Einfaches und sicheres Pairing für Bluetooth Smart

(Präsentiert an der Embedded Computing Conference Winterthur, 5. Juni 2018)

Lukas Widmer, Marcel Meli

Kontakt: Prof. Dr. Marcel Meli

Marcel.Meli@zhaw.ch

Our Activities

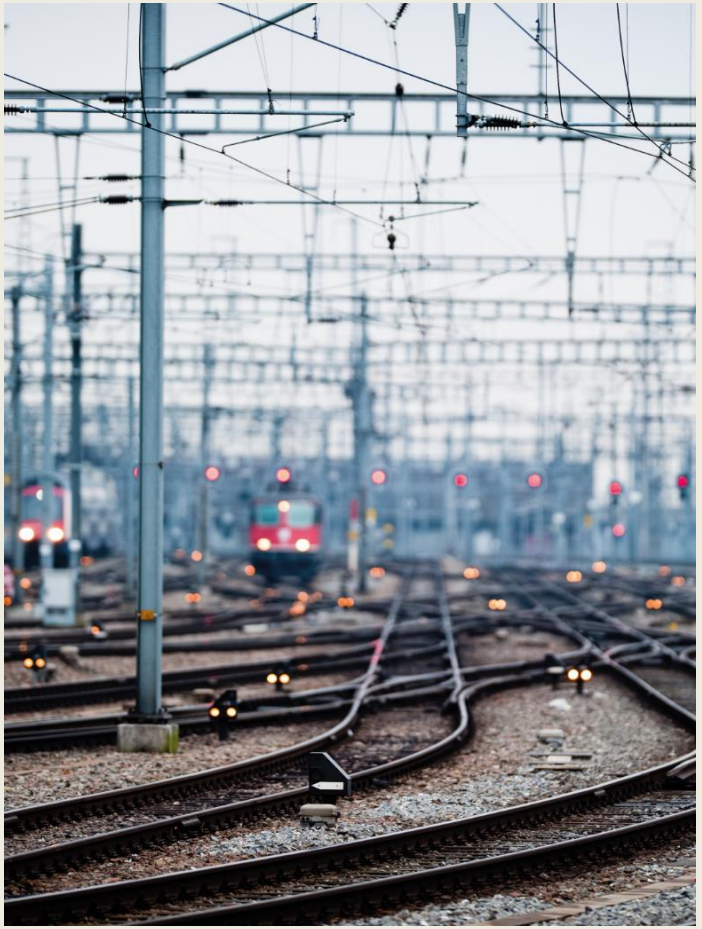
School of Engineering

InES Institute of Embedded Systems

Institute of Embedded Systems

Core Competences

- FPGA-based systems for network communication
- Time synchronization and high availability Networks
- Real-Time-Ethernet, safe and dependable Systems
- **Wireless Communication**
  - **Low Power, Energy Harvesting, Power mgt**
  - **Different wireless/RFID systems**



Source: ZHAW

Übersicht

1. Einleitung und Motivation
2. Konzept
3. Resultate
4. Fazit

Einleitung und Motivation

- Internet of Things (IoT)
  - Milliarden von Objekten mit eingebetteten Systemen
  - Drahtlose Kommunikation
  - Bluetooth Smart, Bluetooth Low Energy (BLE)
  - Benutzerfreundlichkeit
  - Sicherheit
- Pairing von Geräten essentiell
  - Initialer Austausch von Kommunikationsparametern

Einleitung und Motivation

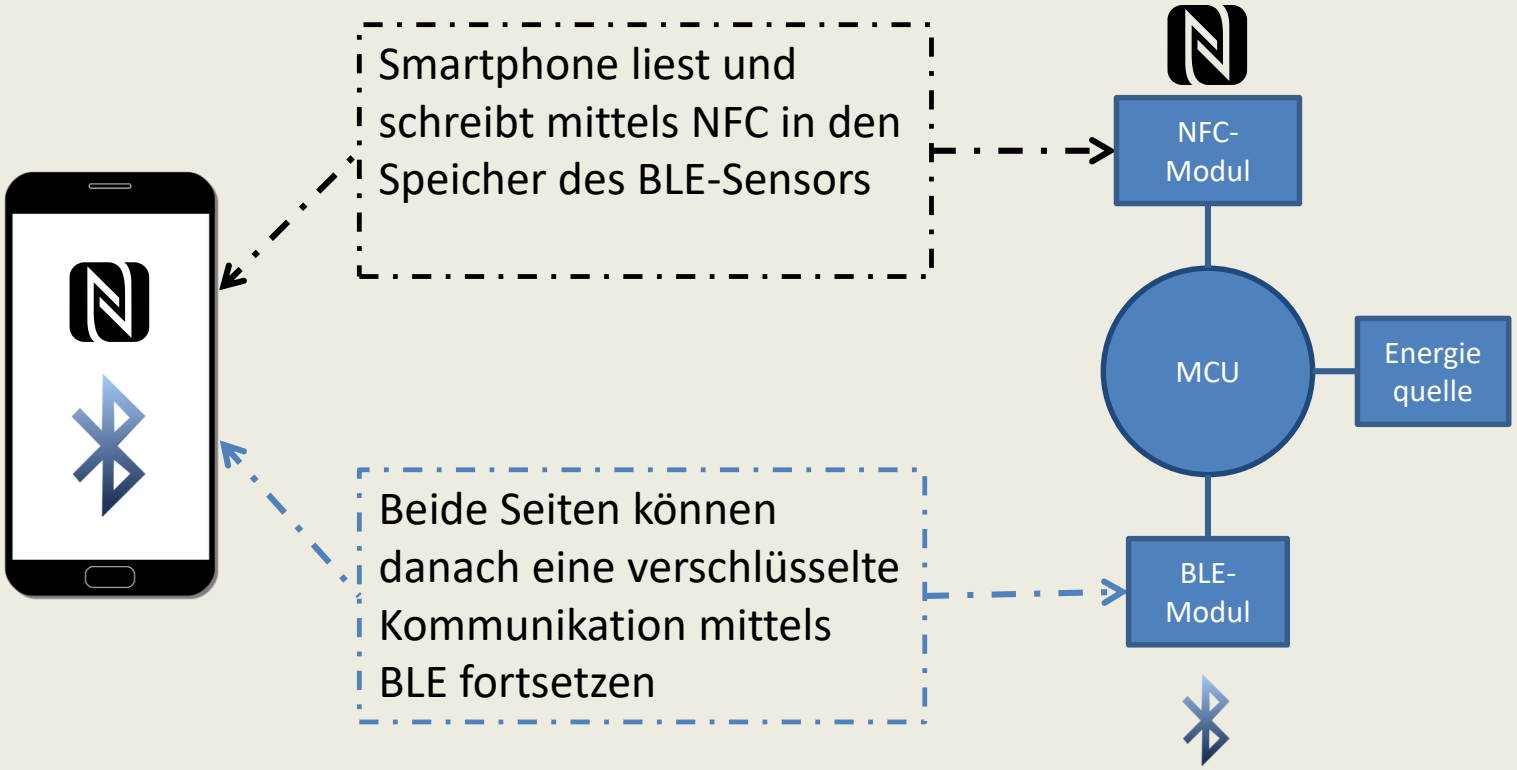
- Jetzt bereits Millionen Smartphones mit BLE
- In Zukunft noch mehr
- Viele Anwendungen welche BLE verwenden
- Mehrheit der Benutzer ohne technischen Hintergrund
  - Sichere Kommunikation soll einfach zu verwenden sein

Einleitung und Motivation

- Konfiguration von Bluetooth Smart Geräten auf eine sicher Weise ist nicht einfach
- Out-of-Band (OOB) als möglicher Weg, um initiale Konfigurationsparameter auszutauschen

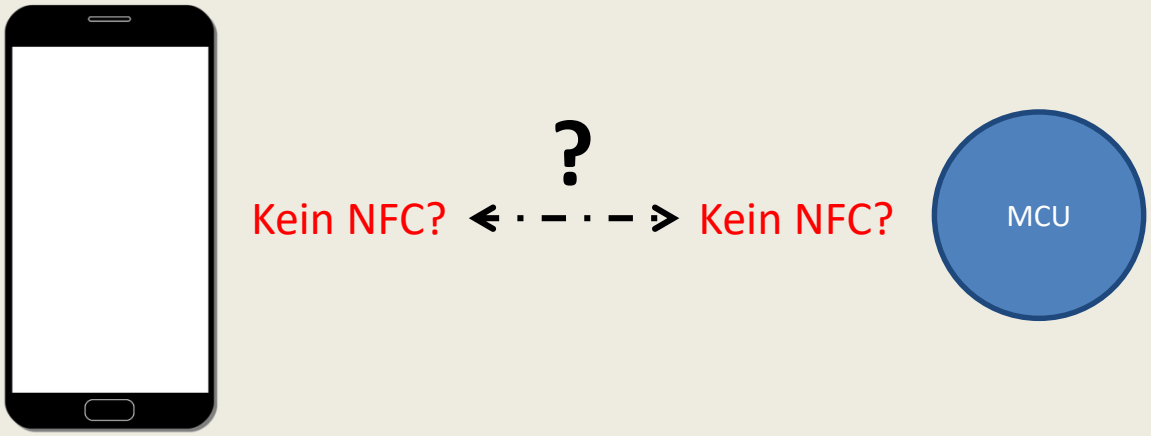
Einleitung und Motivation

- OOB mit NFC

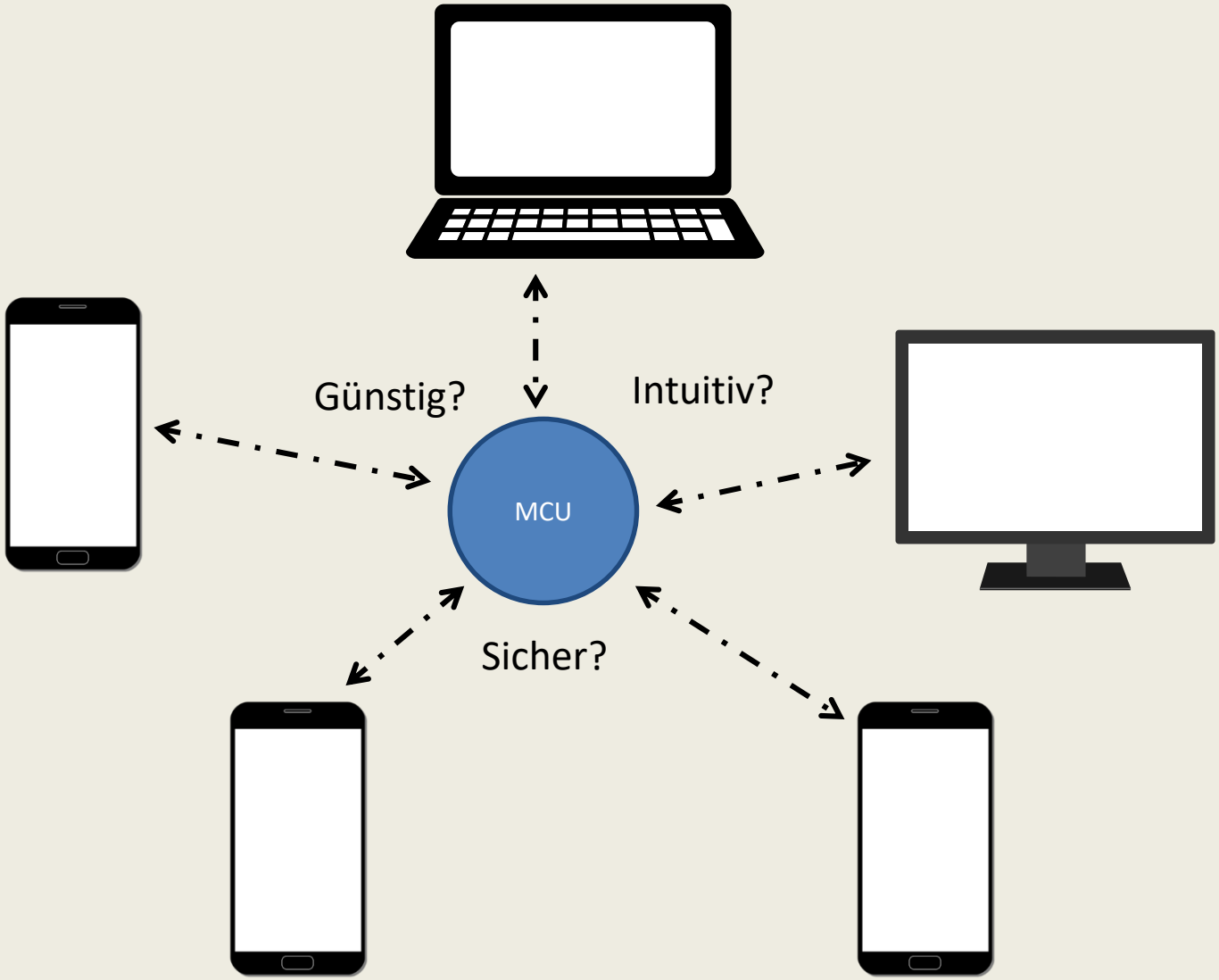


Einleitung und Motivation

- Nachteil des Einsatzes von OOB mit NFC

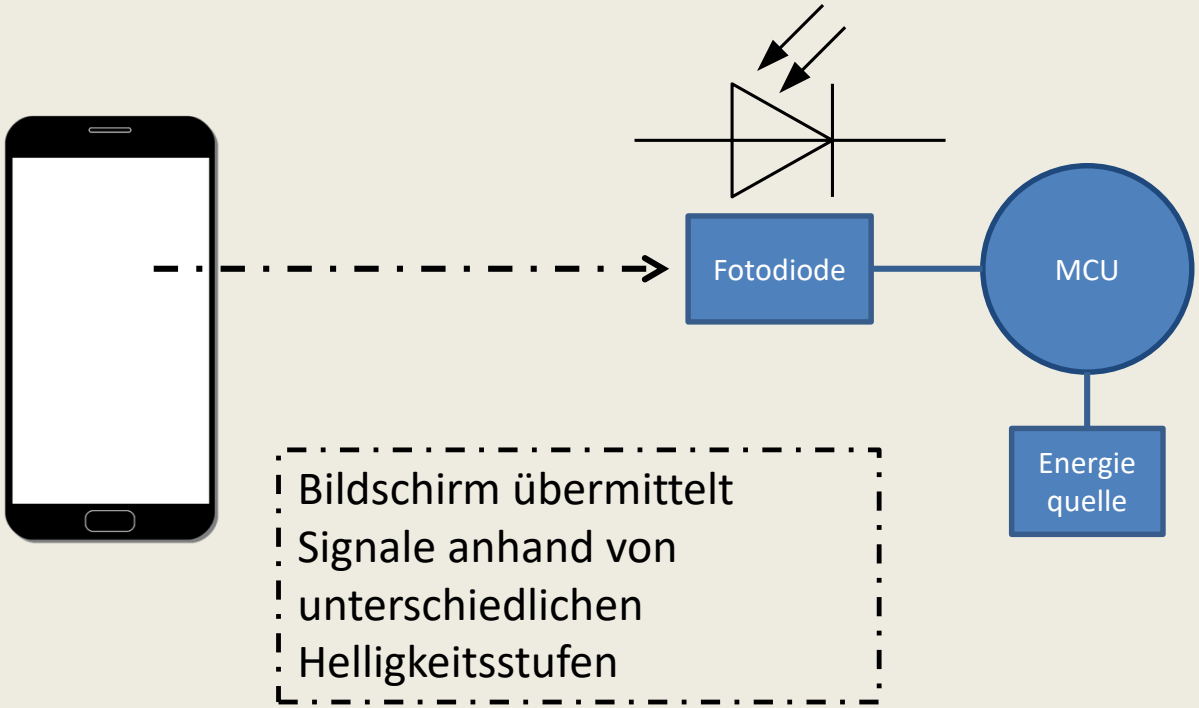


Einleitung und Motivation



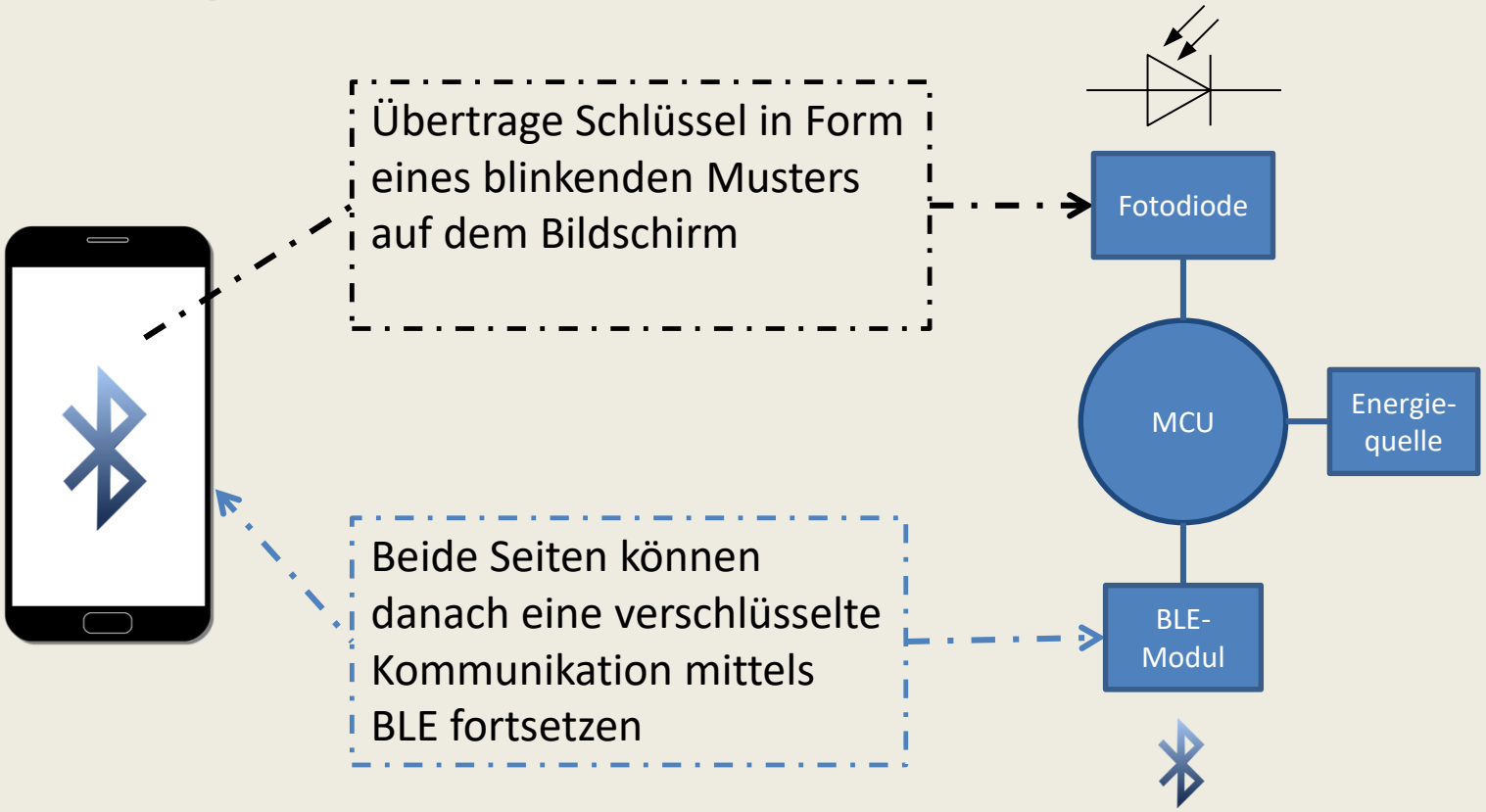
Konzept

- Universell einsetzbare OOB-Methode



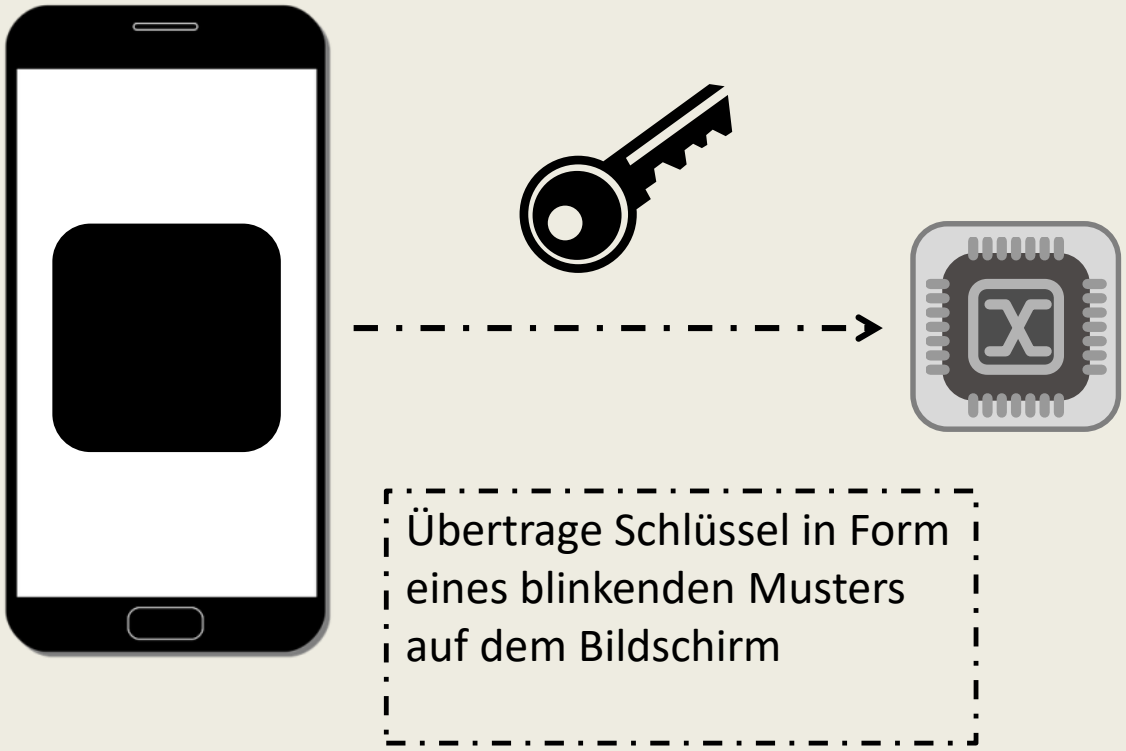
Konzept

- OOB mit optischem Kanal



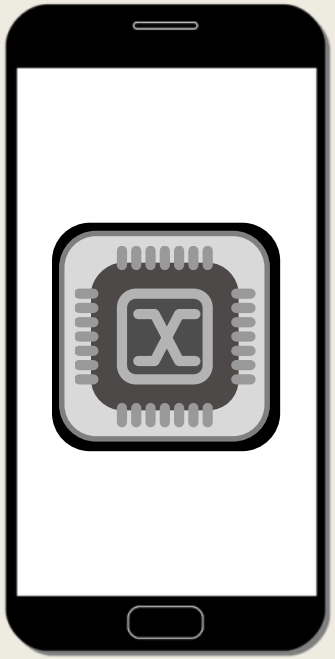
Konzept

- Schlüssel wird optisch übermittelt



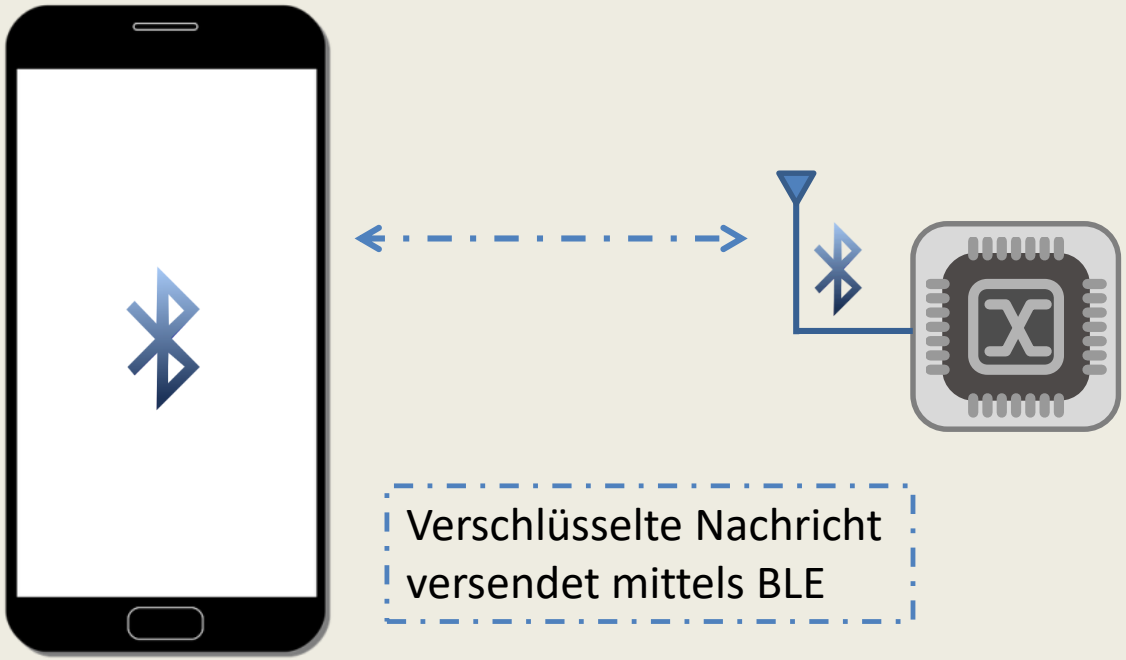
Konzept

- Tag wird auf dem Bildschirm platziert

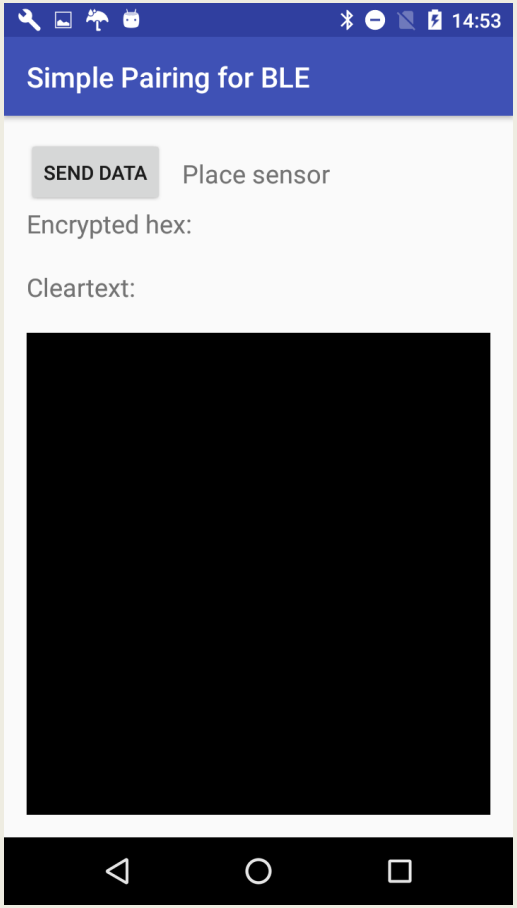


Konzept

- Danach Prozess auf verschlüsseltem Kanal möglich

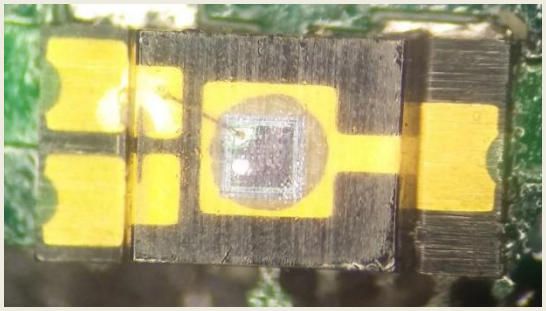


Resultate



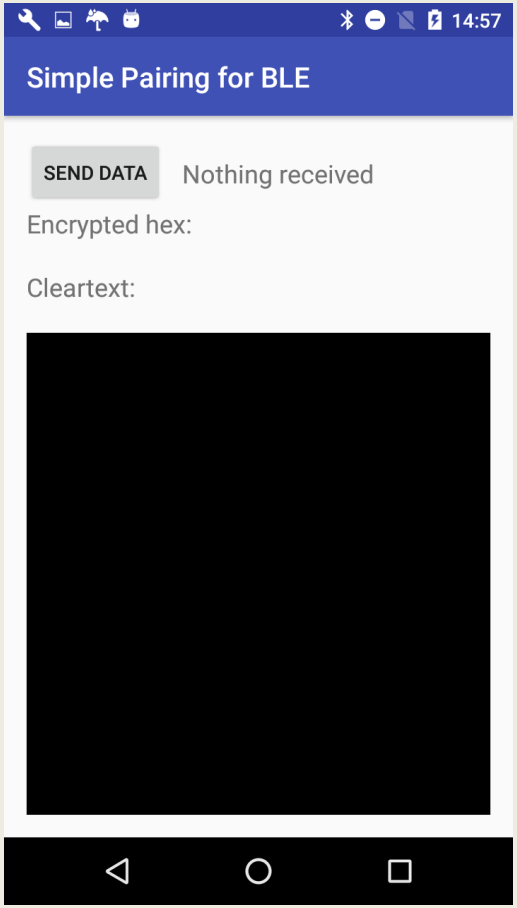
Android-App

Hardware Development Kit für den MCU Renesas RL78/G1D

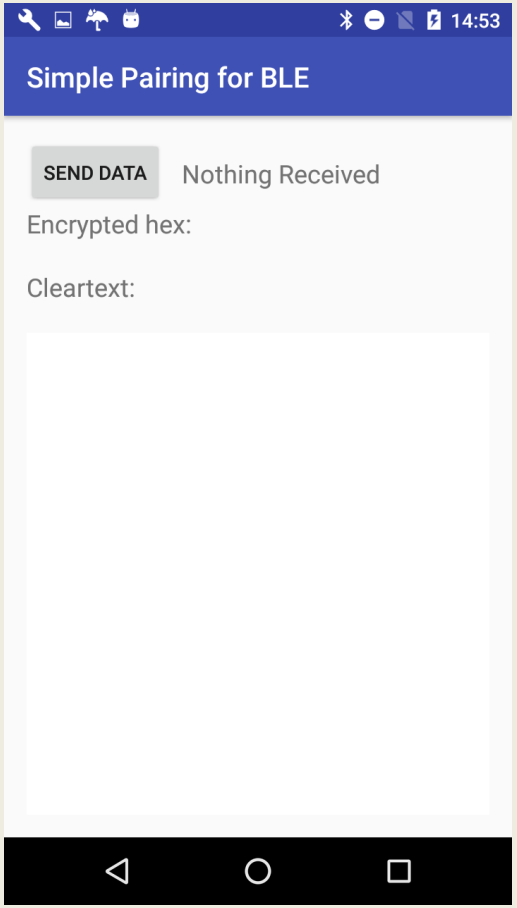


Fotodiode: Vishay ambient light sensor 751-1055-1-ND

Resultate



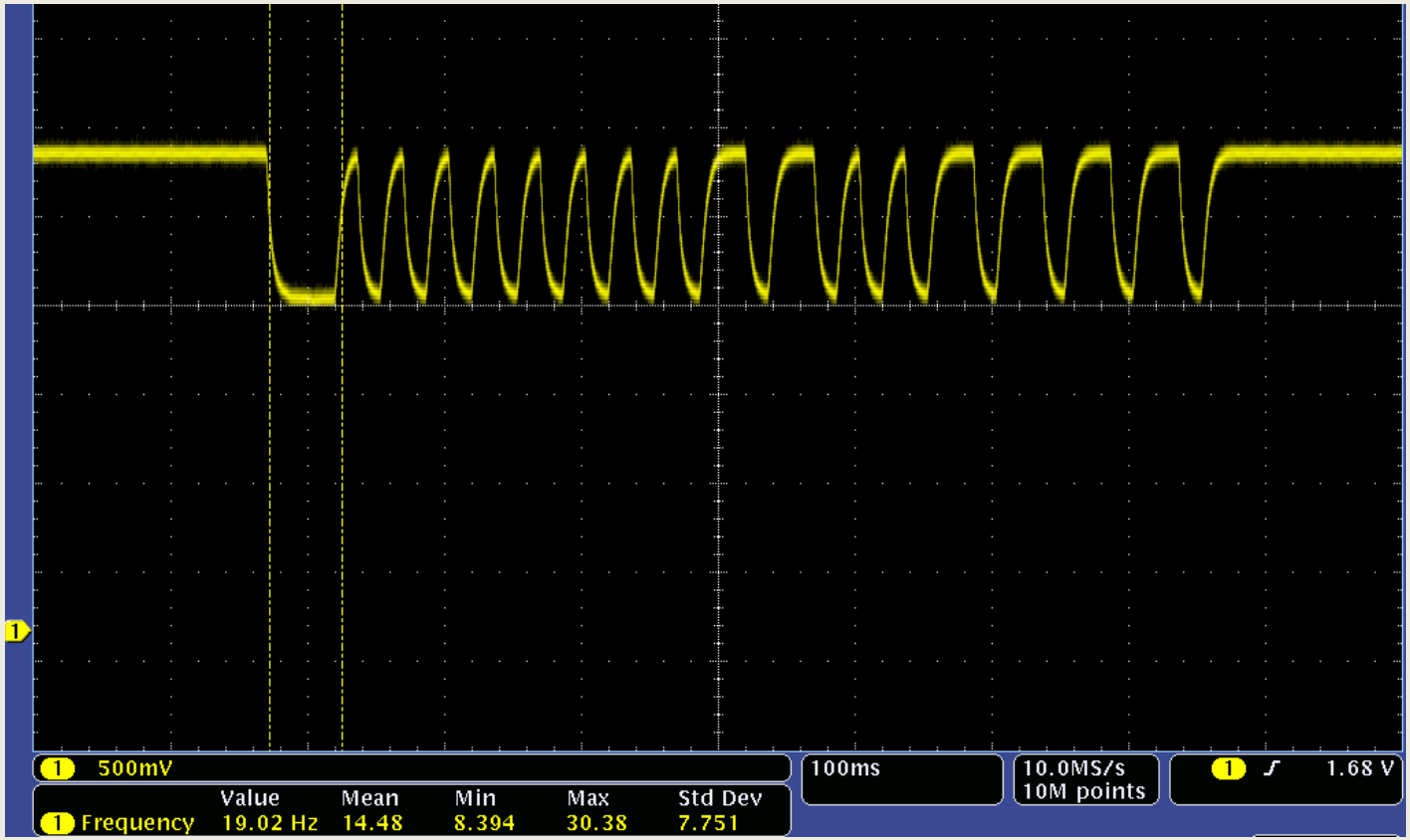
Schwarzer Bereich



Weisser Bereich

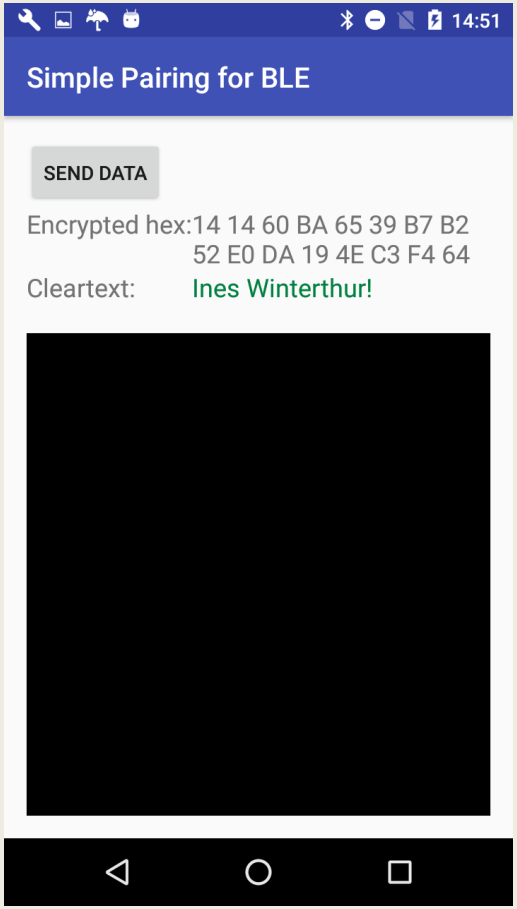
Resultate

- 0000 0000 1100 1111 (0=kurzer Puls, 1=langer Puls)

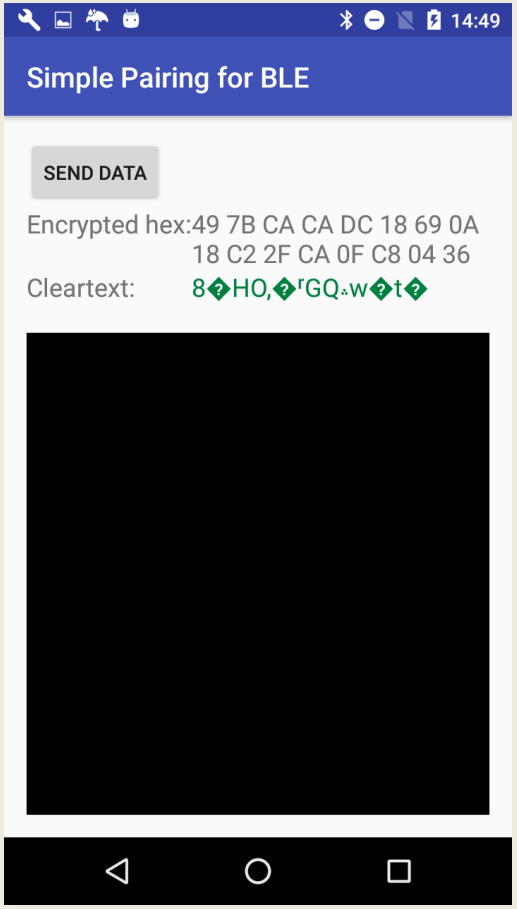


Signal: Spannung an der Fotodiode gemessen mit Oszilloskop

Resultate



Korrekt entschlüsselt



Falsch entschlüsselt

Fazit

- Pairing möglich mit einfacher Elektronik
- Lösung ist so intuitiv wie NFC
- Implementierung auf den meisten Geräten möglich
- Benötigte CPU-Ressourcen minimal

Fazit

- Datenrate gering, jedoch genügend
- Einfluss von Licht kann minimal gehalten werden

School of Engineering
InES Institute of Embedded Systems

Fragen ???

Kontakt: marcel.meli@zhaw.ch

Link zum Bericht

- Easy and Safe Pairing for Bluetooth Smart: https://www.zhaw.ch/no_cache/de/forschung/personen-publikationen-projekte/detailansicht-publikation/publikation/211450/