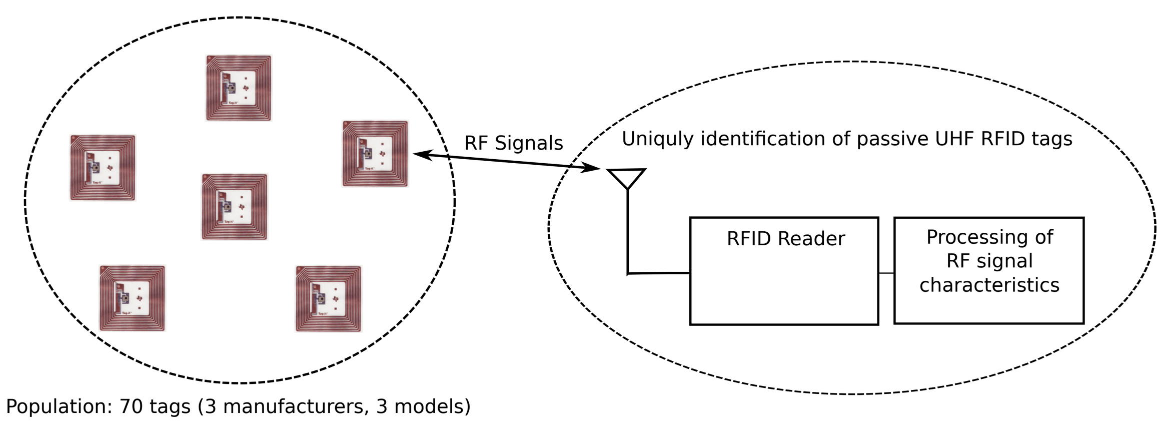
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

System Security Group

# Physical-layer Identification of UHF RFID Tags

## Problem Statement

- We explore the unique identification of passive UHF RFID tags.
- We mainly consider same model, same manufacturer tags.
- Identification is based on physical-layer device identification techniques, i.e., by considering physical characteristics, or *features*, of RF signals.




## Results - Highlights

**Time domain features**

- 50 tags, same model, same manufacturer.
- Distances from up to 6m.
- Different tag orientations and communication powers.
- Classification: Accuracy=71.4%.

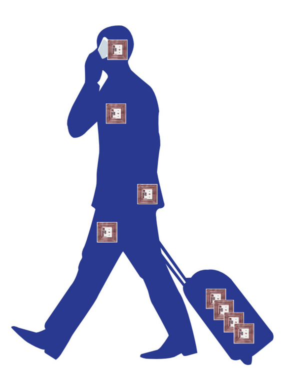
**Spectral features**

- 50 tags, same model, same manufacturer.
- Controlled environment.
- Identification: EER=0.0%.
- Classification: Accuracy=99.6%.

## Implications: Tracking & Cloning Detection

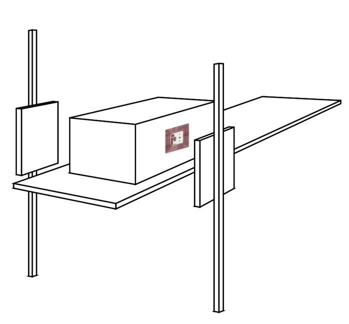
- Our work is the first that shows that tracking of passive UHF RFID tags is possible with high accuracy from their operating distance (i.e., within 6 meters).

→ Tracking is possible despite most privacy-preserving countermeasures on upper communication layers.

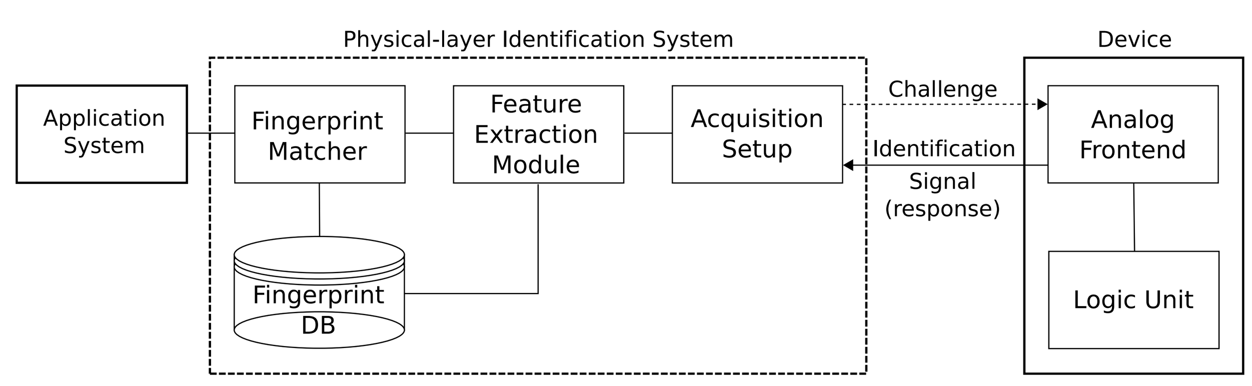


- Our work shows that, in controlled environments, it is possible to achieve highly-accurate classification and identification.

→ This result motivates the use of physical-layer identification for the detection of product cloning in RFID-enabled supply chain.

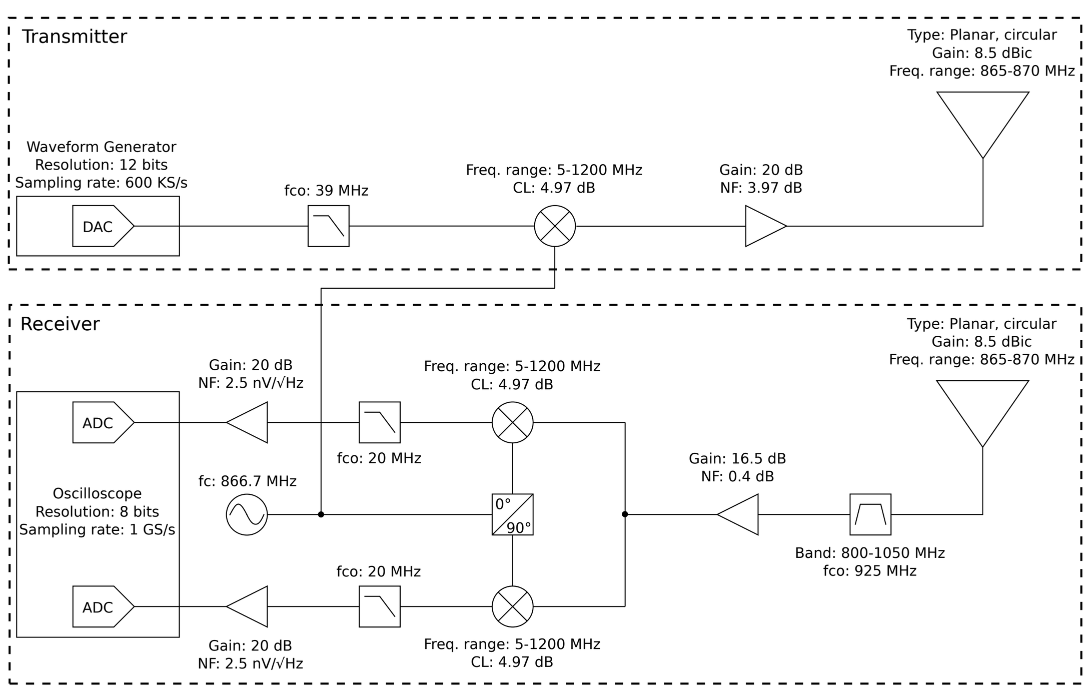


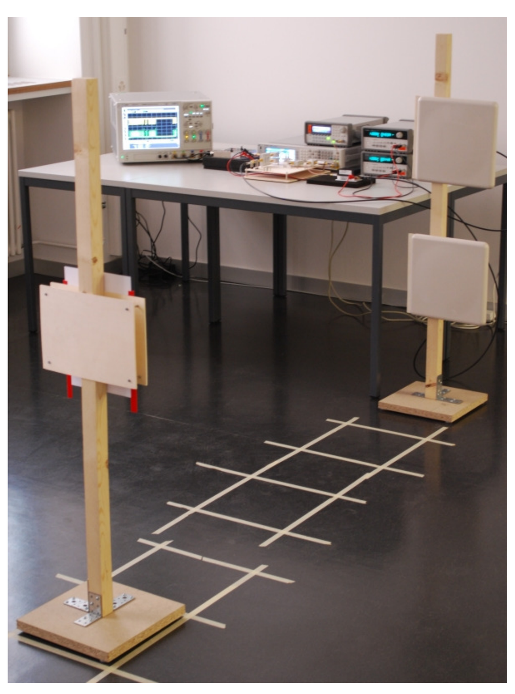
## Physical-layer Device Identification



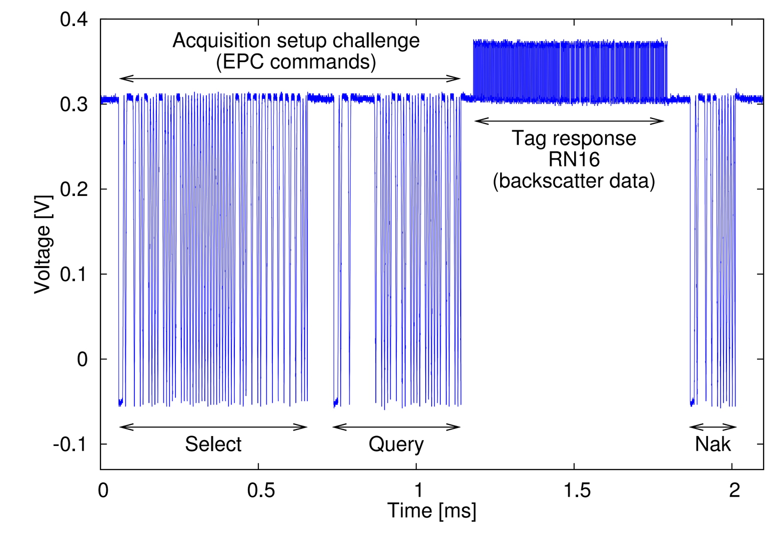

- Physical-layer device identification systems aim at identifying (or verifying the identity of) devices or their affiliation classes based on characteristics of devices that are observable from their communication at the physical layer.

## Acquisition Setup



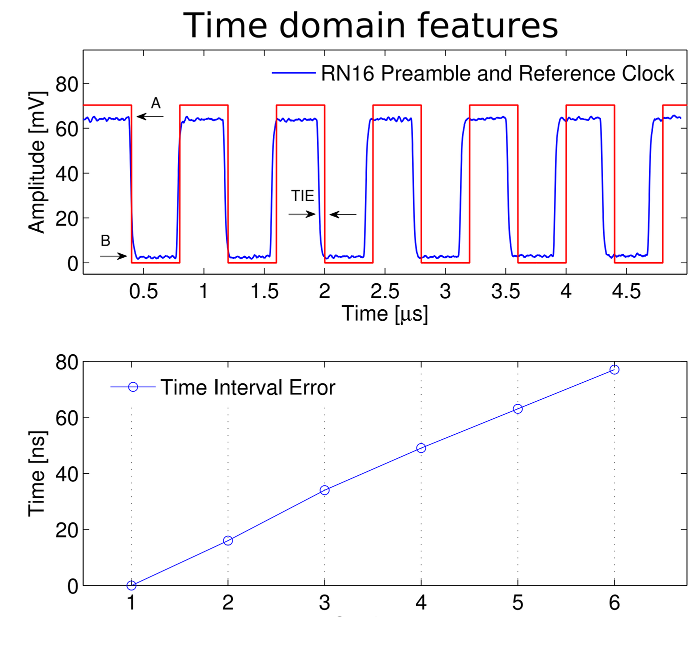



- Tags are challenged by our acquisition setup to initiate an inventory round (to obtain their ID).
- Tag responses are then collected and digitalized at the baseband for feature extraction and fingerprint matching.

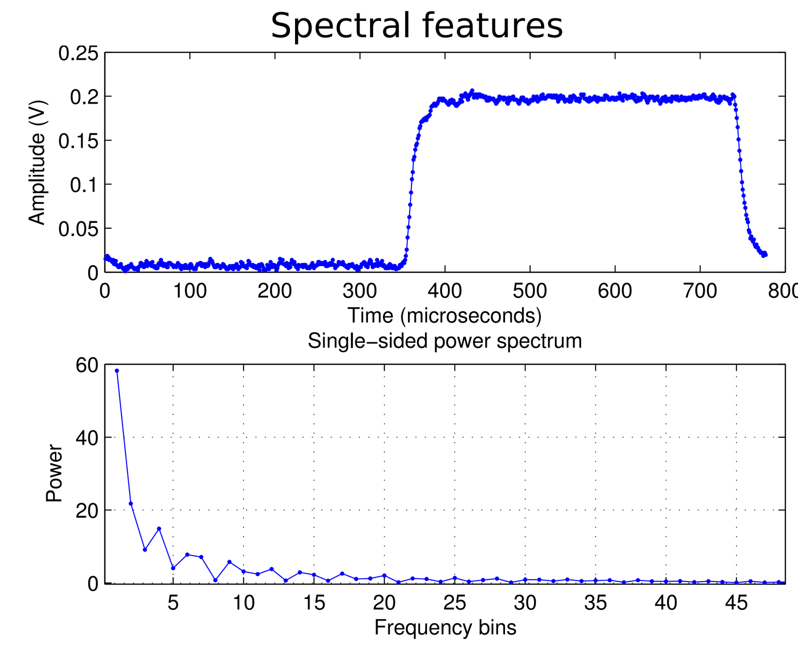



## Feature Extraction and Fingerprint Matching

Time domain features



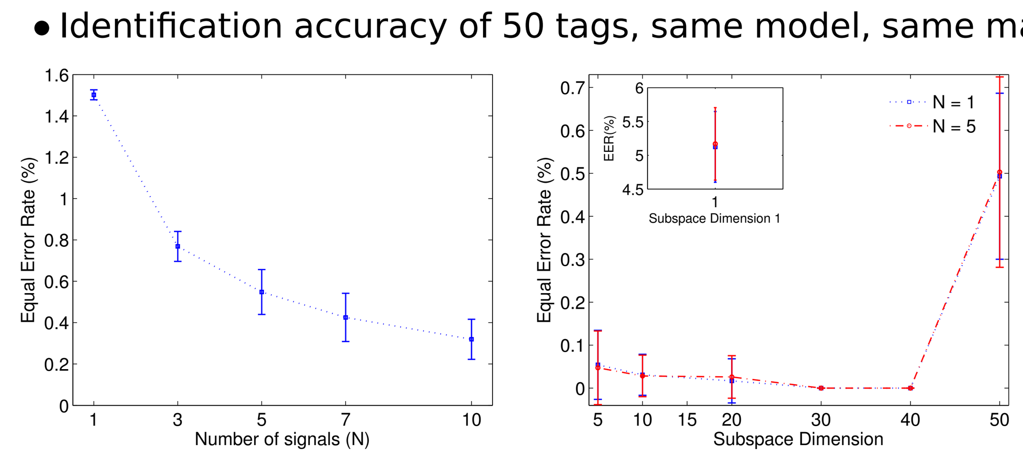

Spectral features




- Time domain features are based on the first derivate $\partial_{TIE}$ of the Time Interval Error (TIE), which measures how far each active edge of a signal, i.e., of a tag response, varies from its ideal position.
- Spectral features are based on the Fast Fourier Transform (FFT) and consider the spectrum of each cycle in a tag response.
- In time domain, we consider two additional features: the average baseband power $\bar{P}_B$ for all cycles in a tag response and the combination of $\partial_{TIE}$ and $\bar{P}_B$.
- For time domain features, fingerprints include one of $\partial_{TIE}$, $\bar{P}_B$ or $(\partial_{TIE}, \bar{P}_B)$. Two fingerprints are matched with Euclidean distance. For spectral features, Principal Component Analysis (PCA) is used to extract fingerprints and Mahalanobis distance to match fingerprints.

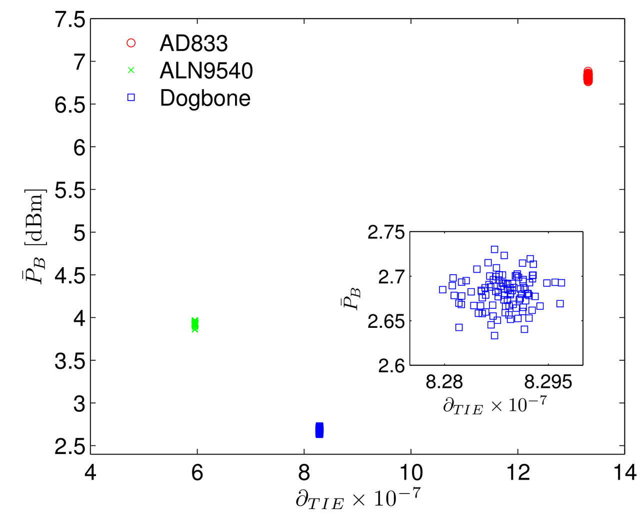
## Detailed Performance Results

- Identification accuracy of 50 tags, same model, same manufacturer.




| Feature | Classification Rate (%) |
|---|---|
| $\partial_{TIE}$ | 71.4 (69.7; 73.0) |
| $\bar{P}_B$ | 43.2 (38.6; 47.7) |
| $(\partial_{TIE}, \bar{P}_B)$ | 98.7 (98.0; 99.4) |
| Spectral | 99.6 (99.3; 99.9) |

- Identification accuracy on different models: 30 tags, 3 different models and manufacturers.




| | Classification Rate (%) | | |
|---|---|---|---|
| Feature | AD833 | Dogbone | ALN9540 |
| $\partial_{TIE}$ | 72.5 | 72.4 | 99.6 |
| $\bar{P}_B$ | 99.9 | 53 | 72.6 |
| $(\partial_{TIE}, \bar{P}_B)$ | 99.9 | 93 | 100 |
| Spectral | 100 | 96.9 | 100 |

- Feature stability: 10 tags (same model and manufacturer), 10 different configurations of tag position, orientation, and transmission power. Additionally, the acquired signals are down-sampled by a factor of 10.

| | Classification Rate (%) | | |
|---|---|---|---|
| Feature | Nominal configuration | Different configurations | Reduced sampling rate (100 MS/s) |
| $\partial_{TIE}$ | 99.8 (99.5; 100) | 96.4 (95.01; 97.86) | 99.88 (99.49; 100) |
| $\bar{P}_B$ | 64.6 (56.9; 72.3) | 15.92 (14.49; 17.35) | 60.25 (54.28; 66.22) |
| $(\partial_{TIE}, \bar{P}_B)$ | 100 (100; 100) | 36.24 (26.73; 45.75) | 100 (100; 100) |
| Spectral | 100 (100; 100) | 37.6 (18.5; 56.8) | 100 (100; 100) |

## References

D. Zanetti, B. Danev and S. Čapkun, "Physical-layer Identification of UHF RFID Tags", In Proceedings of the 16th Annual International Conference on Mobile Computing and Networking (ACM MobiCom), 2010.

Davide Zanetti, Boris Danev and Srdjan Čapkun
{zanettid, bdanev, capkuns}@inf.ethz.ch, System Security Group, Department of Computer Science, ETH Zurich, Switzerland