With funding from the:

Federal Ministry
of Research, Technology
and Space

ConnRAD – Connectivity and Resilience for Automated Driving

Final Presentation 23.10.2025

ConnRAD
Connectivity & Resilience for automated Driving Functions in Germany

Hardware Security for Latency-Constrained Systems

Franz Dielacher, Egla Derraj, Hans-Dieter Wohlmuth, Patrick Weissensteiner, Infineon Technologies AG (IFAG)
Udo Steininger (TÜV-Süd), Alexander Geraldy (Bosch), Frank Kargl (UULM), Nils Gehrke (TUM)

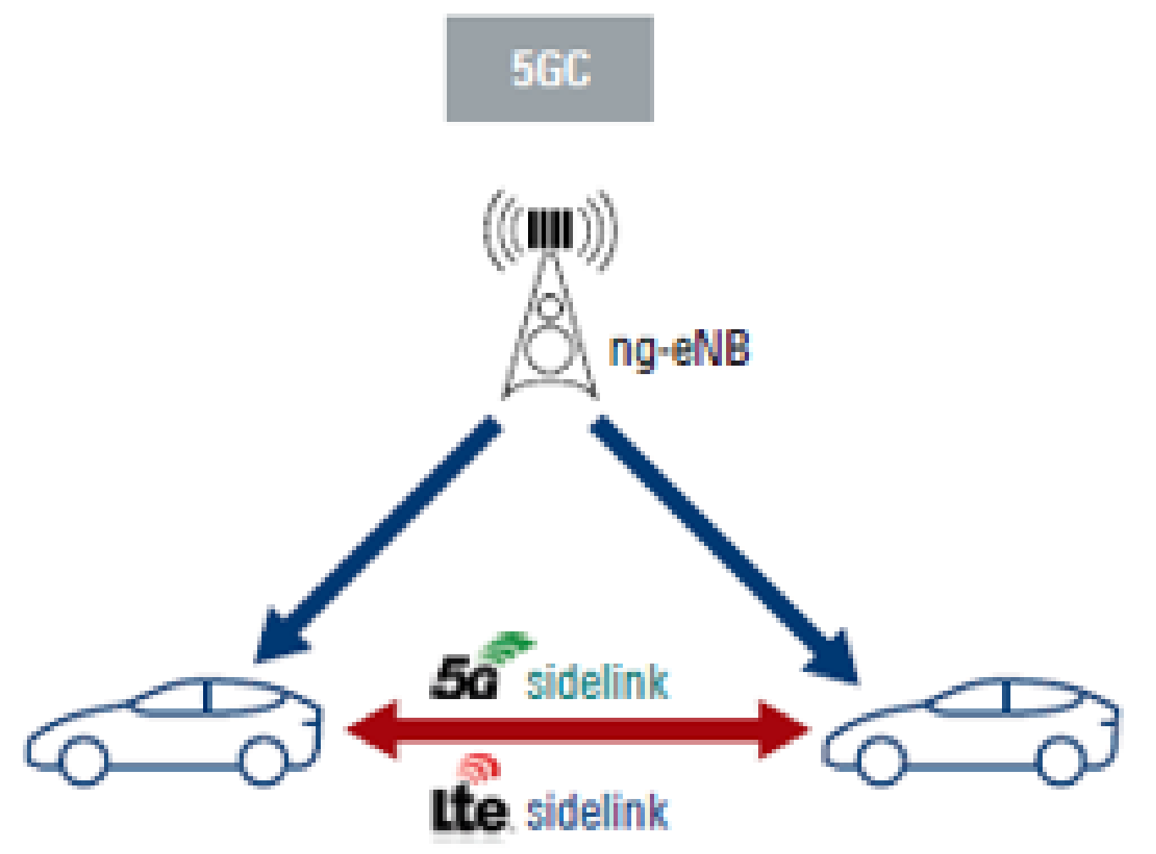
Security and authentication in V2X technologies

C-V2X: Update of the security architecture was necessary due to the change from network based to direct communications

Relevant for physical layer authentication:

- Message authentication is an important mechanism to verify the origin of a received V2X message
- On the sidelink, there is a tradeoff between secure communications on one hand and fast, low-latency communications on the other

Closed/open world V2X System



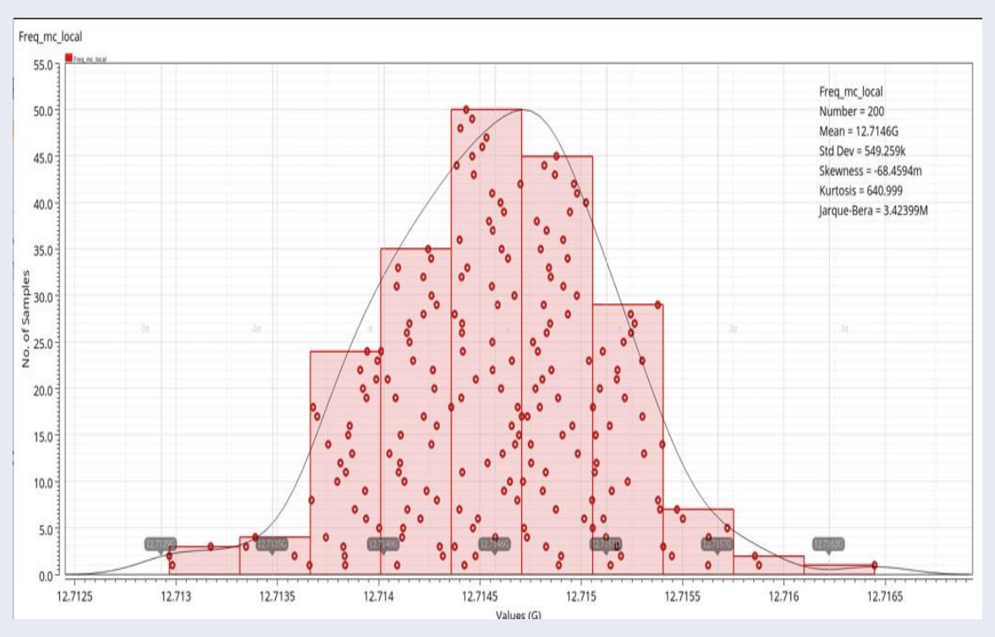
- Protocol-based security approaches show their limitations
- 5G-AKA primary authentication may fail

RF fingerprint state of the art

- RF fingerprinting is still in its infancy, and much research is needed to further improve the detection capabilities
- Very narrow RF fingerprint identification space through **native process variations**
- Deep learning models and transfer learning are used to train the RF fingerprinting models
- Experiment results reveal that classification accuracy strongly depends on hardware quality
- For low-end radios an accuracy of **99%** is achievable but for high-end radios, the accuracy decreased to **below 50%**
- Relevant parameters like temperature and ageing not properly taken into consideration

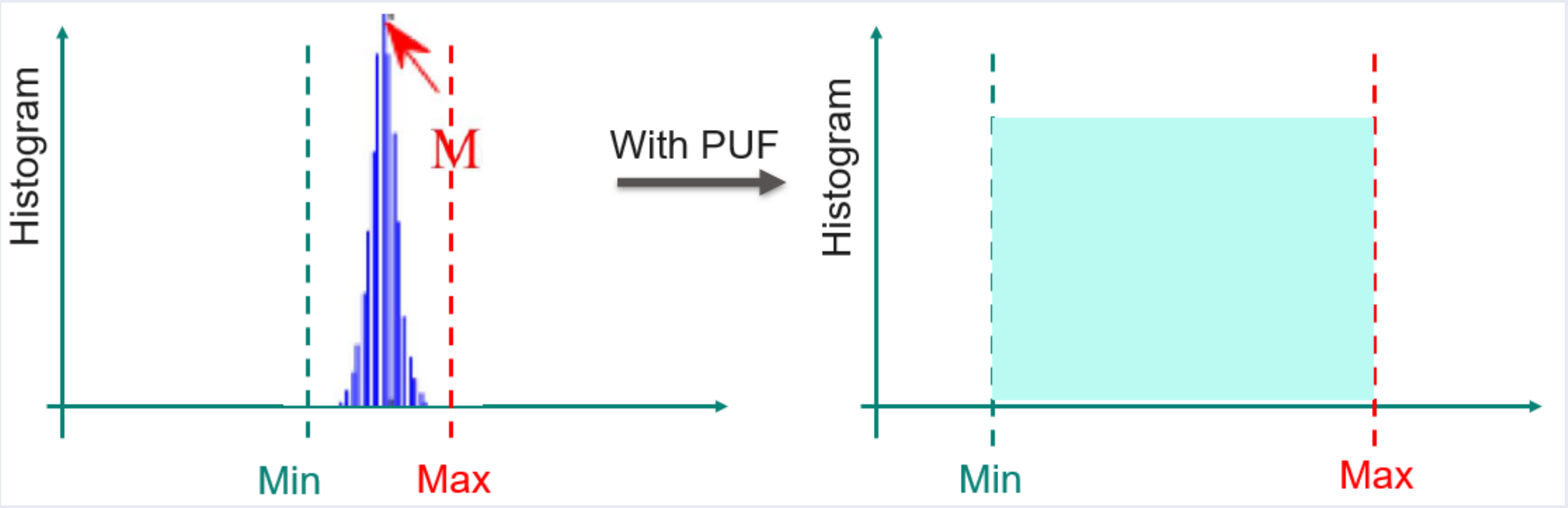
Include PUF-based security engine to enlarge the identification space

PUF-based digital security engine to improve RF-Fingerprint identification space



Very narrow RF-Fingerprint identification space through native process variations: Frequency variation: Mean = 12.7146GHz, **Std Dev = 549.25kHz**

On-chip digital PUF-based security engine enables control of the RF-Fingerprint probability distribution and enlarges the identification space beyond native process variations



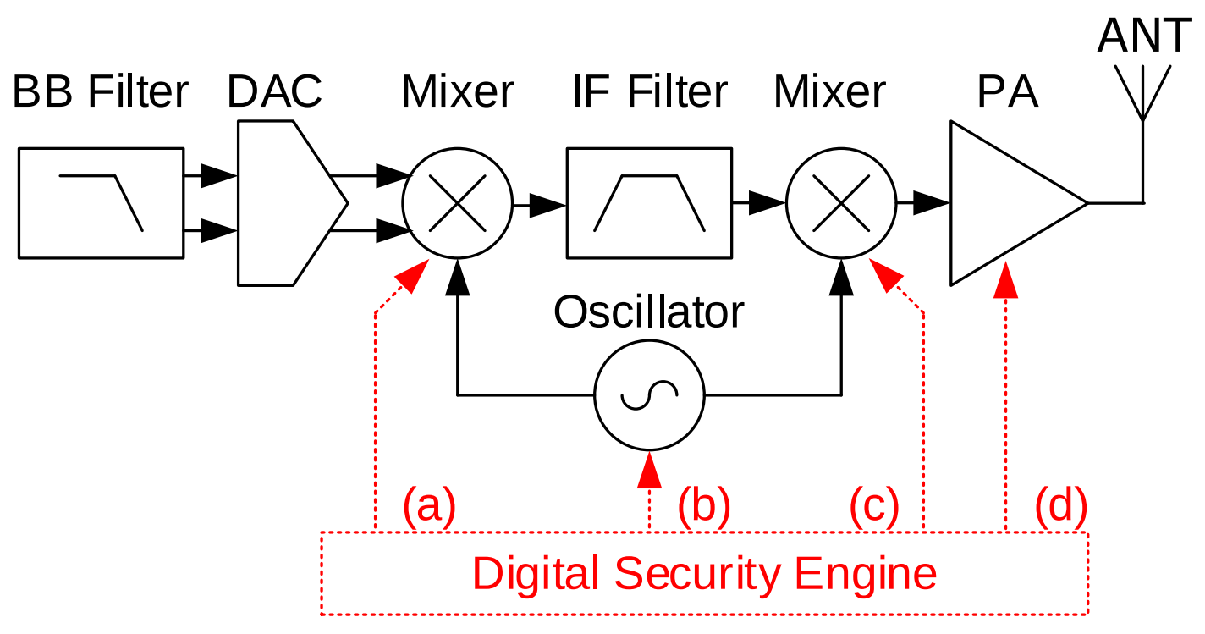
RF fingerprint and physical unclonable function (PUF) for fast authentication

- Device identification is the first line of defense to detect and stop fraud
- RF fingerprint is an analog/RF hardware signature based on native process variation
  - Issues: very narrow probability-density of process variation, temperature, supply, ageing effects
- PUF is a “hardware cryptogram” based on digital hardware encryption
  - Issues: May require error correction mechanisms, especially for unstable responses
- RF fingerprint and PUF can be combined to achieve fast and secure authentication and encryption
- PUF can be used to amplify RF signature
  - Issue: digital security engine required in the transmitter

Focus on RF fingerprinting for fast authentication

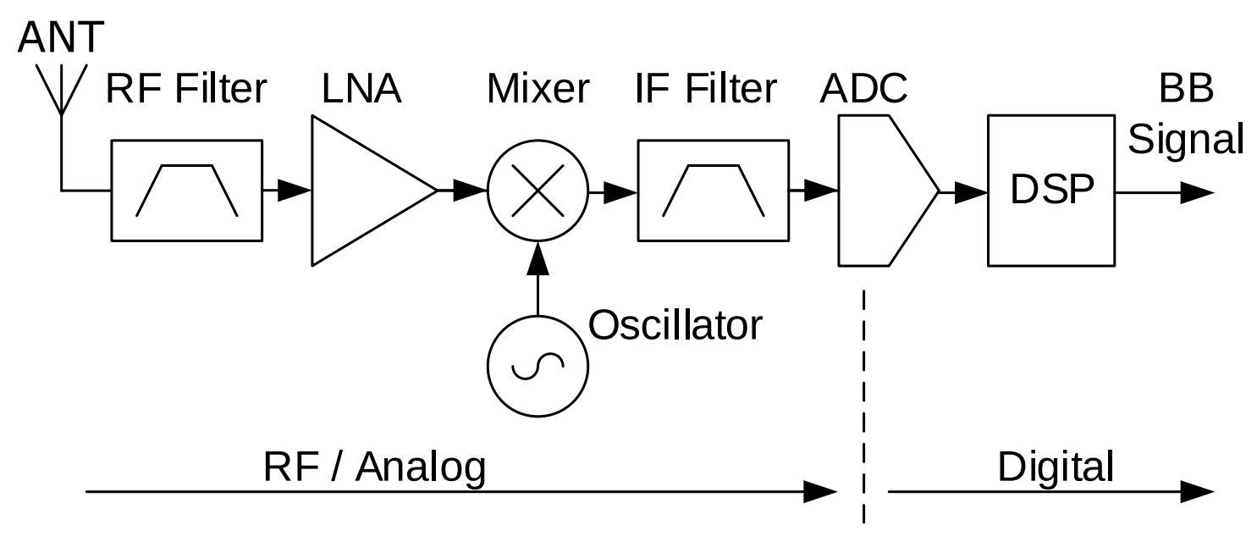
Data throughput, latency and signal integrity are well established properties of the RF frontends, data security and trustworthiness comes on top

RF Transmitter block diagram



Digital security engine to amplify the native process variation effect

RF Receiver block diagram



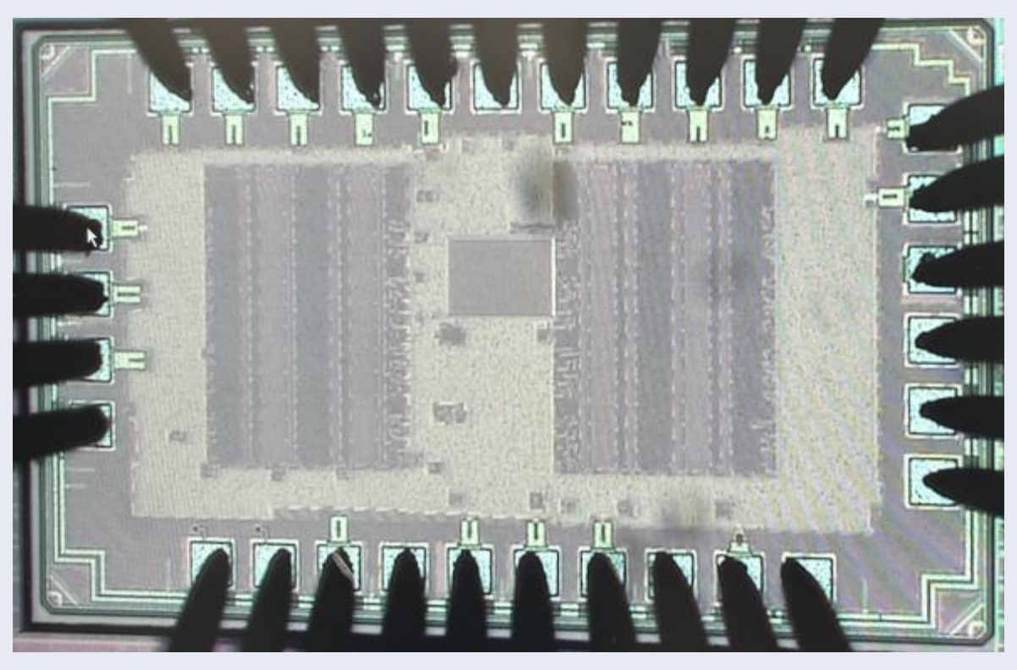
RF-Signal with signature:

- Introduce PA Non-linearity
- Introduce I/Q Mismatch
- Introduce LO Frequency variation

RF-Fingerprint detection:

- Time domain RFF
  - Phase, step-change, …
- Frequ. Domain RFF
  - Frequ., Modulation, …
- Other approaches
  - CLK-skew, PSD, …

Physical unclonable function (PUF) implementation



Chip microphotograph of a PUF macro comprised of a crossbar array of 16x16 PUF cells in 28nm CMOS technology

Measurements will be available by the end of the ConnRAD project and will be included in the final report.
The PUF circuit will be implemented in a RF-Transmitter digital security engine.

BOSCH [ˌdiːsɪ aɪ'tiː] Daimler Center for Automotive IT Innovations Fraunhofer FOKUS Fraunhofer IEM htw saar Forschungsgruppe Verkehrstelematik infineon Technische Universität München TÜV SÜD universität uulm