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

EURECOM
Sophia Antipolis

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

Security threats emerging from the interaction between digital activity and radio transceivers

Menaces de sécurité à la frontière entre le bruit électromagnétique et les émetteurs-récepteurs radio

Giovanni Camurati

December 8th, 2020, Sophia-Antipolis, France

Members of the Jury

Supervisor
Prof. Dr. Aurélien Francillon, EURECOM

Co-supervisor
Prof. Dr. Ludovic Apvrille, Télécom Paris

Reviewers
Prof. Dr. Srđan Čapkun, ETH Zurich
Dr. Markus Kuhn, University of Cambridge

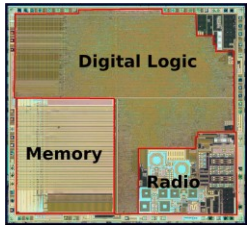
Dr. Rabéa Ameur-Boulifa, Télécom Paris
José Lopes Esteves, Agence nationale de la Sécurité des Systèmes d'Information
Prof. Dr. Raymond Knopp, EURECOM
Prof. Dr. Wenyuan Xu (Guest), Zhejiang University

Thank you for being "here" today!

Something about me

Giovanni Camurati

@GioCamurati
https://giocamurati.github.io



Security

Hardware + Software + Radio

PhD Student

EURECOM
Sophia-Antipolis, France

Context

Challenges & Contributions

Screaming Channels

Noise-SDR

Future Work

Conclusion

How many radios?

Broadcast Radar IoT

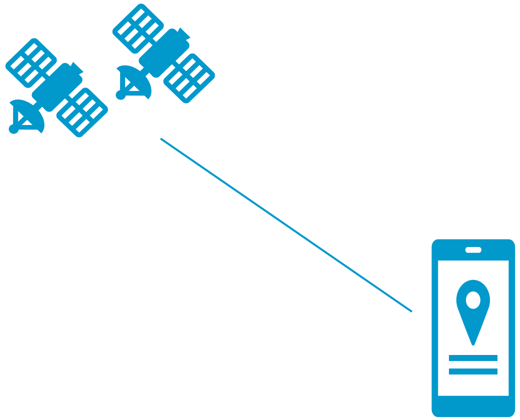
Positioning Mobile

Embedded

How many radios are there on one smartphone?

How many radios are there on one smartphone?

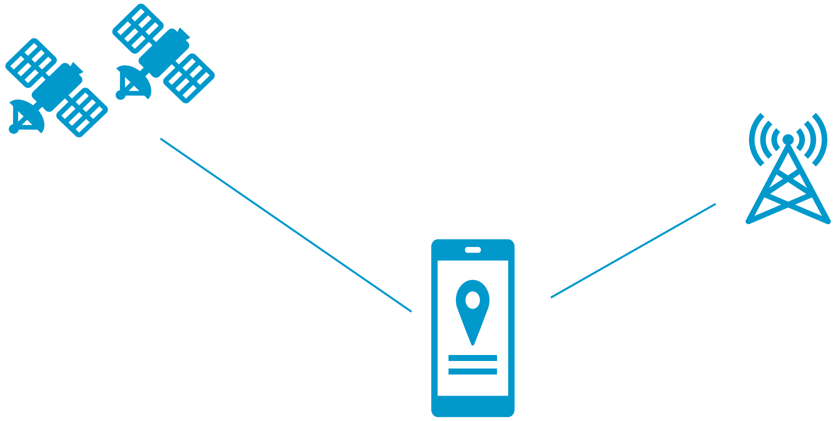
GNSS (km)



How many radios are there on one smartphone?

GNSS (km)

Cellular (km)

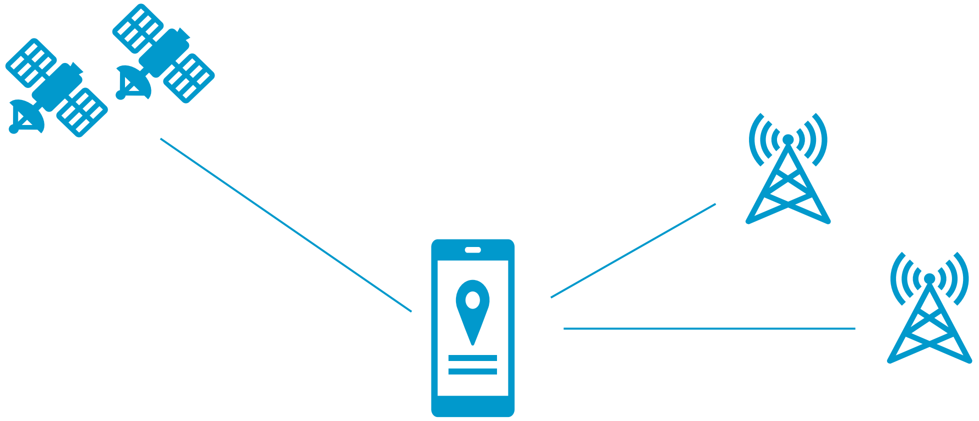


How many radios are there on one smartphone?

GNSS (km)

Cellular (km)

FM (km)



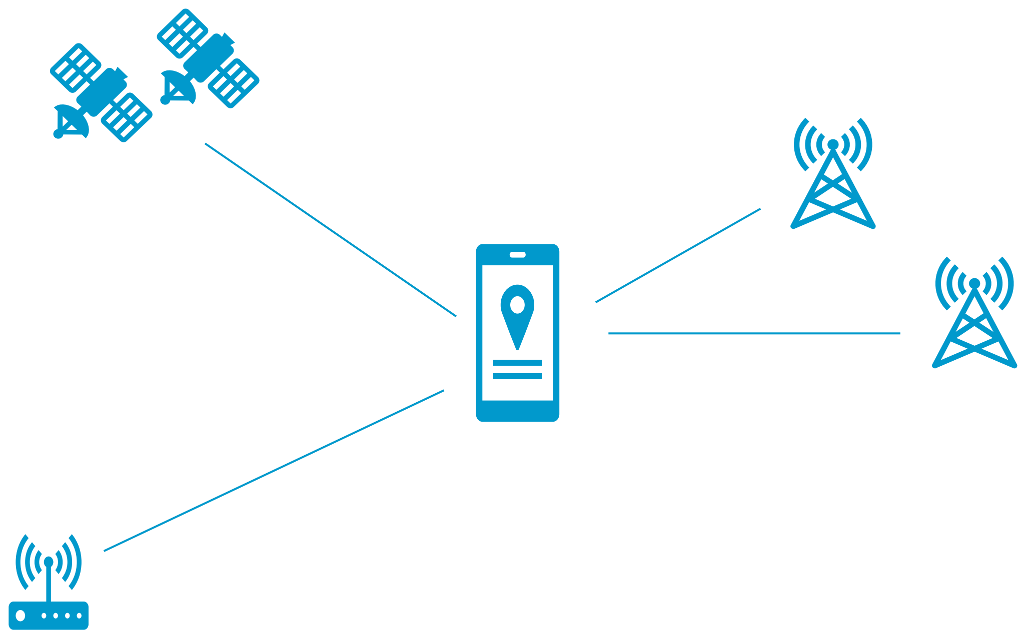
How many radios are there on one smartphone?

GNSS (km)

Cellular (km)

FM (km)

WiFi (m)



How many radios are there on one smartphone?

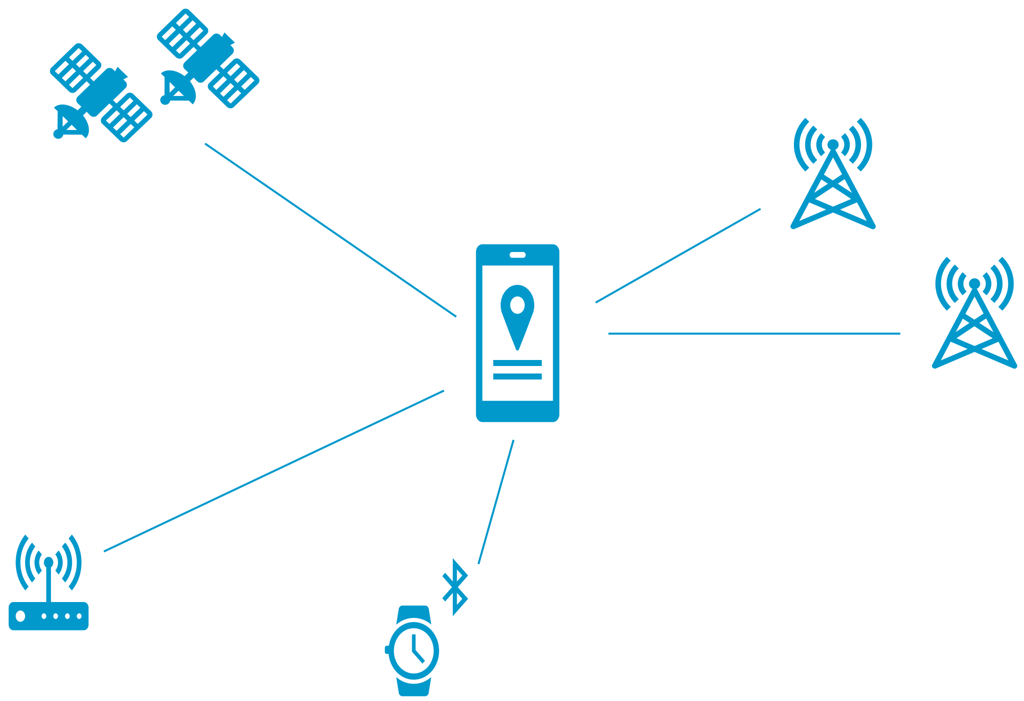
GNSS (km)

Cellular (km)

FM (km)

WiFi (m)

BT/BLE (m)



How many radios are there on one smartphone?

GNSS (km)

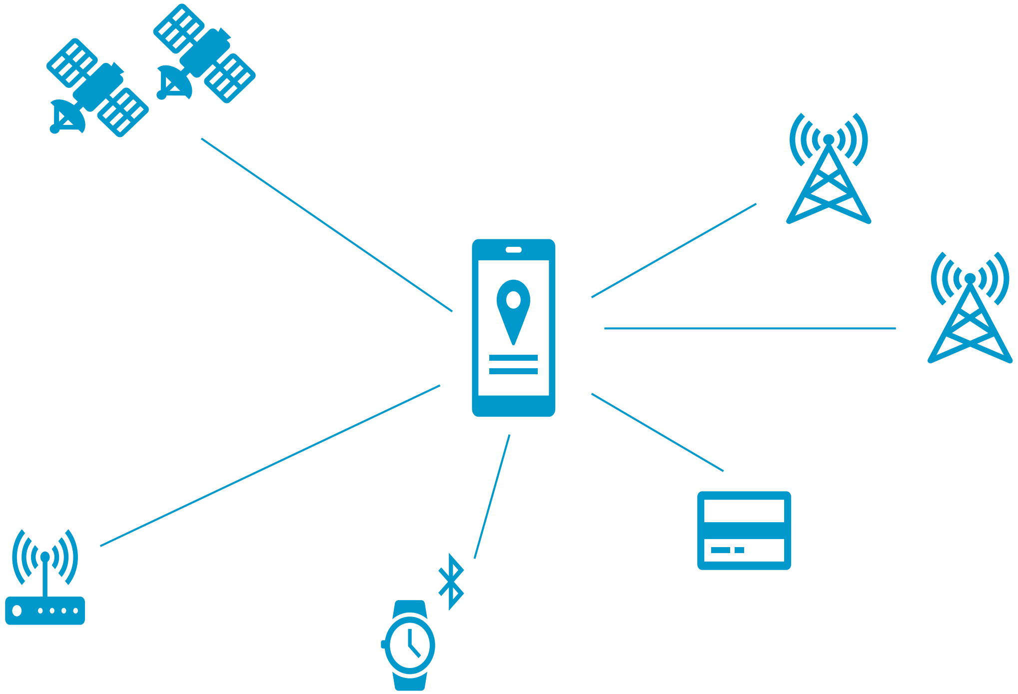
Cellular (km)

FM (km)

WiFi (m)

BT/BLE (m)

NFC (mm)



How many radios are there on one smartphone?

GNSS (km)

Cellular (km)

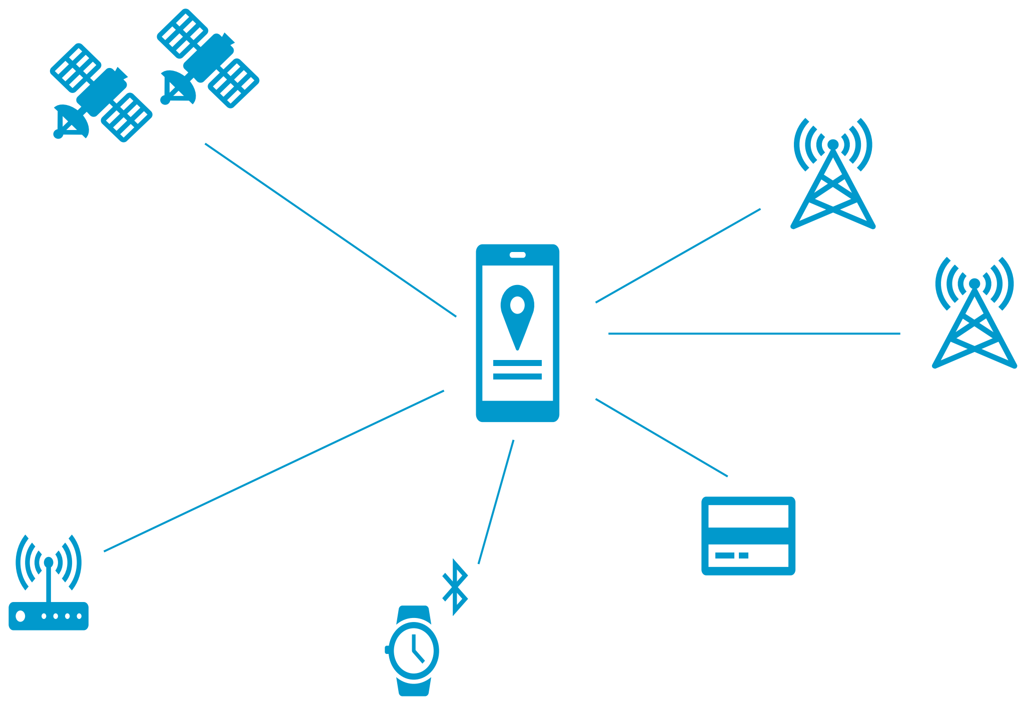
FM (km)

WiFi (m)

BT/BLE (m)

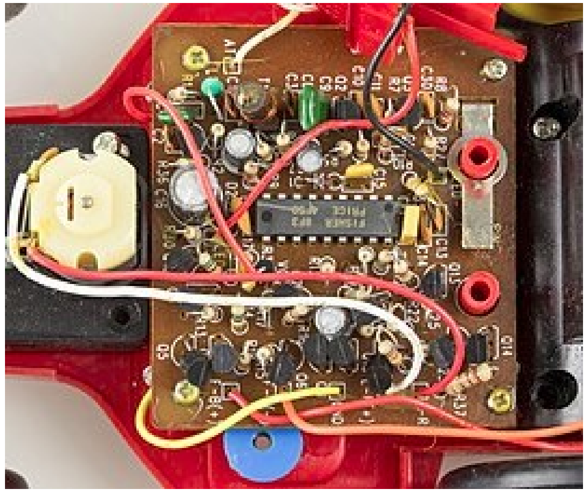
NFC (mm)

UWB, ANT, …



Integration

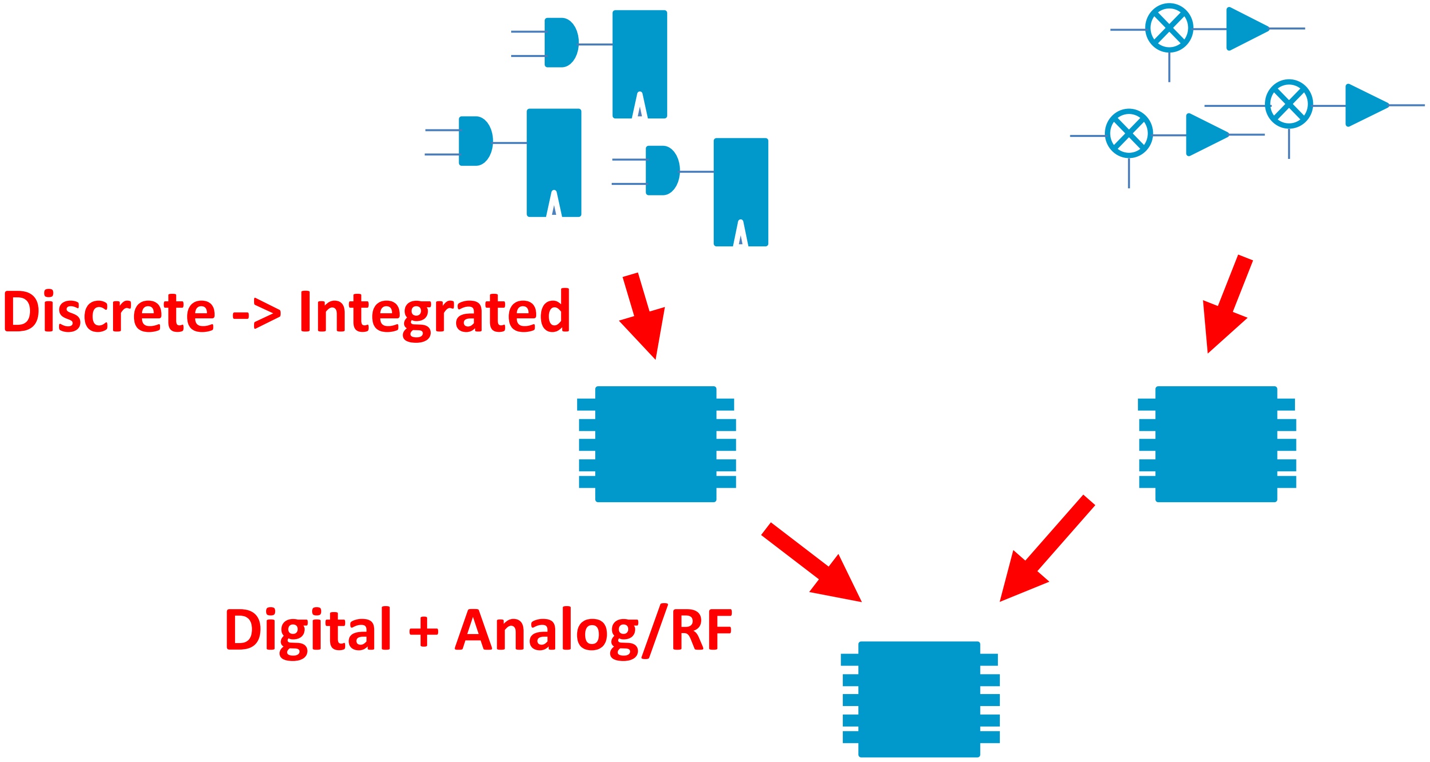
1950



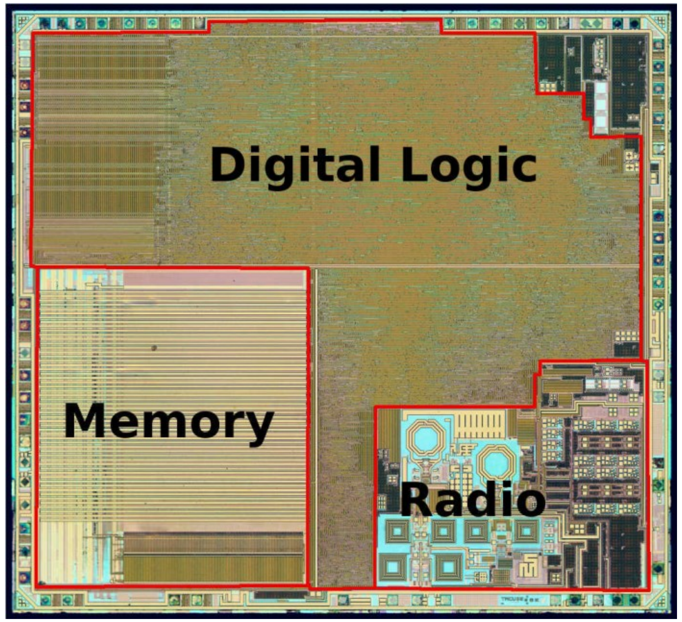
1992

2020

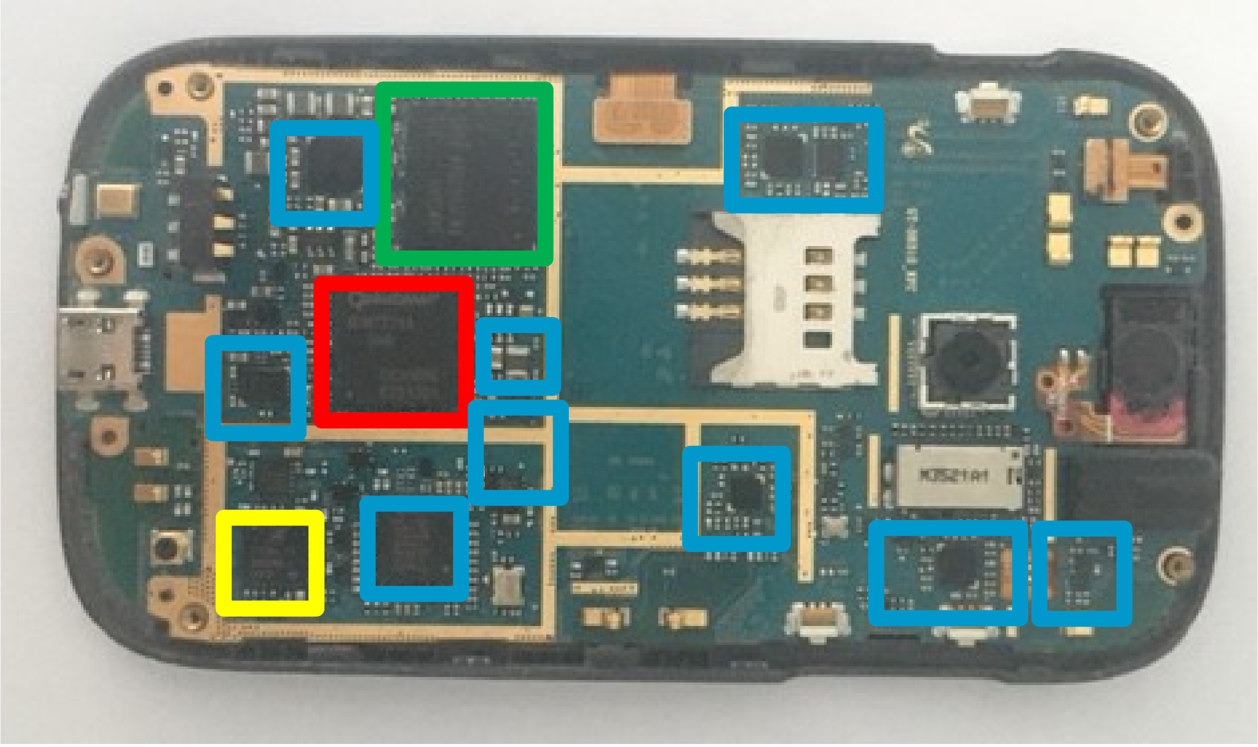
Integration (Chip)



A mixed-signal SoC



Integration (Platform)



A complex platform
(an old one, easy to open …)

- CPU, GPU, GSM, … (red)
- eMCP (eMMC + LPDDR) (green)
- GSM + GPRS (yellow)
- Much more (GPS, FM, WiFi, …) (blue)

Context

Challenges & Contributions

Screaming Channels

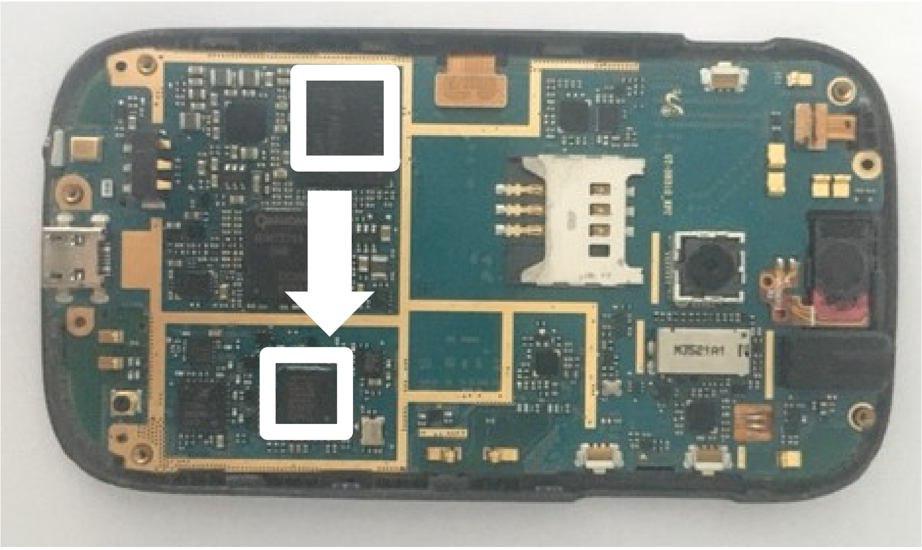
Noise-SDR

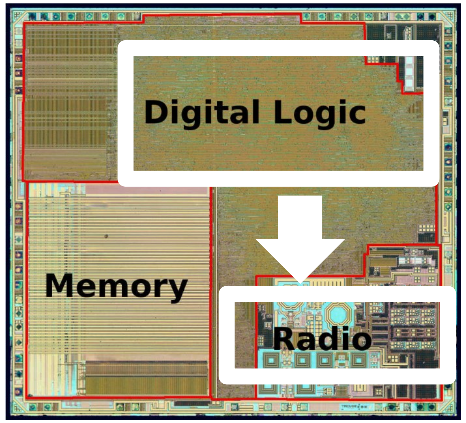
Future Work

Conclusion

Challenge 1:
Integration issues

EM(RF) Interference between electronic components





Emitter “Aggressor”

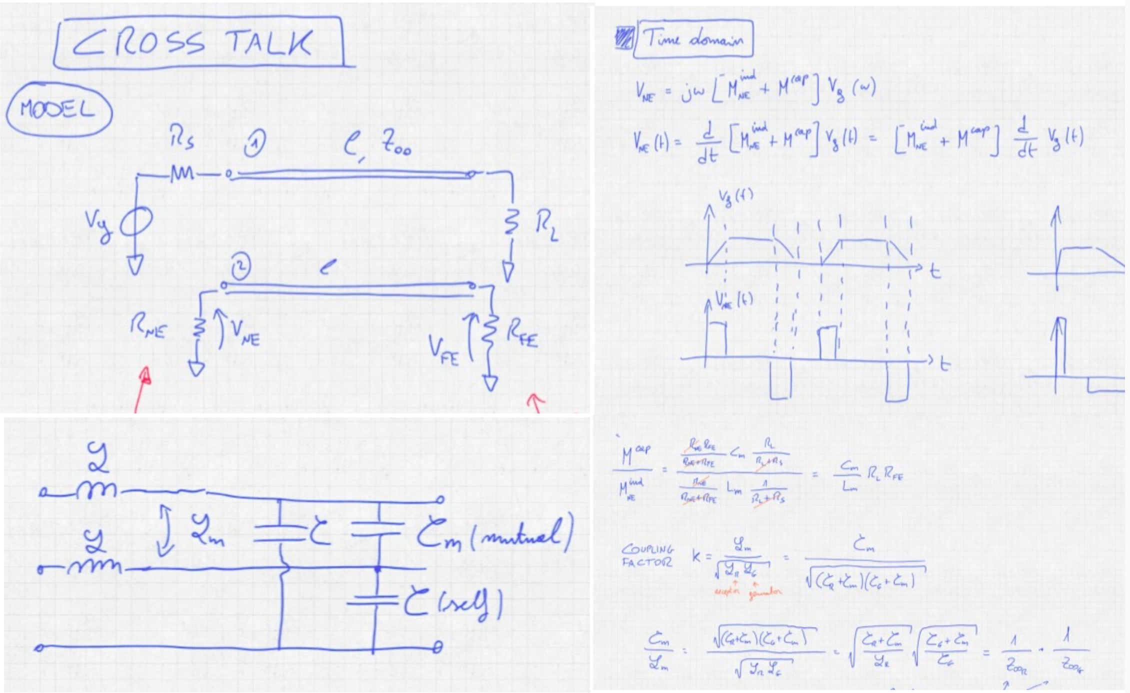
Noise coupling path

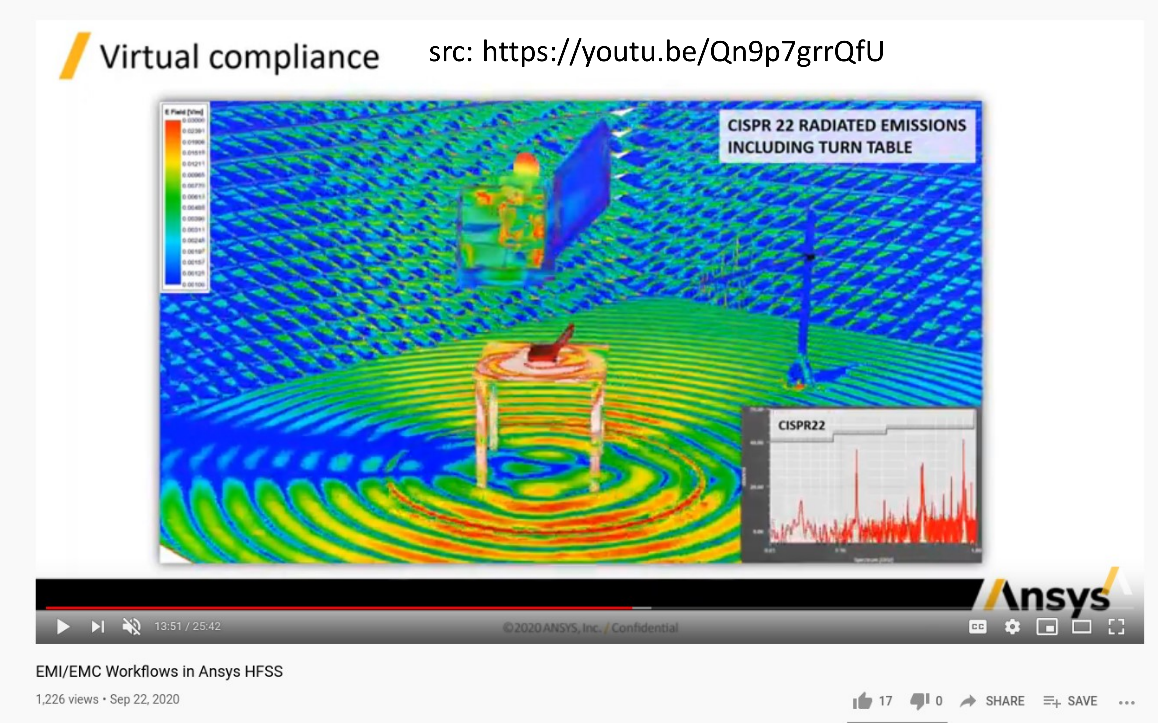
Receptor “Victim”

K. Slattery and H. Skinner, “Platform Interference in Wireless Systems: Models, Measurement, and Mitigation” (Newnes, 2011).

S. Bronckers et al., “Substrate Noise Coupling in Analog/RF Circuits” (Norwood, MA, USA: ARTECH HOUSE, 2009).

Complex modeling/design, expensive simulation/test



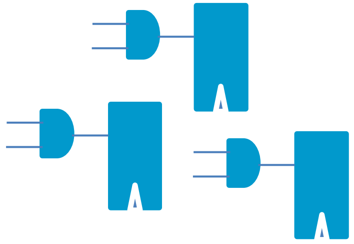


Modeling of cross-talk (personal notes)

Ansys HFSS virtual compliance simulation

C. R. Paul "Introduction to Electromagnetic Compatibility" 2nd Edition (Wiley, 2006)

Additional problem: coexistence of different types

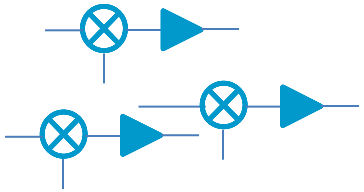


Digital circuits

Noise source

Extrinsic deterministic noise

Distinctive noise properties



Analog/RF circuits

Sensitive to noise

Intrinsic random noise

Thermal noise, flicker noise, …

Coupling

Path for the noise

Overlap in frequency

K. Slattery and H. Skinner, "Platform Interference in Wireless Systems: Models, Measurement, and Mitigation" (Newnes, 2011).

A. Afzali-Kusha et al., "Substrate Noise Coupling in SoC Design: Modeling, Avoidance, and Validation," Proceedings of the IEEE (December 2006).

Challenge 2:
Securing the wireless medium

Security challenge

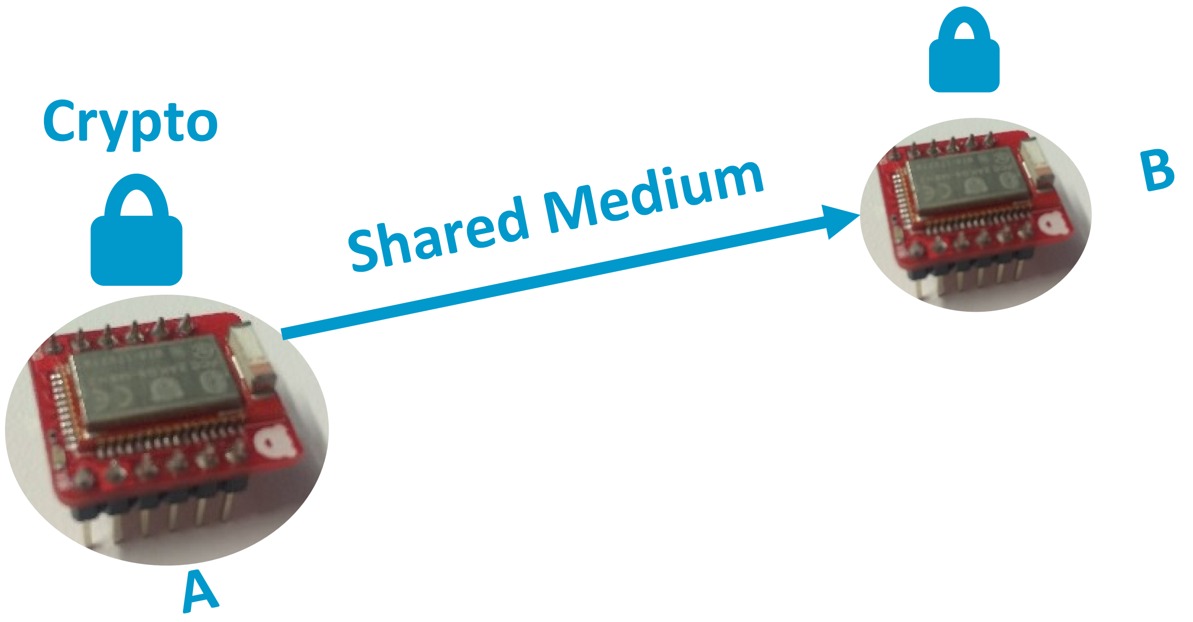
Shared medium

Many attack possibilities

Easy access

Harder in the past

Easier now (e.g., SDRs)



Example: S. Kamkar, “Drive It like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars,” DEFCON 23 (2015).

Security challenge

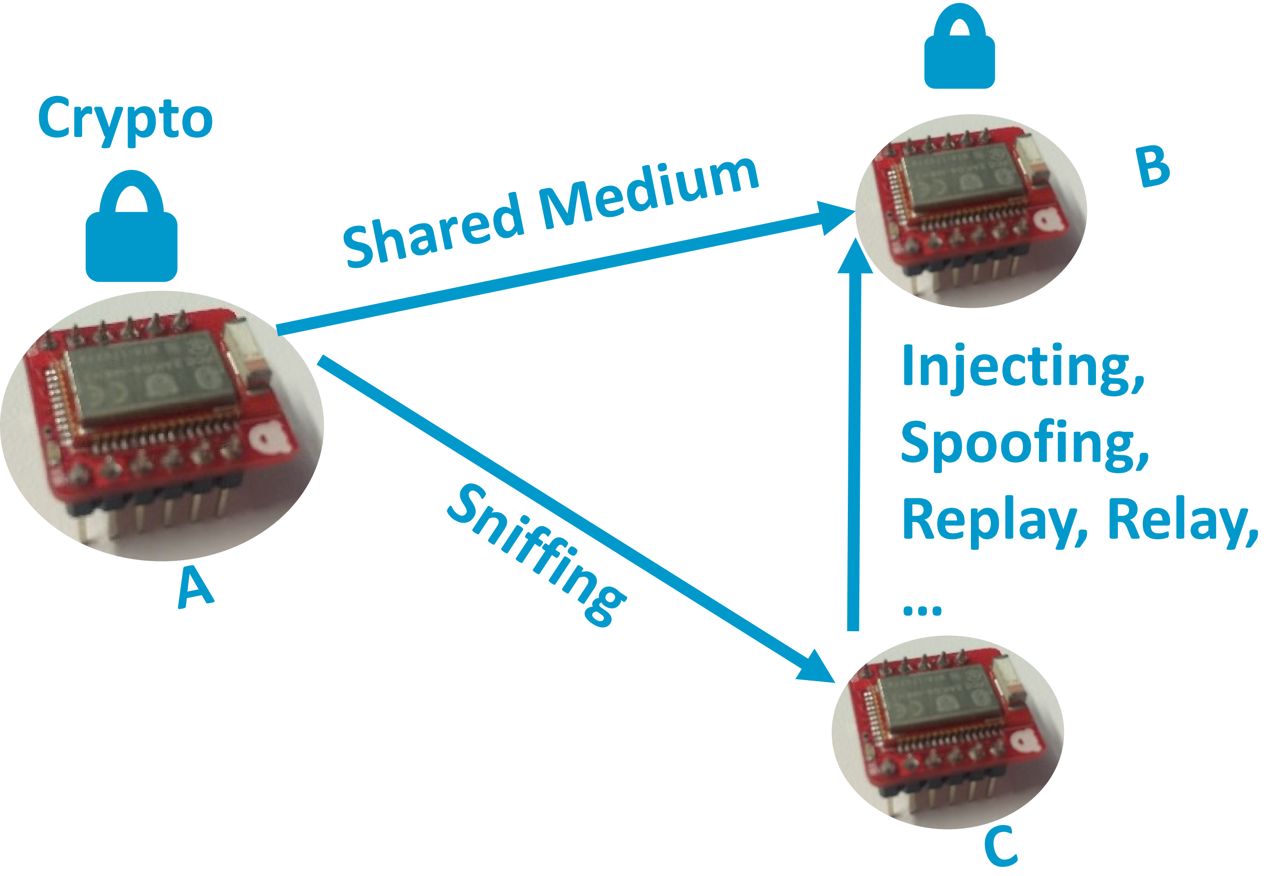
Shared medium

Many attack possibilities

Easy access

Harder in the past

Easier now (e.g., SDRs)



Example: S. Kamkar, "Drive It like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars," DEFCON 23 (2015).

Security challenge

Shared medium

Many attack possibilities

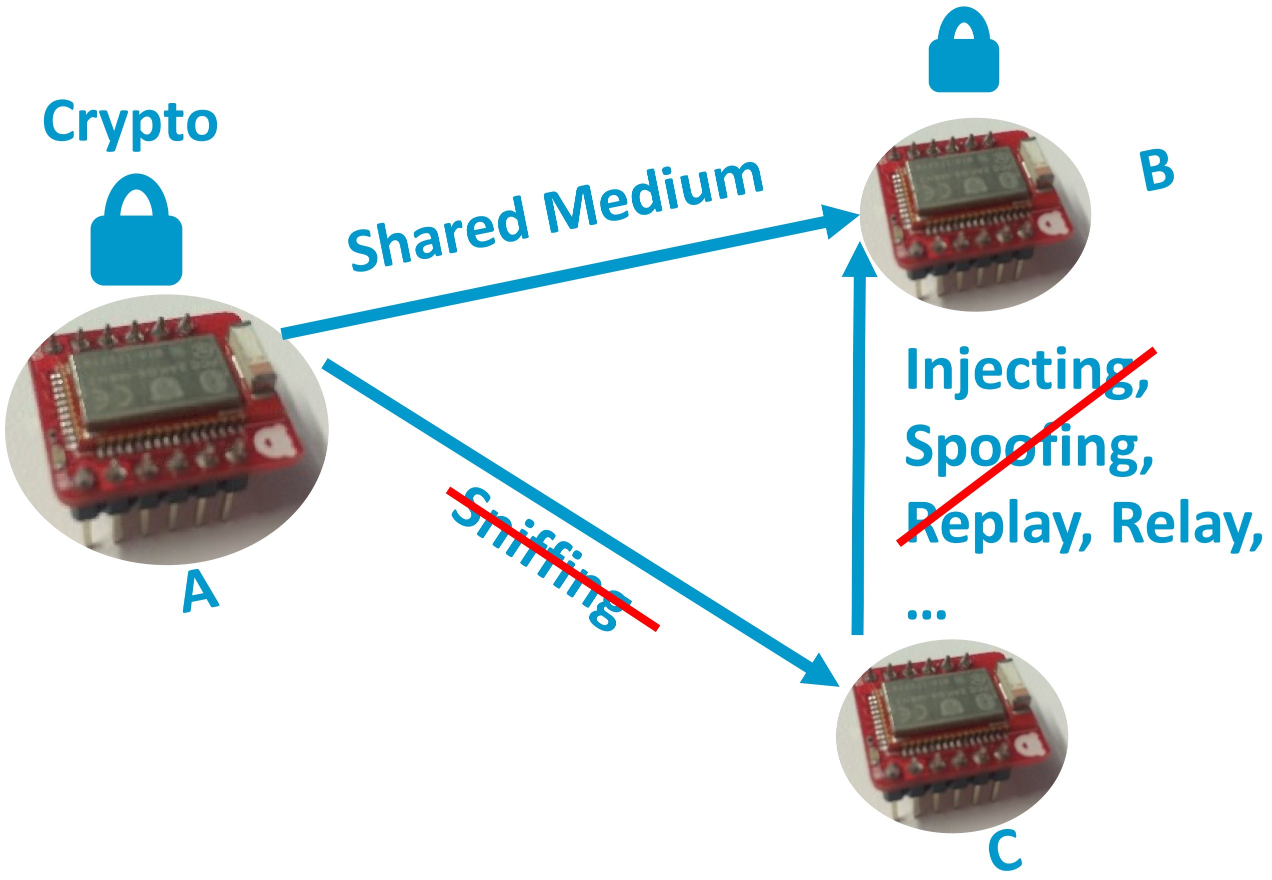
Easy access

Harder in the past

Easier now (e.g., SDRs)

Crypto and Protocols

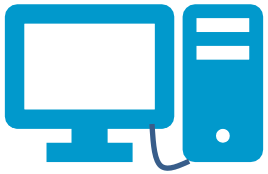
Integrity, Confidentiality, Etc.



Example: S. Kamkar, "Drive It like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars," DEFCON 23 (2015).

Challenge 3:
Unintended emanations

Emission security "EmSec"



R. J. Anderson, "Security Engineering - a Guide to Building Dependable Distributed Systems" (2. Ed.) (Wiley, 2008).

Emission security “EmSec”

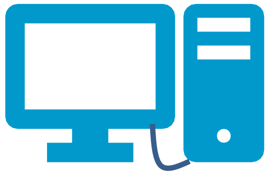
R. J. Anderson, “Security Engineering - a Guide to Building Dependable Distributed Systems” (2. Ed.) (Wiley, 2008).

Emission security “EmSec”

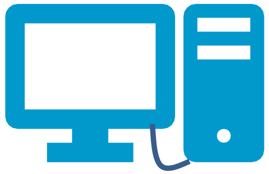
Compromising emanations related to digital activity

R. J. Anderson, “Security Engineering - a Guide to Building Dependable Distributed Systems” (2. Ed.) (Wiley, 2008).

Some categories (informal, non exhaustive)



Some categories (informal, non exhaustive)



P

Some categories (informal, non exhaustive)

“TEMPEST: A Signal Problem” (NSA, 1972).
W. van Eck, “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?,” Comput. Secur. 4, no. 4 (1985).

EURECOM Sophia Antipolis

Some categories (informal, non exhaustive)

“TEMPEST: A Signal Problem” (NSA, 1972).
W. van Eck, “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?,” Comput. Secur. 4, no. 4 (1985).

EURECOM
Sophia Antipolis

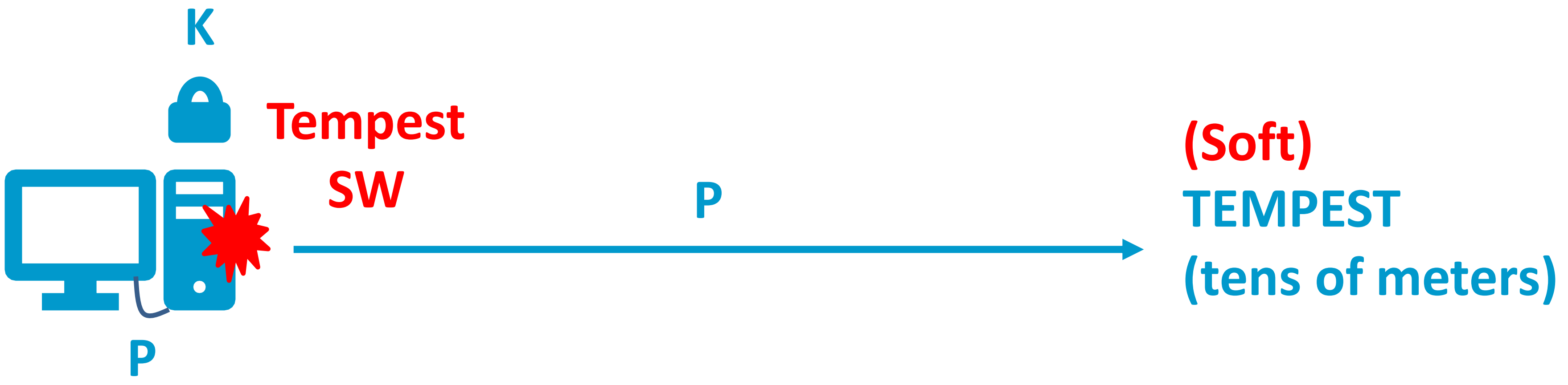
Some categories (informal, non exhaustive)

“TEMPEST: A Signal Problem” (NSA, 1972).

W. van Eck, “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?,” Comput. Secur. 4, no. 4 (1985).

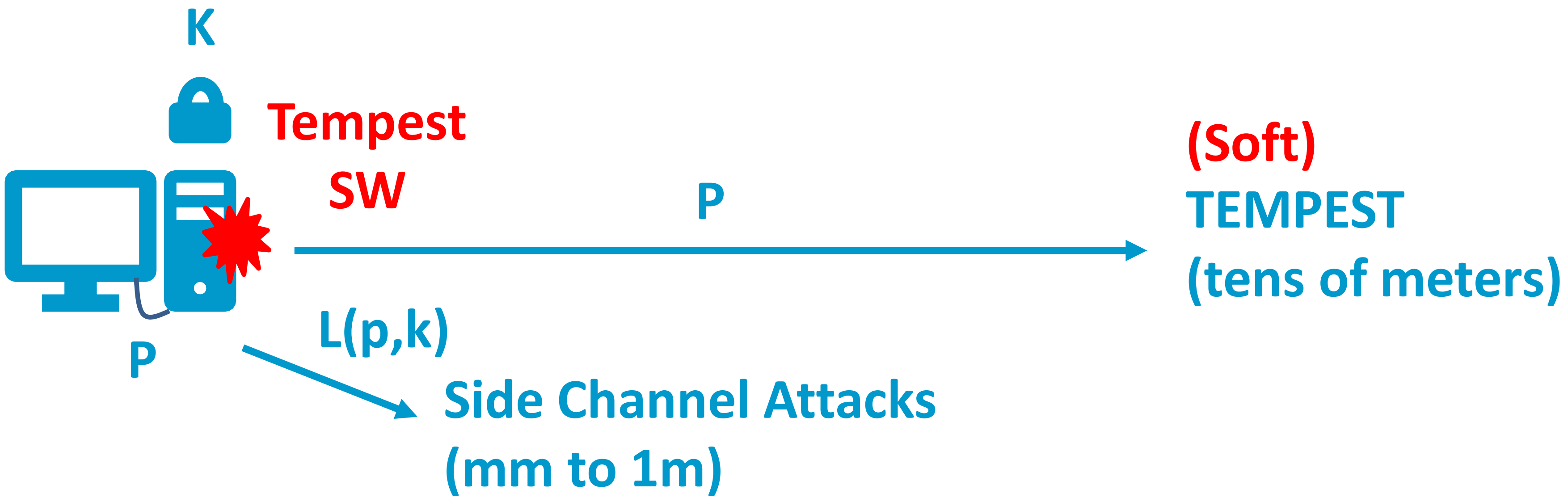
M. G. Kuhn and R. J. Anderson, “Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations,” in Information Hiding (1998).

Some categories (informal, non exhaustive)



“TEMPEST: A Signal Problem” (NSA, 1972).
W. van Eck, “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?,” Comput. Secur. 4, no. 4 (1985).
M. G. Kuhn and R. J. Anderson, “Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations,” in Information Hiding (1998).

Some categories (informal, non exhaustive)



"TEMPEST: A Signal Problem" (NSA, 1972).

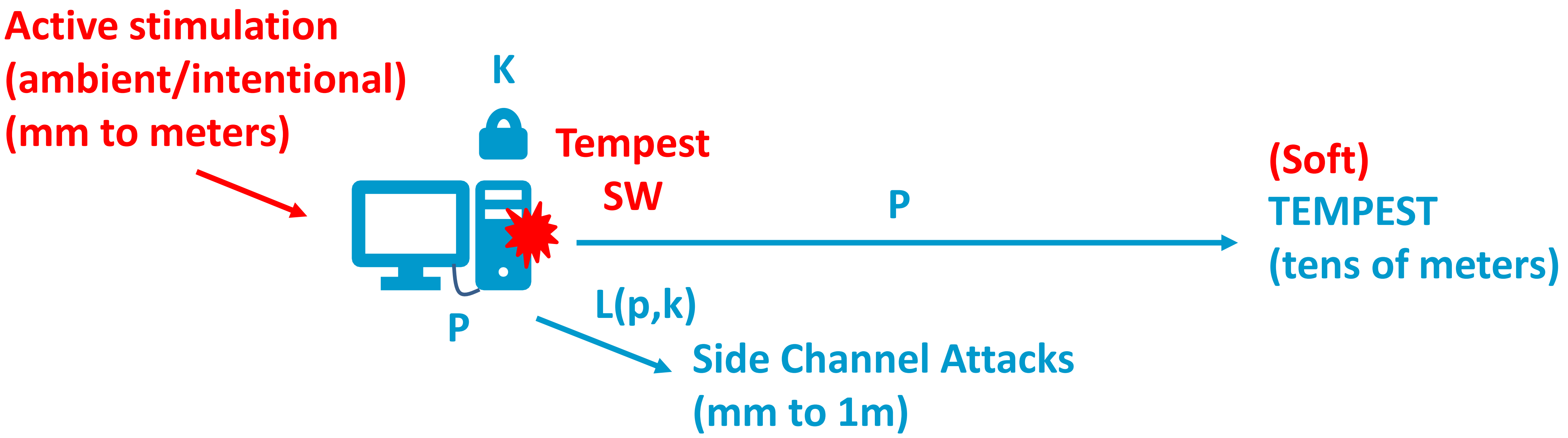
W. van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," Comput. Secur. 4, no. 4 (1985).

M. G. Kuhn and R. J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," in Information Hiding (1998).

D. Agrawal et al., "The EM Side-Channel(s)," in CHES 2002.

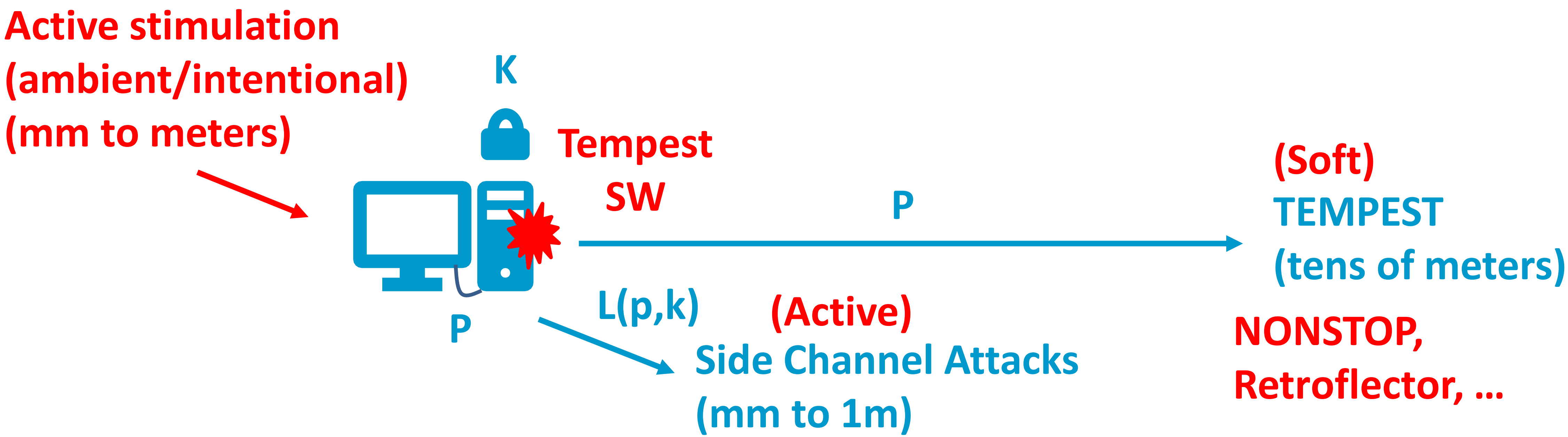
C. Ramsay and J. Lohuis, TEMPEST Attacks against AES, 2017.

Some categories (informal, non exhaustive)



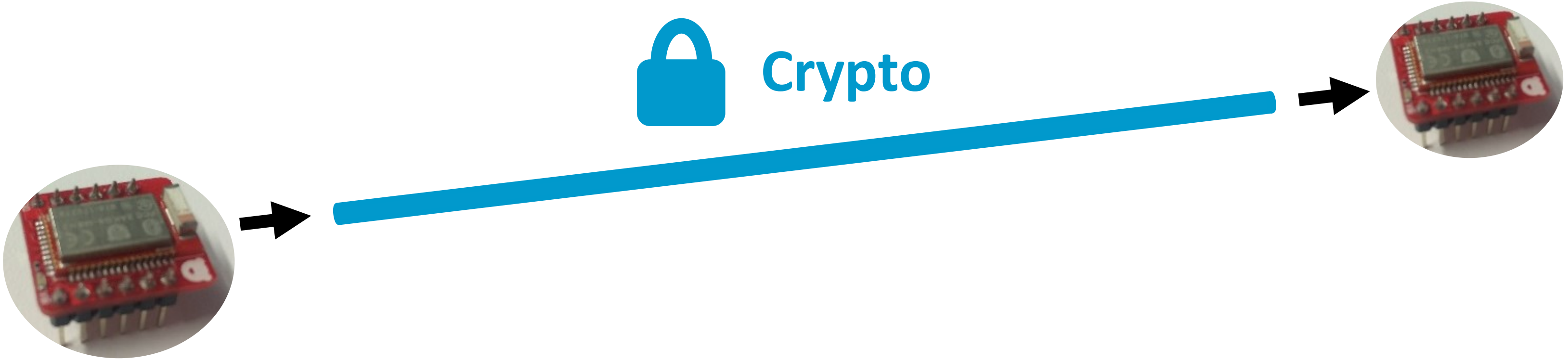
"TEMPEST: A Signal Problem" (NSA, 1972).
W. van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," Comput. Secur. 4, no. 4 (1985).
M. G. Kuhn and R. J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," in Information Hiding (1998).
D. Agrawal et al., "The EM Side-Channel(s)," in CHES 2002.
C. Ramsay and J. Lohuis, TEMPEST Attacks against AES, 2017.

Some categories (informal, non exhaustive)



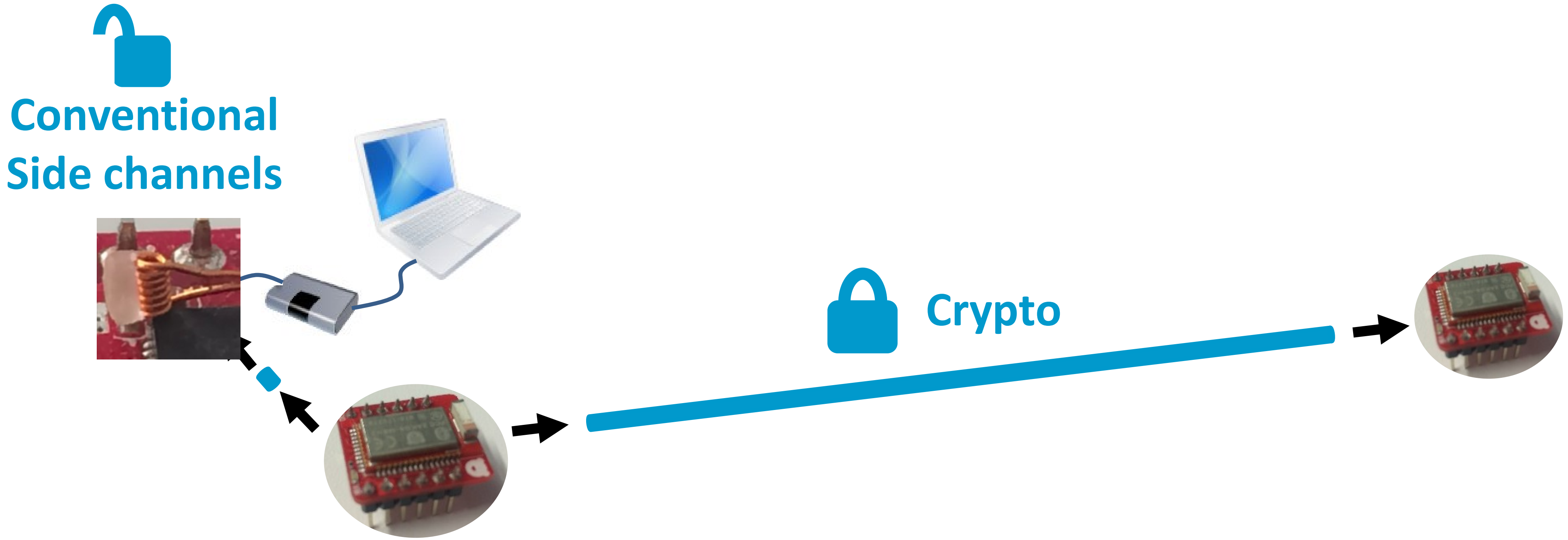
"TEMPEST: A Signal Problem" (NSA, 1972).
W. van Eck, "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?," Comput. Secur. 4, no. 4 (1985).
M. G. Kuhn and R. J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," in Information Hiding (1998).
D. Agrawal et al., "The EM Side-Channel(s)," in CHES 2002.
C. Ramsay and J. Lohuis, TEMPEST Attacks against AES, 2017.
A. T. Markettos, "Active Electromagnetic Attacks on Secure Hardware" (PhD Thesis, University of Cambridge, UK, 2011).

Side channels against communication devices



EURECOM
Sophia Antipolis

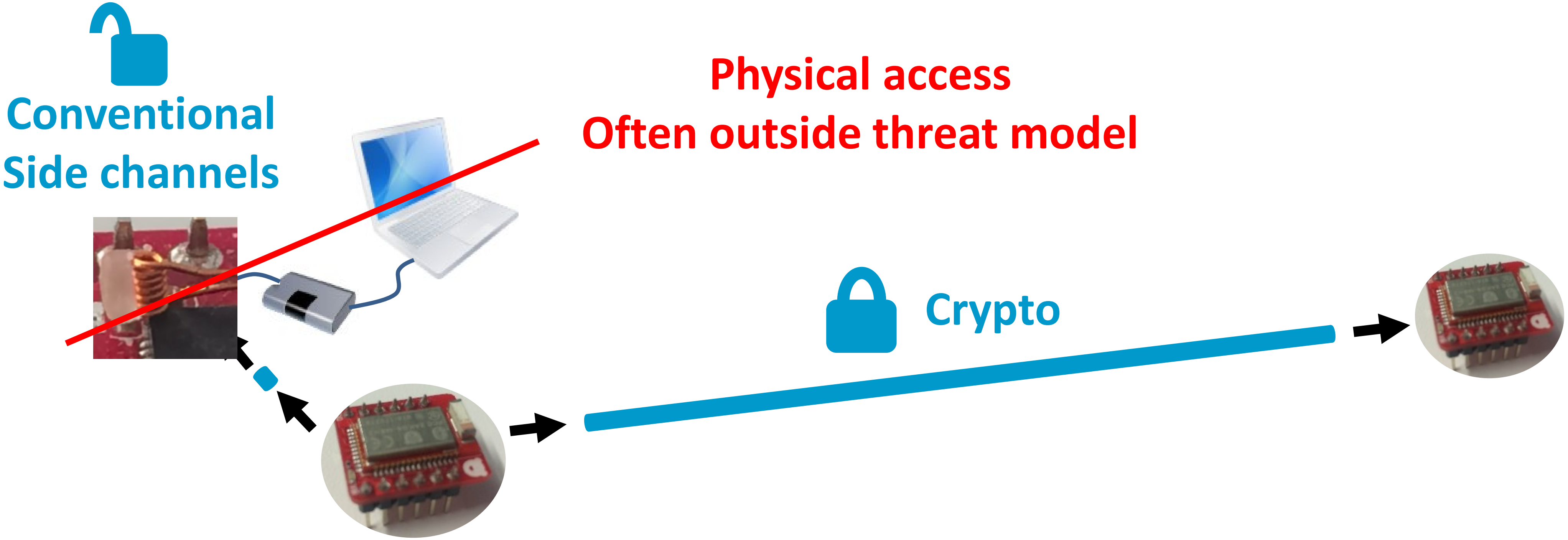
Side channels against communication devices



A. Biryukov, D. Dinu, and Y. Le Corre, “Side-Channel Attacks Meet Secure Network Protocols,” in ACNS 2017.

C. O’Flynn and Z. Chen, “Power Analysis Attacks Against IEEE 802.15.4 Nodes,” in COSADE 2016.

Side channels against communication devices



A. Biryukov, D. Dinu, and Y. Le Corre, "Side-Channel Attacks Meet Secure Network Protocols," in ACNS 2017.

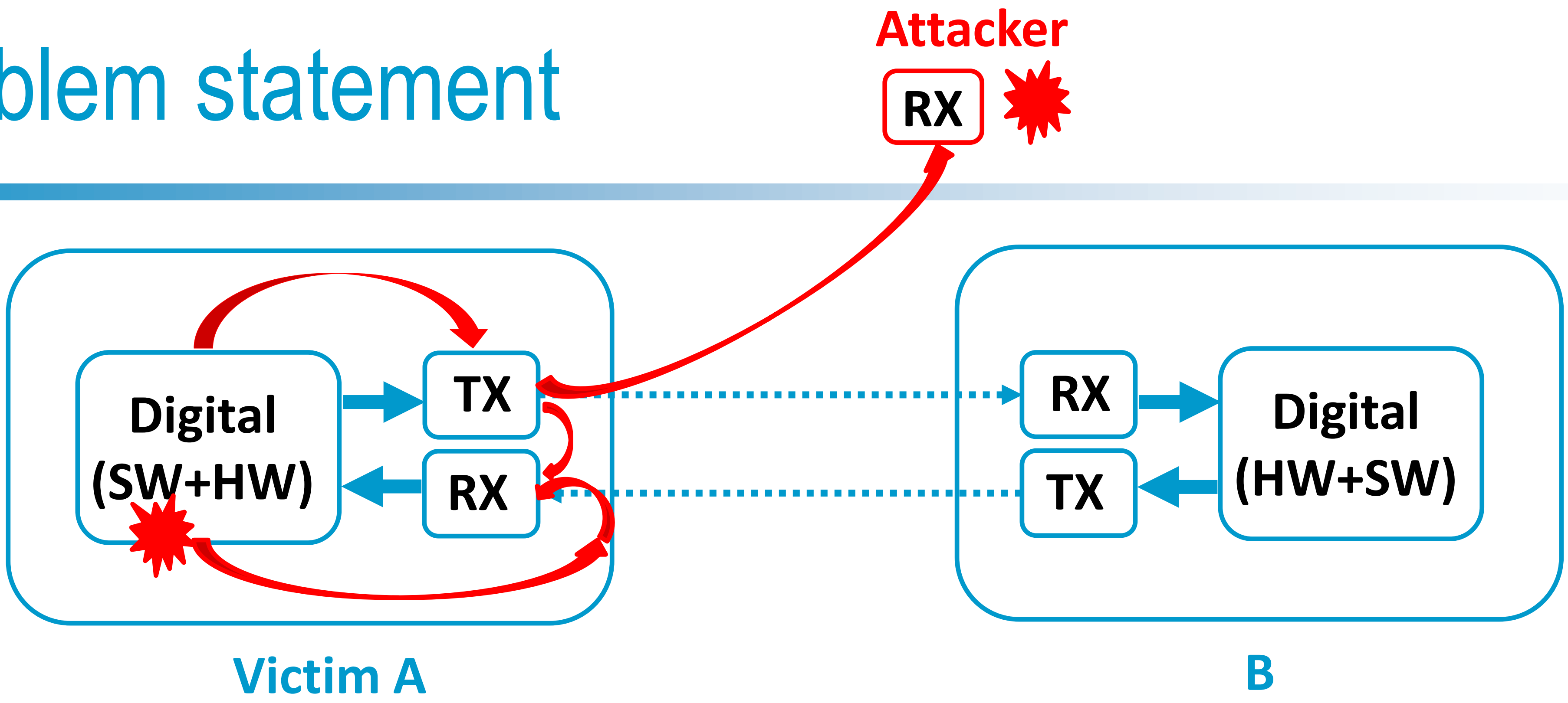
C. O'Flynn and Z. Chen, "Power Analysis Attacks Against IEEE 802.15.4 Nodes," in COSADE 2016.

AES Implementation Resistant to Side-Channel Analysis Attacks? - Discussion Forum - Mbed TLS (Previously PolarSSL)

Putting all together:

Security threats emerging from the interaction between digital activity and radio transceivers

Problem statement



Security research question

(EmSec) (EMI/RFI) (WiSec)

Does logic activity produce physical leakages that flow from digital components to radio blocks breaking the security of the wireless links?

E.g., confidentiality, authenticity

Some related work in this direction

Parasitic backscattering in RFID (Load modulation in NFC)

- **Power modulates impedance seen by reader**
- **Side-channels up to 1m**

T. Plos, "Susceptibility of UHF RFID Tags to Electromagnetic Analysis," in RSA Conference 2008.

Some related work in this direction

Parasitic backscattering in RFID (Load modulation in NFC)
- **Power modulates impedance seen by reader**
- **Side-channels up to 1m**

Backscattering in WiFi cards
- **Card state (on/off) changes impedance**
- **Covert channels**

T. Plos, "Susceptibility of UHF RFID Tags to Electromagnetic Analysis," in RSA Conference 2008.

Z. Yang, Q. Huang, and Q. Zhang, "NICScatter: Backscatter as a Covert Channel in Mobile Devices," in MobiCom 2017.

Some related work in this direction

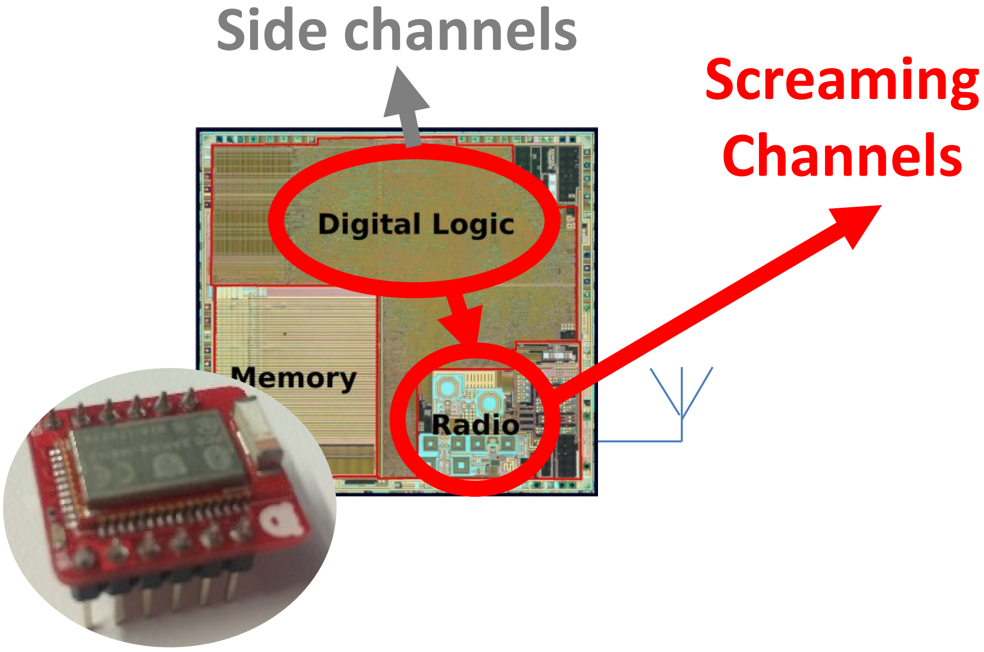
Parasitic backscattering in RFID (Load modulation in NFC)	**Power modulates impedance seen by reader** **Side-channels up to 1m**
Backscattering in WiFi cards	**Card state (on/off) changes impedance** **Covert channels**
Second-Order Soft-TEMPEST	**Soft-TEMPEST + cascaded effects** **Polyglot covert channel on WiFi**

T. Plos, “Susceptibility of UHF RFID Tags to Electromagnetic Analysis,” in RSA Conference 2008.

Z. Yang, Q. Huang, and Q. Zhang, “NICScatter: Backscatter as a Covert Channel in Mobile Devices,” in MobiCom 2017.

E. Cottais, J. Lopes Esteves, and C. Kasmi, “Second Order Soft-TEMPEST in RF Front-Ends: Design and Detection of Polyglot Modulations,” EMC EUROPE 2018.

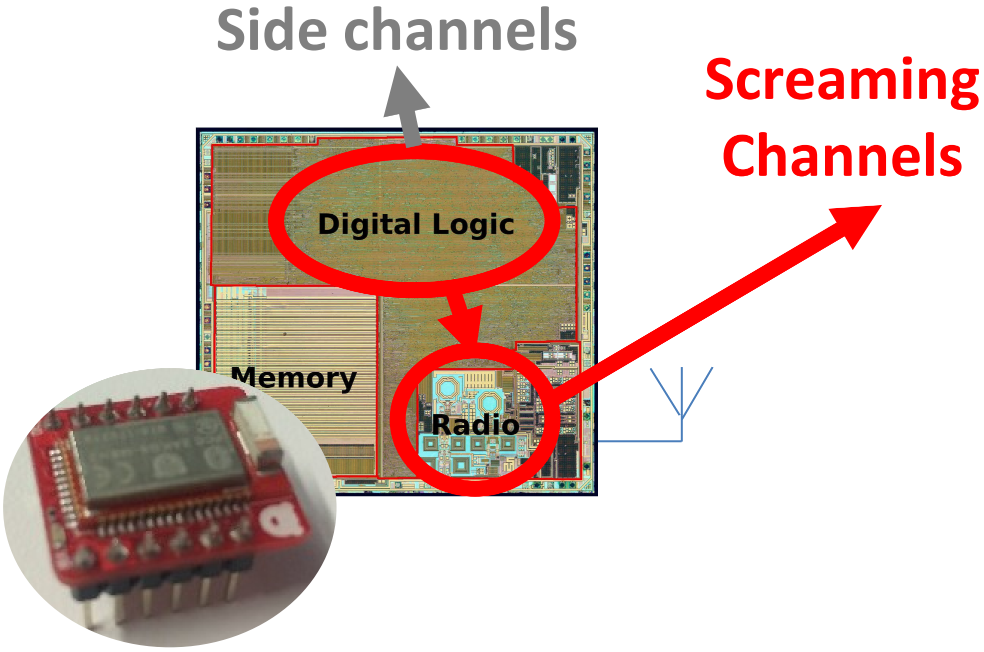
Contributions: two novel security problems

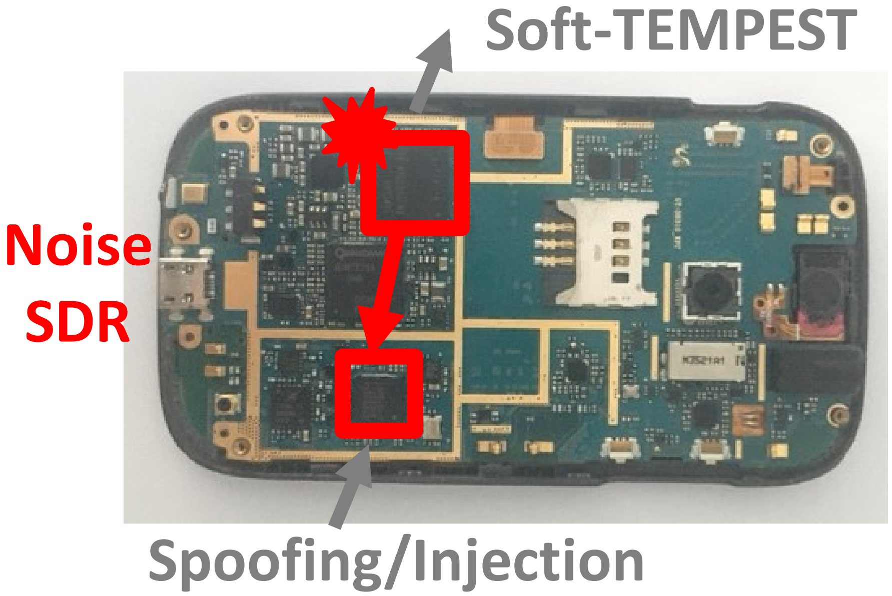


Screaming Channels (Digital to TX)

Passive side channel leakage from digital activity to the radio transmitter and the radio channel

Contributions: two novel security problems





Screaming Channels (Digital to TX)

Passive side channel leakage from digital activity to the radio transmitter and the radio channel

Noise-SDR (Digital to RX)

Active arbitrary modulation of digital noise to generate valid signals to inject in other receivers

Publications

Screaming Channels: When Electromagnetic Side Channels Meet Radio Transceivers
Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, Aurélien Francillon
Proceedings of the 25th ACM conference on Computer and communications security (CCS) , Toronto, Canada (acceptance rate: 16.6%)
Third place at the CSAW Europe applied research competition 2018

Understanding Screaming Channels: From a Detailed Analysis to Improved Attacks
Giovanni Camurati, Aurélien Francillon, François-Xavier Standaert
IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES 2020)
Google Bughunter Hall of Fame Honorable Mention

Screaming Channels

Noise-SDR: Shaping Arbitrary Radio Signals Out of Noise on Modern Smartphones
Giovanni Camurati, Aurélien Francillon
Under submission (major revision)

Noise-SDR

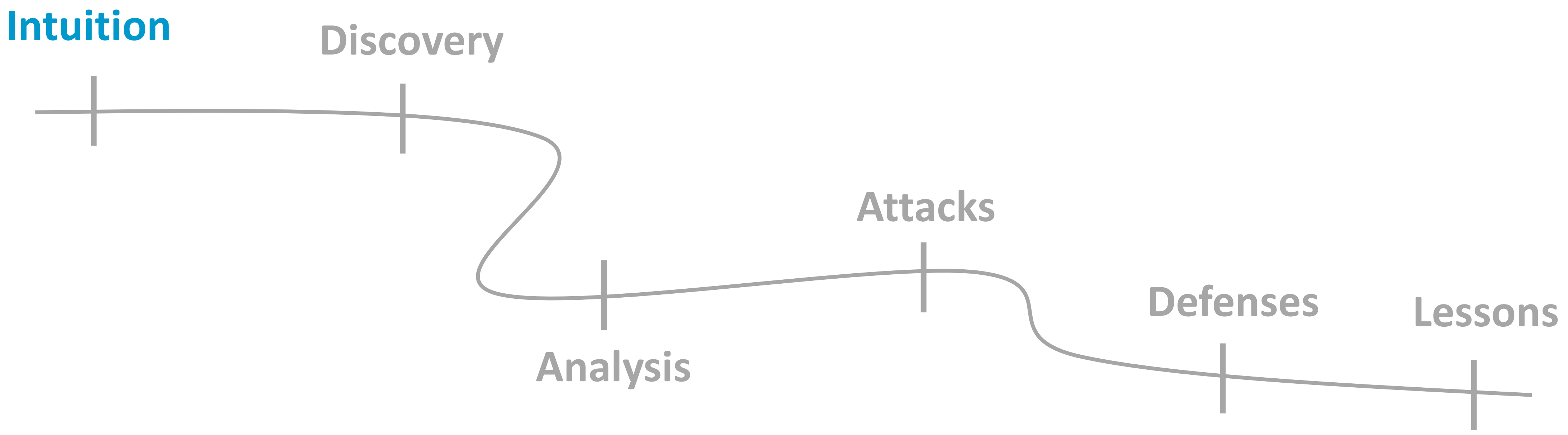
SoC Security Evaluation: Reflections on Methodology and Tooling
Nassim Corteggiani, Giovanni Camurati, Marius Muench, Sebastian Poeplau, Aurélien Francillon
Accepted for publication in IEEE Design and Test, Special Issue on Hack@DAC

Inception: System-wide Security Testing of Real-World Embedded Systems Software
Nassim Corteggiani, Giovanni Camurati, Aurélien Francillon
27th USENIX Security Symposium (USENIX Security 18) , Baltimore, MD (acceptance rate: 19.1%)

Other

- Context
- Challenges & Contributions
- **Screaming Channels**
- Noise-SDR
- Future Work
- Conclusion

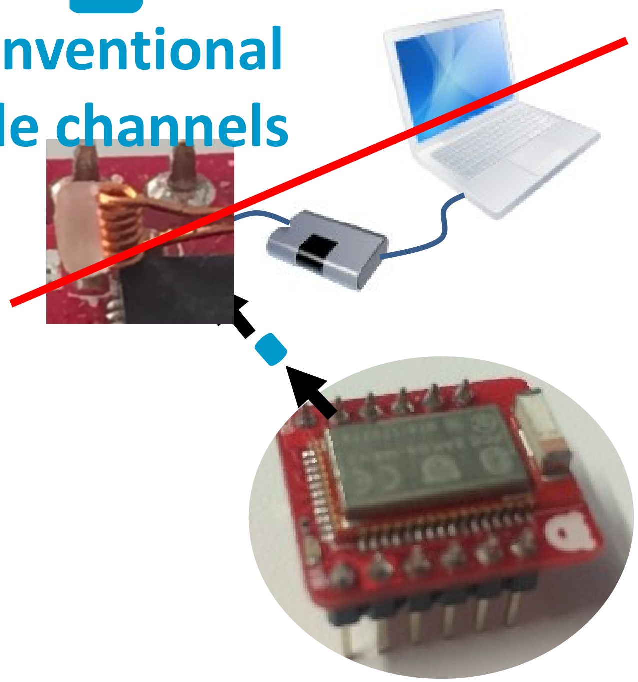
Studying a novel side channel



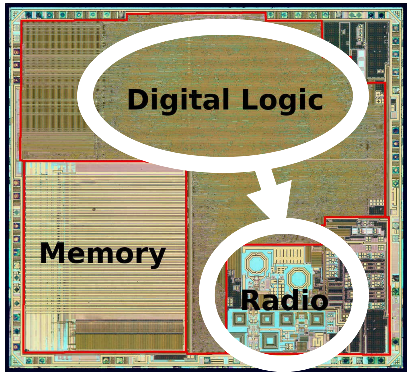
Screaming Channels

Conventional
Side channels

Physical access
Often outside threat model

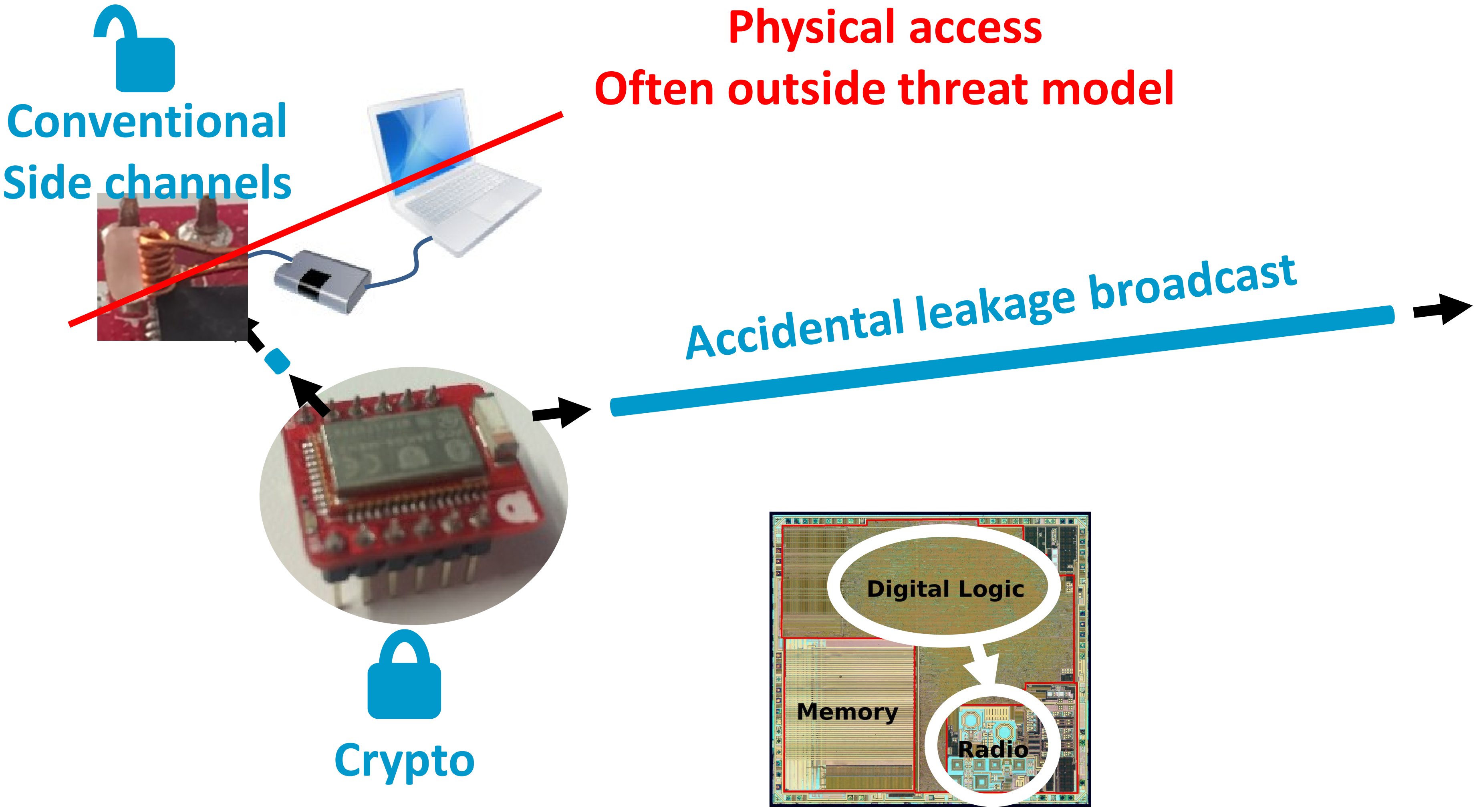


Crypto

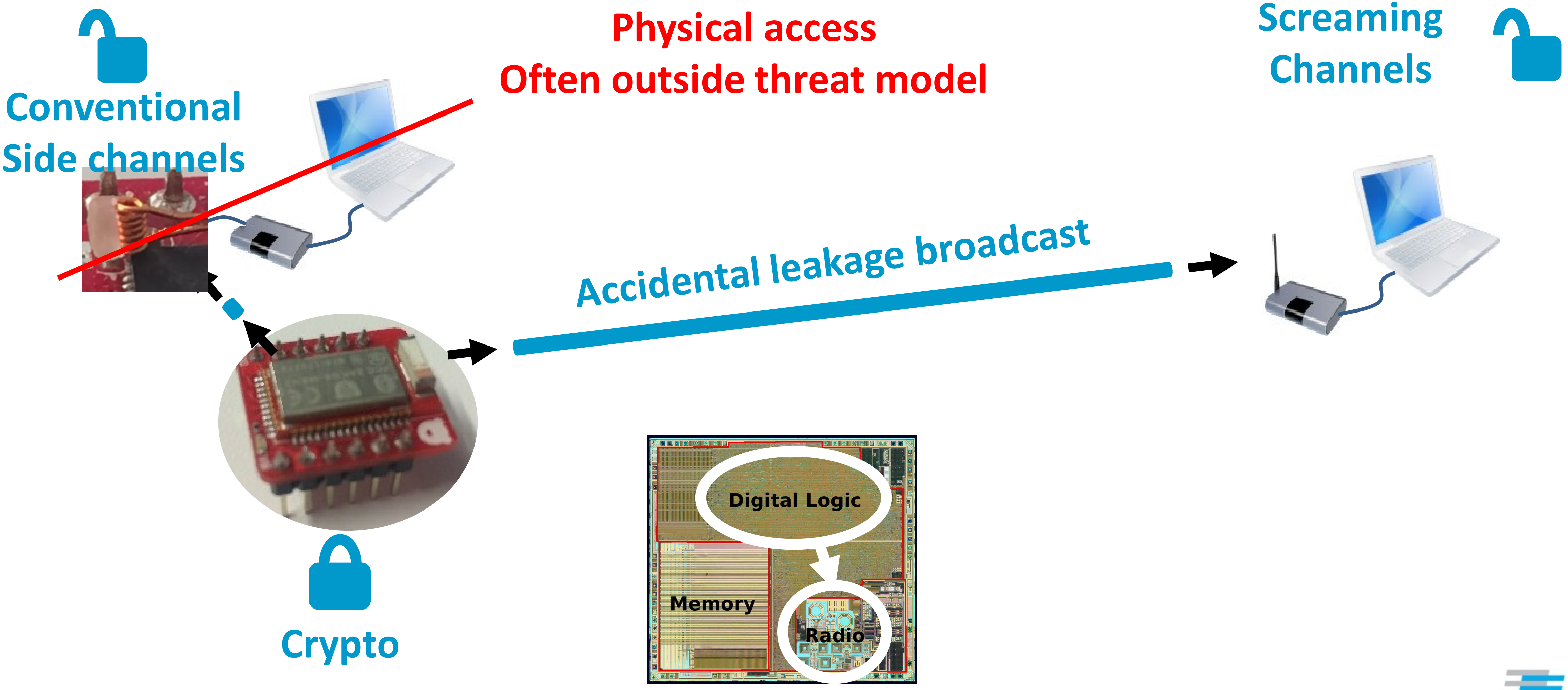


EURECOM
Sophia Antipolis

Screaming Channels



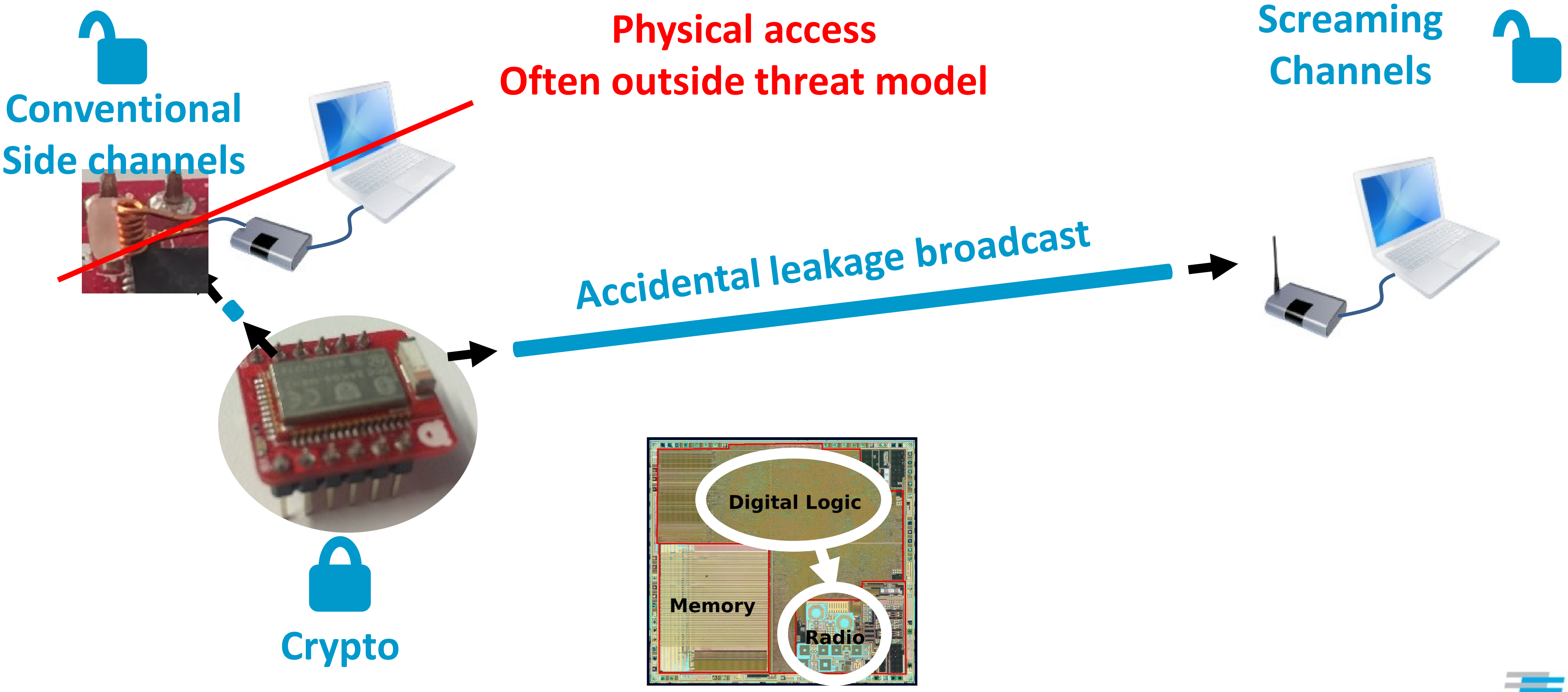
Screaming Channels



EURECOM

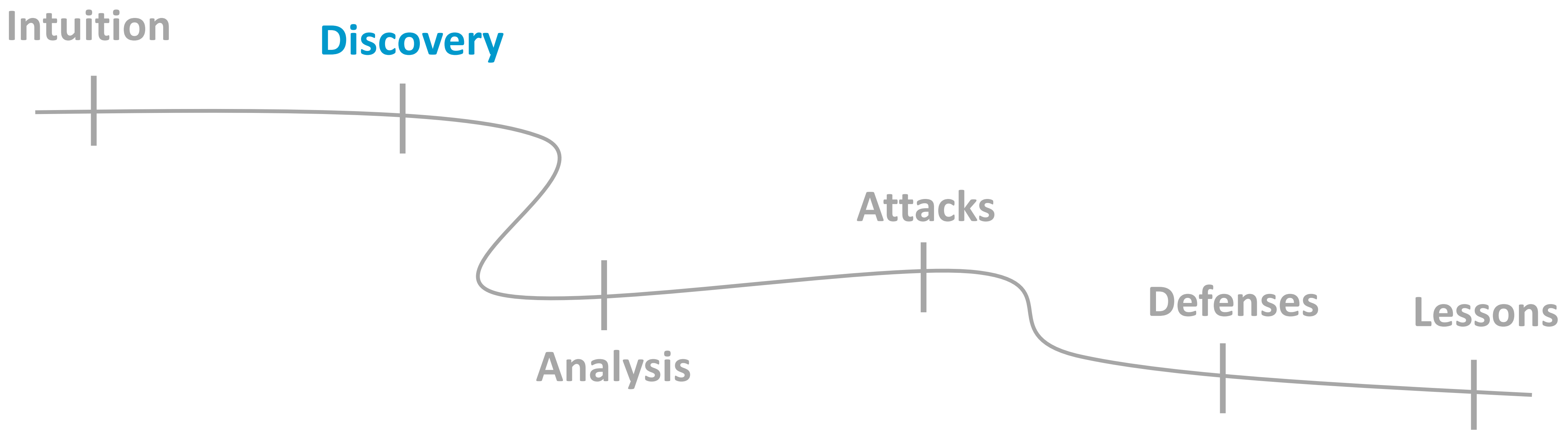
Screaming Channels

Digital activity visible at large distance



EURECOM

Studying a novel side channel

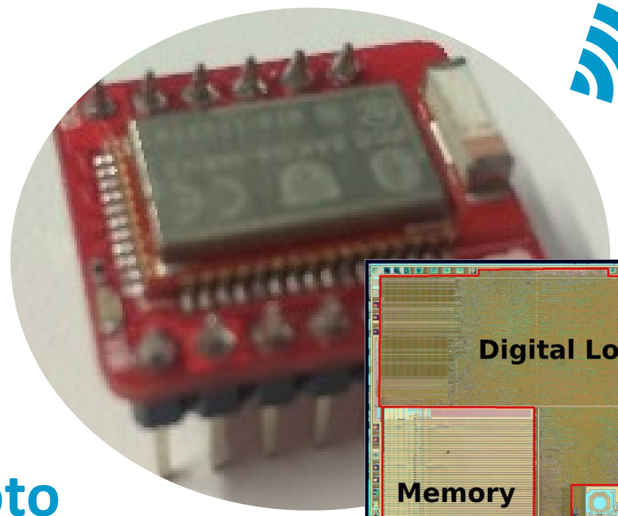


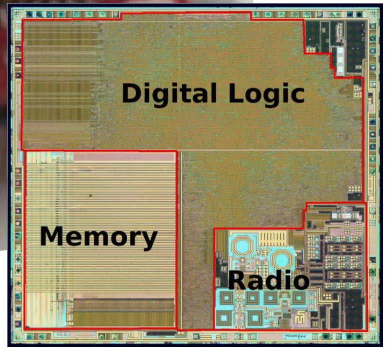
Identifying a possible target

Computation
Arm Cortex-M4 @64MHz

Wireless communication
BLE @2.4GHz

Sensing & Actuation





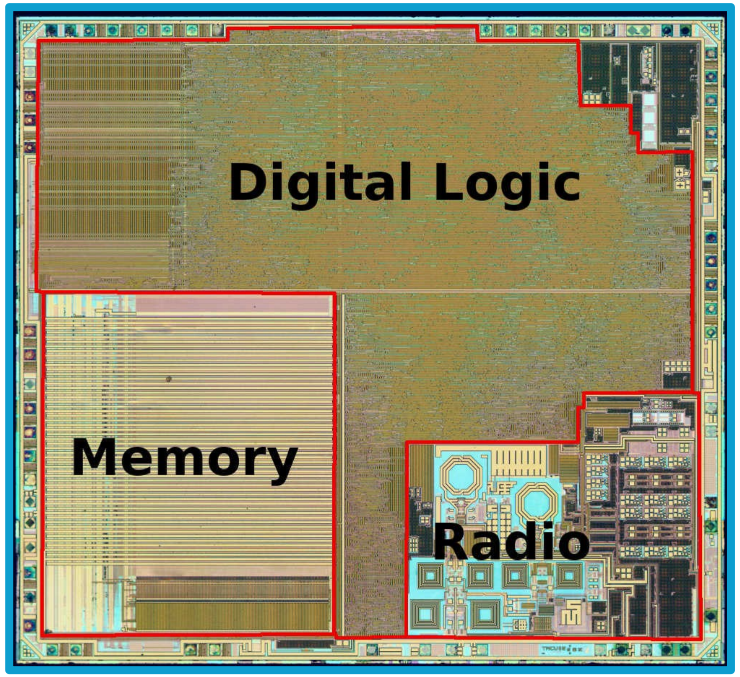
Crypto
(SW/HW)

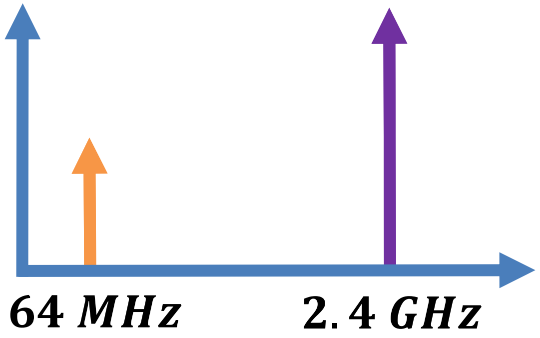
All in one chip
“Mixed-signal”
Low cost, low power
Easy to integrate

Observing the signal

Mixed-signal chip

Strong noise source





Easy propagation

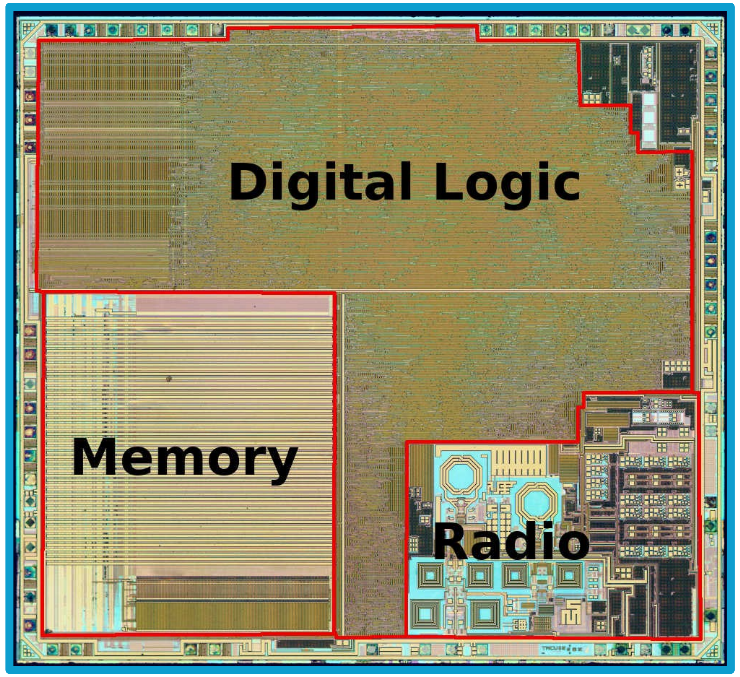
EURECOM

Observing the signal

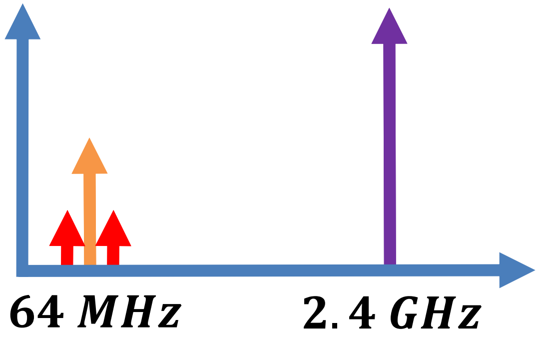
Conventional Side Channel Leak

Mixed-signal chip

Strong noise source



Easy propagation



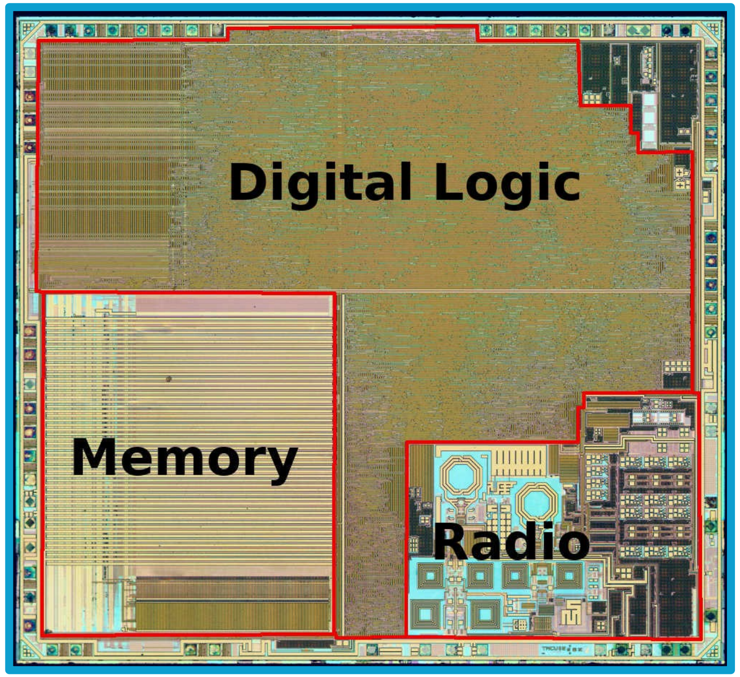
EURECOM

Observing the signal

Conventional Side Channel Leak

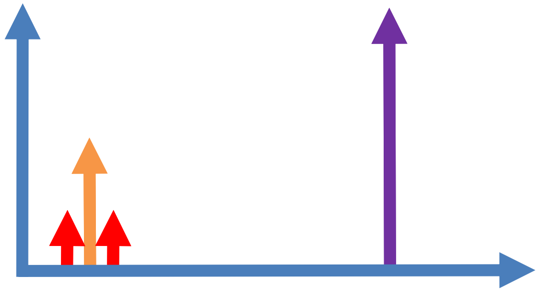
Strong noise source

Mixed-signal chip



Easy propagation

Leak Propagation

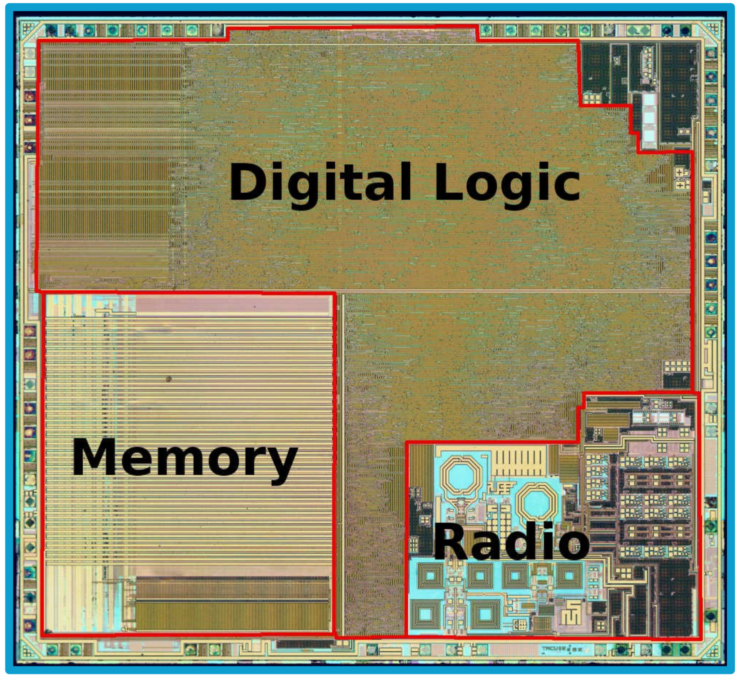


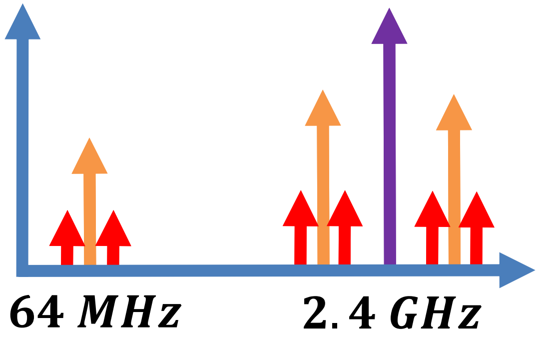
Observing the signal

Conventional Side Channel Leak

Strong noise source

Mixed-signal chip



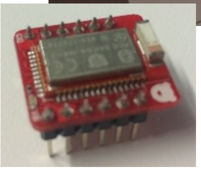


Easy propagation
Leak Propagation

Leak Is Broadcast

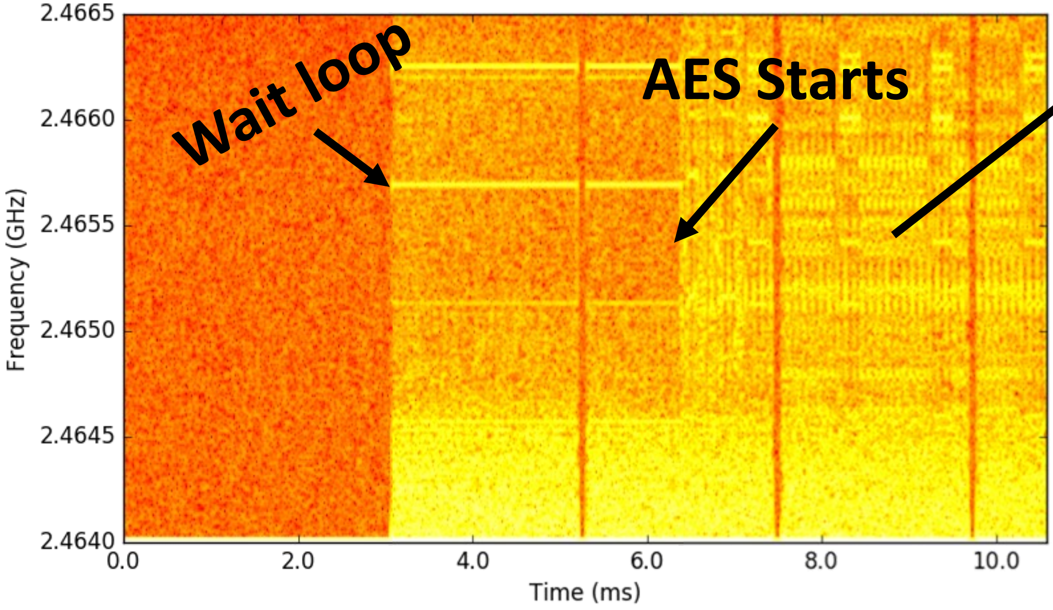
Identifying an attack model: app layer software AES

Antenna + SDR RX

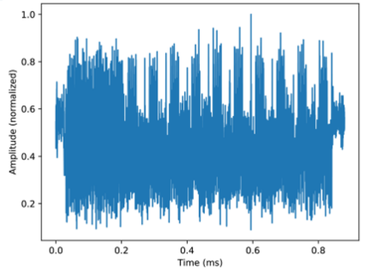


Cortex-M4 + BLE TX

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



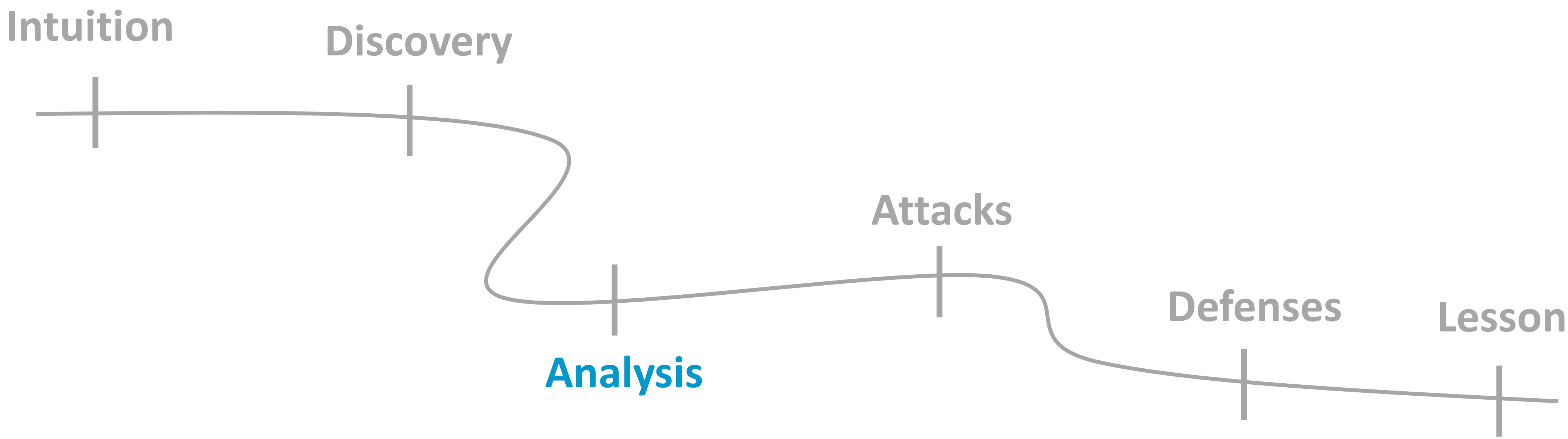
Noise **Packet**



Time domain

EURECOM

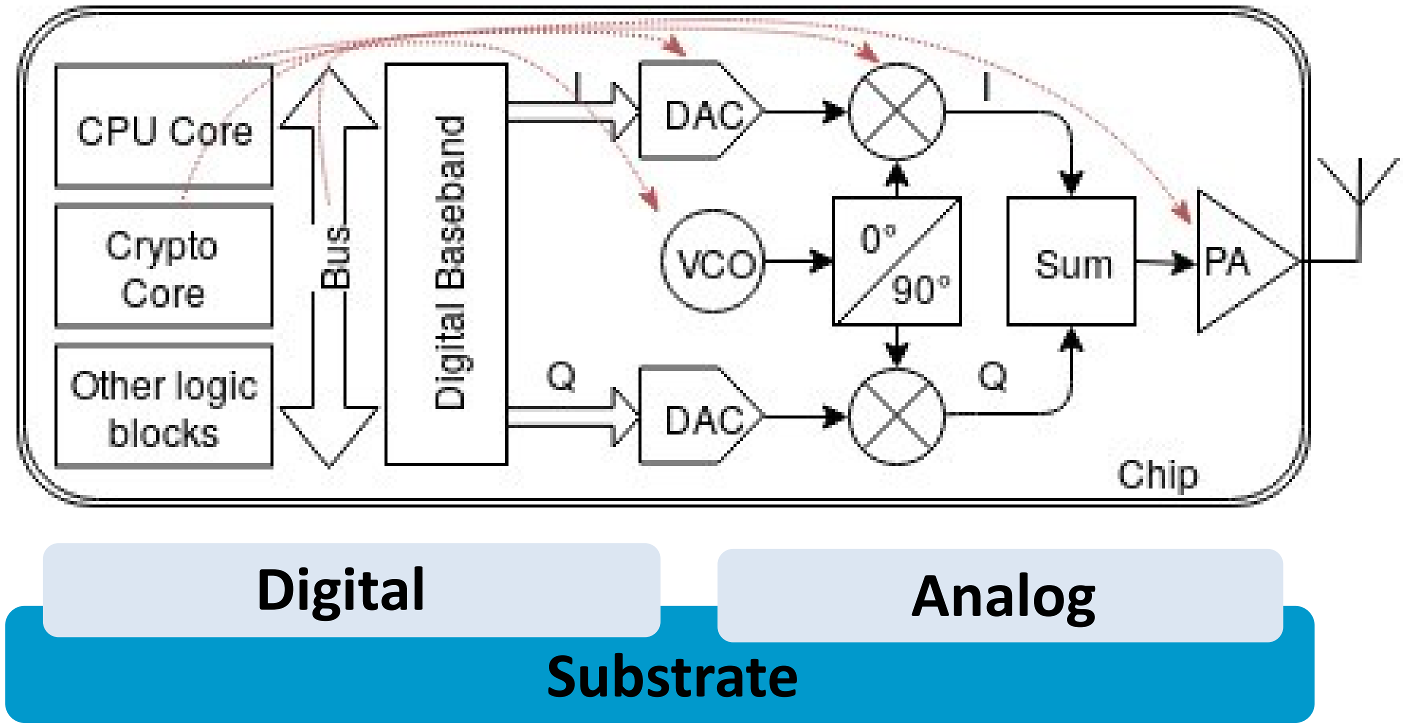
Studying a novel side channel



EURECOM
Sophia Antipolis

Studying the root cause

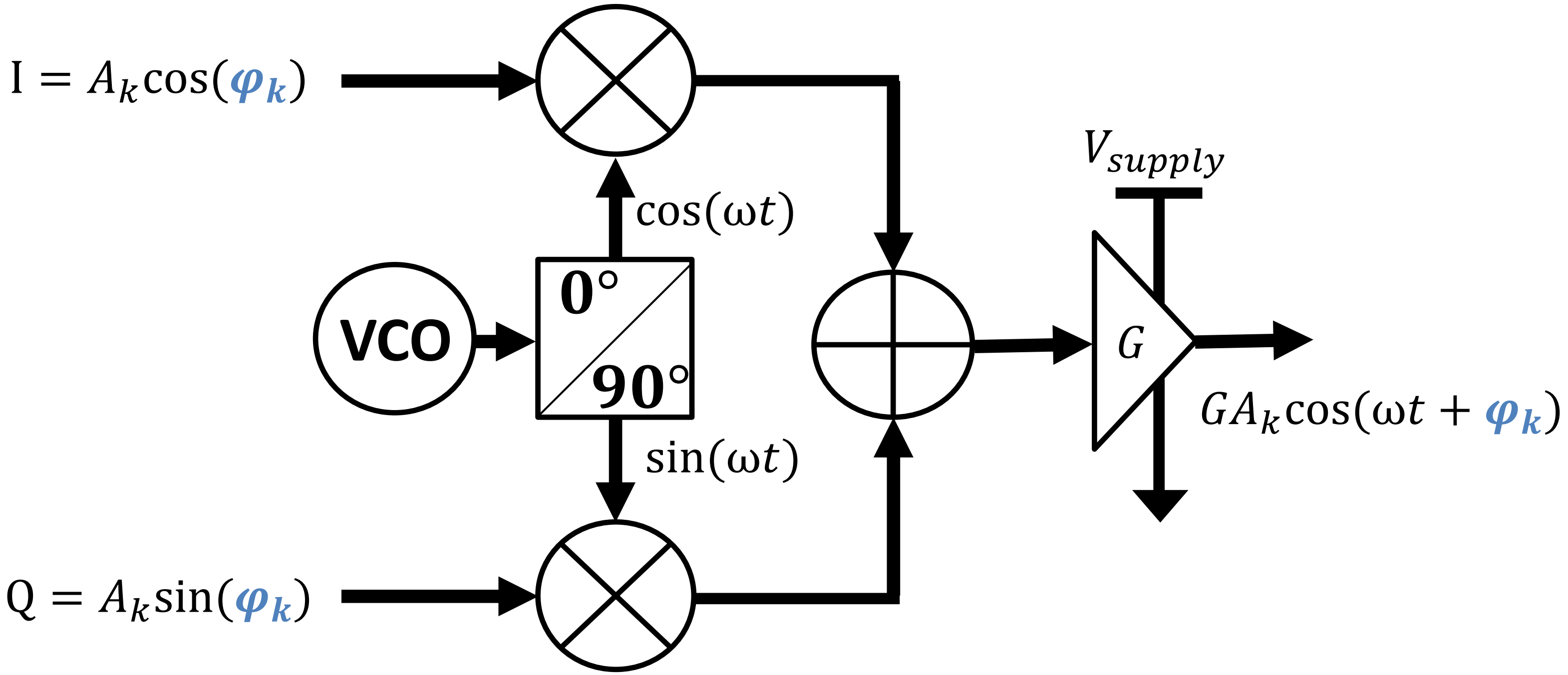
Many Possible coupling paths



Examples: A. Behzad, “Wireless LAN Radios: System Definition to Transistor Design” (IEEE Press Series on Microelectronic Systems) (Hoboken, NJ, USA: John Wiley & Sons, Inc., 2008).

Studying the root cause

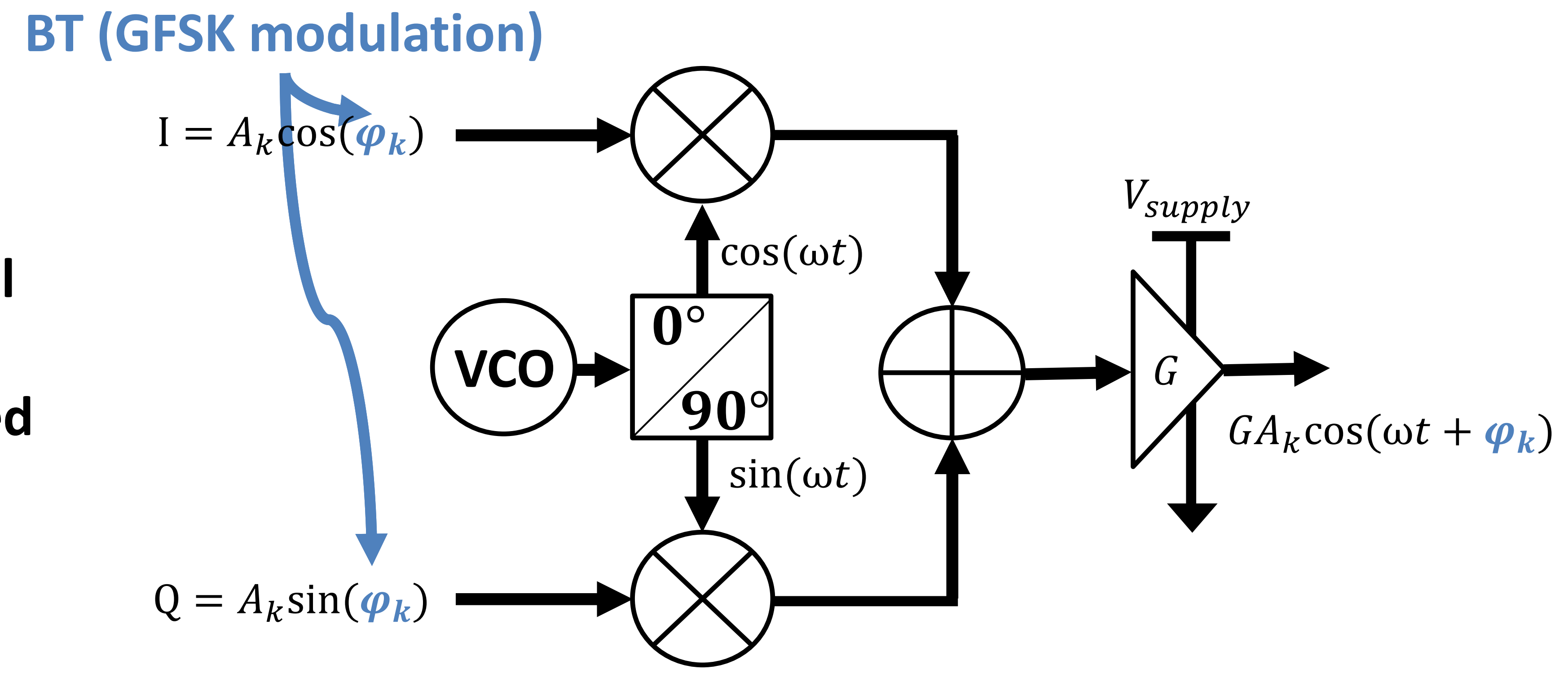
Practical case we observed



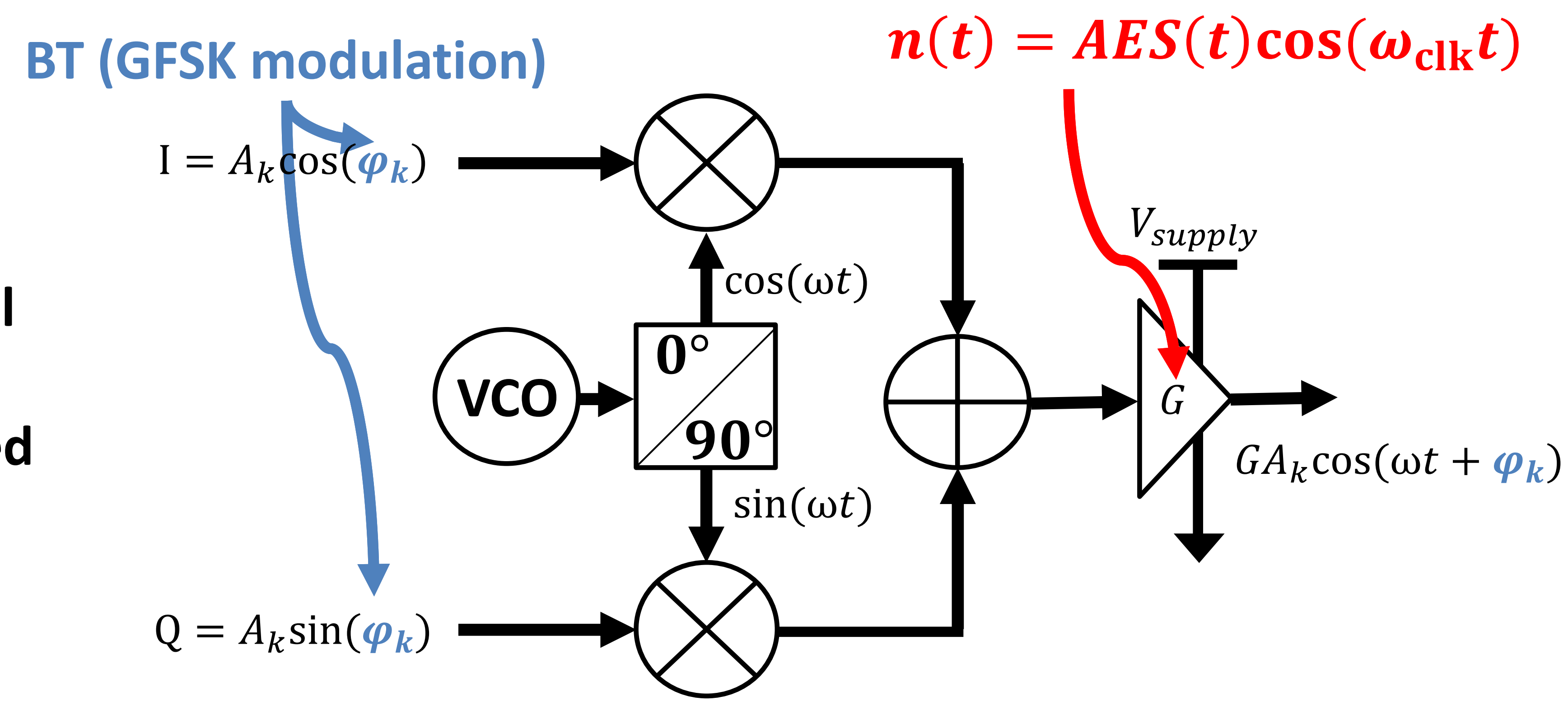
EURECOM

Studying the root cause

Practical case we observed



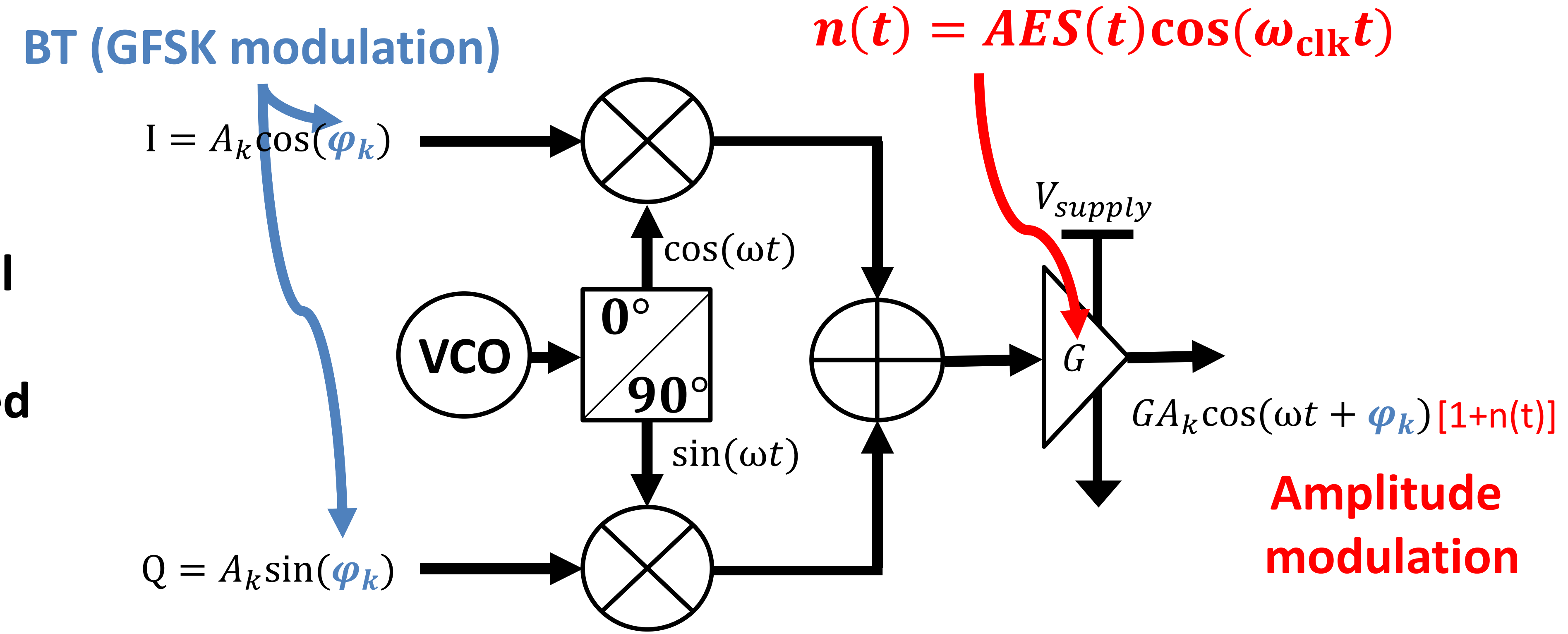
Studying the root cause



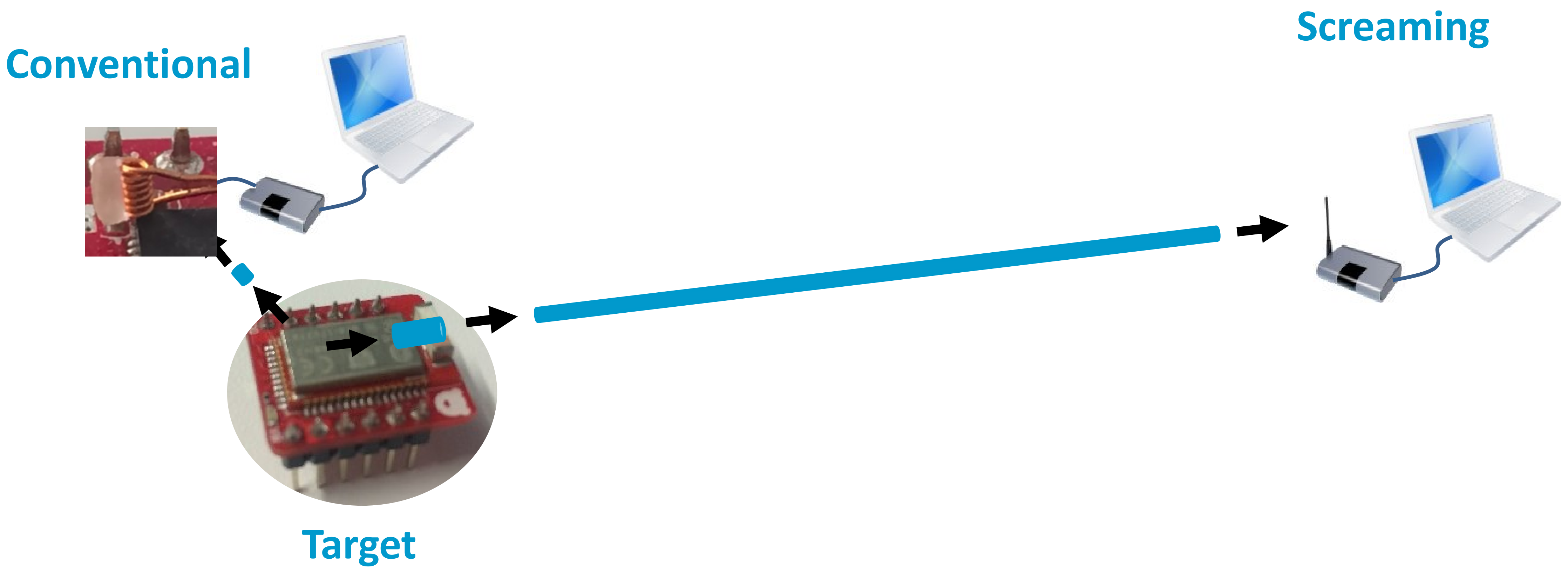
Practical case we observed

Studying the root cause

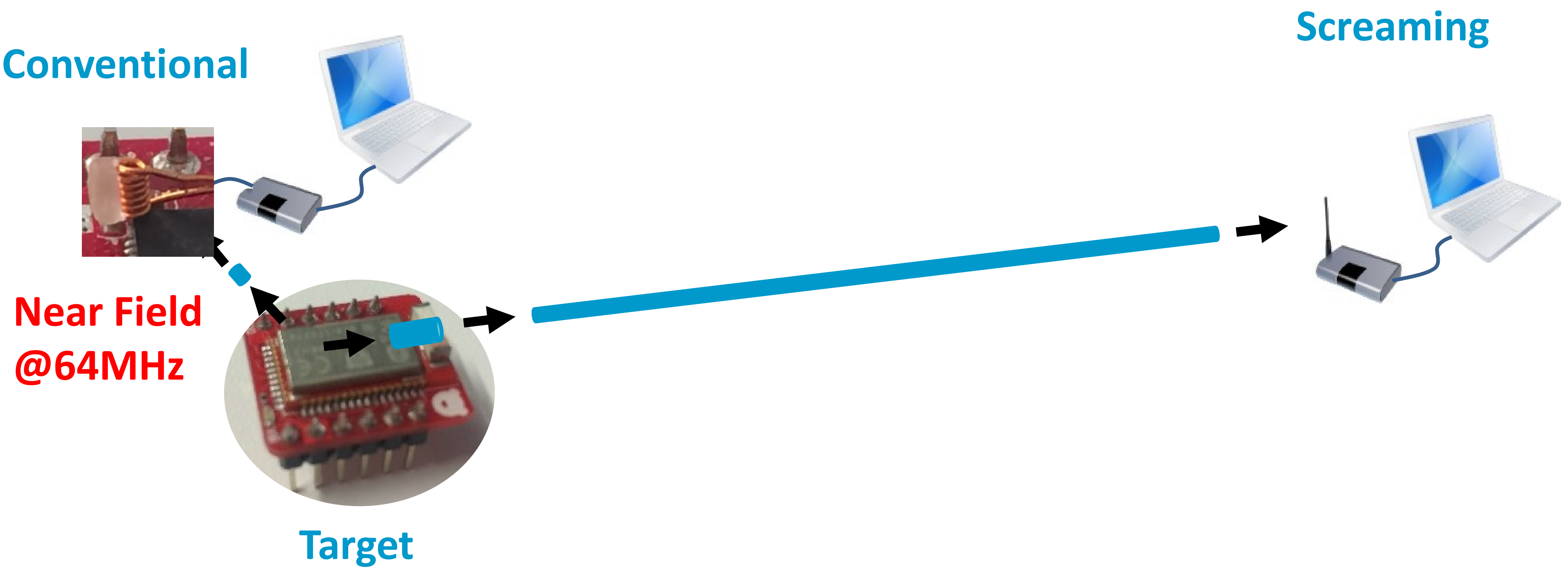
Practical case we observed



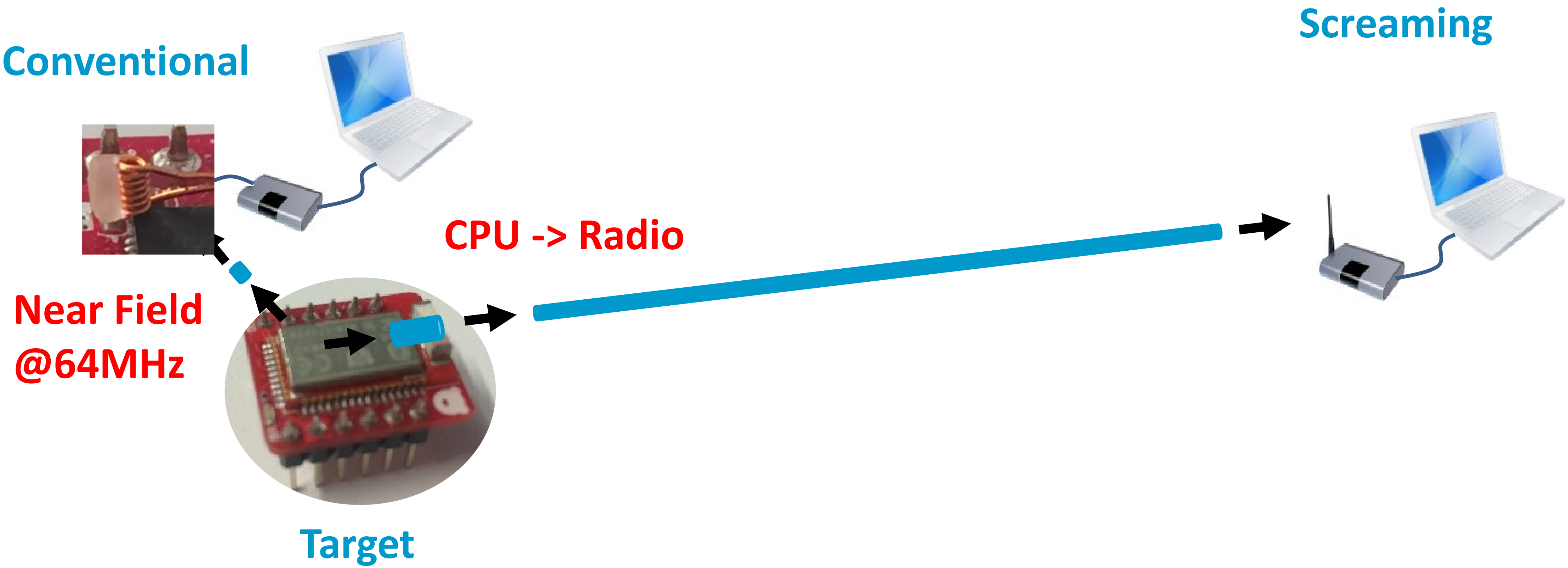
Detailed experimental study of a novel channel



Detailed experimental study of a novel channel

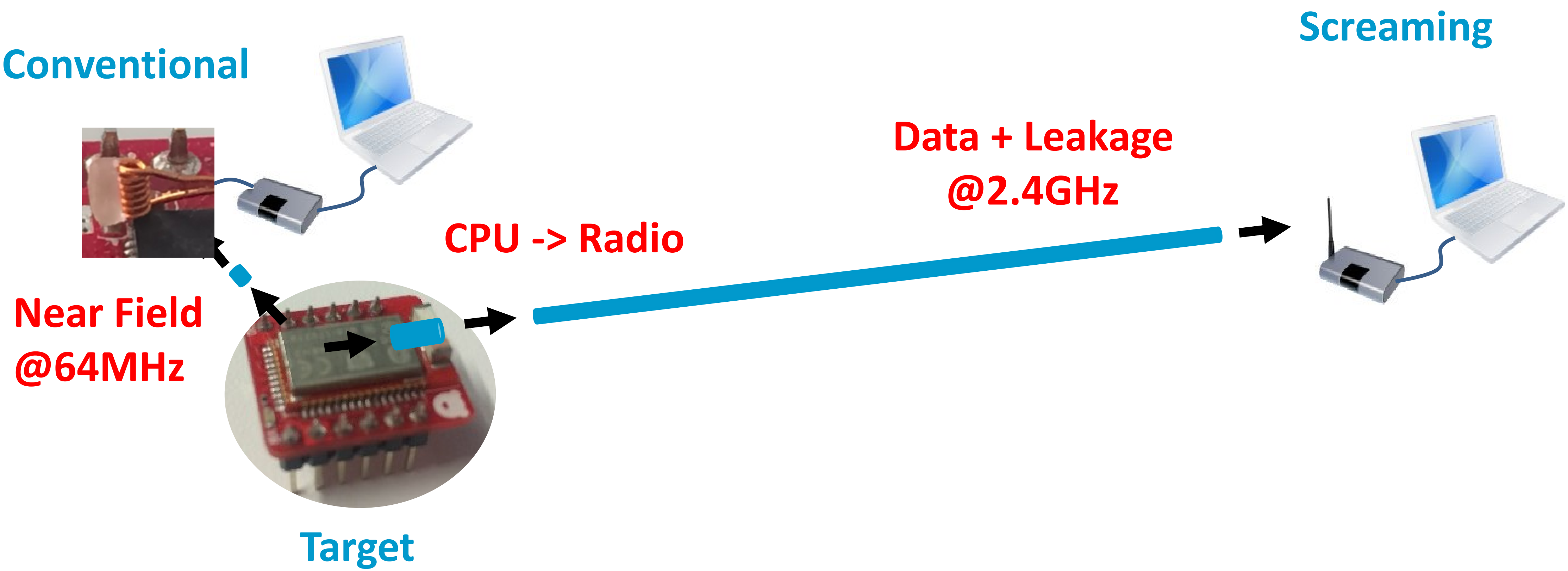


Detailed experimental study of a novel channel

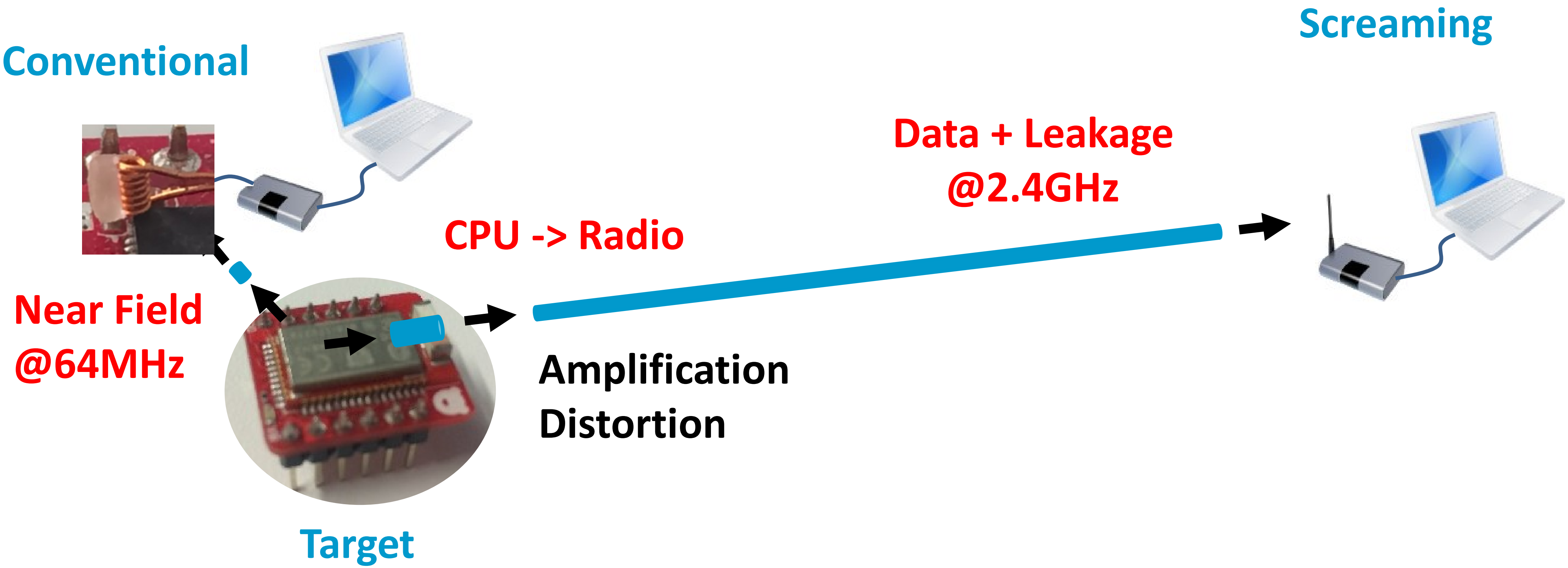


EURECOM

Detailed experimental study of a novel channel

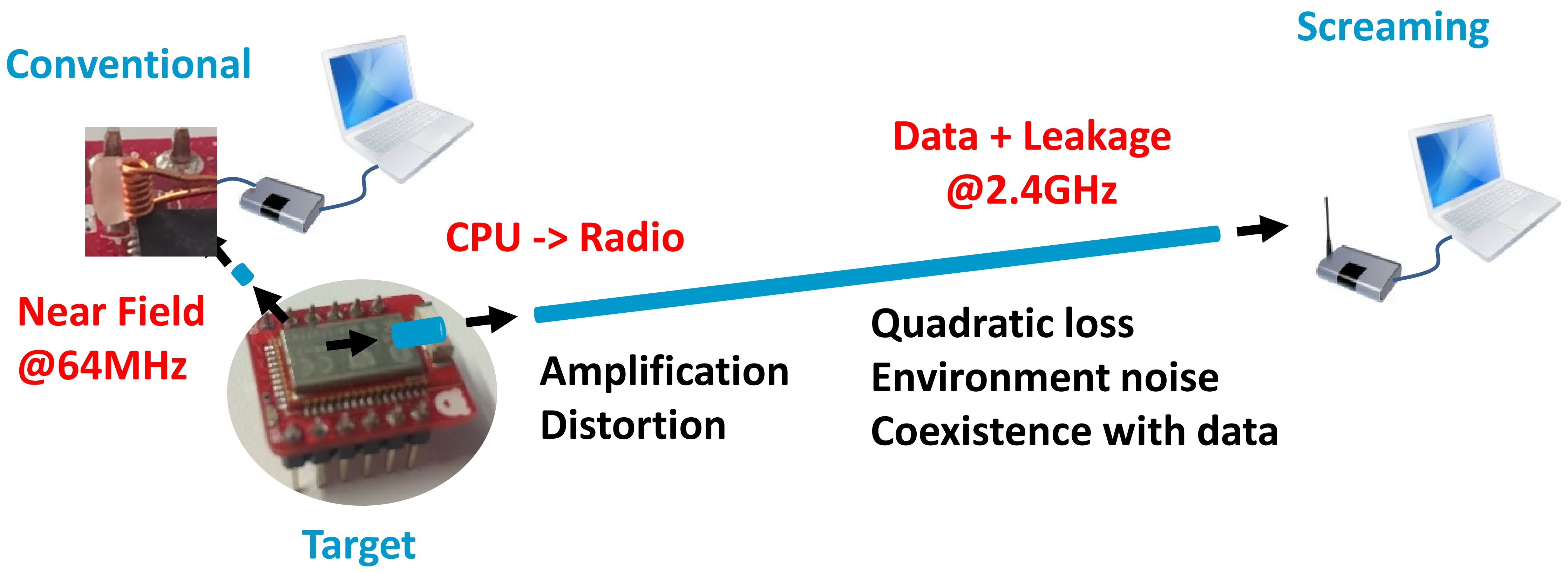


Detailed experimental study of a novel channel

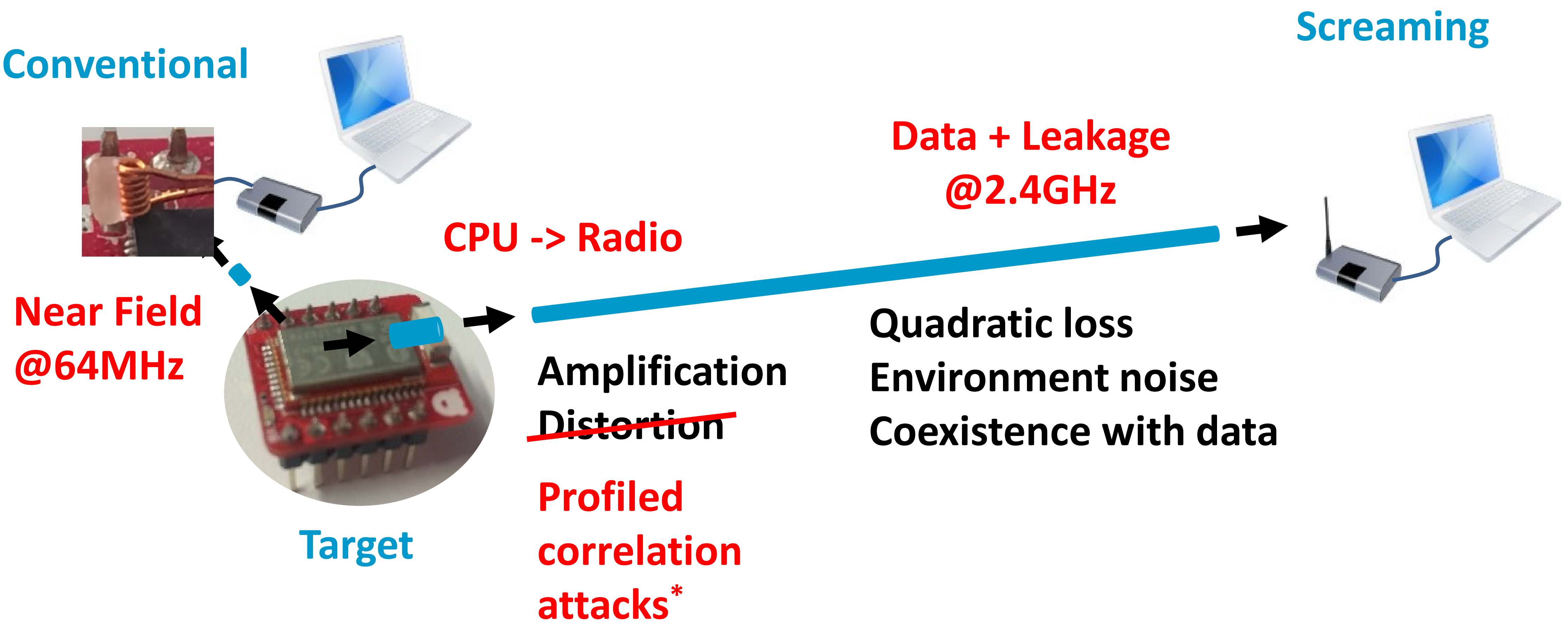


EURECOM

Detailed experimental study of a novel channel

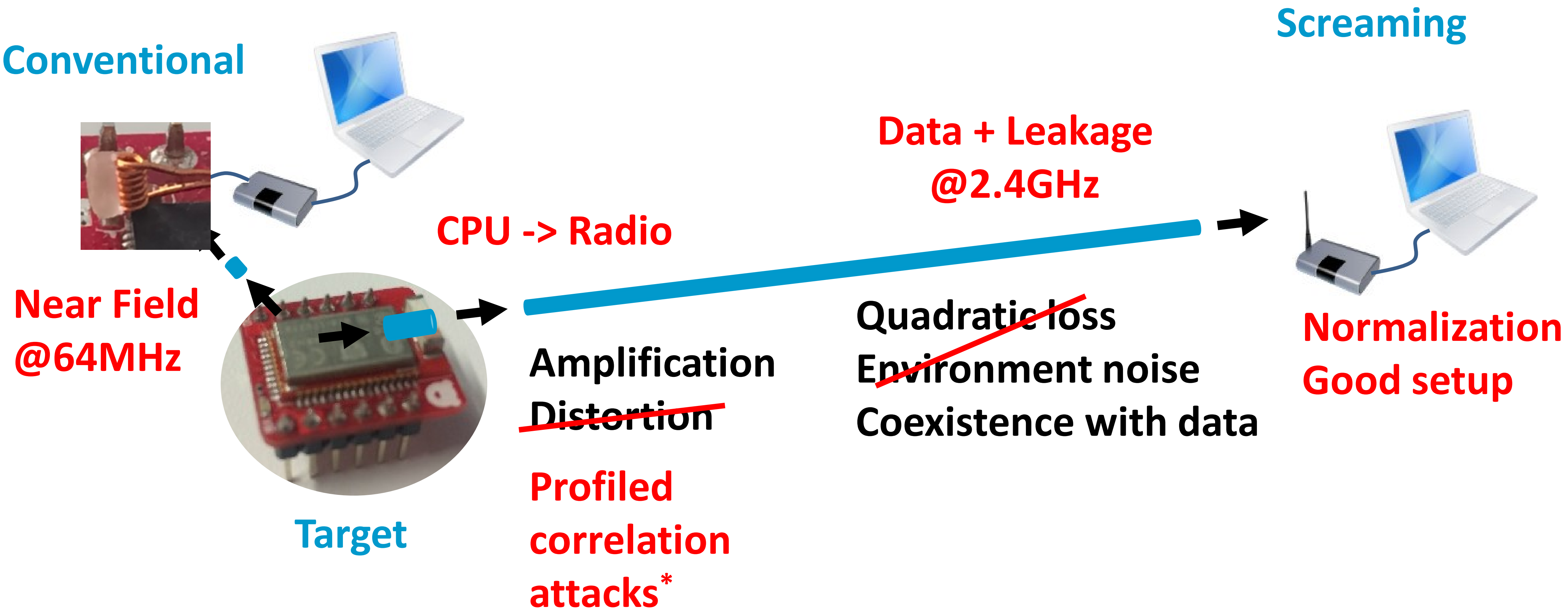


Detailed experimental study of a novel channel



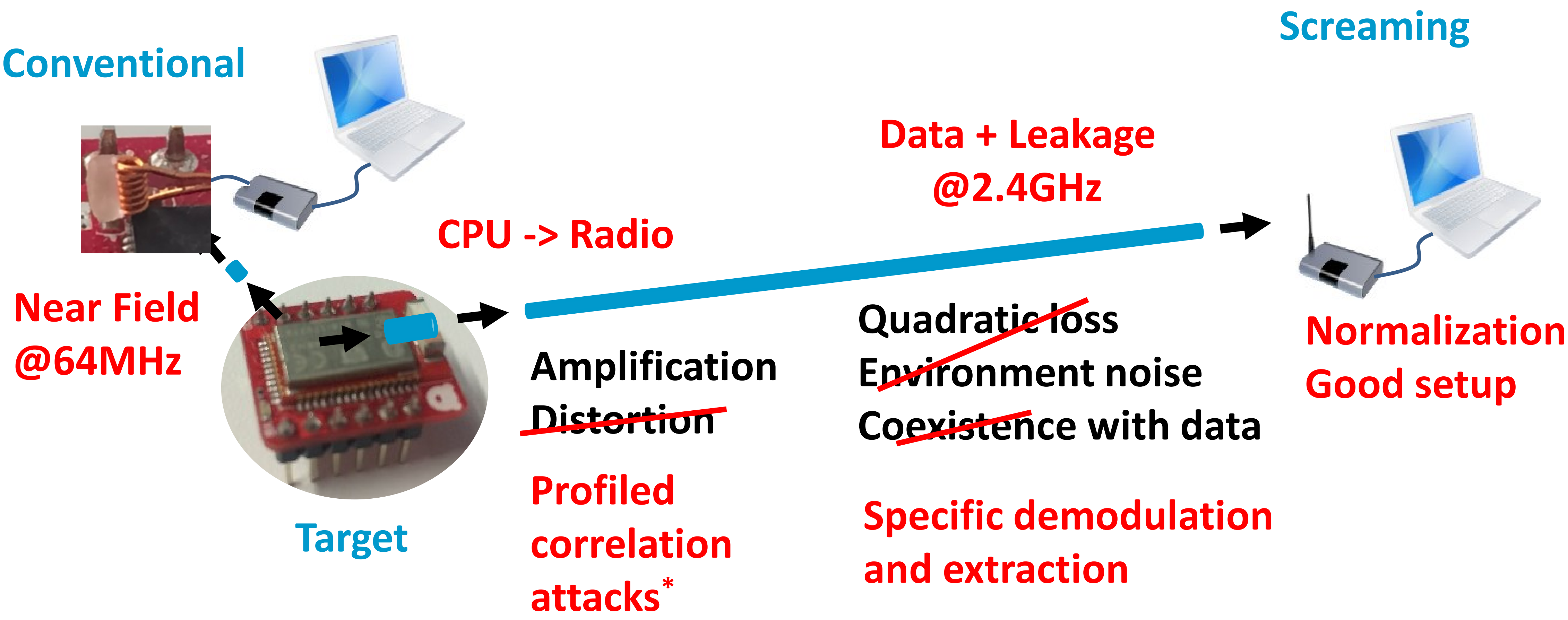
*F. Durvaux and F.-X. Standaert, “From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces,” in EUROCRYPT 2016.

Detailed experimental study of a novel channel



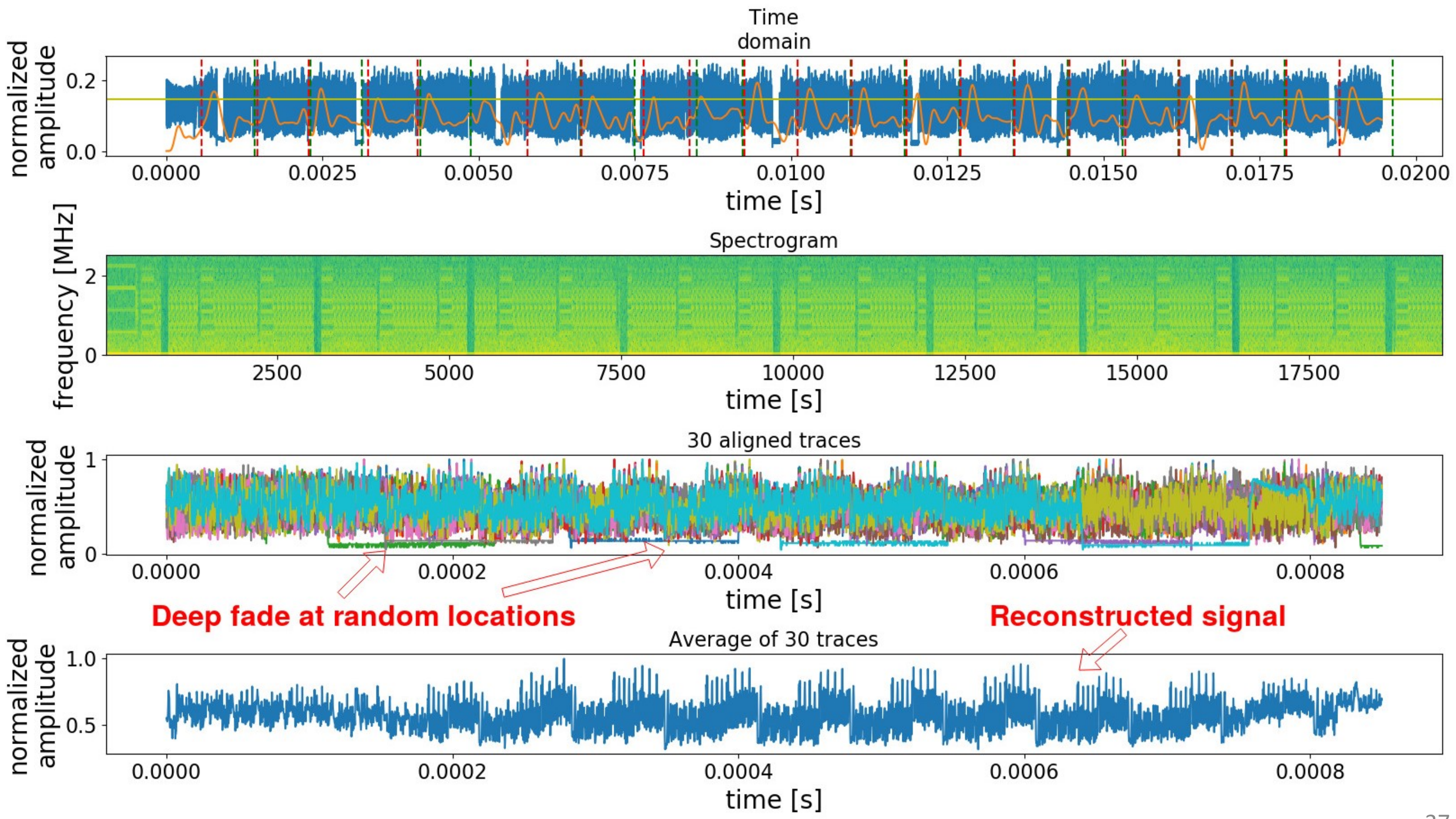
*F. Durvaux and F.-X. Standaert, “From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces,” in EUROCRYPT 2016.

Detailed experimental study of a novel channel



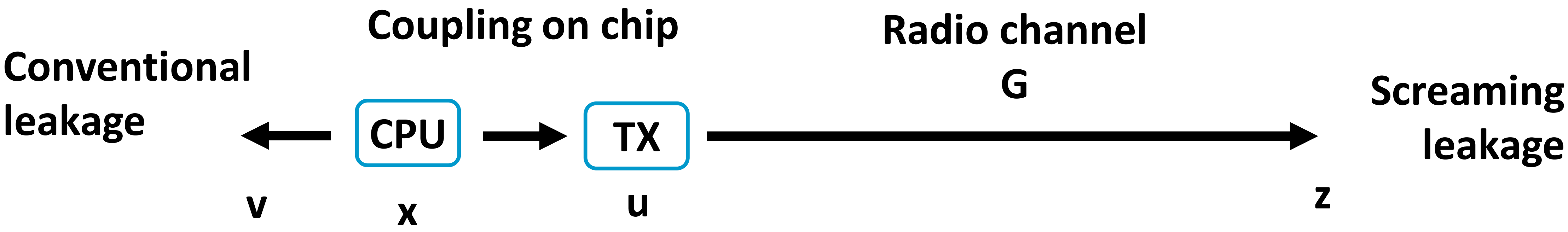
*F. Durvaux and F.-X. Standaert, "From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces," in EUROCRYPT 2016.

Example: data-leakage coexistence



EURECOM Sophia Antipolis

Example: distorted leakage model

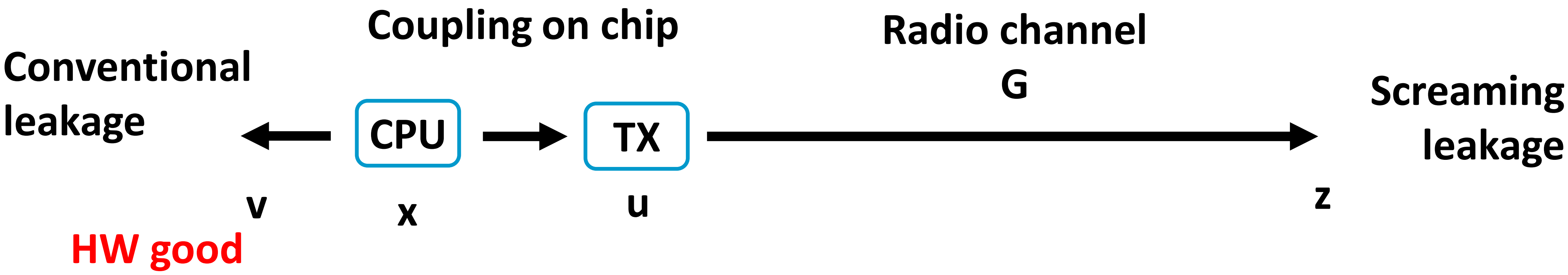


*F. Durvaux and F.-X. Standaert, “From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces,” in EUROCRYPT 2016.

**F.-X. Standaert et al., “An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays,” Proceedings of the IEEE 94, no. 2 (2006).

***W. Schindler, K. Lemke, and C. Paar, “A Stochastic Model for Differential Side Channel Cryptanalysis,” in CHES 2005.

Example: distorted leakage model

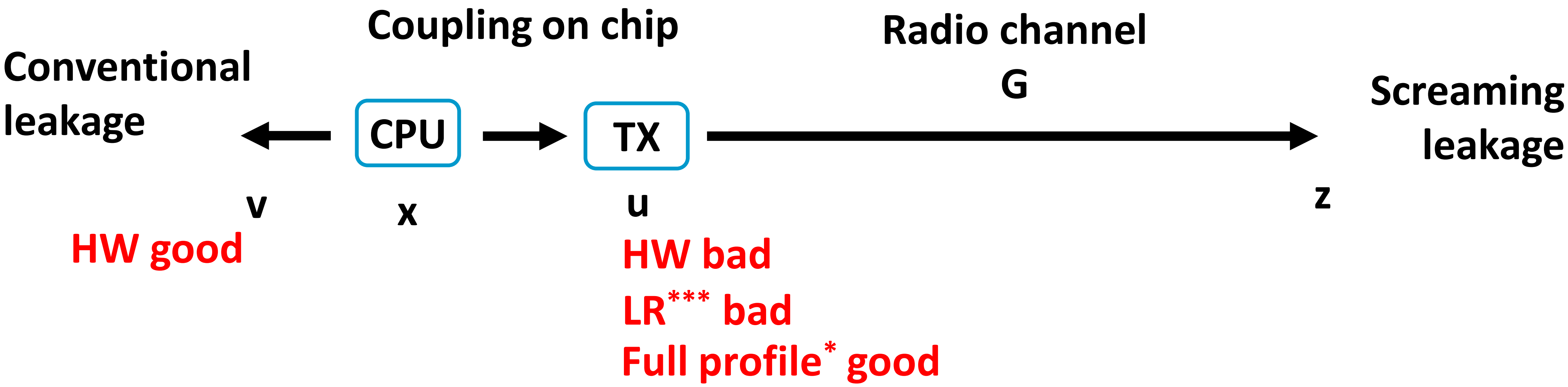


*F. Durvaux and F.-X. Standaert, “From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces,” in EUROCRYPT 2016.

**F.-X. Standaert et al., “An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays,” Proceedings of the IEEE 94, no. 2 (2006).

***W. Schindler, K. Lemke, and C. Paar, “A Stochastic Model for Differential Side Channel Cryptanalysis,” in CHES 2005.

Example: distorted leakage model

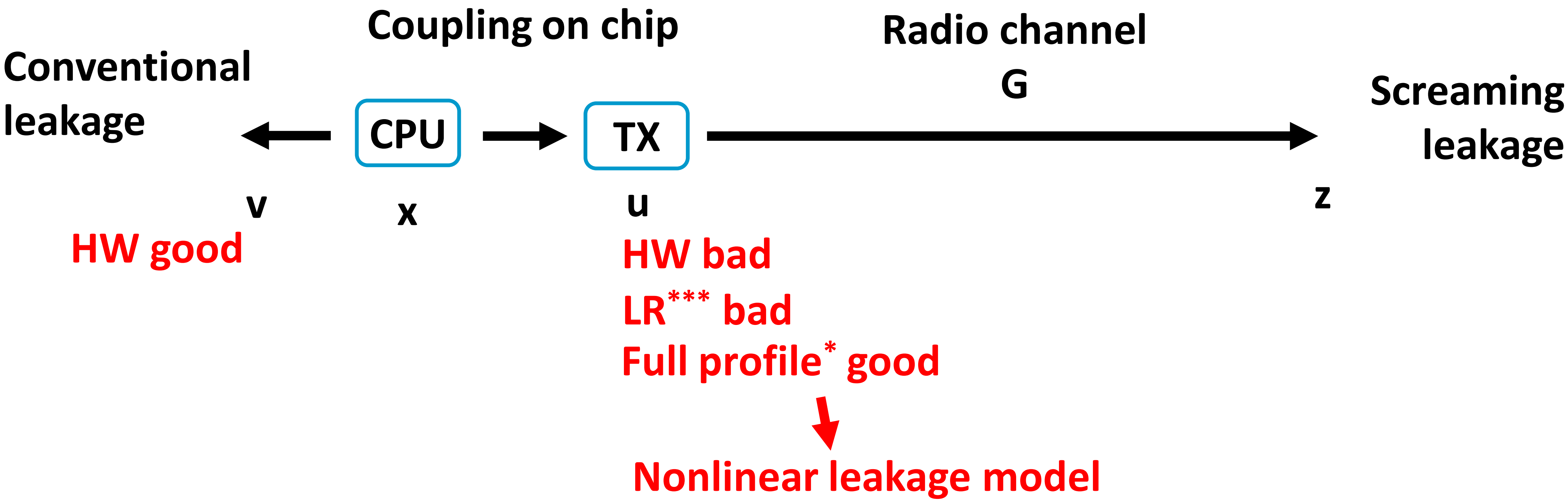


*F. Durvaux and F.-X. Standaert, "From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces," in EUROCRYPT 2016.

**F.-X. Standaert et al., "An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays," Proceedings of the IEEE 94, no. 2 (2006).

***W. Schindler, K. Lemke, and C. Paar, "A Stochastic Model for Differential Side Channel Cryptanalysis," in CHES 2005.

Example: distorted leakage model

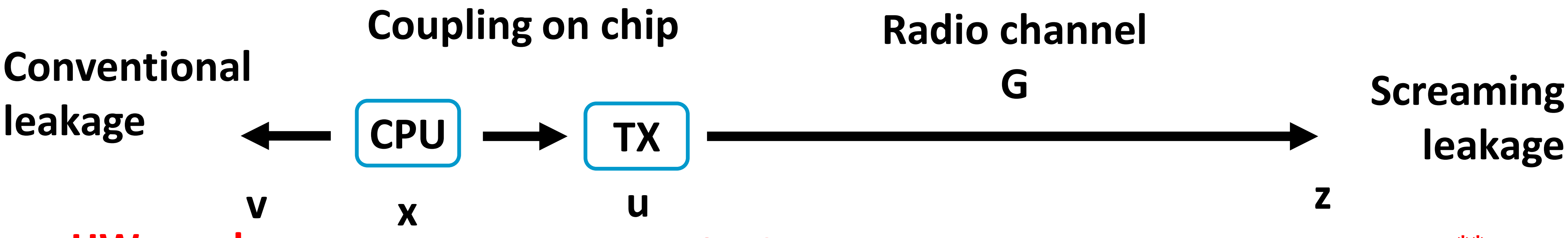


*F. Durvaux and F.-X. Standaert, "From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces," in EUROCRYPT 2016.

**F.-X. Standaert et al., "An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays," Proceedings of the IEEE 94, no. 2 (2006).

***W. Schindler, K. Lemke, and C. Paar, "A Stochastic Model for Differential Side Channel Cryptanalysis," in CHES 2005.

Example: distorted leakage model



HW good

HW bad

LR*** bad

Full profile* good

↓

Nonlinear leakage model

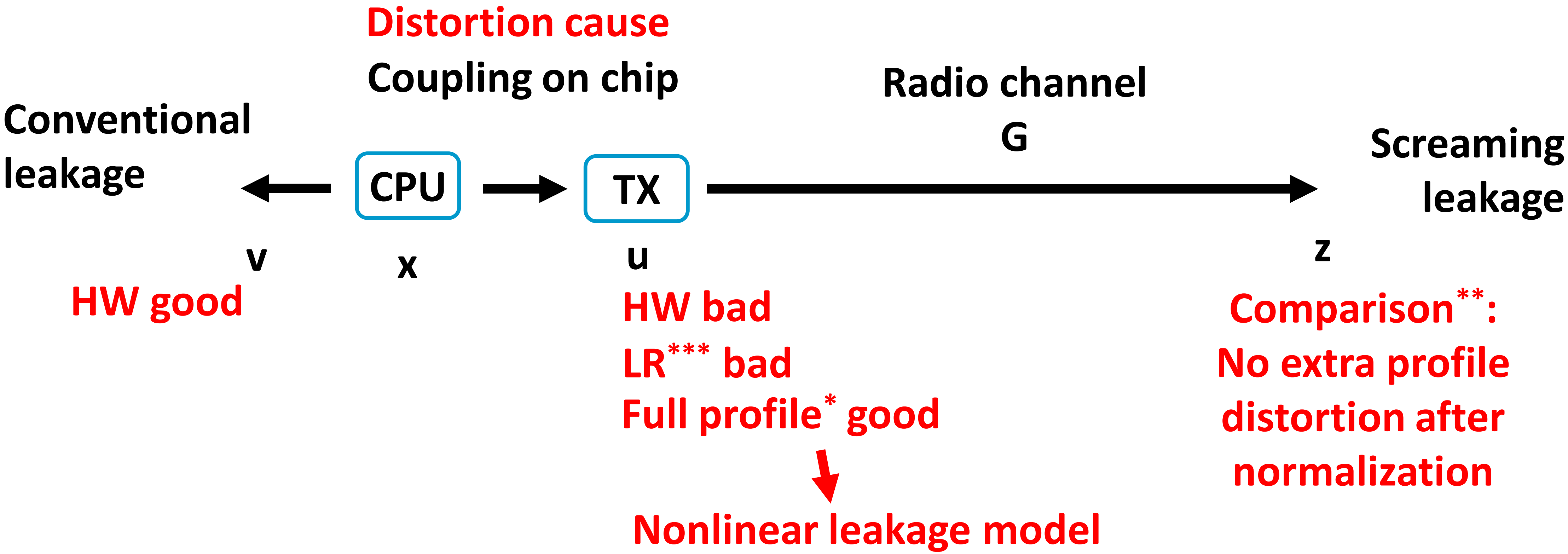
Comparison**:
No extra profile
distortion after
normalization

*F. Durvaux and F.-X. Standaert, “From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces,” in EUROCRYPT 2016.

**F.-X. Standaert et al., “An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays,” Proceedings of the IEEE 94, no. 2 (2006).

***W. Schindler, K. Lemke, and C. Paar, “A Stochastic Model for Differential Side Channel Cryptanalysis,” in CHES 2005.

Example: distorted leakage model



*F. Durvaux and F.-X. Standaert, “From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces,” in EUROCRYPT 2016.

**F.-X. Standaert et al., “An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays,” Proceedings of the IEEE 94, no. 2 (2006).

***W. Schindler, K. Lemke, and C. Paar, “A Stochastic Model for Differential Side Channel Cryptanalysis,” in CHES 2005.

Example: distorted leakage model

Distortion cause

Coupling on chip

Radio channel G

Conventional leakage

Screaming leakage

v x u z

HW good

HW bad

LR[***] bad

Full profile[*] good

→ **Nonlinear leakage model**

Comparison[**]: No extra profile distortion after normalization

Future work:
Why distorsion?
y = f(v)? Trace vs. signal?
Channel state? Memory effect?

*F. Durvaux and F.-X. Standaert, "From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces," in EUROCRYPT 2016.

**F.-X. Standaert et al., "An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays," Proceedings of the IEEE 94, no. 2 (2006).

***W. Schindler, K. Lemke, and C. Paar, "A Stochastic Model for Differential Side Channel Cryptanalysis," in CHES 2005.

Example: profile comparison with distance

	d (m)	environment	antenna	$\hat{r}(P_i,P_2)$, -log10(p)	$max \rho, r_z$
P_2	0.10	home	standard	1.00, inf	0.79, 75.72
P_3	0.20	home	standard	0.96, 142.77	0.77, 72.30
P_4	1.00	office	directional	0.40, 10.32	0.41, 30.66
P_5	5.00	anechoic	directional	0.96, 139.51	0.85, 89.84
P_6	10.00	anechoic	directional	0.92, 107.80	0.77, 71.71

High correlation between profiles

High correlation at each distance

What really matters are setup quality and environment noise

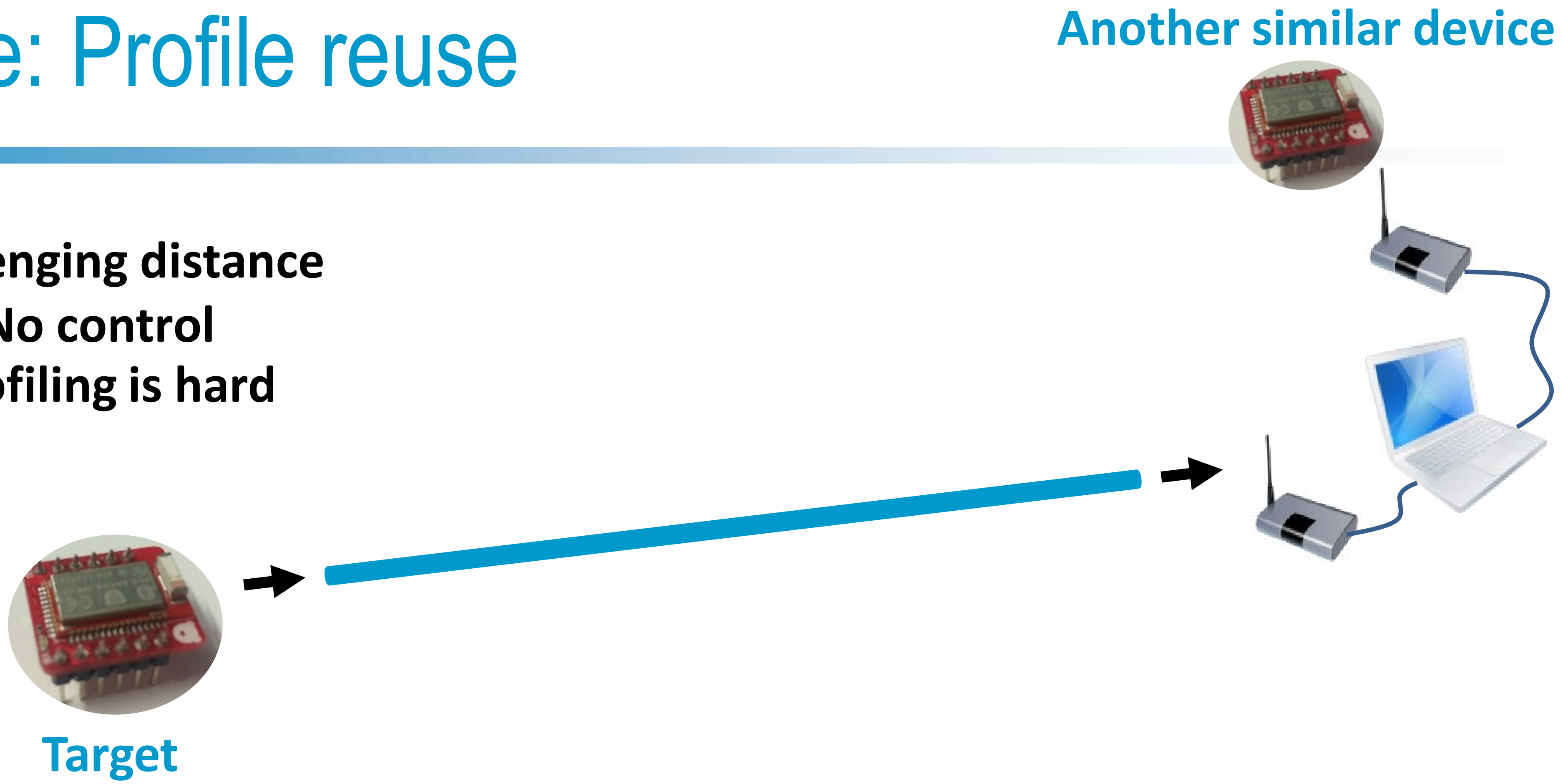
Example: Profile reuse

Challenging distance
No control
Profiling is hard

D. P. Montminy et al., “Improving Cross-Device Attacks Using Zero-Mean Unit-Variance Normalization,” J. Cryptographic Engineering 3, no. 2 (2013).
N. Hanley et al., “Empirical Evaluation of Multi-Device Profiling Side-Channel Attacks,” in IEEE SIPS 2014.
O. Choudary and M. G. Kuhn, “Template Attacks on Different Devices,”in COSADE 2014.
M. Abdelaziz Elaabid and S. Guilley, “Portability of Templates,” J. Cryptographic Engineering 2, no. 1 (2012).

Example: Profile reuse

Challenging distance
No control
Profiling is hard



D. P. Montminy et al., "Improving Cross-Device Attacks Using Zero-Mean Unit-Variance Normalization," J. Cryptographic Engineering 3, no. 2 (2013).
N. Hanley et al., "Empirical Evaluation of Multi-Device Profiling Side-Channel Attacks," in IEEE SIPS 2014.
O. Choudary and M. G. Kuhn, "Template Attacks on Different Devices,"in COSADE 2014.
M. Abdelaziz Elaabid and S. Guilley, "Portability of Templates," J. Cryptographic Engineering 2, no. 1 (2012).

Example: Profile reuse

Another similar device

Profile in favorable controlled conditions

Challenging distance

No control

~~**Profiling is hard**~~

Target

D. P. Montminy et al., “Improving Cross-Device Attacks Using Zero-Mean Unit-Variance Normalization,” J. Cryptographic Engineering 3, no. 2 (2013).
N. Hanley et al., “Empirical Evaluation of Multi-Device Profiling Side-Channel Attacks,” in IEEE SIPS 2014.
O. Choudary and M. G. Kuhn, “Template Attacks on Different Devices,”in COSADE 2014.
M. Abdelaziz Elaabid and S. Guilley, “Portability of Templates,” J. Cryptographic Engineering 2, no. 1 (2012).

Example: Profile reuse

Another similar device

Profile in favorable controlled conditions

Challenging distance

No control

~~**Profiling is hard**~~

The profile can be reused here

Target

D. P. Montminy et al., "Improving Cross-Device Attacks Using Zero-Mean Unit-Variance Normalization," J. Cryptographic Engineering 3, no. 2 (2013).

N. Hanley et al., "Empirical Evaluation of Multi-Device Profiling Side-Channel Attacks," in IEEE SIPS 2014.

O. Choudary and M. G. Kuhn, "Template Attacks on Different Devices,"in COSADE 2014.

M. Abdelaziz Elaabid and S. Guilley, "Portability of Templates," J. Cryptographic Engineering 2, no. 1 (2012).

EURECOM

Example: Profile reuse

Another similar device

Profile in favorable controlled conditions

Challenging distance

No control

~~**Profiling is hard**~~

The profile can be reused here

Target

<u>Per-trace</u> z-score normalization as channel estimation

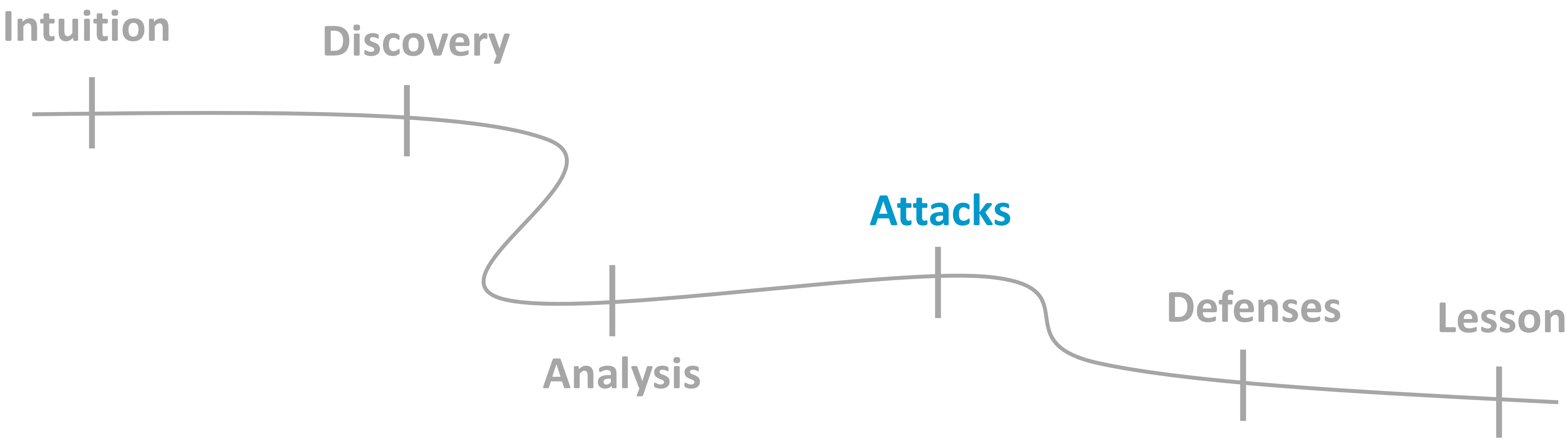
D. P. Montminy et al., "Improving Cross-Device Attacks Using Zero-Mean Unit-Variance Normalization," J. Cryptographic Engineering 3, no. 2 (2013).

N. Hanley et al., "Empirical Evaluation of Multi-Device Profiling Side-Channel Attacks," in IEEE SIPS 2014.

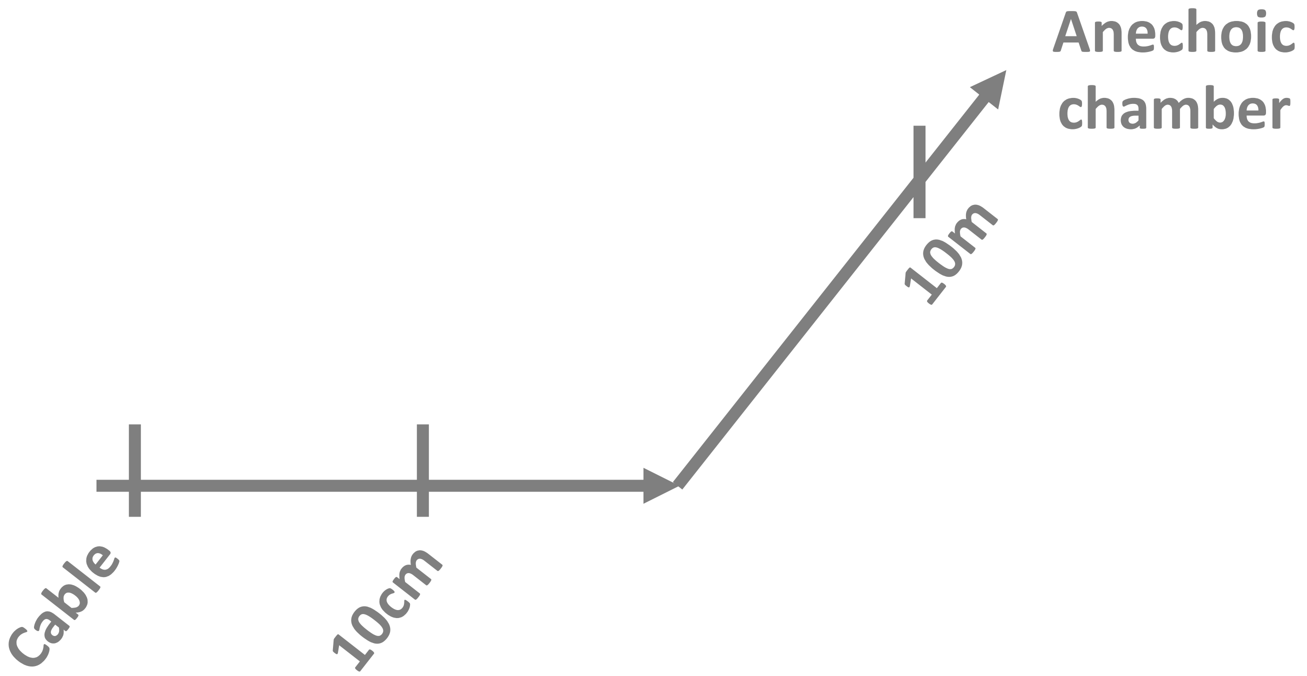
O. Choudary and M. G. Kuhn, "Template Attacks on Different Devices,"in COSADE 2014.

M. Abdelaziz Elaabid and S. Guilley, "Portability of Templates," J. Cryptographic Engineering 2, no. 1 (2012).

Studying a novel side channel



Attacks at large distance in realistic environments

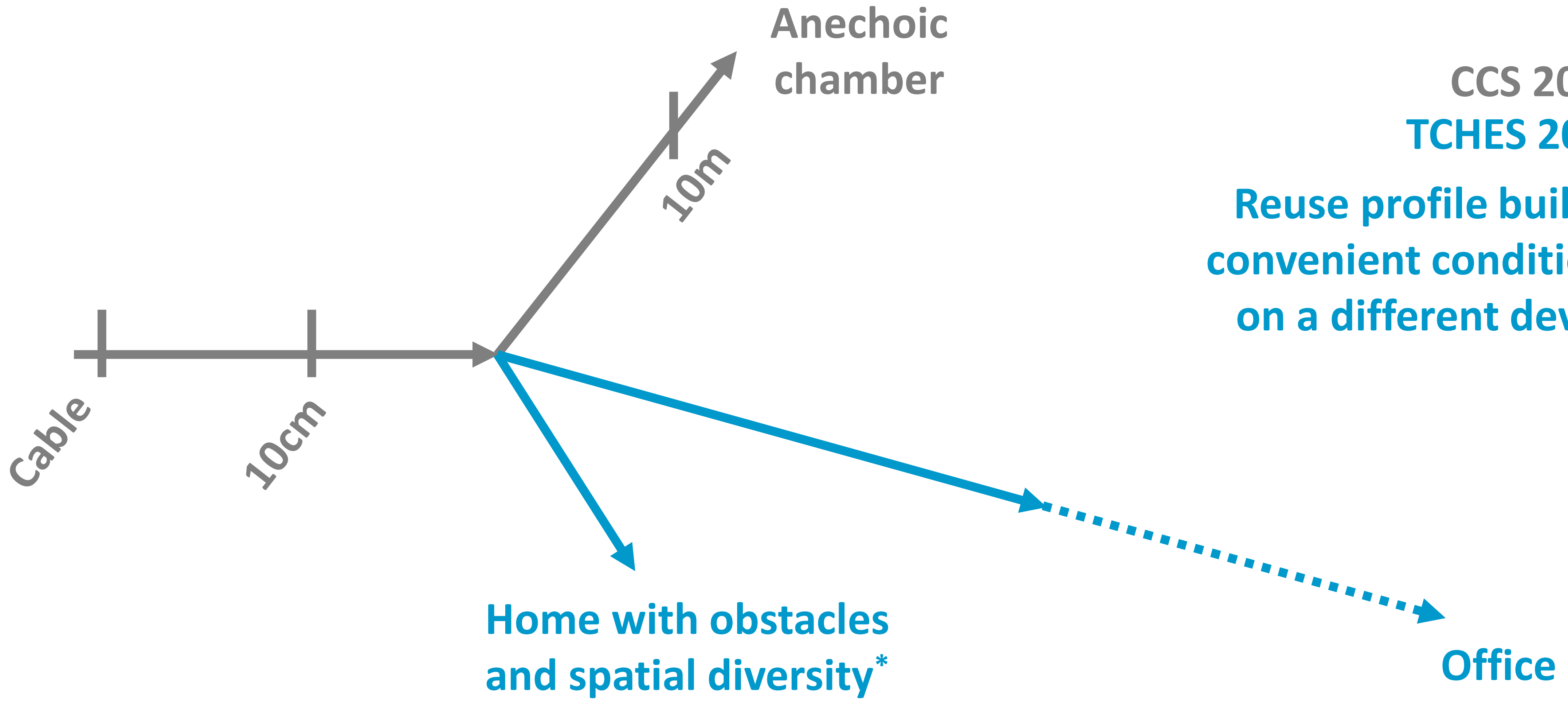


CCS 2018

*D. G. Brennan, “Linear Diversity Combining Techniques,” Proceedings of the IRE 47, no. 6 (1959).

EURECOM

Attacks at large distance in realistic environments



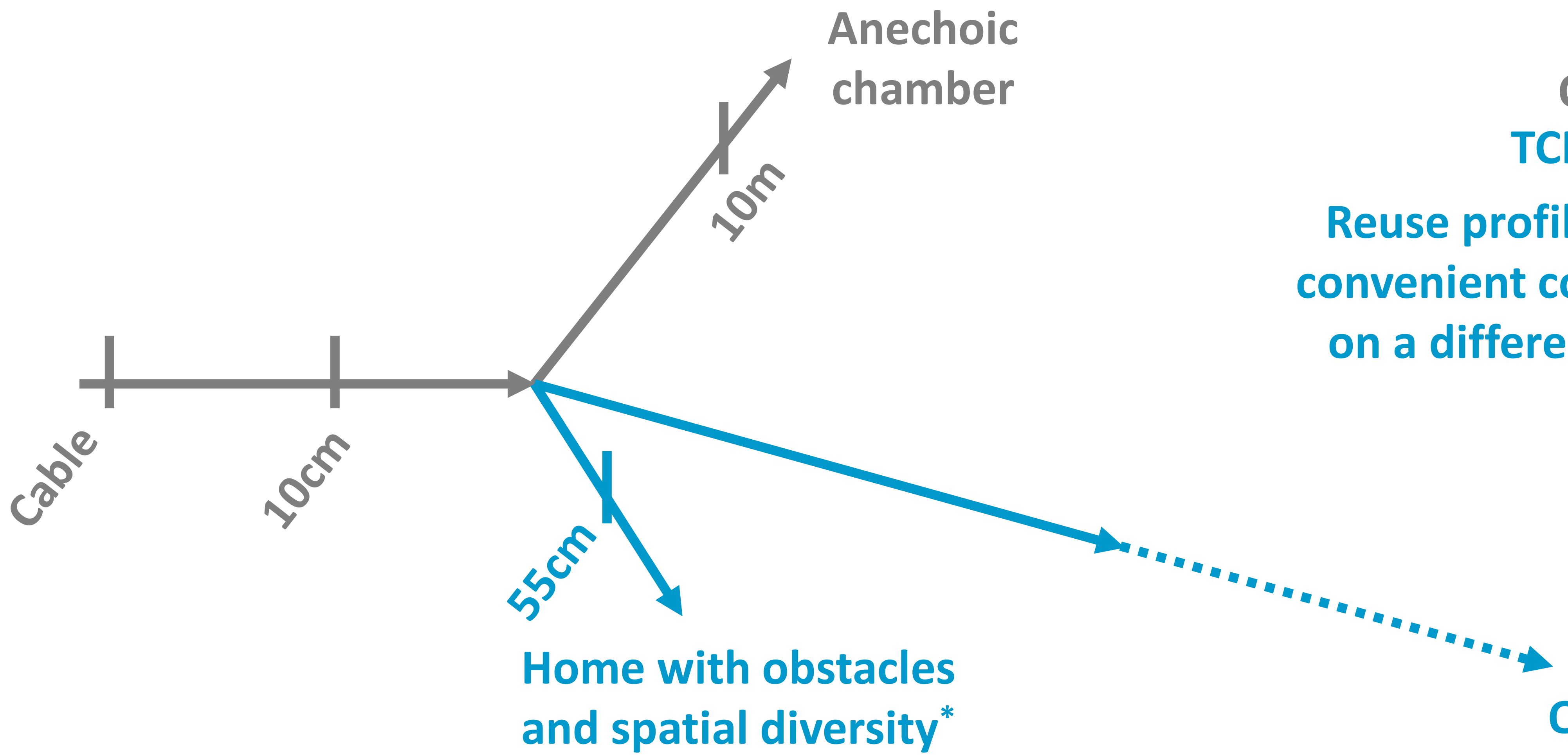
CCS 2018
TCHES 2020

Reuse profile built in convenient conditions on a different device

*D. G. Brennan, “Linear Diversity Combining Techniques,” Proceedings of the IRE 47, no. 6 (1959).

EURECOM

Attacks at large distance in realistic environments



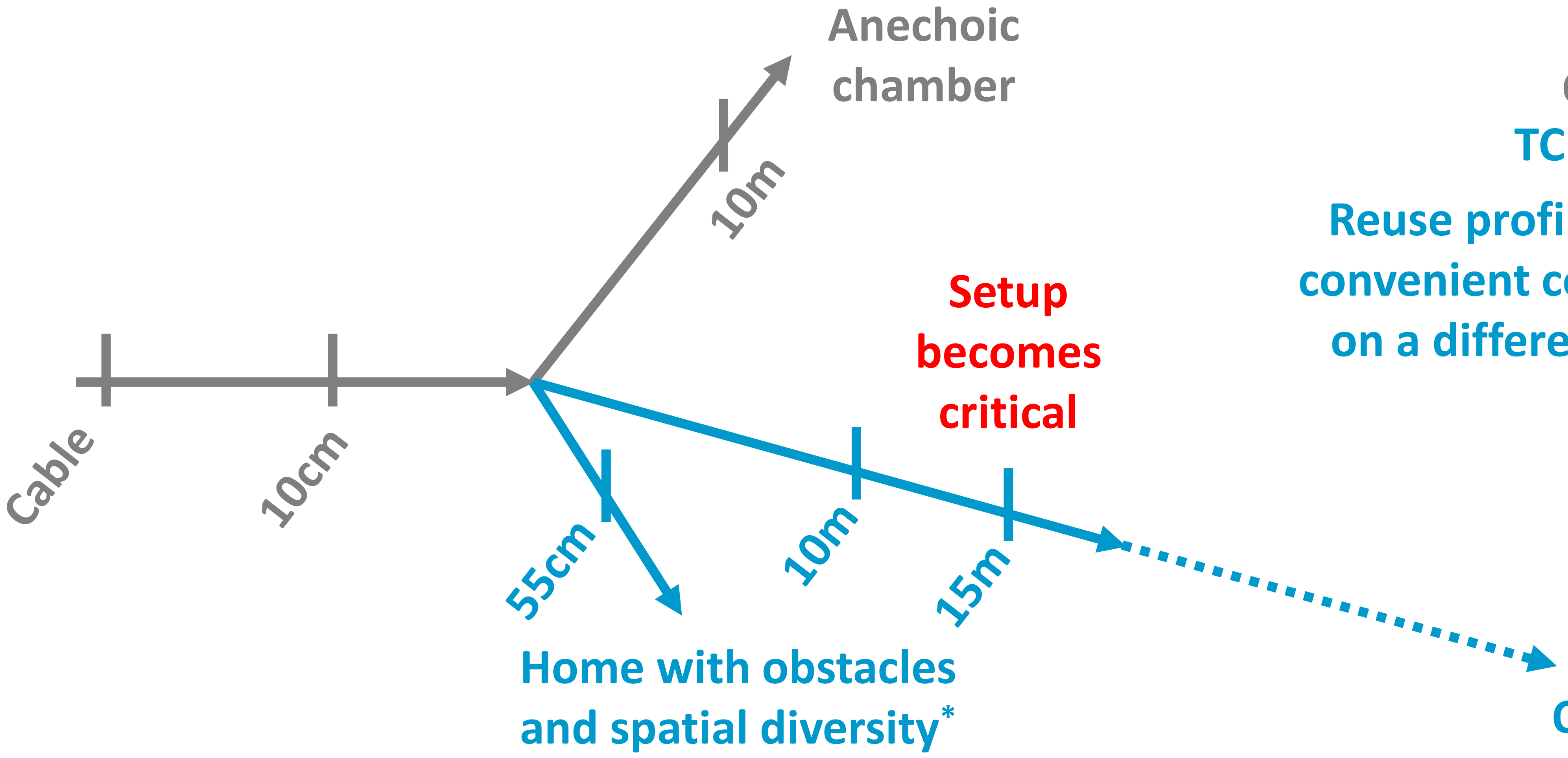
CCS 2018
TCHES 2020

Reuse profile built in convenient conditions on a different device

*D. G. Brennan, "Linear Diversity Combining Techniques," Proceedings of the IRE 47, no. 6 (1959).

EURECOM

Attacks at large distance in realistic environments



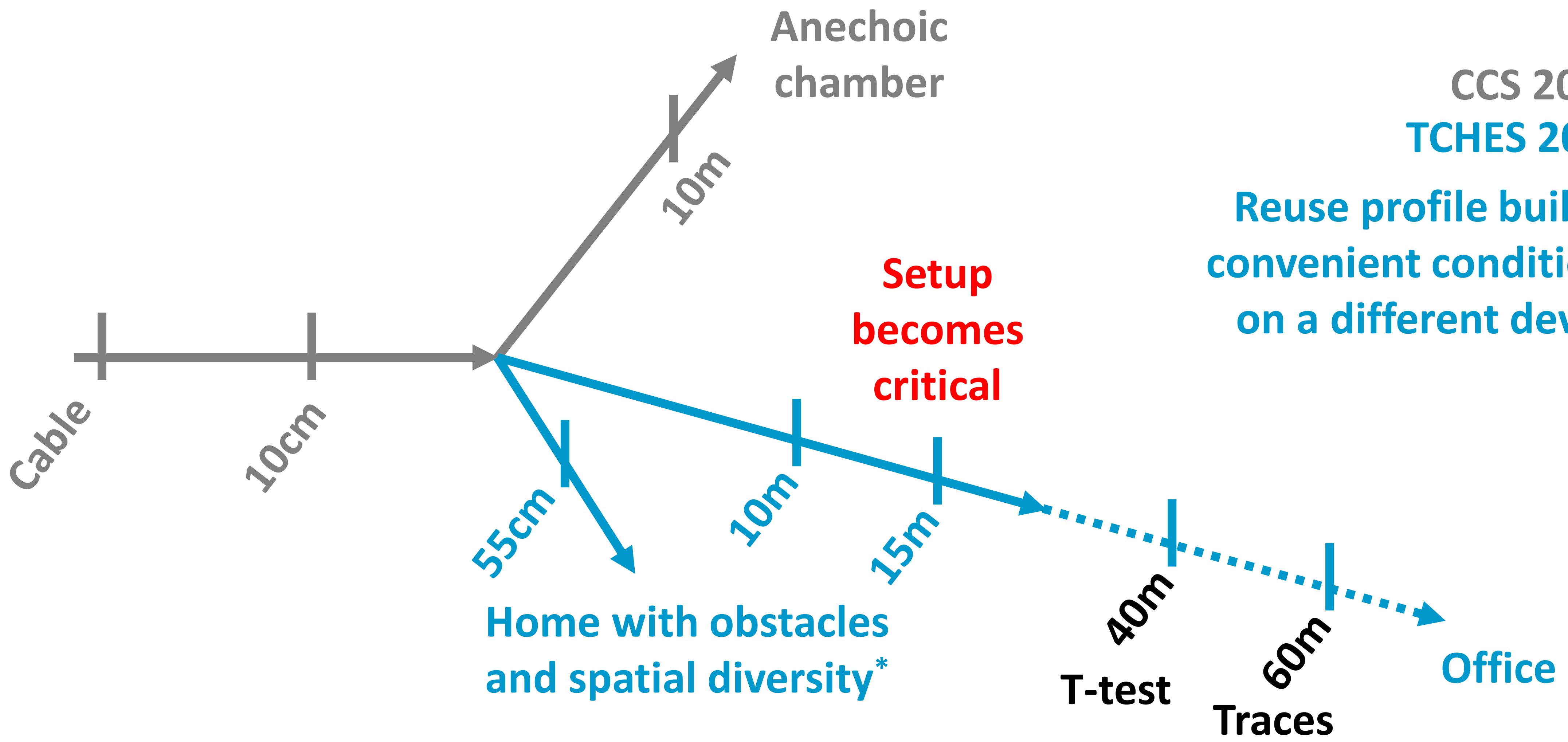
CCS 2018

TCHES 2020

Reuse profile built in convenient conditions on a different device

*D. G. Brennan, "Linear Diversity Combining Techniques," Proceedings of the IRE 47, no. 6 (1959).

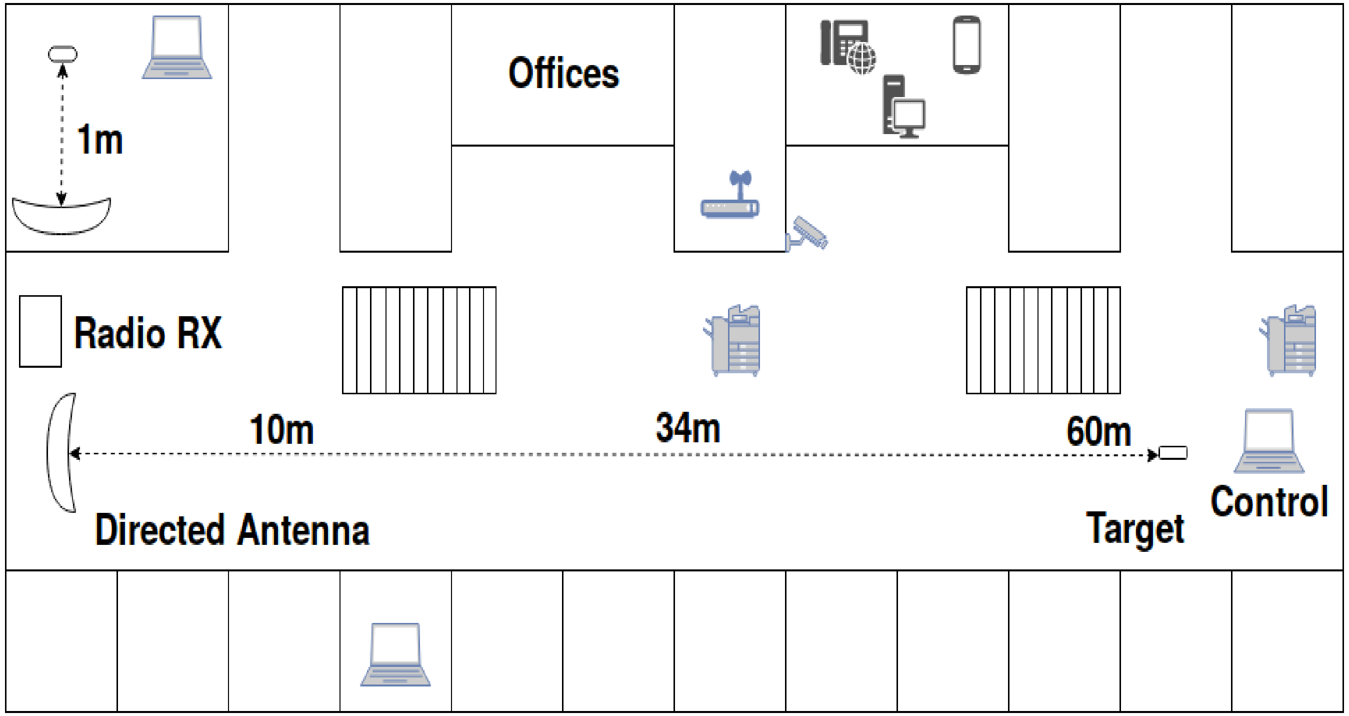
Attacks at large distance in realistic environments



CCS 2018
TCHES 2020

Reuse profile built in convenient conditions on a different device

*D. G. Brennan, "Linear Diversity Combining Techniques," Proceedings of the IRE 47, no. 6 (1959).



Simple Profiling

Connection via cable

(10k x 500 traces)

Complex Attack

Different instance and time

15m (5k x 1000 traces, 2^23, hard)

EURECOM

Attacking Google Eddystone Beacons authentication

Broadcast

URL, ID, Telemetry

Ephemeral, Encrypted

Configuration

Authentication

(GATT layer, pre-shared AES key)

Legitimate user

Legitimate owner

Security & privacy in mind during design

Google/Eddystone, C (2015; repr., Google, 2020), https://github.com/google/eddystone.

Attacking Google Eddystone Beacons authentication

Attacker

Broadcast

URL, ID, Telemetry

Ephemeral, Encrypted

Configuration

Authentication

(GATT layer, pre-shared AES key)

Legitimate user

Legitimate owner

Security & privacy in mind during design

Google/Eddystone, C (2015; repr., Google, 2020), https://github.com/google/eddystone.

Attacking Google Eddystone Beacons authentication

1. Minimize hopping

Attacker

Broadcast

URL, ID, Telemetry

Ephemeral, Encrypted

Legitimate user

Configuration

Authentication

(GATT layer, pre-shared AES key)

Legitimate owner

Security & privacy in mind during design

Google/Eddystone, C (2015; repr., Google, 2020), https://github.com/google/eddystone.

Attacking Google Eddystone Beacons authentication

1. Minimize hopping
2. Trigger encryption with known plaintext

Attacker

Broadcast

URL, ID, Telemetry

Ephemeral, Encrypted

Legitimate user

Configuration

Authentication

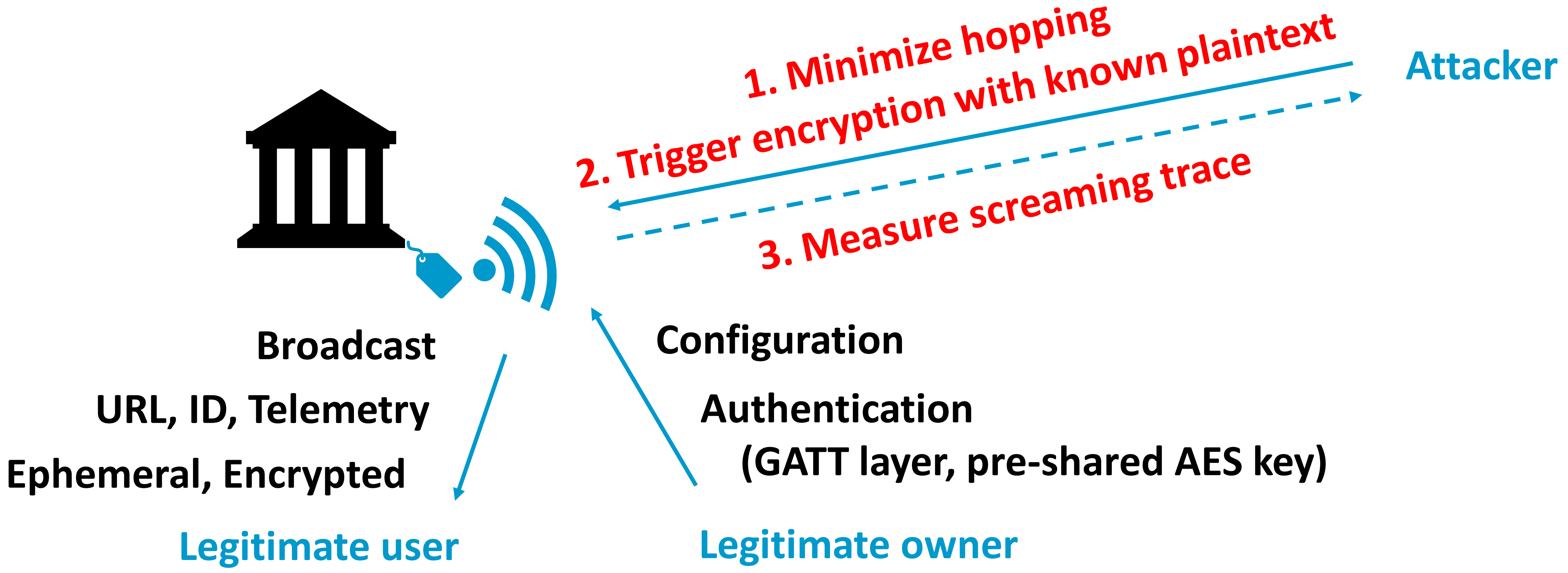
(GATT layer, pre-shared AES key)

Legitimate owner

Security & privacy in mind during design

Google/Eddystone, C (2015; repr., Google, 2020), https://github.com/google/eddystone.

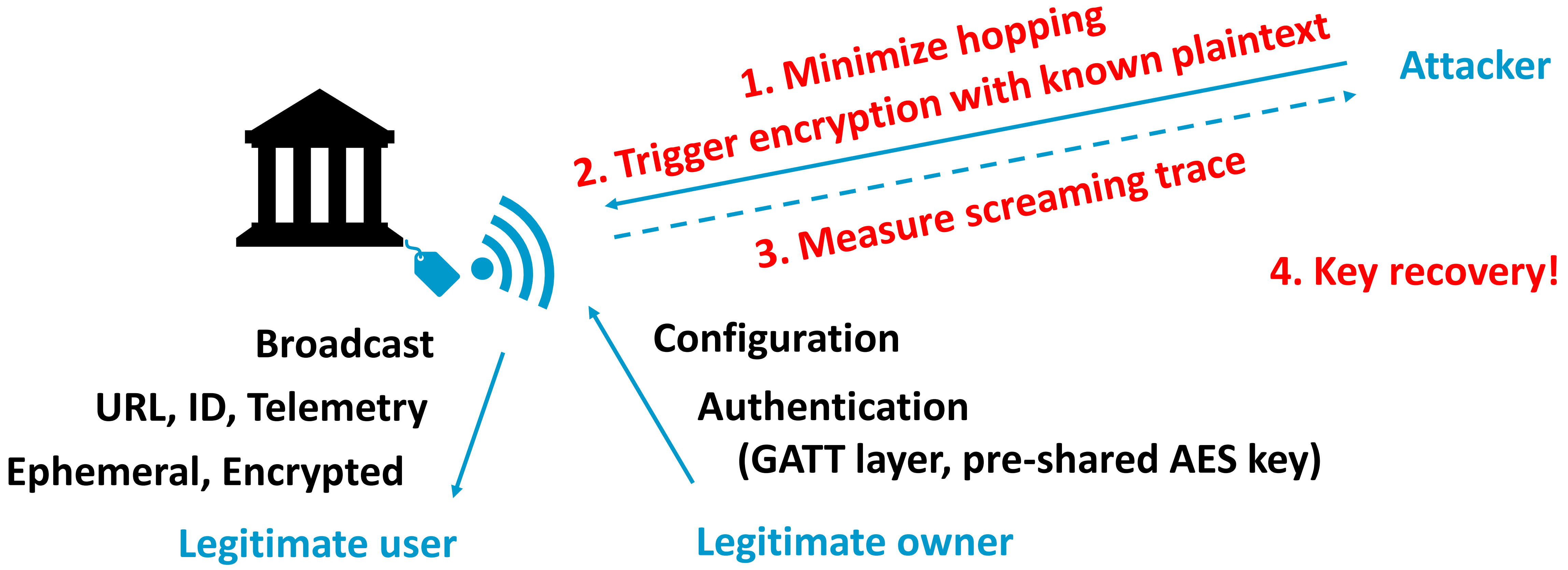
Attacking Google Eddystone Beacons authentication



Security & privacy in mind during design

Google/Eddystone, C (2015; repr., Google, 2020), https://github.com/google/eddystone.

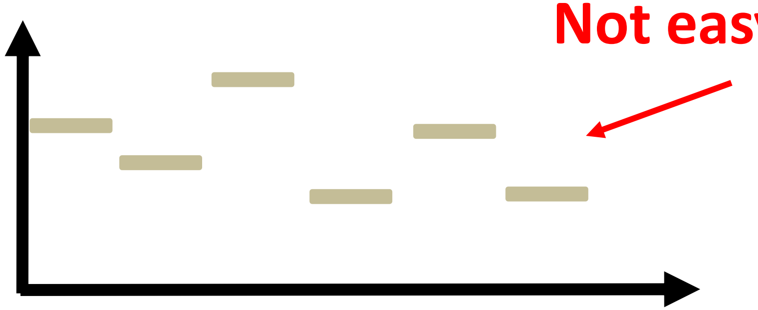
Attacking Google Eddystone Beacons authentication



Security & privacy in mind during design

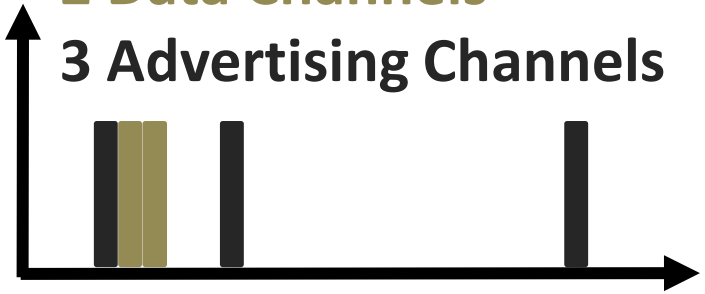
Google/Eddystone, C (2015; repr., Google, 2020), https://github.com/google/eddystone.

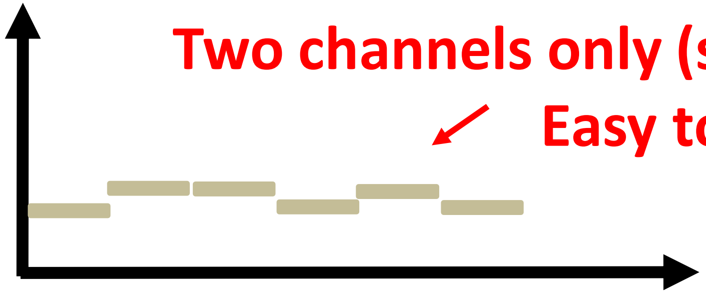
Minimizing the problem of frequency hopping



EURECOM

Minimizing the problem of frequency hopping

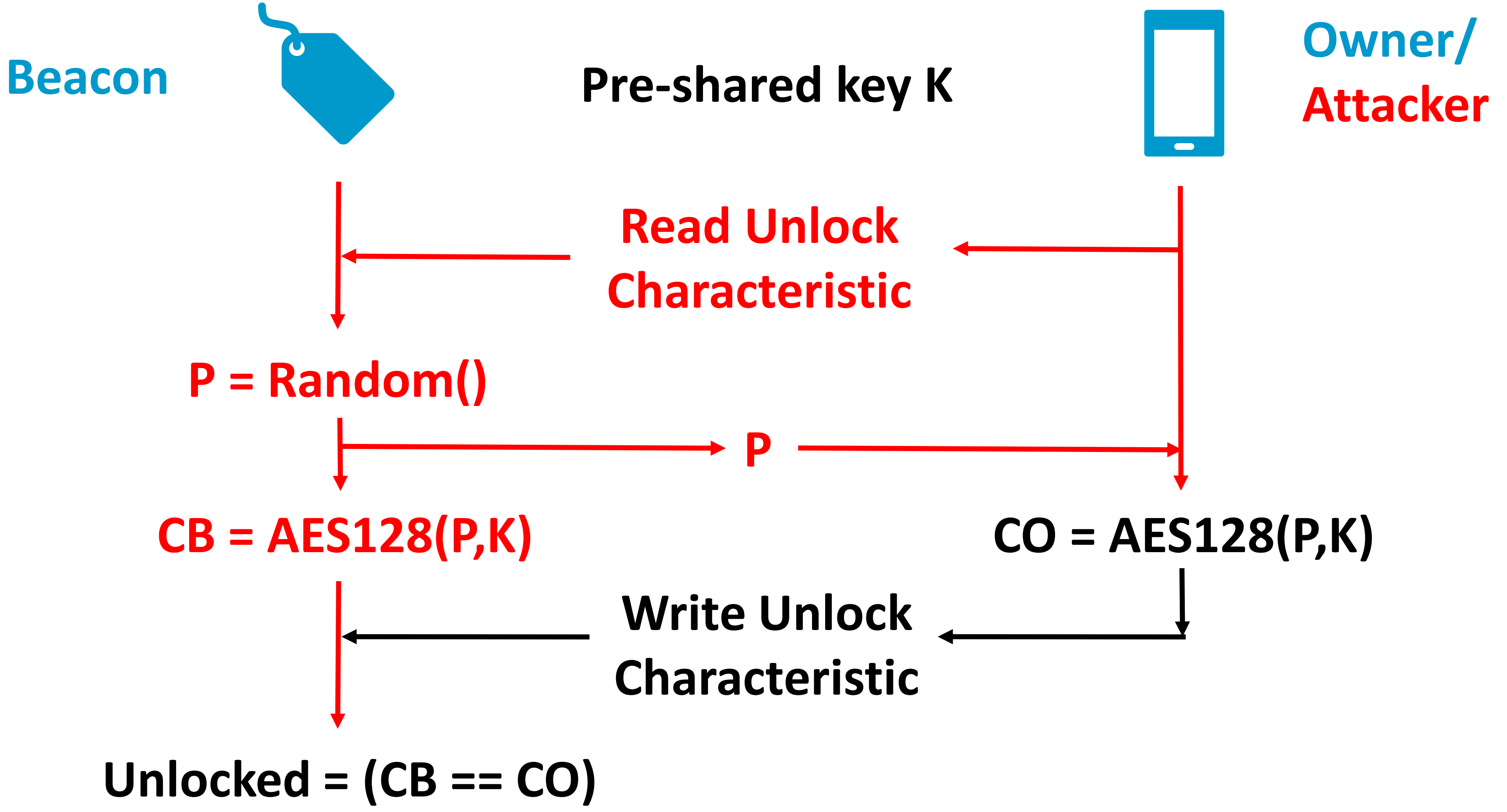




*Bluetooth SIG, Bluetooth 5.0 Core Specification, 2016.

EURECOM

Triggering AES encryptions with known plaintext



Proof-of-concept attack

Google Bughunter Program
Honorable Mention

Realistic Demo

Unmodified Nordic SDK demo*

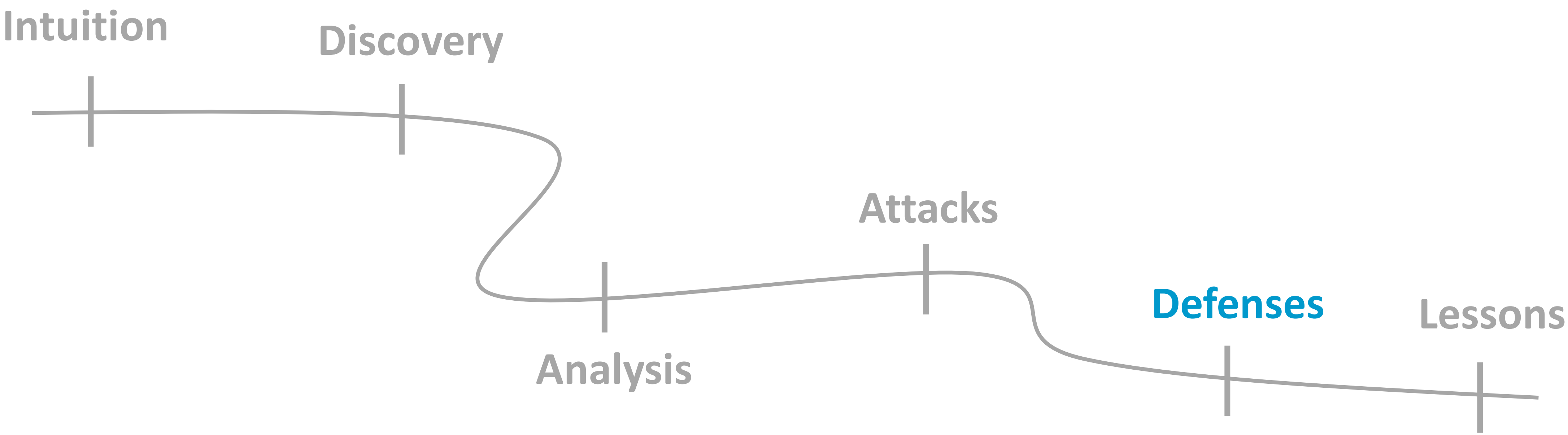
- **Optimized code (O3)**
- **Hopping Enabled (reduced with channel map)**
- **TinyAES software (hardware in later versions)**

Proof-of-Concept Attack (connection via cable on PCA10040)

70k x 1 profiling traces, 33k x 1 attack traces, rank 2^30

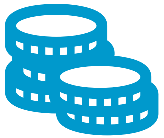
*https://developer.nordicsemi.com/nRF5_SDK/nRF5_SDK_v14.x.x/nRF5_SDK_14.2.0_17b948a.zip

Studying a novel side channel



EURECOM
Sophia Antipolis

Countermeasures



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

Countermeasures

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

Classic HW/SW:
Masking, noise, key refresh, limit attempts, ...

Countermeasures

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

Classic HW/SW:
Masking, noise, key refresh, limit attempts, ...

Specific (SW):
Radio off during sensitive computations
Force use of HW encryption (for now)

Countermeasures

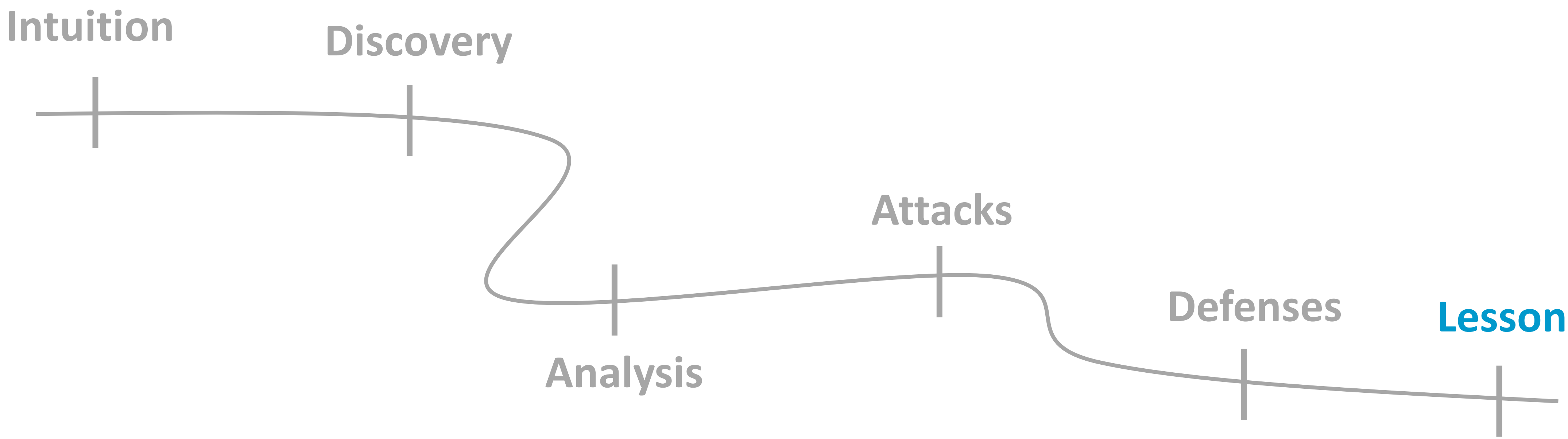
Resource constraint devices:
Cost, power, time to market, etc.

Classic HW/SW:
Masking, noise, key refresh, limit attempts, ...

Specific (SW):
Radio off during sensitive computations
Force use of HW encryption (for now)

Specific (HW):
Consider impact of coupling on security during design and test

Studying a novel side channel



EURECOM

Lessons learned

General Problem: Radios and Side Channels
New threat point: Digital activity visible from a large distance

Lessons learned

General Problem: Radios and Side Channels
New threat point: Digital activity visible from a large distance

Distinctive: Not a conventional side channel vector
Easier: Amplified leak, large distance, simple and cheap setup
Harder: Distortion, channel noise, data/leak coexistence

Lessons learned

General Problem: Radios and Side Channels
New threat point: Digital activity visible from a large distance

Distinctive: Not a conventional side channel vector
Easier: Amplified leak, large distance, simple and cheap setup
Harder: Distortion, channel noise, data/leak coexistence

Threat: More and more realistic attacks
Potential threat: More devices or new devices are vulnerable
Countermeasures: Clever, specific countermeasures

Lessons learned

General Problem: Radios and Side Channels
New threat point: Digital activity visible from a large distance

Distinctive: Not a conventional side channel vector
Easier: Amplified leak, large distance, simple and cheap setup
Harder: Distortion, channel noise, data/leak coexistence

Threat: More and more realistic attacks
Potential threat: More devices or new devices are vulnerable
Countermeasures: Clever, specific countermeasures

WiFi? Preliminary results
Hardware AES? Preliminary results

Side note: modulation of an intended signal

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.]

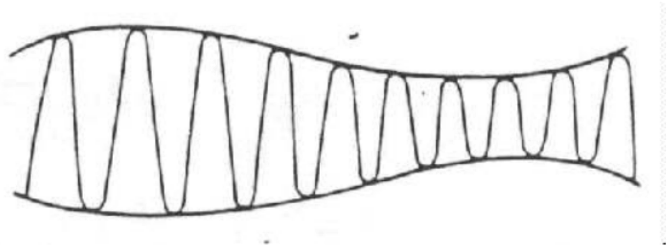


Figure 1-5. - Amplitude-Modulated Carrier (U) (U)

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.

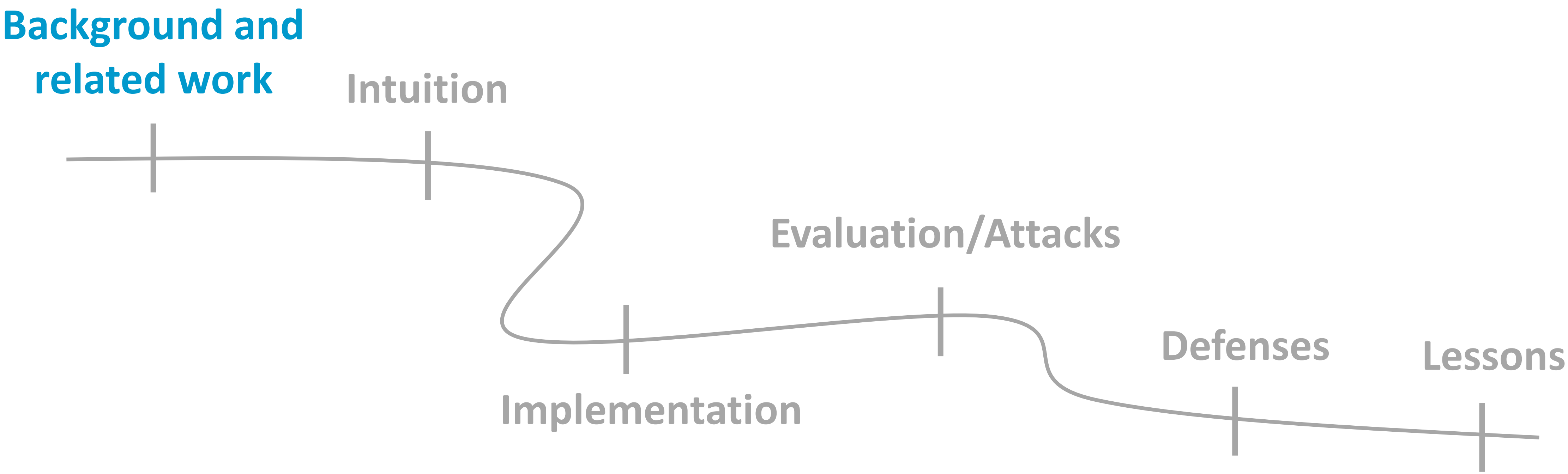
Propagation of leaks:

1. **Radiation**
2. **Conduction**
3. **Modulation of an intended signal (redacted)**
4. **Acoustic**

NSA, "NACSIM 5000, Tempest Fundamentals," 1982. Declassified in 2000

- Context
- Challenges & Contributions
- Screaming Channels
- Noise-SDR
- Future Work
- Conclusion

Achieving arbitrary noise modulation



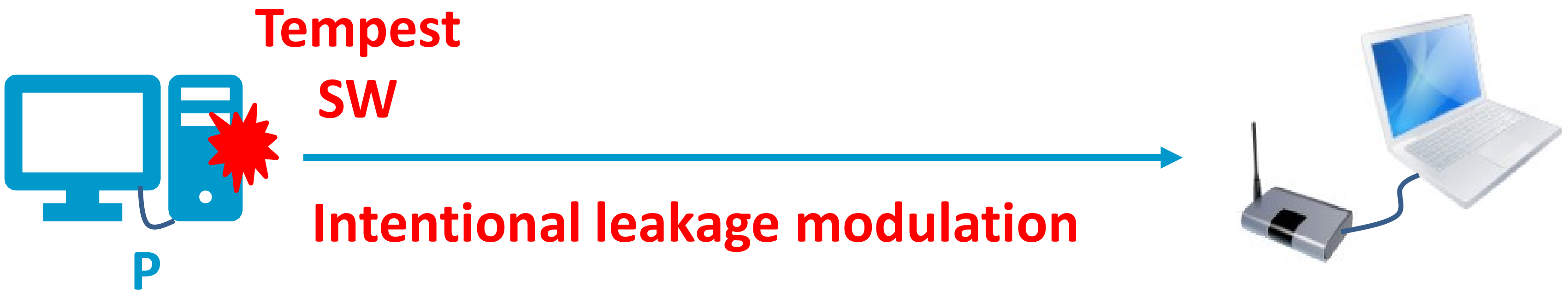
EURECOM

Background and related work

The idea
1998, Kuhn et. al
Soft-TEMPEST

+

Vast literature on air-gap exfiltration
Many physical methods
Generally simple modulation
Generally for air-gap exfiltration



M. G. Kuhn and R. J. Anderson, "Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations," in Information Hiding (1998).
B. Carrara and C. Adams, "Out-of-Band Covert Channels—A Survey," ACM Comput. Surv. 49, no. 2 (2016).

The primitive (generalized, simplified)

```
start = now()
while( now() – start < T/2 )
        doSomething()
while( now() – start < T )
        doNothing()
```


EURECOM
Sophia Antipolis

The primitive (generalized, simplified)

```
start = now()
while( now() – start < T/2 )
        doSomething()
while( now() – start < T )
        doNothing()
```

Trigger leakage @$F_{leakage}$ from SW
E.g., with memory accesses*

*M. Guri et al., "GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies," in USENIX Security 2015.
*Z. Zhan, Z. Zhang, and X. Koutsoukos, "BitJabber: The World's Fastest Electromagnetic Covert Channel," in IEEE ITC 2010

EURECOM

The primitive (generalized, simplified)

“Square wave”@f=1/T
E.g., sys-bus-radio**

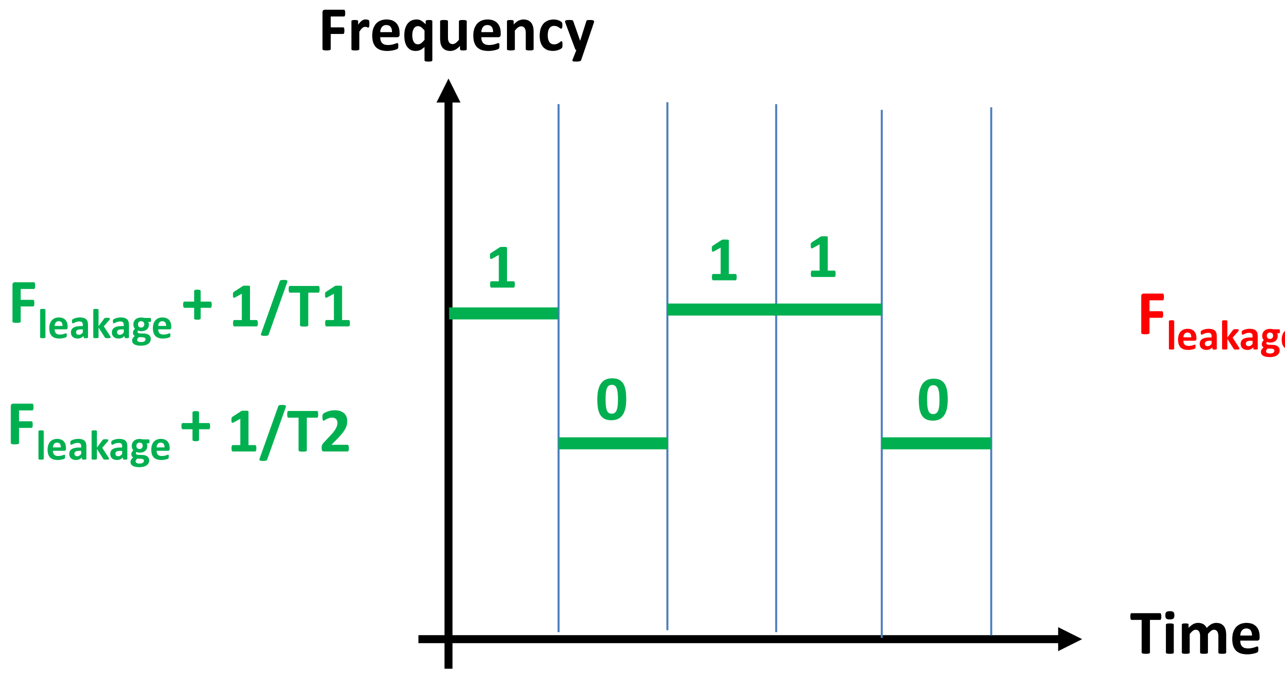
```
start = now()
while( now() – start < T/2 )
    doSomething()
while( now() – start < T )
    doNothing()
```

Trigger leakage @$F_{leakage}$ from SW
E.g., with memory accesses*

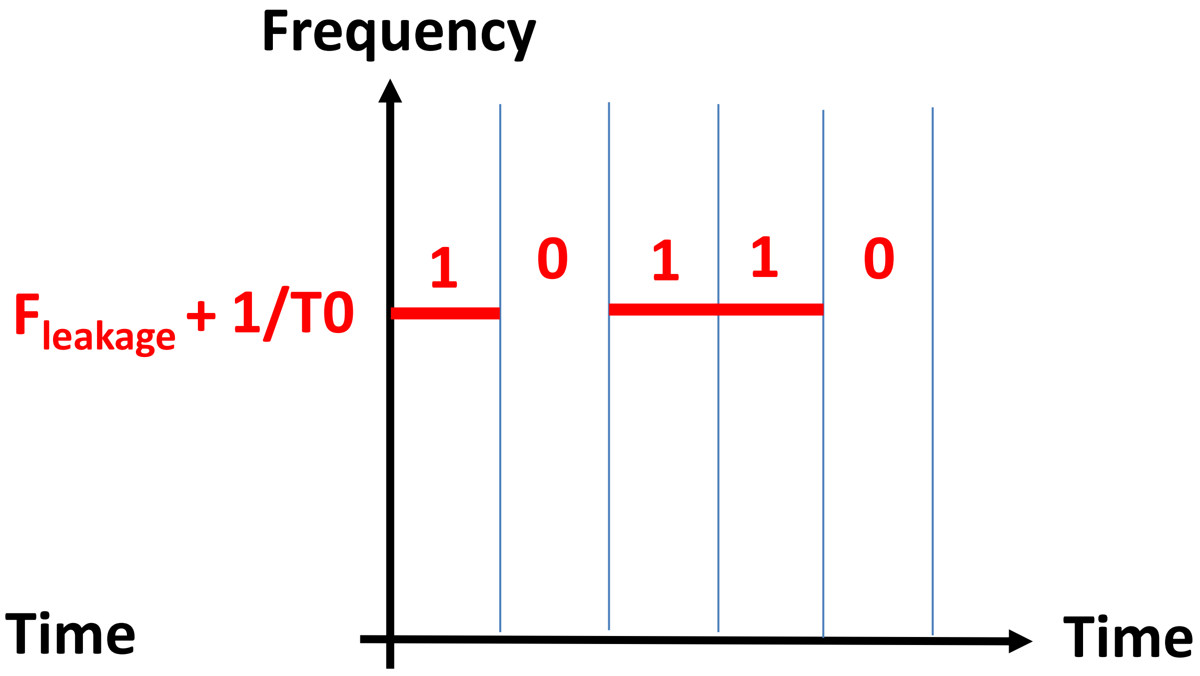
*M. Guri et al., “GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies,” in USENIX Security 2015.
*Z. Zhan, Z. Zhang, and X. Koutsoukos, “BitJabber: The World’s Fastest Electromagnetic Covert Channel,” in IEEE ITC 2010

**C. Shen et al., “When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient”, IEEE S&P 2021
**W. Entriken, System Bus Radio, 2013, https://github.com/fulldecent/system-bus-radio.

In general, simple custom modulation and protocol



2-FSK (or M-FSK)



OOK

EURECOM
Sophia Antipolis

Related work (EM)

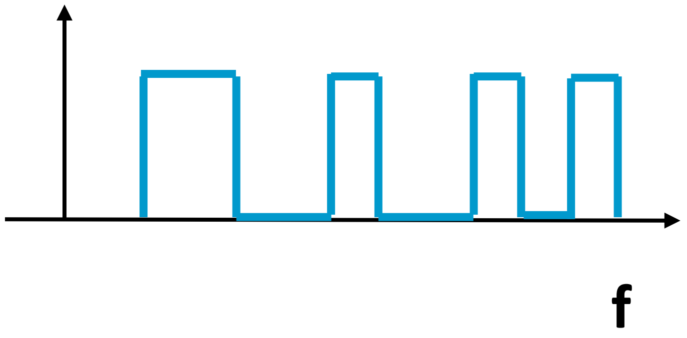
Simple custom modulation/protocol

Name	Leakage Type	Modulation Type	Publication Venue
Soft-TEMPEST	Electromagnetic	AM, FSK	Information Hiding 1998
AirHopper	Elecromagnetic	FSK	MALWARE 2014
USBee	Elecromagnetic	FSK	PST 2016
GSMem	Elecromagnetic	OOK	USENIX Security 2015
BitJabber	Elecromagnetic	OOK, FSK	IEEE ITC 2020
MAGNETO	Magnetic	OOK, FSK	ArXiv 2018
ODINI	Magnetic	OOK-(many cores), FSK	IEEE Trans. Inf. Forensics Secur. 2020
Matyunin et. al	Magnetic	OOK, FSK	ASP-DAC 2016

Background: 1-bit coding (e.g., PWM)

Fundamental frequency f_0
Generic pulse width and phase

$$squarewave(t) =$$

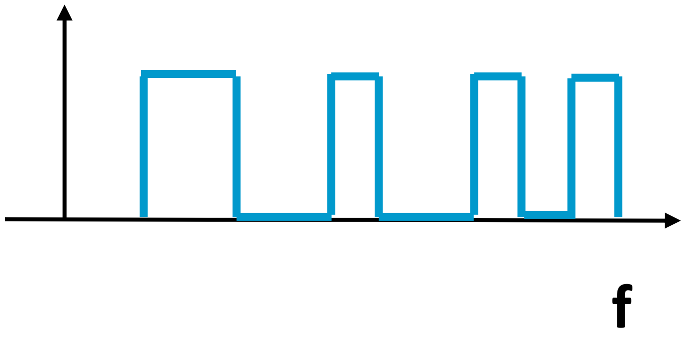


P. AJ Nuyts, P. Reynaert, and W. Dehaene, “Continuous-Time Digital Front-Ends for Multistandard Wireless Transmission” (Springer, 2014).

Background: 1-bit coding (e.g., PWM)

Fundamental frequency f_0
Generic pulse width and phase

$$squarewave(t) = \begin{cases} \delta(t) = \dfrac{T_{\text{high}}}{T_0} \\ \dfrac{2}{\pi}\sin\big(\pi\delta(t)\big)\cos(2\pi f_0 t + \theta(t)) \\ \displaystyle\sum_{k=1}^{k=+\infty} \dfrac{2}{k\pi}\sin\big(k\pi\delta(t)\big)\cos(2k\pi f_0 t + k\theta(t)) \end{cases}$$



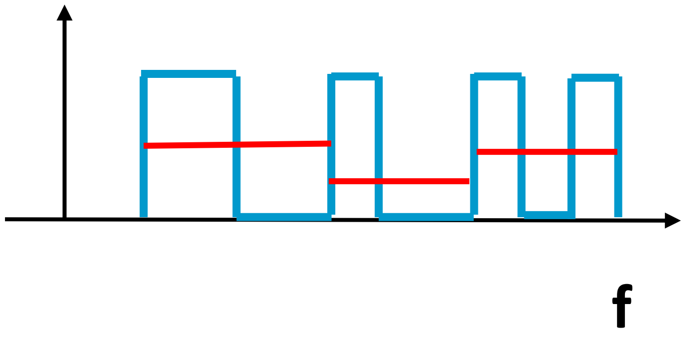
P. AJ Nuyts, P. Reynaert, and W. Dehaene, “Continuous-Time Digital Front-Ends for Multistandard Wireless Transmission” (Springer, 2014).

Background: 1-bit coding (e.g., PWM)

Fundamental frequency f_0
Generic pulse width and phase

$$squarewave(t) = \begin{cases} \delta(t) = \frac{T_{high}}{T_0} \\ \frac{2}{\pi}\sin(\pi\delta(t))\cos(2\pi f_0 t + \theta(t)) \\ \sum_{k=1}^{k=+\infty} \frac{2}{k\pi}\sin(k\pi\delta(t))\cos(2k\pi f_0 t + k\theta(t)) \end{cases}$$

Baseband PWM



P. AJ Nuyts, P. Reynaert, and W. Dehaene, "Continuous-Time Digital Front-Ends for Multistandard Wireless Transmission" (Springer, 2014).

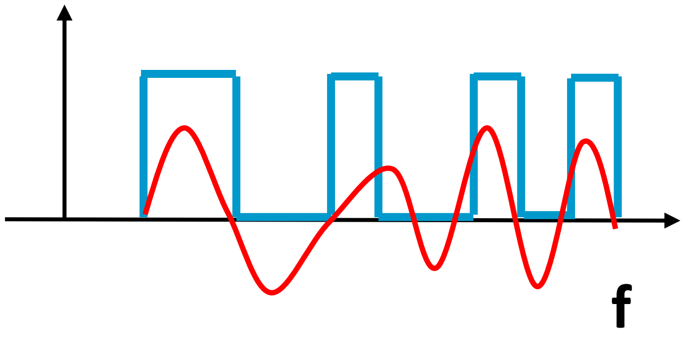
EURECOM

Background: 1-bit coding (e.g., PWM)

Fundamental frequency f_0
Generic pulse width and phase

$$squarewave(t) = \begin{cases} \delta(t) = \frac{T_{high}}{T_0} \\ \frac{2}{\pi}\sin(\pi\delta(t))\cos(2\pi f_0 t + \theta(t)) \\ \sum_{k=1}^{k=+\infty} \frac{2}{k\pi}\sin(k\pi\delta(t))\cos(2k\pi f_0 t + k\theta(t)) \end{cases}$$

Passband PWM



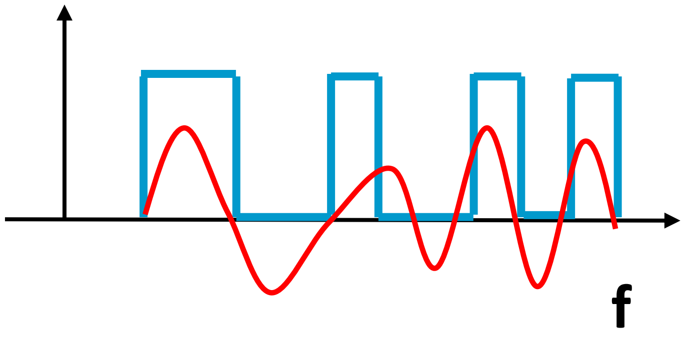
P. AJ Nuyts, P. Reynaert, and W. Dehaene, "Continuous-Time Digital Front-Ends for Multistandard Wireless Transmission" (Springer, 2014).

Background: 1-bit coding (e.g., PWM)

Fundamental frequency f_0
Generic pulse width and phase

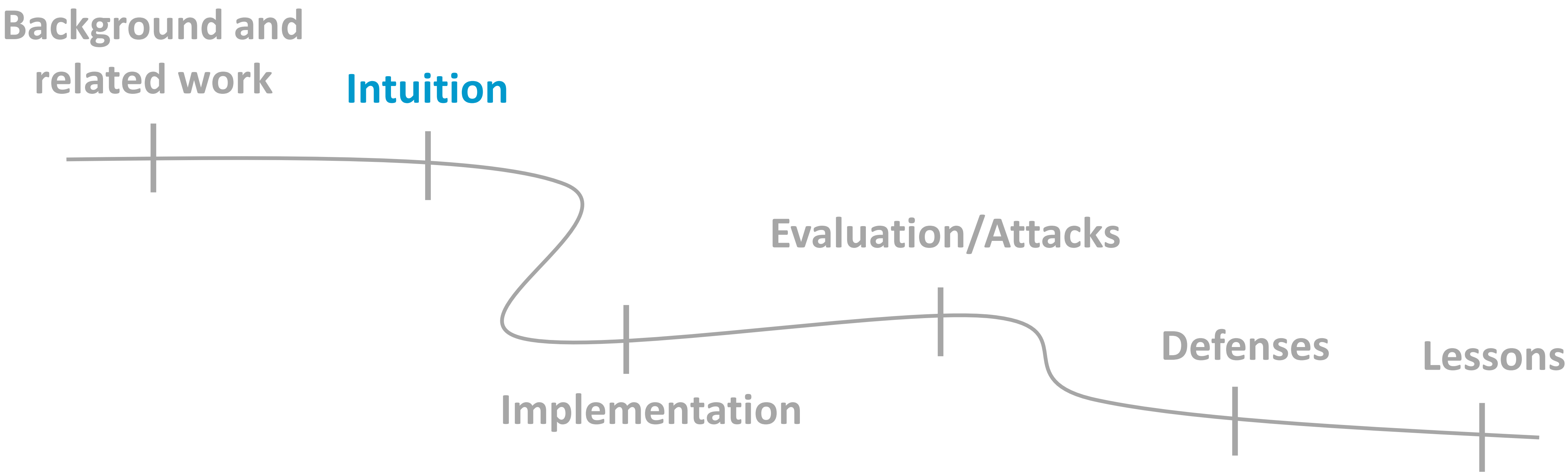
$$squarewave(t) = \begin{cases} \delta(t) = \frac{T_{high}}{T_0} \\ \frac{2}{\pi}\sin(\pi\delta(t))\cos(2\pi f_0 t + \theta(t)) \\ \sum_{k=1}^{k=+\infty} \frac{2}{k\pi}\sin(k\pi\delta(t))\cos(2k\pi f_0 t + k\theta(t)) \end{cases}$$

Passband PWM



P. AJ Nuyts, P. Reynaert, and W. Dehaene, "Continuous-Time Digital Front-Ends for Multistandard Wireless Transmission" (Springer, 2014).

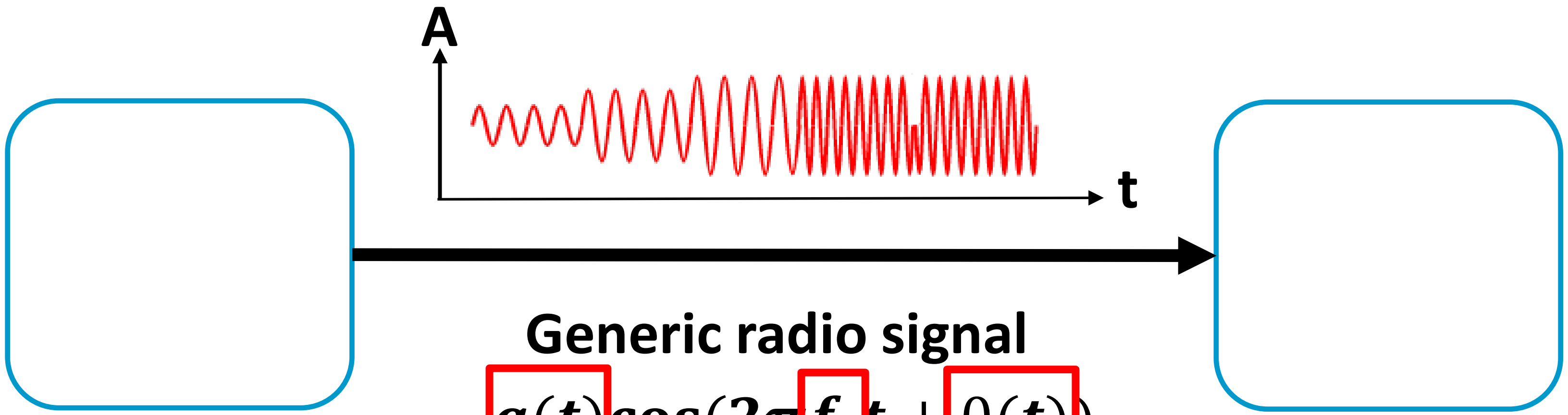
Achieving arbitrary noise modulation



EURECOM Sophia Antipolis

The goal: injecting arbitrary packets

Protocol
(Higher layers to PHY)



Generic radio signal

$$a(t)\cos(2\pi f_c t + \theta(t))$$

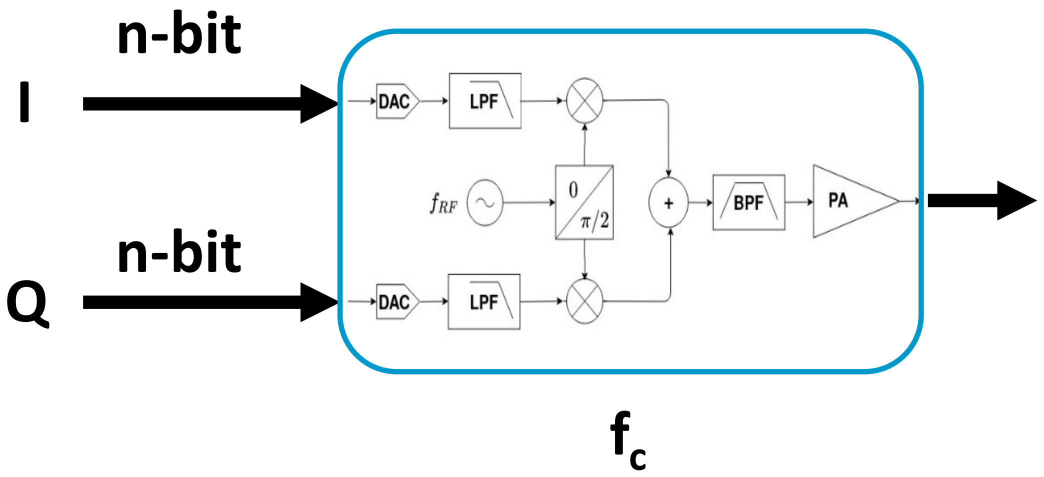
Noise source

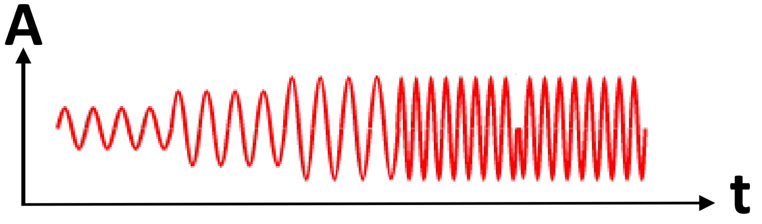
Radio receiver
(Possibly on the same platform)

The problem: dream vs. reality

What we want

Generic SDR





$$a(t)\cos(2\pi f_c t + \theta(t))$$

The problem: dream vs. reality

What we want

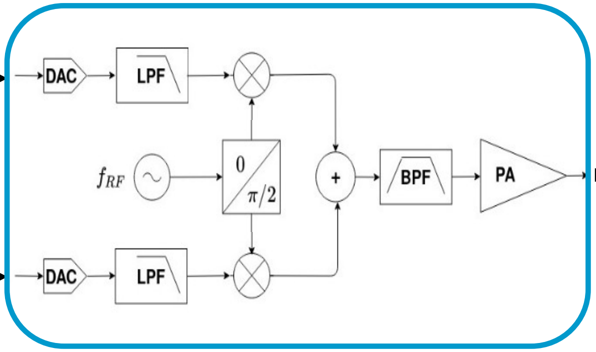
Generic SDR

n-bit

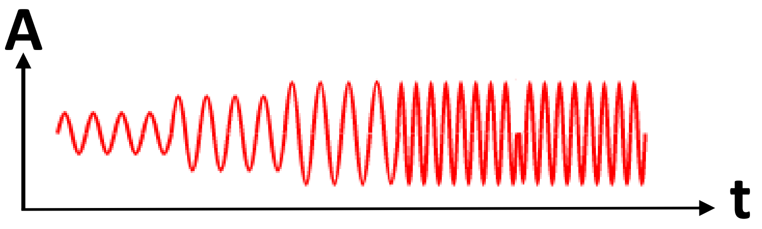
I

Q

n-bit



f_c



$$a(t)\cos(2\pi f_c t + \theta(t))$$

What we have

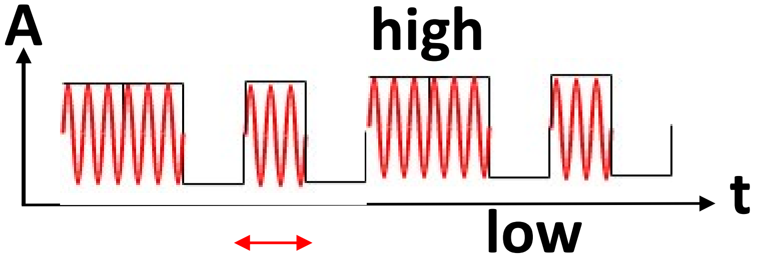
OOK @$F_{leakage}$

1-bit

on/off

Simple OOK modulator (e.g. DRAM accesses)

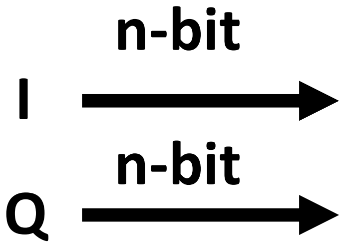
$F_{leakage}$

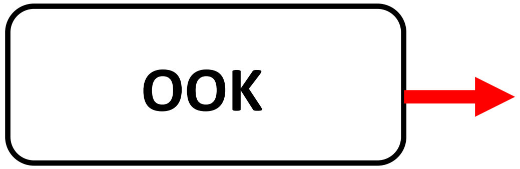


T_{symbol}

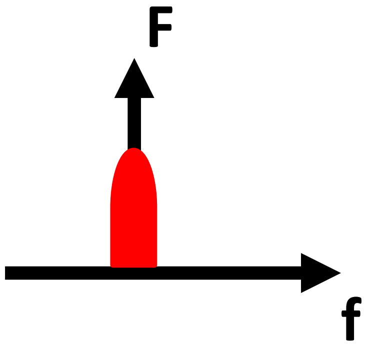
EURECOM

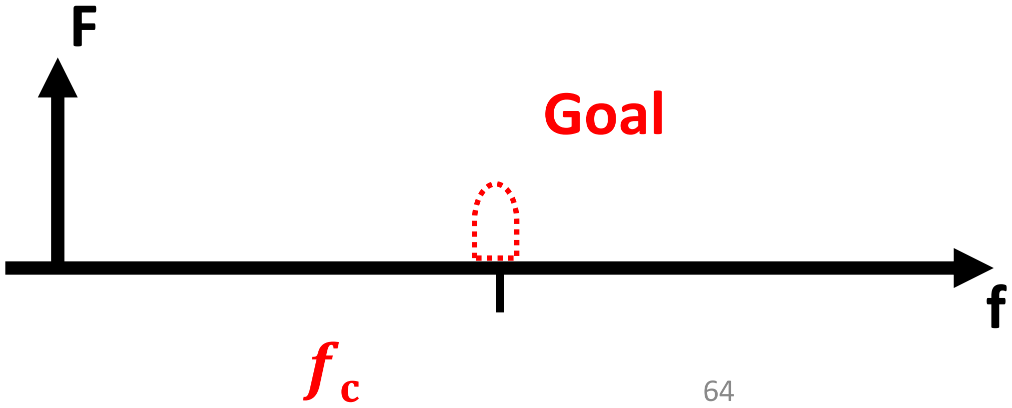
The solution: fully digital radio with 1-bit coding





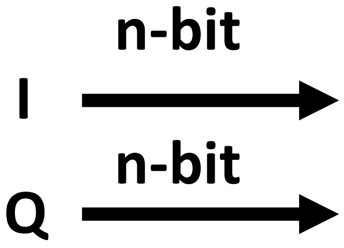
$F_{leakage}$

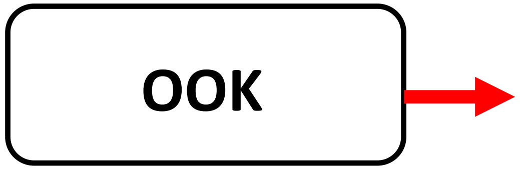




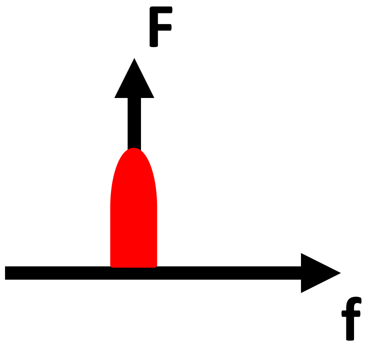
EURECOM

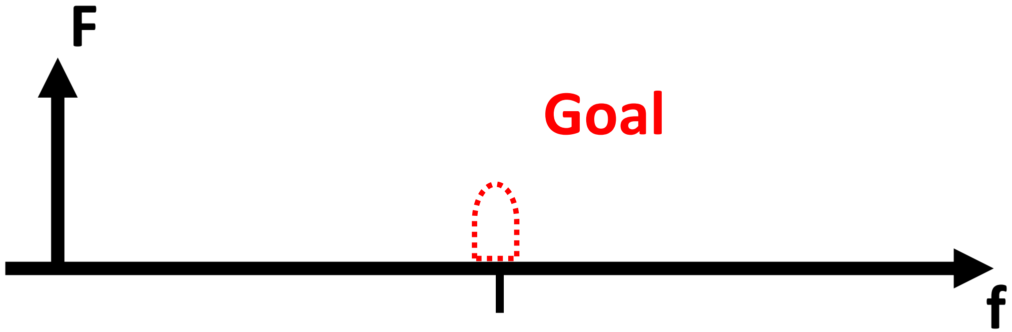
The solution: fully digital radio with 1-bit coding





$F_{leakage}$



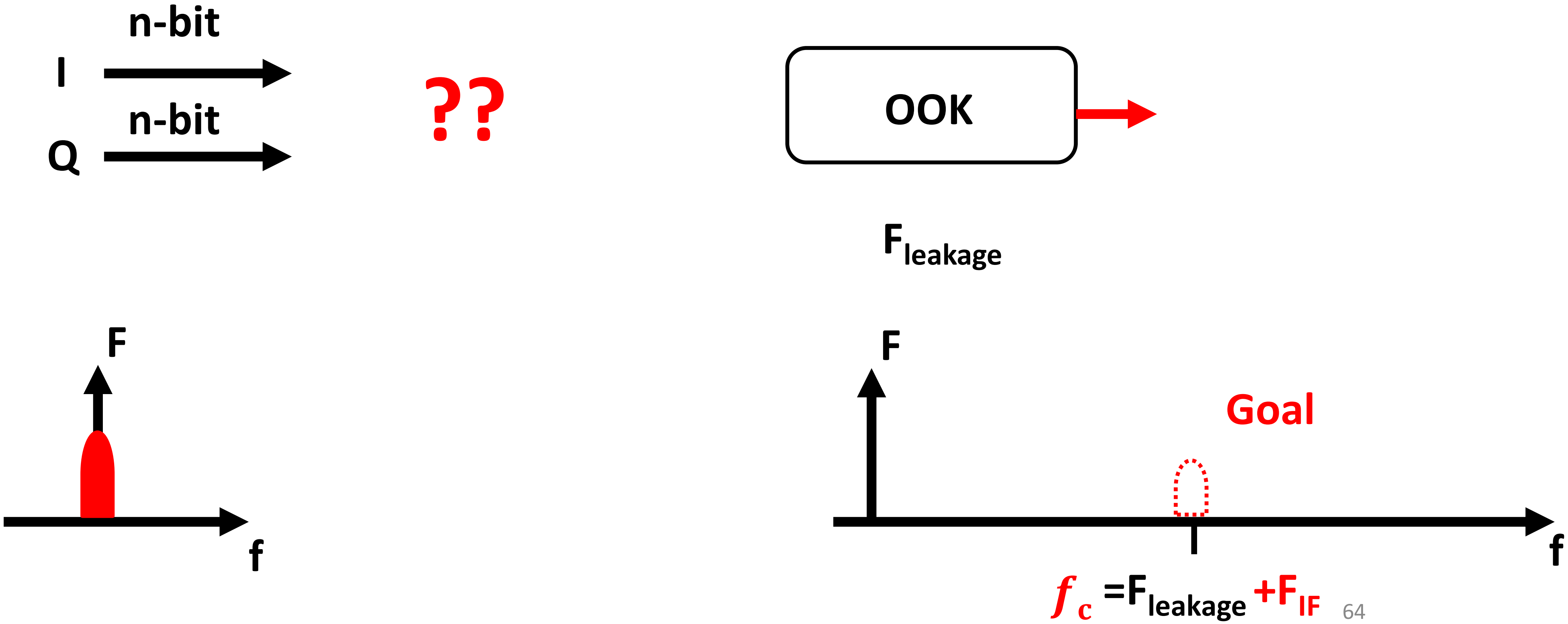


$f_c = F_{leakage} + F_{IF}$

The solution: fully digital radio with 1-bit coding

complex n-bit -> real 1-bit

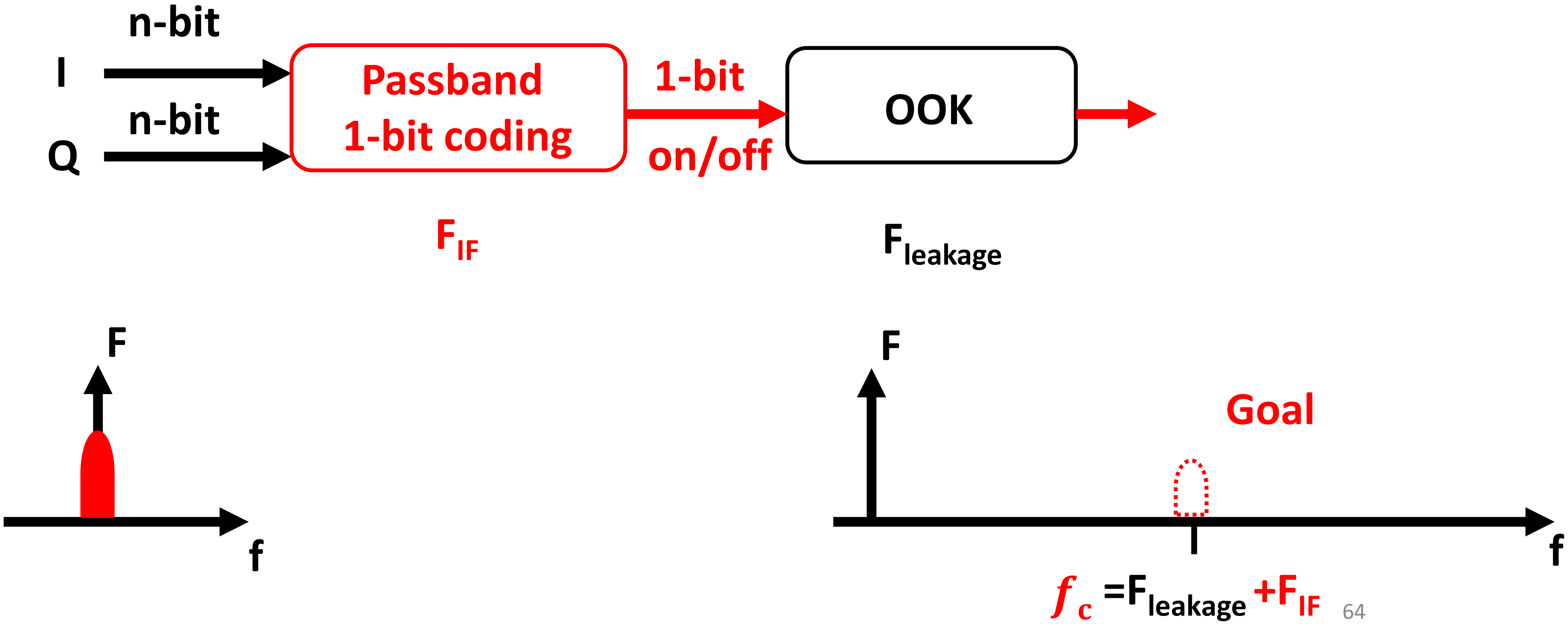
Baseband -> IF



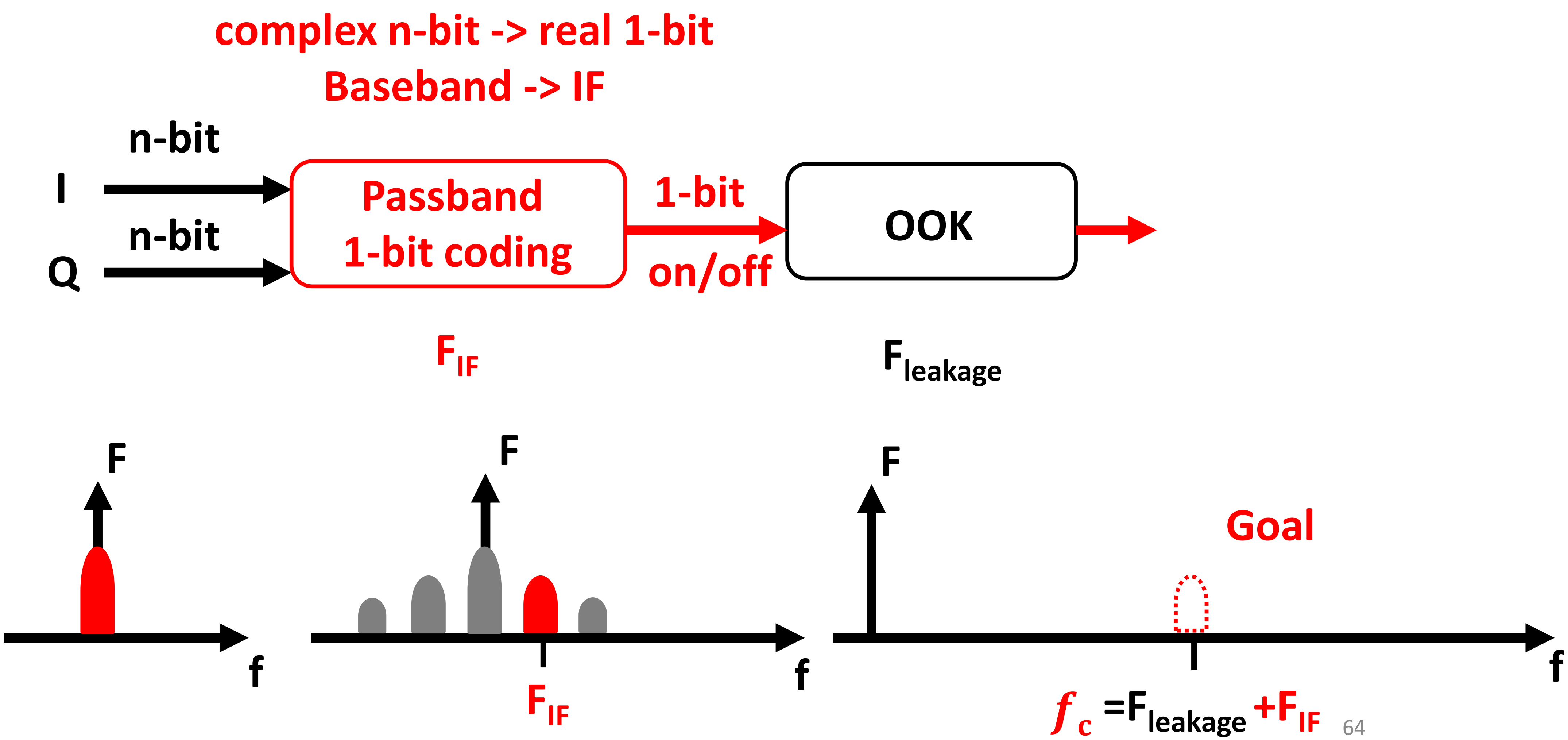
The solution: fully digital radio with 1-bit coding

complex n-bit -> real 1-bit

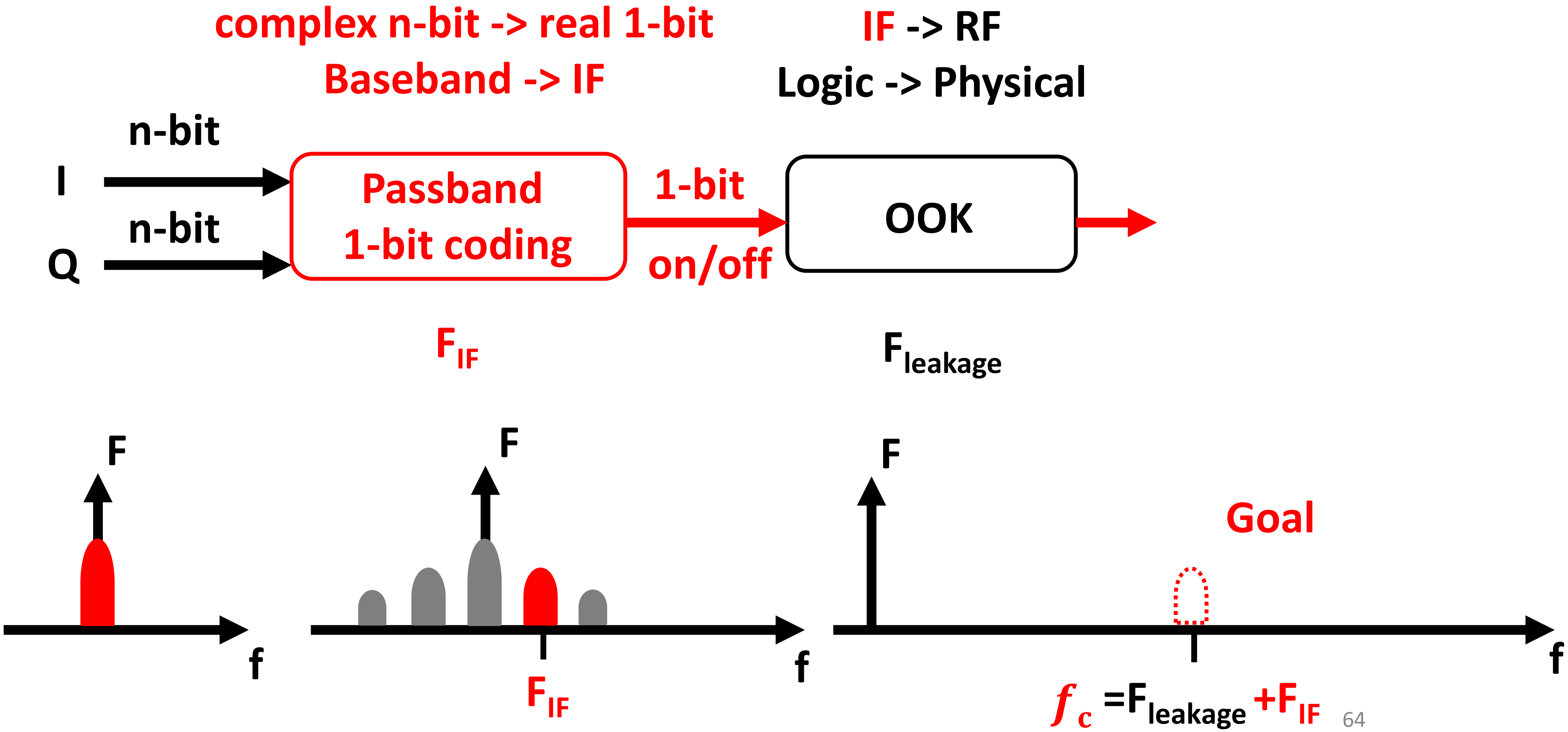
Baseband -> IF



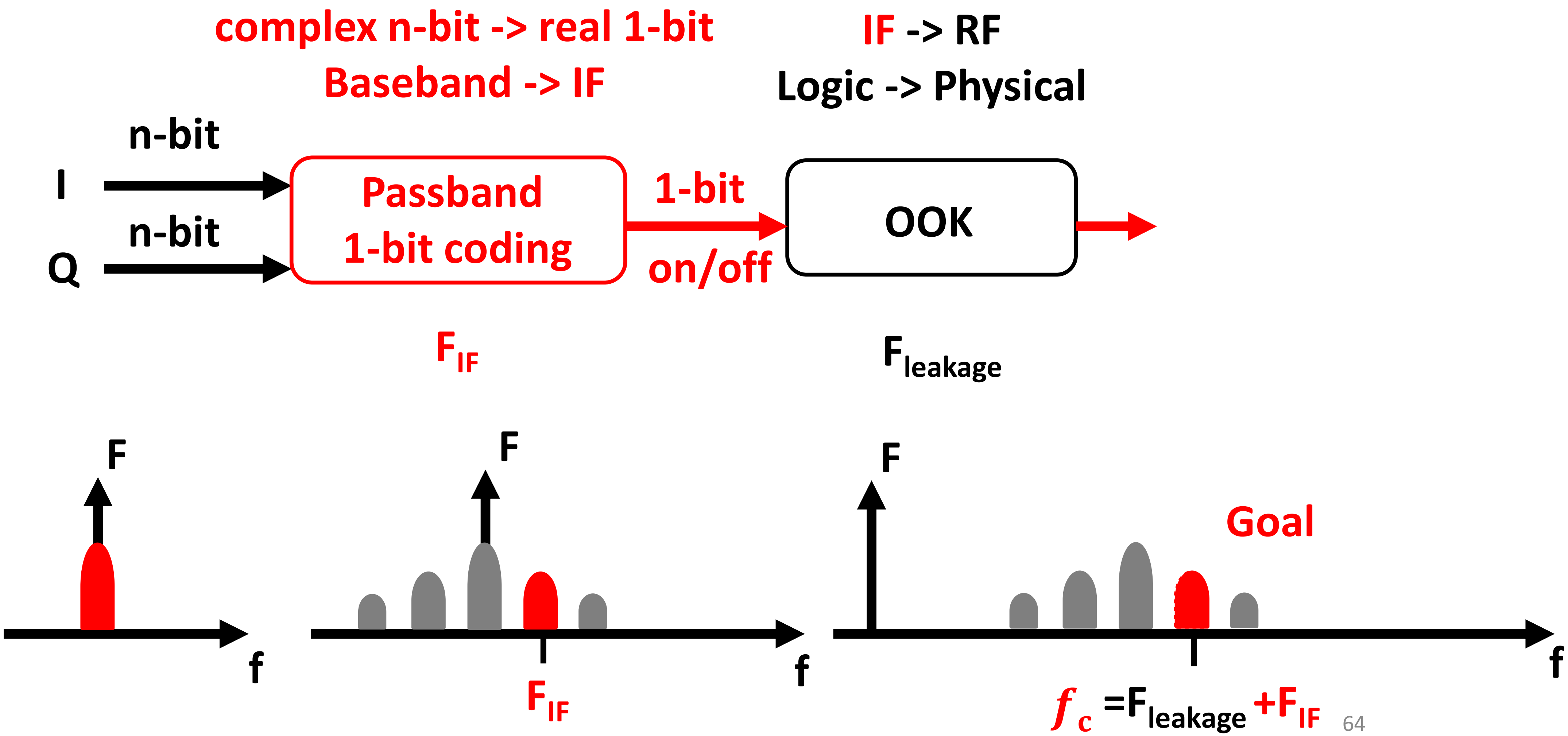
The solution: fully digital radio with 1-bit coding



The solution: fully digital radio with 1-bit coding

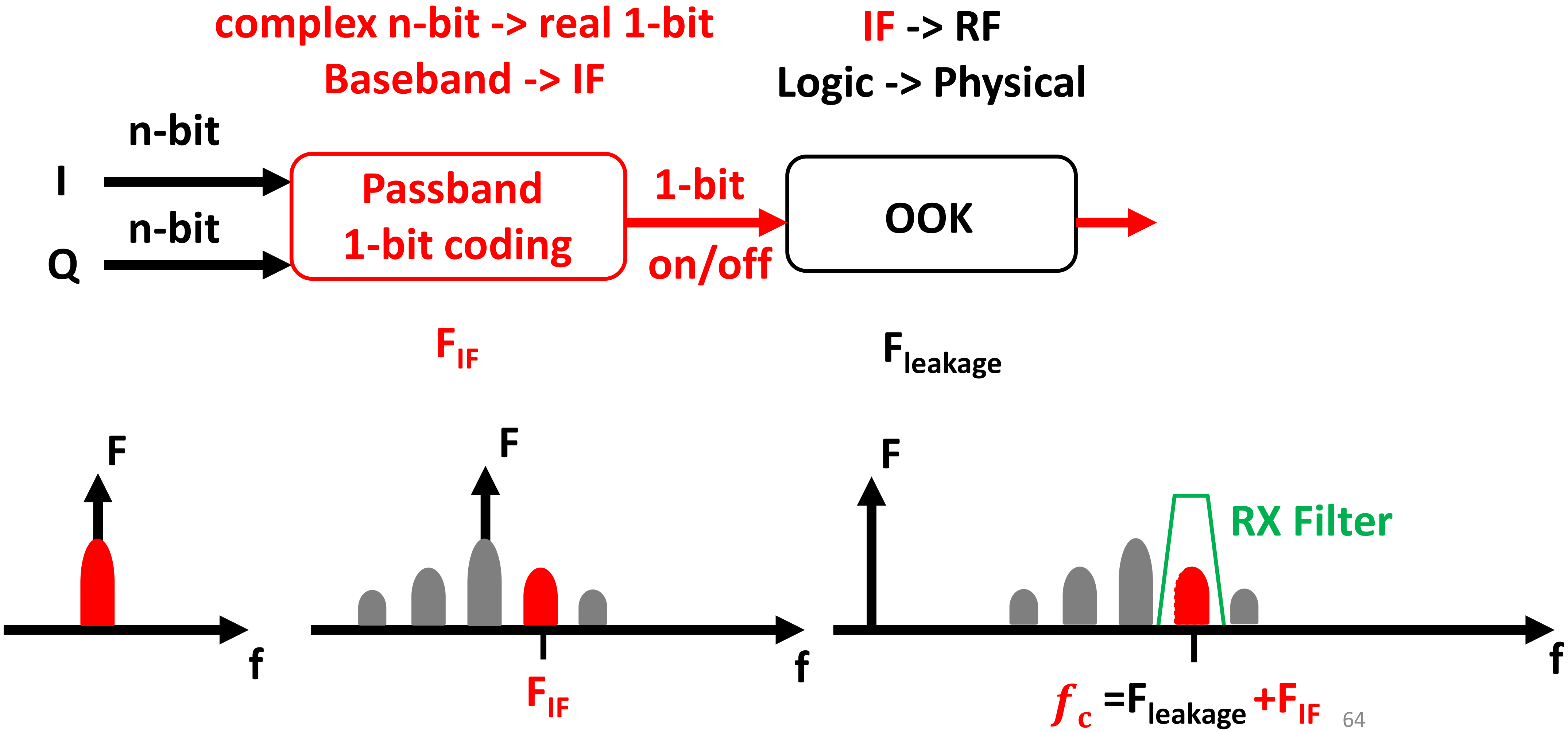


The solution: fully digital radio with 1-bit coding

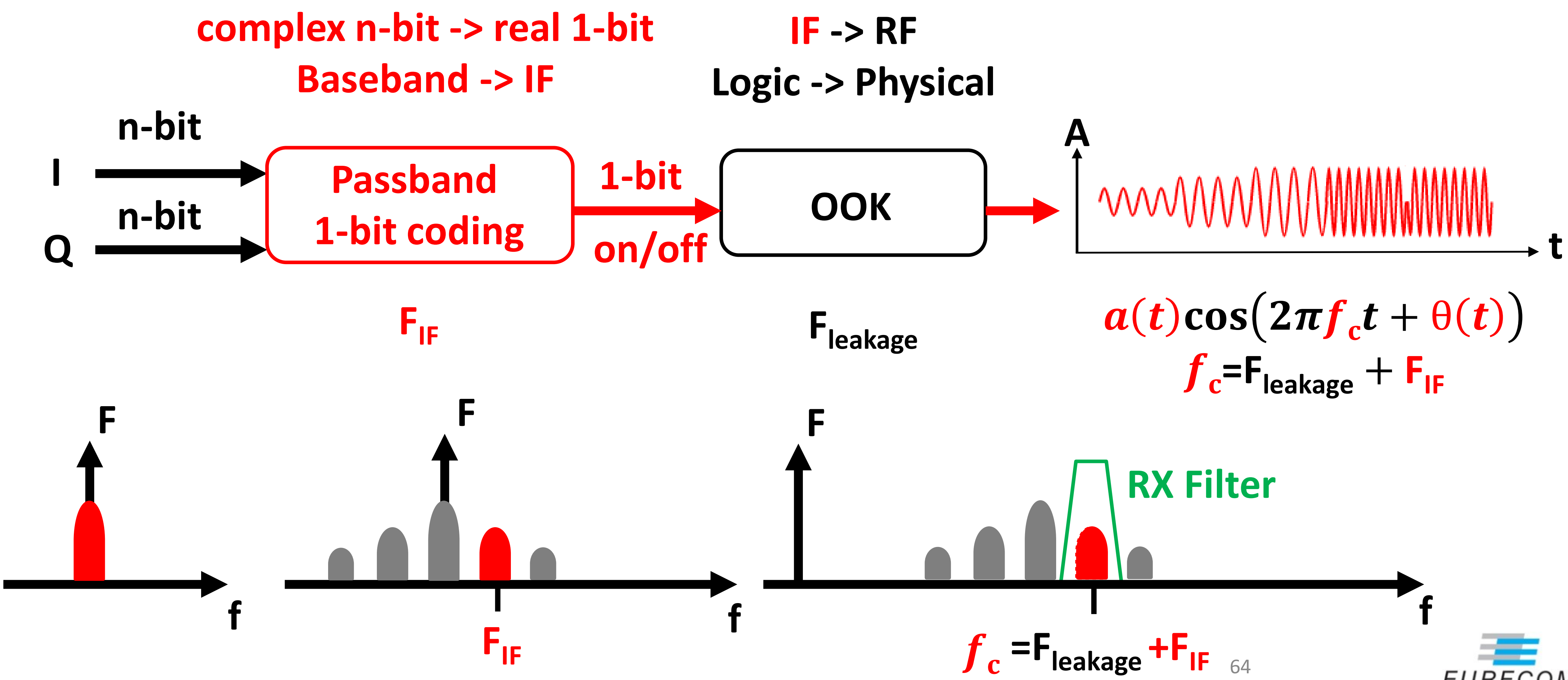


EURECOM Sophia Antipolis

The solution: fully digital radio with 1-bit coding

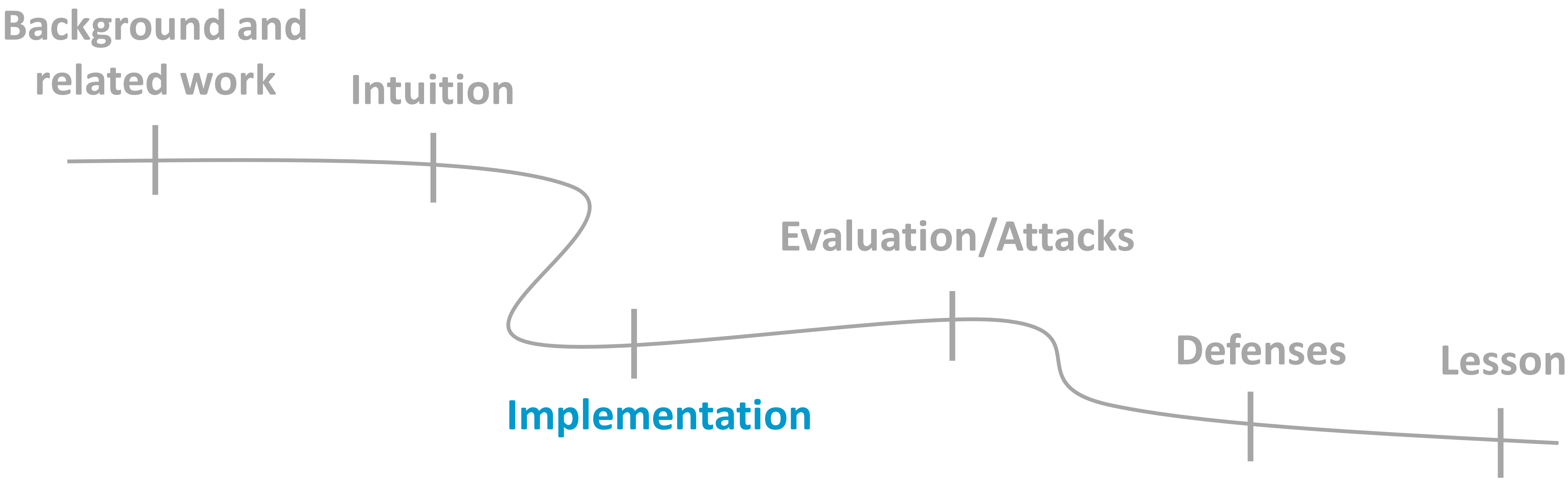


The solution: fully digital radio with 1-bit coding

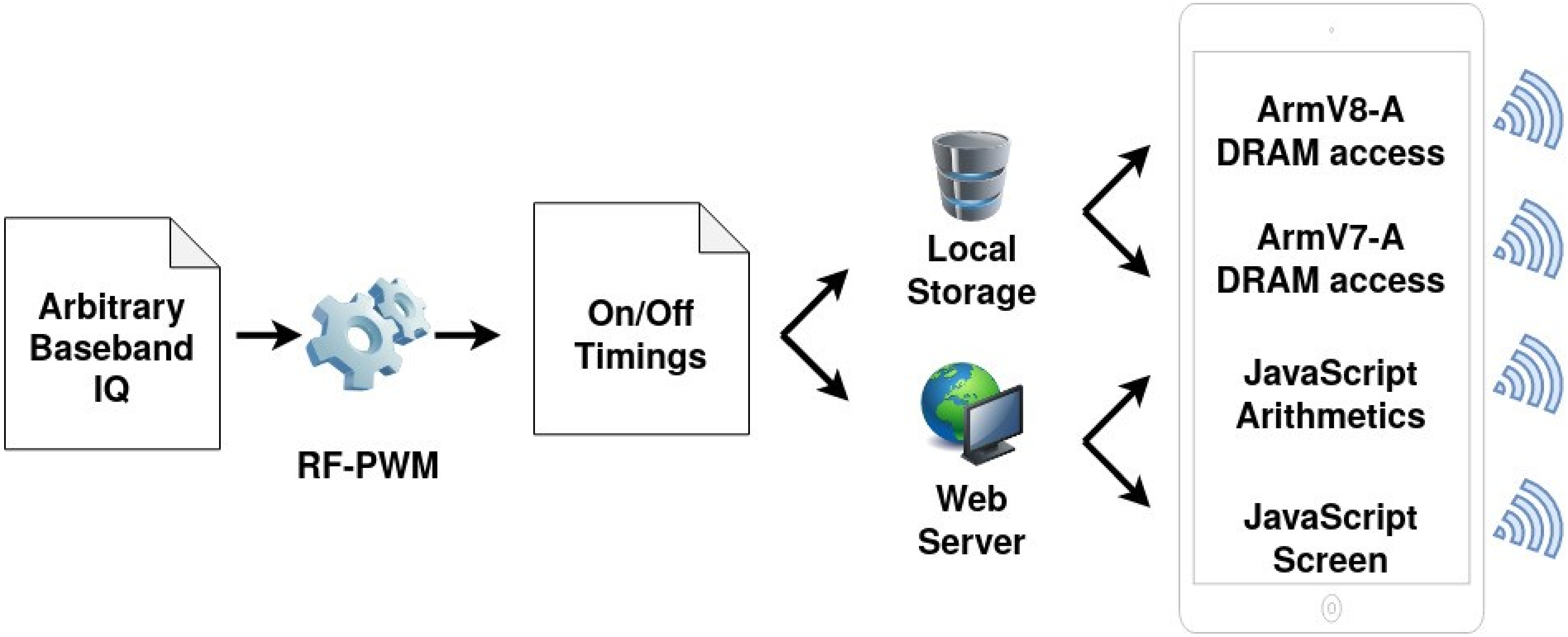


EURECOM

Achieving arbitrary noise modulation

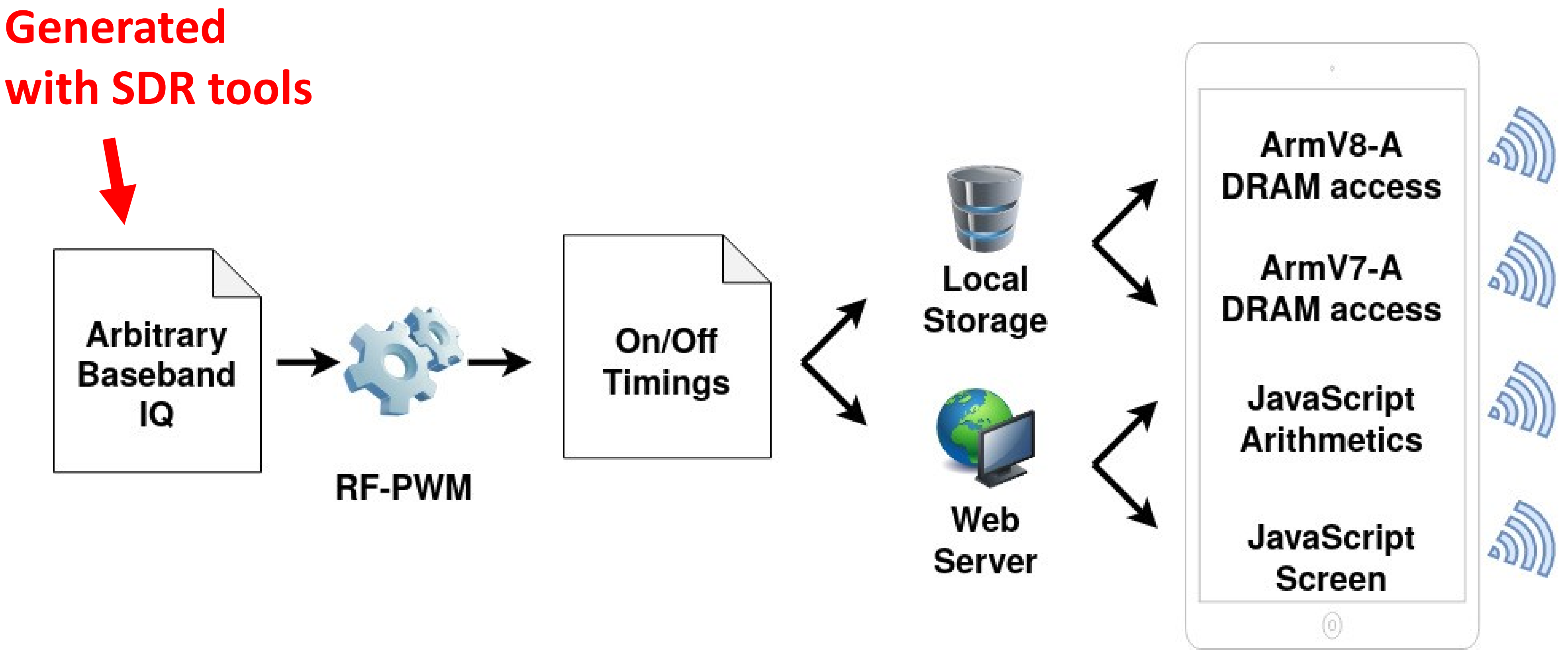


Example of implementation



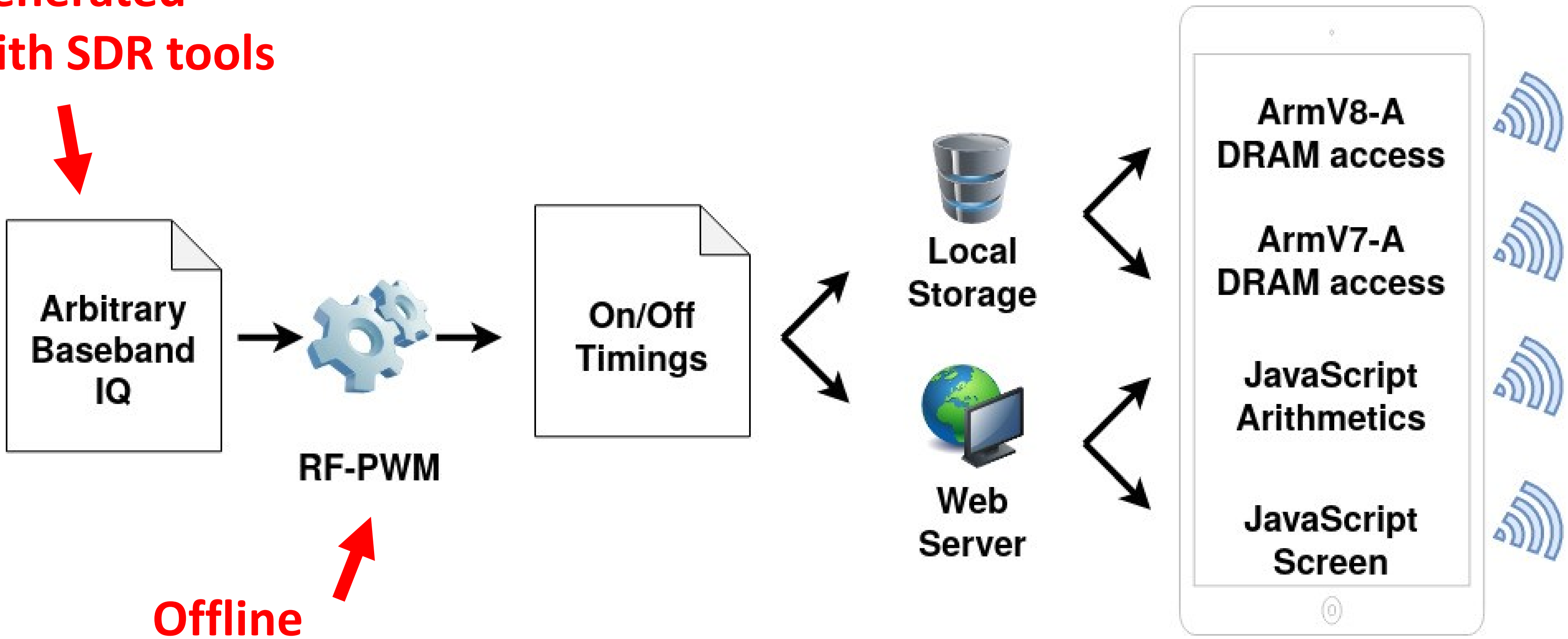
EURECOM

Example of implementation



Example of implementation

Generated with SDR tools



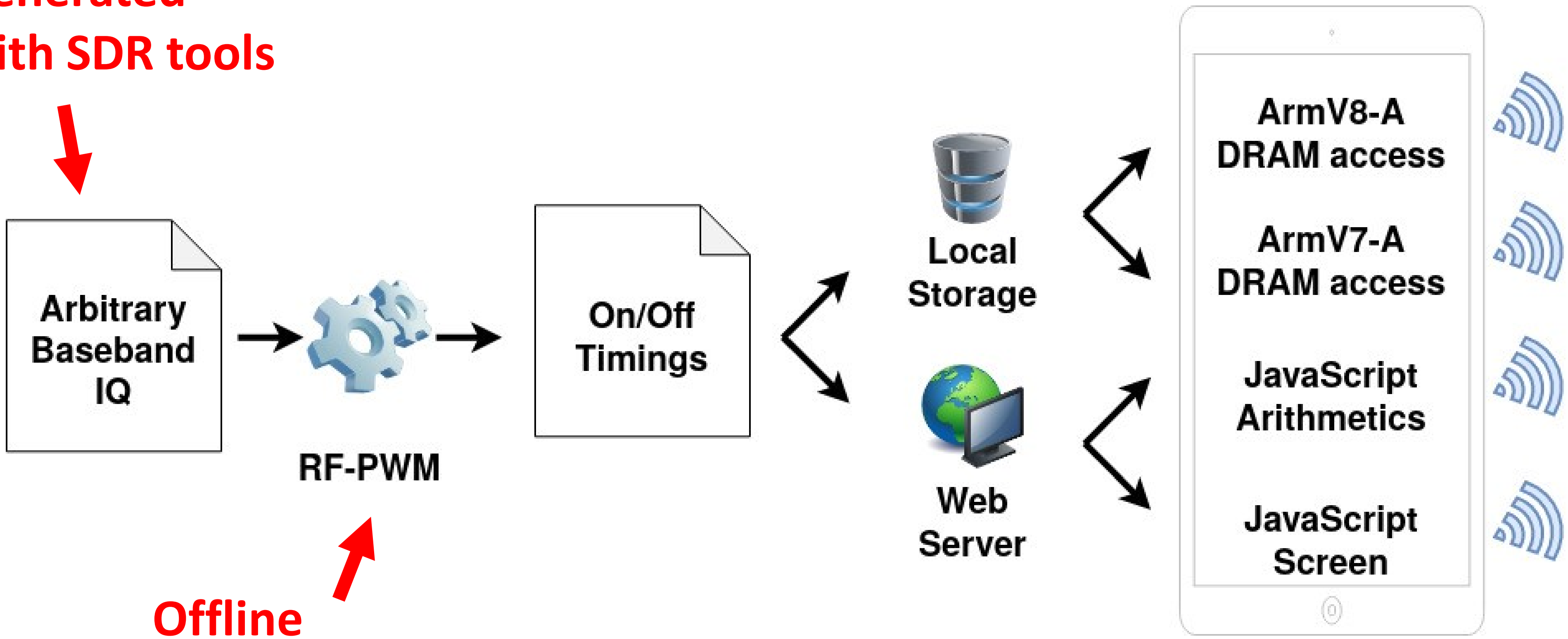
Offline discrete-time RF-PWM

EURECOM

Example of implementation

Several leakage types of Arm smartphones

Generated with SDR tools



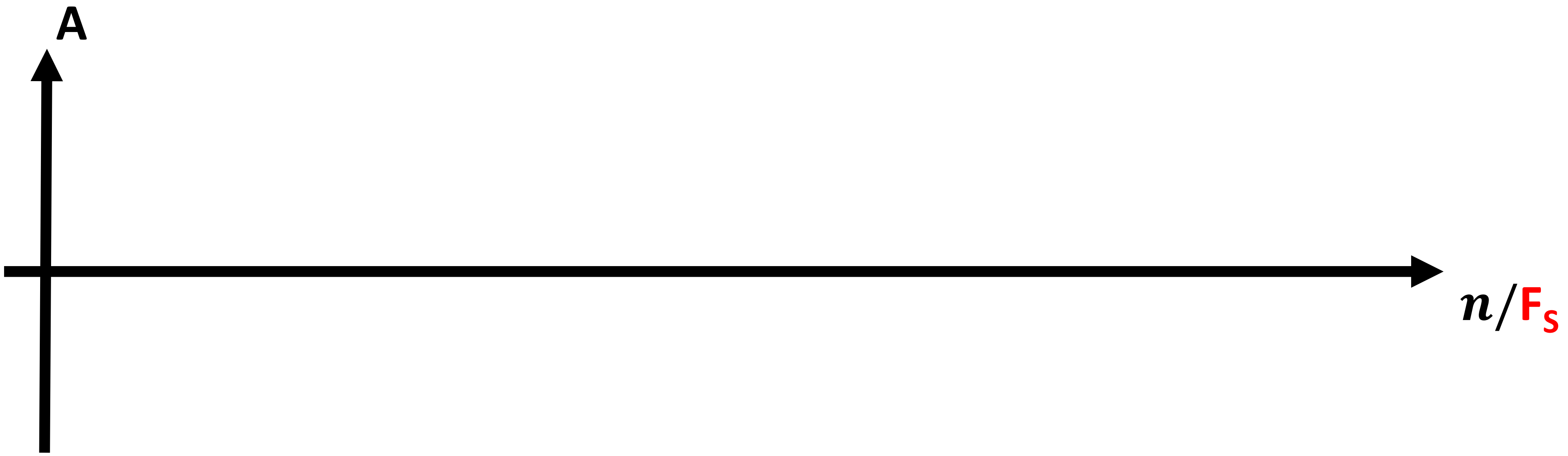
Offline discrete-time RF-PWM

EURECOM

Implementation: discrete-time RF-PWM

Simplified explanation

Input: F_S, $a(n/F_S)$, $\theta(n/F_S)$, F_{IF}

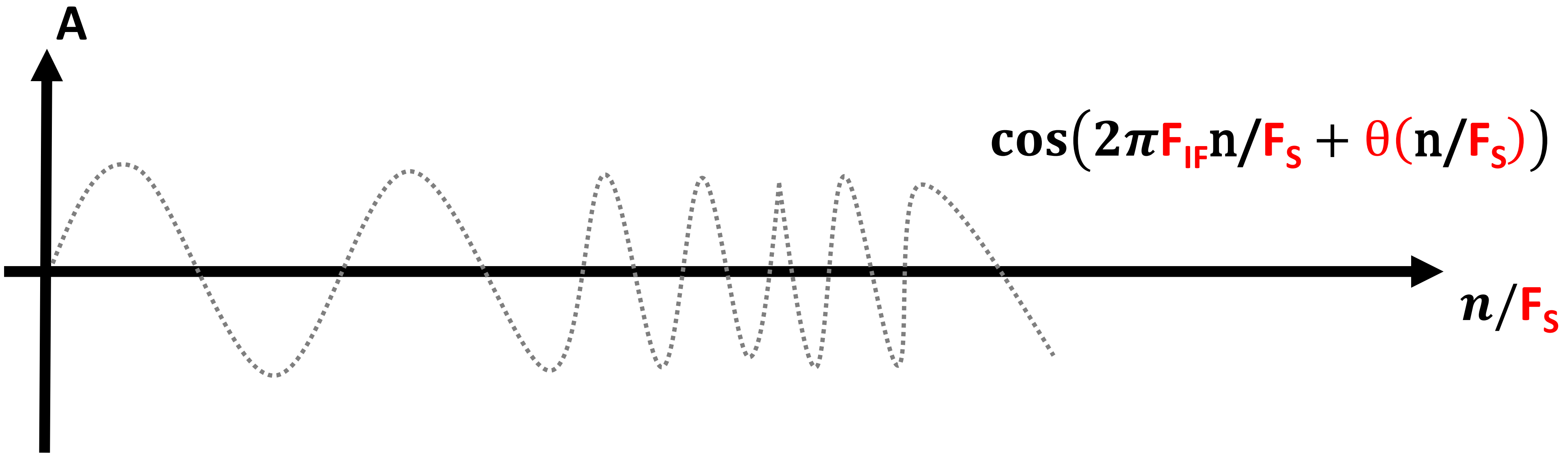


Output:

Implementation: discrete-time RF-PWM

Simplified explanation

Input: F_S, $a(n/F_S)$, $\theta(n/F_S)$, F_{IF}

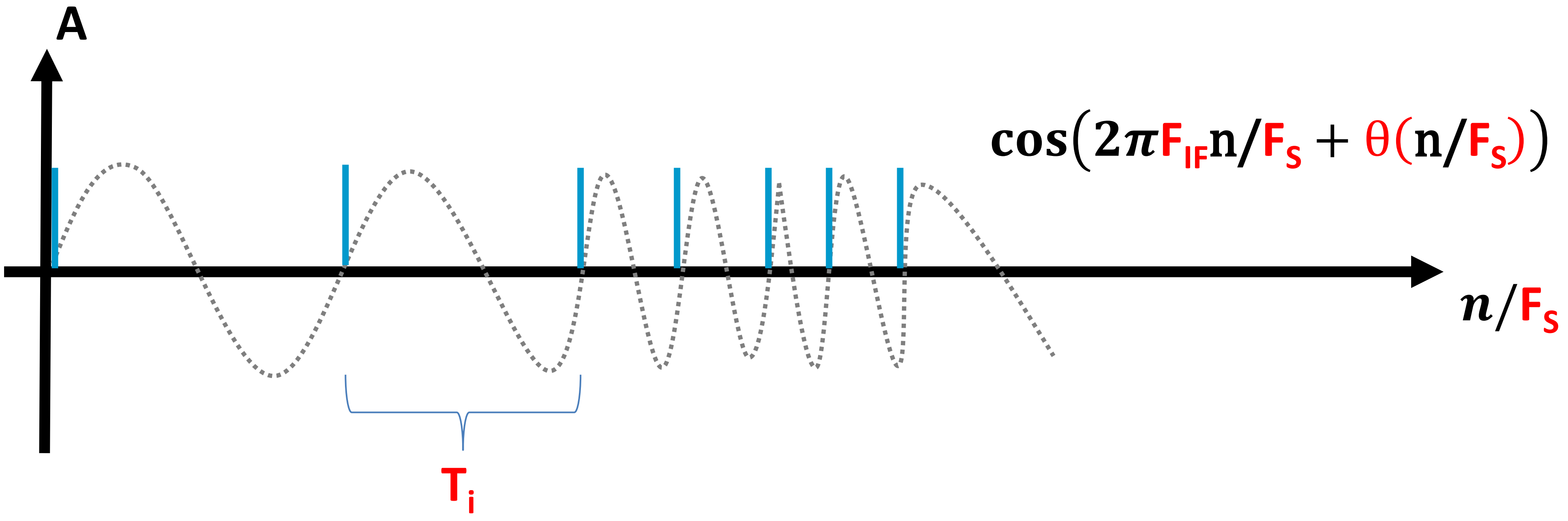


Output:

Implementation: discrete-time RF-PWM

Simplified explanation

Input: F_S, $a(n/F_S)$, $\theta(n/F_S)$, F_{IF}

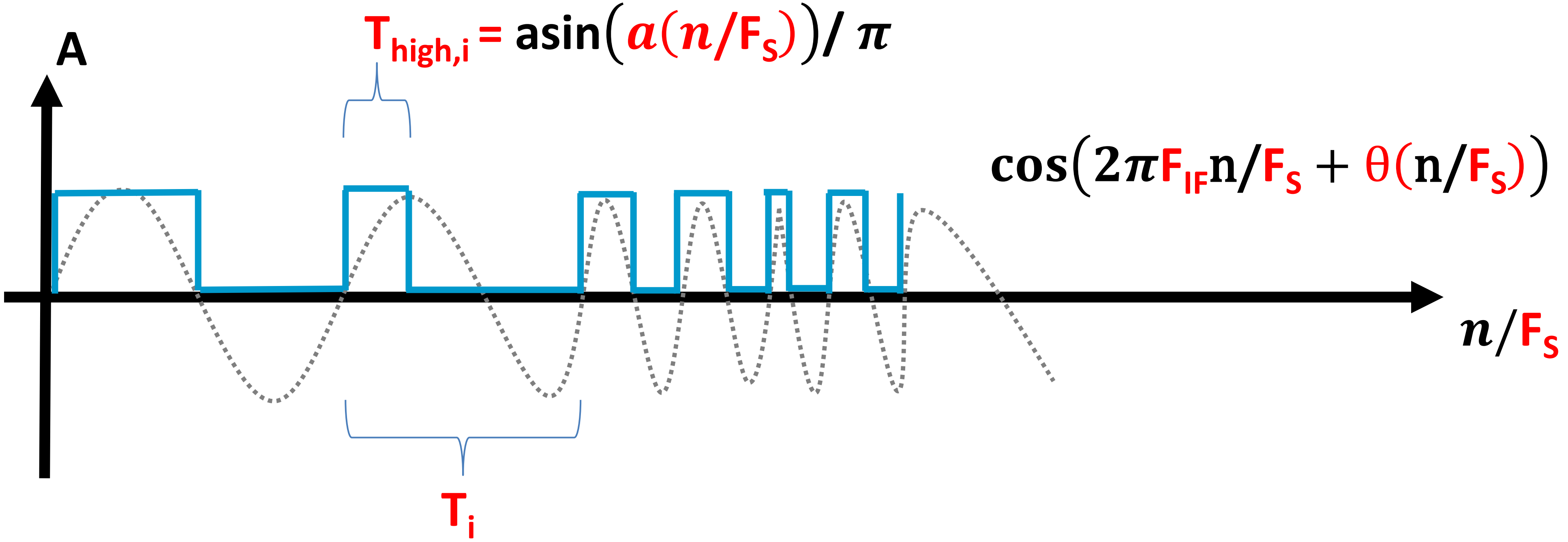


Output: T_1, T_2, T_3, …

Implementation: discrete-time RF-PWM

Simplified explanation

Input: F_S, $a(n/F_S)$, $\theta(n/F_S)$, F_{IF}



Output: $T_{high,1}$ T_1, $T_{high,2}$ T_2, $T_{high,3}$ T_3, ...

EURECOM

Implementation: software control

```
start = now()
while( now() – start < T_high,i )
        leakyOperation()
while( now() – start < T_i )
        doNothing()
```

-: Time accuracy is fundamental!**
(Bandwidth, am/fm/pm quantization)

*M. Schwarz et al., "Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript," in FC 2017.
**Z. Zhang et al., "Leveraging EM Side-Channel Information to Detect Rowhammer Attacks," in IEEE S&P 2020
***Z. Zhang et al., "Triggering Rowhammer Hardware Faults on ARM: A Revisit," ASHES@CCS 2018.

EURECOM Sophia Antipolis

Implementation: software control

*-***: **Time accuracy is fundamental!**
(Bandwidth, am/fm/pm quantization)

```
start = now()
while( now() – start < T_high,i )
        leakyOperation()        →  Leaky**, fast***
while( now() – start < T_i )
        doNothing()
```

Accurate*, stable

*M. Schwarz et al., "Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript," in FC 2017.
**Z. Zhang et al., "Leveraging EM Side-Channel Information to Detect Rowhammer Attacks," in IEEE S&P 2020
***Z. Zhang et al., "Triggering Rowhammer Hardware Faults on ARM: A Revisit," ASHES@CCS 2018.

Implementation: software control

*- ***: Time accuracy is fundamental!
(Bandwidth, am/fm/pm quantization)

```
start = now()
while( now() – start < T_high,i )
        leakyOperation()
while( now() – start < T_i )
        doNothing()
```

Leaky**, fast***

Accurate*, stable
clock_gettime()
(or µ-arch attacks literature)

*M. Schwarz et al., “Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript,” in FC 2017.
**Z. Zhang et al., “Leveraging EM Side-Channel Information to Detect Rowhammer Attacks,” in IEEE S&P 2020
***Z. Zhang et al., “Triggering Rowhammer Hardware Faults on ARM: A Revisit,” ASHES@CCS 2018.

Implementation: software control

start = now()
while(now() – start < $T_{high,i}$)
leakyOperation()
while(now() – start < T_i)
doNothing()

Accurate*, stable
clock_gettime()
(or µ-arch attacks literature)

-: Time accuracy is fundamental!**
(Bandwidth, am/fm/pm quantization)

Leaky, fast*****
Many in the paper and in general

*M. Schwarz et al., “Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript,” in FC 2017.
**Z. Zhang et al., “Leveraging EM Side-Channel Information to Detect Rowhammer Attacks,” in IEEE S&P 2020
***Z. Zhang et al., “Triggering Rowhammer Hardware Faults on ARM: A Revisit,” ASHES@CCS 2018.

Implementation: software control

start = now()
while(now() – start < $T_{high,i}$)
leakyOperation()
while(now() – start < T_i)
doNothing()

Accurate[*], stable
clock_gettime()
(or µ-arch attacks literature)

[*-*]: Time accuracy is fundamental!**
(Bandwidth, am/fm/pm quantization)

Leaky[**], fast[***]
Many in the paper and in general
E.g., on Arm-v8 (re)use DRAMMER

```
__attribute__((naked)) \
void hammer_civac(uint64_t *addr) {
  __asm volatile("LDR X9, [X0]");
  __asm volatile("DC CIVAC, X0");
  __asm volatile("DSB 0xB");
  __asm volatile("RET");
}
```

*M. Schwarz et al., "Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript," in FC 2017.
**Z. Zhang et al., "Leveraging EM Side-Channel Information to Detect Rowhammer Attacks," in IEEE S&P 2020
***Z. Zhang et al., "Triggering Rowhammer Hardware Faults on ARM: A Revisit," ASHES@CCS 2018.

Achieving arbitrary noise modulation

Evaluation: Protocols

Variety

Voice AM, NBFM, PSK31, 2x 2PSK, RTTY45.45, MFSK128, Olivia 64/2000, SSTV, HamDRM, FT4, LoRa, GLONASS C/A Code

Modulation

Analog and digital

AM, FM, OOK, FSK, M-FSK, GFSK, PSK, OFDM, CSS, DSSS

Bandwidth

31 Hz (PSK31) to 0.511MHz (GLONASS)

Extra

Forward Error Correction, addressing, upper layers in general

Tradeoffs

Speed (2x 2PSK at 1000bps), SNR (FT4 at SNR < -10dB), etc.

Evaluation: Arm-based smartphones

Variety

19 Arm-based phones

Major vendors

Limitations on leakage

9 phones have a leakage visible outside

Not always strong

Limitations on bandwidth and stability

Tens of kHz on ArmV7-A, few MHz on ArmV8-A

But still enough for many useful protocols

Limitations on leakage frequency

DRAM (e.g., 400MHz, 800MHz, 1600MHz, 1794MHz) and harmonics (up to GHz)

But still overlap with other radios + F_{IF} offers some freedom

Evaluation: Arm-based smartphones

Variety

19 Arm-based phones

Major vendors

This is just one possible implementation

Might be better/worse on other platforms

Limitations on leakage

9 phones have a leakage visible outside

Not always strong

Limitations on bandwidth and stability

Tens of kHz on ArmV7-A, few MHz on ArmV8-A

But still enough for many useful protocols

Limitations on leakage frequency

DRAM (e.g., 400MHz, 800MHz, 1600MHz, 1794MHz) and harmonics (up to GHz)

But still overlap with other radios + F_{IF} offers some freedom

Evaluation: Arm-based smartphones

Variety

19 Arm-based phones

Major vendors

This is just one possible implementation
Might be better/worse on other platforms

Limitations on leakage

9 phones have a leakage visible outside

Not always strong

Time resolution and stability is critical for the Noise-SDR idea

Limitations on bandwidth and stability

Tens of kHz on ArmV7-A, few MHz on ArmV8-A

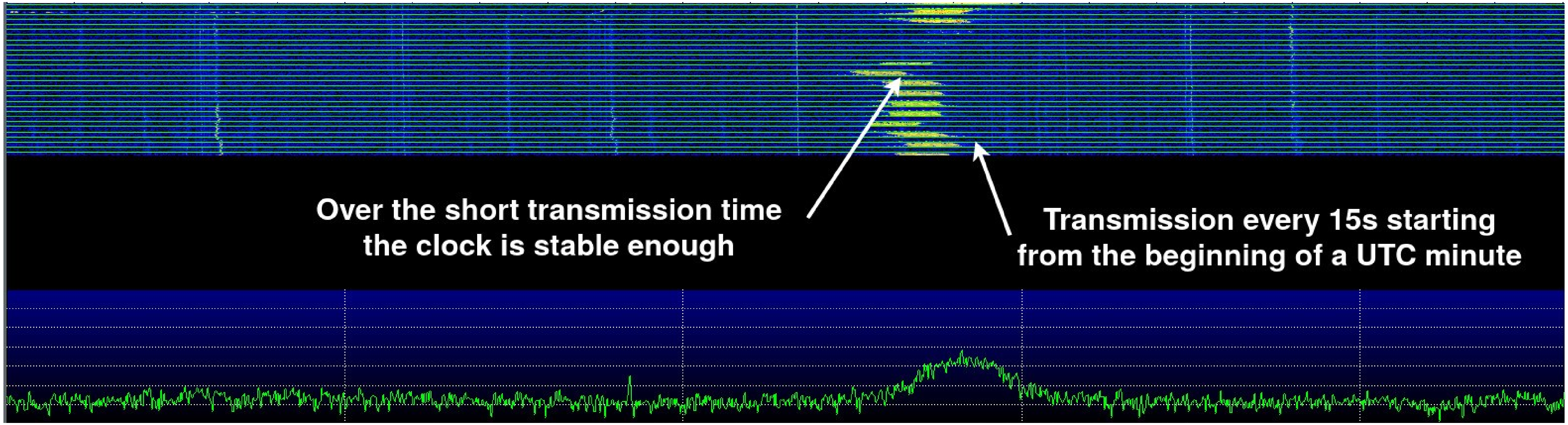
But still enough for many useful protocols

Limitations on leakage frequency

DRAM (e.g., 400MHz, 800MHz, 1600MHz, 1794MHz) and harmonics (up to GHz)

But still overlap with other radios + F_{IF} offers some freedom

Applications: tracking, detection, injection, tx, ...

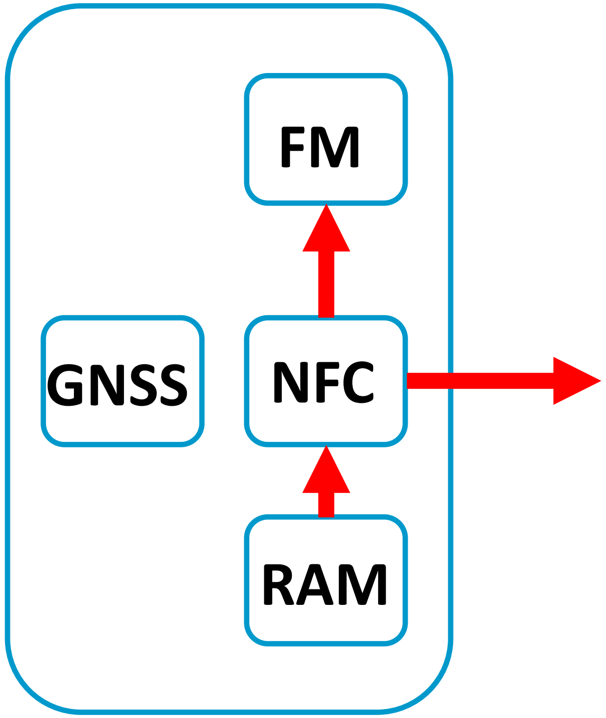


Tracking using FT4 beacons, up to 5m on Galaxy S5 Mini
Using existing reception tools

J. Taylor, FT4, https://physics.princeton.edu/pulsar/k1jt/FT4_Protocol.pdf.
J. Taylor, WSJT, https://physics.princeton.edu/pulsar/K1JT/.

Applications: tracking, detection, injection, tx, …

Noise injection
FM injection
NFC modulation
GPS jamming



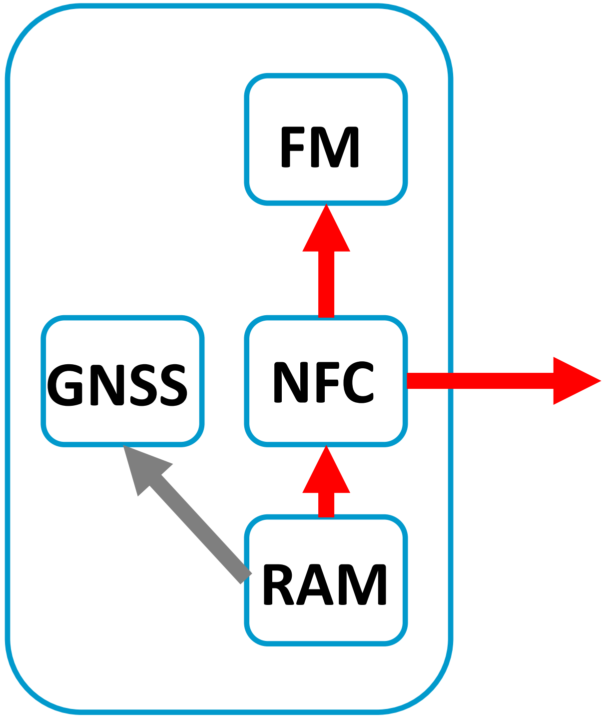
Example

EURECOM
Sophia Antipolis

Applications: tracking, detection, injection, tx, …

Noise injection
FM injection
NFC modulation
GPS jamming

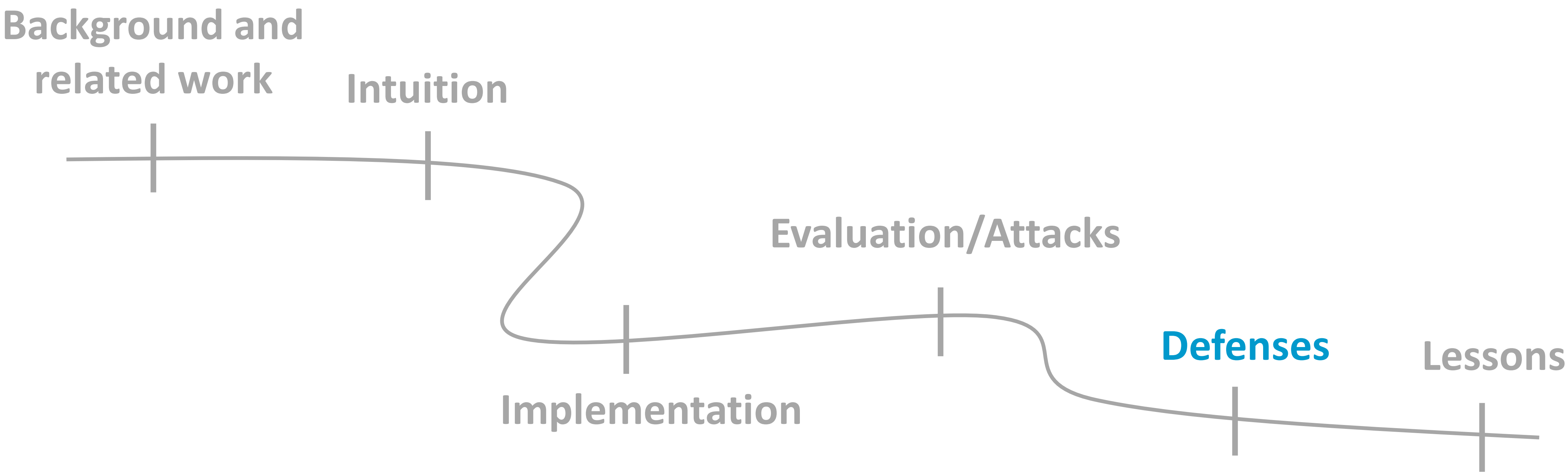
Future work
DRAM @1.6GHz
GLONASS @1.6GHz
Can we spoof the position?



Example

EURECOM

Achieving arbitrary noise modulation



EURECOM

Defenses

Soft-TEMPEST-specific (HW)

Reduce leakages and coupling

Defenses

Soft-TEMPEST-specific (HW)
Reduce leakages and coupling

Soft-TEMPEST-specific (SW)
Reduce timing resolution and software control on hardware

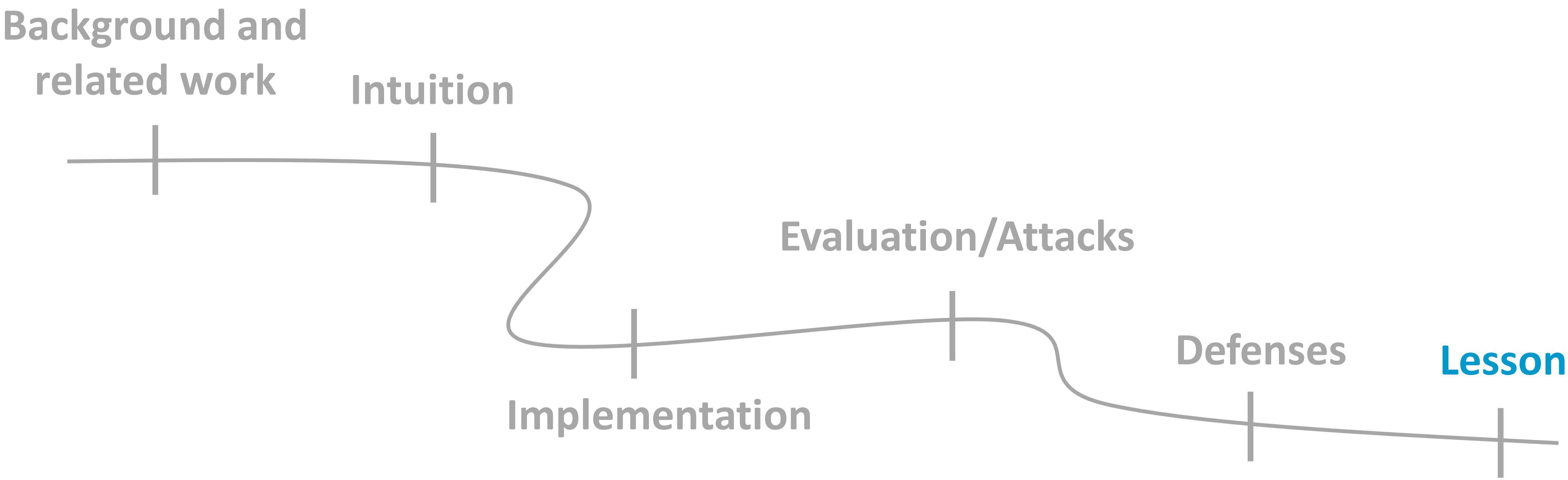
Defenses

Soft-TEMPEST-specific (HW)
Reduce leakages and coupling

Soft-TEMPEST-specific (SW)
Reduce timing resolution and software control on hardware

Applications specific (SW/HW):
Shield smartphone, spoofing detection, …

Achieving arbitrary noise modulation



Lessons learned

The idea

Arbitrary modulation of noise

Leveraging fully-digital radios ideas

Lessons learned

The idea

Arbitrary modulation of noise

Leveraging fully-digital radios ideas

A vision for applications and attacks

Signal injection (preliminary results)

Signal transmission with all advantages of SDRs

Lessons learned

The idea

Arbitrary modulation of noise

Leveraging fully-digital radios ideas

A vision for applications and attacks

Signal injection (preliminary results)

Signal transmission with all advantages of SDRs

Implementation

If there is a good leakage, then it works well

Time resolution is probably the biggest challenge

Context

Challenges & Contributions

Screaming Channels

Noise-SDR

Future Work

Conclusion

Future work (Screaming Channels)

Preliminary results

Techniques
- **Reception:** **radio techniques (e.g., CSI, errors)**
- **Attack:** **low-freq/multivariate, deep learning[3], more applications**

[1]D. R. E. Gnad, J. Krautter, and M. Baradaran Tahoori, "Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices," IACR TCHES 2019.

[2]J. Choi, H.-Y. Yang, and D.-H. Cho, "TEMPEST Comeback: A Realistic Audio Eavesdropping Threat on Mixed-Signal SoCs," ACM CCS 2020.

[3]R. Wang, H. Wang, and E. Dubrova, "Far Field EM Side-Channel Attack on AES Using Deep Learning," ACM ASHES 2020.

Future work (Screaming Channels)

Preliminary results

Techniques
- **Reception:** radio techniques (e.g., CSI, errors)
- **Attack:** low-freq/multivariate, deep learning[3], more applications

Analysis
- **Distortion:** can it be modeled without knowing the design?
- **Coupling:** analysis with access to the design

[1]D. R. E. Gnad, J. Krautter, and M. Baradaran Tahoori, "Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices," IACR TCHES 2019.

[2]J. Choi, H.-Y. Yang, and D.-H. Cho, "TEMPEST Comeback: A Realistic Audio Eavesdropping Threat on Mixed-Signal SoCs," ACM CCS 2020.

[3]R. Wang, H. Wang, and E. Dubrova, "Far Field EM Side-Channel Attack on AES Using Deep Learning," ACM ASHES 2020.

Future work (Screaming Channels)

Preliminary results

Techniques
- **Reception:** radio techniques (e.g., CSI, errors)
- **Attack:** low-freq/multivariate, deep learning[3], more applications

Analysis
- **Distortion:** can it be modeled without knowing the design?
- **Coupling:** analysis with access to the design

Types
- **Modulation:** other blocks, FM/PM, LO reradiation, WiFi and others
- **Targets and threat model:** link-layer, PKC, hardware block, peripherals, …
- **Beyond mixed-signal:** smartphone NFC, platforms, planes, …
- **Beyond radios:** CPU->ADC side channel[1], Audio IN -> SWREG noise TEMPEST[2]

[1]D. R. E. Gnad, J. Krautter, and M. Baradaran Tahoori, "Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices," IACR TCHES 2019.

[2]J. Choi, H.-Y. Yang, and D.-H. Cho, "TEMPEST Comeback: A Realistic Audio Eavesdropping Threat on Mixed-Signal SoCs," ACM CCS 2020.

[3]R. Wang, H. Wang, and E. Dubrova, "Far Field EM Side-Channel Attack on AES Using Deep Learning," ACM ASHES 2020.

Future work (Screaming Channels)

Preliminary results

Techniques
- **Reception:** radio techniques (e.g., CSI, errors)
- **Attack:** low-freq/multivariate, deep learning[3], more applications

Analysis
- **Distortion:** can it be modeled without knowing the design?
- **Coupling:** analysis with access to the design

Types
- **Modulation:** other blocks, FM/PM, LO reradiation, WiFi and others
- **Targets and threat model:** link-layer, PKC, hardware block, peripherals, …
- **Beyond mixed-signal:** smartphone NFC, platforms, planes, …
- **Beyond radios:** CPU->ADC side channel[1], Audio IN -> SWREG noise TEMPEST[2]

Defenses
- **Countermeasures:** specific, lightweight, cheap
- **Simulation/Testing:** automated analysis, functional+EM simulation

[1] D. R. E. Gnad, J. Krautter, and M. Baradaran Tahoori, "Leaky Noise: New Side-Channel Attack Vectors in Mixed-Signal IoT Devices," IACR TCHES 2019.

[2] J. Choi, H.-Y. Yang, and D.-H. Cho, "TEMPEST Comeback: A Realistic Audio Eavesdropping Threat on Mixed-Signal SoCs," ACM CCS 2020.

[3] R. Wang, H. Wang, and E. Dubrova, "Far Field EM Side-Channel Attack on AES Using Deep Learning," ACM ASHES 2020.

Future work (Noise-SDR)

Preliminary results

Techniques

- **Time resolution:** **better timing sources, calibration, compensation, …**
- **1-bit coding:** **passband sigma-delta, mathematical modeling**

*C. Shen et al., "When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient", IEEE S&P 2021.

Future work (Noise-SDR)

Preliminary results

Techniques
- **Time resolution:** better timing sources, calibration, compensation, …
- **1-bit coding:** passband sigma-delta, mathematical modeling

Implementation
- **Leakage sources:** screen, camera, GPU, …
- **Software control:** JavaScript, WebAssembly, …
- **Platform:** x86, laptops, smartwatches, IoT, …
- **SSC:** dealing* with spread spectrum clocking

*C. Shen et al., "When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient", IEEE S&P 2021.

Future work (Noise-SDR)

Preliminary results

Techniques
- **Time resolution:** better timing sources, calibration, compensation, …
- **1-bit coding:** passband sigma-delta, mathematical modeling

Implementation
- **Leakage sources:** screen, camera, GPU, …
- **Software control:** JavaScript, WebAssembly, …
- **Platform:** x86, laptops, smartwatches, IoT, …
- **SSC:** dealing* with spread spectrum clocking

Applications
- **GNSS spoofing:** GLONASS, …
- **Beyond radios:** injecting signals in sensors
- **Soft-RFI:** finding software-controlled RFI effects

*C. Shen et al., “When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient”, IEEE S&P 2021.

EURECOM

Future work (Other dangerous interactions)

Other interactions with radios

- **"NONSTOP": unintentional backscattering of ambient signals**
- **Analog/RF to Digital: are there problems in the other direction?**
- **Analog/RF to Analog/RF: from radio to radio**
- **…**

Context

Challenges & Contributions

Screaming Channels

Noise-SDR

Future Work

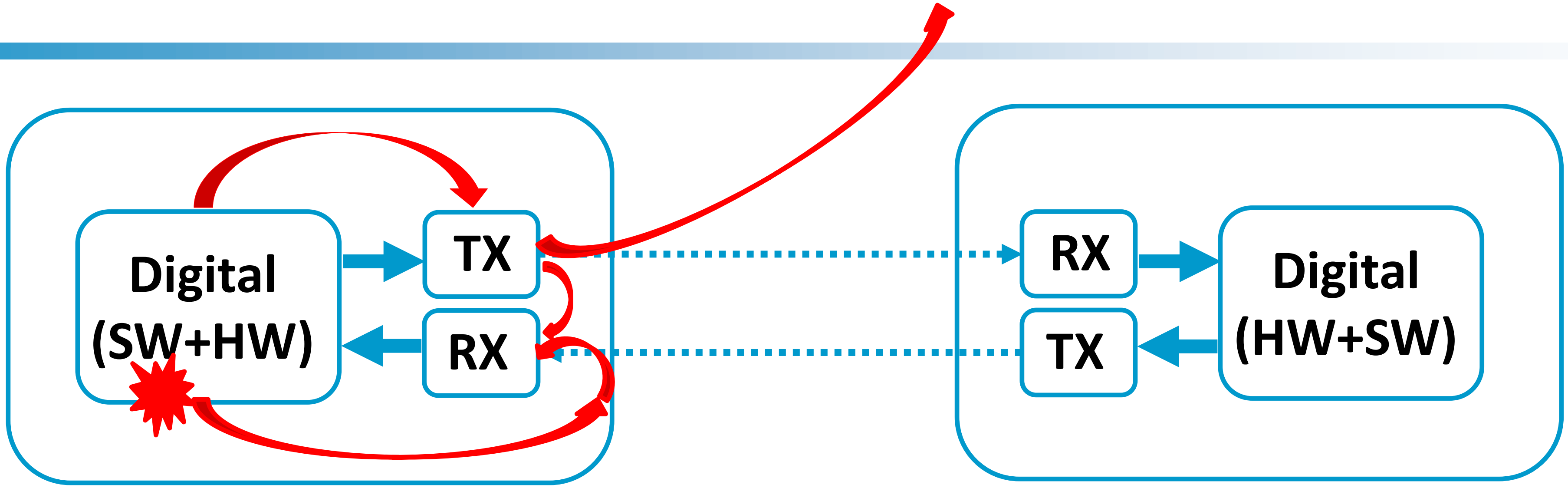
Conclusion

Answer to the question

Digital activity is broadcast

Screaming Channels

E.g., side channel



Noise-SDR

Victim A

B

Arbitrary modulation
of digital noise

E.g., injection

Security research question

~~Does~~ logic activity produce physical leakages that flow from digital components to radio blocks breaking the security of the wireless links~~?~~

Yes!

EURECOM

Conclusion

CONTEXT: Modern connected systems (computation close to communication)

PROBLEM: Do unexpected interactions between high-speed digital logic and radio transceivers threat the security of the data processed and communicated by these devices?

FINDINGS: Digital activity leaks over the radio channel (e.g., side channels over the air)
Digital noise shaped into arbitrary RF signals (e.g., injection)

DISCUSSION: Many open research directions for consolidation or related effects

CONCLUSION: Wireless security should consider the threats brought by EMI/RFI during design, simulation, test, and security analysis

EURECOM Sophia Antipolis

Open Source!

https://eurecom-s3.github.io/screaming_channels/

Code + Data + Instructions

Already replicated by many in industry and academia

Thank You!

@GioCamurati
https://giocamurati.github.io
camurati@eurecom.fr

Backup Slides

“Hubris”

"Nature does not support straight lines […]

8.2.3.3. However, humans, in their infinite wisdom, attempt to defy nature and make computers that use square waves […]

That extra energy […] has to go somewhere.”

"IMG_7006A Martin Ryckaert. 1587-1633. Anvers. Paysage avec la chute d'Icare. Landscape with the Fall of Icarus. Vers 1625. Cologne Wallraf Richartz Museum" by jean louis mazieres is licensed with CC BY-NC-SA 2.0.

AIR FORCE SYSTEMS SECURITY MEMORANDUM 7011
https://cryptome.org/afssm-7011.htm
1 MAY 1998

Some informal terminology

Signal: useful intended signal carrying some information
Noise: other spurious signals (in EMSec they are useful signals, with other noise, e.g., thermal, on top)

Compromising emanation: noise signal unexpectedly carrying information
Application: TEMPEST (recover P), Soft-TEMPEST/covert ch. (send data), side channel (recover k)

Trace: Portion of a compromising emanation corresponding to a sensitive operation (e.g., AES encryption)
Signal-to-Noise Ratio: don't confuse SNR of a trace with the SNR of the data dependency with p or k

Leakage variable y: intermediate value processed in the algorithm, e.g., y = Sbox(p xor k)
Leakage l(y): the actual leakage that we measure
Leakage model m(y): a model of the leakage, e.g., HW[y], or estimated with profiling set

Order: m can be linear or nonlinear, the relation between m and l can be first order, second order, …

Backup (Screaming Channels)

Screaming Channels, a general problem?

Our targets

Nordic Semiconductor nRF52832 (BLE Nano v2, PCA10040, Rigado BDM301)

Nordic Semiconductor nRF52840 (PCA10056)

Qualcom Atheros AR9271 (PENGUIN WiFi adapter, Alfa Network WiFi adapter)

ExpressIF ESP32 WiFi/BLE

Nokia 3.1 NFC modulation

Used in many real-world products (e.g., Eddystone)

Leakages in test mode + LO modulation

Leakages in test mode (regulator to radio)

Platform level coupling, active modulation

Disclosure

General problem acknowledged by the manufacturer(s)

General challenges

We presented general challenges (e.g., orthogonality, many other GFSK protocols)

Future work

Automating analysis to reach larger scale, with/without access to the physical design and test mode firmware

Screaming Channels and WiFi (1/3)

Challenges

Non-orthogonal modulation (we must demodulate and compute packet errors)
Higher signal/hardware quality (e.g., PA linearity*)
ADC resolution when extracting the error from packets

Preliminary results

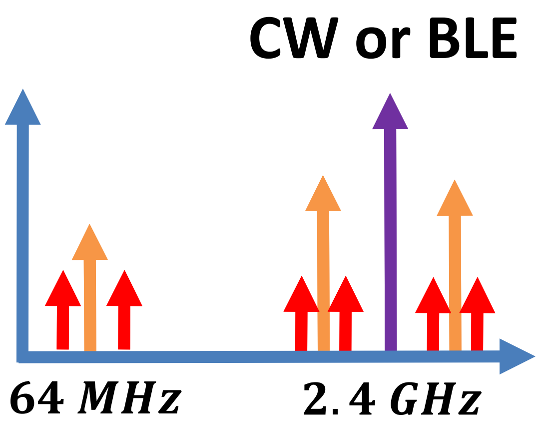
Leakages detected in test mode on some cards (AR9271, ESP32)
(Programming + having test mode is not always straightforward)

Ideas

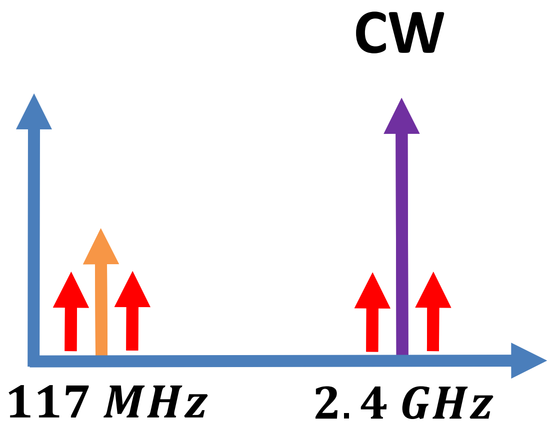
Low-frequency non-uniform sampling of many packet errors and parameters

*A. Behzad, "Wireless LAN Radios: System Definition to Transistor Design" (IEEE Press Series on Microelectronic Systems) (Hoboken, NJ, USA: John Wiley & Sons, Inc., 2008).

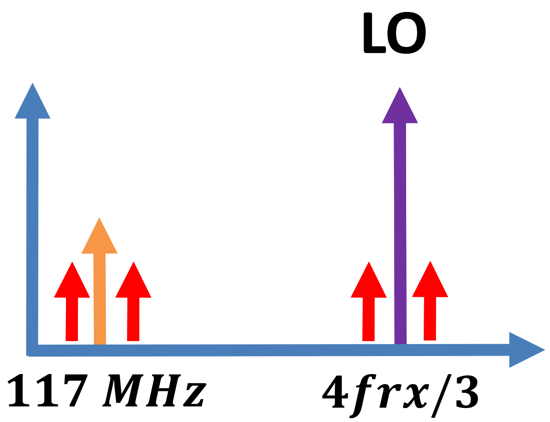
Screaming Channels and WiFi (2/3)



nRF52832

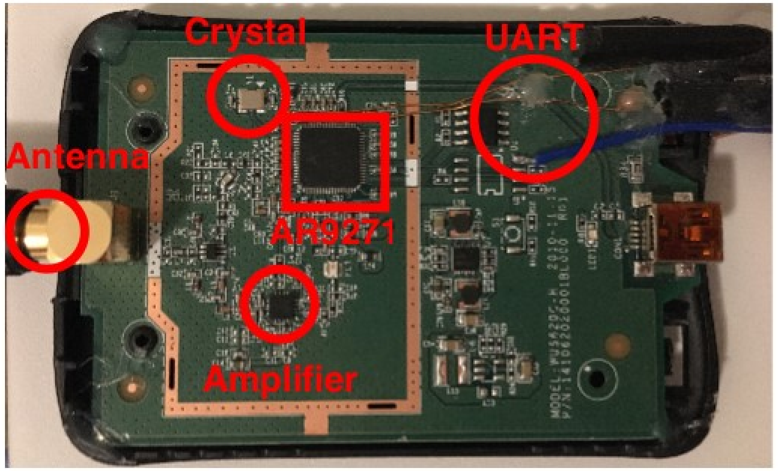


AR9271

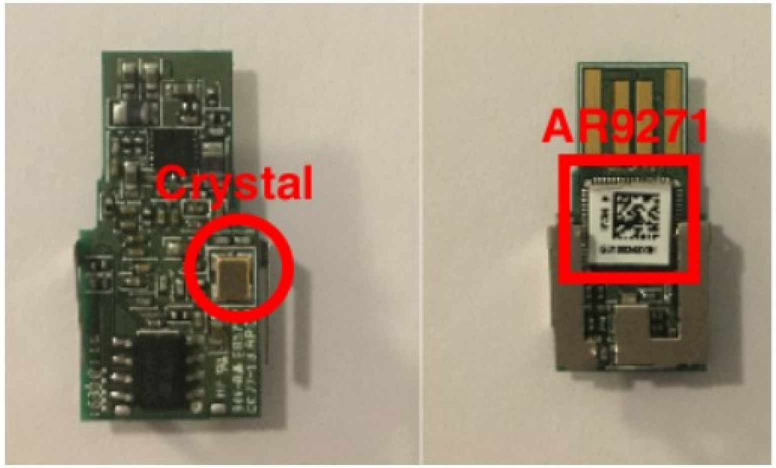


AR9271

Screaming Channels and WiFi (3/3)

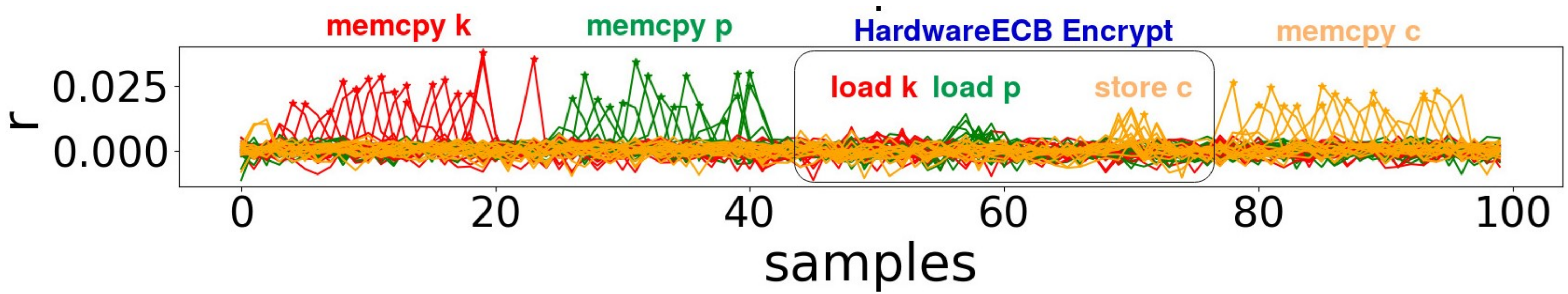


(a) *Alfa Network Long-Range USB Adapter AWUS036NHA*



(b) *Penguin Wireless N USB Adapter (TPE-N150USB)*

Security of the hardware AES block

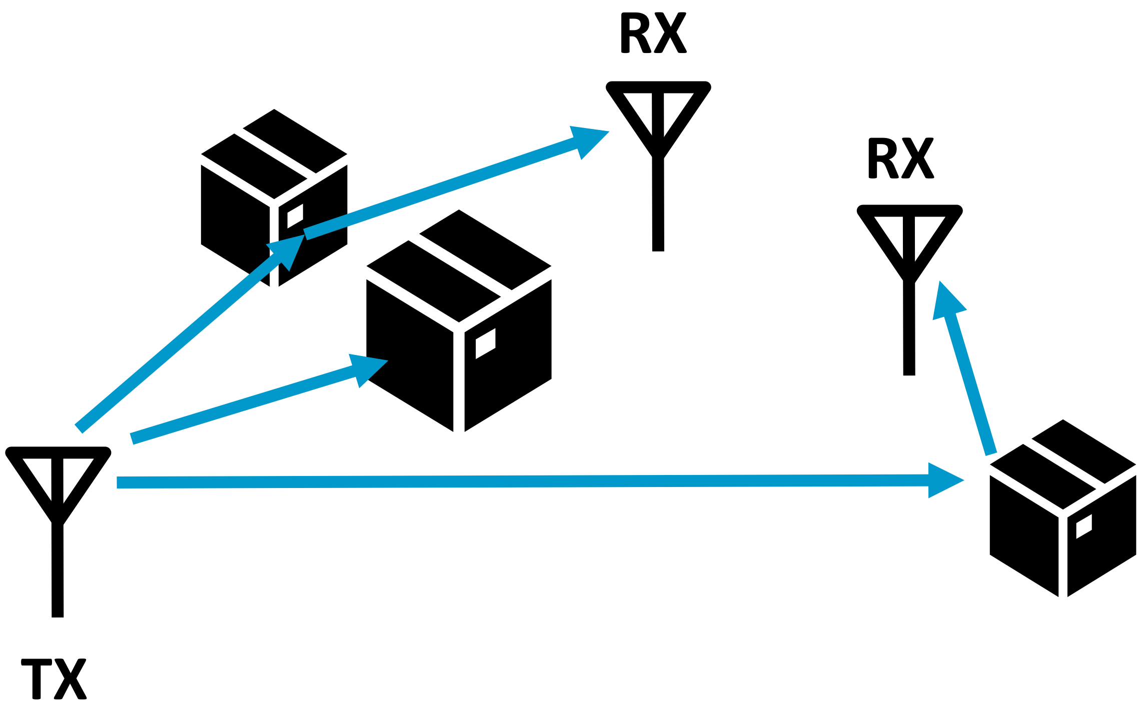


Simple Setup
10cm in office
USRP N210
350k x 100 traces

Leaks from Memory Transfers
Firmware *memcpy* of p,c,k
Hardware DMA of p,c,k
No leak detected inside the AES

Attacks
Only SPA attack are possible
As of now we have not succeeded

Obstacles and spatial diversity



Spatial Diversity

Different paths

Uncorrelated noise

Combine with Maximal Ratio

Attack

55cm in home environment

37k x 500 profiling traces

1990 x 500 attack traces

Rank 2^26

D. G. Brennan, “Linear Diversity Combining Techniques,” Proceedings of the IRE 47, no. 6 (1959): 1075–1102, https://doi.org/10.1109/JRPROC.1959.287136.

Trace Extraction: Quadrature Amplitude Demodulation

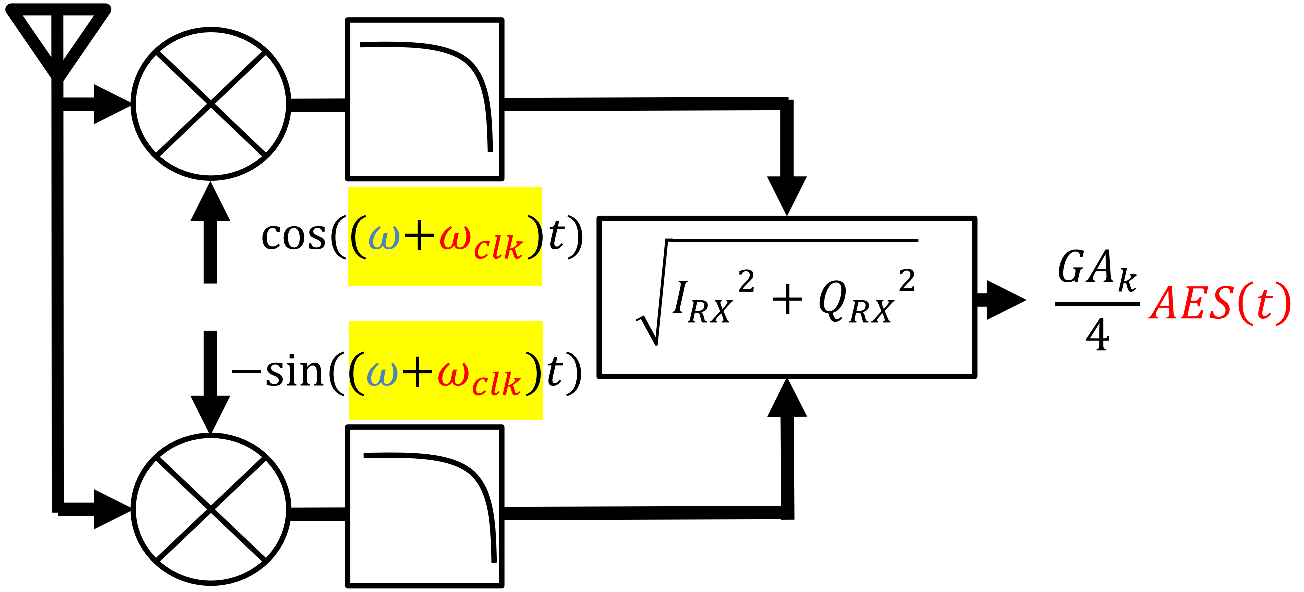
$$GA_k\cos(\omega t + \varphi_k) + \frac{GA_k}{2} AES(t) \cos((\omega+\omega_{clk})t+\varphi_k) + \ldots$$

Main Data — $GA_k\cos(\omega t + \varphi_k)$

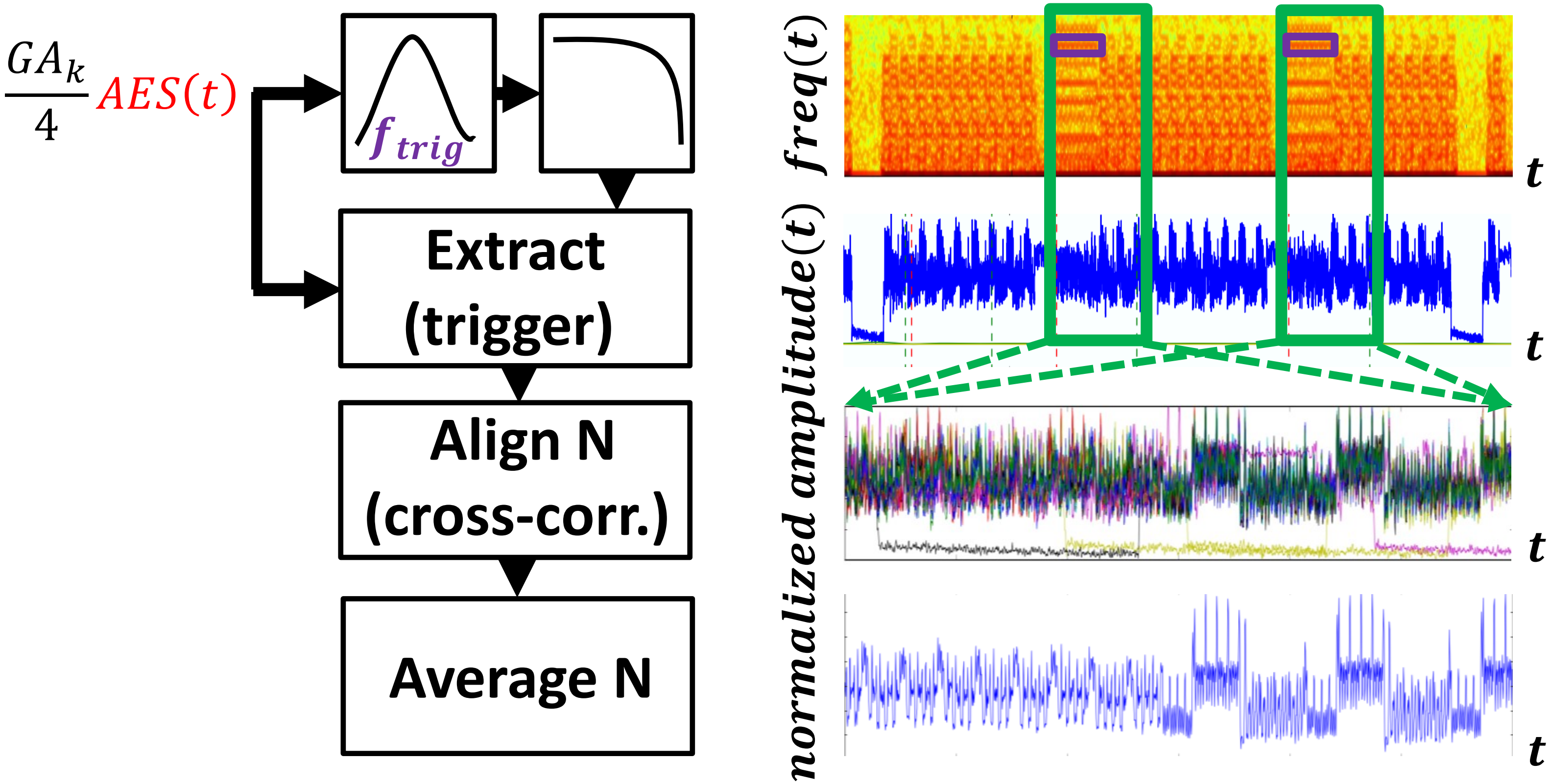
Leak + Data — $\frac{GA_k}{2} AES(t) \cos((\omega+\omega_{clk})t+\varphi_k)$

Yellow: **Separated by n*fclk**
Outside the ISM band
Assume fixed channel
More on hopping later

Green: **Orthogonal Modulation**



Extraction



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

Normalization + Channel Estimation

1. **Z-score normalization inspired by previous work**
2. **Per-trace normalization removes the effect of the channel!**

$$y(t) = Gx(t)$$

$$y' = \frac{y - avg(y)}{std(y)} = \frac{Gx - Gavg(x)}{Gstd(x)} = x'$$

D. P. Montminy et al., “Improving Cross-Device Attacks Using Zero-Mean Unit-Variance Normalization,” J. Cryptographic Engineering 3, no. 2 (2013).

N. Hanley et al., “Empirical Evaluation of Multi-Device Profiling Side-Channel Attacks,” in IEEE SIPS 2014.

O. Choudary and M. G. Kuhn, “Template Attacks on Different Devices,”in COSADE 2014.

M. Abdelaziz Elaabid and S. Guilley, “Portability of Templates,” J. Cryptographic Engineering 2, no. 1 (2012).

Understanding the Leakage

Leakage variable y = SBox(p xor k)

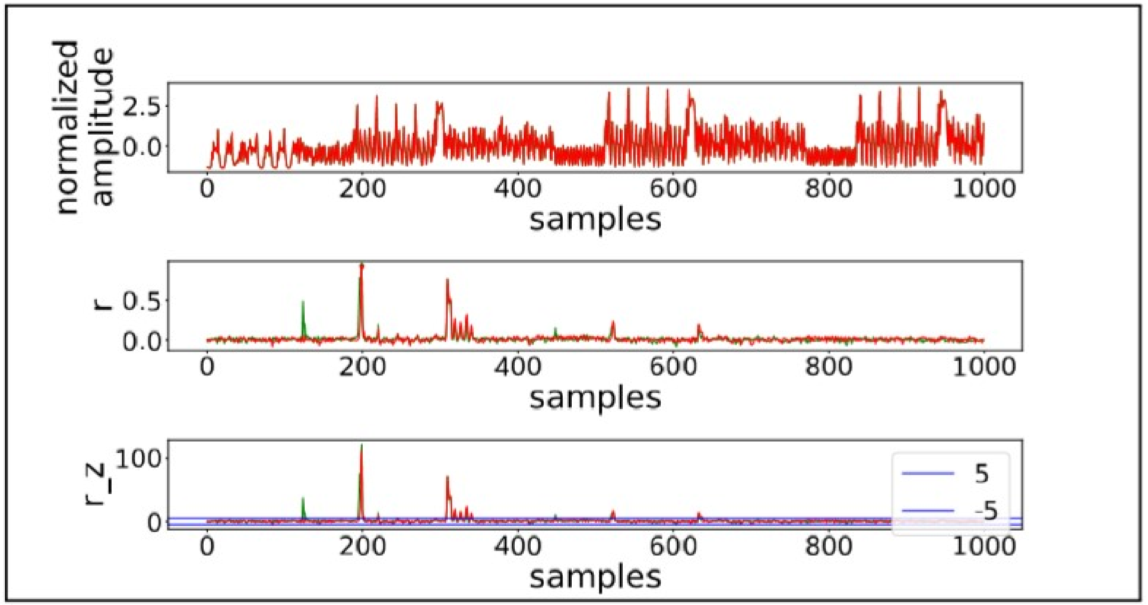
Leakage model m(y) = ~~HW~~[y] model(y) Estimate (nonlinear) leakage model for each y, using the profiling set

Leakage l(y)

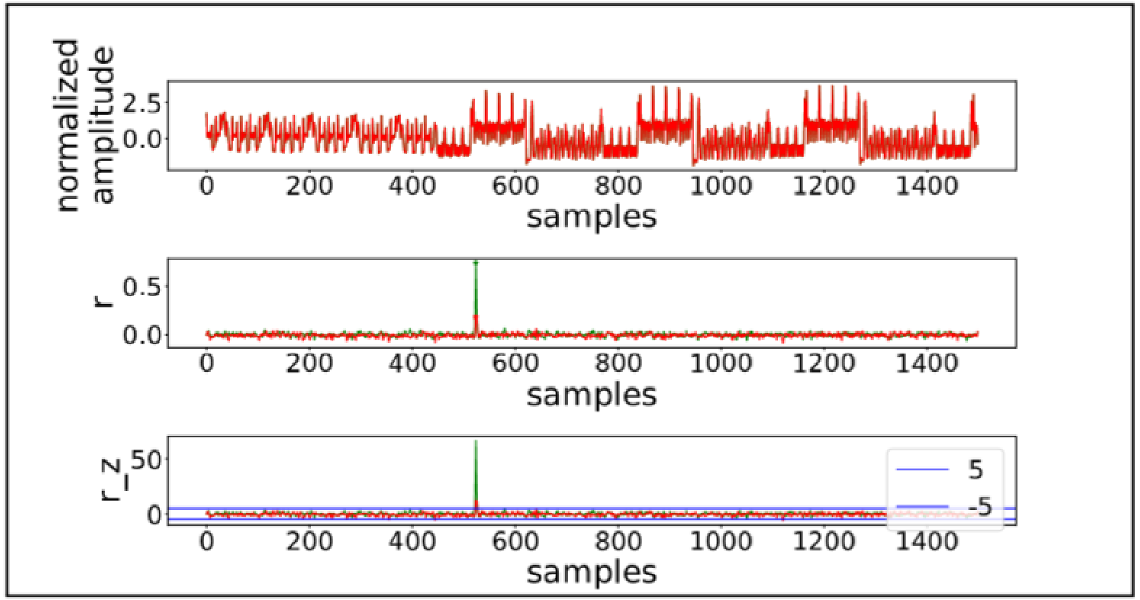
Estimate the linear correlation between m(y) and l(y) on test set

This is the r-test*

*F. Durvaux and F.-X. Standaert, “From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces,” in EUROCRYPT 2016.



(a) ρ-test with $p \oplus k$ (green) and $HW(Sbox(p \oplus k))$



(b) Screaming 10 cm: ρ-test with $p \oplus k$ (green) and $HW(Sbox(p \oplus k))$ (red)

Results for Screaming vs. Conventional

- **Less POIs**
- **Slightly lower but still high correlation**
- **HW is not a good model**

SNR is comparable

But the leakage is distorted

Understanding the Leakage

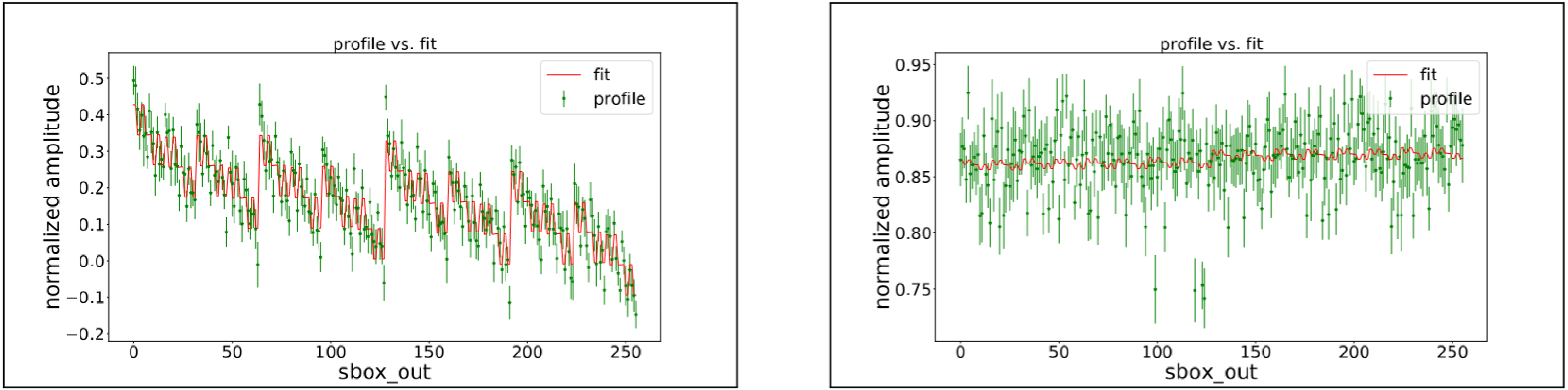
Leakage variable **y** = SBox(p xor k)

Leakage model **m(y)** = ~~HW~~[y] Linear combination of the bits of y

Leakage **l(y)**

Estimate a linear model of the bits of y using linear regression*

*W. Schindler, K. Lemke, and C. Paar, "A Stochastic Model for Differential Side Channel Cryptanalysis," in CHES 2005.



(a) Conventional

(b) Screaming at 10 cm

Results for Screaming vs. Conventional

- **Confirm leakage from Sbox output**
- **Linear model is good for conventional traces**
- **Bad for screaming traces** **The leakage model is nonlinear**

EURECOM

Understanding the Leakage

Leakage variable y

Leakage model m(y)

Leakage l(y)

Templates* can capture a second order relation between m(y) and l(y)

Results for Screaming vs. Conventional

- **Templates attacks are not considerably better than profiled correlation attacks**

First-order leakage (for our sample size)

*S. Chari, J. R. Rao, and P. Rohatgi, "Template Attacks," in CHES 2002.

EURECOM

Conclusion

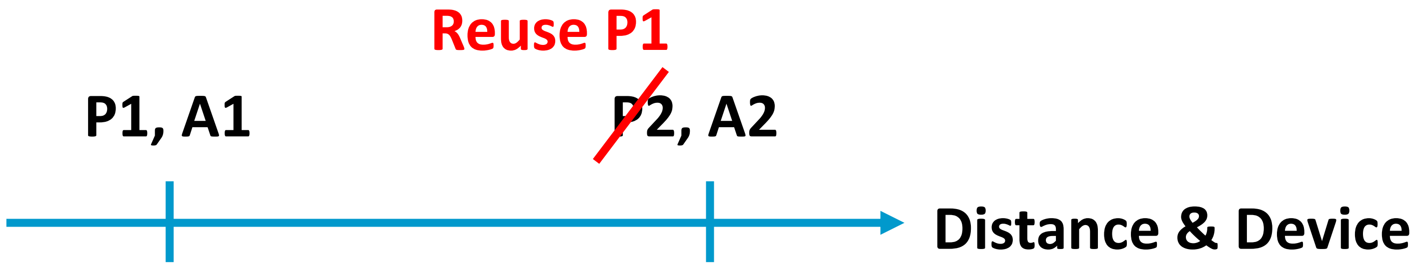
1. **Comparable SNR, distorted leakage model**
2. **Nonlinear leakage model**
3. **First order leakage**

↓

Profiled Correlation Attacks

How To Compare Profiles

#Traces for key recovery given profile P and attack traces A*



$\mathbf{N11} \propto \boldsymbol{r}^{-2}(\boldsymbol{P1}, \boldsymbol{A1})$

~~$\mathbf{N22} \propto \boldsymbol{r}^{-2}(\boldsymbol{P2}, \boldsymbol{A2})$~~

$\mathbf{N12} \propto \boldsymbol{r}^{-2}(\boldsymbol{P1}, \boldsymbol{A2})$

$\boldsymbol{r}(\boldsymbol{P1}, \boldsymbol{A2}) = \boldsymbol{r}(\boldsymbol{P2}, \boldsymbol{A2})\boldsymbol{r}(\boldsymbol{P1}, \boldsymbol{P2})$

The higher the better

*F.-X. Standaert et al., "An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays," Proceedings of the IEEE 94, no. 2 (2006).

Distance, Setup, Channel Frequency, Instance, Time

Distance

- **Quadratic power loss, but we can amplify**
- **Normalization cancels the multiplicative channel gain**
- **No extra distortion (different from conventional*)**

Environment (noise) and setup

- **Bigger role than distance, but we can improve the setup**
- **Some connections are better**

Device instance

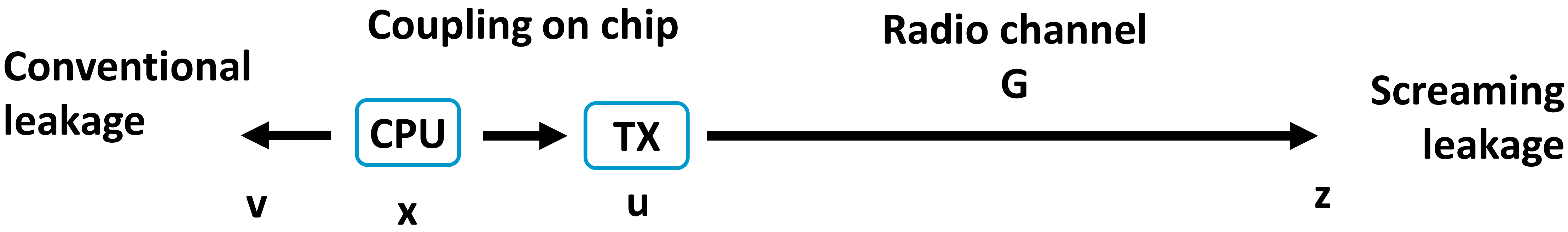
- **No significant impact, per-trace normalization helps**

Big Advantage

- **Profile in good conditions, attack another instance in harsh conditions**

*O. Meynard et al., “Far Correlation-Based EMA with a Precharacterized Leakage Model,” in DATE 2010.

Understanding the SC distorted leakage model



Trace vs side channel signal

Do not confuse them

In general, there is not relation between their SNRs, what about distortion?

Conventional vs. screaming

Can we express a relation between a screaming trace and a conventional trace?

Can we express a relation between the two leakage models?

Can we use a fixed portion of a trace to relate the two?

Simple channel estimation between u and v does not seem to work

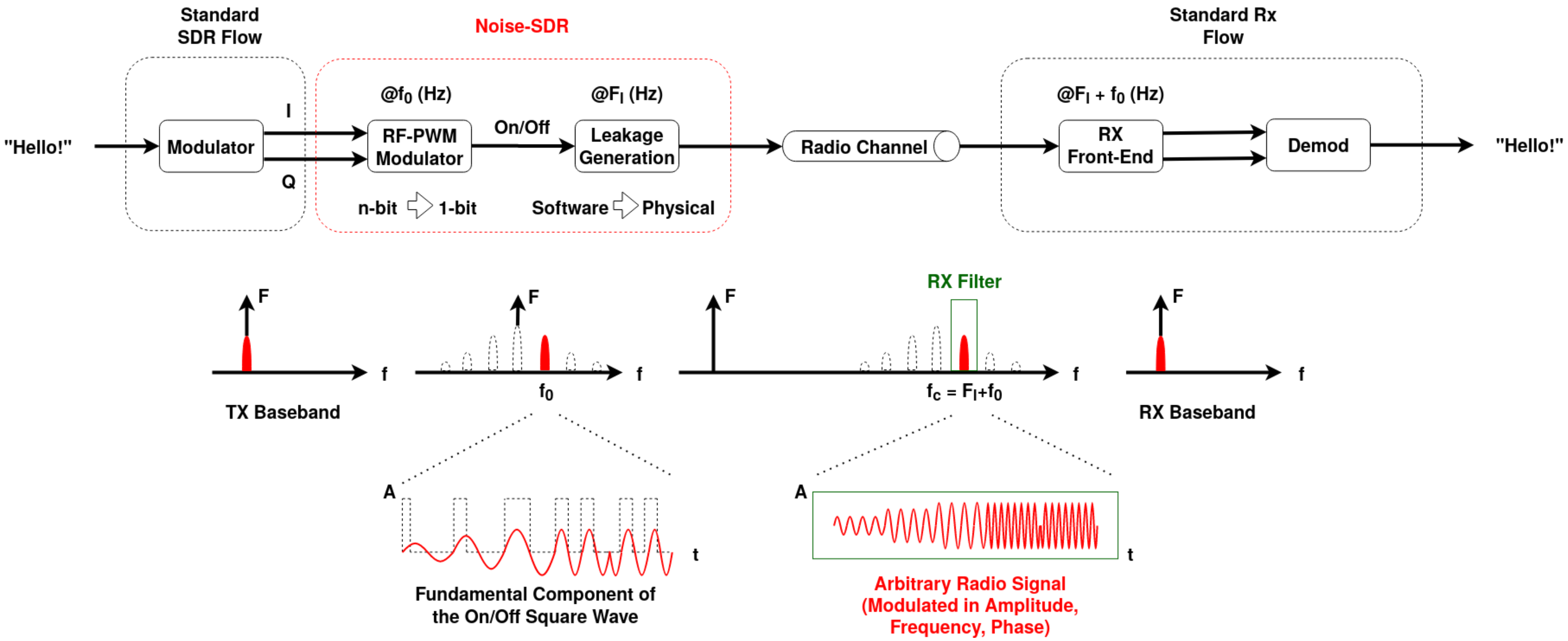
Potential useful application

Conventional profile, screaming attack?

EURECOM

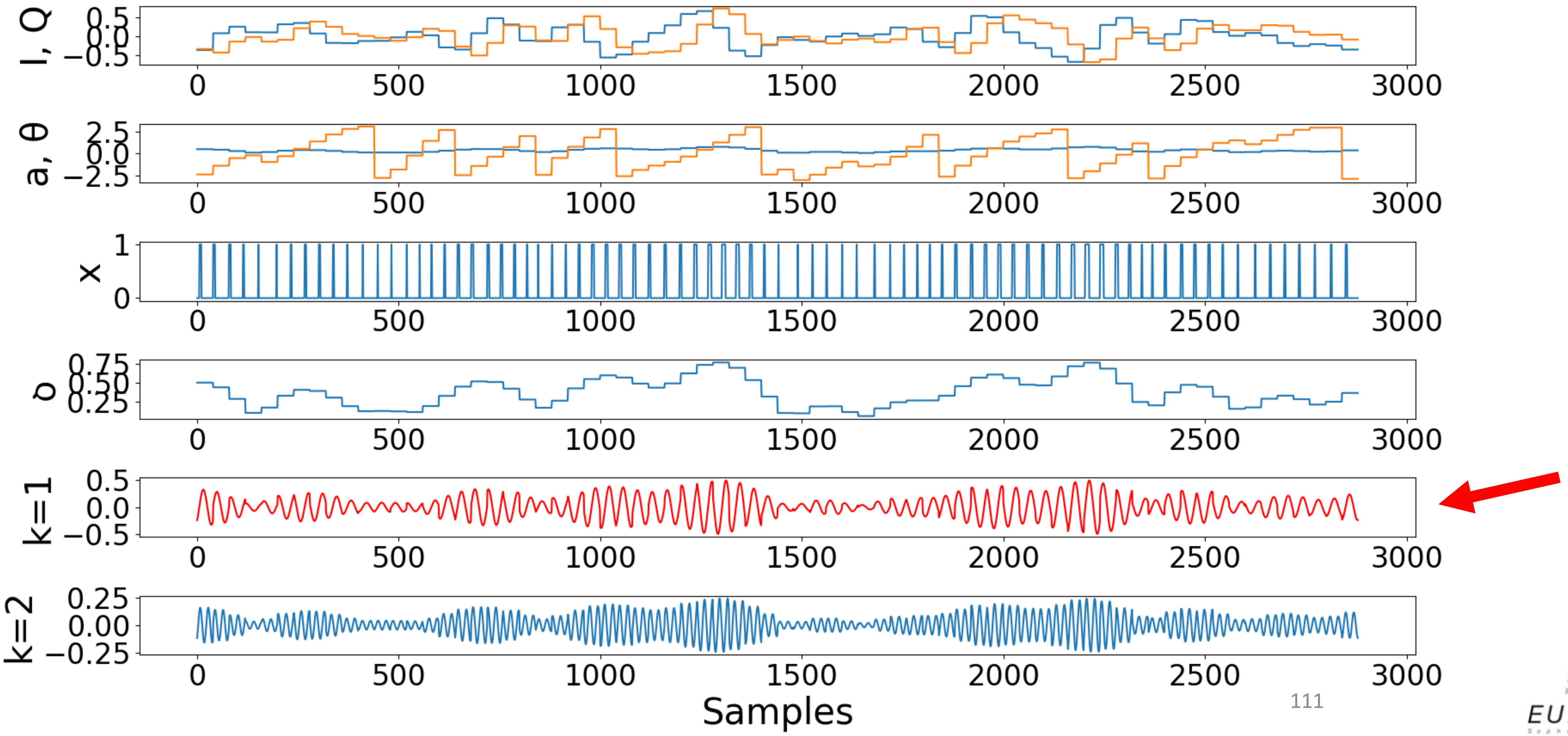
Backup (Noise-SDR)

Intuition: the full chain



EURECOM Sophia Antipolis

Example: HamDRM RF-PWM



EURECOM
Sophia Antipolis

Implementation: discrete-time RF-PWM

Algorithm 1 Baseband to RF-PWM Modulation.

Input: Complex baseband signal x_{bb} sampled at $T_{s_{bb}} = 1/F_{s_{bb}}$, fundamental frequency $IF = f_0$, time resolution $T_{res} = 1/F_{res}$, assuming x_{bb} is normalized and F_{res} is a multiple of $F_{s_{bb}}$

Output: Lists of RF-PWM pulse timings T_{high}, T at resolution T_{res}

```
rep ← T_s/T_res
T_high ← []
T ← []
for k = 0 to len(x_bb) − 1 do
    a_bb[k], θ_bb[k] ← toPolar(x_bb[k])
    a_bb[k] ← arcsin(a_bb[k])/π
end for
for i = 0 to len(x_bb) · rep − 1 do
    x_pwm[i] ← cos(2πf_0 i/F_res + θ_bb[i/rep])
end for
i ← 0
while x_pwm(i) < 0 do
    i ← i + 1
end while
while i < len(x_pwm) do
    t ← 0
    while i + t < len(x_pwm) and x_pwm(i + t) ⩾ 0 do
        t ← t + 1
    end while
    while i + t < len(x_pwm) and x_pwm(i + t) < 0 do
        t ← t + 1
    end while
    T ← [T, t]
    T_high ← [T_high, a_bb[i/res] · t]
    i ← i + t
end while
```

Discrete-time RF-PWM

$$f_0 = \frac{F_{res}}{q}, q \geqslant 2$$

$$\theta_k = 2k\pi f_0 \frac{q}{F_{res}}, q \in \left[-\left\lfloor\frac{F_{res}}{2kf_0}\right\rfloor, \left\lfloor\frac{F_{res}}{2kf_0}\right\rfloor\right)$$

$$a_k = \sin(k\pi q \frac{f_0}{F_{res}}), q \in \left[0, \frac{1}{2k}\frac{F_{res}}{f_0}\right]$$

Future Work

Model the spectrum in detail

Effect of the edges

Effect of interpolation

Effect of jitter

Etc.

EURECOM Sophia Antipolis

Implementation: mathematical modeling

Very large design space

Many variations of RF-PWM with impact on the spectrum properties*

We have chosen those most adapted to our very constrained scenario

E.g., no interpolation of the baseband signal, natural sampling of the IF carrier, …

Some specific properties of noise modulation and injection

Inaccurate time source, with jitter

Properties (e.g., frequency and phase) of the underlying leakage

To which point we can approximate and simplify the desired signal?

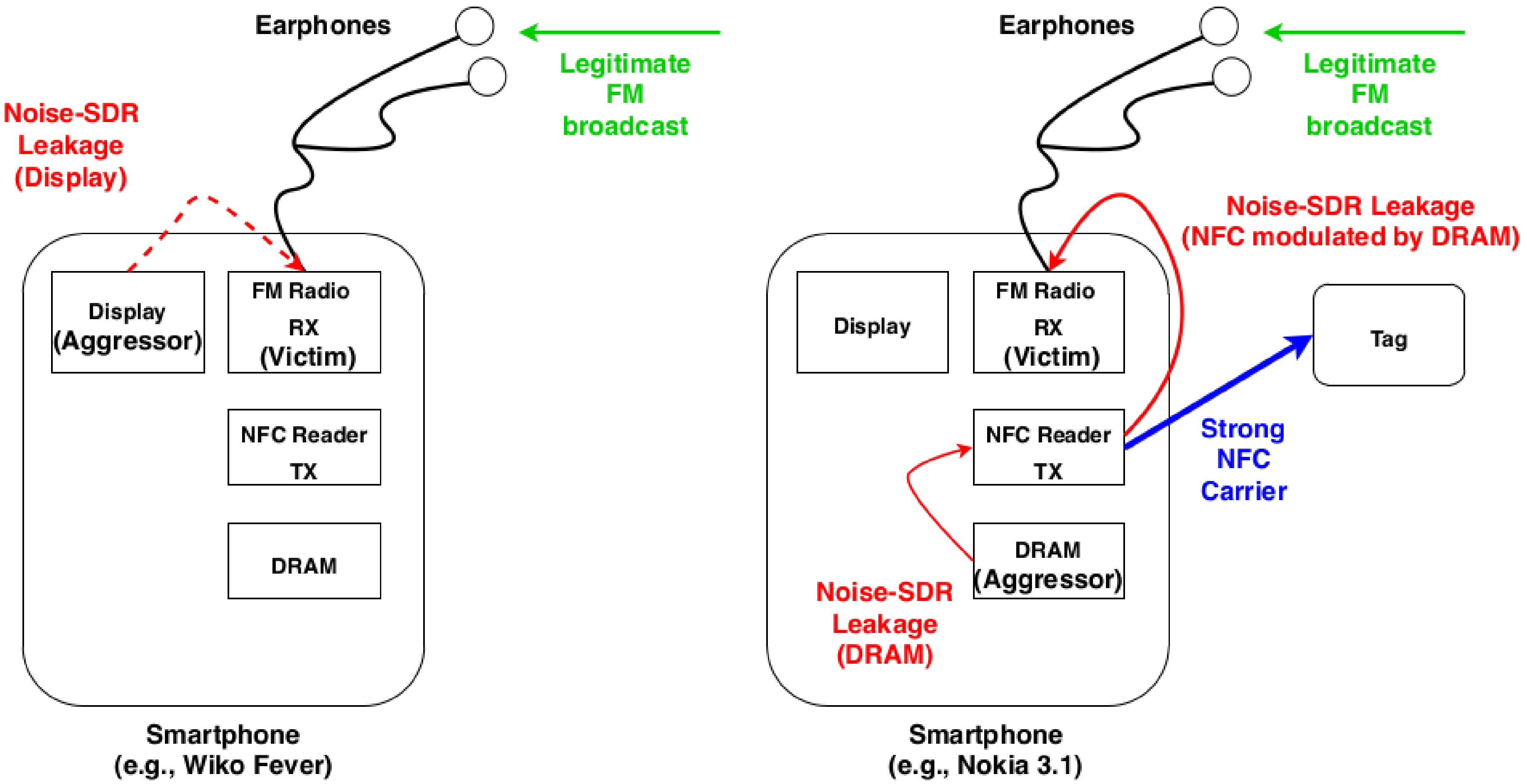
Future work

Model the additional features of RF-PWM applied to noise modulation

Improve signal quality by optimizing some design choices

*P. AJ Nuyts, P. Reynaert, and W. Dehaene, “Continuous-Time Digital Front-Ends for Multistandard Wireless Transmission” (Springer, 2014).

Injection



EURECOM

GPS jamming

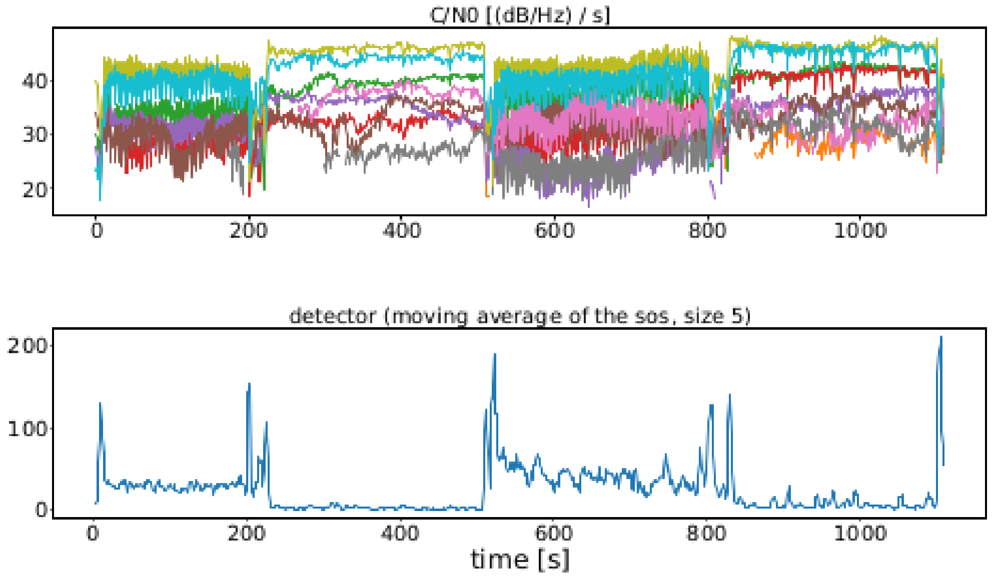


Fig. 11. The sum-of-squares detector catches a degradation of the carrier-to-noise ratio at the *GPS* receiver when the camera is on.

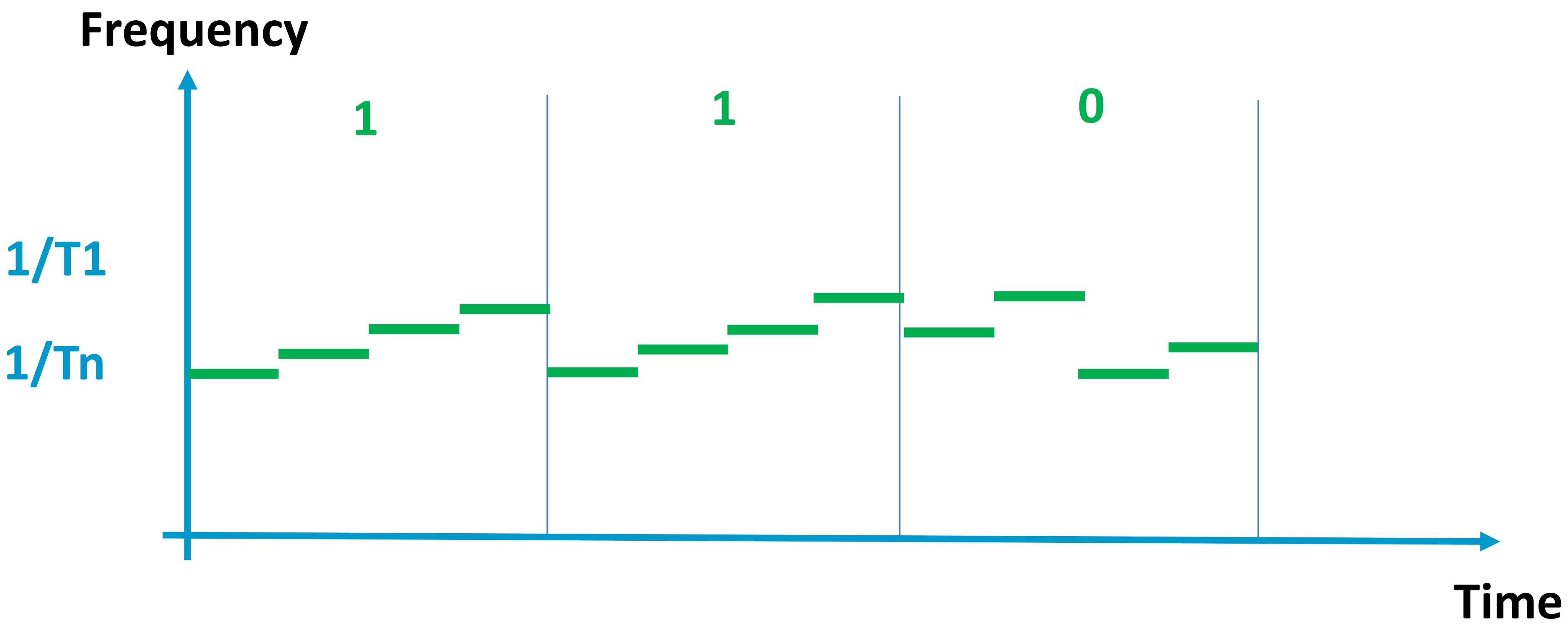
Evaluation: Ham to GLONASS, choose best tradeoff!

Name	Modulation	Bandwidth
Voice AM	AM	10 kHz
Voice FM	NBFM	12.5 kHz
PSK31	2-PSK, USB	31 Hz
2xPSK500	2 2-PSK subcarriers, USB	1.2 kHz
RTTY45.45	2-FSK, USB	170 Hz
MFSK128	M-FSK, USB	1.928 kHz
Olivia 64/2000	M-FSK USB	2 kHz
SSTV	FM, USB	2.5 kHz
HamDRM	QAM, OFDM, USB	2.4 kHz
FT4	4-GFSK, USB	90 Hz
LoRa	CSS	8 kHz (customizable)
GLONASS C/A	DSSS	0.511 MHz

Evaluation: Arm-based smartphones

Model	Architecture	LPDDR	Frequency	Harmonics n	Bandwidth	Tested Protocols
Innos D6000	ArmV8-A	3	400 MHz	$1-4$	few MHz	All but *HamDRM*, $n = 2$
Nokia 3.1 (TA-1063)	ArmV8-A	3	13.56 MHz (*NFC*)	7	few kHz	*PSK31*, $n = 7$
Samsung Galaxy A30S (SM A397FN)	ArmV8-A	4	1794 MHz	1	few MHz	*GLONASS C/A*, $n = 1$
Samsung S7 Exynos (SM-G930F)	ArmV8-A	4	1794 MHz	1	few kHz	Simple tunes and chirps
Samsung Galaxy S5 Mini (SM G800F)	ArmV7-A	n.a.	200 MHz	1-11,13-19,26	tens of kHz	All but *GLONASS*, $n = 1$
Samsung M31 (SM-M315F/DSN)	ArmV8-A	4	1794 MHz (rare)	1	few MHz	*NBFM*
Samsung Galaxy J7 (SM-J730FM)	ArmV8-A	3	None identified	-	-	-
Samsung Galaxy Young (GT-S6310N)	ArmV7-A	n.a.	None identified	-	-	-
Sony Xperia C5 (E5533)	ArmV8-A	4	400 MHz	1-11	few MHz	*NBFM*, *LoRa*, $n = 6$
Sony Xperia X (F5121)	ArmV8-A	3	None identified	-	-	-
Motorola Moto E6S	ArmV7-A	3	400 MHz	1,2	few kHz	Simple tunes and chirps
Google Nexus 5 (D821)	ArmV7-A	2	200 MHz	$1-5, 8, 12$ $16, 20, 24$	tens of kHz	*NBFM*, *MFSK128*, *FT4*, *SSTV*, *Olivia*, *LoRa*, $n = 1$
Google Pixel XL	ArmV8-A	4	None identified	-	-	-
Google Pixel 2	ArmV8-A	4	None identified	-	-	-
Wiko Fever	ArmV8-A	3	None identified	-	-	-
Huawei P8 Lite (PRA-LX1)	ArmV8-A	3	None identified	-	-	-
Huawei P10 (VTR-L09)	ArmV8-A	4	None identified	-	-	-
Huawei P8 SE (GRA-L09)	ArmV8-A	3	None identified	-	-	-
OnePlus 7 Pro PE (GM1913)	ArmV8-A	4	None identified	-	-	-

Concurrent work: LoRa-like Chirp Spread Spectrum



CCS (Simplified)

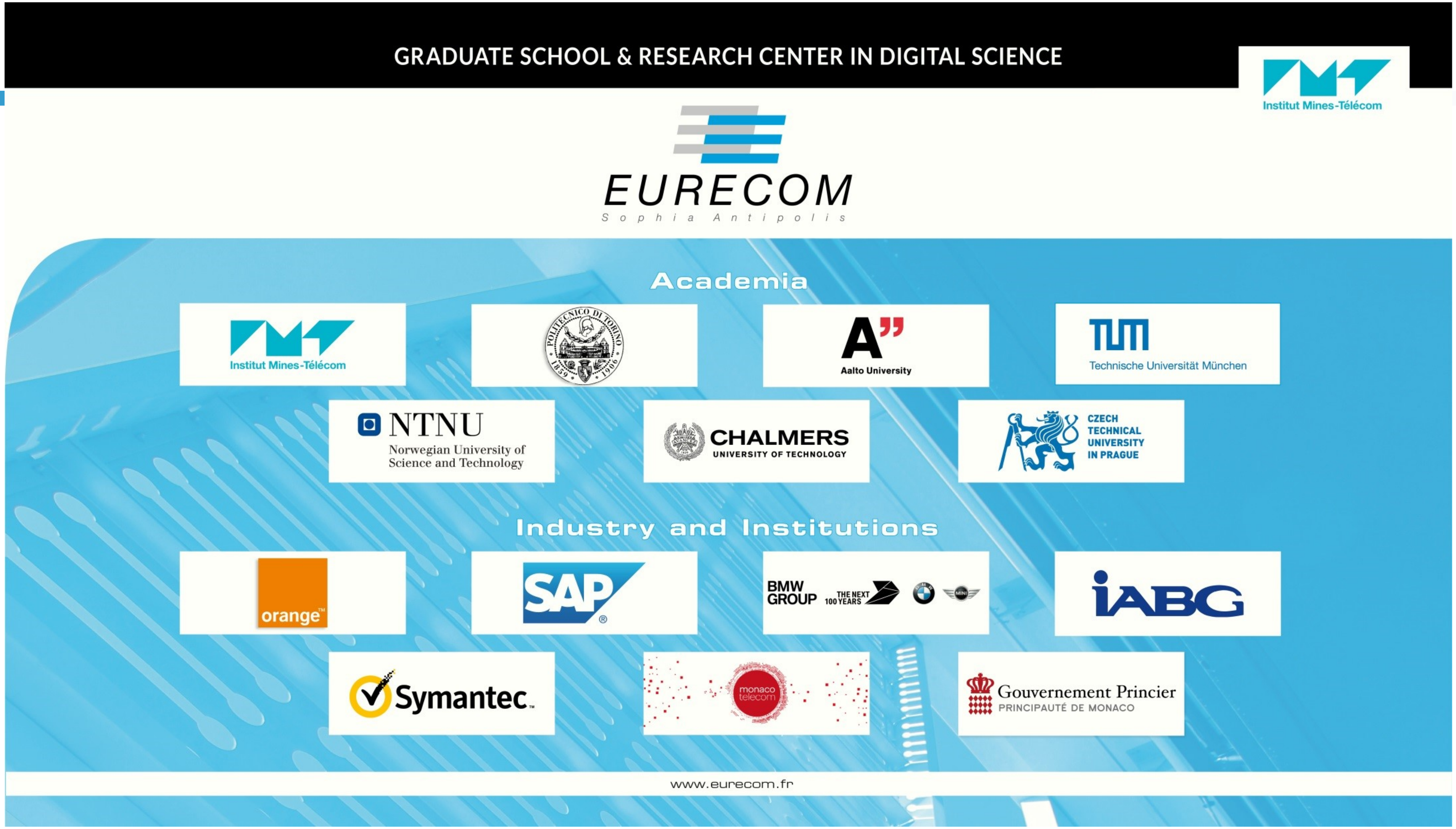
C, Shen et al., “When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient”, IEEE S&P 2021

Acknowledgements

We would like to thank:

- The SeCiF project within the French-German Academy for the Industry of the future, the DAPCODS/IOTics ANR 2016 project (ANR-16-CE25-0015).
- The COST action CRYPTACUS.
- Google for the Faculty Award assigned to Aurélien Francillon.
- The R2Lab at Inria for their support with measurements in their anechoic chamber.

EURECOM
Sophia Antipolis


GRADUATE SCHOOL & RESEARCH CENTER IN DIGITAL SCIENCE
Institut Mines-Télécom
EURECOM
Sophia Antipolis
Academia
Institut Mines-Télécom
Aalto University
Technische Universität München
NTNU
Norwegian University of Science and Technology
CHALMERS
UNIVERSITY OF TECHNOLOGY
CZECH TECHNICAL UNIVERSITY IN PRAGUE
Industry and Institutions
orange
SAP
BMW GROUP
THE NEXT 100 YEARS
iABG
Symantec.
monaco telecom
Gouvernement Princier
PRINCIPAUTÉ DE MONACO
www.eurecom.fr