



CNRS Images. © Jean-Claude MOSCHETTI / IETR / CNRS Photothèque



# Cryptographic screaming-channel attacks

Jeremy Guillaume

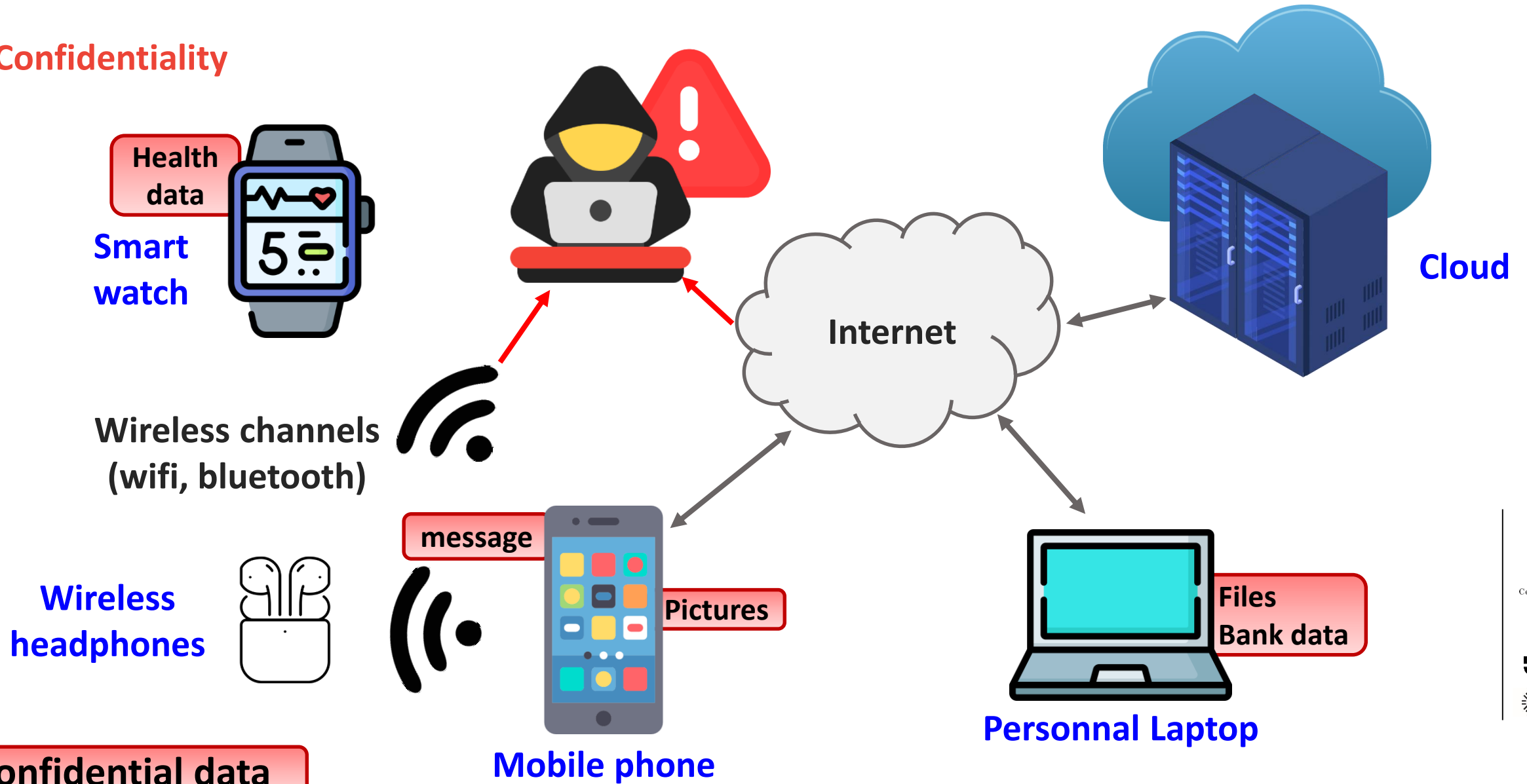
04/11/2025 – Spring school



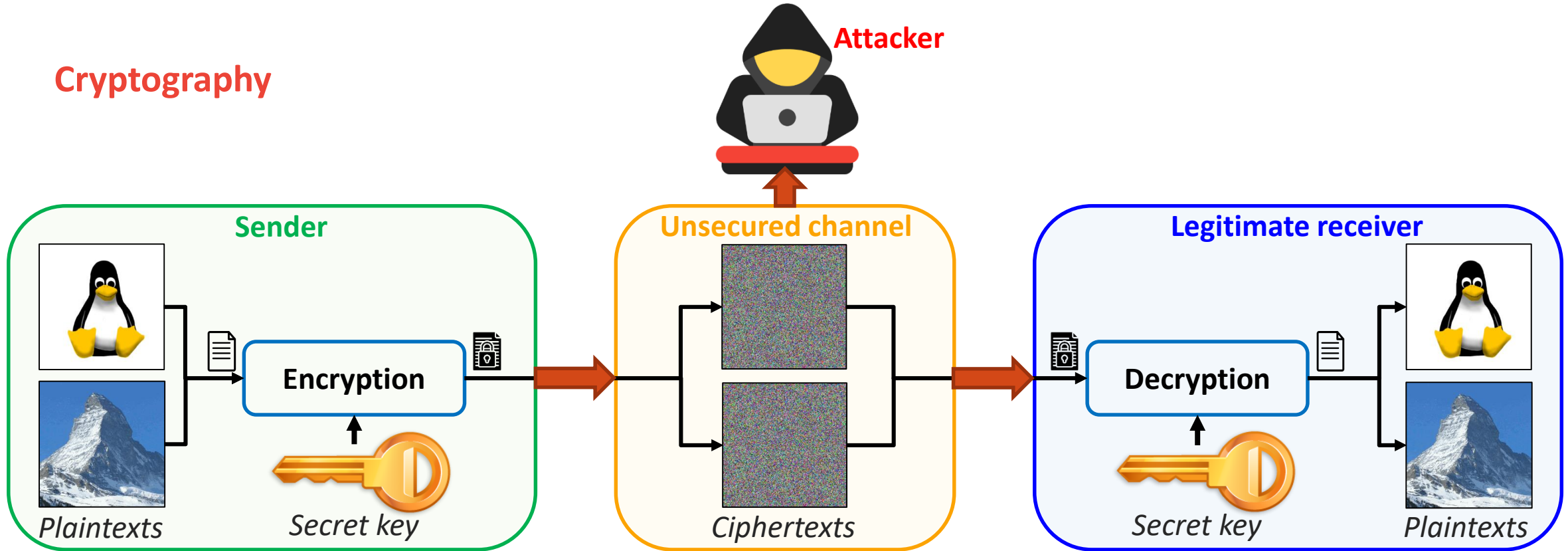
[www.ietr.fr](http://www.ietr.fr)

- 1. Introduction and context**
- 2. Side-channel attacks**
- 3. Screaming-channel attacks**
- 4. Contributions and experimental results**
- 5. Conclusion and perspectives**

## Confidentiality



## Cryptography



## AES (Advanced Encryption Standard):



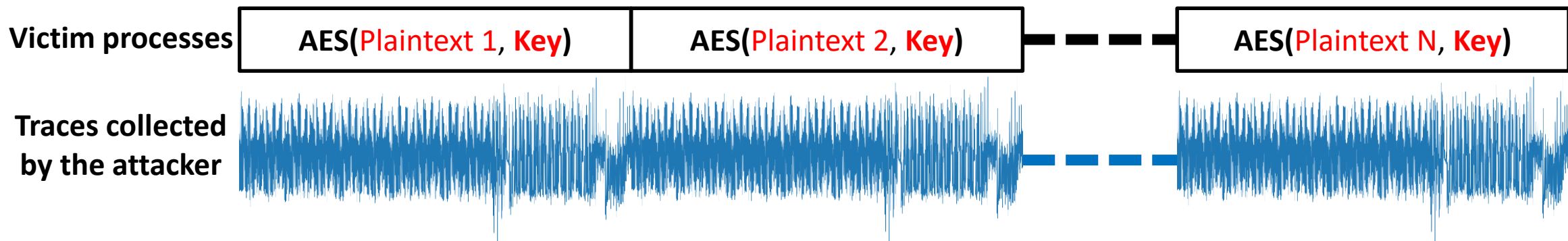
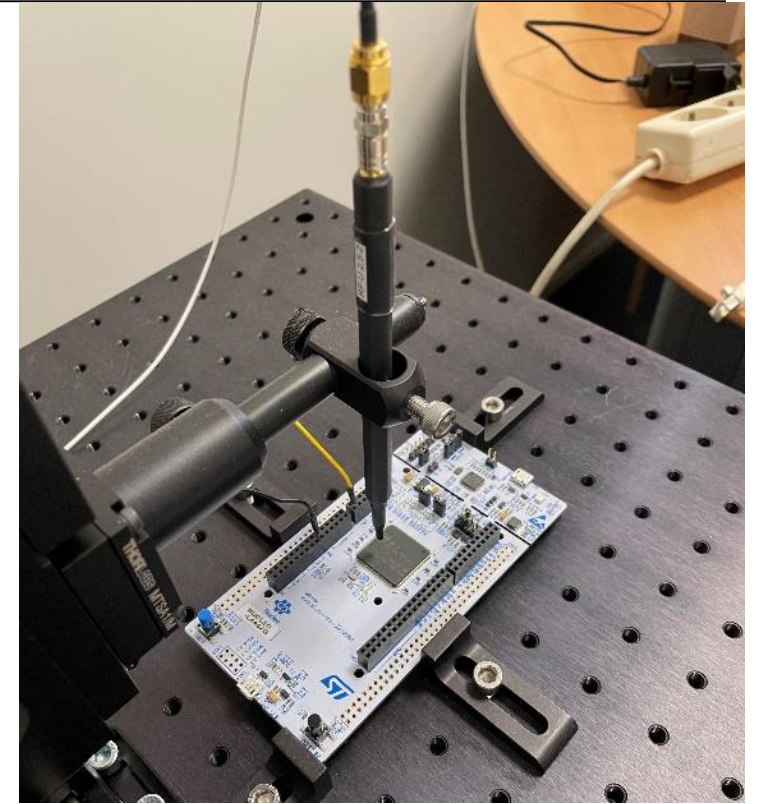
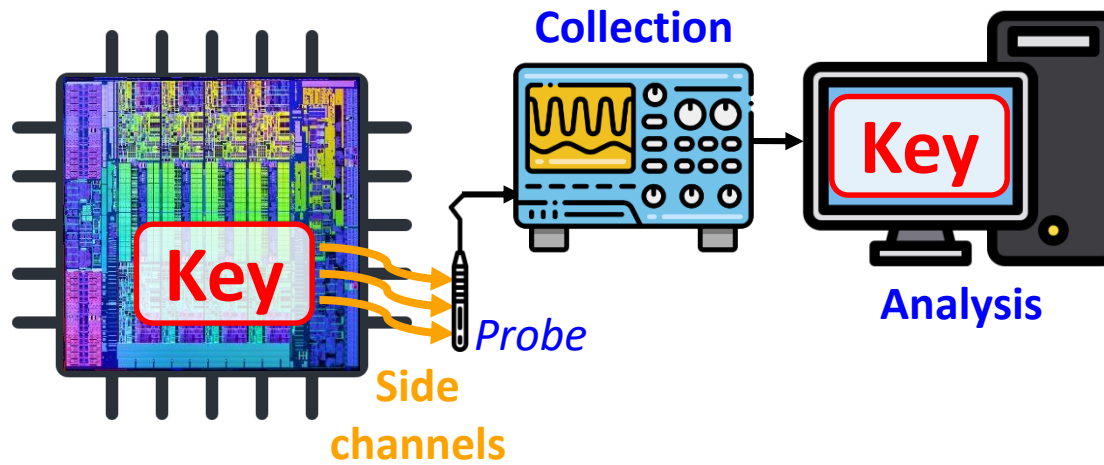
AES-128 Key

10010100001110101011001010101100011010011101000011010100 ----- 0010110001111100

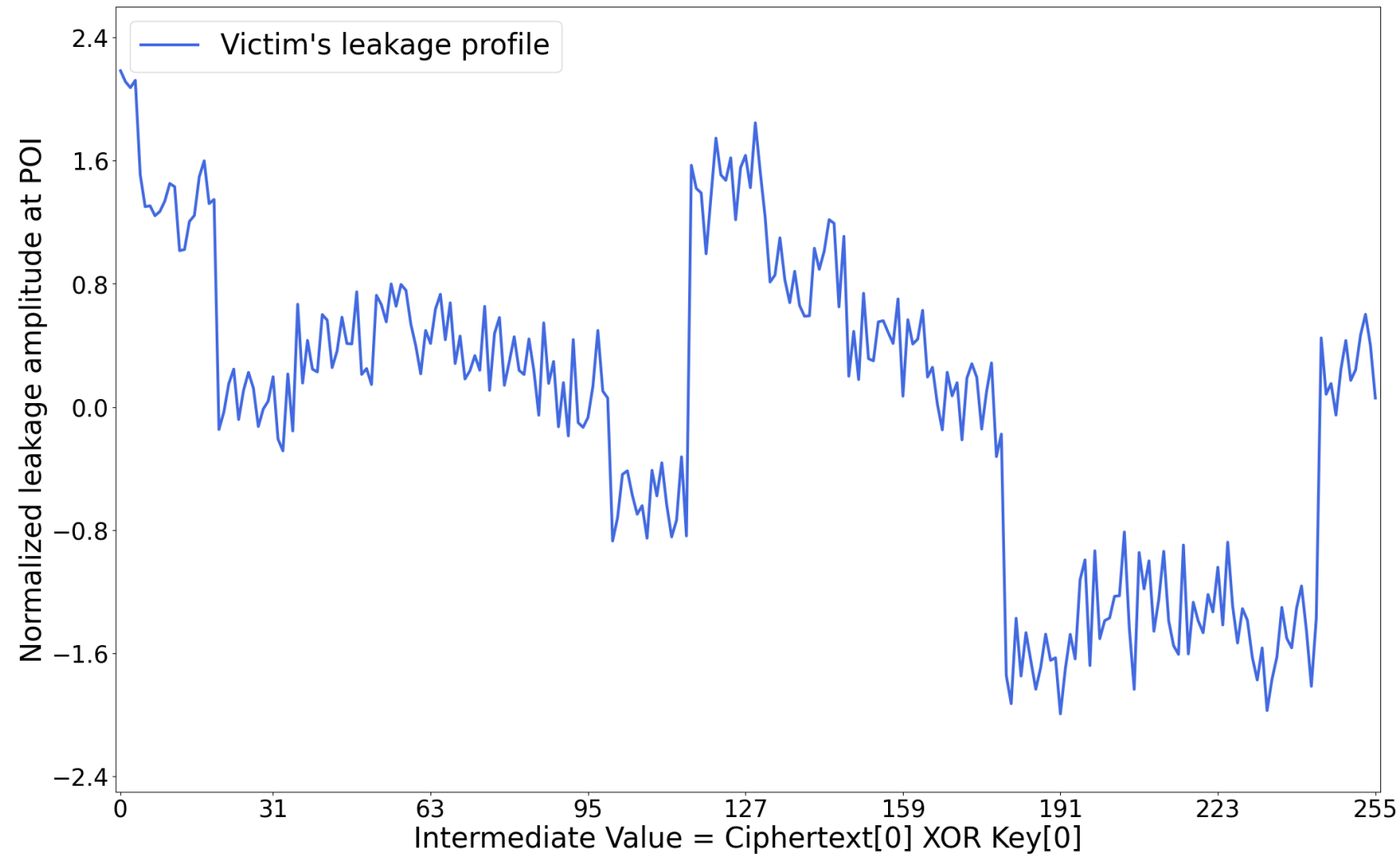
**128** bits  $\rightarrow 2^{128} > 10^{37}$  possible keys



## Recovering internal data

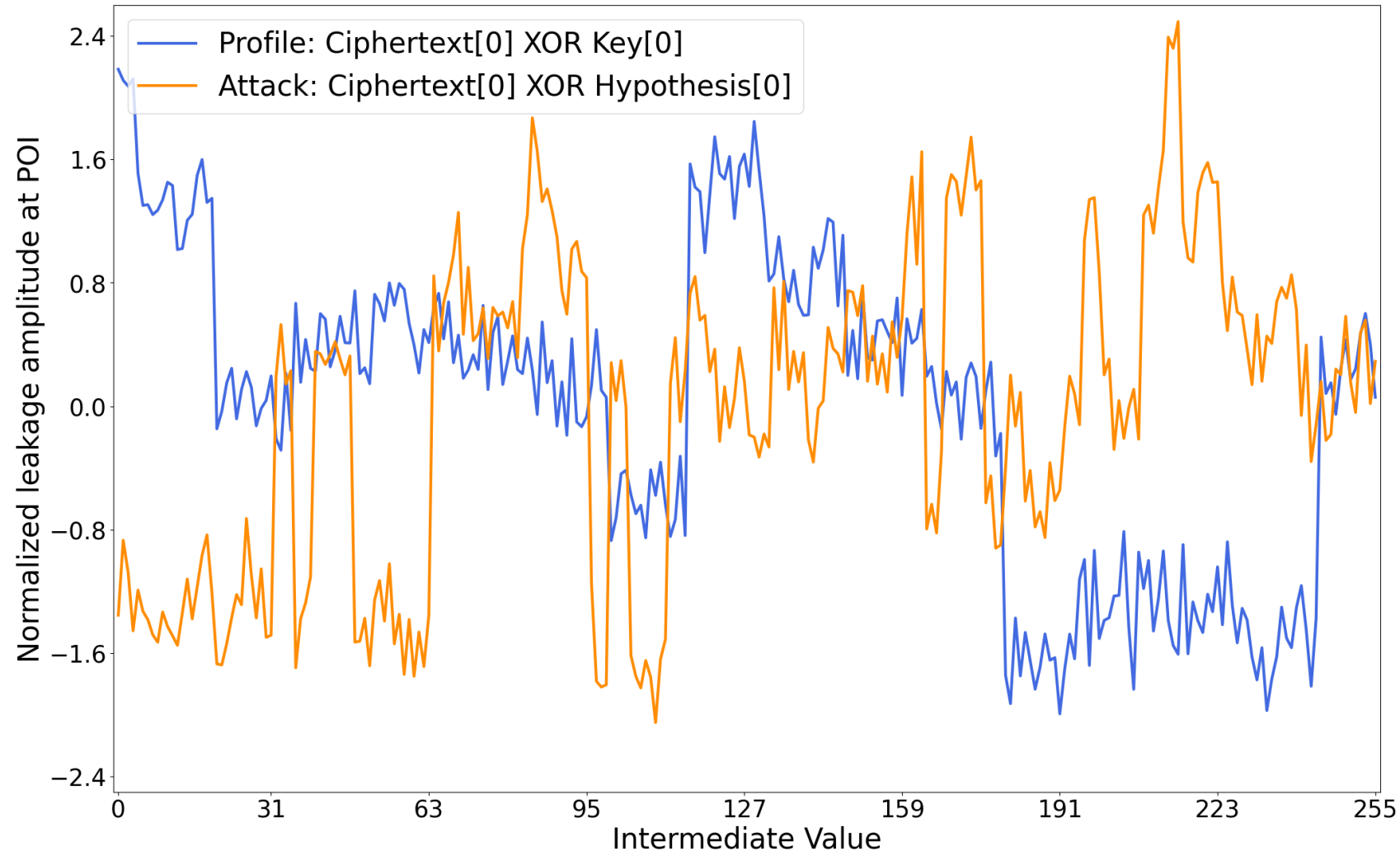


## Analysis attack



## Analysis attack

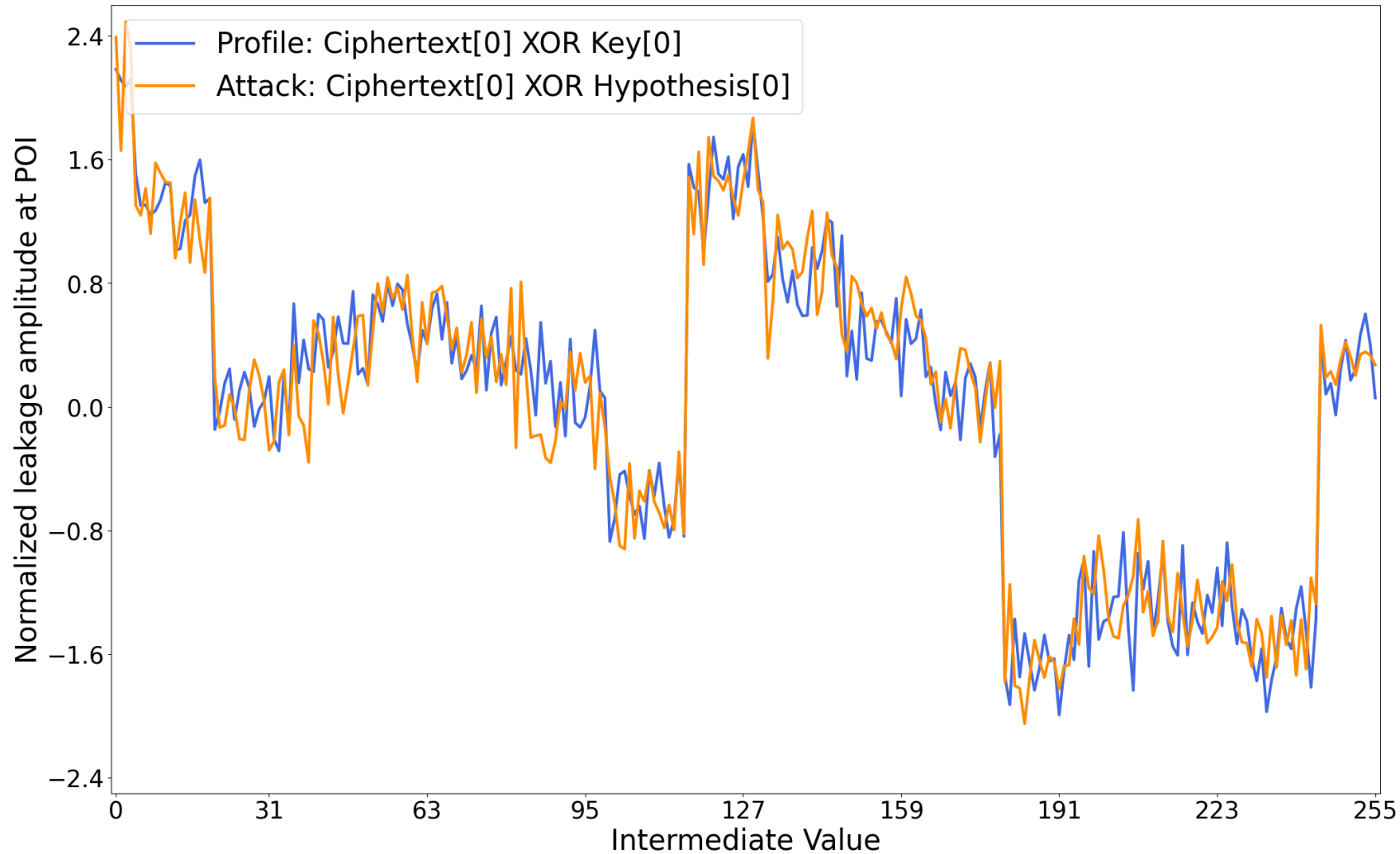
**X** Hypothesis[0] != Key[0]



## Analysis attack

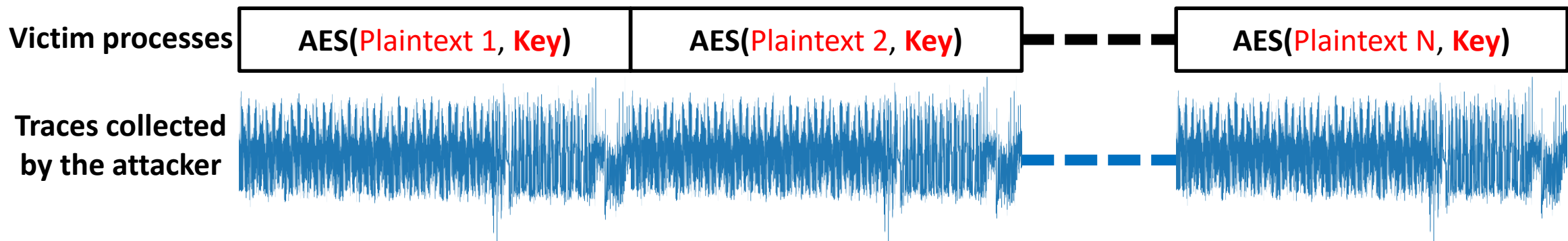
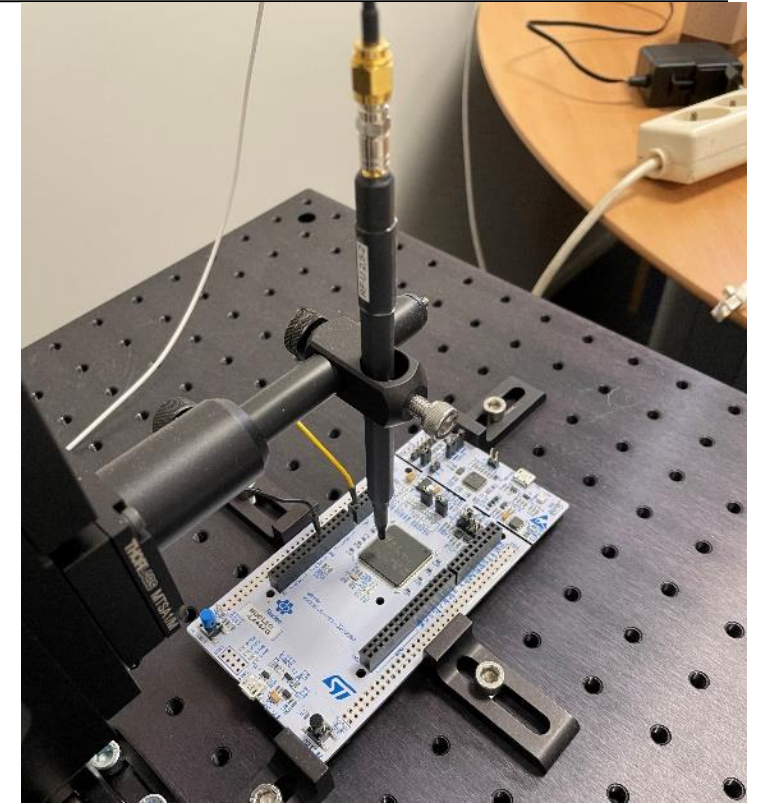
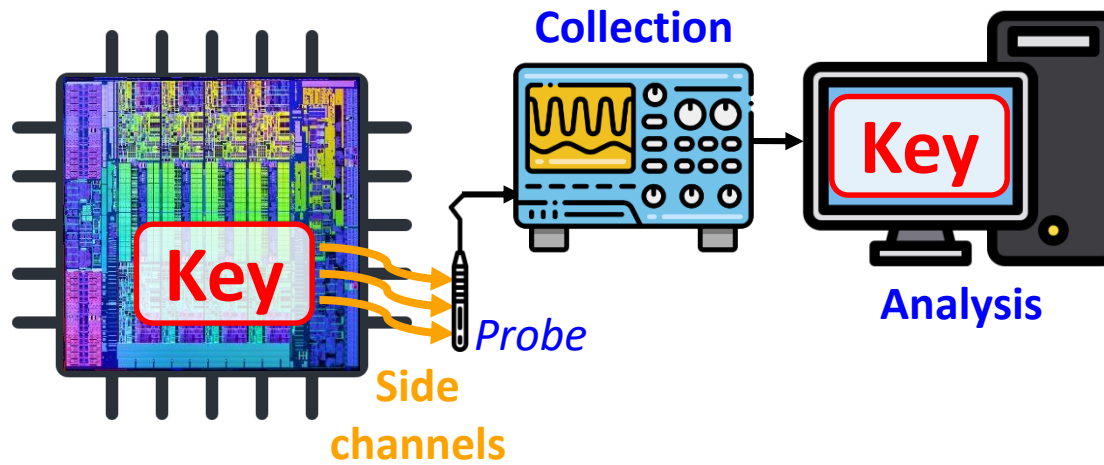


Hypothesis[0] == Key[0]

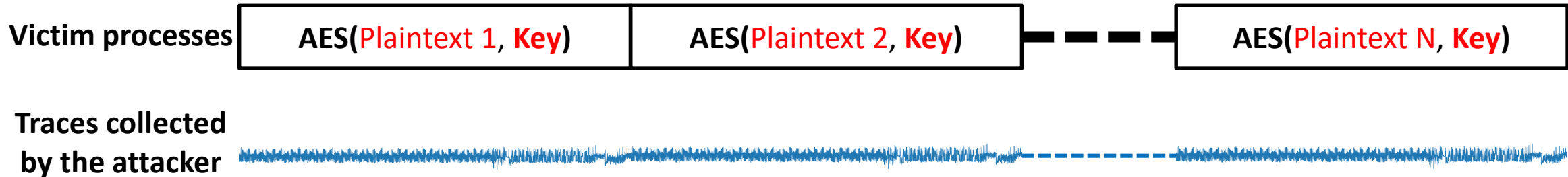
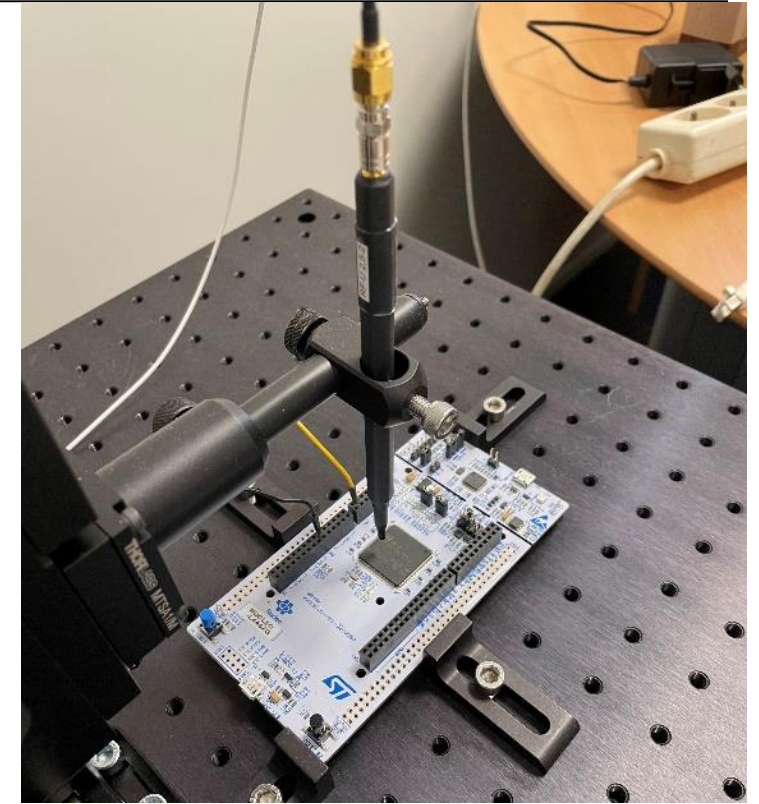
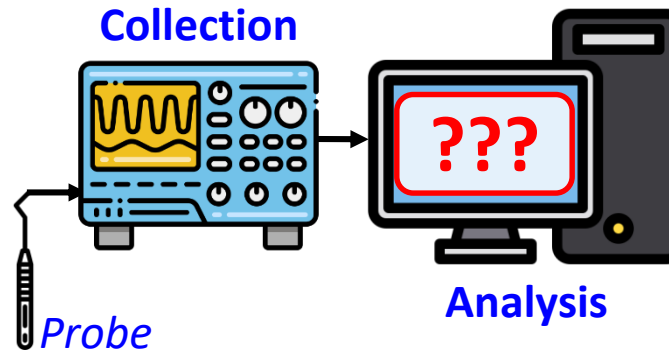
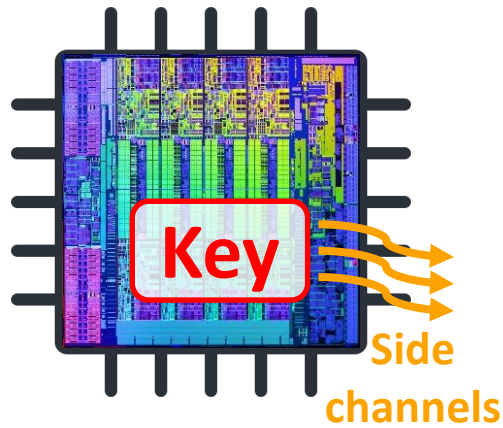




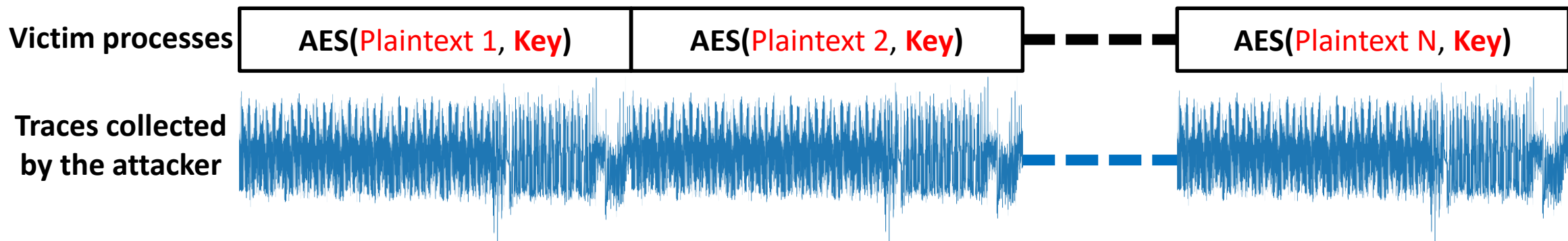
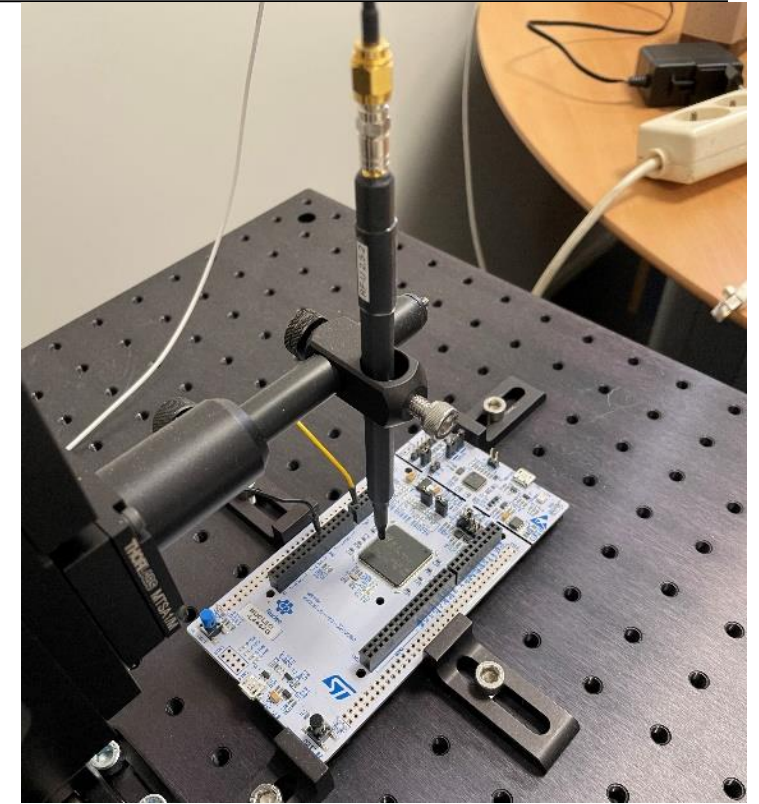
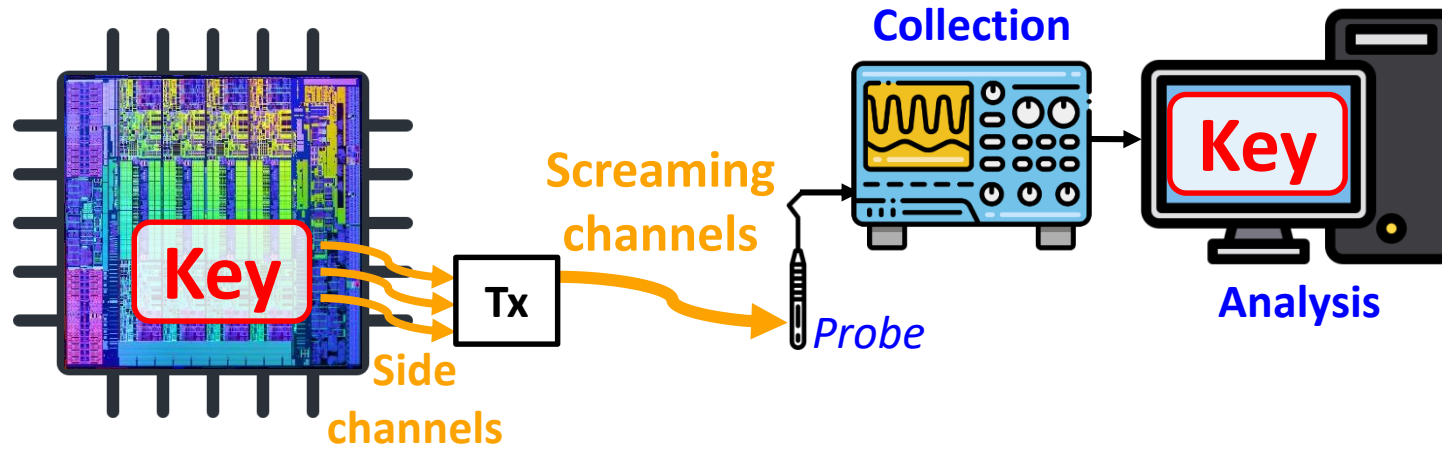
Limitation: Needs proximity



Limitation: Needs proximity

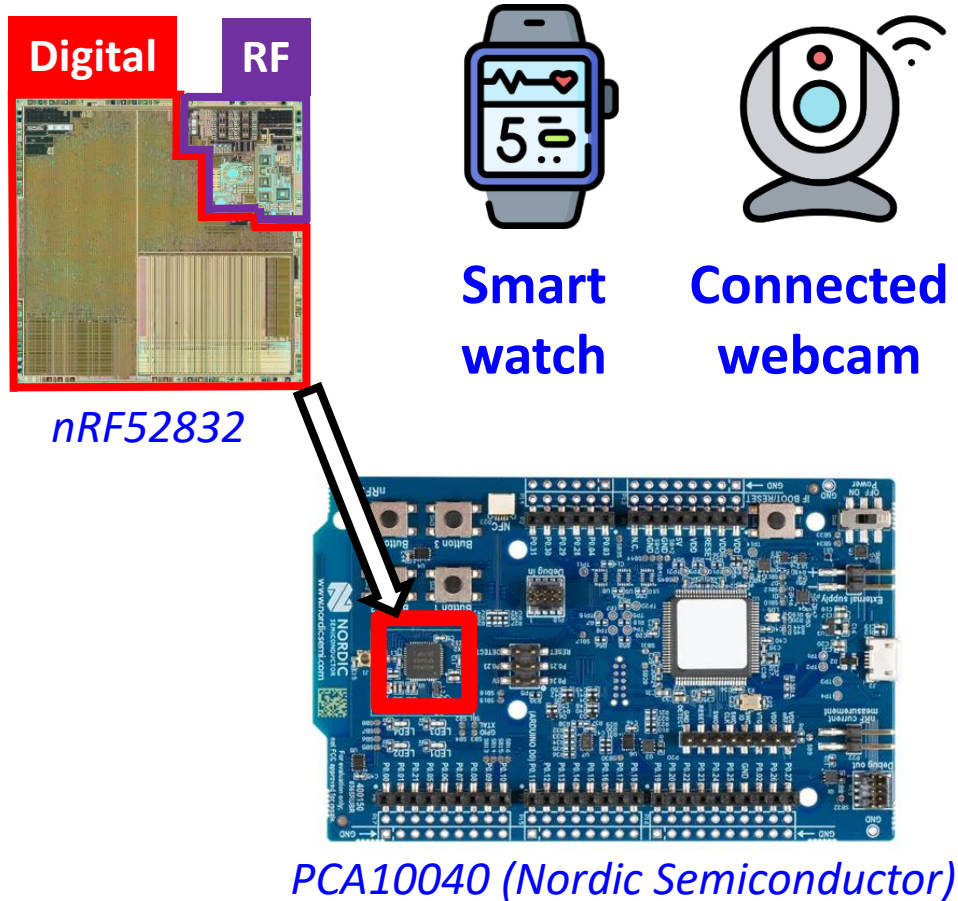


## Screaming-channel attacks



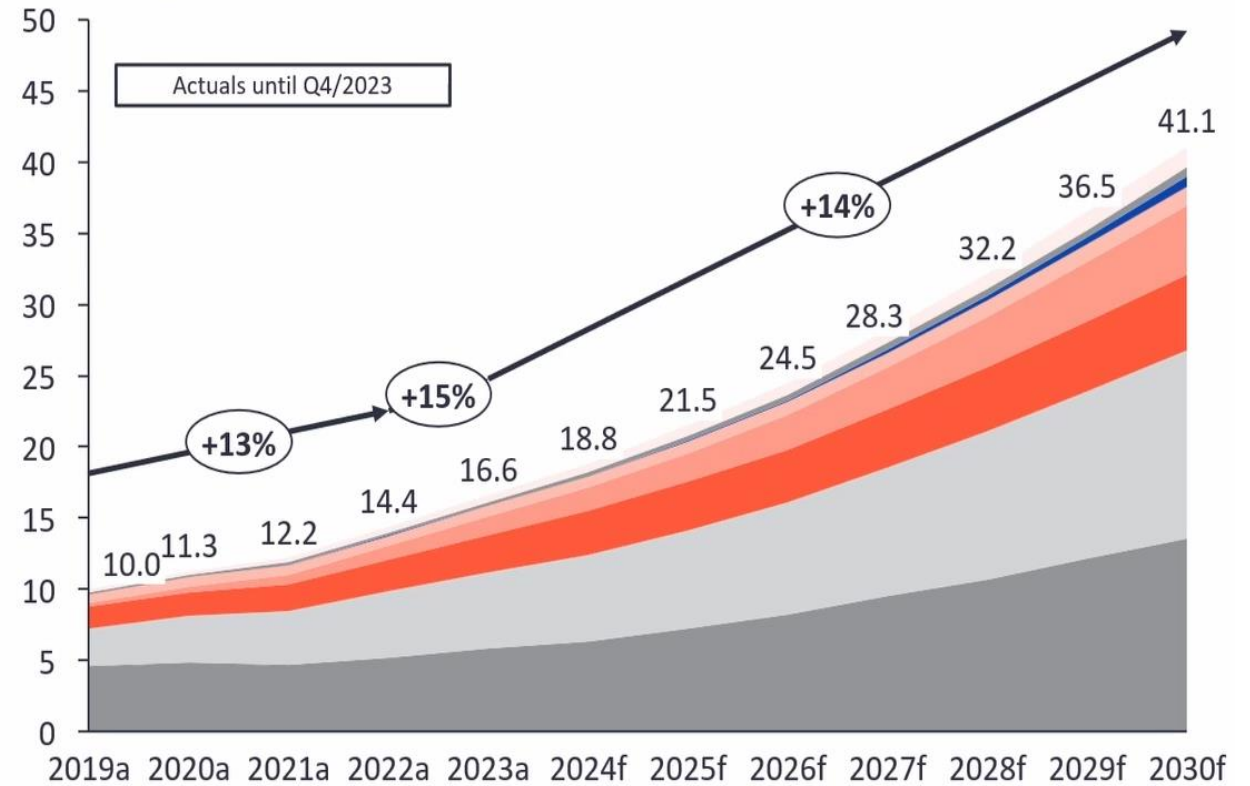


## Mixed-signal devices



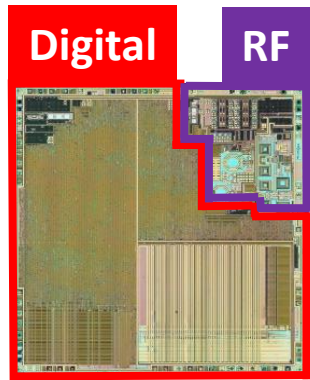
## Global IoT market forecast

Number of global active IoT connections (installed base) in billions

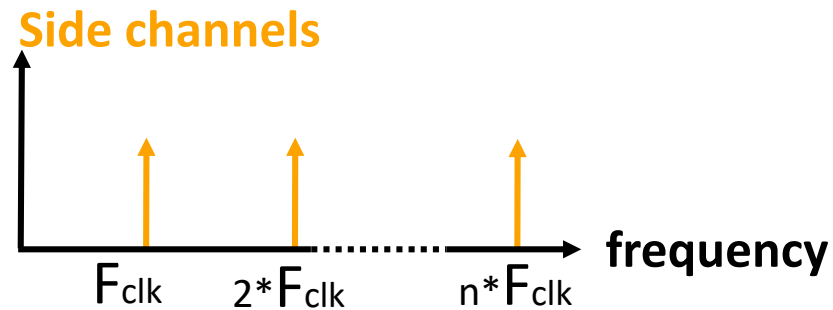
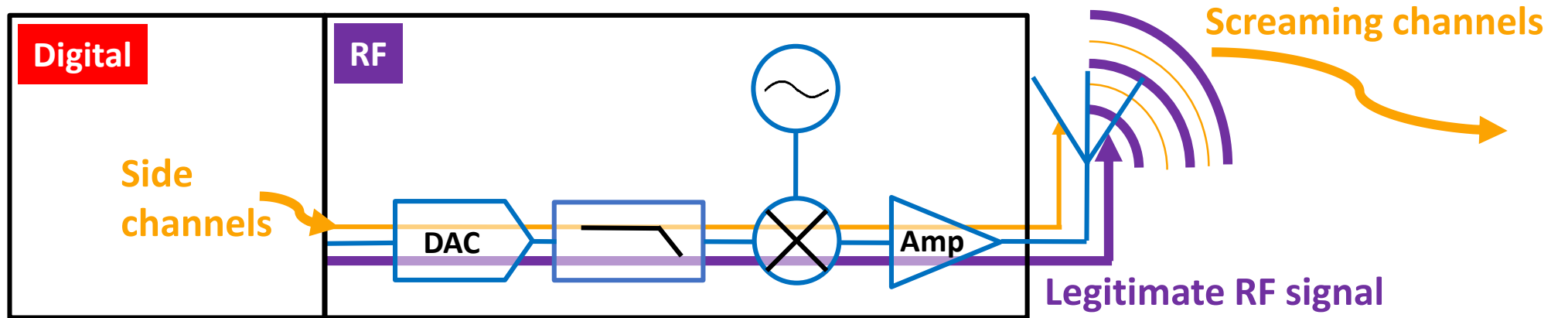


Source: <https://iot-analytics.com/number-connected-iot-devices/>

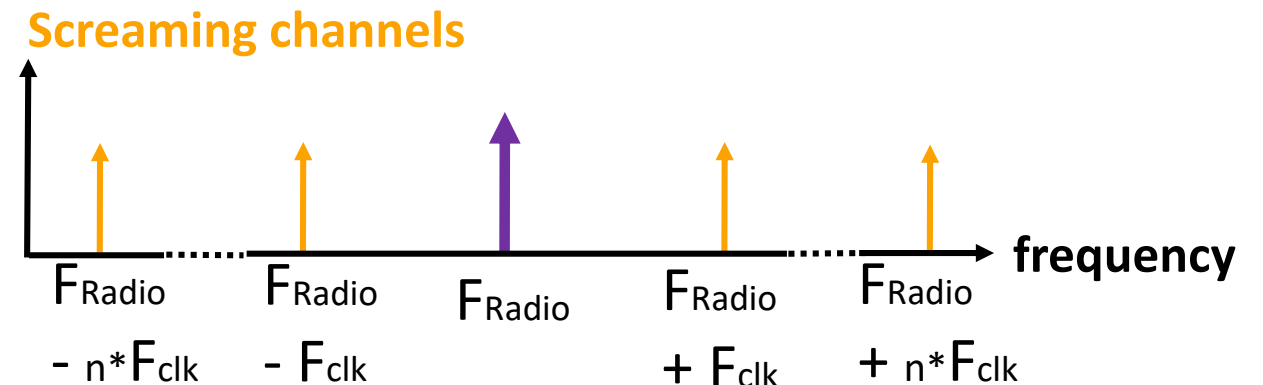
Side-channels transmitted at a large distance



*nRF52832*

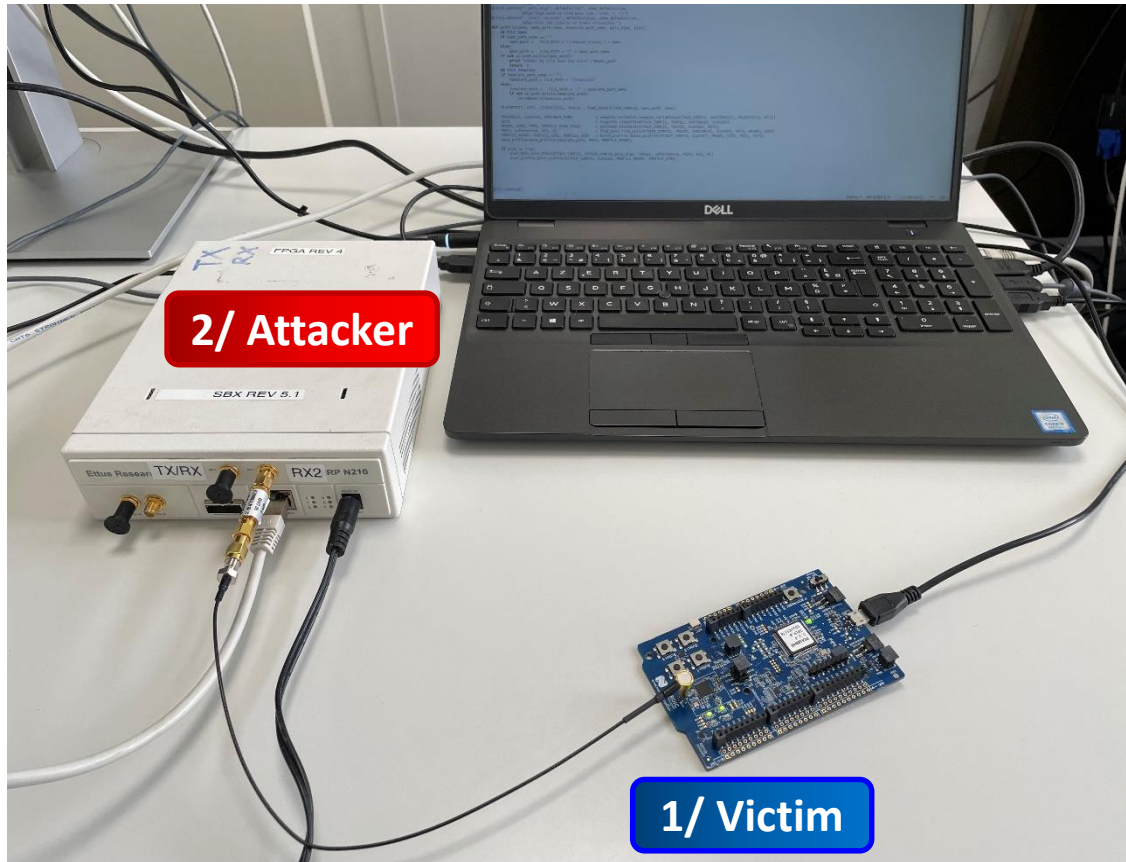


$F_{clk}$  = Digital clock frequency





## Leakage collected by cable



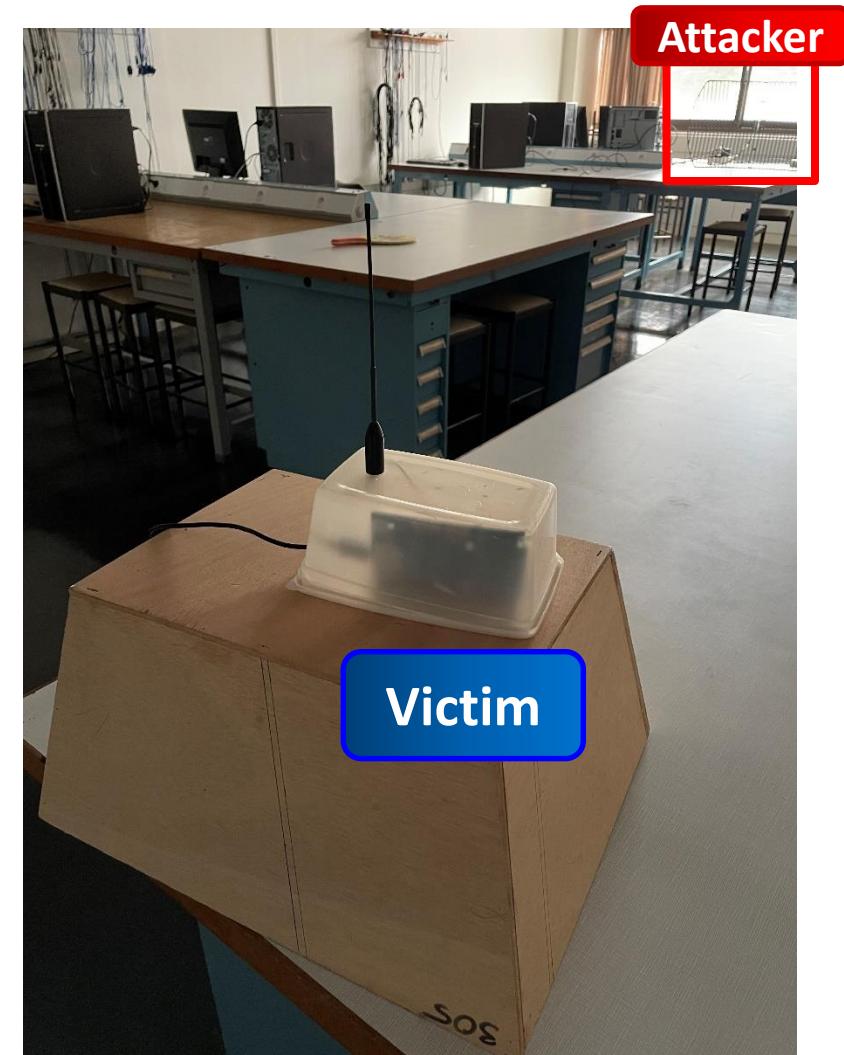
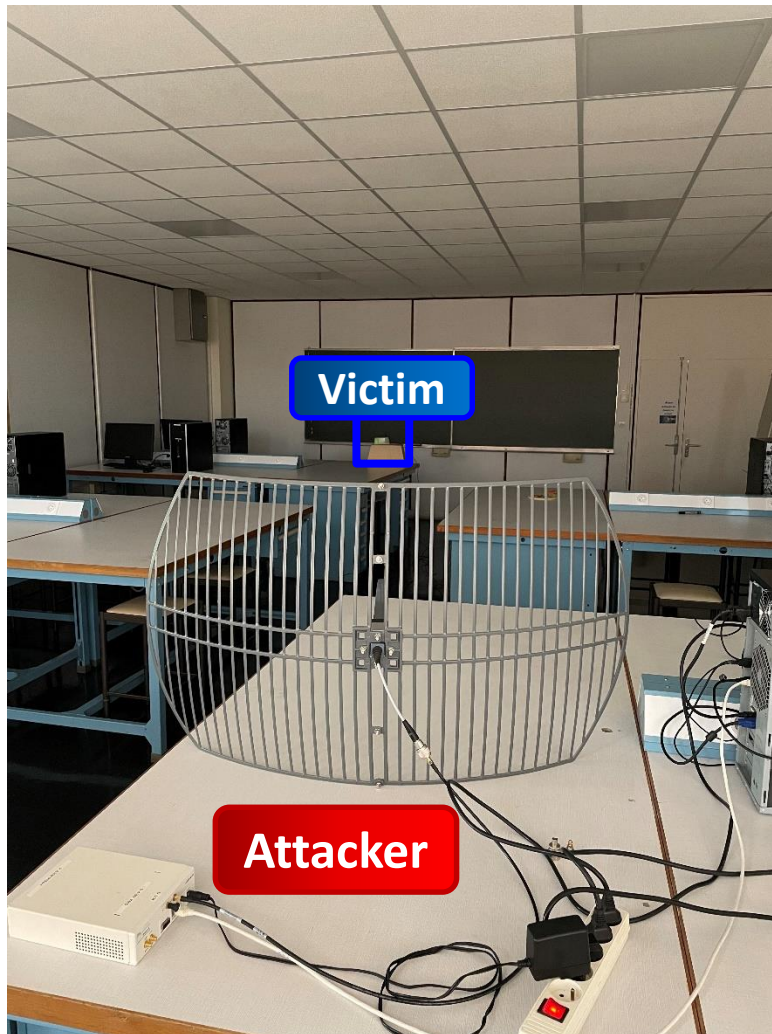
### 1) Victim device: nRF52832

- Low cost device for IoT applications
- Digital part: ARM cortex M4
- RF part: Bluetooth module

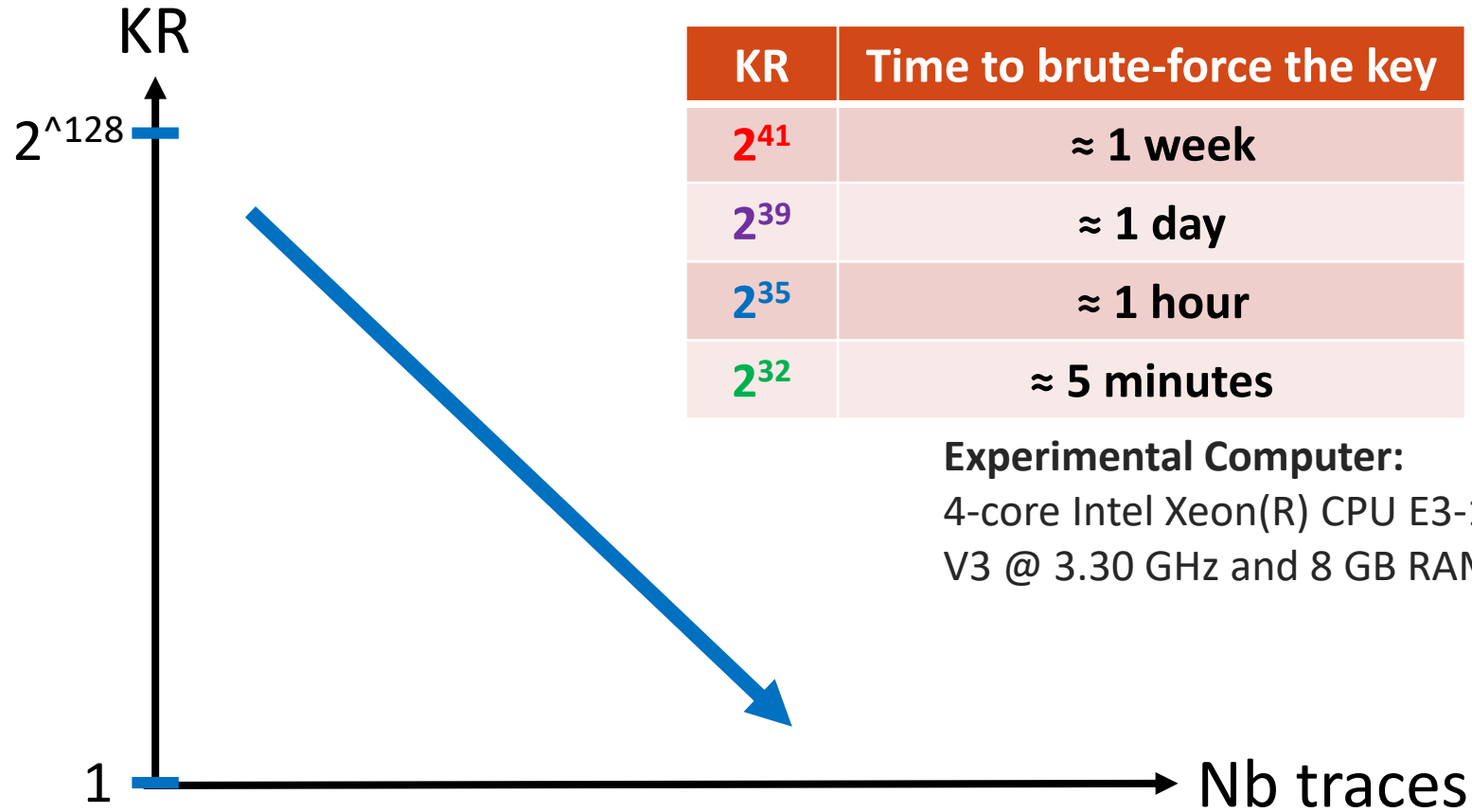
### 2) SDR (Software Defined Radio): USRP N210

- Low cost
- open software

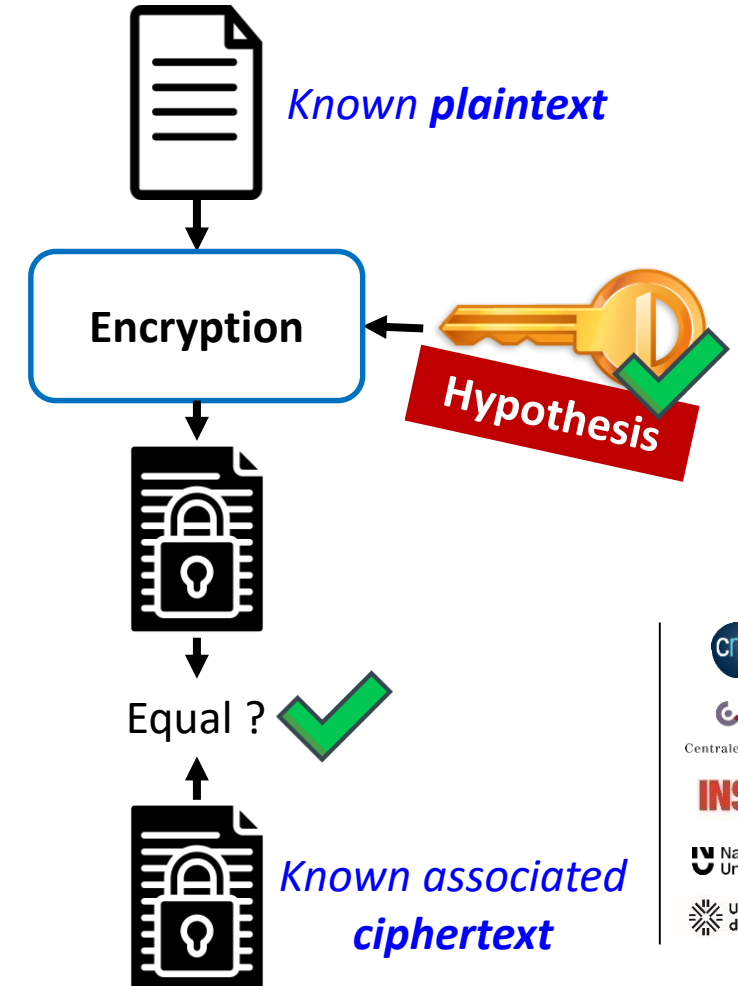
## Leakage collected at distance



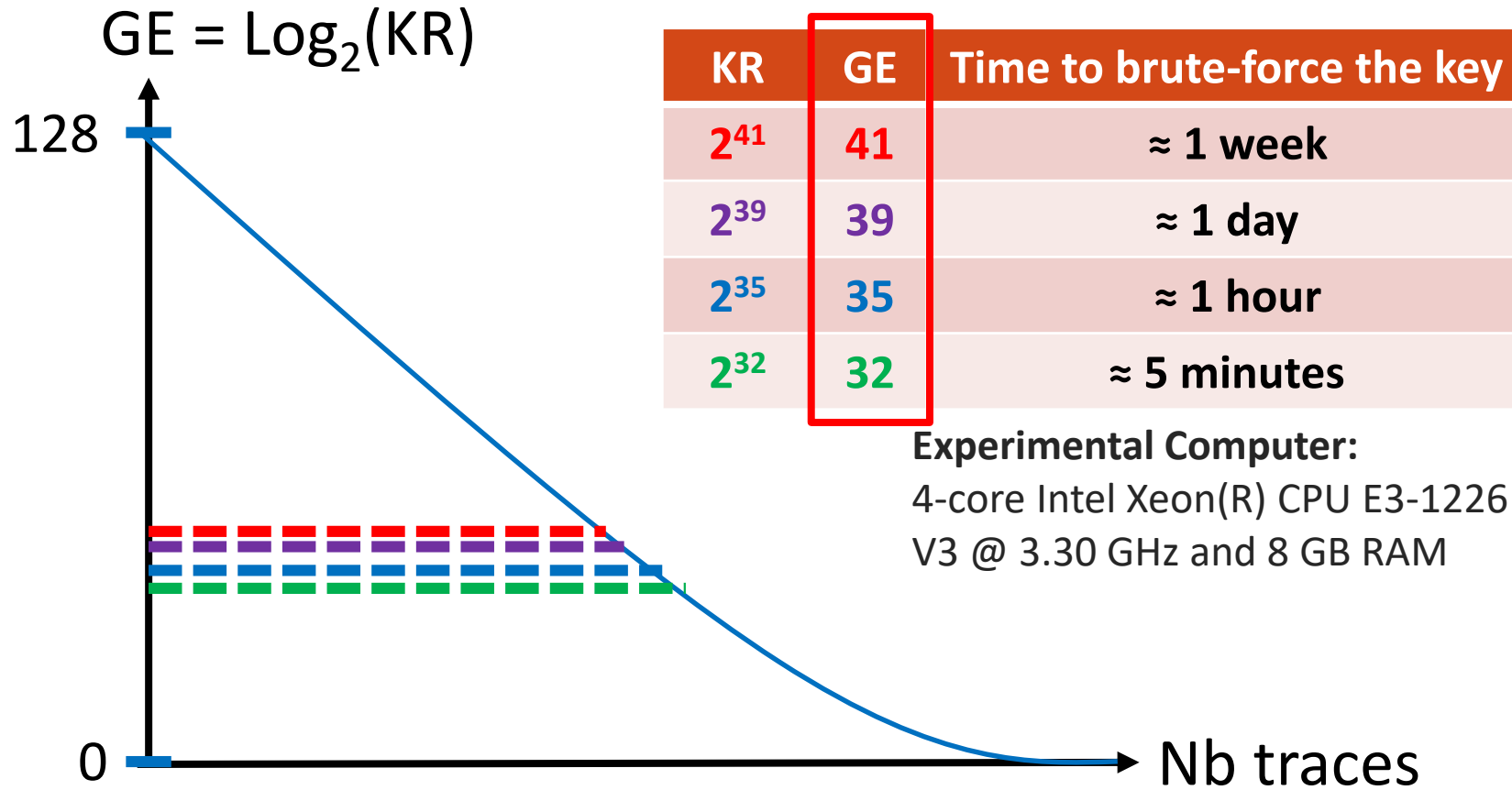
## Key Rank (KR)



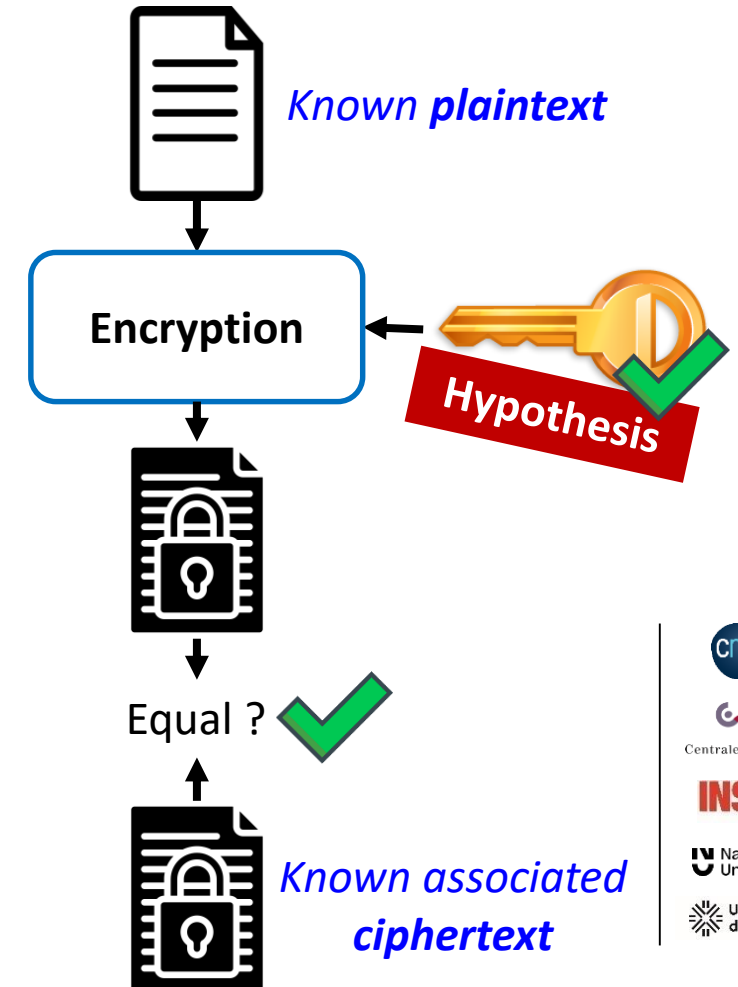
## Brute-force attack:



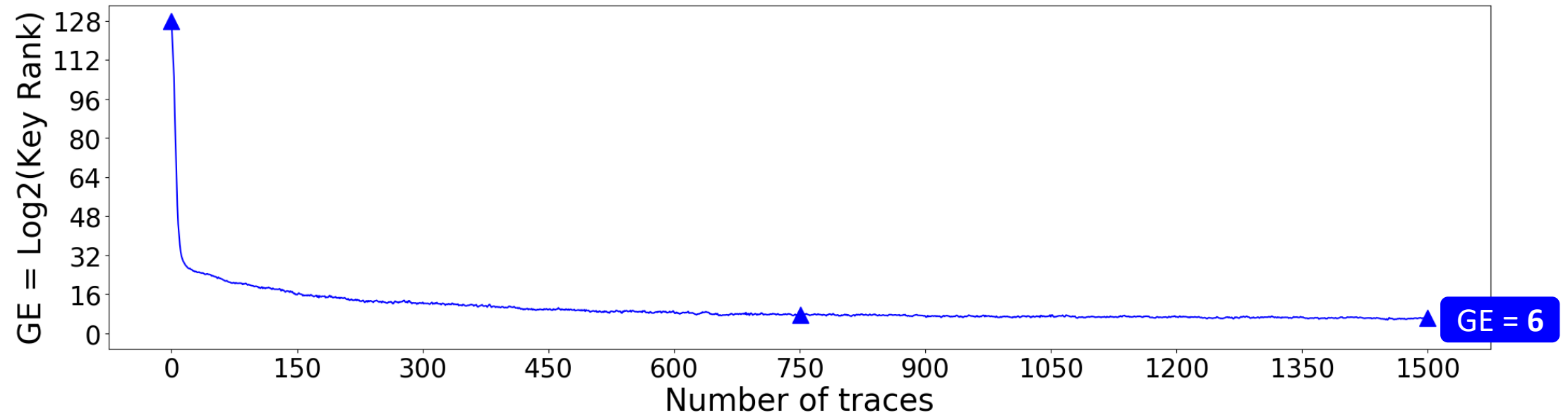
## Guessing Entropy (GE)



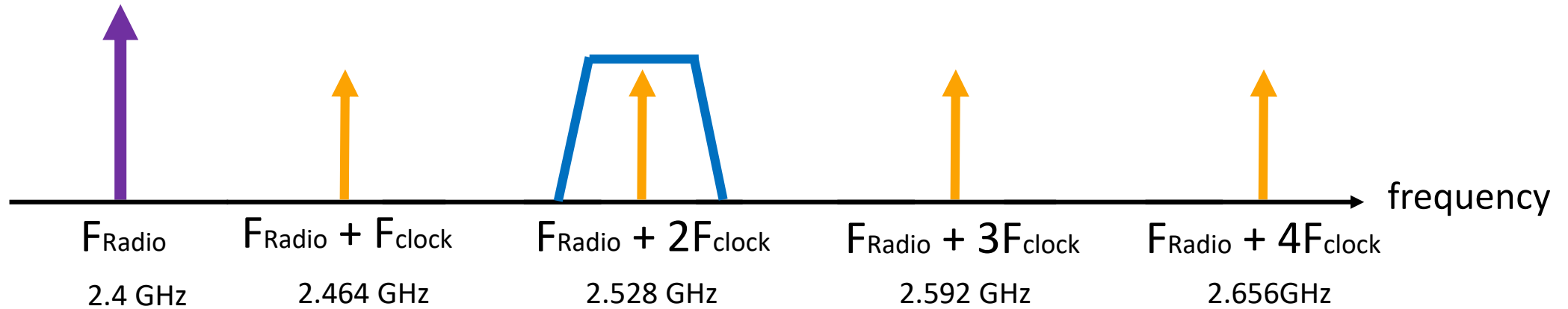
## Brute-force attack:



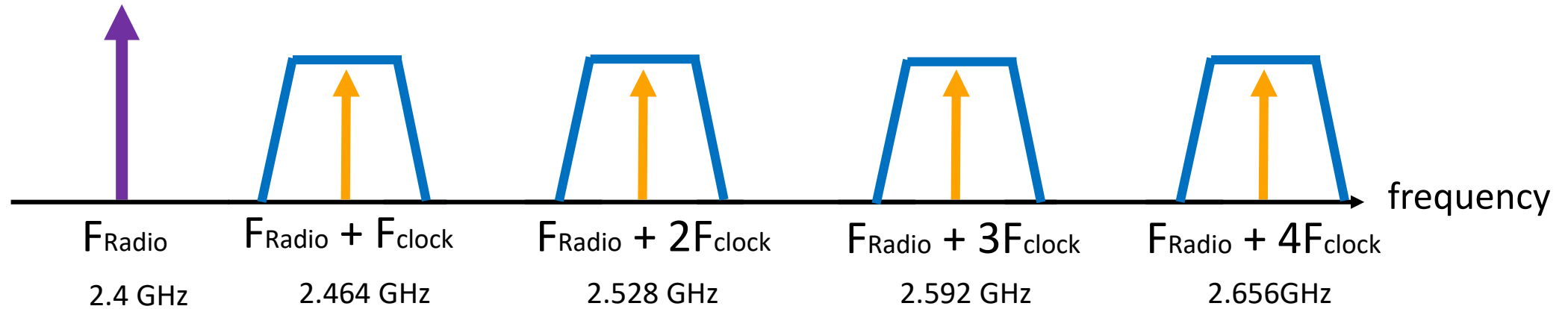
## Initial performance







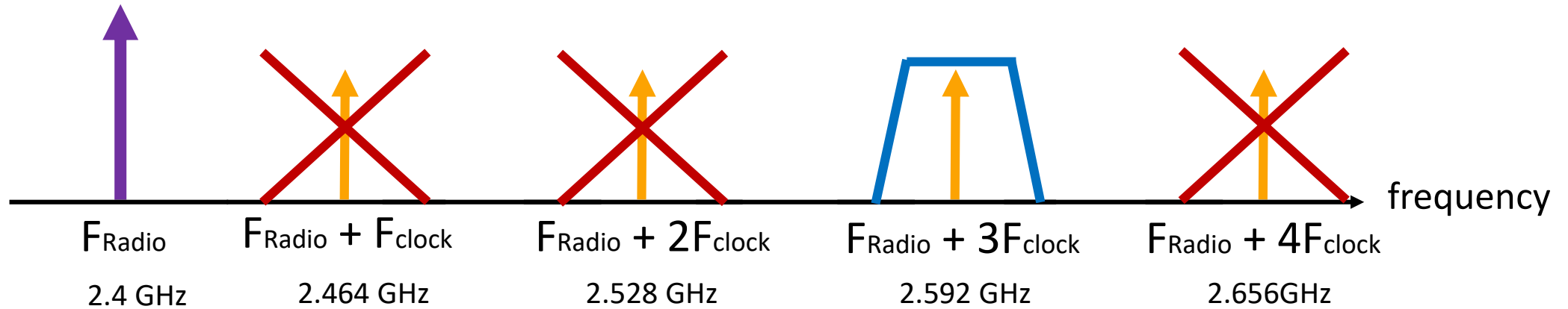
- The leakage is present at each harmonic of the digital clock frequency
- Previous works [2][3][4] on screaming channel used only the second at 2,528 GHz



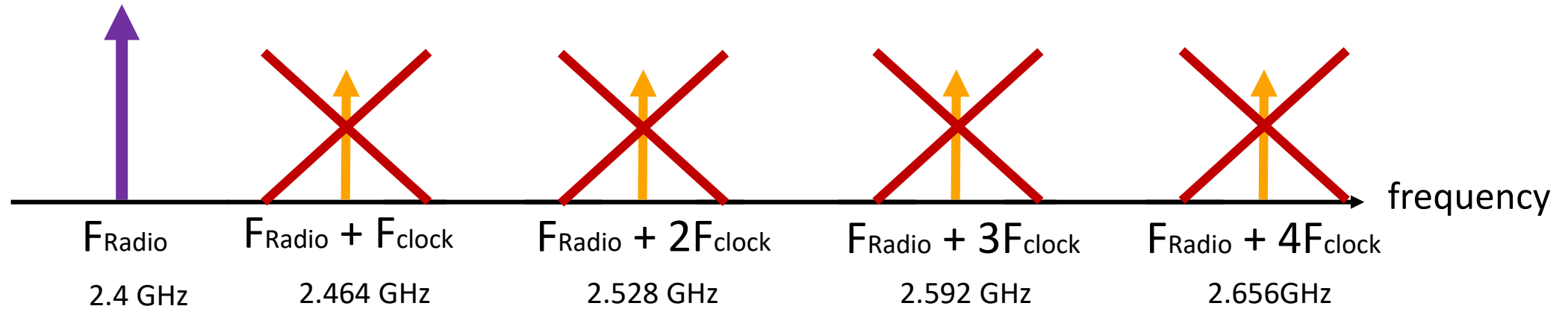
## Question:

Can we improve the attack by combining multiple harmonics?





- Only one harmonic is both unpolluted and sufficiently strong to mount a successful attack

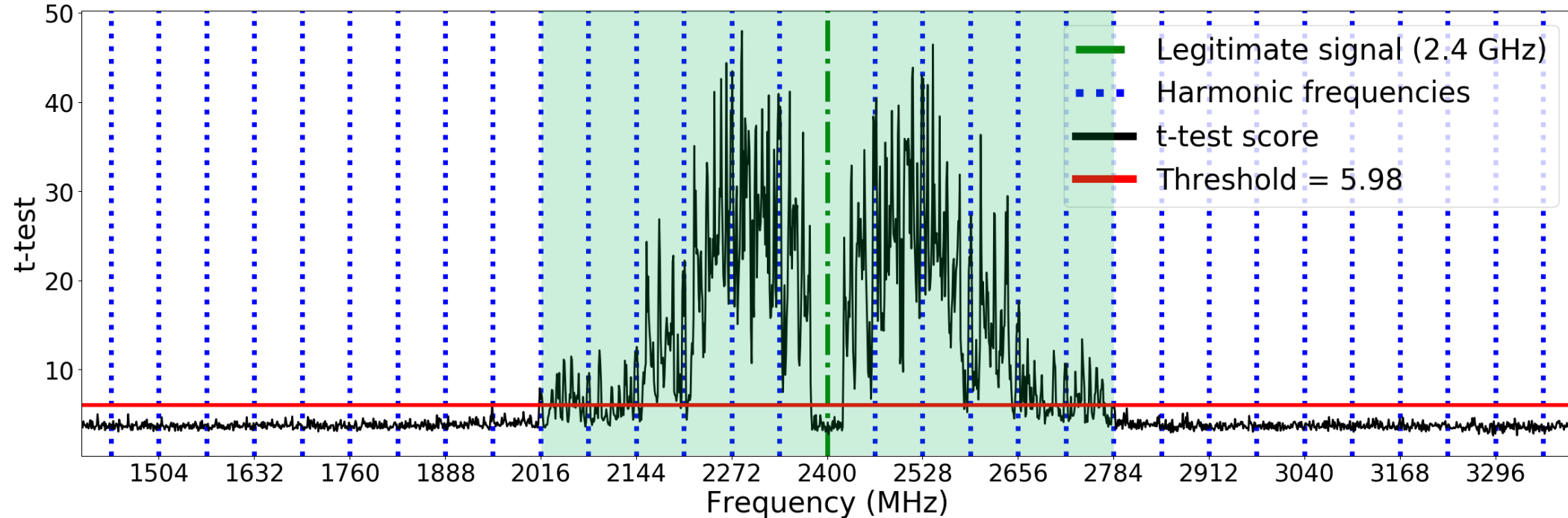


## Questions:

- What happen if all harmonics are polluted?
- Can we use other frequencies?



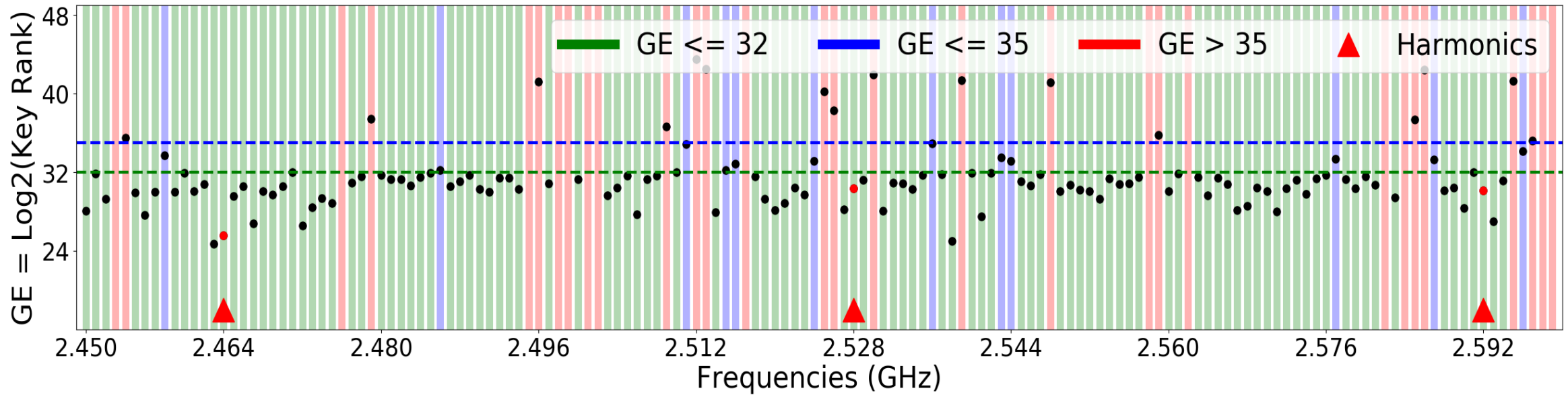
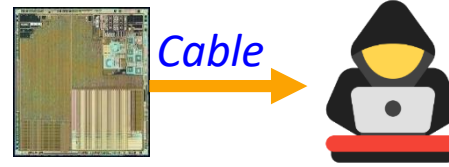
## T-test results



- Range of selected frequencies: 1,4GHz – 3,4GHz (1MHz resolution)
- t-test: fixed vs fixed [8]
  - 1000 collected traces per frequency
  - Leakage is detected if  $t\text{-test} \geq 5,98$  (Computed from [9])



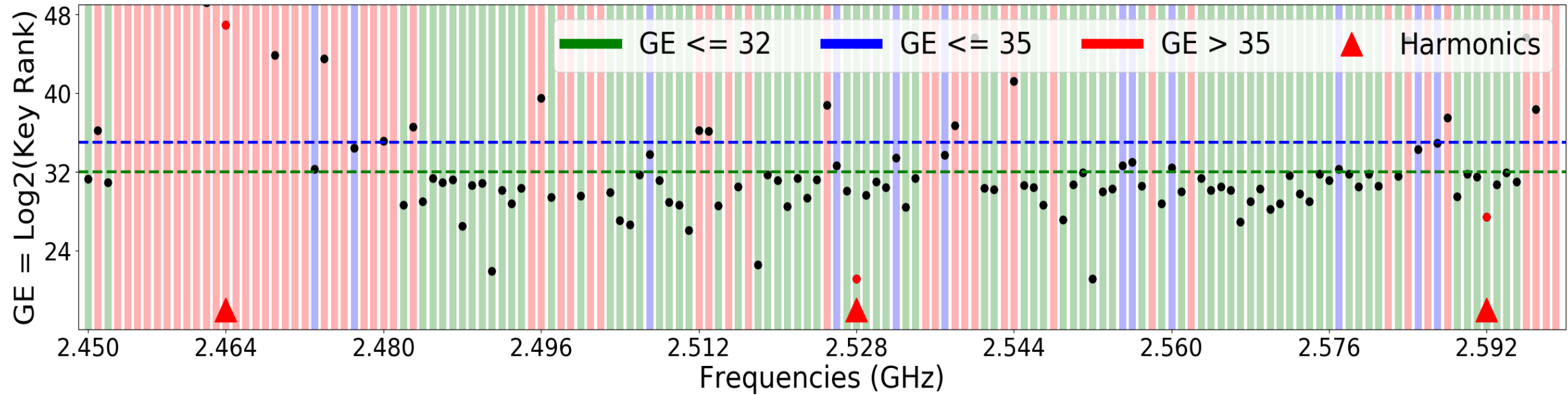
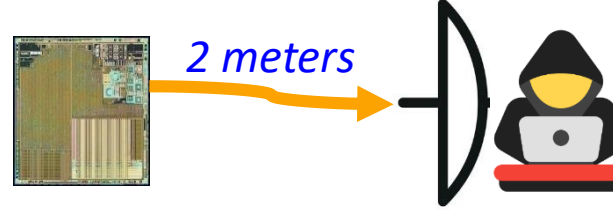
By cable:



- Profiling phase: 15k Traces
- Attacking phase: 15k Traces

GE	Time to bruteforce the key
32	≈ 5 minutes
35	≈ 1 hour
39	≈ 1 day
41	≈ 1 week

At 2 meters:

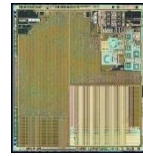


- Profiling phase: 15k Traces
- Attacking phase: 15k Traces

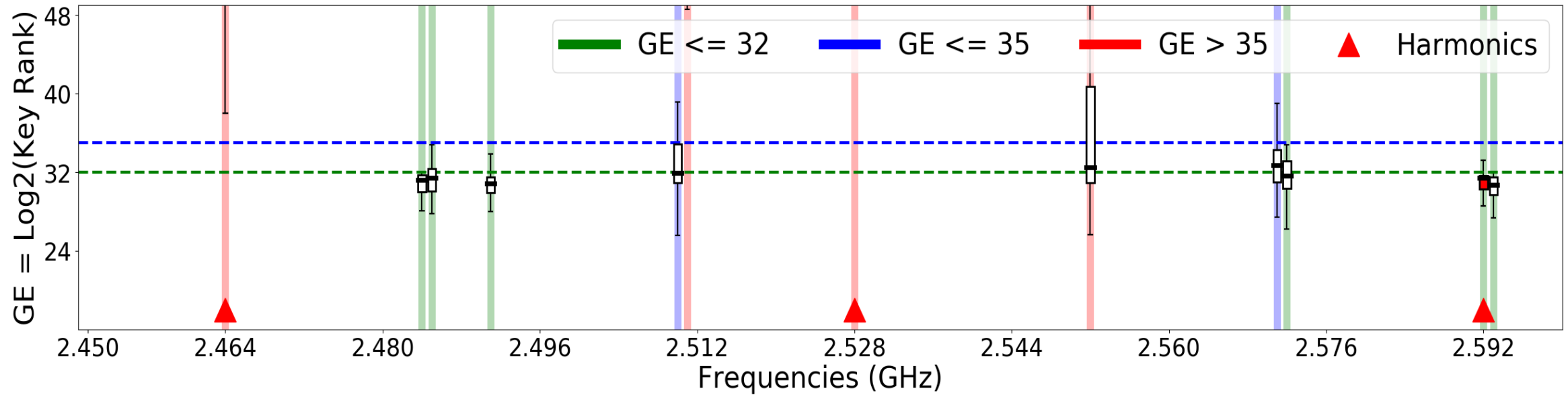
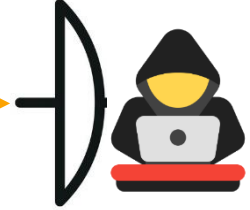
→ Loss of the first harmonic

GE	Time to bruteforce the key
32	≈ 5 minutes
35	≈ 1 hour
39	≈ 1 day
41	≈ 1 week

At 7 meters, 50 attacks per frequency:



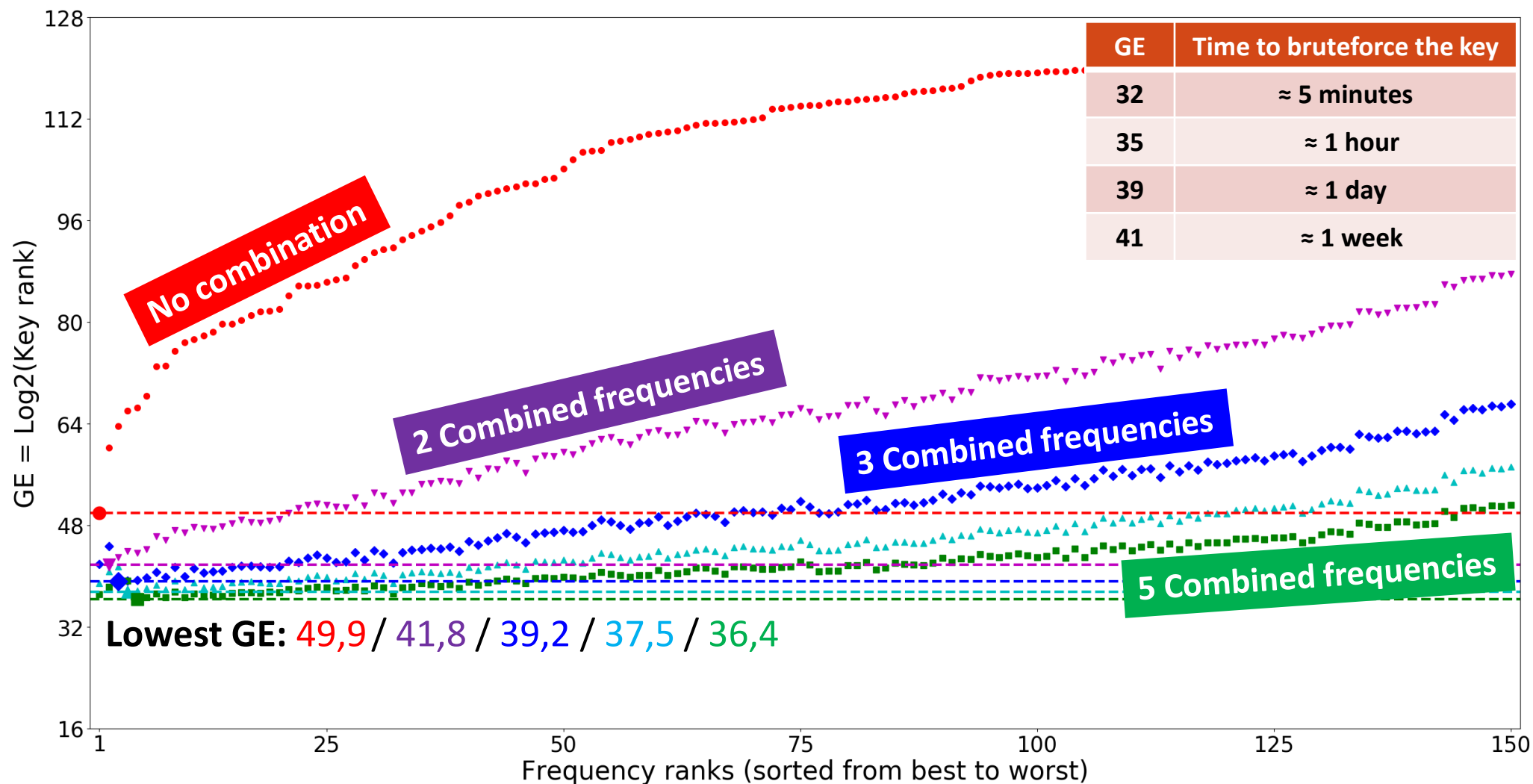
7 meters



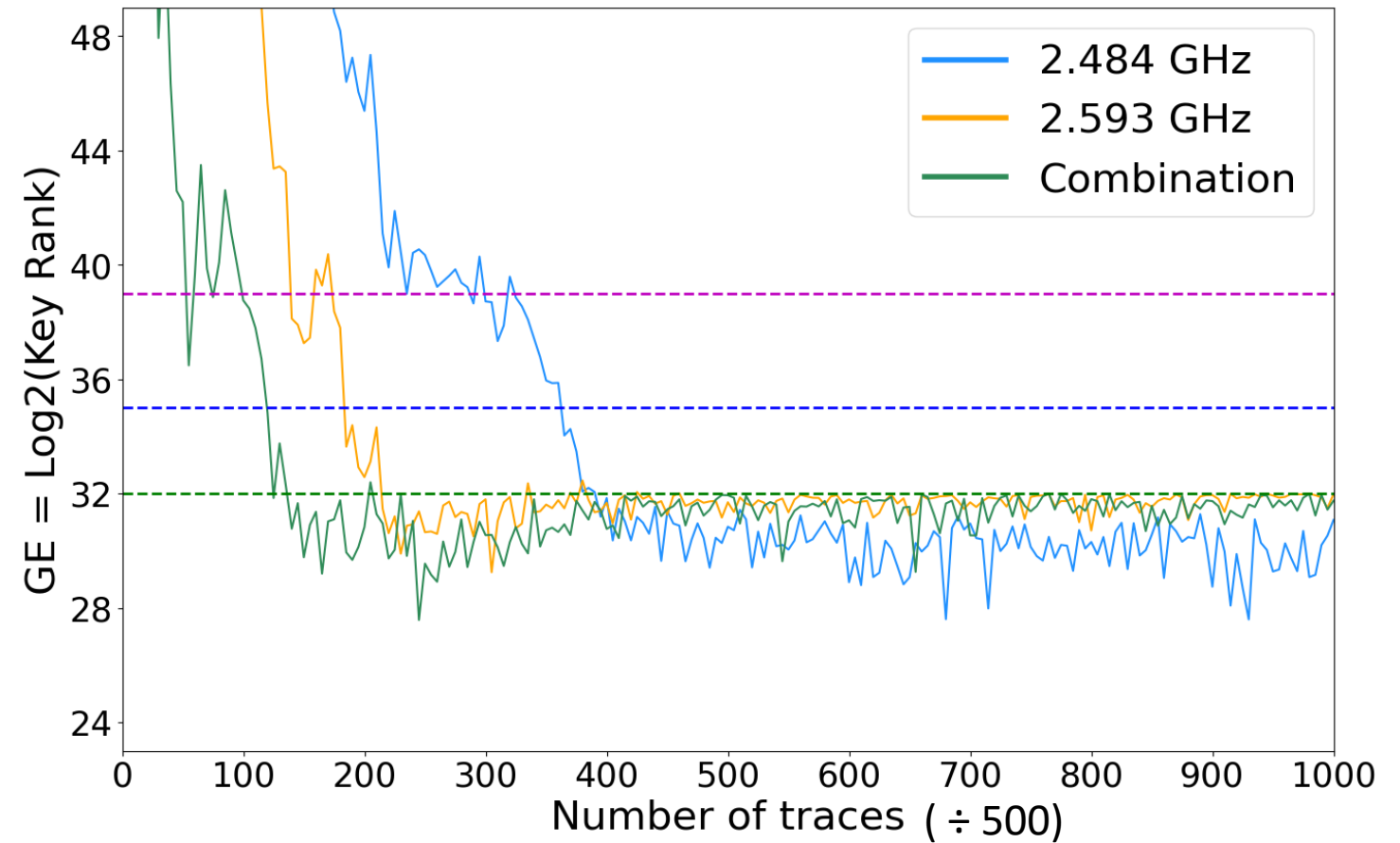
- Profiling phase: 15k Traces
- Attacking phase: 750 Traces

→ Loss of the 2 first harmonics

GE	Time to bruteforce the key
32	≈ 5 minutes
35	≈ 1 hour
39	≈ 1 day
41	≈ 1 week

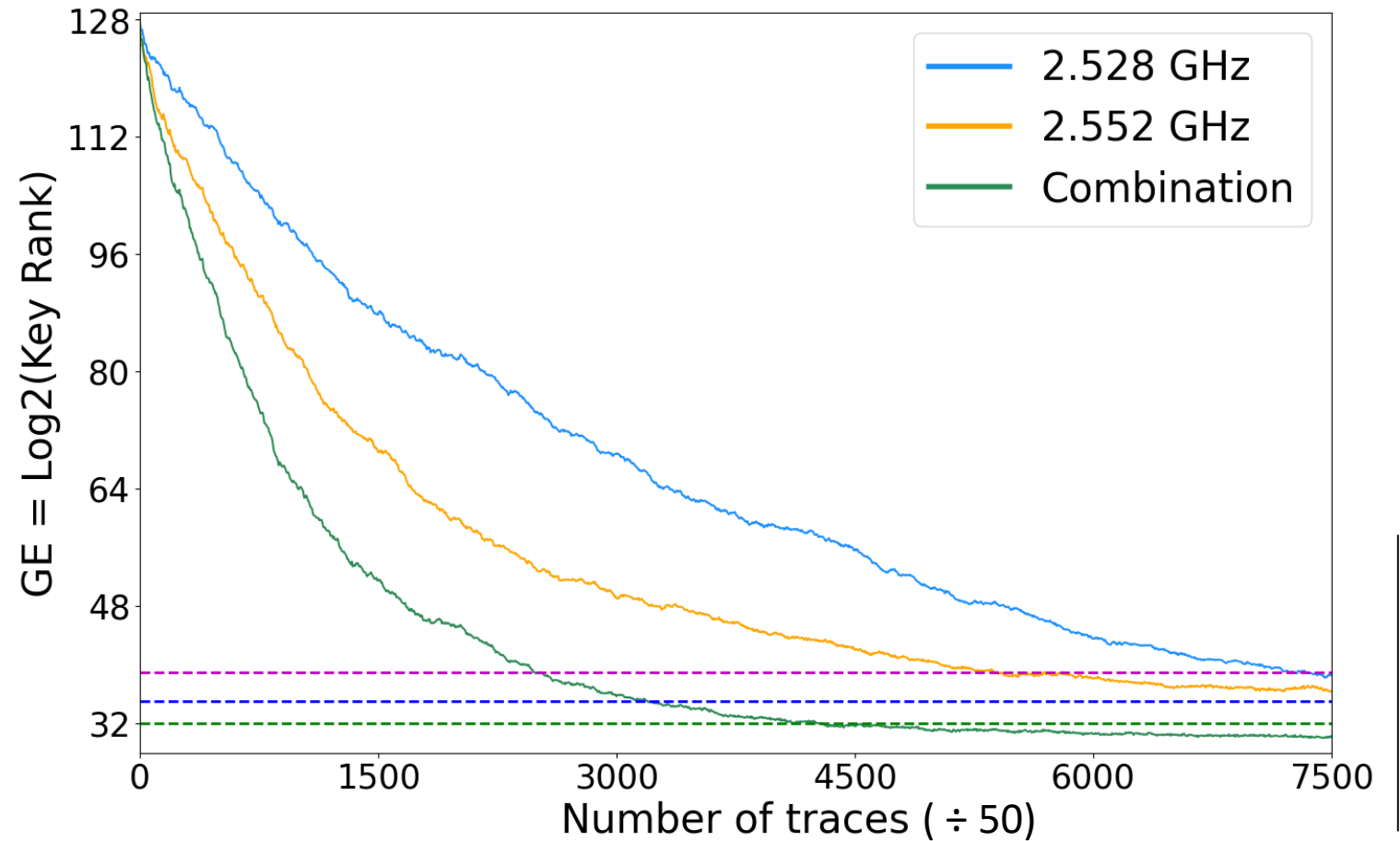


## Attacking at 15 meters





## Attacking at 30 meters



➤ How to detect the most optimal frequencies to mount an attack in an unknown polluted environment ?



➤ How to optimize the attack performance improvement with frequency combination ?  
With frequency and spatial diversity?



➤ Can we attack more complex systems by analyzing the impact of the digital activity on analog characteristics of the DAC, e.g., Total Harmonic Distortion ?





**Thank you !  
Do you have any questions?**

E-mail:  
[Jeremy.guillaume@univ-ubs.fr](mailto:Jeremy.guillaume@univ-ubs.fr)

## ➤ Synchronization challenges at a distance from the victim

[5] J.Guillaume, M.Pelcat, A.Nafkha, R.Salvador, “Virtual Triggering: a Technique to Segment Cryptographic Processes in Side-Channel Traces,” IEEE SIPS, 2022.



## Frequency diversity

### ➤ Attacking at non-harmonic frequencies

[6] J.Guillaume, M.Pelcat, A.Nafkha, R.Salvador, “Attacking at non-harmonic frequencies in screaming-channel attacks,” CARDIS, 2023.



### ➤ Frequency combination

[10] J.Guillaume, M.Pelcat, A.Nafkha, R.Salvador, “Frequency Combination: multi-channel attacks in the context of screaming-channels,” Submitted at IEEE Transactions on Information Forensics & Security (TIFS).

