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

Attacking at non-harmonic frequencies in screaming-channel attacks

Jeremy Guillaume[1]

Directeur de thèse: Maxime Pelcat[2]

Co-directeur: Amor Nafkha[1]

Encadrant: Ruben Salvador [3]

[1] Equipe ASIC, CentraleSupelec, IETR - UMR CNRS 6164

[2] Equipe VAADER, INSA Rennes, IETR - UMR CNRS 6164

[3] Equipe CIDRE, CentraleSupelec, IRISA - UMR CNRS 6074

11/15/2023

www.ietr.fr

Outline

Screaming channel attacks:

- Side-channel leakage transmited by a RF module

Limitation of this attack:

- Polluted harmonics

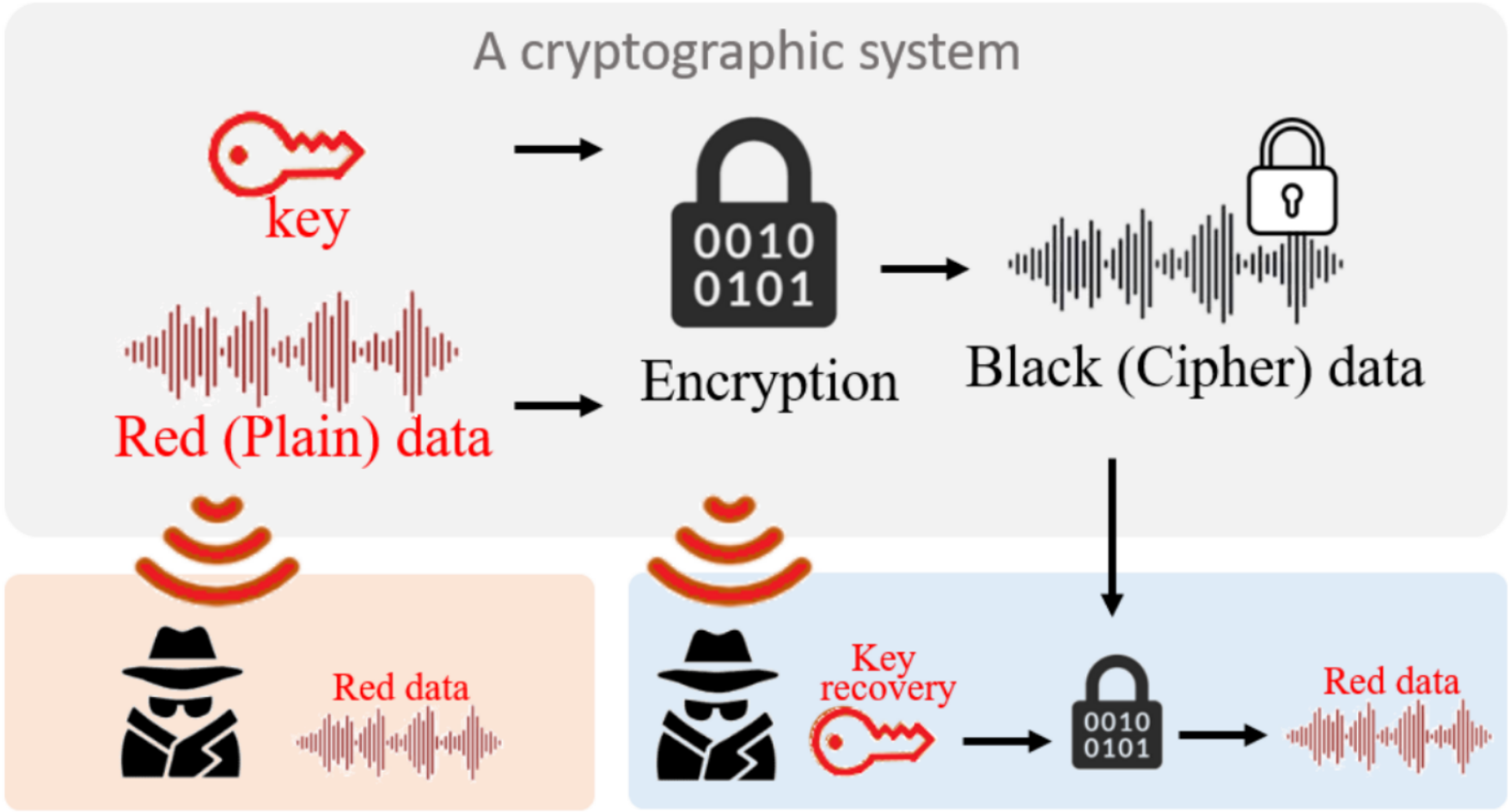
Proposed solution:

- Investigating the screaming-channel attack at other frequencies than the harmonics

Impact on the attack:

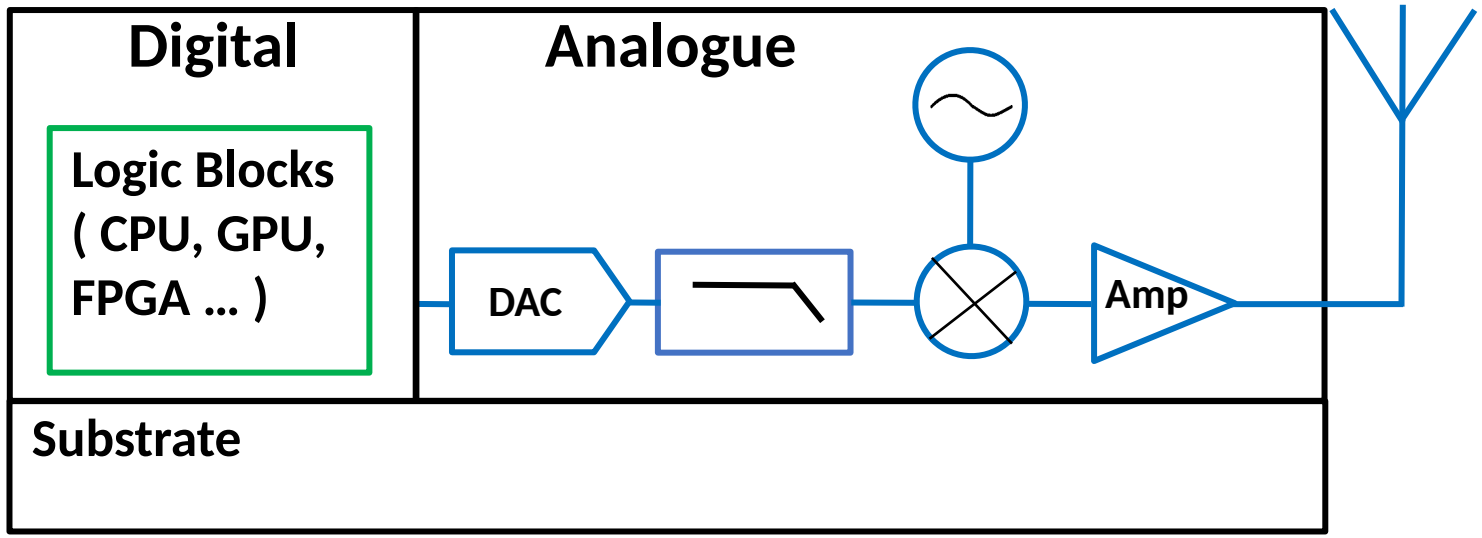
- Demonstrate that non-harmonics are good enough for attacks

Side-channel attacks



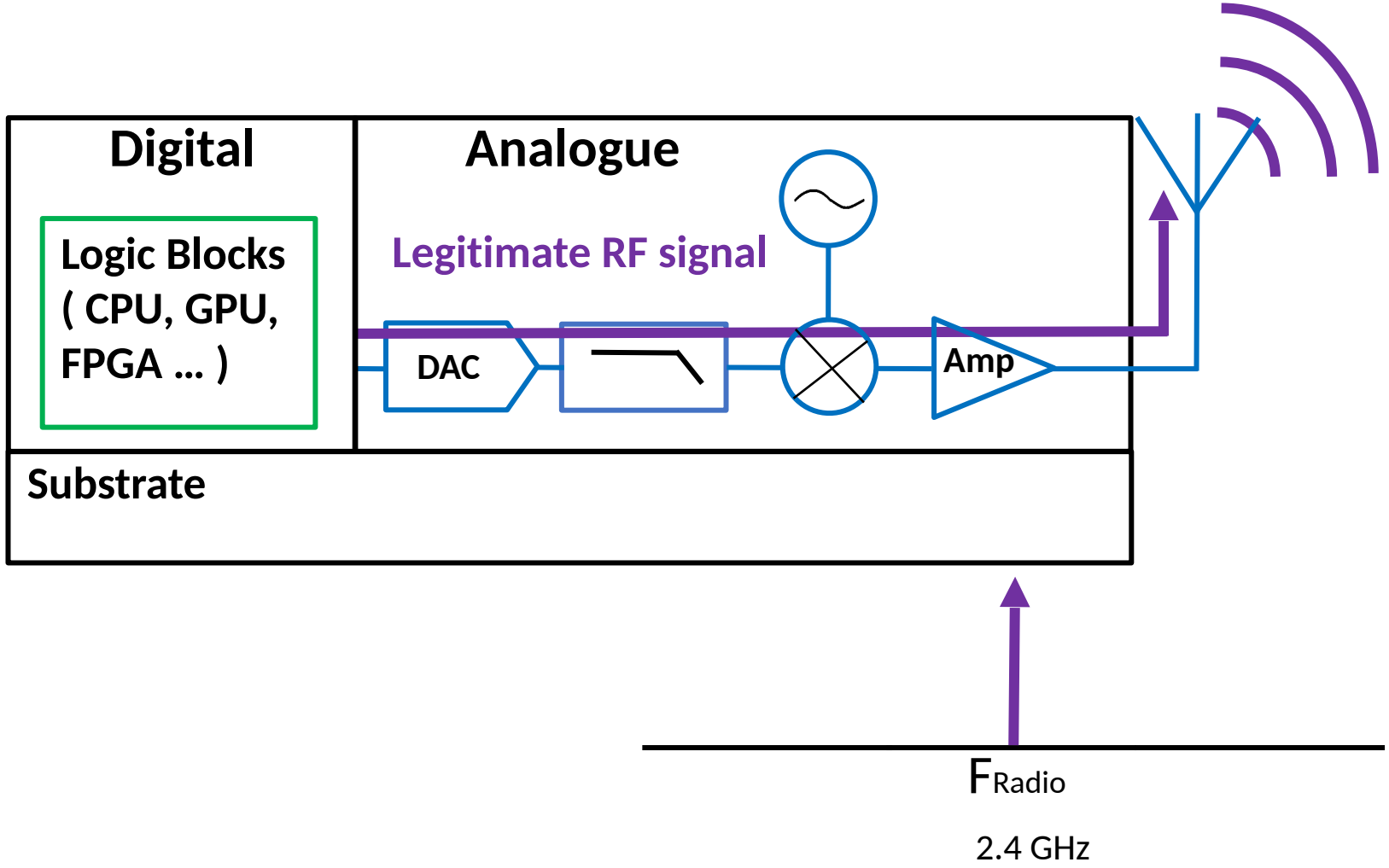
[1] J. Choi, H.-Y. Yang, and D.-H. Cho, “TEMPEST Comeback: A Realistic Audio Eavesdropping Threat on Mixed-signal SoCs,”, ACM SIGSAC, 2020.

Screaming channel attacks



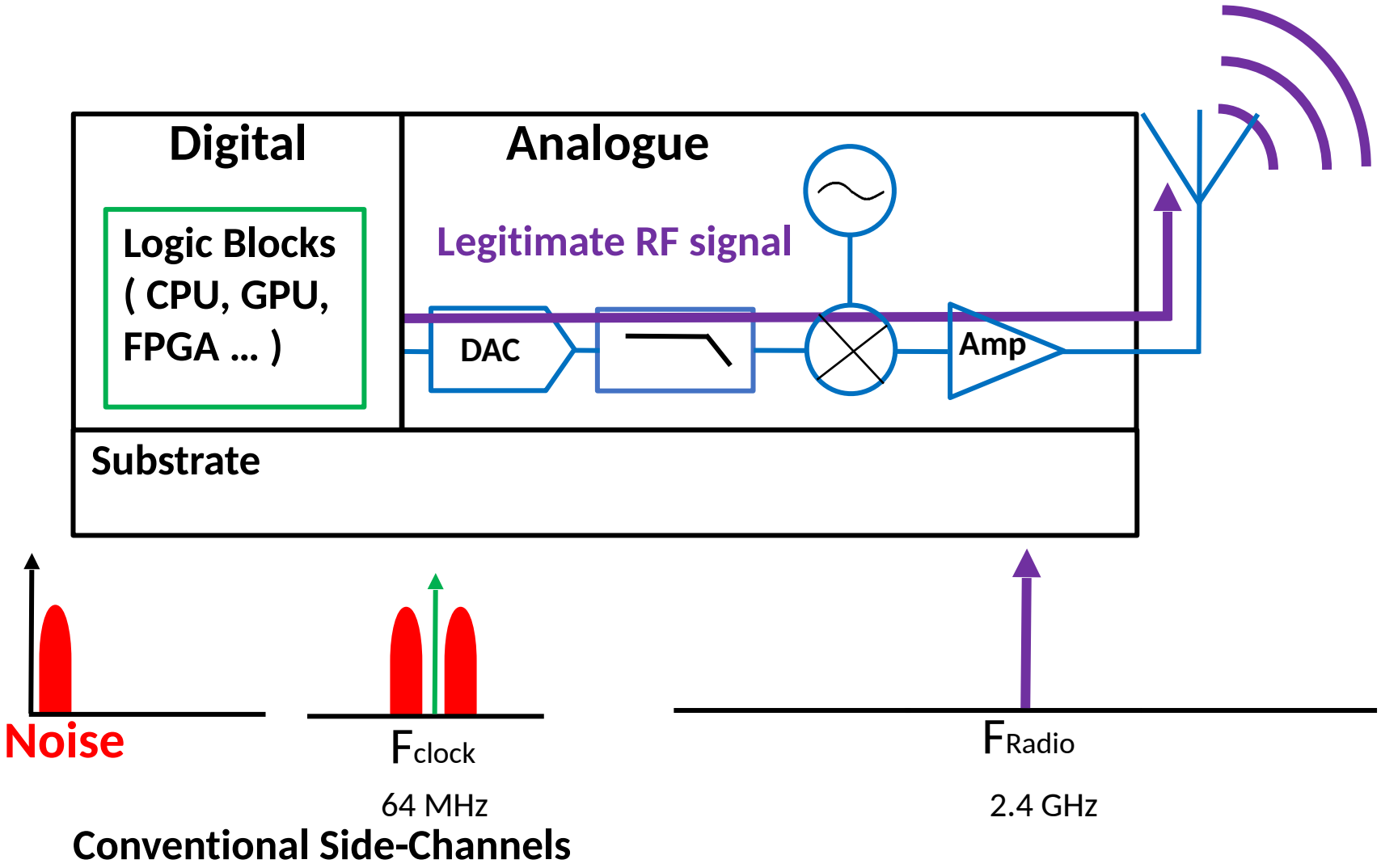
[2] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," ACM SIGSAC, 2018

Screaming channel attacks



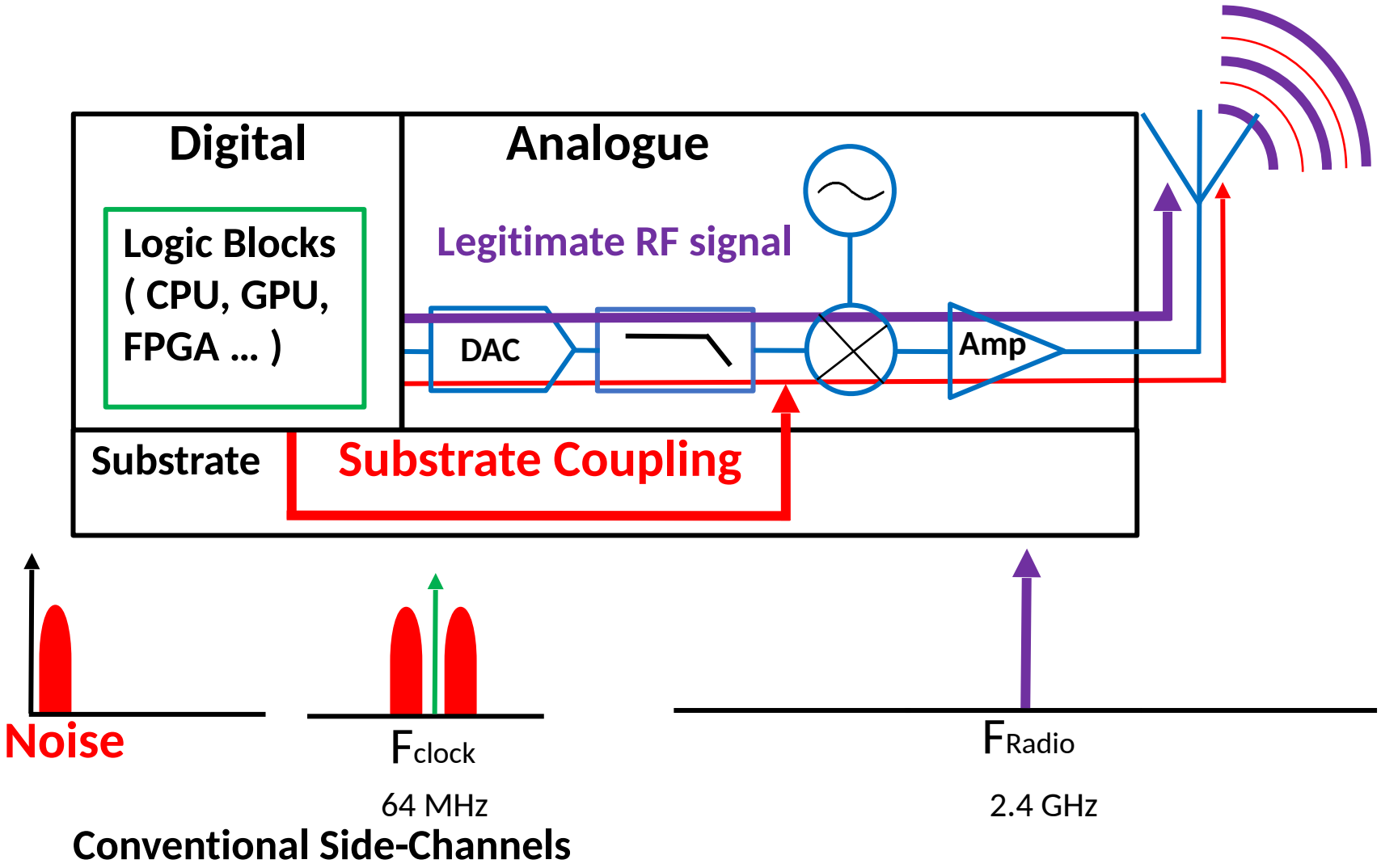
[2] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," ACM SIGSAC, 2018

Screaming channel attacks



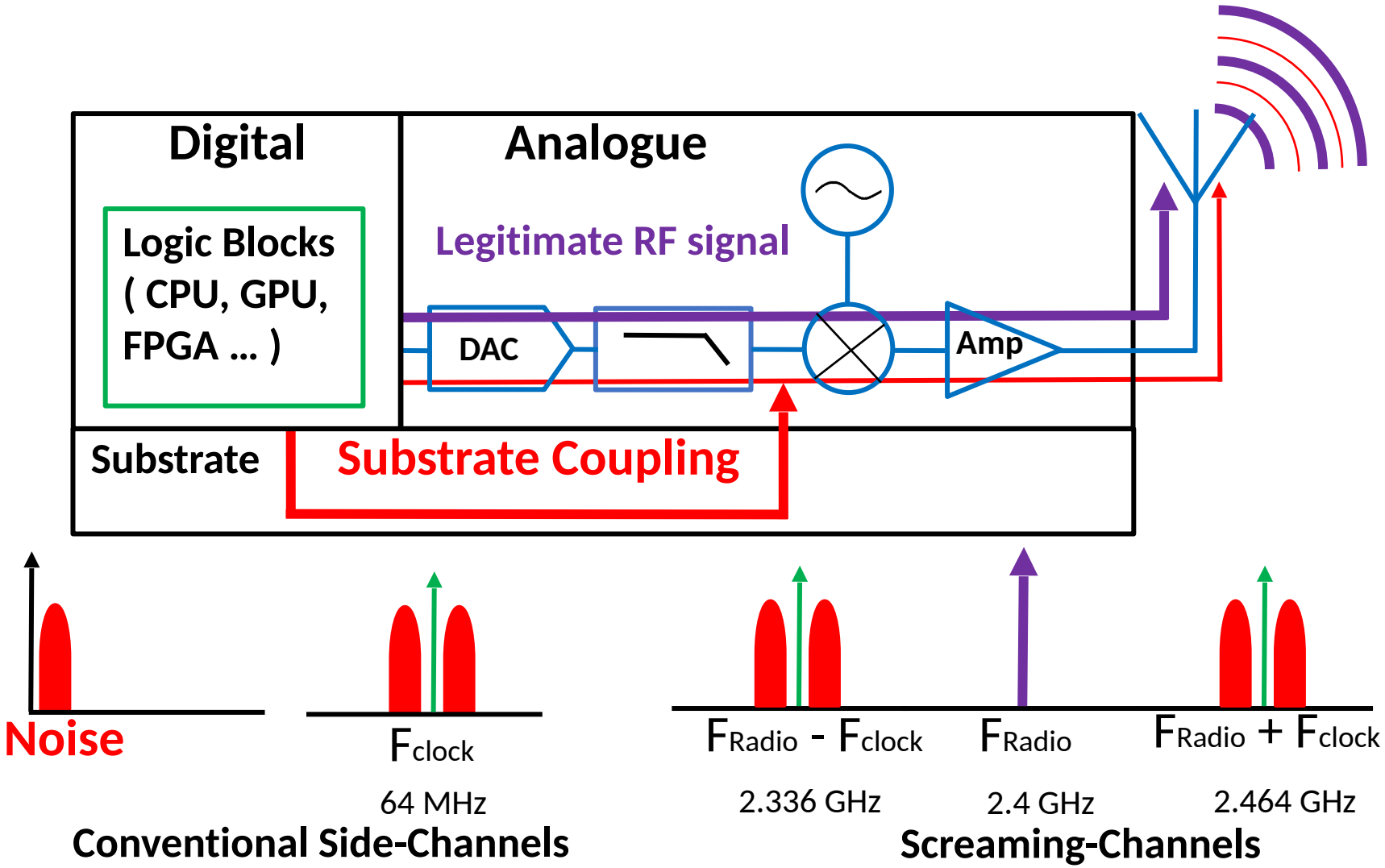
[2] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," ACM SIGSAC, 2018

Screaming channel attacks



[2] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," ACM SIGSAC, 2018

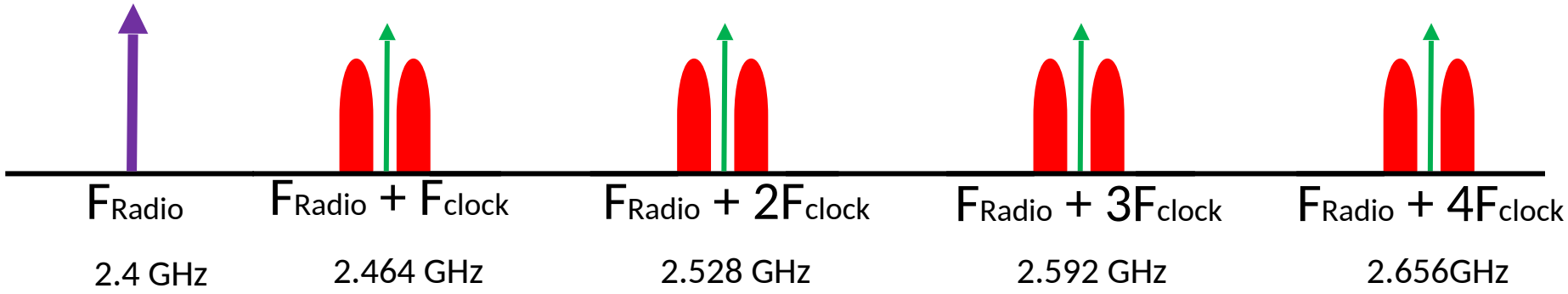
Screaming channel attacks



[2] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," ACM SIGSAC, 2018

Frequency diversity

Previous works:



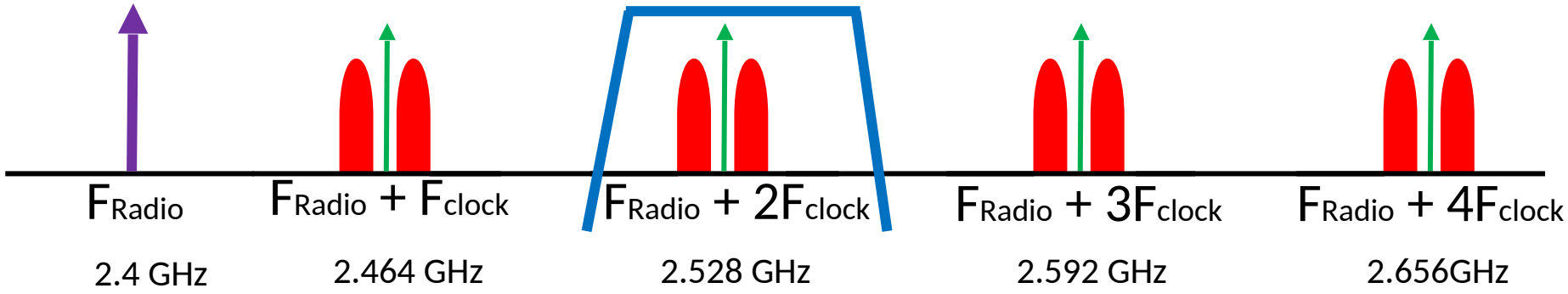
- The leakage is present at each harmonic of the digital clock frequency

[2] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," ACM SIGSAC, 2018

[3] R.Wang, H.Wang, E.Dubrova, "Far field em side-channel attack on aes using deep learning," ACM, 2020

Frequency diversity

Previous works:



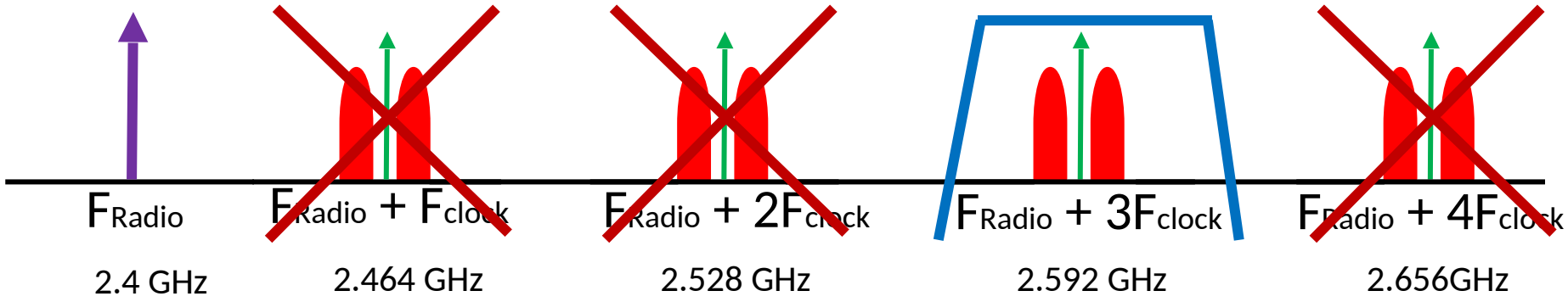
- The leakage is present at each harmonic of the digital clock frequency
- Previous works on screaming channel used only the second at 2,528 GHz

[2] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, "Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers," ACM SIGSAC, 2018

[3] R.Wang, H.Wang, E.Dubrova, "Far field em side-channel attack on aes using deep learning," ACM, 2020

Frequency diversity

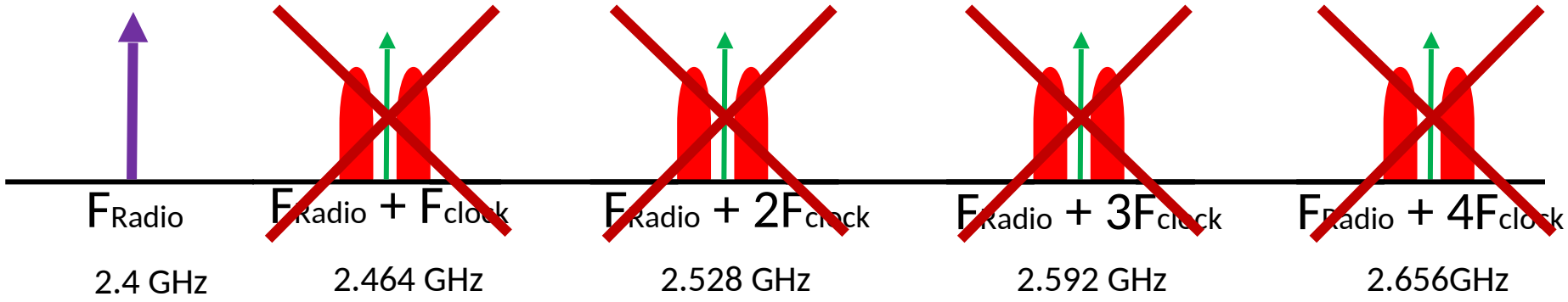
In our environment:



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

Frequency diversity

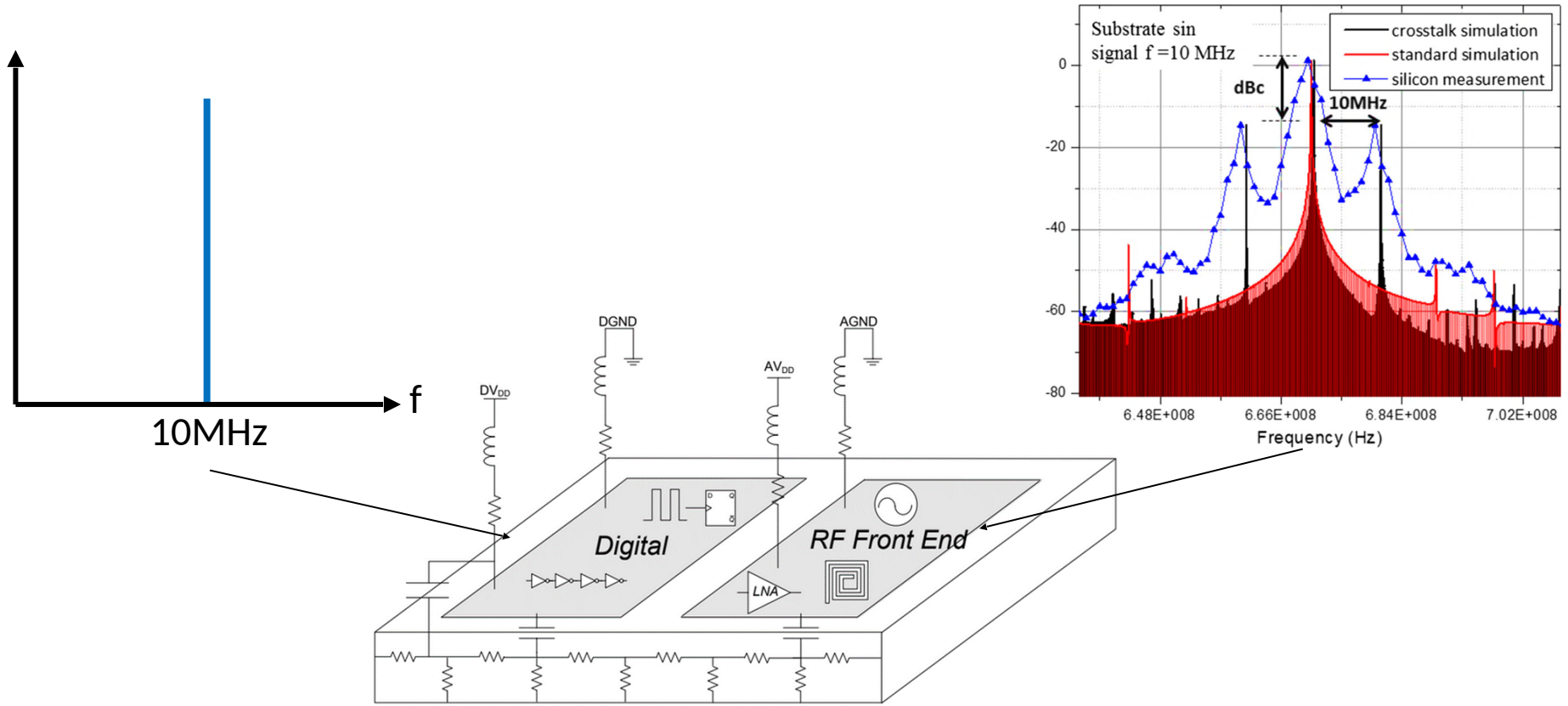
Questions:



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

Leakage at non-harmonics frequencies

Substrate spreading a harmonic over a large band of frequencies:

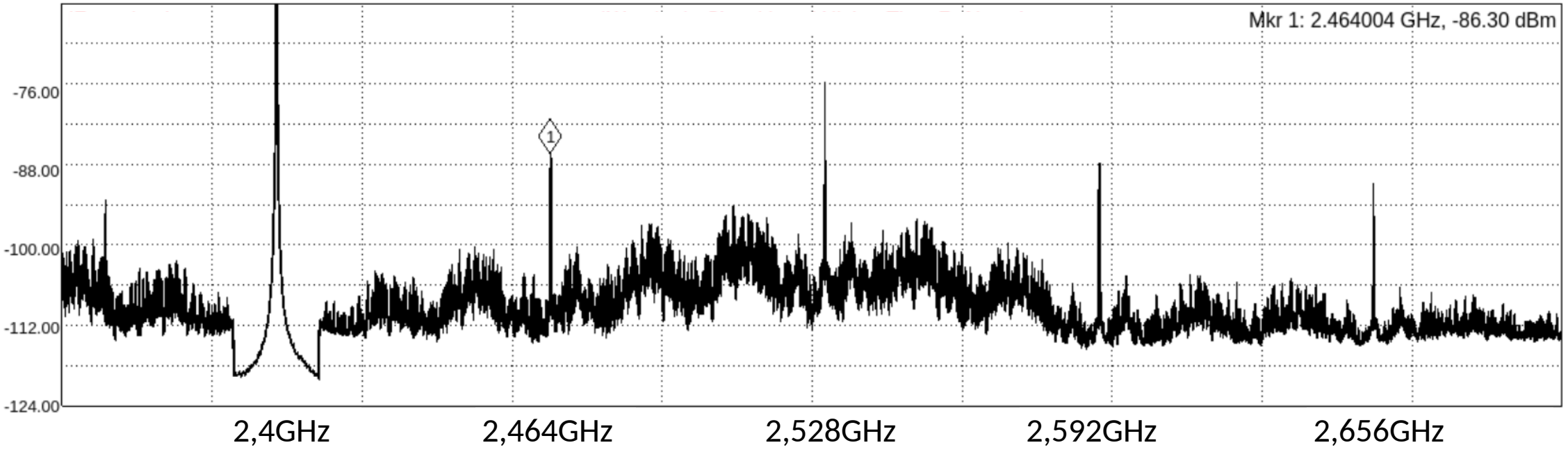


[4] T.Noulis, and P.Baumgartner, "CMOS substrate coupling modeling and analysis flow for submicron SoC design". Analog Integrated Circuits and Signal Processing, 2017

Leakage at non-harmonics frequencies

Radio spectrum at the output of the victim device

- Energy is also present between the harmonics

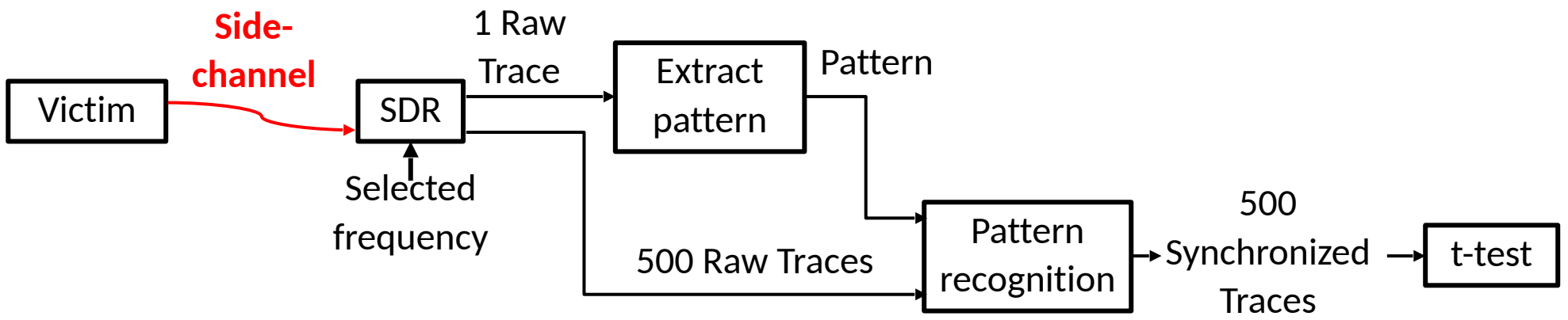


Leakage at non-harmonics frequencies

Questions:

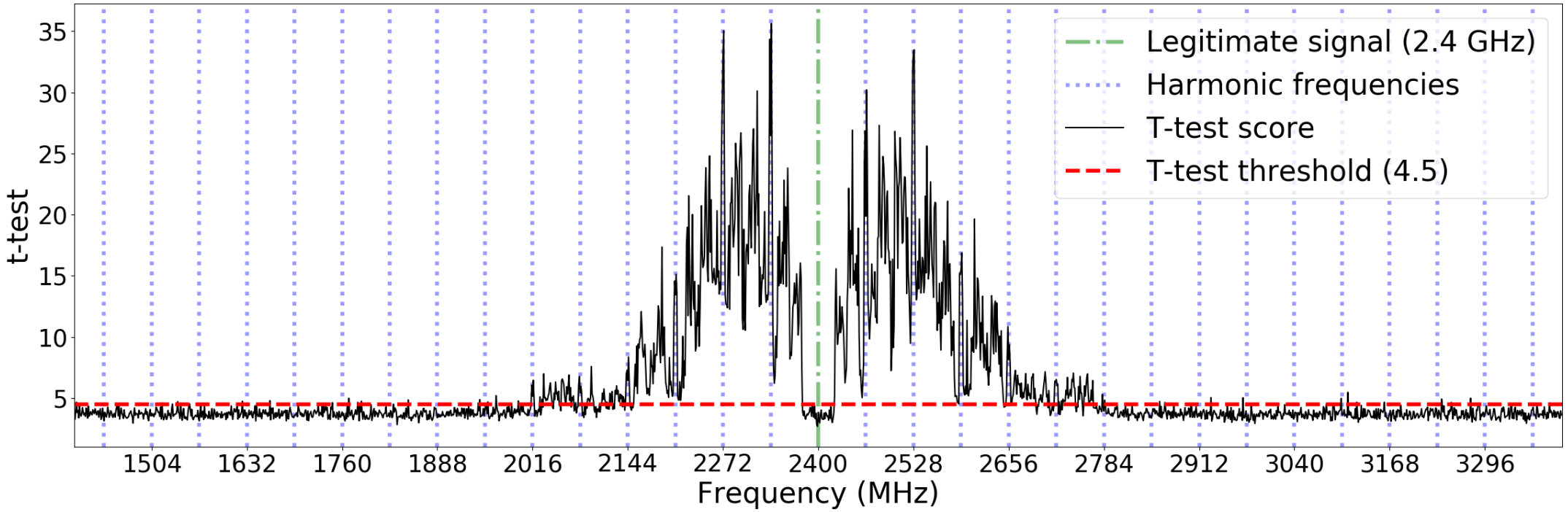
- Is the leakage also present at non-harmonic frequencies?
  - Perform a t-test at multiple frequencies over the spectrum.
- In case it is, is the attack more difficult there than at the harmonics?
  - Perform a template attack at frequencies where leakage is detected.

T-test



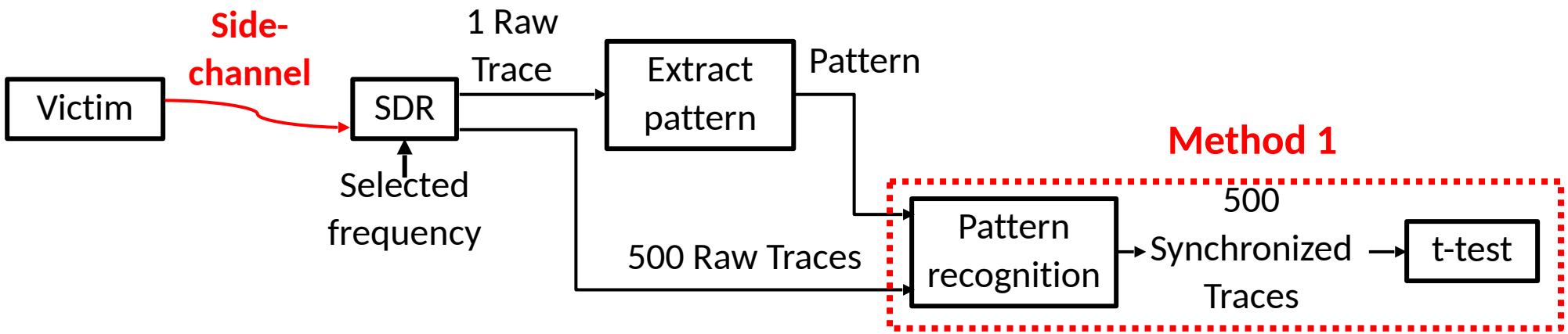
- Range of frequency: from 1,4GHz – 3,4GHz (1MHz resolution)
- Fixed vs fixed t-test, 500 traces per frequency:
  - 250 Plaintexts full of 0s, 250 Plaintexts full of 1s.
- The key is full of 0s

T-test

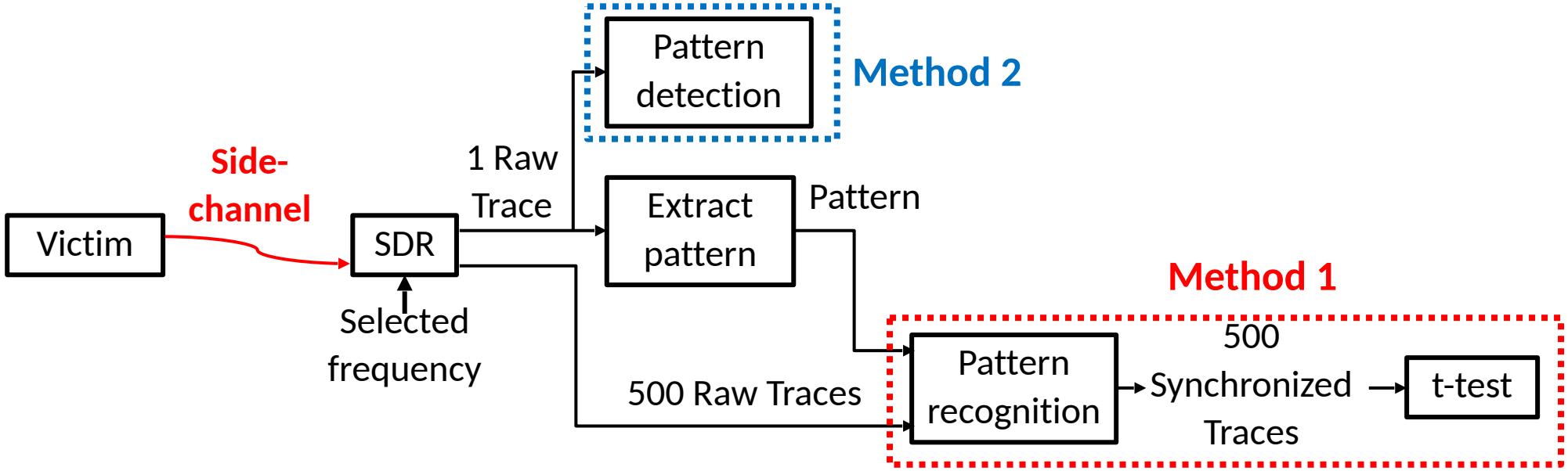


- Fixed vs fixed t-test
- 500 traces per frequency
- 27 hours of computation

Pattern detection



Pattern detection



Pattern detection

Based on the concept of Virtual Trigger[3]:

- A series of Cryptographic Process (CP) is executed recursively without interruptions

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

Pattern detection

Based on the concept of Virtual Trigger[3]:

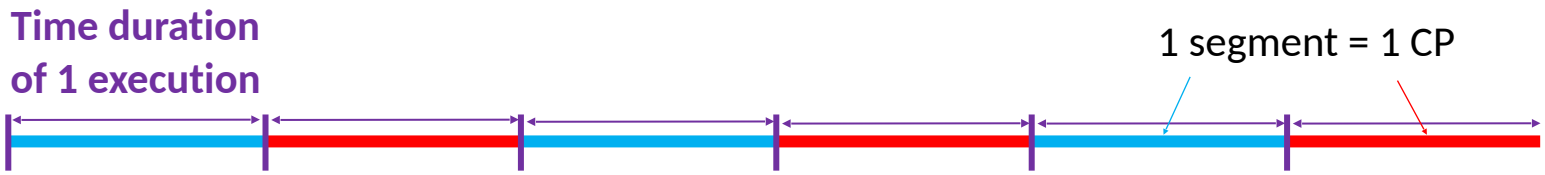
- A series of Cryptographic Process (CP) is executed recursively without interruptions

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

Pattern detection

Based on the concept of Virtual Trigger[3]:

- A series of Cryptographic Process (CP) is executed recursively without interruptions
- By knowing precisely enough the CP execution time: possibility to create a Virtual Trigger (VT) that points to a common instant in each CP

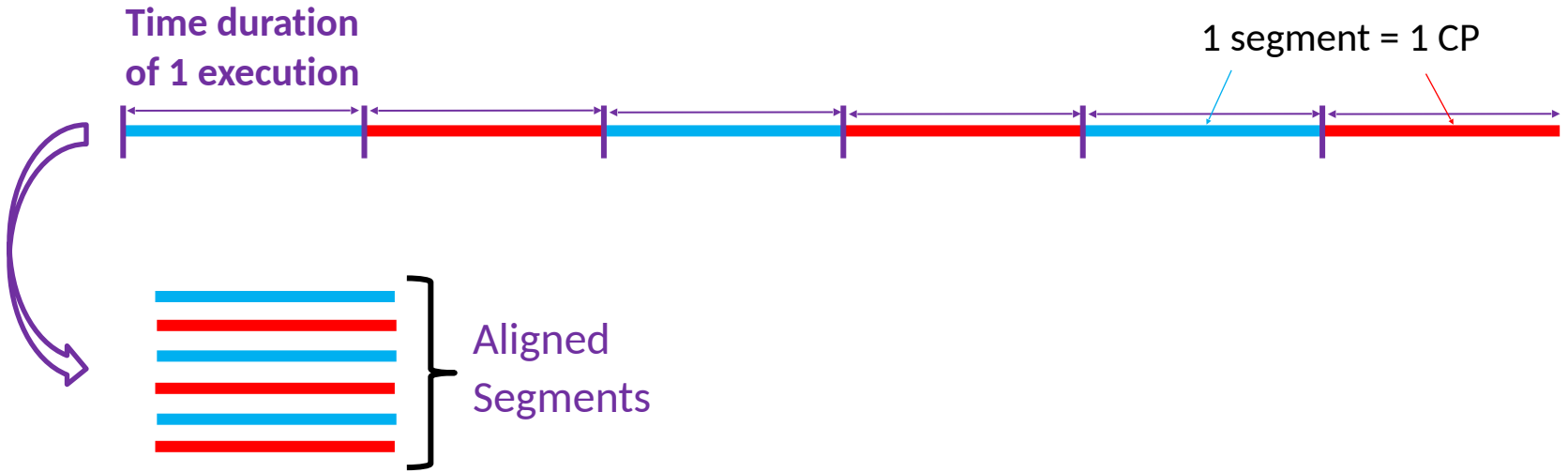


[5] J.Guillaume, M.Pelcat, A.Nafkha, R.Salvador, "Virtual Triggering: a Technique to Segment Cryptographic Processes in Side-Channel Traces," SIPS, 2022.

Pattern detection

Based on the concept of Virtual Trigger[3]:

- A series of Cryptographic Process (CP) is executed recursively without interruptions
- By knowing precisely enough the CP execution time: possibility to create a Virtual Trigger (VT) that points to a common instant in each CP
- Trace segmentation: separate the CP segments using VT

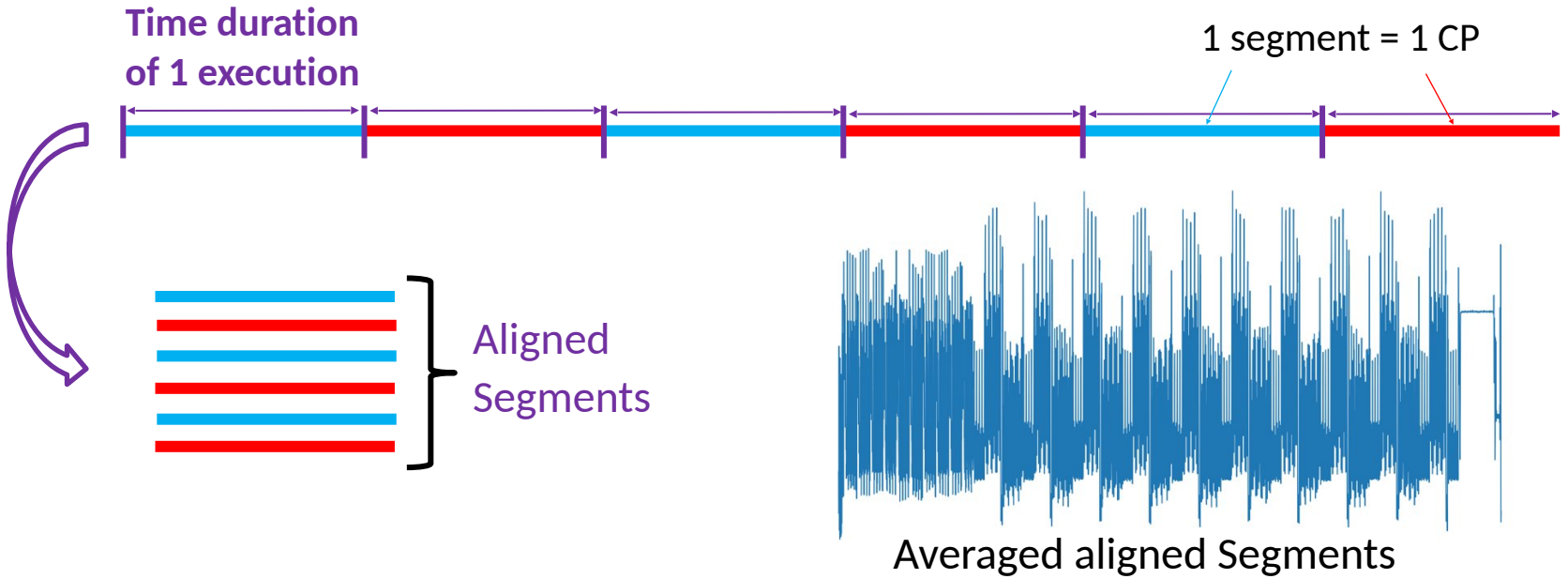


[5] J.Guillaume, M.Pelcat, A.Nafkha, R.Salvador, "Virtual Triggering: a Technique to Segment Cryptographic Processes in Side-Channel Traces," SIPS, 2022.

Pattern detection

Based on the concept of Virtual Trigger[3]:

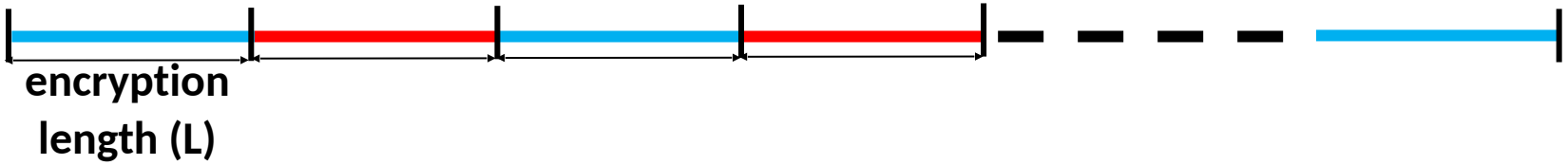
- A series of Cryptographic Process (CP) is executed recursively without interruptions
- By knowing precisely enough the CP execution time: possibility to create a Virtual Trigger (VT) that points to a common instant in each CP
- Trace segmentation: separate the CP segments using VT



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

Pattern detection

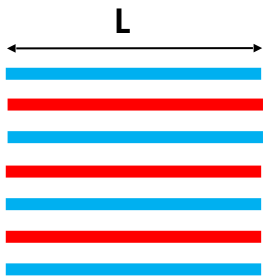
Initial trace



Pattern detection

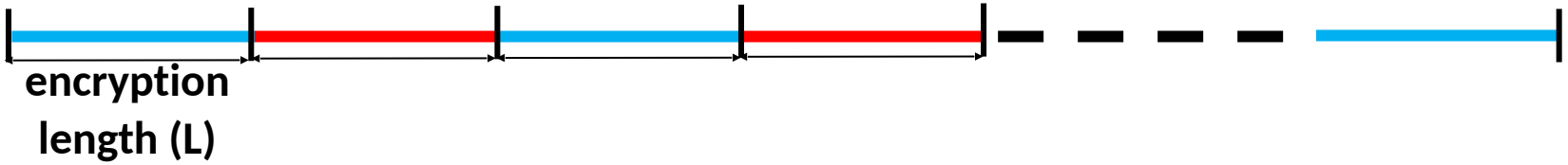
Initial trace

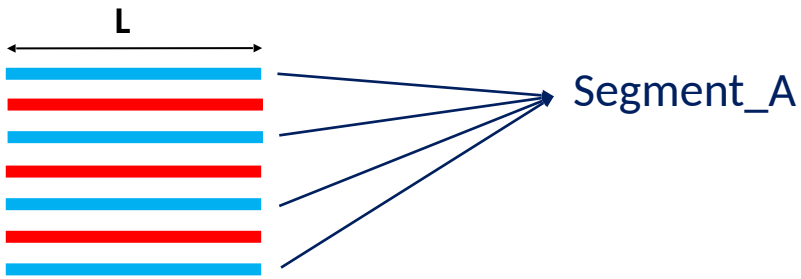
encryption length (L)



Pattern detection

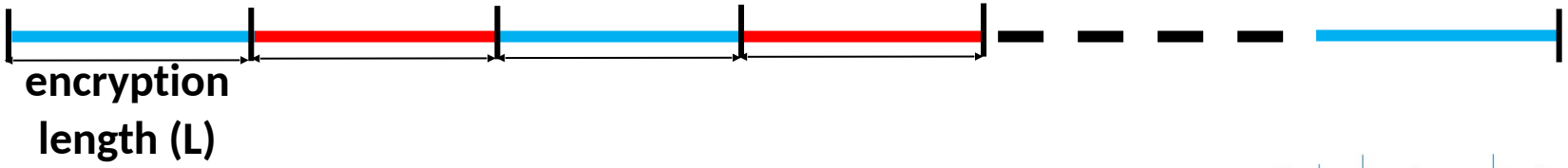
Initial trace

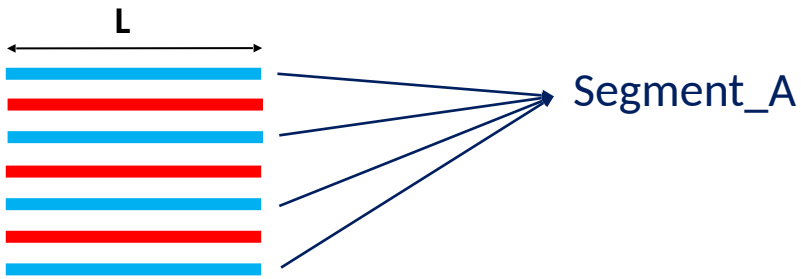


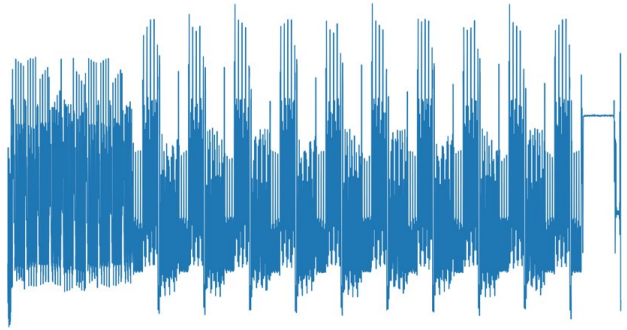


Pattern detection

Initial trace

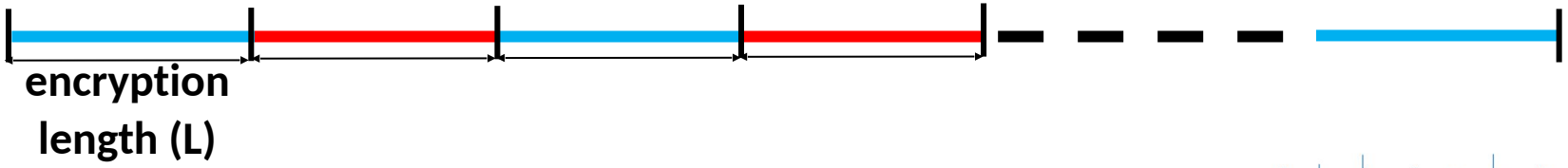


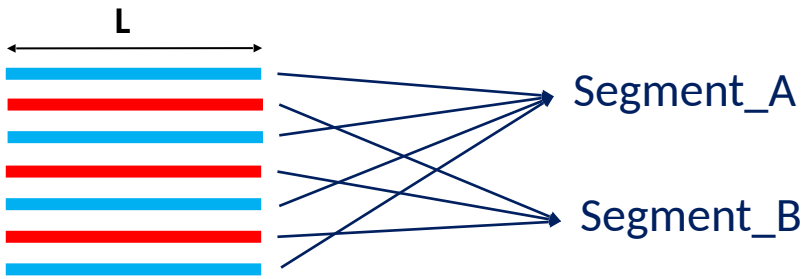


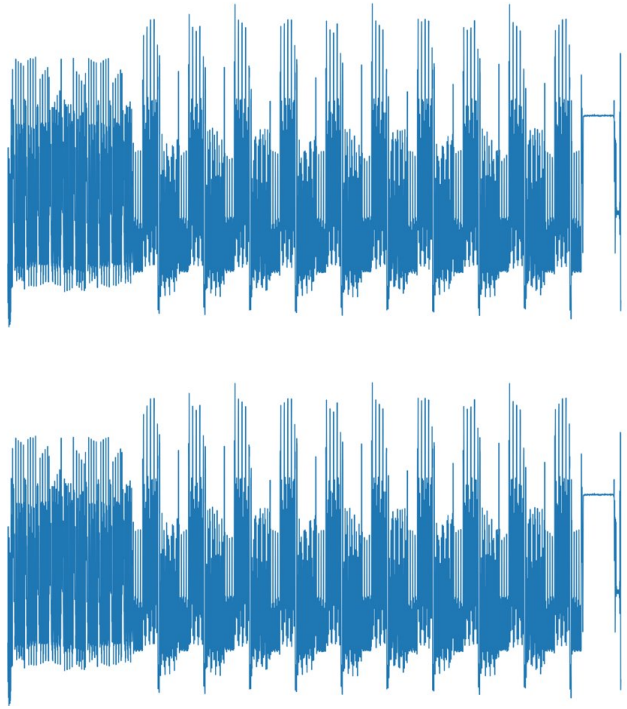


Pattern detection

Initial trace

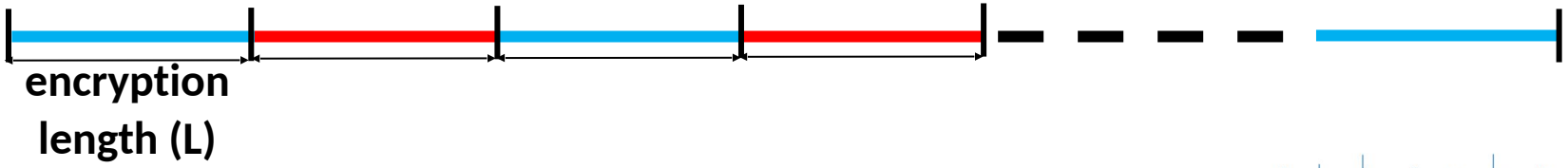


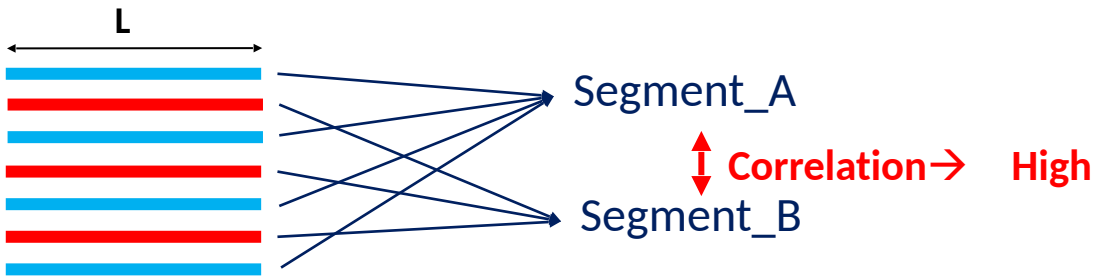


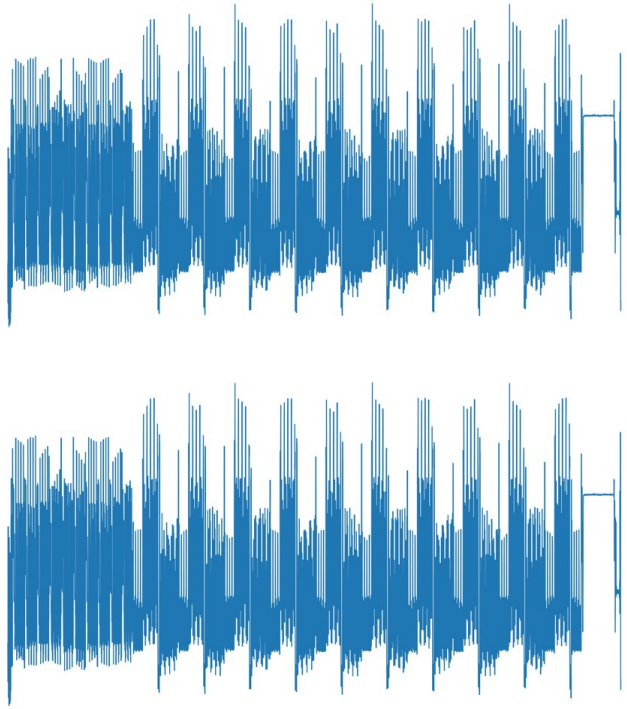


Pattern detection

Initial trace

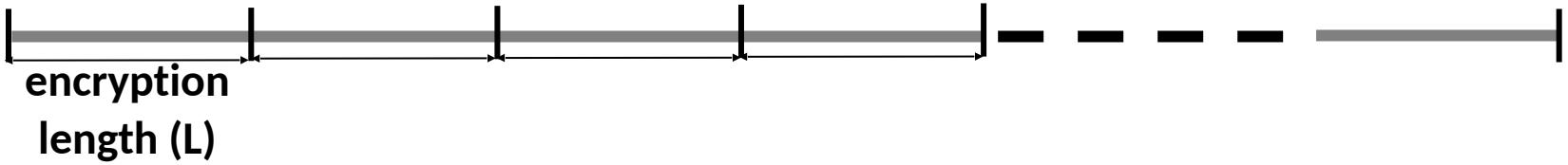


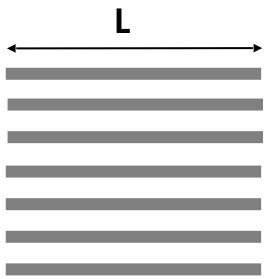




Pattern detection

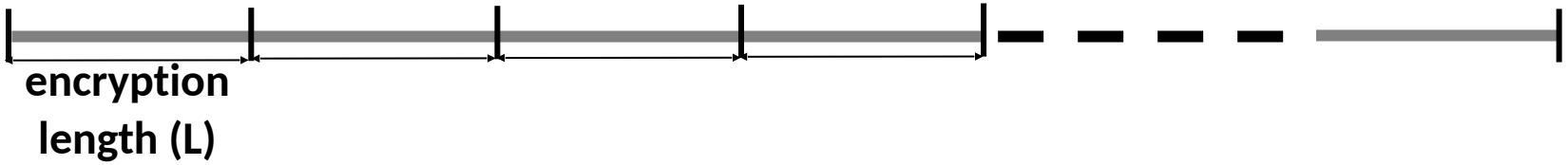
Initial trace

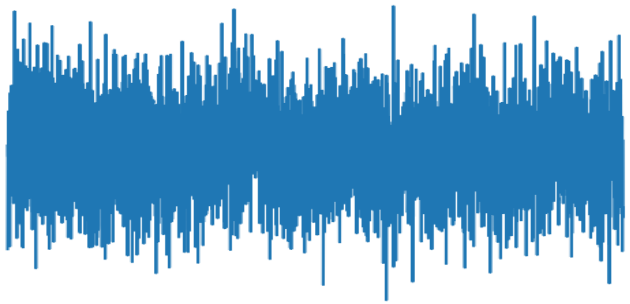


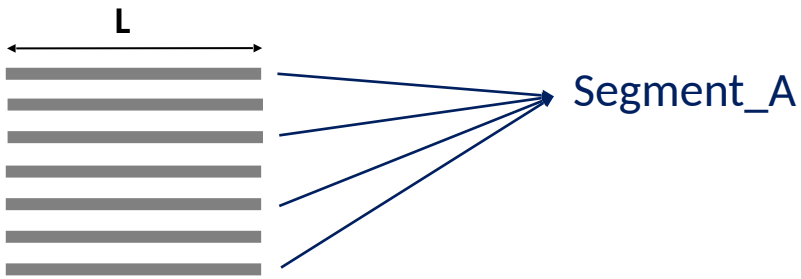


Pattern detection

Initial trace

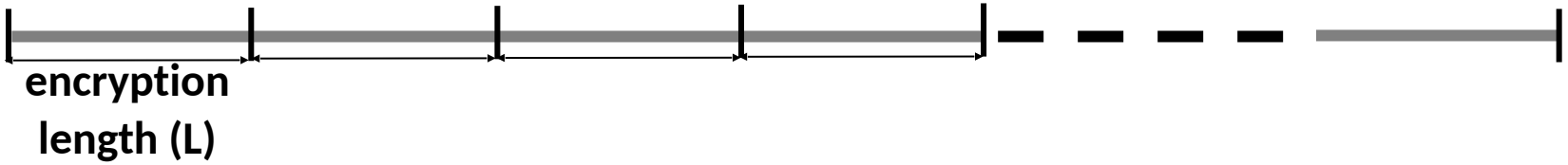


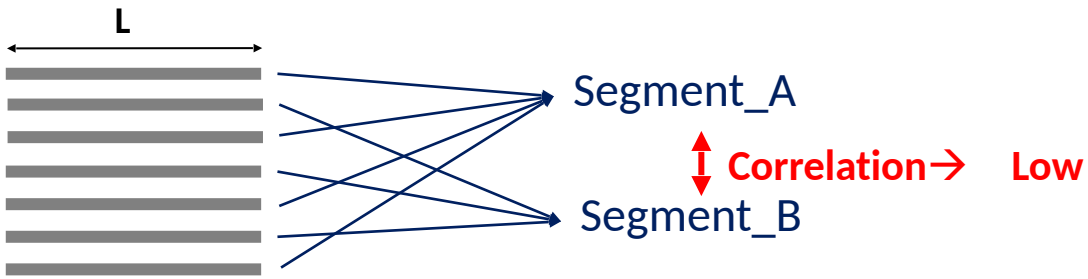


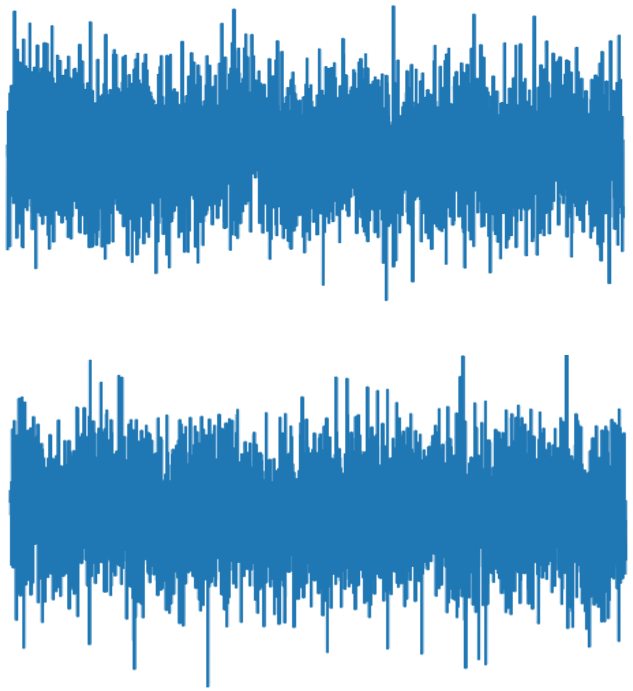


Pattern detection

Initial trace

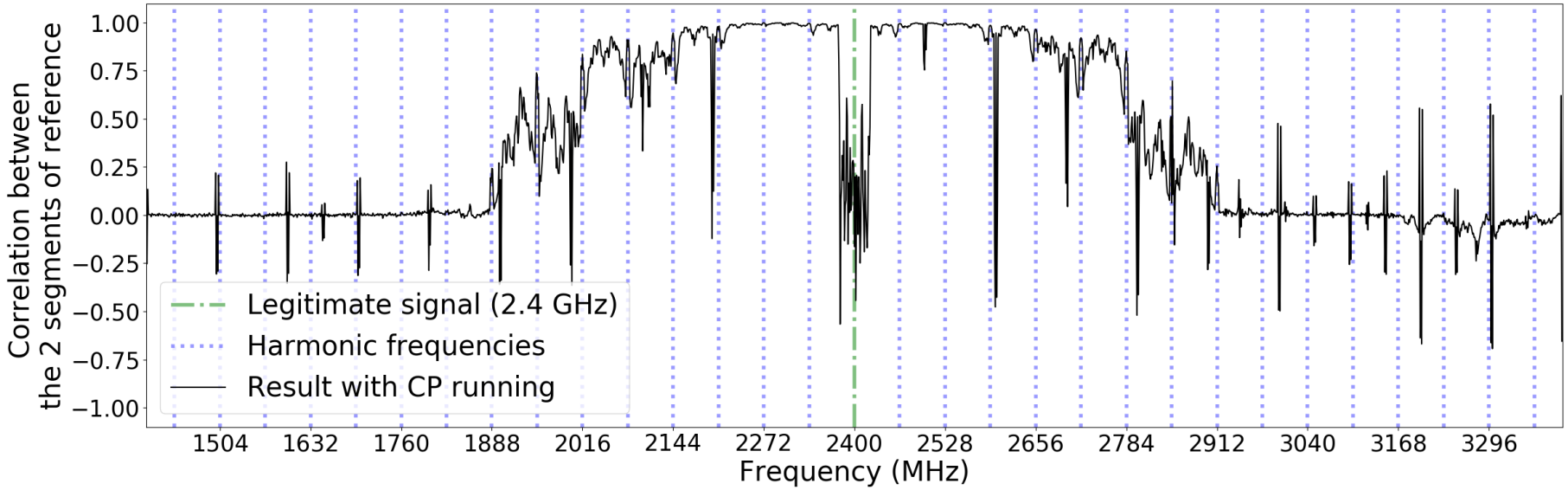






Pattern detection

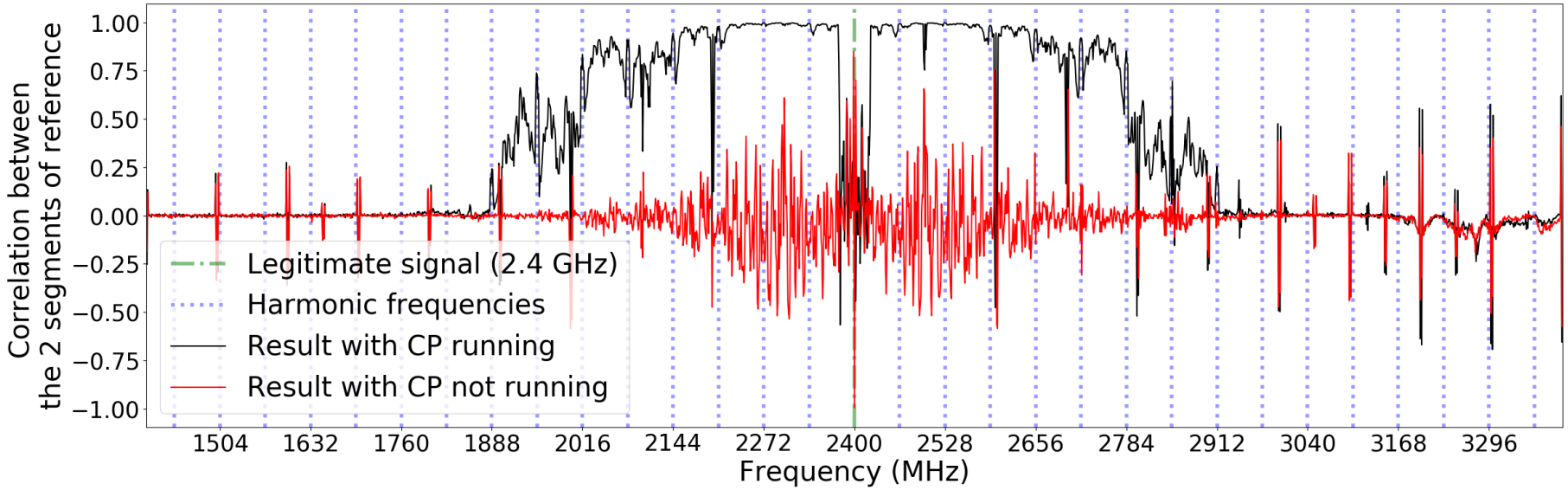
With running encryptions:



- 52 minutes of computation

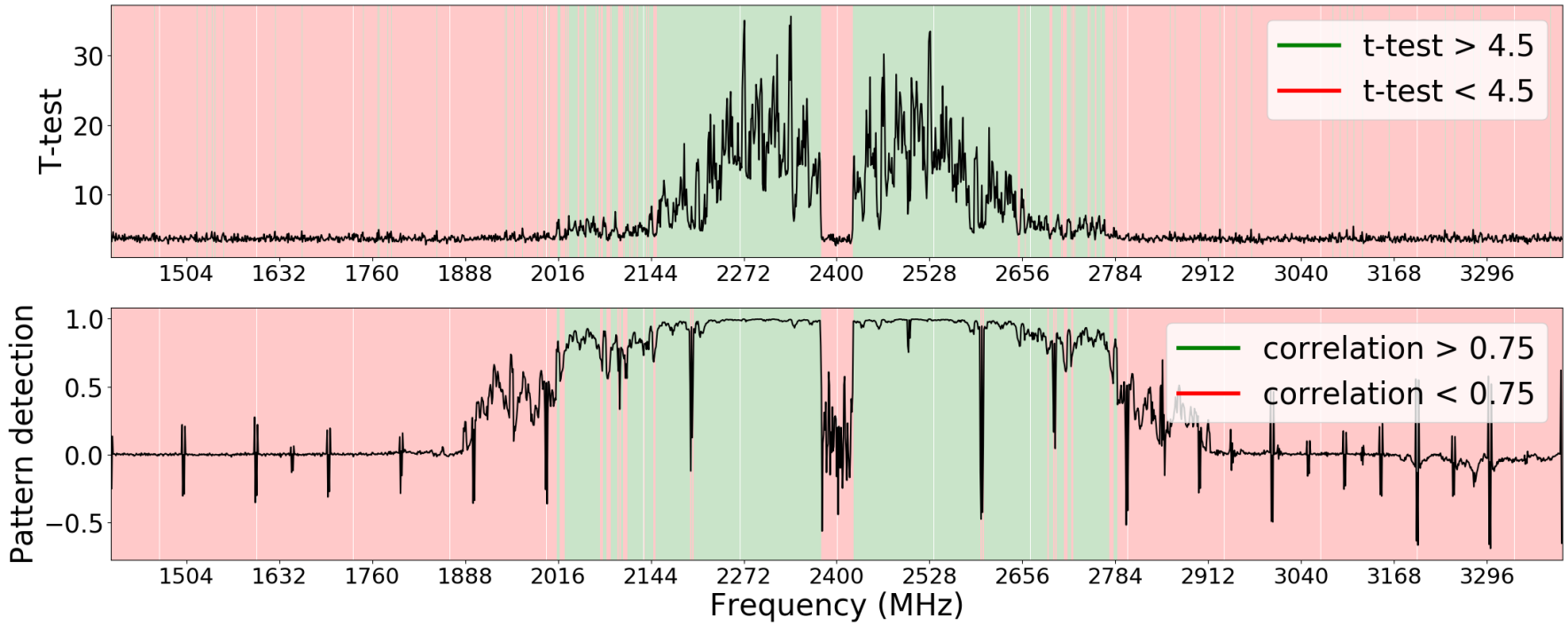
Pattern detection

Without running encryptions:



- 52 minutes of computation

Comparison of the 2 methods



- T-test: 27 hours of computation
- Pattern detection: 52 minutes

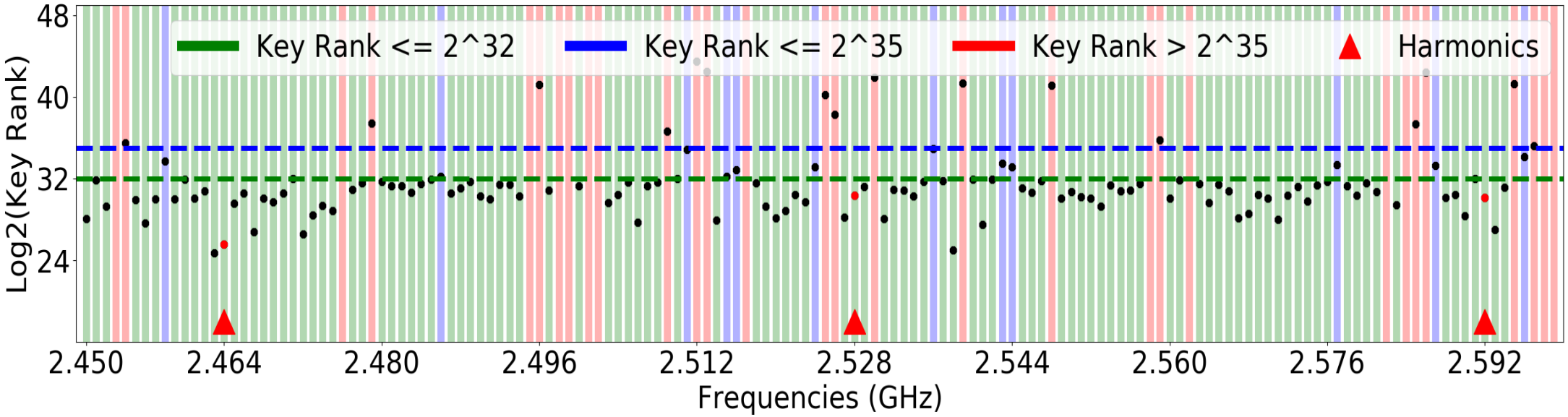
Attack at non-harmonic frequencies

- Evaluate attack potential: Attack in idealistic conditions
  - Attack by cable
  - Template attack with a big number of traces

- Increase the difficulty to get the attack more realistic
  - Add distance
  - Reduce the number of traces

Attack at non-harmonic frequencies

By cable:

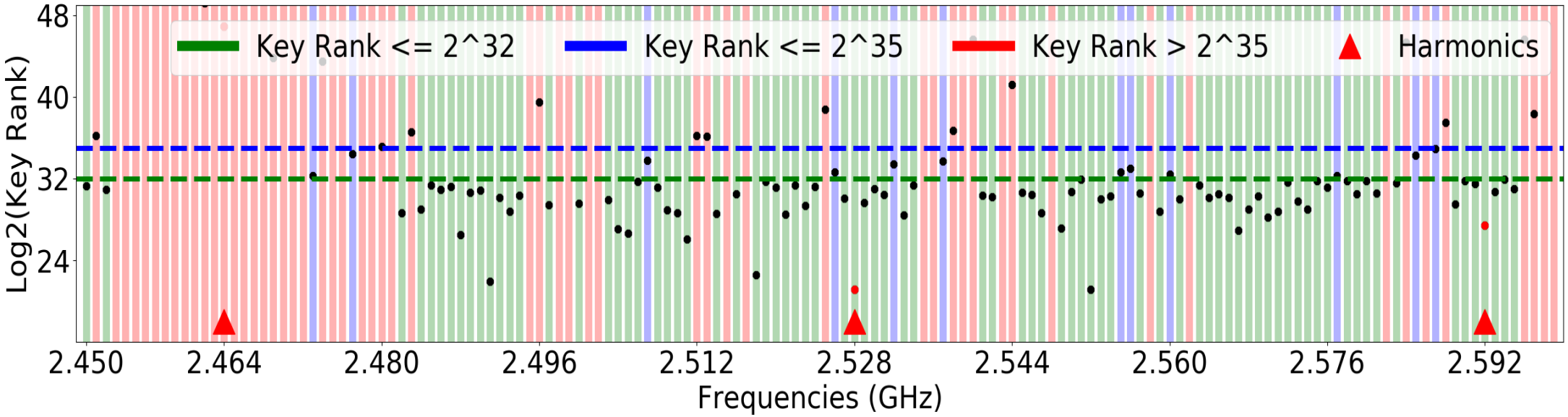


- Profiling phase: 15k Traces
- Attacking phase: 15k Traces

Key Rank	Time order
2^32	5min
2^35	1hour
2^39	1day
2^41	1week

Attack at non-harmonic frequencies

At 2 meters:



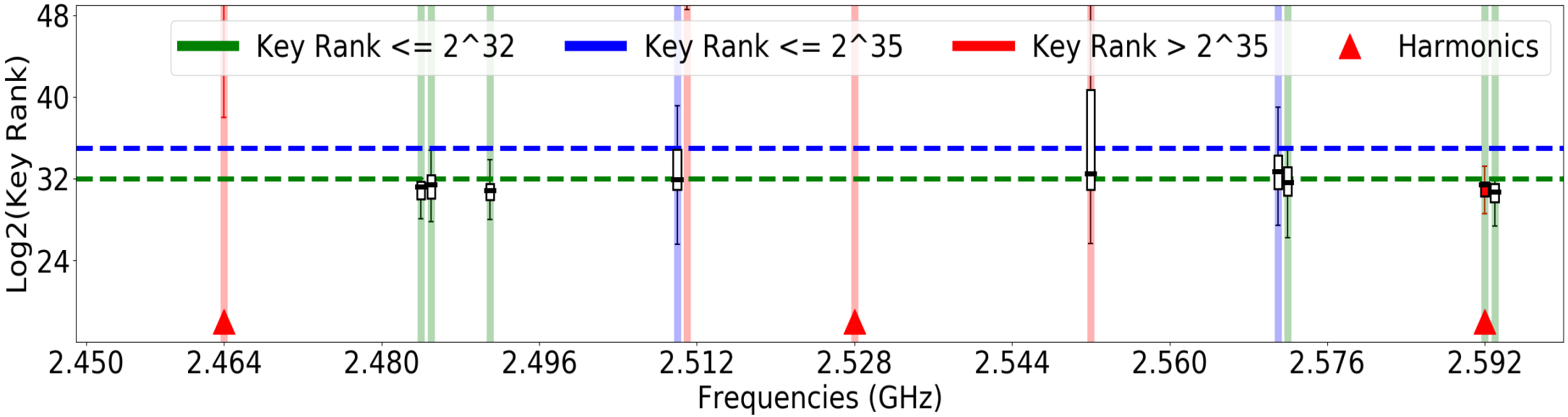
- Profiling phase: 15k Traces
- Attacking phase: 15k Traces

→ Loss of the first harmonic

Key Rank	Time order
2^32	5min
2^35	1hour
2^39	1day
2^41	1week

Attack at non-harmonic frequencies

At 7 meters, 50 attacks per frequency:



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

→ Loss of the 2 first harmonics

Key Rank	Time order
2^32	5min
2^35	1hour
2^39	1day
2^41	1week

Conclusion

- Demonstrated **the presence of leakage over the spectrum**:
  - By using t-test, a method frequently used by the community.
- Proposed **pattern detection, a second method that optimizes the time duration**.
- In the context of this work, the attack can be **as effective at non-harmonics as at harmonics**.
- This work cannot demonstrate that leakage will always be exploitable at non-harmonics on any devices, but **non-harmonics cannot be ignored**.

Future works

Evaluate the impact of frequency diversity:

Evaluate the **Key rank reduction** between the best frequency and the most efficient combination for different configurations:

- Distance: 5 / 10 / 15 meters and maybe further
- Number of traces used
- Environment: noise less / noisy

In which conditions is frequency diversity is interesting to apply?

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

IETR

Thank you !
Do you have any questions ?

E-mail:
Jeremy.guillaume@centralesupelec.fr

cnrs
CentraleSupélec
INSA RENNES
Nantes Université
Université de Rennes

References

[1] J. Choi, H.-Y. Yang, and D.-H. Cho, “TEMPEST Comeback: A Realistic Audio Eavesdropping Threat on Mixed-signal SoCs,”, ACM SIGSAC, 2020.

[2] G. Camurati, S. Poeplau, M. Muench, T. Hayes, and A. Francillon, “Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers,” ACM SIGSAC, 2018

[3] R.Wang, H.Wang, E.Dubrova, “Far field em side-channel attack on aes using deep learning,” ACM, 2020

[4] T.Noulis, and P.Baumgartner, “CMOS substrate coupling modeling and analysis flow for submicron SoC design“. Analog Integrated Circuits and Signal Processing, 2017

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