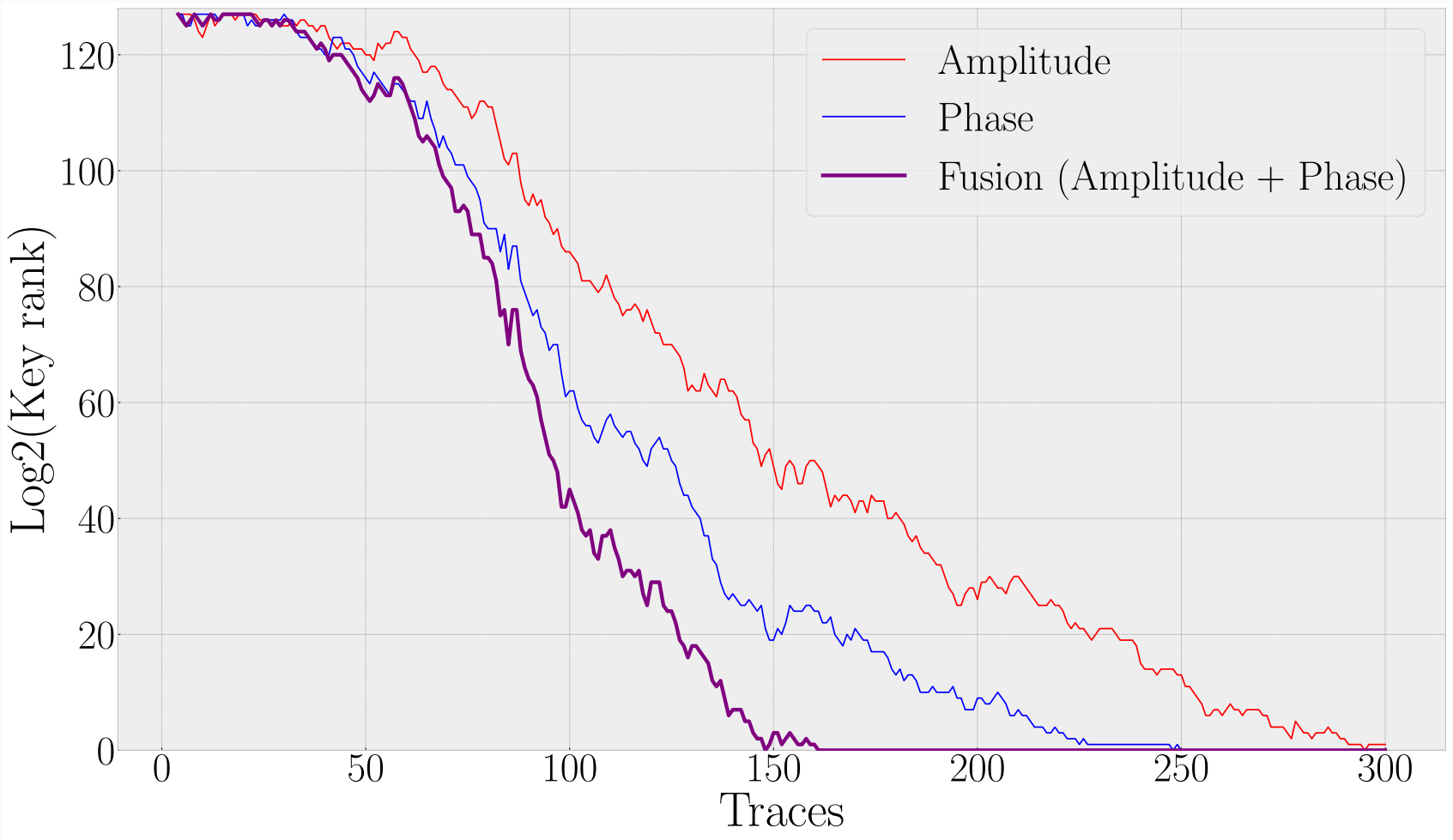
Solution

Multi-channel attacks are to side channels what diversity is to radio communications

Multi-Channel Attack



Non-Profiled Side-Channel Attack on nRF52

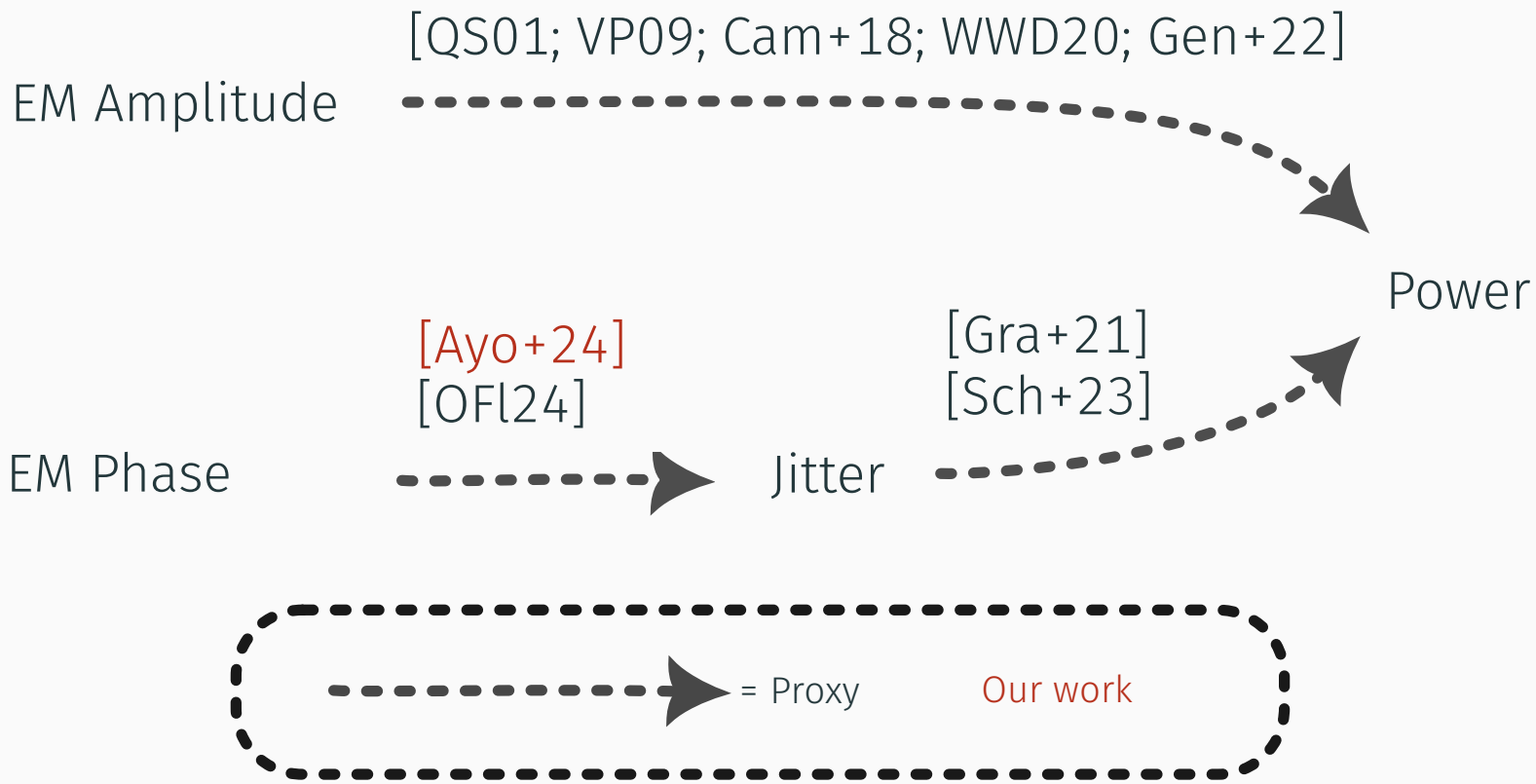


Root-cause characterization

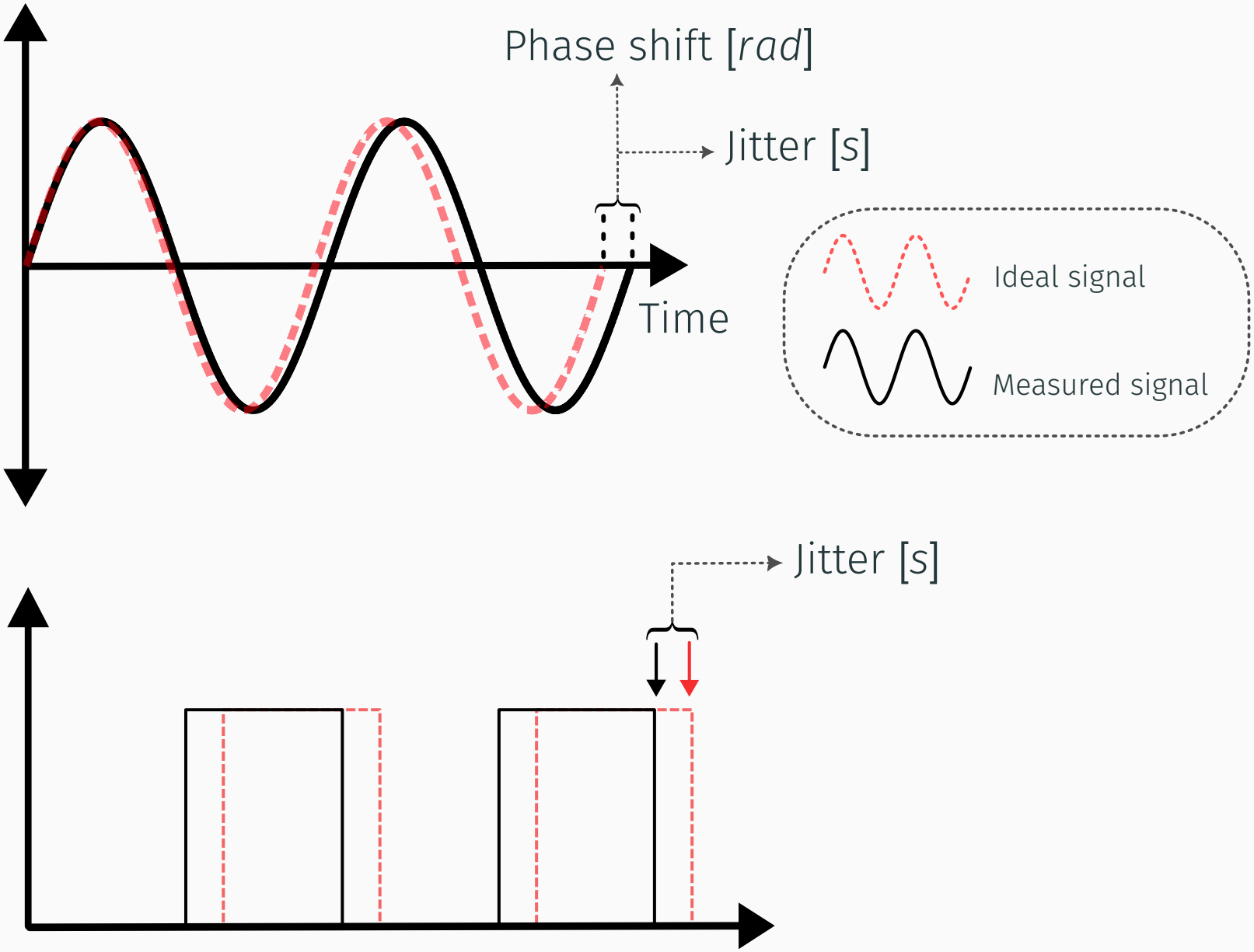
Root-cause characterization

Hypotheses

Phase to CPU Power: Something is Missing



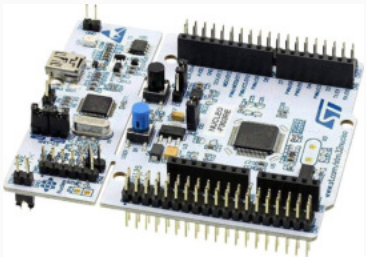
Phase to Jitter Equivalence

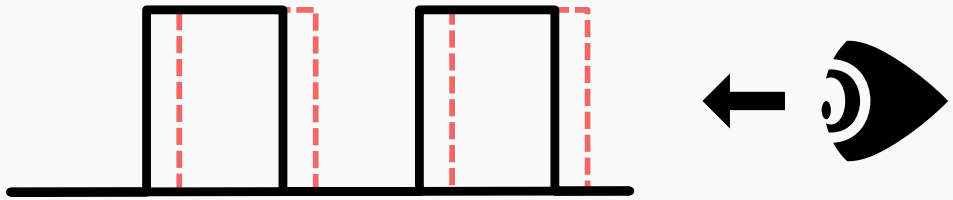


State-of-the-Art: Jitter Side-Channels

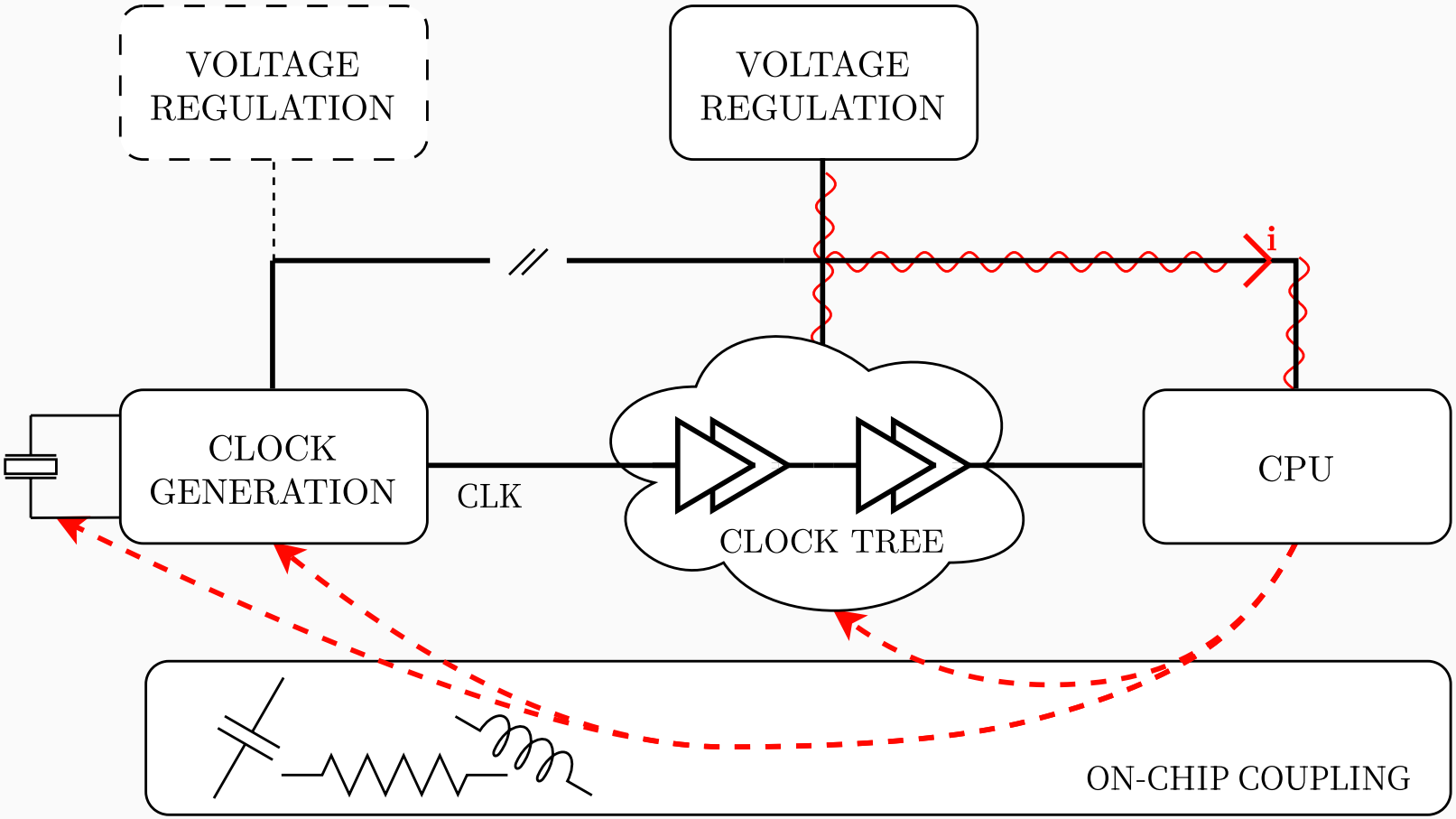
Recent Work: Timing Side Channels Exploiting Jitter

- *Gravellier et al.* [Gra+21] (2021)
  By software, they exploited the jitter correction coefficients of delay lines in high-speed digital buses (DDR).
- *Schoos et al.* [Sch+23] (2023)
  External Jitter measurement from a cryptographic target using a timing sensor at the picosecond scale.





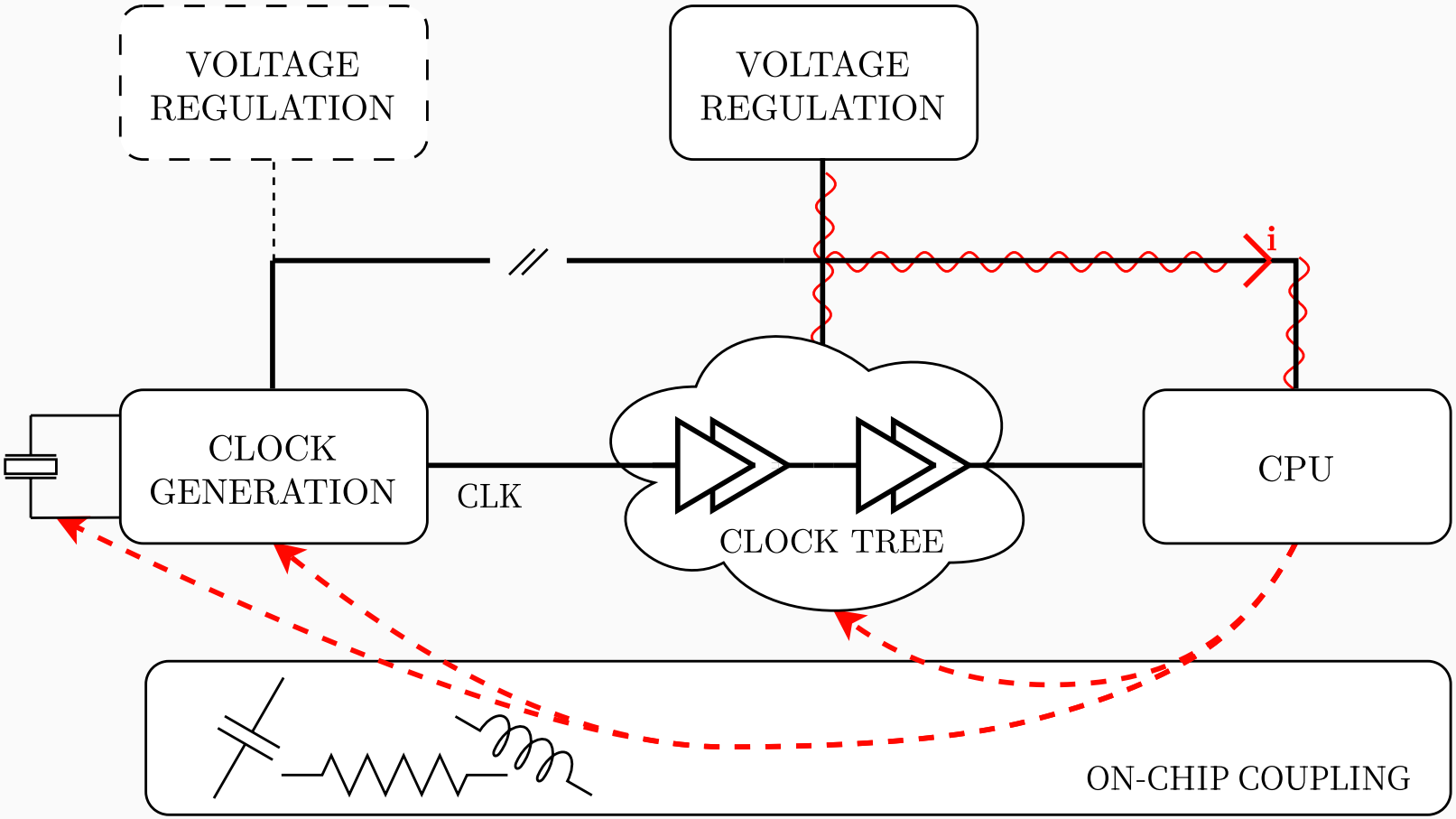
Generalization of Jitter Sources Candidates for MCUs / SoCs



Questions

- Noise-sensitive components (Clock Generation and Clock Tree)
- **Conducted noise** via power rails
- **Indirect noise coupling** via parasitic effects

Generalization of Jitter Sources Candidates for MCUs / SoCs



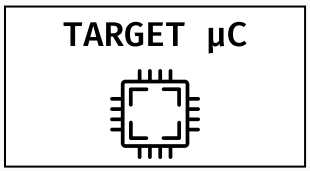
Challenge: Such hypotheses are particularly hard to verify...

- On-chip probing is particularly costly
- SoC / MCU designs diversity
- Complexity of EM simulation and lack of design knowledge

Root-cause characterization

Experiments

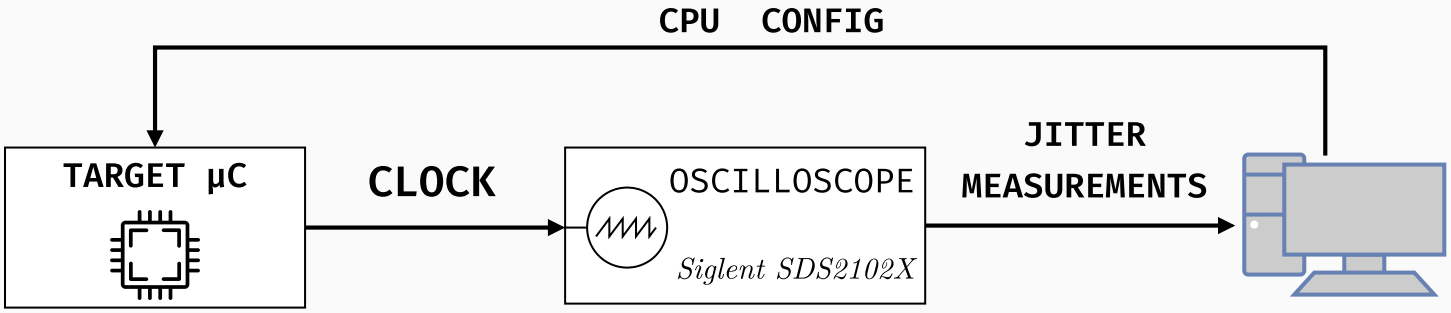
Experimental Setup for Jitter Source Study



STM32F µC familly (STM32F103)

- **Flexibility** Highly configurable internal clock generation circuit
- **Observability** Internal clocks can be routed externally

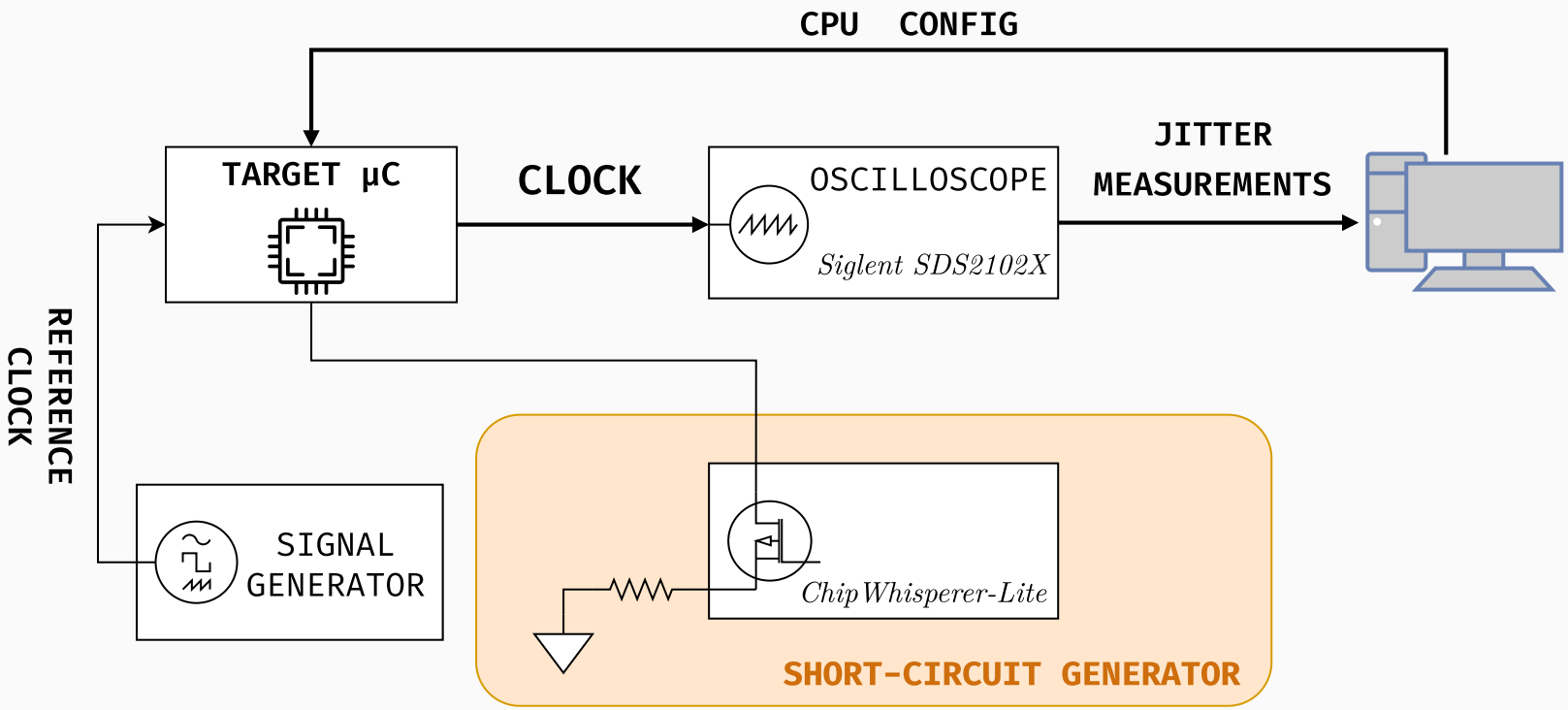
Experimental Setup for Jitter Source Study



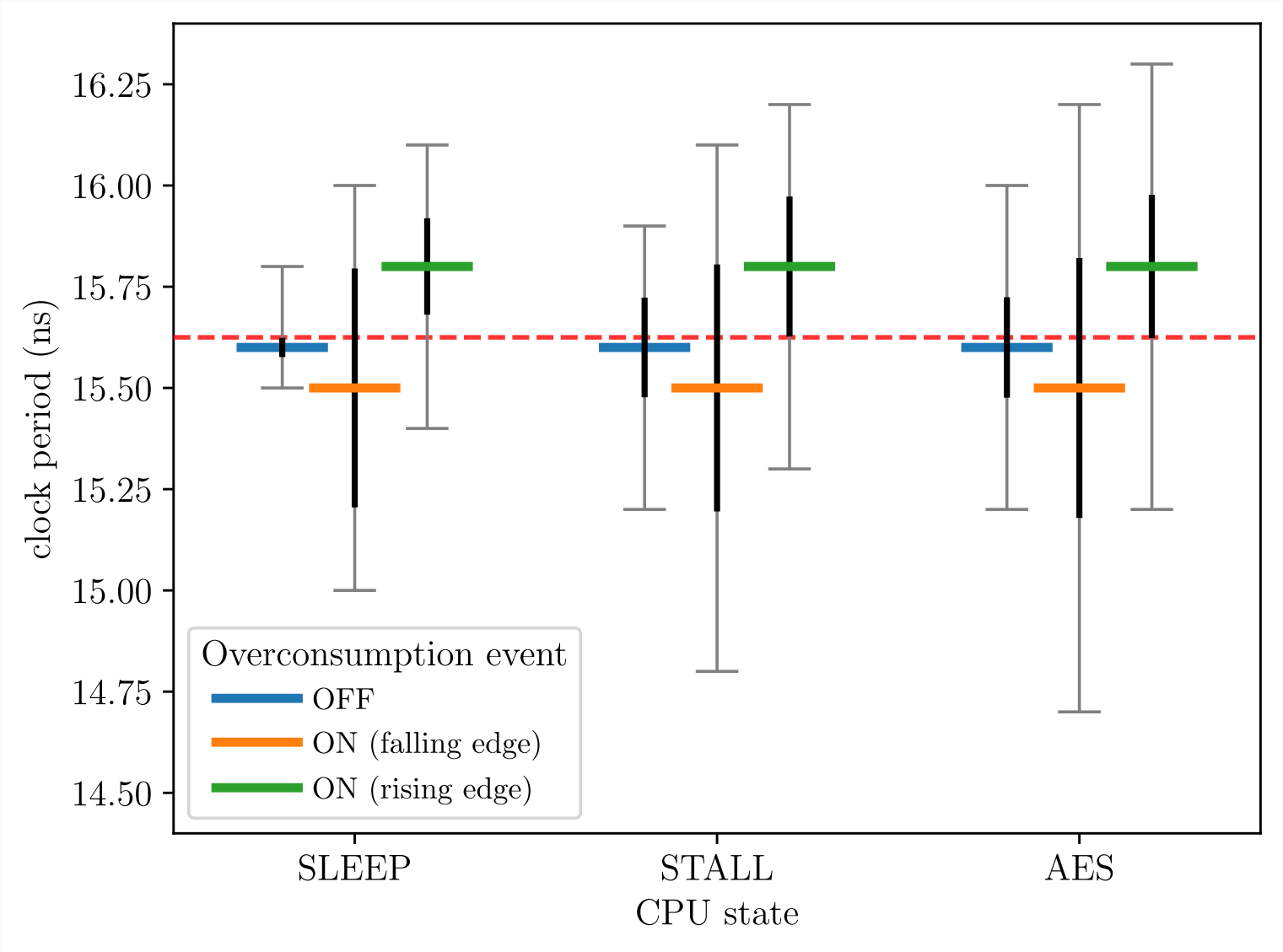
CPU Configurations

- **SLEEP** CPU powered off
- **STALL** Infinite while-loop (branching only)
- **AES** Continuous AES computation

Experimental Setup for Jitter Source Study

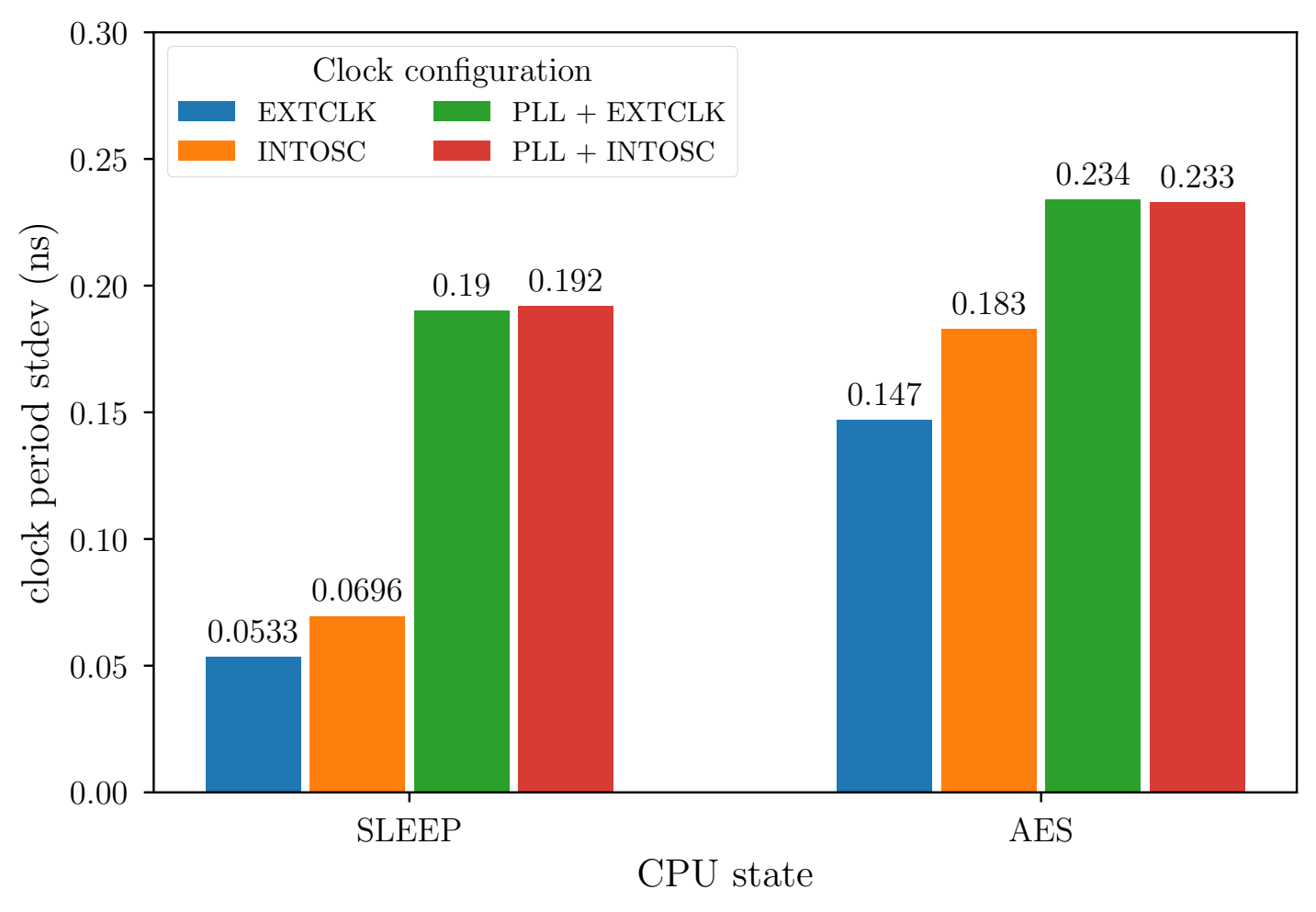


Jitter *vs.* Consumption



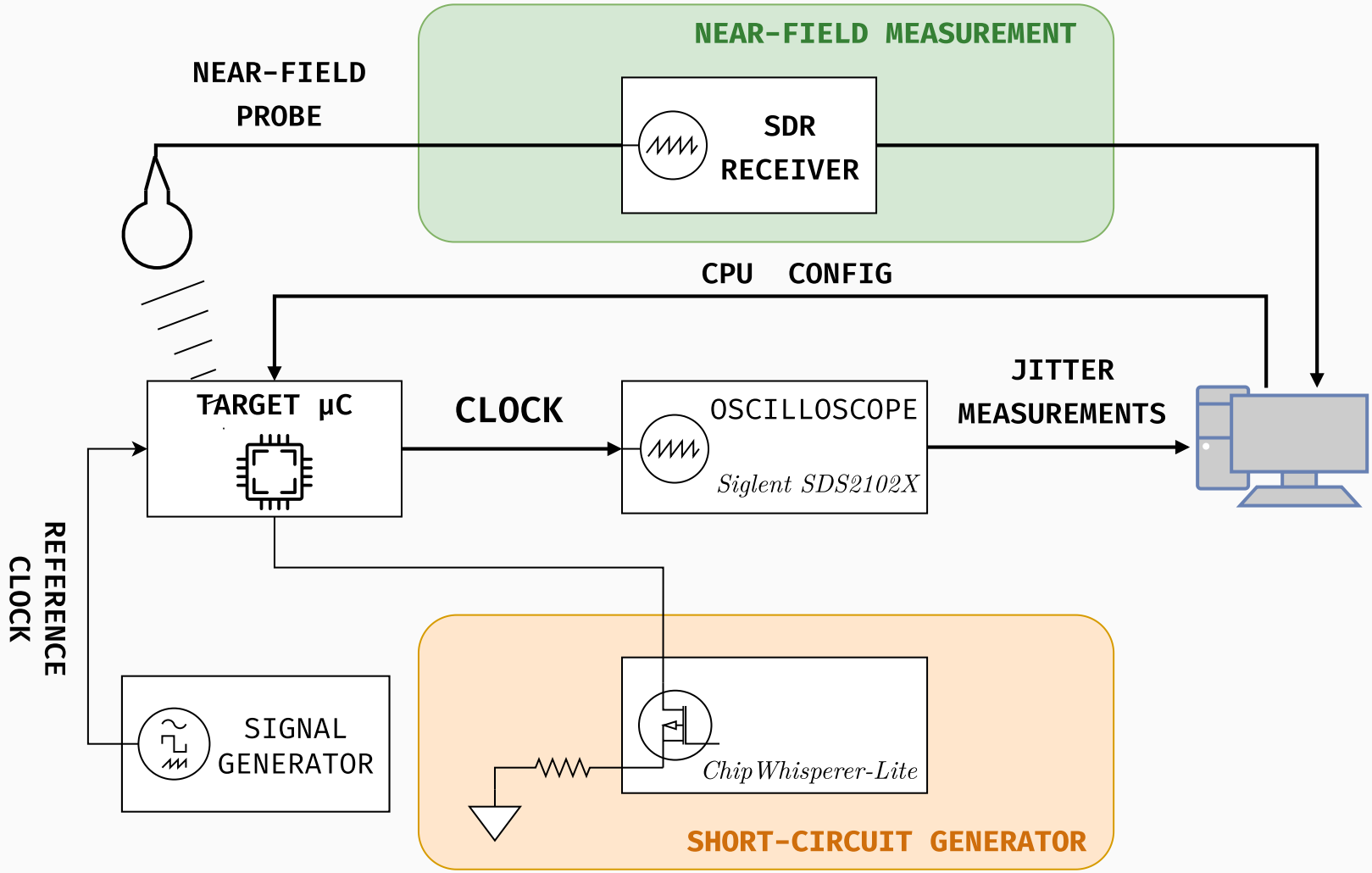
Clock Jitter under various consumption conditions

Jitter *vs.* Clock Configuration

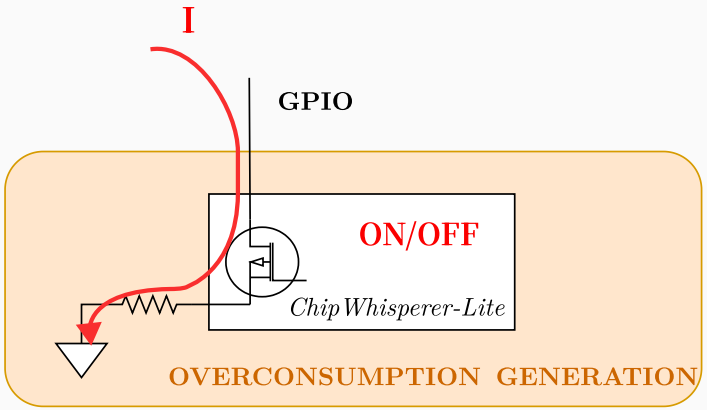


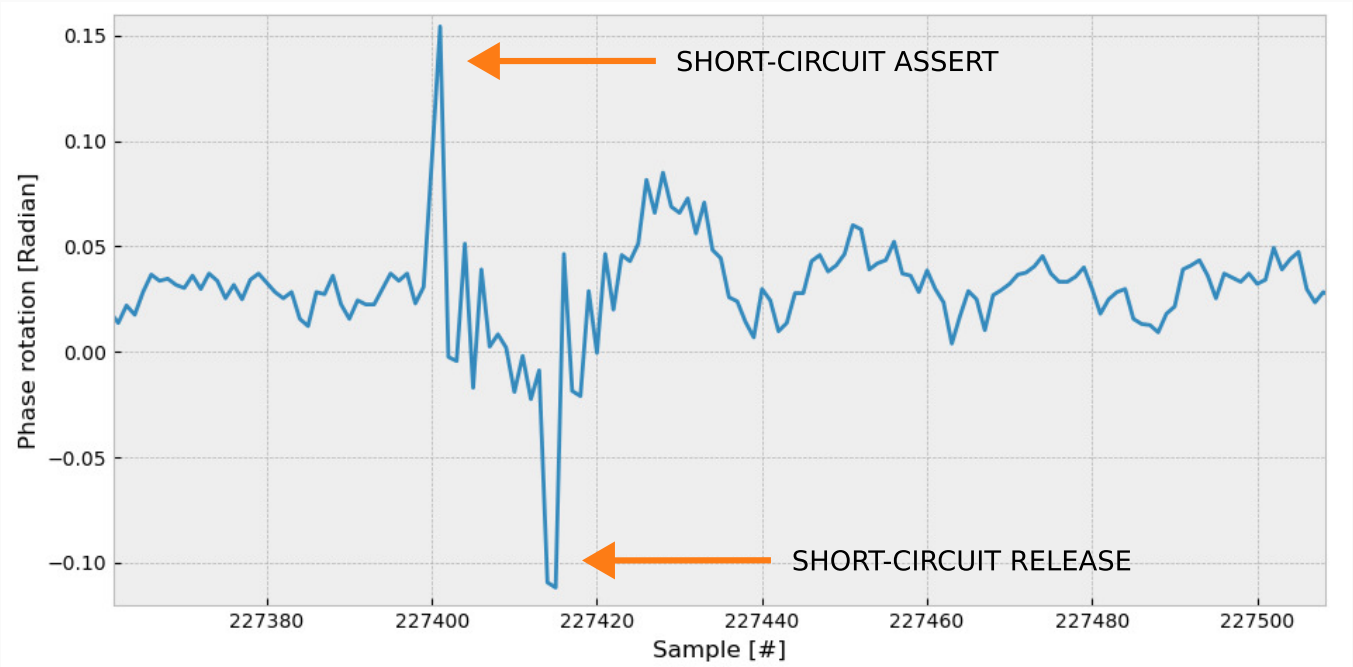
Clock Jitter under various internal clock circuit configurations.

Short-Circuit Effect (Overconsumption) on EM Phase



Short-Circuit Effect (Overconsumption) on EM Phase





EM phase measurement under a GPIO short-circuit

Characterization Results

- Results must be treated with precaution for now
  - Complexity of chip designs and observability
- Shows an interesting correlation linked with key internal components (clock circuits)

Conclusion

Attacks Summary

SoC	Key Recovery using Amplitude / Phase Shift
STM32L1	✅ / ✅
nRF52832	✅ / ✅
nRF51422	✅ / ✅
ATmega328	✅ / ✅
RP2040	❌ / ❌

Lots of devices seems to be impacted...

Root Causes

From a higher level Interactions between software, hardware, and physical environment.

From a lower level Physical phenomena exploitable usually below the engineering scope (*e.g.*, EMC, functional integrity, specifications).

Conclusion

Future work

- Statistically prove that information on amplitude and phase are **complementary**
- Assess to which extent an **SDR** can perform compared to an **oscilloscope** using multi-channel attack

Applications

- Attacks not considered threatening because of limited performance may become threatening
- Systems not vulnerable to **amplitude EM analysis** may be vulnerable to **phase EM analysis**

Questions?

Pierre Ayoub, Aurélien Hernandez, Romain Cayre, Aurélien Francillon, Clémentine Maurice “PhaseSCA: Exploiting Phase-Modulated Emanations in Side Channels”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)*, 2024

Artifacts, Code, Tooling, Datasets:

`https://github.com/pierreay/phase_data`

References

[Agr+03] Dakshi Agrawal, Bruce Archambeault, Josyula Rao, and Pankaj Rohatgi. ***The EM Side-Channel(s): Attacks and Assessment Methodologies.*** Tech. rep. IBM, 2003.

[Ayo+24] Pierre Ayoub, Aurélien Hernandez, Romain Cayre, Aurélien Francillon, and Clémentine Maurice. **"PhaseSCA: Exploiting Phase-Modulated Emanations in Side Channels".** In: *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)* 2025.1 (Dec. 2024), pp. 392–419. DOI: 10.46586/tches.v2025.i1.392-419. URL: https://tches.iacr.org/index.php/TCHES/article/view/11934.

References ii

[Cam+18] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. **“Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers”.** In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. CCS ’18. New York, NY, USA: Association for Computing Machinery, 2018, pp. 163–177. ISBN: 9781450356930. DOI: 10.1145/3243734.3243802. URL: https://doi.org/10.1145/3243734.3243802.

References iii

[Gen+22] Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer. **"Stealing Keys from PCs Using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation".** In: *Cryptographic Hardware and Embedded Systems – CHES 2015*. Berlin, Heidelberg: Springer-Verlag, 2022, pp. 207–228. ISBN: 978-3-662-48323-7. DOI: 10.1007/978-3-662-48324-4_11. URL: https://www.tau.ac.il/~tromer/radioexp/.

[Gra+21] Joseph Gravellier, Jean-Max Dutertre, Yannick Teglia, and Philippe Loubet Moundi. **"SideLine: How Delay-Lines (May) Leak Secrets from Your SoC".** In: *Constructive Side-Channel Analysis and Secure Design*. Ed. by Shivam Bhasin and Fabrizio De Santis. Cham: Springer International Publishing, 2021, pp. 3–30. ISBN: 978-3-030-89915-8.

References iv

[LMM05] Huiyun Li, A. Theodore Markettos, and Simon Moore. **"Security Evaluation Against Electromagnetic Analysis at Design Time".** In: *Proceedings of the 7th International Conference on Cryptographic Hardware and Embedded Systems*. CHES'05. Edinburgh, UK: Springer-Verlag, 2005, pp. 280–292. ISBN: 3540284745. DOI: 10.1007/11545262_21. URL: https://doi.org/10.1007/11545262_21.

[Mey12] Olivier Meynard. **"Characterization and Use of the EM Radiation to Enhance Side Channel Attacks".** PhD thesis. Télécom ParisTech, Jan. 2012.

References v

[OFl24] Colin O'Flynn. **"Phase Modulation Side Channels: Jittery JTAG for On-Chip Voltage Measurements".** In: *IACR Transactions on Cryptographic Hardware and Embedded Systems (TCHES)* 2024.4 (Sept. 2024), pp. 382–424. DOI: 10.46586/tches.v2024.i4.382-424. URL: https://tches.iacr.org/index.php/TCHES/article/view/11797.

[QS01] Jean-Jacques Quisquater and David Samyde. **"ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards".** In: *Proceedings of the International Conference on Research in Smart Cards: Smart Card Programming and Security*. E-SMART '01. Berlin, Heidelberg: Springer-Verlag, 2001, pp. 200–210. ISBN: 3540426108.

References vi

[Ros82] Howard E. Rosenblum. ***NACSIM 5000: Tempest Fundamentals.*** Tech. rep. National Security Agency (NSA), 1982. URL: https://cryptome.org/jya/nacsim-5000/nacsim-5000.htm.

[Sch+23] Kai Schoos, Sergej Meschkov, Mehdi B. Tahoori, and Dennis R. E. Gnad. **"JitSCA: Jitter-based Side-Channel Analysis in Picoscale Resolution".** In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2023.3 (June 2023), pp. 294–320. DOI: 10.46586/tches.v2023.i3.294-320. URL: https://tches.iacr.org/index.php/TCHES/article/view/10965.

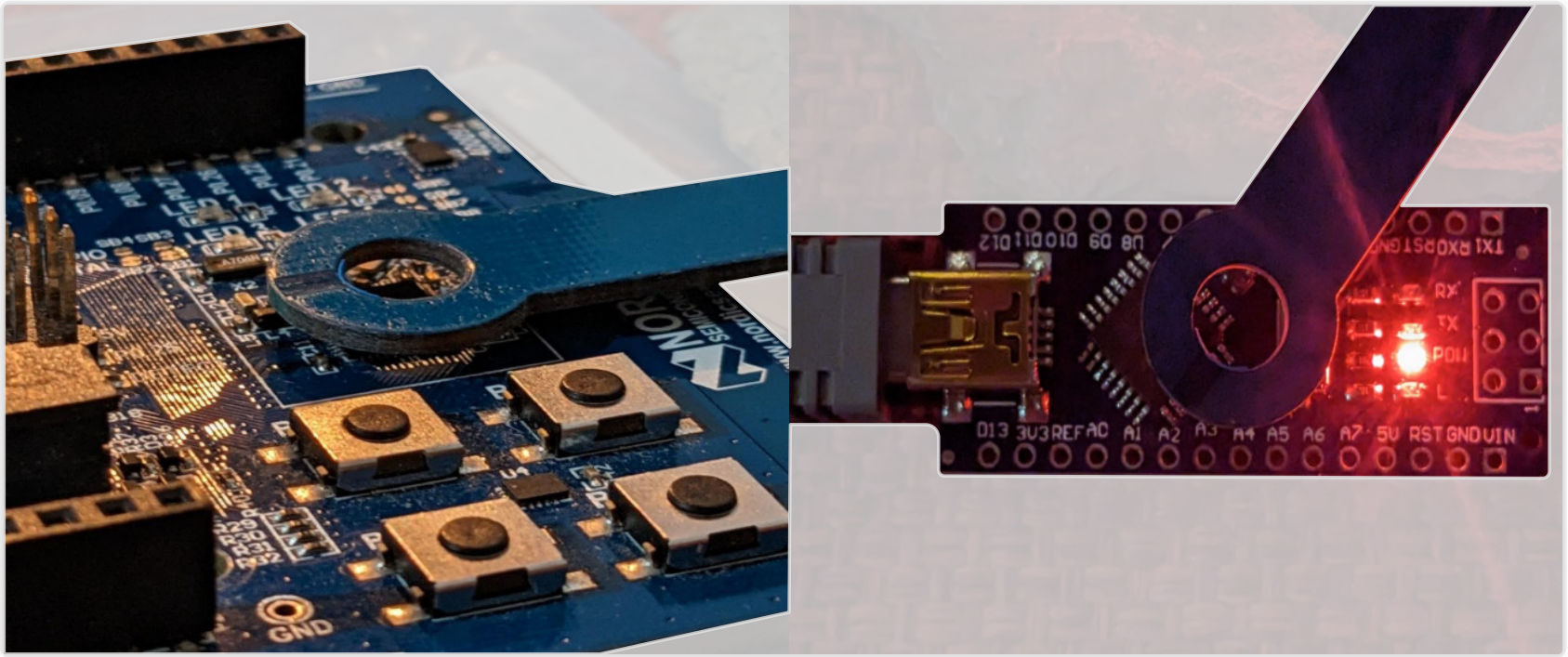
References vii

[VP09] Martin Vuagnoux and Sylvain Pasini. **“Compromising Electromagnetic Emanations of Wired and Wireless Keyboards”.** In: *Proceedings of the 18th Conference on USENIX Security Symposium*. SSYM’09. Montreal, Canada: USENIX Association, 2009, pp. 1–16.

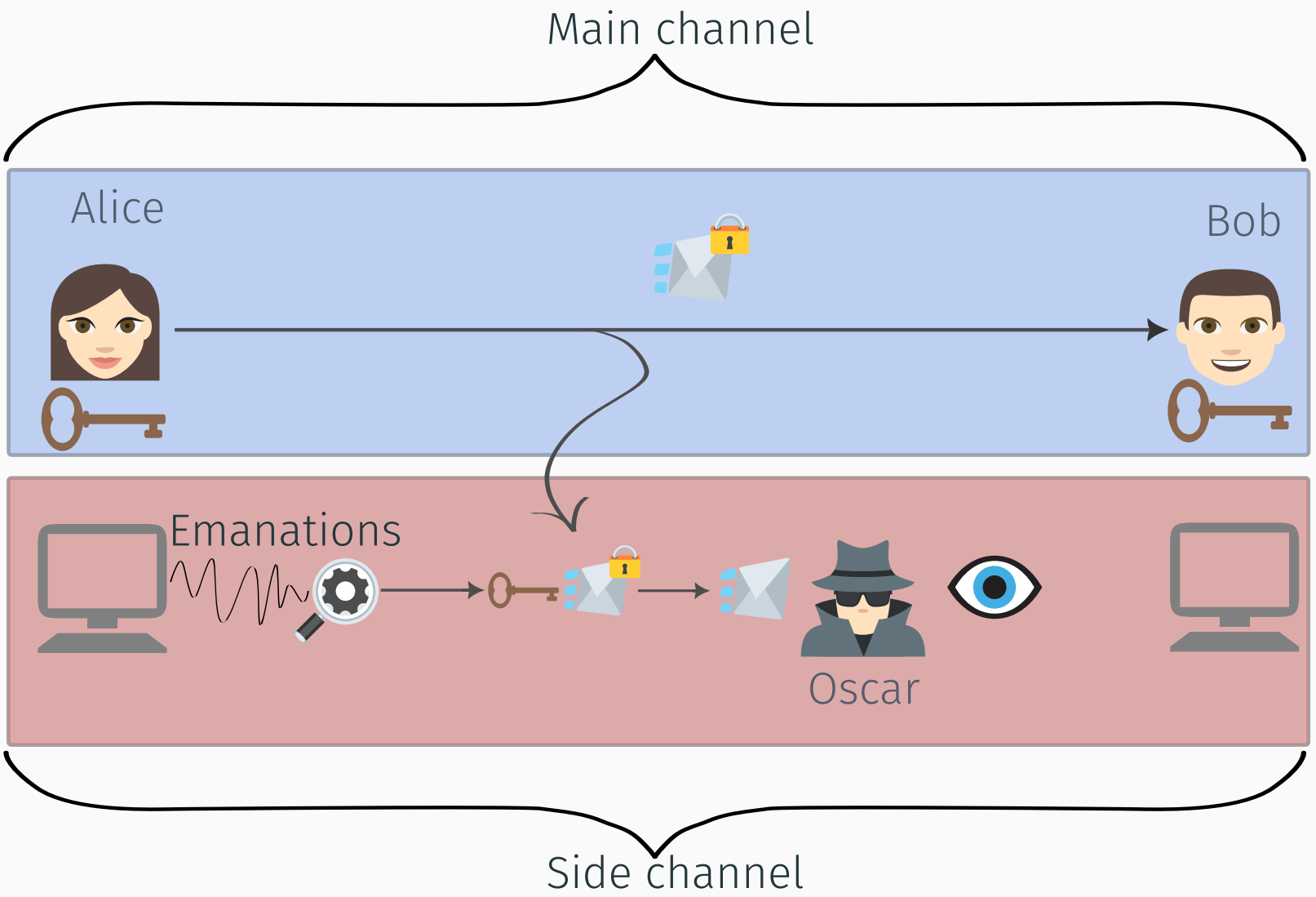
[WWD20] Ruize Wang, Huanyu Wang, and Elena Dubrova. **“Far Field EM Side-Channel Attack on AES Using Deep Learning”.** In: *Proceedings of the 4th ACM Workshop on Attacks and Solutions in Hardware Security* (Nov. 2020). DOI: 10.1145/3411504.3421214. URL: http://dx.doi.org/10.1145/3411504.3421214.

Backup Slides

Measuring EM emanations

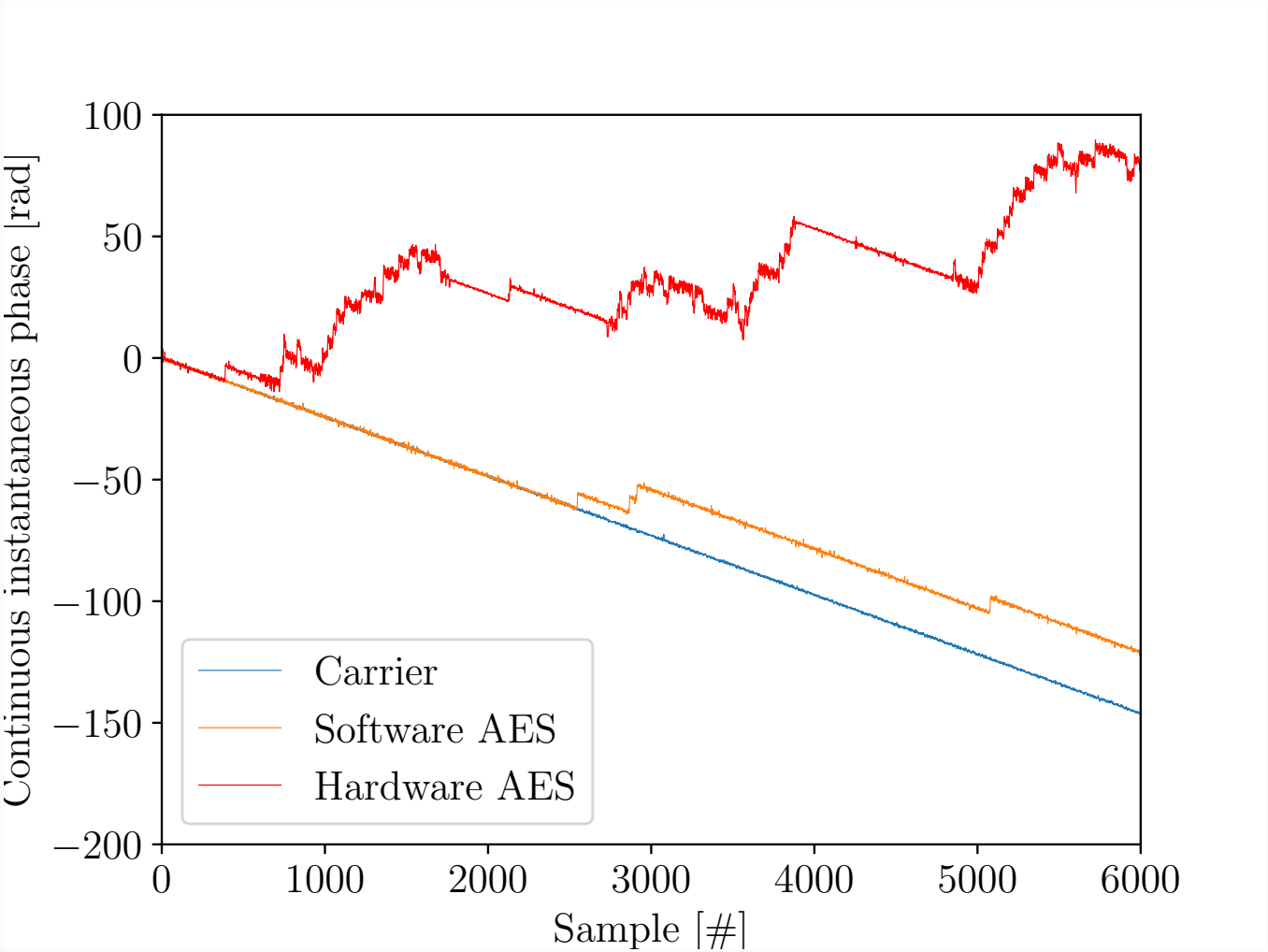


Main channel *vs.* Side channel



Embedded System Complexity is Increasing

Identifying Phase-Modulated Leakage on a Target SoC



Filtering the Leaked Signal: Principle

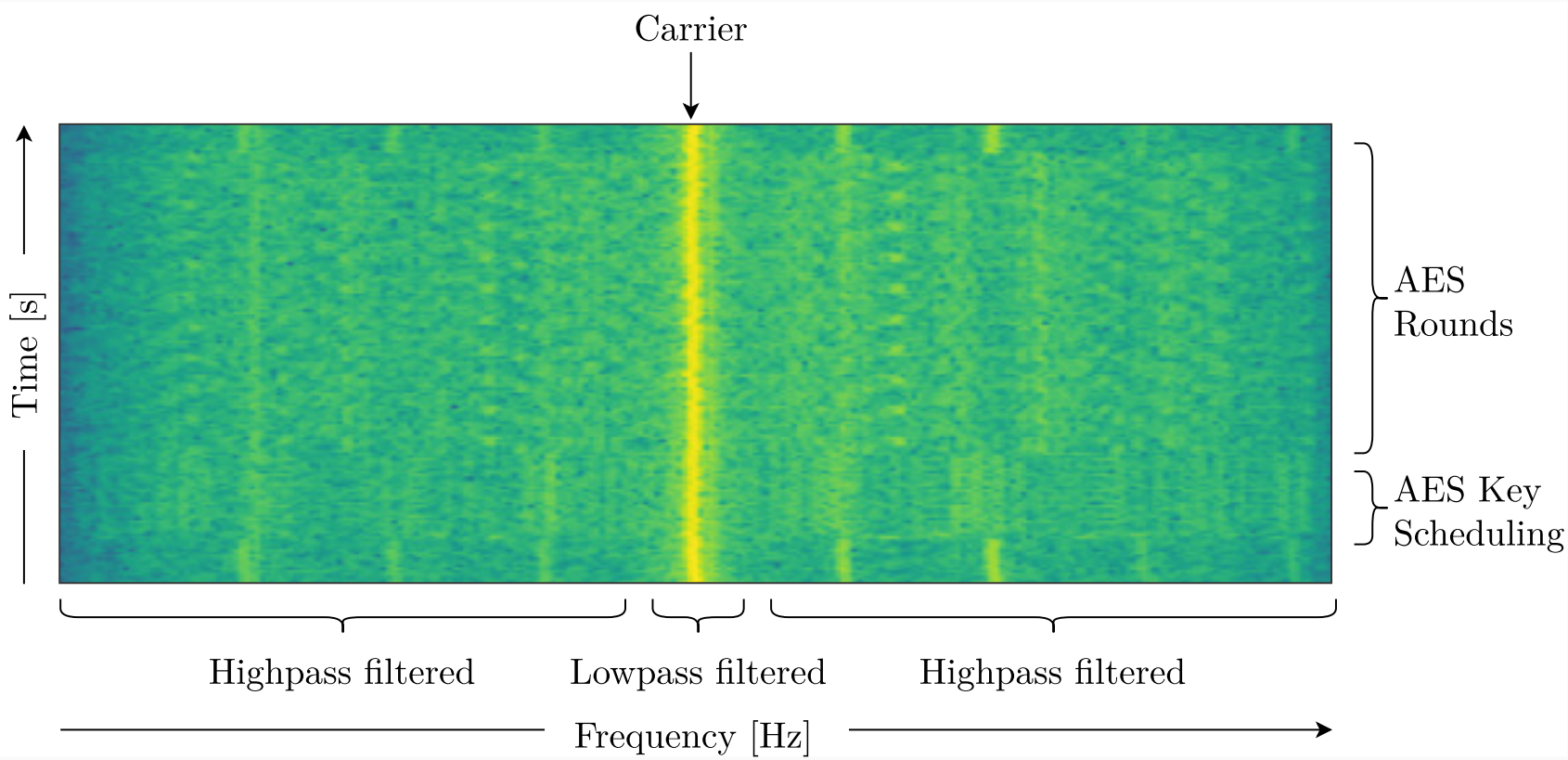
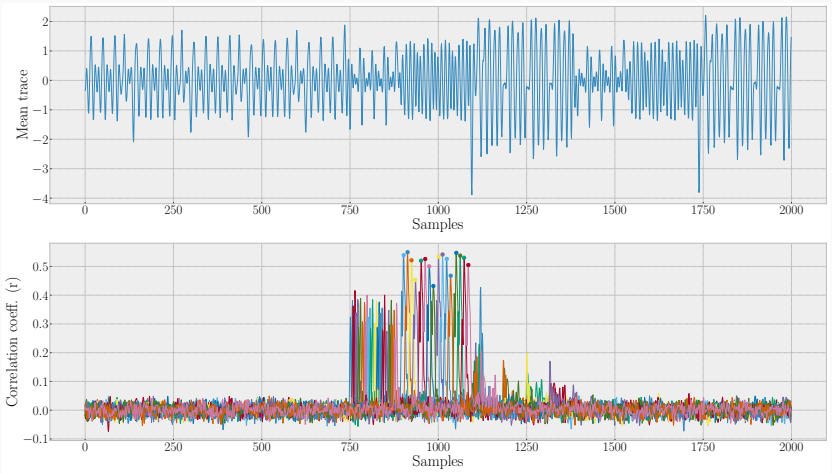
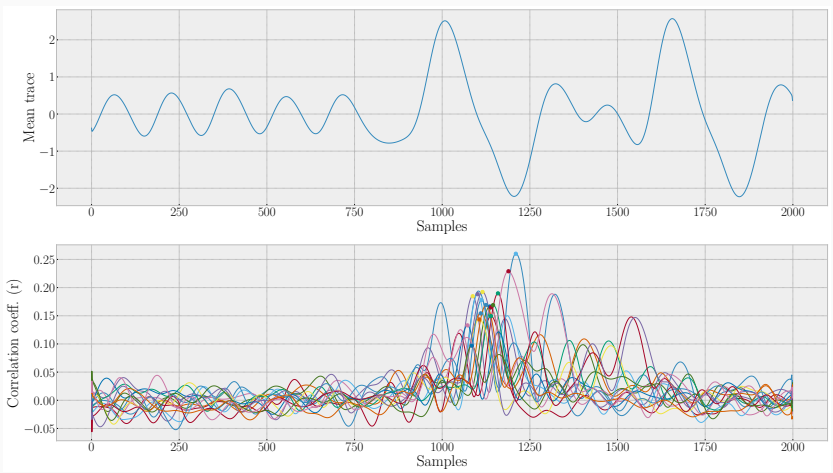


Figure 1: Waterfall illustrating filters isolating amplitude and phase shift leakage. A low-pass filter is used to isolate the phase-modulated leakage, while a high-pass filter is used to isolate the amplitude-modulated leakage.

Filtering the Leaked Signal: Results



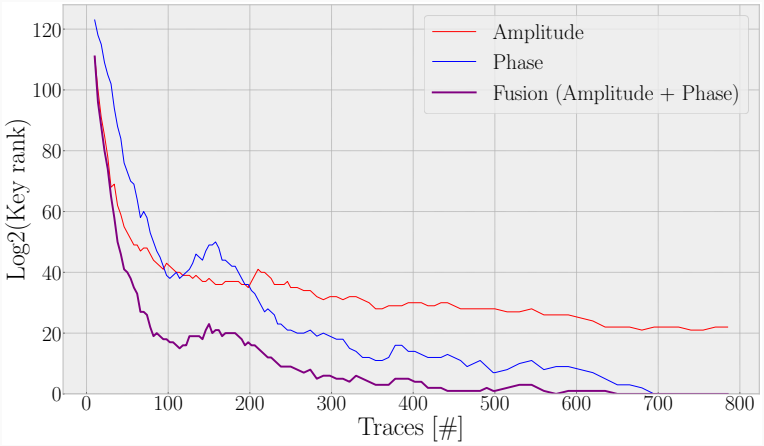
(a) Using a low-pass filtered signal at 1 MHz.



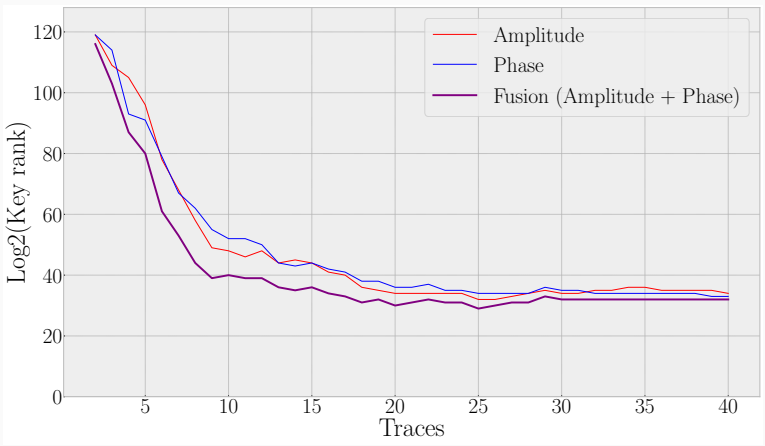
(b) Using a low-pass filtered signal at 50 kHz.

Figure 2: Correlation coefficients (ρ) for POIs on phase shift for the nRF52.

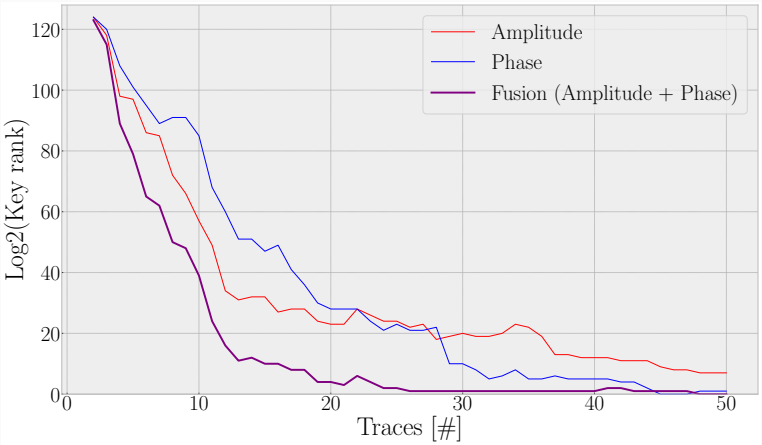
Performance for Profiled Attacks



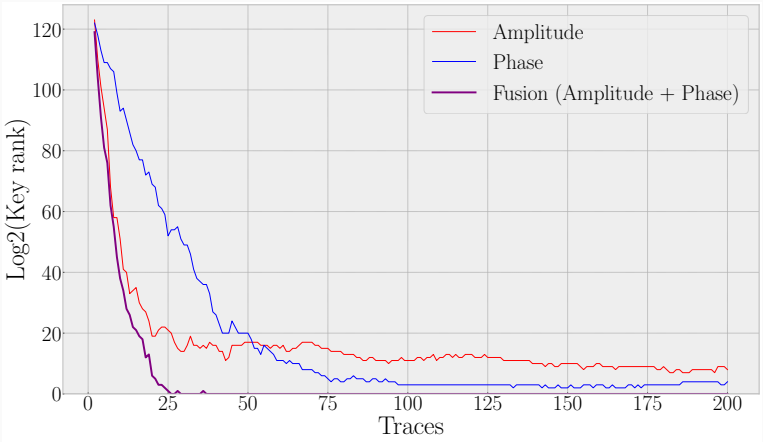
(a) Key rank for the nRF52.



(b) Key rank for the nRF51.

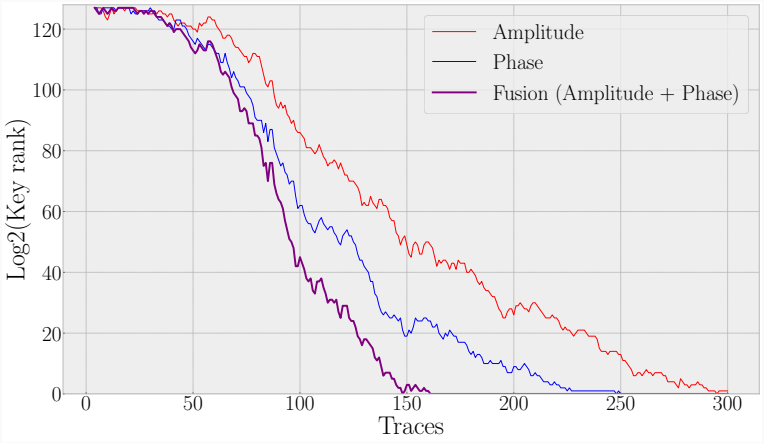


(c) Key rank for the STM32L1.

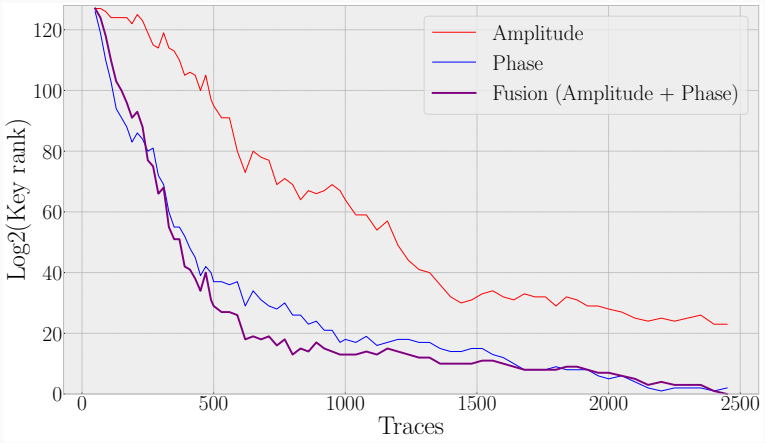


(d) Key rank for the ATmega328.

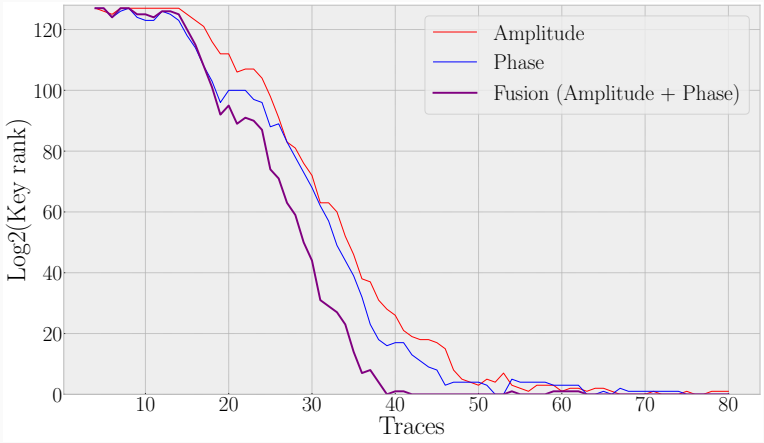
Performance for Non-Profiled Attacks



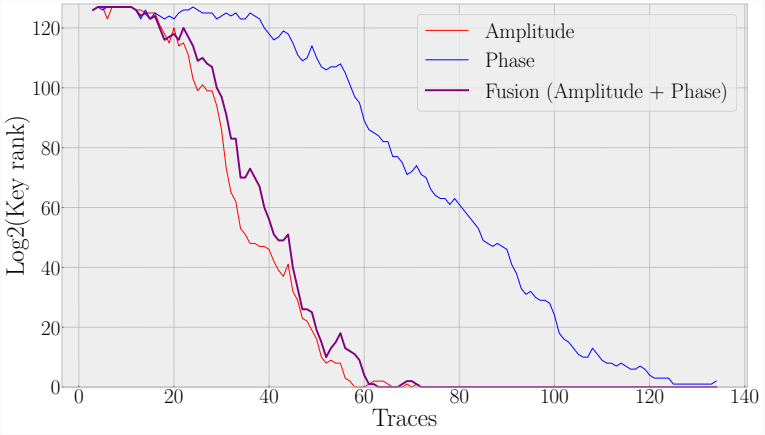
(a) Key rank for the nRF52.



(b) Key rank for the nRF51.



(c) Key rank for the STM32L1.



(d) Key rank for the ATmega328

Phase in Screaming Channels (Custom)

AES leak signal at Screaming Channels frequencies in the Far Field (FF) 2.5 GHz).

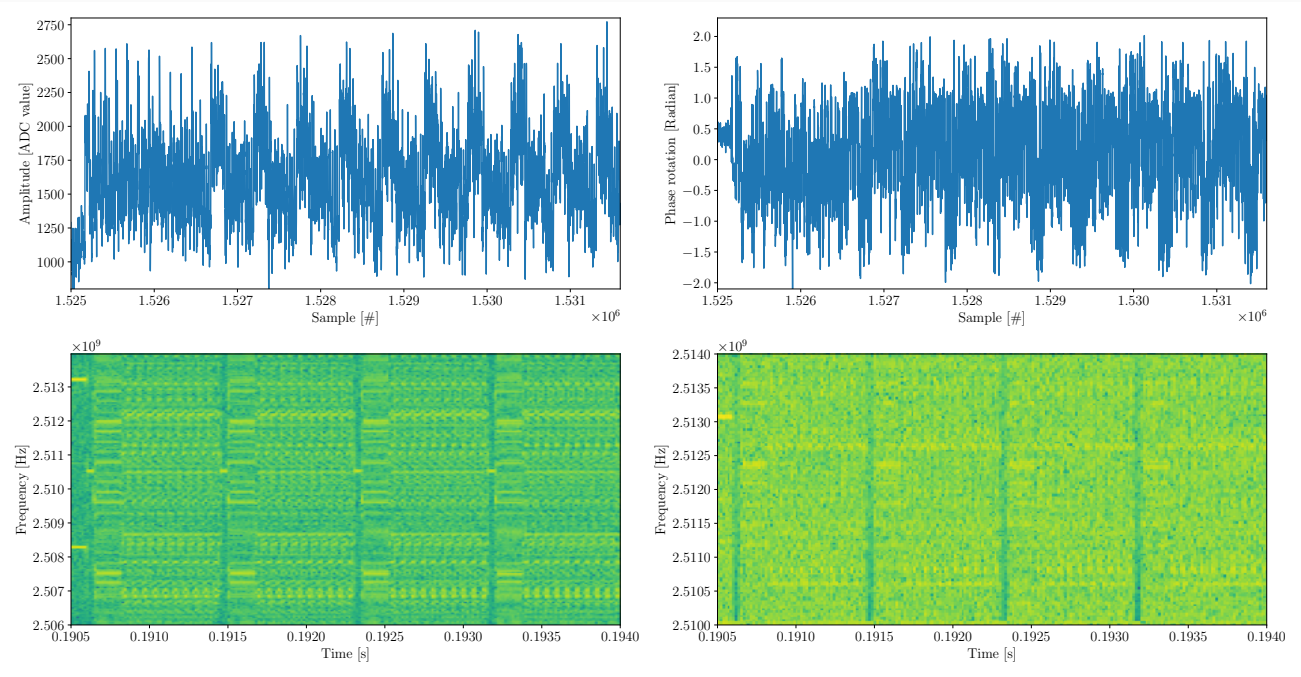


Figure 5: Signal captured during radio broadcast from an instrumented firmware in both time-domain (upper) and frequency-domain (down) for both amplitude (left) and phase (right). We can observe the key scheduling of AES and its 10 rounds in time-domain and 4 full run of AES in frequency-domain.

Phase in Screaming Channels (NimBLE)

AES leak signal at Screaming Channels frequencies in the Far Field (FF) 2.5 GHz).

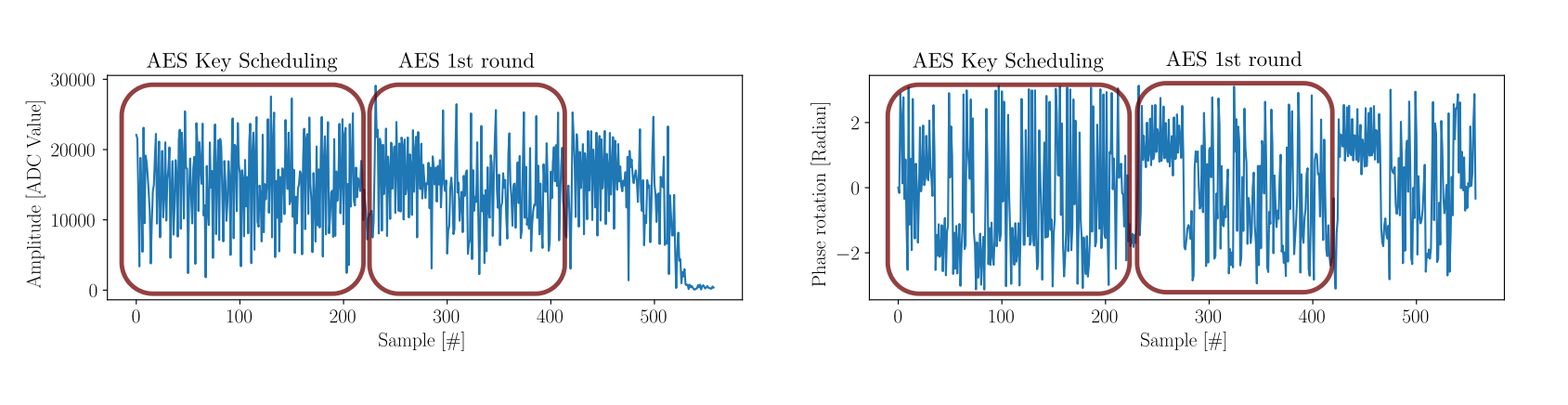


Figure 6: Signal captured during a BLE communication from NimBLE for both amplitude (left) and phase (right).

Zoom on a Example Clocking Circuit

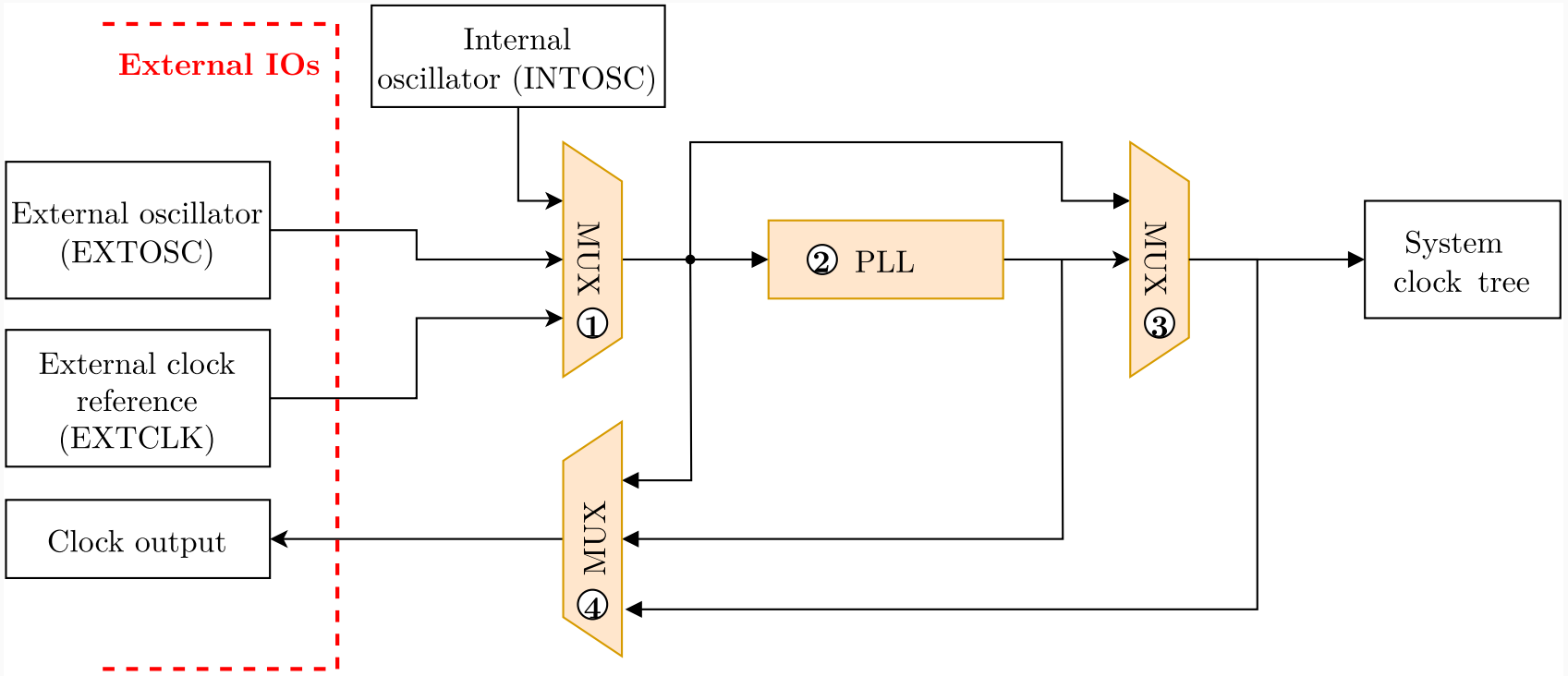


Figure 7: Simplified view of the STM32F103RB internal clocking circuit.

Jitter *vs.* Phase Shift

Procedure

1. Produce the overconsumption event with ChipWhisperer
2. Measure both jitter and phase shift in parallel

Results

- Jitter measure: 275 ps
- Phase shift measure: 0.125 rad
- Jitter to Phase shift conversion: $\phi = 2\pi f \cdot \Delta t$
- Incertitude of around 0.014 rad or 11%

Countermeasures

Physical

- Filtering
- Shielding
- Grounding
- Decoupling
- PCB Design

Cryptography

- Masking
- Hiding

State-of-the-Art

Foundational Work: EM Side Channels

- *NSA's NACSIM 5000: TEMPEST Fundamentals* [Ros82]
- *Agrawal et al.* [Agr+03]
- *Li et al.* [LMM05]

Recent Work: Timing Side Channels exploiting Jitter

- *Gravellier et al.* [Gra+21]
- *Schoos et al.* [Sch+23]

Parallel Work: Side Channels exploiting Phase Modulation

- *Colin O'Flynn* [OFl24]