Schlussbericht zum Verbundvorhaben

sensIC

Eindeutige Identifizierbarkeit für vertrauenswürdige Hybrid-Sensor-elektronik mit Hilfe additiver Fertigung

Teilvorhaben:

Sichere Hardware für Identifikation und Kommunikation

Förderkennzeichen	16ME0303
Förderzeitraum	01. Mai 2021 – 30. April 2024
Ausführende Stelle	Hochschule Offenburg, Institut für verlässliche Embedded Systems und Kommunikationselektronik (ivESK)
Projektleitung	Prof. Dr.-Ing. Sikora, Axel

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor

Inhalt

I. Kurze Darstellung ... 3
1. Aufgabenstellung ... 3
2. Planung und Ablauf des Vorhabens ... 3
3. Wissenschaftlicher und technischer Stand, an den angeknüpft wurde ... 4
4. Zusammenarbeit mit anderen Stellen ... 4
II. Eingehende Darstellung ... 5
1. Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele ... 5
2. Die wichtigsten Positionen des zahlenmäßigen Nachweises ... 24
3. Notwendigkeit und Angemessenheit der geleisteten Arbeit ... 25
4. Voraussichtlicher Nutzen und Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans ... 25
5. Während der Durchführung des Vorhabens dem ZE bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen ... 26
6. Erfolgte oder geplante Veröffentlichungen des Ergebnisses nach Nr. 11 ... 26

I. Kurze Darstellung

1. Aufgabenstellung

Ziel des Projekts war die Entwicklung eines vertrauenswürdigen hybriden Sensorelektroniksystems unter Verwendung additiver Fertigungstechniken. Das Projekt zielte insbesondere darauf ab, sichere Hardware für Identifizierungs- und Kommunikationszwecke zu entwickeln, die sich auf physisch nicht klonierbare Funktionen (PUFs) und drahtlose Kommunikationstechnologien wie Bluetooth Low Energy (BLE) und RFID stützen sollte. Das System musste Vertraulichkeit und Integrität gewährleisten, wobei der Schwerpunkt auf der Sicherung der Identität des Schlauchsensorsystems (PUF-Schlüssel) und der Temperaturdaten im Projektdemonstrator lag. Zu diesem Zweck wurde ein sicherer gemeinsamer Schlüssel generiert, der auf den Variationen der BLE-Kommunikationskanaldämpfung basiert und für die AES-Verschlüsselung der zwischen dem Schlauchsystem und einem externen Host übertragenen Daten verwendet wird.

2. Planung und Ablauf des Vorhabens

Das Projekt war in mehrere Hauptphasen unterteilt, die im Mai 2021 begannen und im April 2024 endeten. In der ersten Phase (Mai 2021 - Dezember 2021) lag der Schwerpunkt auf der Festlegung der spezifischen Anforderungen und Ziele des Projekts. In dieser Phase wurden die detaillierten Systemanforderungen gesammelt und die Struktur des Demonstrators entworfen. Ein Mikrocontroller (STM32F746) wurde ausgewählt, um die Kommunikations- und Hardwareanforderungen des Projekts zu erfüllen, einschließlich SPI- und LIN-Protokolle. Das Team untersuchte auch Methoden zur gemeinsamen Schlüsselerzeugung mit Bluetooth Low Energy (BLE) und RFID.

Im Jahr 2022 (Januar 2022 - Dezember 2022) konzentrierten wir uns auf die Fertigstellung des Gesamtdesigns und der Sicherheitskonzepte des Systems und arbeiteten eng an der Entwicklung der gemeinsamen Schlüsselerzeugung. Wir haben die Probleme erkannt, die mit der Verwendung des NFC-Protokolls in unserem System verbunden sind, nämlich die Notwendigkeit, dass sich das Lesegerät und der Tag in unmittelbarer Nähe befinden. Wir entschieden uns für die Schlüsselgenerierung unter Verwendung des BLE Received Signal Strengh Indicator (RSSI). Wir haben die Eigenschaften der Signalausbreitung von BLE unter verschiedenen Umgebungsbedingungen sowohl in einer kontrollierten HF-Kammer als auch in einer normalen Büroumgebung untersucht. Anschließend arbeiteten wir daran, die besten Quantisierungsmethoden zu ermitteln, um die geringste Anzahl von Bitfehlern zwischen dem Schlauch und dem Host zu optimieren.

Im Jahr 2023 (Januar 2023 - Dezember 2023) ging das Projekt in eine technischere Phase über, in der das Team mit der Integration von Schlüsselkomponenten wie gedruckten Physical Unclonable Functions (PUFs) und Temperatursensoren in das System begann. Diese Komponenten wurden mit einem von Cyient entwickelten anwendungsspezifischen integrierten Schaltkreis (ASIC) kombiniert, und die Kommunikation zwischen diesen Teilen wurde getestet und validiert. Der BLE-basierte Schlüsselgenerierungsalgorithmus wurde verfeinert, um eine starke Verschlüsselung und gegenseitige Authentifizierung zwischen den Systemkomponenten zu gewährleisten. Die Zusammenarbeit mit Partnern wie dem KIT und Continental spielte eine wichtige Rolle bei der Optimierung der Hardware-Integration und der Sicherheitsmerkmale des Systems. Dann verlagerte sich der Schwerpunkt des Projekts auf die Fertigstellung des Demonstrators und die Durchführung umfassender Validierungen und Tests des integrierten Systems. Außerdem wurden gedruckte Sensoren und PUFs getestet, und das Gesamtsystem wurde einer Kalibrierung unterzogen, um genaue Temperaturmessungen zu gewährleisten.

In der letzten Phase des Projekts (Januar 2024 - April 2024) wurde der Demonstrator einer abschließenden Prüfung und Validierung unterzogen. Dazu gehörten weitere Tests der BLE-basierten Kommunikation zur gegenseitigen Authentifizierung und sicheren Datenübertragung. Die gedruckten PUFs und Temperatursensoren wurden vollständig integriert, und das endgültige System wurde für

mögliche reale Anwendungen vorbereitet. Der Demonstrator kombinierte erfolgreich sichere Kommunikation und Identifikation durch die Generierung von geheimen Schlüsseln und PUFs sowie die Integration von Sensoren, was ihn zu einem hochsicheren System für industrielle und automobile Anwendungen macht.

3. Wissenschaftlicher und technischer Stand, an den angeknüpft wurde

Angabe bekannter Konstruktionen, Verfahren und Schutzrechte, die für die Durchführung des Vorhabens benutzt wurden

- Cascade algorithm for Information Reconciliation

Angabe der verwendeten Fachliteratur sowie der benutzten Informations- und Dokumentationsdienste

[1] Gilles Brassard and Louis Salvail. 1994. Secret-key reconciliation by public discussion. In Workshop on the theory and application of cryptographic techniques on Advances in cryptology (EUROCRYPT '93). Springer-Verlag, Berlin, Heidelberg, 410–423.

4. Zusammenarbeit mit anderen Stellen

Zusammenarbeit mit dem KIT:

- Es wurde festgelegt, welche Systemkomponenten miteinander kommunizieren müssen und welche Kommunikationskanäle sicher sein müssen.
- Identifizierung der Daten, die privat, vertraulich und vollständig sein müssen.
- Arbeitete an der Identifizierung von Sicherheitsbedrohungen und der Abwehr dieser Bedrohungen.
- Der Schwerpunkt liegt auf der Kombination des gemeinsamen Schlüssels, der aus BLE-RSSI und dem PUF-Schlüssel generiert wird, um die Systemsicherheit zu maximieren.
- Validierung der ausgedünnten ASICs und Identifizierung der funktionalen ASICs.
- Validierung der Funktionalität der Temperatursensoren und des PUF nach der Integration in die Bulk- und Thinned-ASICs.

Zusammenarbeit mit Cyient:

- Implementierte Software für die im Schlauch integrierte MCU, um die Kommunikation mit dem ASIC über die SPI-Schnittstelle zu erleichtern.

Zusammenarbeit mit Continental:

- Zusammenarbeit bei der Erstellung des Schaltplans für die Demonstrator-Leiterplatte.
- Arbeitete an der Integration der Demonstrator-Leiterplatte mit den verschiedenen Hardwareteilen.

II. Eingehende Darstellung

1. Verwendung der Zuwendung und des erzielten Ergebnisses im Einzelnen, mit Gegenüberstellung der vorgegebenen Ziele

Im Antrag wurden die Projektziele einzelnen Arbeitspaketen zugeordnet. Im Folgenden wird der wissenschaftlich-technische Fortschritt anhand der Arbeitspakete, an denen der Zuwendungsempfänger beteiligt ist, dokumentiert und mit den ursprünglich geplanten Zielen abgeglichen.

Arbeitspaket 1

01. Mai 2021 – 31. Dezember 2021

Es wurden zunächst – basierend auf den Überlegungen aus der Antragsstellung – die genauen Anforderungen für die avisierten Anwendungen gesammelt und analysiert. Hierauf aufbauend wurde in Abstimmung mit den Projektpartnern ein Demonstratoraufbau konzipiert (vgl.: Abbildung 1) mit dessen Hilfe die Funktionen implementiert und evaluiert werden können.

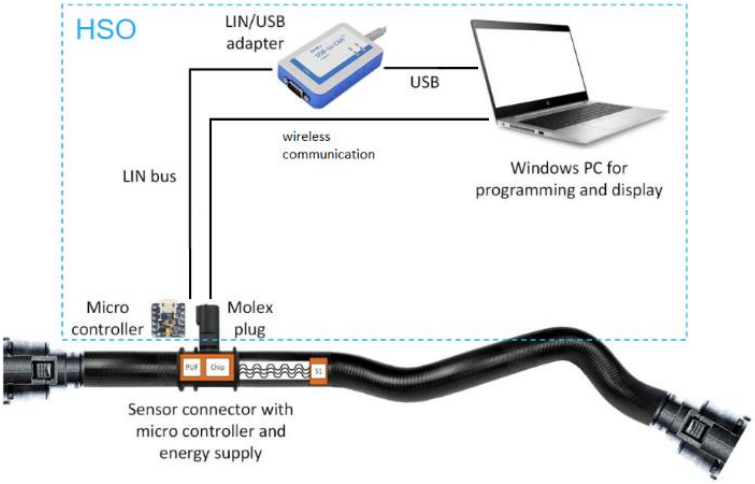

Abbildung 1: Demonstratoraufbau

Für die Definition der Demonstratorbauteile und deren Spezifikationen wurde vom ivESK ein Mikrocontroller herausgesucht. Die Spezifikationen sind nachfolgend aufgelistet:

- Kommunikationsprotokolle
  - SPI (13 MHz): Chip vom Projektpartner Cyient
  - I2C: RFID-Tag nach ISO 15693 (NFC: 13,56 MHz)
  - Tx/Rx (UART): LIN 2.0
- Strobe (Clock-Signal): 26 MHz
- Maximale PCB-Größe:2,5 x 3 cm²

Es wurde der STM32F746 Mikrocontroller der Firma ST Microelectronics ausgesucht, der diese Anforderungen erfüllt.

Im nächsten Schritt wurde die Anwendung der Drahtloskommunikation in dem Demonstrator definiert. Dieser soll den LIN-Bus bei einer späteren Anwendung ersetzen und die Daten verschlüsselt übertragen. Während der Planung wurde überlegt, die Daten nicht nur über RFID zu senden, sondern auch über Bluetooth Low Energy (BLE)/ Bluetooth classic. Der Aufbau der Kommunikation ist in Abbildung 2 gezeigt. Der Chip vom Projektpartner Cyient wird durch SPI konfiguriert. Alle Daten des PUF Kerns und der Temperaturmessung werden von dem Mikrocontroller erfasst, verarbeitet und entweder über LIN oder drahtlos an einen Host (PC) weitergeleitet.

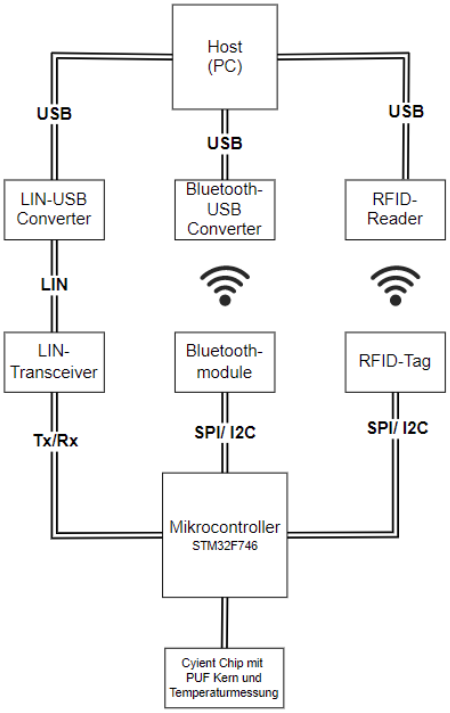

Abbildung 2: Aufbau der Kommunikationsstruktur

01. Januar 2022 – 31. Dezember 2022

Während dieses Zeitraums wurde die ursprüngliche Struktur des Demonstrators weiter definiert und fertiggestellt. Nach Gesprächen mit unseren Projektpartnern haben wir einen detaillierten Demonstratoraufbau entworfen, der alle wichtigen Systeme umfasst, die derzeit im Projekt entwickelt werden (vgl.:Abbildung 3).

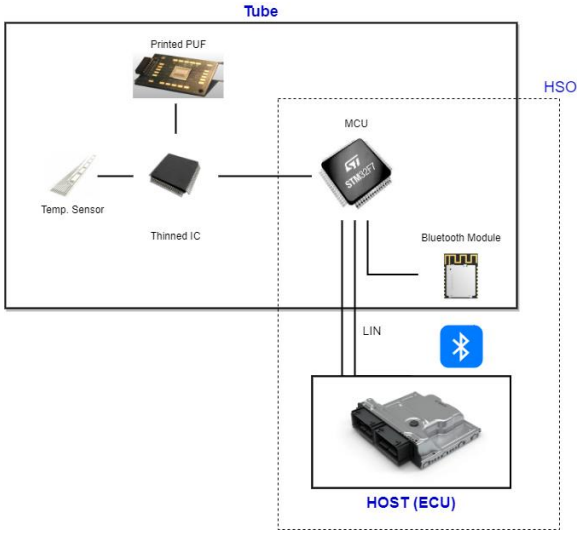

Abbildung 3: Demonstratoraufbau

Der zuvor ausgewählte STM32F746 wird die Mikrocontrollereinheit (MCU) im Schlauch sein und den verdünnten Chip unseres Projektpartners Cyient auslesen. Dieser Chip wird den gedruckten PUF-Kern und den Temperatursensor auslesen. Für die drahtlose Kommunikation zur Schlüsselgenerierung wurde ein Bluetooth Low Energy (BLE) Modul gewählt. Zu Demonstrationszwecken wird ein weiterer Mikrocontroller als Ersatz für einen Host-Computer im Fahrzeug verwendet. Dieser Host verfügt ebenfalls über ein BLE-Modul und nimmt an der Schlüsselgenerierung teil. Der daraus resultierende

gemeinsame Schlüssel wird dann verwendet, um eine gegenseitige Authentifizierung zwischen dem Schlauch und dem Host zu gewährleisten und den LIN-Bus-Kommunikationskanal zwischen ihnen zu verschlüsseln.

Die erforderlichen Verbindungen zwischen dem STM32-Mikrocontroller und dem ASIC wurden in Zusammenarbeit mit Cyient weiterentwickelt und charakterisiert.

01. Januar 2023 – 31. Dezember 2023
Dieses AP wurde bereits im vorangegangenen Zeitraum fertiggestellt. Der endgültige Aufbau des Demonstrators ist in Abbildung 3 **Error! Reference source not found.**dargestellt. Das so definierte System wird in den folgenden Arbeitspaketen entwickelt und getestet.

01. Januar 2024 – 30. April 2024
-

Arbeitspaket 2 und Arbeitspaket 5

Diese Arbeitspakete sind eng miteinander verknüpft und die geleistete Arbeit hängt voneinander ab, so dass es überflüssig wäre, sie getrennt zu beschreiben. Daher haben wir sie für den Bericht zusammengefasst.
01. Mai 2021 – 31. Dezember 2022
-
01. Januar 2023 – 31. Dezember 2023
In diesen Arbeitspaketen arbeiteten wir eng mit dem KIT zusammen, um die Integration und Funktionsprüfung der gedruckten Physically Unclonable Function (PUF) und der gedruckten Temperatursensoren zu unterstützen. Eine erste Version der gedruckten PUF und die gedruckten Temperatursensoren wurden vom KIT entwickelt. Diese Teile wurden mit einem gehäusten ASIC auf einer Testleiterplatte (PCB) integriert. Die elektrischen Verbindungen zwischen diesen Teilen sowie die elektrischen Verbindungen zwischen dem ASIC und dem STM32F746-Mikrocontroller (MCU) wurden in diesem Arbeitspaket definiert und getestet. Abbildung 4 zeigt die Hardware-Integration dieser verschiedenen Teile, zusätzlich zu den Bluetooth-Modulen, LIN-Modulen und anderer Hardware.
Für Testzwecke entwickelte HSO zwei Softwaremodule für die STM32F746 MCU, die auf dem von Cyient entwickelten ASIC basieren. Das erste Modul programmiert den ASIC, um die von der PUF-Schaltung erzeugten Bits auszulesen. Das zweite Modul programmiert den ASIC für das Auslesen der gemessenen Temperaturwerte. Diese Module werden in AP 6 besprochen.

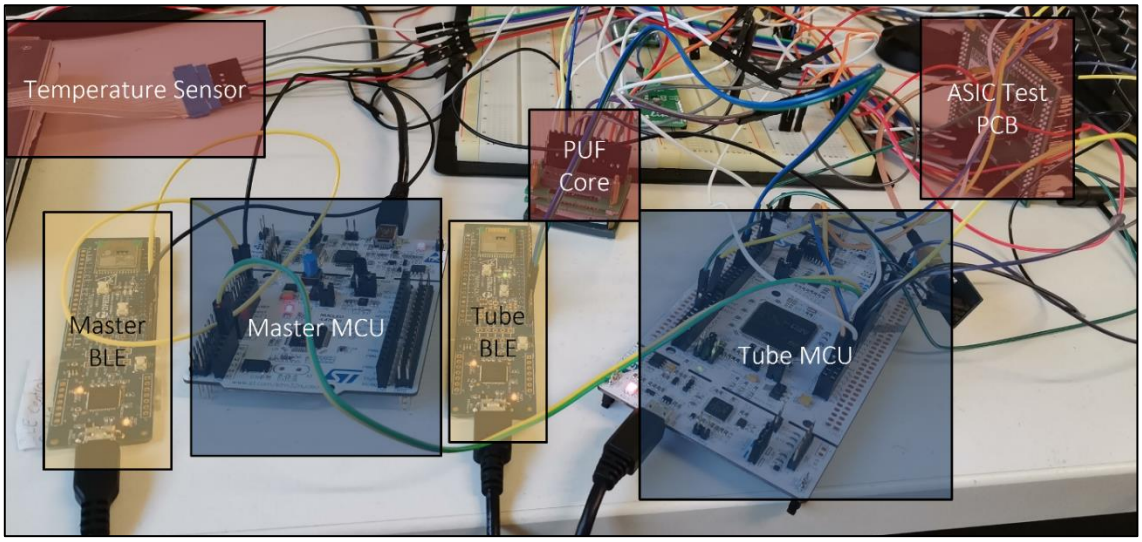

Abbildung 4: Hardware-Integration des gedruckten PUF, des gedruckten Temperatursensors und der Ausleseelektronik

Für den finalen Demonstrator arbeiteten wir mit den Kollegen von Continental und dem KIT zusammen, um ein PCB-Design für die Elektronik des Schlauchs zu entwickeln. Von unserer Seite aus haben wir einen Schaltplan erstellt, der alle für den Schlauch relevanten elektronischen Bauteile und die notwendigen elektrischen Verbindungen und Stecker enthält. Die wichtigsten Bauteile sind:

- STM32F746ZGT MCU
- CYBLE-416045-02 BLE-Modul
- ATA663254 LIN-chip
- FPC-Anschluss, um die Verbindung zwischen dem ausgedünnten ASIC und dem Rest der Hardware zu ermöglichen

Die ersten Schaltpläne sind in Abbildung 5 dargestellt.

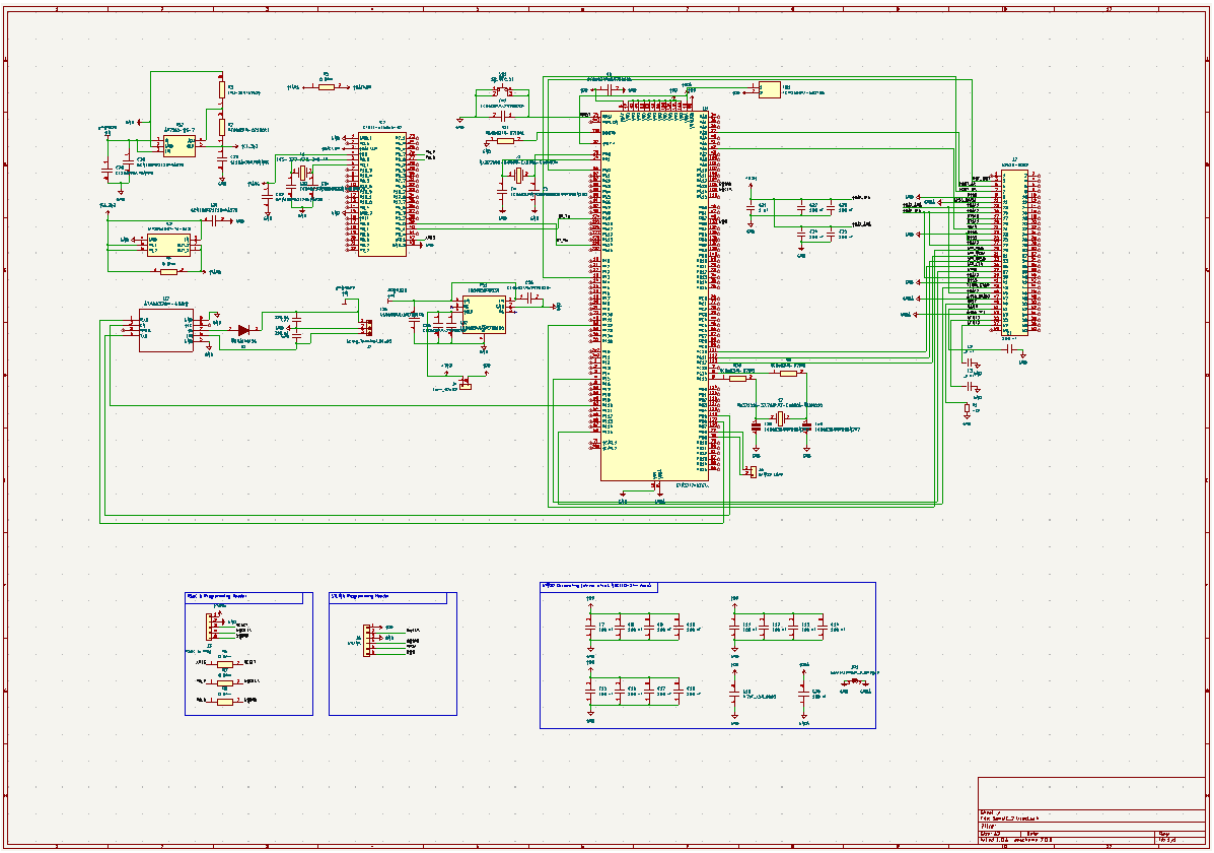

Abbildung 5: Demonstrator PCB-Schaltpläne

01. Januar 2024 – 30. April 2024

Die Schaltpläne für die Demonstrationsplatine wurden fertiggestellt und mehrere Platinen wurden von Continental bestellt. Eine einfachere Version der Demonstrator-Leiterplatte diente als Adapterplatte, die nur den FPC-Anschluss enthielt. Der Zweck dieser Platinen bestand darin, die Funktionalität der ausgedünnten ASICs zu validieren, indem dieselbe Verdrahtung wie bei den ASICs in Großpackung verwendet wurde. Nachdem die ausgedünnten ASICs von IMS hergestellt worden waren, arbeiteten wir eng mit dem KIT zusammen, um die Funktionalität der ASICs zu testen und zu validieren. Abbildung 6 zeigt den Testaufbau. Zu den Tests gehörten:

- Validierung der Konnektivität der ausgedünnten ASICs und der Folienbahnen.
- Validierung der Ausgangssignale und Spannungen der ASICs.
- Validierung der Funktionalität des Temperatursensormoduls und des PUF-Schlüsselgenerierungsmoduls. Zu diesem Zweck wurde eine mechanische Vorrichtung hergestellt und uns von Continental zugesandt, die den externen Thermistoren mit Pogo-Pins an die Folie anschließt.

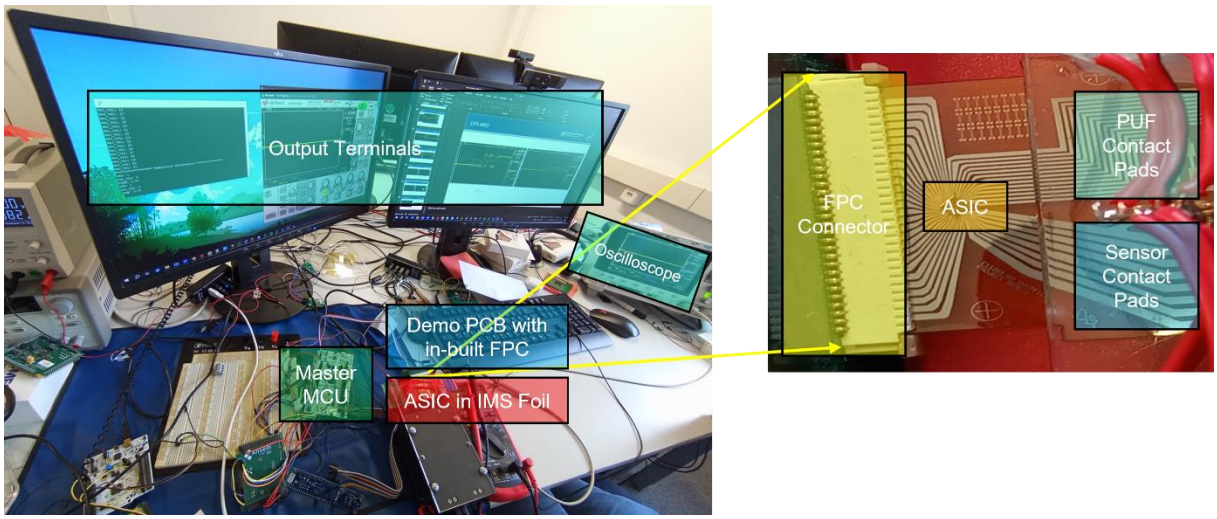

Abbildung 6: Ausgedünnte ASICs signalen Validierungstests

Die voll funktionsfähigen, ausgedünnten ASICs wurden identifiziert und an Continental zur Integration des Temperatursensors und anschließend an KIT zur Integration der PUFs geschickt.
Nachdem das PUF-Modul integriert war, gab es noch einen letzten Schritt, um den Demonstrator fertigzustellen. Um eine Temperaturmessung in Celsiusgraden zu erhalten, müssen die vom ASIC ausgegebenen „Zählwerte“ umgerechnet werden. Um dies zu erreichen, führten wir die Kalibrierung des integrierten ASIC und der gedruckten Sensoren durch. Dieser Schritt umfasst die Messung der Zählwerte bei zwei verschiedenen Temperaturen in einer kontrollierten Umgebung (Temperaturkammer) und dann, da die Zählwerte linear mit der Temperatur ansteigen, die Formulierung einer linearen Interpolation für jeden der beiden Sensoren. Anschließend haben wir Messungen durchgeführt, um die Leistung der beiden Sensoren zu überprüfen. Der Kalibrierungsaufbau ist in Abbildung 7 dargestellt. Die Ergebnisse sind in Abbildung 8 dargestellt, wo die Sensoren bei 30°C und 90°C gemessen und entsprechend kalibriert wurden.

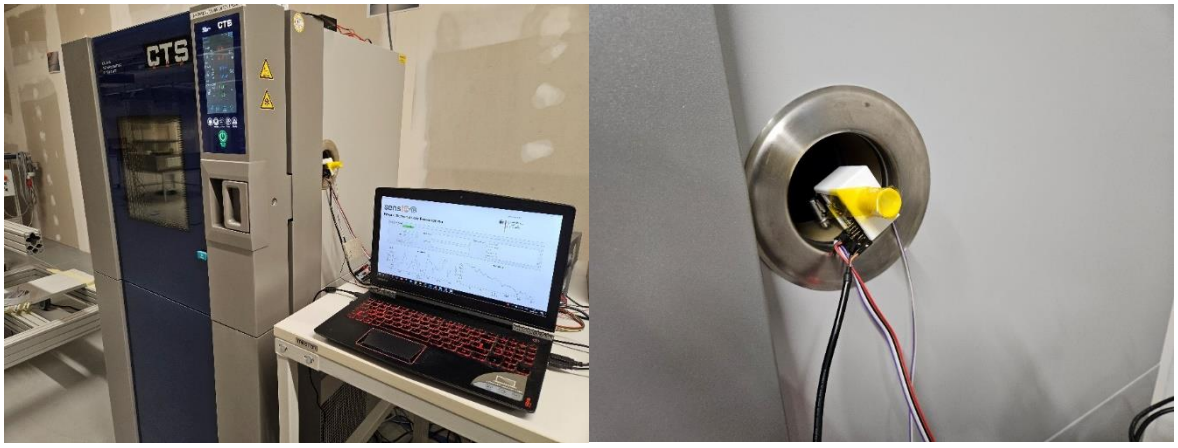

Abbildung 7: Einstellung der Kalibrierung

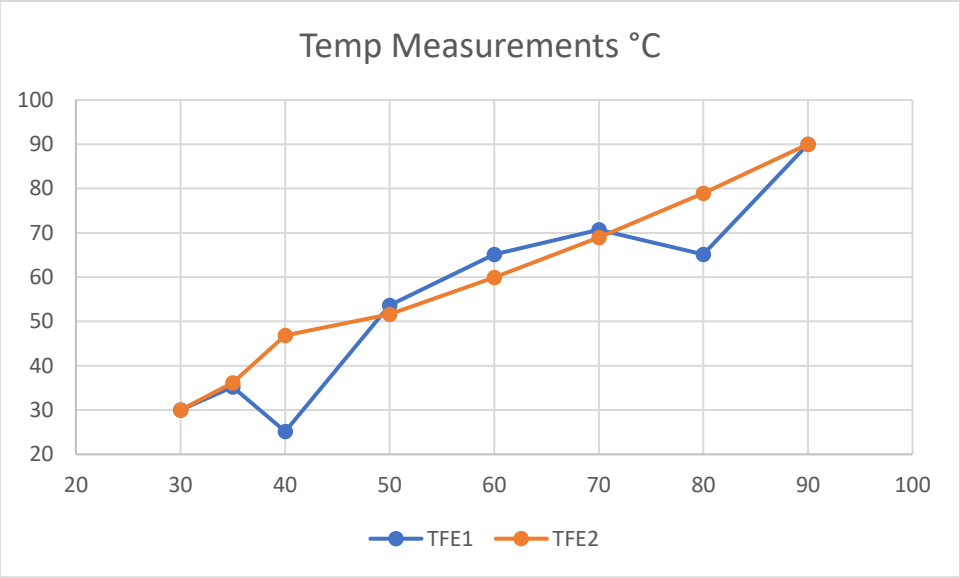

Abbildung 8: Ergebnisse der Kalibrierung von Temperatursensoren

Arbeitspaket 6

01. Mai 2021 – 31. Dezember 2021

Mit der zunehmenden Digitalisierung und Vernetzung wird die Sicherheit von IoT-Geräten immer wichtiger. Damit sicherheitsrelevante Daten von Unbefugten/Attackierter nicht mitgelesen werden können, müssen die Daten durch kryptographische Verfahren verschlüsselt werden. Dabei müssen die drei Sicherheitsanforderungen, Vertraulichkeit, Integrität und Authentizität gewährleistet sein. Wie sicher so eine Verschlüsselung ist, hängt nicht nur vom Algorithmus ab, sondern auch vom verwendeten Schlüssel. Jede drahtlose Kommunikation hat einzigartige Kanaleigenschaften, welche im Rahmen des Projekts evaluiert und zur Generierung eines Schlüssels genutzt werden soll. Der Vorteil eines solchen Verfahrens ist, dass jeder neu generierte Schlüssel sich vom vorherigen Schlüssel unterscheidet und somit ein Ausspionieren der Daten erschwert/ unmöglich macht. Da es sich bei diesem Sicherheitskonzept um eine symmetrische Verschlüsselung handelt, bei der beide Kommunikationspartner den gleichen Schlüssel generieren müssen, müssen die Kanaleigenschaften von beiden Seiten messbar und zu dem gleichen Schlüssel führen. Es konnten zum Beispiel folgende Kanaleigenschaften untersucht werden:

- Distanz und Orientierung der Kommunikationspartner zueinander
- Zeitbasierte Messungen (können von einem Angreifer leicht gemessen werden)
- Phasenverschiebung durch Vibrationen (Vibrationen müssen bei beiden Kommunikationspartnern gleich sein)
- Feldstärke
- RSSI-Wert

Die RSSI-Messung wird für die Schlüsselgenerierung weiter betrachtet, da diese von vielen verschiedenen Faktoren abhängt. Diese sind zum Beispiel: Distanz und Ausrichtung der Geräte zueinander, Umgebung, Interferenzen durch andere Kommunikationen mit derselben Frequenz.

RFID

Für die Entwicklung eines Sicherheitskonzepts bei einer RFID-Kommunikation wurden der Reader ST25r3911b und der Tag ST25DV04K von ST Microelectronics ausgewählt. Die Kommunikation erfolgt bei 13,56 MHz (NFC). Der Tag kann über drei verschiedene Methoden beschrieben und ausgelesen werden: NDEF (NFC Data Exchange Format); direktes schreiben in die Mailbox und FTM (fast transfer modus).

Bei den ersten Messungen wurde der FTM verwendet. Bei der Kommunikation werden zwei Bytes in den Tag geschrieben und anschließend wieder ausgelesen. Die Programmstruktur ist in Abbildung 9 zu sehen.

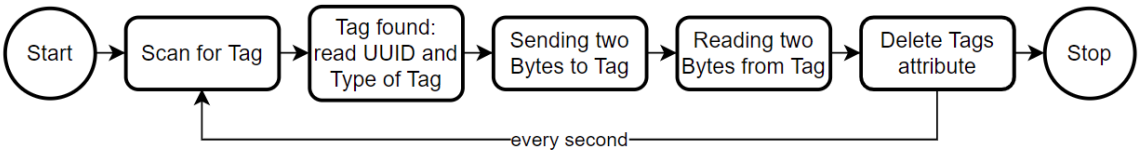

Abbildung 9: Programmstruktur der RFID Kommunikation

Da der Tag keine RSSI-Messung bietet, wurde ein logarithmischer Amplifier (AD8310) ausgewählt, der auch zur Bestimmung des RSSI-Werts genutzt werden kann. Der Messaufbau und die ersten Ergebnisse sind in Abbildung 10 und Abbildung 11 dargestellt.

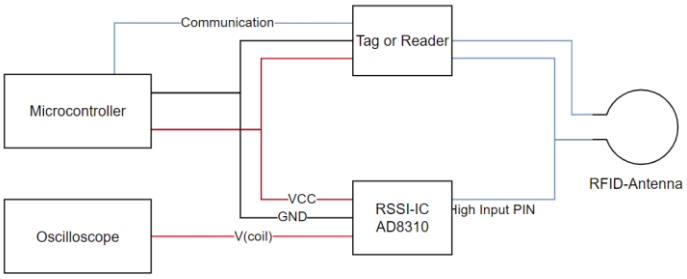

Abbildung 10:Messaufbau zur Bestimmung des RSSI Wertes

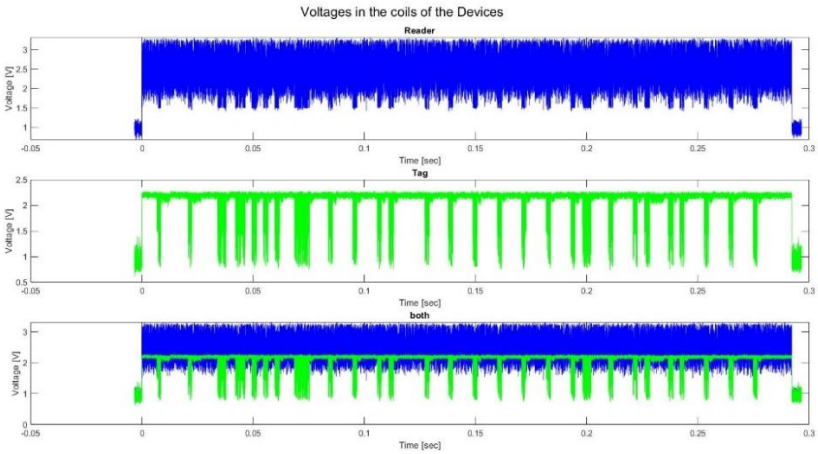

Abbildung 11:Messergebnis mit AD8310

Bluetooth Low Energy (BLE)/ Bluetooth classic (BT)

Bei der Bluetooth-Kommunikation wird das 2.4 GHz Frequenzband in Channels eingeteilt. Bei BLE sind es 37 Kommunikations-Kanal und 3 Advertisement-Kanäle, während es bei BT insgesamt 79 Kanäle gibt. Alle Kanäle weisen unterschiedliche Eigenschaften insbesondere in Bezug auf die Mehrwegeausbreitung auf, was zu verschiedenen RSSI-Werten führt. Diesen Effekt bezeichnet man als Deep-Fading, der als Quelle für die Entropie der Kanaleigenschaften genutzt werden kann.

Die vereinfachte Programmstruktur, welche für BLE und BT angewendet wurde, ist in Abbildung 12 gezeigt. Nach dem Aufbau einer Verbindung zwischen den Kommunikationspartnern wird ein Timer mit 100msec gestartet. Nach dieser Zeit werden Daten in beide Richtungen ausgetauscht und den RSSI Wert beim Empfänger berechnet.

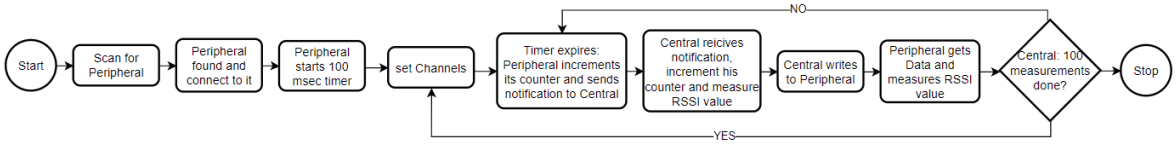

Abbildung 12: allgemeine Programmstruktur zur Messung von RSSI Werten von BLE und BT kommunikation

Um die verschiedenen Eigenschaften der Kanäle auszunutzen, wurden die Channels durch einen Algorithmus gezielt selektiert. Laut der Bluetooth Specification müssen bei BLE mindestens zwei Channels ausgewählt sein. Der Algorithmus selektiert daher immer zwei benachbarte Channels (Channel 0 und 1; anschließend Channel 1 und 2 …). Von jedem Kanalpaar werden 100 RSSI-Messungen durchgeführt. Bei BT müssen mindestens 20 Channels selektiert sein.

Die Messungen wurden u.a. in einer HF-Kammer durchgeführt, um störenden Signalen (aktive Interferenz durch WiFi oder andere elektronische Geräte) und Mehrwegeausbreitung zu vermeiden, bzw. kontrollieren zu können. Die Messungen wurden unter verschiedenen Bedingungen durchgeführt:

- Der Abstand der Kommunikationspartner beträgt immer 1 m.
- Es wurden zwei Platten vertikal und parallel zum direkten Kommunikationsweg mit einem Abstand von 10 cm bzw. 50 cm
- Absorber zwischen den Kommunikationspartnern
- WiFi load Test auf Channel 6 (Bandbreite: 20MHz)

Der Aufbau einer Messung ist in Abbildung 13 gezeigt.

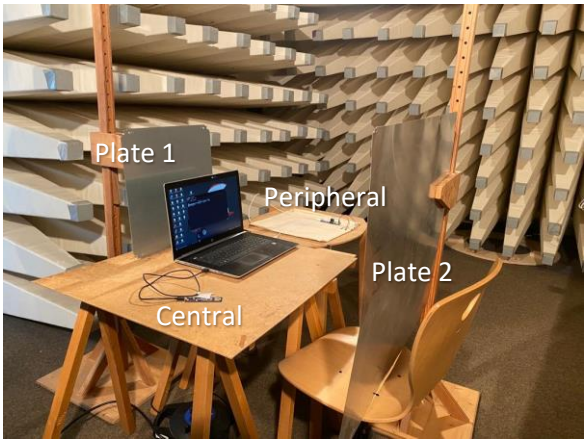

Abbildung 13: Beispielhafter Messaufbau zur Bestimmung der RSSI-Werte

Die gemessenen RSSI Werte werden über USB-UART an einen Laptop weitergeleitet und gespeichert. In Abbildung 14 ist ein beispielhaftes Messergebnis gezeigt.

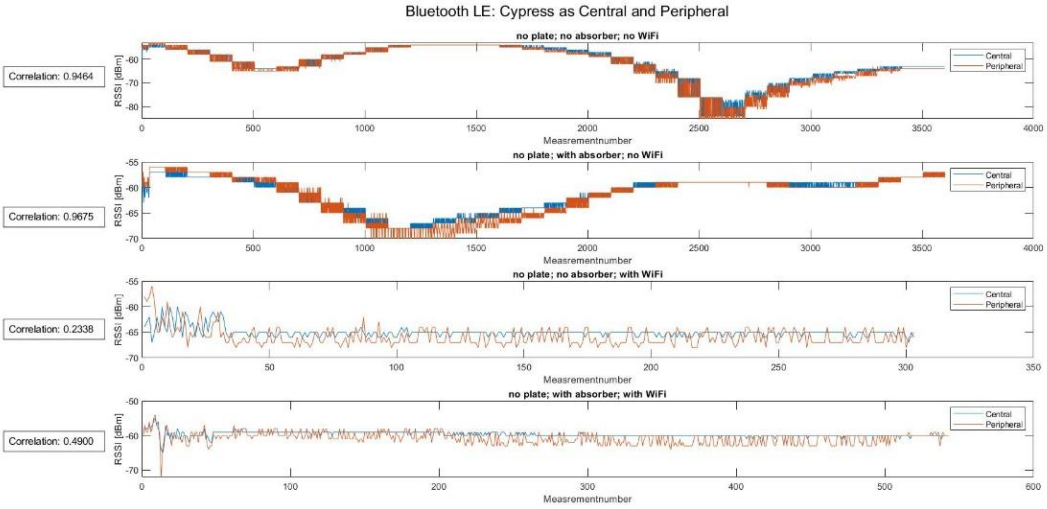

Abbildung 14: RSSI Messung einer BLE Kommunikation

01. Januar 2022 – 31. Dezember 2022

Wir haben die folgenden Sicherheitsanforderungen für das System definiert:

- Mutual Authentication: Das Schlauchsystem und der Host müssen ihre Identität nachweisen.
- Privacy: Die Identität des Schlauchsystems und des Hosts bleibt geheim.
- Data confidentiality: Die übermittelten Daten, d. h. der Temperaturwert, bleiben geheim.
- Data availability: Das Schlauchsystem muss in der Lage sein, bei Bedarf Temperaturdaten zu übertragen.
- Data integrity: Die Integrität der übertragenen Temperaturdaten muss gewährleistet sein.

Der Prozess der gegenseitigen Authentifizierung ist in Abbildung 15 beschrieben. Jede Einheit hat einen ID-Wert: PUF-ID für den Schlauch und eine Pre-Shared-ID für den Host. Diese ID-Werte sind eindeutig und konstant und dürfen daher nicht offengelegt werden. Sie werden mit dem gemeinsamen Sitzungsschlüssel verschlüsselt. Dieser Sitzungsschlüssel wird durch unseren drahtlosen Schlüsselgenerierungsalgorithmus erzeugt. Der Sitzungsschlüssel wird auch für die Ende-zu-Ende-Verschlüsselung der LIN-Kommunikation verwendet, um die Vertraulichkeit der Daten zu gewährleisten.

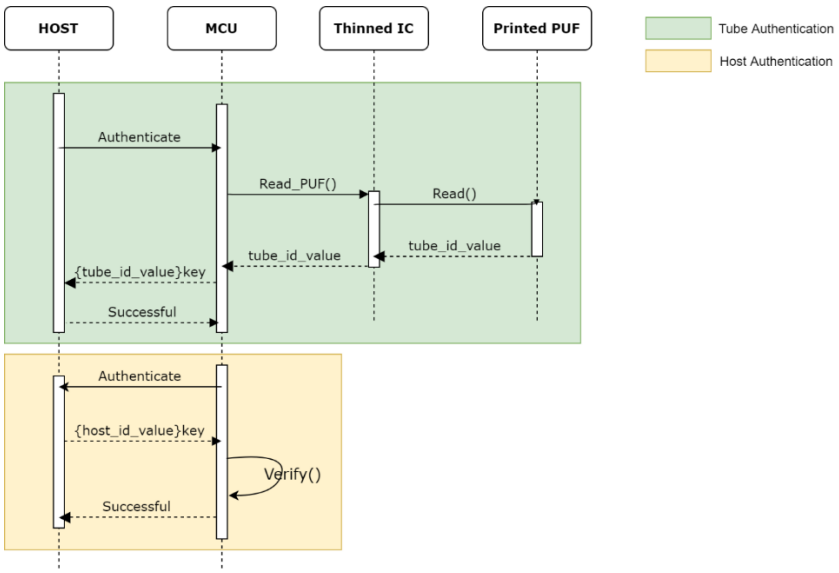

Abbildung 15: Mutual Authentication

Die gemeinsame Schlüsselgenerierung zauf der Grundlage drahtloser Kommunikation nutzt die einzigartigen Kanaleigenschaften zur Schlüsselgenerierung. Wie in unserem vorherigen Projektbericht beschrieben, haben wir den Received Signal Strength Indicator (RSSI) als Entropiequelle für unseren

Schlüsselgenerierungsalgorithmus gewählt. Wir haben uns mit zwei drahtlosen Kommunikationsprotokollen beschäftigt, die sich durch außerordentlich geringe Kosten sowie eine geringe Energieaufnahme auf Geräteseite auszeichnen: RFID und Bluetooth.

Um das Schutzziel der Vertraulichkeit zu gewährleisten, dass sicherheitsrelevante Daten nicht von Unbefugten gelesen werden können, müssen die Daten mit kryptografischen Verfahren verschlüsselt werden. Bei symmetrischen Verfahren wird ein gemeinsamer Schlüssel für diese Verschlüsselung verwendet. Ein weiteres Schutzziel ist die Authentisierung als Nachweis der korrekten Identität der Teilnehmer.

Abbildung 16 fasst die Schritte der Schlüsselerzeugung, der gegenseitigen Authentifizierung und des Auslesens der Temperatursensoren des Demonstrators zusammen.

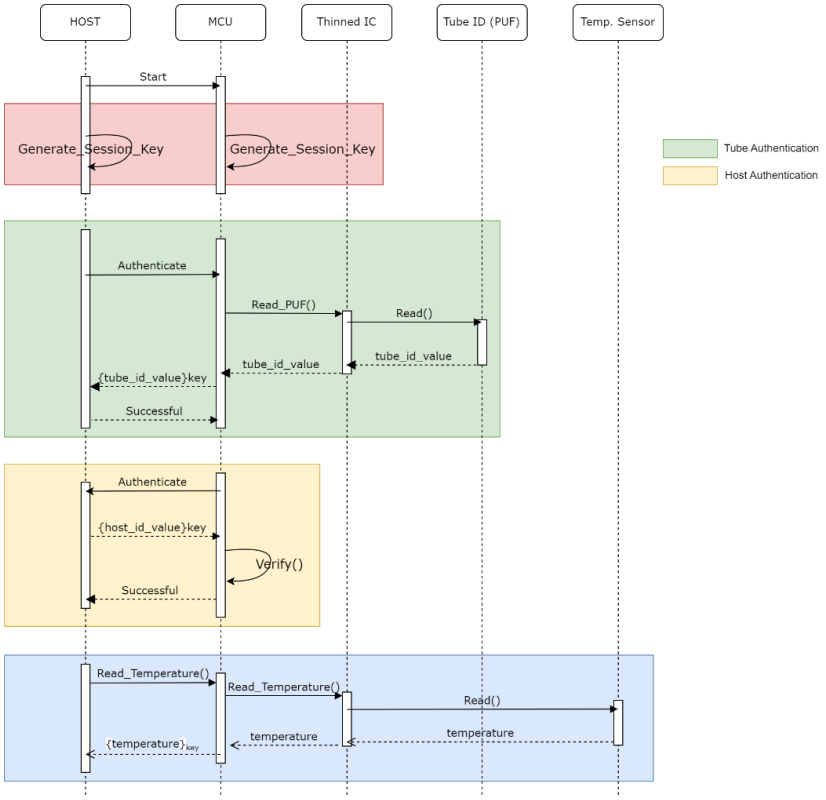

Abbildung 16: Zusammenfassendes Sequenzdiagramm des Demonstrators

RFID

Wir haben uns für das am häufigsten kommerziell genutzte Protokoll NFC entschieden, das auf der Frequenz 13,56 MHz und meist nur über kurze Entfernungen (< 10 cm) betrieben wird. Nachdem wir die Eigenschaften der getesteten Geräte gründlich untersucht hatten, stellten wir fest, dass es bei NFC inhärente Einschränkungen gibt, die es unmöglich machen, Entropie aus der NFC-Kommunikation abzuleiten. Bei NFC gibt es ein Lesegerät und ein Etikett. Das Lesegerät sendet ein Signal aus, das die Kommunikationskarriere darstellt, und versorgt das Etikett durch ein elektromagnetisches Feld mit Strom. Wenn das Signal stark genug ist, um den internen Chip des Tags mit Strom zu versorgen, moduliert es die Laufbahn, und das Lesegerät erkennt diese Modulation und liest die Daten. Zunächst einmal funktioniert das Signal nur über eine sehr kurze Distanz und ist sehr schwach. Wenn man mit normalen Laboroszilloskopen die Signalschwankungen an den Antennen des Lesegeräts und des Tags misst, werden die ursprünglichen Signale abgeschwächt. Die Verwendung eines logarithmischen Verstärkers (AD8310) an der Antenne des Tags führt ebenfalls zu einem starken Rauschen im Signal. Außerdem ist es unrealistisch, sie im Inneren dem Schlauch zu installieren, da der Abstand zwischen

Lesegerät und Tag kurz sein muss, um RSSI-Änderungen zu erhalten. Zusammenfassend lässt sich sagen, dass die subtilen Änderungen in der Signalstärke im verrauschten Tag-Signal verloren gehen würden und nicht genug Entropie aus einer statischen Installation im Inneren dem Schlauch gewonnen werden könnte, weshalb wir NFC für unseren Anwendungsfall der Schlüsselgenerierung ausschließen. Andere RFID-Technologien wurden diskutiert, aber das Bluetooth-Protokoll zeigte gute und vielversprechende Ergebnisse, so dass wir beschlossen, in diese Richtung weiterzugehen.

Bluetooth Low Energy (BLE)/ Bluetooth classic (BT)
Wie in unserem vorherigen Bericht gezeigt, nutzt die Bluetooth-Kommunikation das 2,4-GHz-IMS-Frequenzband, das in Kanäle unterteilt ist. Für BLE gibt es 37 Kommunikationskanäle und 3 Werbekanäle, während BT über insgesamt 79 Kanäle verfügt. Alle Kanäle haben unterschiedliche Eigenschaften, insbesondere in Bezug auf die Mehrwegeausbreitung, was zu unterschiedlichen RSSI-Werten führt. Dieser Effekt wird als Deep Fading bezeichnet und kann als Quelle für die Entropie der Kanaleigenschaften verwendet werden.

RSSI-Messungen können direkt über Software berechnet werden. Wir haben weitere Messungen in der HF-Kammer mit verschiedenen BT- und BLE-Geräten durchgeführt.

Abbildung 17 zeigt unser anfängliches Verfahren zur Schlüsselgenerierung mit Bluetooth:

- Herstellen der Verbindung zwischen den Geräten
- Senden/Empfangen von Daten auf jedem Kanal
- Messen Sie die RSSI-Werte
- Vorverarbeitung der RSSI-Werte (Kurvenanpassung, Approximation, ...)
- Quantisierung der RSSI-Werte
- Generierung des gemeinsamen Schlüssels anhand der extrahierten Punkte

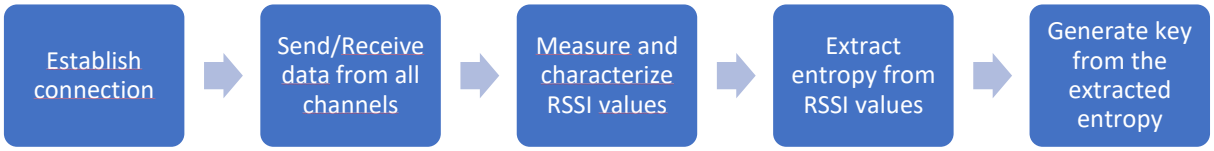

Abbildung 17: Generierung von Sitzungsschlüsseln

Abbildung 18 zeigt ein Beispiel für die Erzeugung von gemeinsamen Schlüsseln aus den RSSI-Wertekurven.

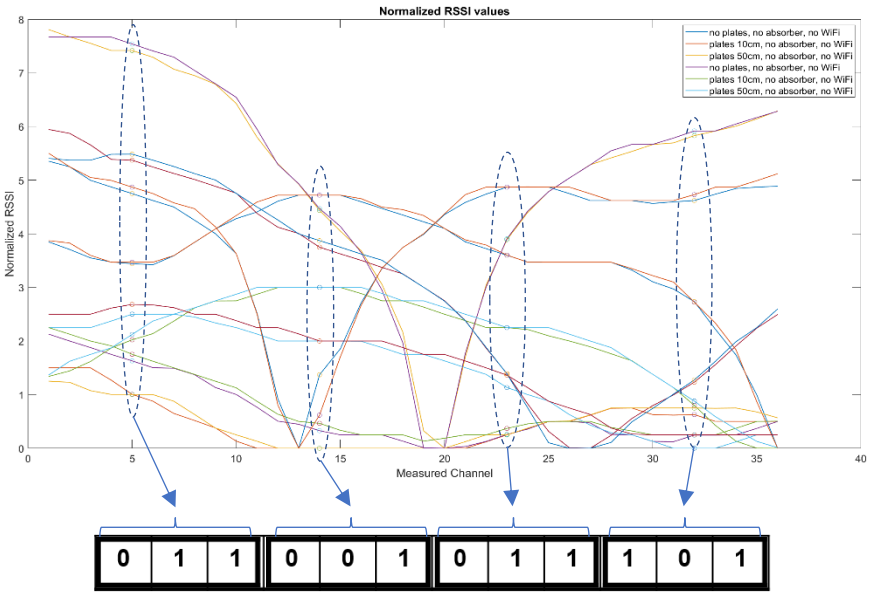

Abbildung 18: Beispiel für die Generierung von Sitzungsschlüsseln

Wir haben die RSSI-Messungen in der RF-Kammer mit den folgenden Gerätekonfigurationen durchgeführt:

- BT:
  - 2 x **BT122 Dual-Mode BR/EDR** von Silicon Labs.
- BLE:
  - 2 x **PSoC™ 6 BLE Prototyping Kit** von Cypress.
  - 1 x **BT122 Dual-Mode BR/EDR** und 1 x **PSoC™ 6 BLE Prototyping Kit.**

Abbildung 19 zeigt ein Beispiel für den Aufbau in der HF-Kammer in der HSO.

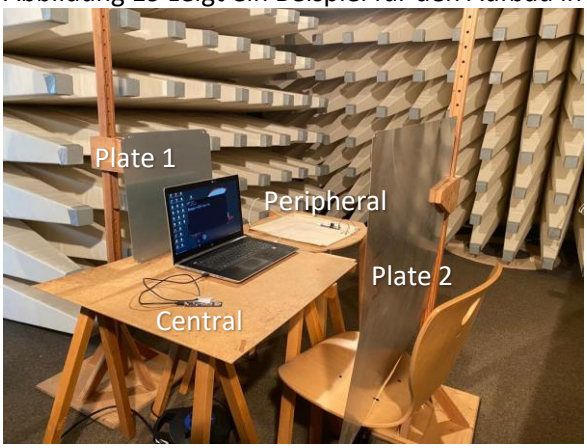

Abbildung 19: Beispielhafter Messaufbau zur Bestimmung der RSSI-Werte

Wir fügten einige Variationen in der drahtlosen Ausbreitungsumgebung hinzu, indem wir verschiedene Gerätepositionen, Reflektoren, Absorber und Störungen verwendeten. Wir führten Messungen auf allen BT- und BLE-Kanälen durch und verglichen die Korrelation der RSSI-Messungen der beiden Geräte. Anschließend sammelten wir die Daten und verarbeiteten sie vor. Abbildung 20 zeigt die BT-RSSI-Kurven Abbildung 21 und Abbildung 11 zeigt die BLE-RSSI-Kurven.

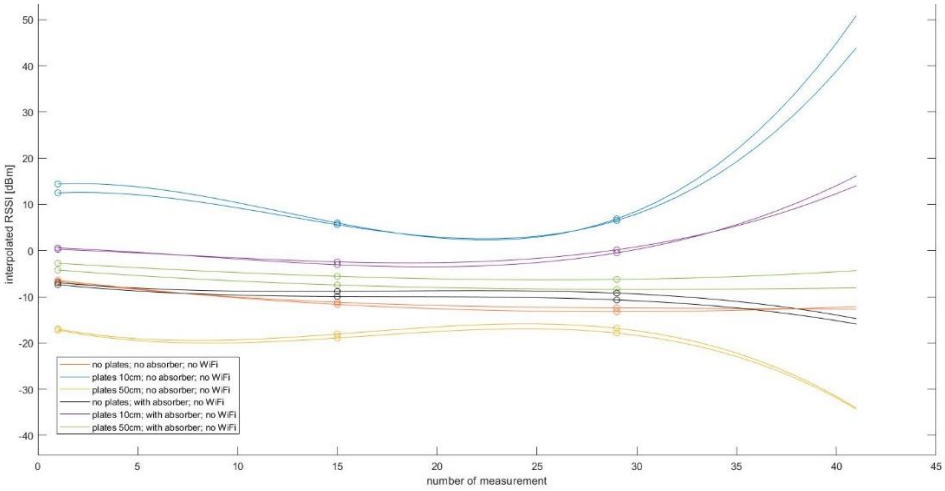

Abbildung 20: BT-RSSI-Kurven

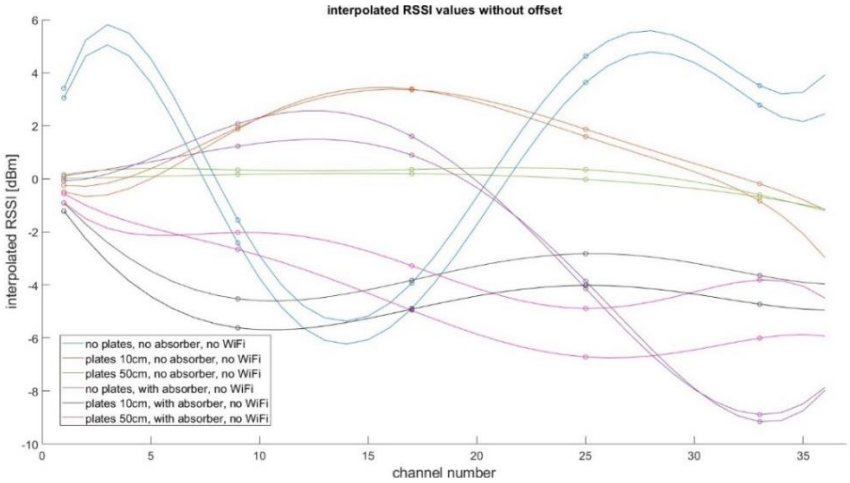

Abbildung 21: BLE-RSSI-Kurven

Abbildung 22 zeigt die Korrelation der BT-RSSI-Werte und Abbildung 23 zeigt die Korrelation der BLE-RSSI-Werte. Die Korrelation r zwischen den Messungen wird anhand der folgenden Gleichung berechnet, wobei cov(Meas1, Meas2) die Kovarianz zwischen zwei Messungen Meas1 und Meas2 und σ_{Meas1} und σ_{Meas2} die Standardabweichungen von Meas1 und Meas2 sind.

$$r = \frac{cov(Meas1, Meas2)}{\sigma_{Meas1} * \sigma_{Meas2}}$$

	BT; NP; NA; NW	BT; P10; NA; NW	BT; P50; NA; NW	BT; NP; A; NW	BT; P10; A; NW	BT; P50; A; NW
BT; NP; NA; NW	1	0,948	0,212	0,999	0,338	0,9998
BT; P10; NA; NW	0,948	1	0,511	0,962	0,619	0,954
BT; P50; NA; NW	0,212	0,511	1	0,257	0,991	0,230
BT; NP; A; NW	0,999	0,962	0,257	1	0,380	0,9996
BT; P10; A; NW	0,338	0,619	0,991	0,380	1	0,355
BT; P50; A; NW	0,9998	0,954	0,230	0,9996	0,35491	1

Abbildung 22: Korrelation der BT-RSSI-Werte

	Cy; NP; NA; NW	Cy; P10; NA; NW	Cy; P50; NA; NW	Cy; NP; A; NW	Cy; P10; A; NW	Cy; P50; A; NW	BtCy; NP; NA; NW	BtCy; P10; NA; NW	BtCy; P50; NA; NW	BtCy; NP; A; NW	BtCy; P10; A; NW	P50; A; NW
Cy; NP; NA; NW	1	-0,250	0,871	-0,639	0,673	0,477	0,534	-0,496	-0,575	-0,564	0,325	-0,163
Cy; P10; NA; NW	-0,250	1	-0,338	0,752	-0,698	0,326	-0,589	0,627	0,321	0,234	-0,869	-0,407
Cy; P50; NA; NW	0,871	-0,338	1	-0,710	0,684	0,070	0,368	-0,225	-0,307	-0,367	0,199	-0,304
Cy; NP; A; NW	-0,639	0,752	-0,710	1	-0,991	0,267	-0,664	0,554	0,527	0,536	-0,675	0,131
Cy; P10; A; NW	0,673	-0,698	0,684	-0,991	1	-0,185	0,697	-0,597	-0,596	-0,599	0,677	-0,150
Cy; P50; A; NW	0,477	0,326	0,070	0,267	-0,185	1	0,147	-0,332	-0,345	-0,235	-0,016	0,225
BtCy; NP; NA; NW	0,534	-0,589	0,368	-0,664	0,697	0,147	1	-0,935	-0,947	-0,911	0,860	-0,128
BtCy; P10; NA; NW	-0,496	0,627	-0,225	0,554	-0,597	-0,332	-0,935	1	0,884	0,771	-0,917	-0,205
BtCy; P50; NA; NW	-0,575	0,321	-0,307	0,527	-0,596	-0,345	-0,947	0,884	1	0,974	-0,697	0,249
BtCy; NP; A; NW	-0,564	0,234	-0,367	0,536	-0,599	-0,235	-0,911	0,771	0,974	1	-0,585	0,457
BtCy; P10; A; NW	0,325	-0,869	0,199	-0,675	0,677	-0,016	0,860	-0,917	-0,697	-0,585	1	0,323
BtCy; P50; A; NW	-0,163	-0,407	-0,304	0,131	-0,150	0,225	-0,128	-0,205	0,249	0,457	0,323	1

Abbildung 23: Korrelation der BLE-RSSI-Werte

Die Ergebnisse zeigen, dass es bei Bluetooth Classic eine starke Korrelation zwischen Messungen gibt, die in unterschiedlichen drahtlosen Umgebungen durchgeführt wurden. Dies führt zu sehr ähnlichen generierten Schlüsseln, die u.U. zu schwach und anfällig für Angriffe sein könnten. Die BLE-RSSI-Messungen sind dagegen weniger korreliert und können bei leichten Abweichungen in der Funkumgebung zu unterschiedlichen Schlüsseln führen. Dies kann durch die höhere Bandbreite von BLE (2 MHz) im Vergleich zur Bandbreite von BT (1 MHz) verursacht werden. Die höhere Bandbreite bietet mehr Raum für die Fading-Effekte und die Schwankungen des RSSI. Aus diesem Grund haben wir uns entschieden, BLE für die gemeinsame Schlüsselgenerierung zu verwenden.

Unter Verwendung der BLE-Messungen in der RF-Kammer bestand unser nächster Schritt darin, die RSSI-Werte vorzuverarbeiten und zu quantisieren und sie in Bits zu kodieren, um verschiedene gemeinsame Schlüssel zu erzeugen. Anschließend haben wir die Schlüssel mit statistischen Analysemethoden untersucht, um die Eindeutigkeit und Zuverlässigkeit zu ermitteln. Die Zuverlässigkeit der Schlüsselgenerierung bestimmt, wie oft derselbe gemeinsame Schlüssel auf beiden Geräten unter verschiedenen Umgebungsbedingungen generiert werden kann. Die Einzigartigkeit der Schlüssel misst, wie gut sich ein einzelner gemeinsamer Schlüssel von anderen Schlüsseln unterscheidet, die unter verschiedenen Umgebungsbedingungen erzeugt wurden. Abbildung 24 und Abbildung 25 zeigen ein Beispiel für die Eindeutigkeit von 8 gemeinsam genutzten Schlüsseln auf dem Host und auf der Tube (Idealwert ist 0,5). zeigt die Zuverlässigkeit dieser Schlüssel (Idealwert ist 1).

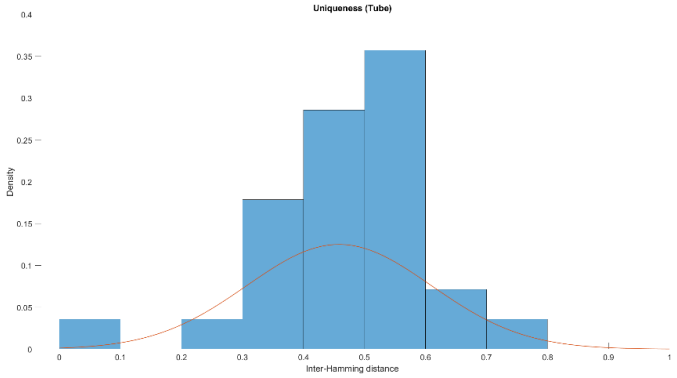

Abbildung 24: Einzigartigkeit von 8 Schlüsseln (Schlauch)

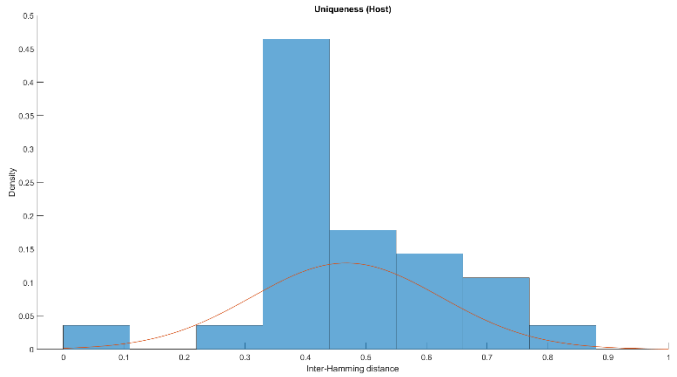

Abbildung 25: Einzigartigkeit von 8 Schlüsseln (Host)

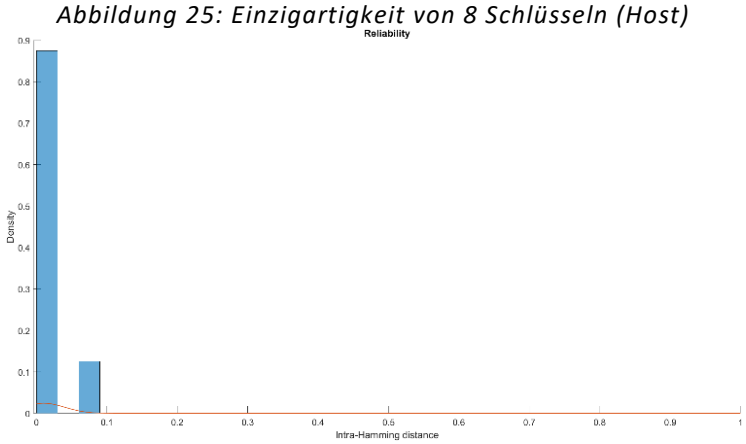

Abbildung 26: Verlässlichkeit der 8 Schlüssel

Wir haben festgestellt, dass wir gute erste Ergebnisse erzielt haben, aber noch einiges an Arbeit vor uns liegt. Unsere nächsten Schritte werden darin bestehen, die Zuverlässigkeit des

Schlüsselgenerierungsalgorithmus zu verbessern, indem wir weitere Vorverarbeitungs-, Quantisierungs-, Kodierungs- und Fehlerkorrekturalgorithmen erforschen.

01. Januar 2023 – 31. Dezember 2023

In diesem diesem Zeitraum haben wir an mehreren Aspekten des Projekts gearbeitet. Die erste Facette ist der Algorithmus zur gemeinsamen Schlüsselgenerierung aus der Bluetooth Low-Energy Signalstärke. Der zweite Teil ist die Hardware-Integration, Software-Entwicklung und das Testen der verschiedenen Komponenten des Systems. Die dritte Facette sind unsere Aktivitäten bei der Entwicklung des endgültigen Demonstrators für SensIC.

Verbesserungen des Algorithmus zur Generierung des Shared Key

Der bereits etablierte Algorithmus zur Erzeugung gemeinsamer Sitzungsschlüssel wurde weiterentwickelt und getestet. In einer ersten Testreihe wollten wir die Zuverlässigkeit der erzeugten Schlüssel prüfen. Wir haben den zuvor definierten Algorithmus zur Schlüsselgenerierung verwendet, um einen Datensatz von Sitzungsschlüsselpaaren zu erzeugen und ihre Leistung zu analysieren. Abbildung 27 zeigt 255 RSSI-Messungen, die über einen Zeitraum von 1,5 Tagen in einer stationären Position gesammelt wurden.

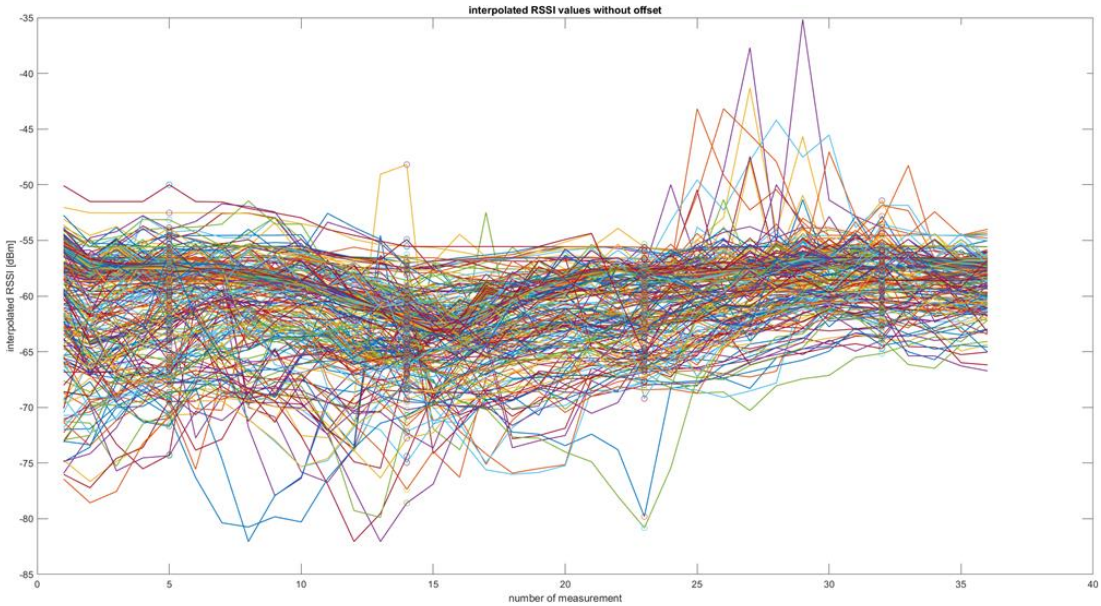

Abbildung 27: 255 Messungen, die für die Analyse der Schlüsselerzeugung verwendet werden

Mit diesen Daten haben wir den Algorithmus zur Schlüsselerzeugung ausgeführt, um 255 Schlüsselpaare zu erhalten. Die Zuverlässigkeit dieser Schlüssel, wie im vorherigen Bericht definiert, wurde wie in Abbildung 28 dargestellt analysiert.

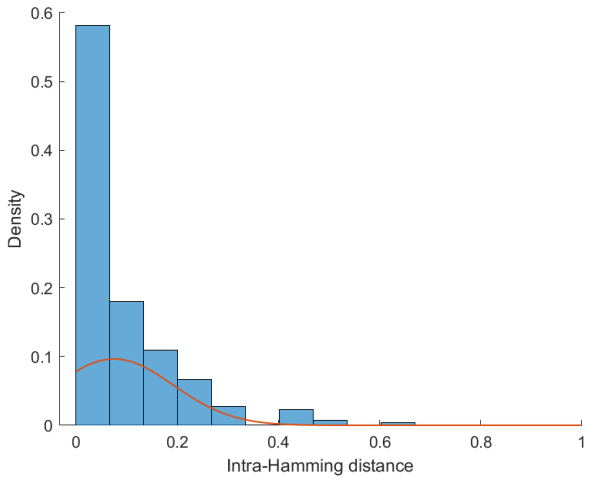

Abbildung 28: Verlässlichkeit der 255 Schlüsselpaare

Da diese Schlüssel für die symmetrische Verschlüsselung verwendet werden, müssen sie auf beiden Geräten, der Tube und dem Host, identisch sein. Das bedeutet, dass die Zuverlässigkeit immer gleich 1 sein muss, was hier nicht der Fall ist.

Dieser Effekt wird durch einen Offset zwischen den RSSI-Werten des Tube-BLE-Moduls und des Host-BLE-Moduls verursacht. Dieser Versatz ist zwischen den verschiedenen BLE-Kanälen variabel und daher schwer zu korrigieren. Um dieses Problem zu lösen, haben wir verschiedene Methoden eingesetzt. Wir konzentrierten uns auf den Schritt der Vorverarbeitung. In diesem Schritt haben wir versucht, den Offset vor der Quantisierung zu eliminieren. Es wurden verschiedene Methoden verwendet, darunter:

- Angleichung der Daten wie in Abbildung 29.

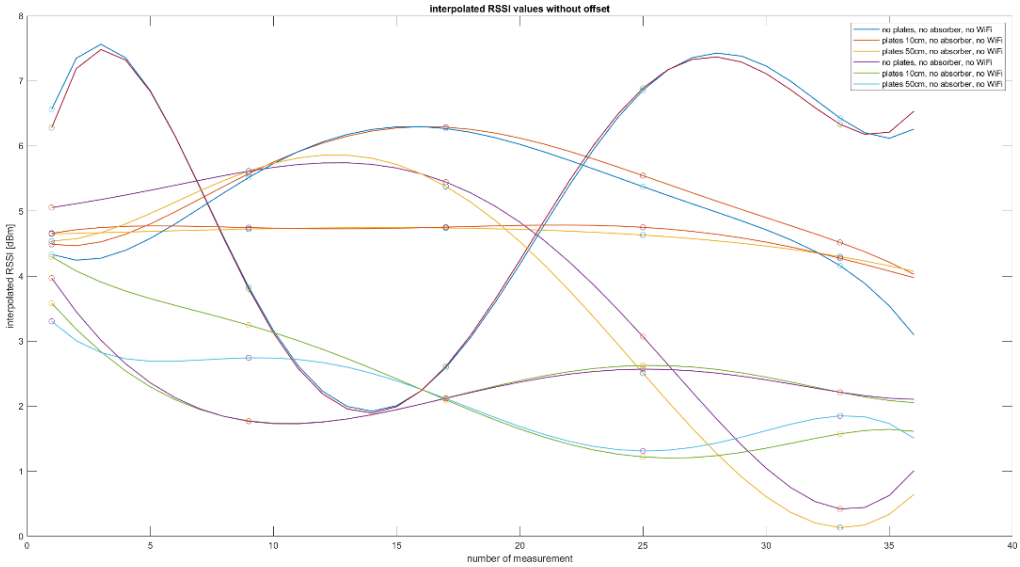

Abbildung 29: Angleichung der Daten

- Interpolation der Daten mittels Spline-Interpolation wie in Abbildung 30.

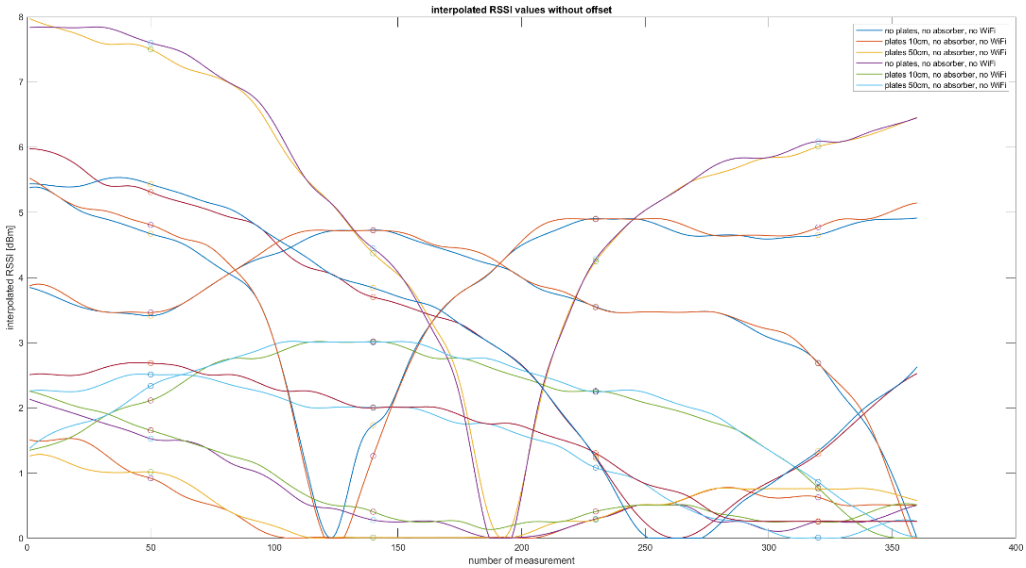

Abbildung 30: Dateninterpolation mit Splines

Diese Methoden waren jedoch nicht in der Lage, die Abweichungen zwischen den RSSI-Daten der beiden Geräte zu korrigieren und vollständig zu beseitigen. Wir kamen zu dem Schluss, dass wir unseren Schlüsselgenerierungsalgorithmus verbessern müssen.

Unser neuer Schlüsselgenerierungsalgorithmus, der in Abbildung 31 dargestellt ist, umfasst zwei neue Schritte: Informationsabgleich und Verstärkung der Privatsphäre.

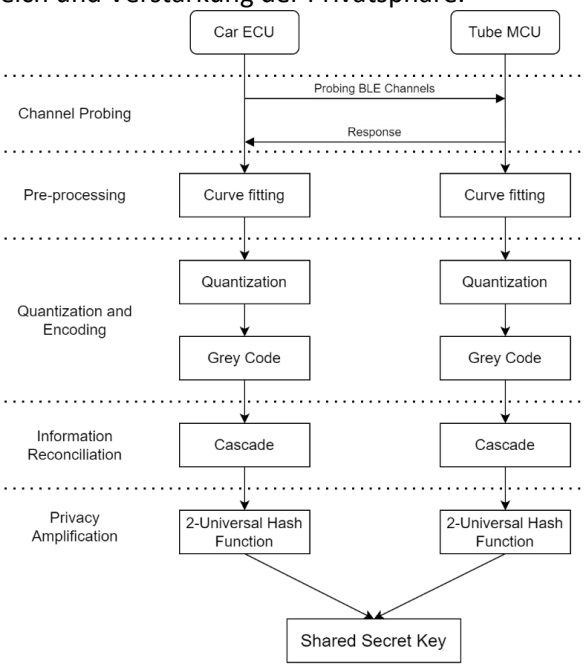

Abbildung 31: Verbesserter Algorithmus zur Generierung des Session Key

Der Informationsabgleich ist ein Schritt der Fehlerkorrektur. Er beseitigt die Fehler im Schlüsselpaar, das durch die Quantisierung entstanden ist. In unserem Algorithmus haben wir uns für den Kaskadenalgorithmus entschieden, einen Algorithmus zur Fehlererkennung und -korrektur. Bei diesem Algorithmus durchlaufen die Schlauch- und die Host-Geräte ihre Schlüssel, um die fehlerhaften Bits zu identifizieren und sie umzudrehen. Während dieser Iterationen werden die ursprünglichen geheimen Schlüssel nicht über den öffentlichen Kanal diskutiert. Stattdessen werden die Schlüssel gemischt und in Blöcke zerlegt. Die Geräte berechnen die Parität (basierend auf der Anzahl des Nullens und Einsen) und tauschen die Mischinformationen und die Parität untereinander aus. Liegt ein Paritätsfehler vor, wird

eine kleinere Teilmenge des Schlüsselblocks erstellt und getestet, bis der Fehler gefunden und behoben ist. Dieser Algorithmus ist in Abbildung 32 dargestellt.

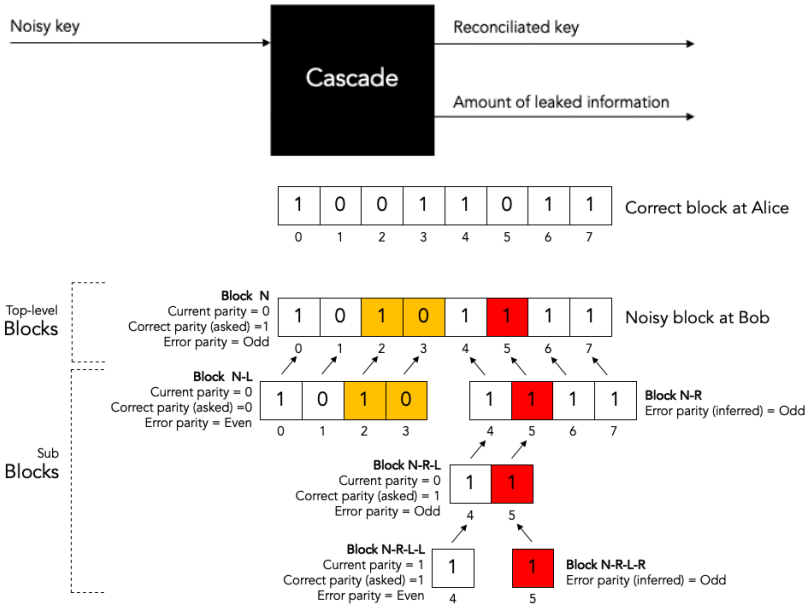

Abbildung 32: Cascade-Algorithmus

Dieser Algorithmus wurde auf der Schlauch-MCU und der Host-MCU implementiert und war bei der Korrektur der Bitfehler erfolgreich. Dieser Algorithmus führt jedoch dazu, dass eine gewisse Menge an Informationen über den Schlüssel durchsickert. An dieser Stelle kommt der Schritt der Privacy Amplification ins Spiel. Bei diesem Schritt werden universelle Hash-Funktionen verwendet, um die Schlüssel zu hacken und zu vervielfältigen. Selbst wenn ein Angreifer in der Lage wäre, einige Informationen über den ursprünglichen Schlüssel in Form von Bits zu erhalten, würde der endgültige Schlüssel ganz anders aussehen und wäre unmöglich abzuleiten. Dieser Schritt befindet sich zum Zeitpunkt der Erstellung dieses Berichts noch in der Entwicklung.

Hardware-Integration und Software-Entwicklung

Für den ASIC, den Temperatursensor und die PUF-Integration haben wir die erforderlichen Softwaremodule in der STM32F7 MCU im Schlauch entwickelt. Die Schlauch-MCU kann mit dem ASIC über eine serielle Peripherieschnittstelle (SPI) kommunizieren. Über diese SPI-Schnittstelle kann die MCU die Messwerte des Temperatursensors und den gedruckten PUF vom ASIC auslesen. Abbildung 33 zeigt den Ausgang des Temperatursensors und den vom ASIC während der Debugging-Phase ausgelesenen PUF.

```
================== PUF Key Generation ==================
PUF key: 1 1 0 1 0 1 1 1 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 1 1 0 0 0 0 1 0 1 0 0 0
================== END ==================
================== Temperature Measurements ==================
cnt_valid: 1
gain: 0
itrim: 0
tfe: 1
cnt_val: 42220
cnt_valid: 1
gain: 0
itrim: 0
tfe: 2
cnt_val: 58626
================== PUF Key Generation ==================
PUF key: 1 1 0 1 0 1 1 1 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 0 0 0 0 0 1 0 1 0 0 0
================== END ==================
================== Temperature Measurements ==================
cnt_valid: 1
gain: 0
itrim: 0
tfe: 1
cnt_val: 42225
cnt_valid: 1
gain: 0
itrim: 0
tfe: 2
cnt_val: 58626
================== PUF Key Generation ==================
PUF key: 1 1 0 1 1 1 1 1 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 1 0 1 0 0 0 0 1 0 1 0 0 0
================== END ==================
================== Temperature Measurements ==================
cnt_valid: 1
gain: 0
itrim: 0
tfe: 1
cnt_val: 42222
cnt_valid: 1
gain: 0
itrim: 0
tfe: 2
cnt_val: 58619
================== PUF Key Generation ==================
PUF key: 1 1 0 1 1 1 1 1 0 0 0 0 0 0 0 0 1 0 0 0 0 1 0 0 0 0 0 0 0 0 1 0 0 0 0 1
================== END ==================
```

Abbildung 33: Temperatursensor und PUF Fehlerbehebung

Die PUF Challenge-Reponse Pairs (CRPs) wurden in enger Zusammenarbeit mit unseren Kollegen am KIT programmiert. In dieser Phase haben wir festgestellt, dass es beim Lesen der PUFs Bitflips gibt. Daraufhin haben wir alle möglichen Eingangsspannungen des PUF getestet und die Daten an das KIT übermittelt. Die Fehlersuche ist zum Zeitpunkt des Berichts noch nicht abgeschlossen.
Die Messungen des Temperatursensors wurden von einem Zeitzähler auf dem ASIC gelesen. Um den Zählerwert in die Temperatur in Celsiusgraden umzuwandeln, muss dieser Zählerwert für jeden spezifischen Temperatursensor und den zugehörigen ASIC und die Hardware gemessen werden. Daher wird dieser Schritt zu einem späteren Zeitpunkt im Projektablauf erfolgen.

01. Januar 2024 – 30. April 2024

Nach erfolgreicher Ausführung des Kaskadenalgorithmus teilen sich die Tube-MCU und die Host-MCU denselben geheimen Schlüssel. Während des Austauschs von Bitparitätsinformationen beim Informationsabgleich zwischen den Geräten über den unsicheren Kanal werden einige Informationen über die Schlüssel preisgegeben. Eines der ermittelten Sicherheitsrisiken besteht darin, dass ein Angreifer, der den Kanal abhören kann, diese Informationen sammeln und auswerten kann. Auch wenn die Informationen vielleicht nicht ausreichen, um den gesamten Schlüssel zu rekonstruieren, kann der Angreifer mit genügend Zeit Teile des Schlüssels herausfinden und systematische Muster in statischen Umgebungen erkennen. Um dies zu verhindern, wird Privacy Amplification eingesetzt. Der BLE-basierte Schlüssel wird mit einer zufällig generierten Matrix (aus einem gemeinsamen Seed) gehasht und in einen neuen, vollständig sicheren 256-Bit langen Schlüssel umgewandelt.
Um die Sicherheit der generierten Schlüssel zu bewerten, haben wir die Tube und die Host-MCUs in eine physisch statische Umgebung (Bürotisch mit normalen 2,4-GHz-Wi-Fi- und Bluetooth-Interferenzen) gestellt und den Schlüsselgenerierungsalgorithmus 8000 Mal laufen lassen. Anschließend haben wir die erzeugten Bits in die NIST Statistical Test Suite eingegeben, um die Zufälligkeit der Schlüssel zu testen. Wie in Tabelle 1 dargestellt, bestanden alle Tests den erforderlichen 8/10-Anteil mit akzeptablen p-values.

Test	Acceptable P-Value	P-Value	Proportion
Approximate Entropy	≥ 0.05	0.739918	10/10
Frequency	≥ 0.05	0.350485	10/10
Block Frequency	≥ 0.05	0.739918	10/10
Cumulative Sums	≥ 0.05	0.911413	10/10
Runs	≥ 0.05	0.350485	10/10
Longest Run of Ones	≥ 0.05	0.534146	10/10
Rank	≥ 0.05	0.122325	10/10
FFT	≥ 0.05	0.911413	10/10
Serial	≥ 0.05	0.911413	10/10

Tabelle 1: NIST Statistical Test Suite Ergebnisse

Wie in Abbildung 16 dargestellt, wird der BLE-Schlüssel generiert und für die Verschlüsselung der PUF-ID sowie der restlichen Temperaturdaten verwendet. Abbildung 34 zeigt den endgültigen Demonstratoraufbau mit dem PUF-Schlüssel, dem BLE-basierten Schlüssel und den Temperaturmessungen.

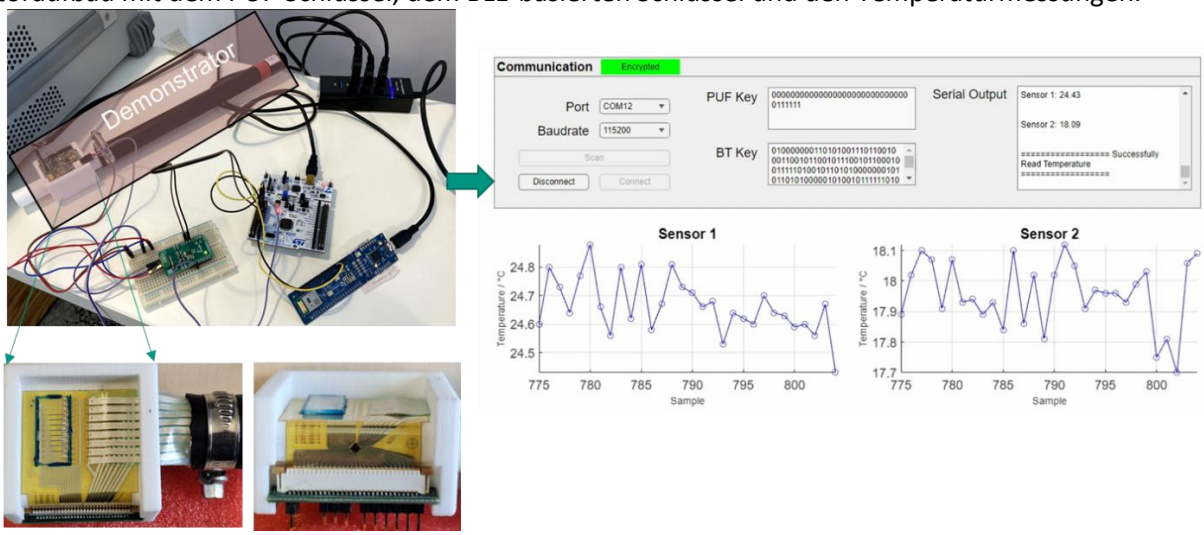

Abbildung 34: Endgültiger Demonstrator, der verschlüsselte Temperaturdaten mit einer Host-MCU kommuniziert. Ein Laptop erfasst die Ausgabe des Hosts und zeigt den PUF-Schlüssel sowie den aktuellen BLE-Schlüssel und die Temperatur an.

2. Die wichtigsten Positionen des zahlenmäßigen Nachweises

Ausgabearten (gesamt)	ZUW gesamt	AUS anerkannt	in %	noch verfügbar
812 E12 bis E15	0,00 €	0,00 €	0,00%	0,00 €
817 E1 bis E11	180.450,00 €	182.826,91 €	102,45%	-2.376,91 €
820 Lohnempfänger(innen) MTArb	0,00 €	0,00 €	0,00%	0,00 €
822 Beschäftigungsentgelte	0,00 €	0,00 €	0,00%	0,00 €
831 Gegenstände bis 800 €	0,00 €	0,00 €	0,00%	0,00 €
834 Mieten und Rechnerkosten	0,00 €	0,00 €	0,00%	0,00 €

835 Vergabe von Aufträgen	0,00 €	0,00 €	0,00%	0,00 €
843 Sonst. Verwaltungsausgaben	3.000,00 €	1.865,80 €	62,19%	1.134,20 €
846 Dienstreisen	6.000,00 €	3.218,63 €	53,64%	2.781,37 €
850 Gegenstände über 800 €	0,00 €	0,00 €	0,00%	0,00 €
gesamt	189.450,00 €	187.911,34 €	99,19%	1.538,66 €

3. Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die durchgeführten Arbeiten waren notwendig und angemessen, um die technischen Herausforderungen des Projekts zu bewältigen und die gewünschten Ergebnisse zu erzielen. Insbesondere die Entwicklung des Demonstrators, der mit einem geheimen gemeinsamen Schlüssel auf der Grundlage drahtloser Kommunikation und physikalisch nicht verschlüsselbarer Funktionen gesichert wurde, war entscheidend für die erfolgreiche Umsetzung der Projektziele. Die Integration des STM32F746-Mikrocontrollers, des gedruckten PUF-Kerns und des Temperatursensors sowie die Entwicklung von Softwaremodulen für die verschlüsselte Kommunikation und die Datenauswertung zeigten die technische Machbarkeit und Innovation des Projekts. Die sorgfältige Auswahl der Technologien, wie z.B. die Verwendung von BLE zur Schlüsselgenerierung auf Basis von RSSI-Werten und die Integration von gedruckten PUFs und Temperatursensoren auf flexibler Folie, waren notwendig, um die hohen Sicherheitsanforderungen zu erfüllen.

Die Anpassung und Optimierung von Kommunikationsprotokollen, drahtlosen Schnittstellen und der Hardware-Integration waren angemessen, um die Zuverlässigkeit der Ergebnisse zu gewährleisten. Die durchgeführten Tests und Kalibrierungen, wie z. B. die Validierung von Temperatursensoren und PUFs, haben den Projektfortschritt deutlich vorangetrieben. Zwar waren geringfügige Abweichungen vom ursprünglichen Plan erforderlich, wie z. B. die Anpassung der RSSI-Messungen und die Auswahl von BLE anstelle von RFID, doch waren diese durch die spezifischen technischen Anforderungen gerechtfertigt und führten zu einer effizienteren Lösung. Insgesamt war die geleistete Arbeit sowohl notwendig als auch völlig angemessen im Hinblick auf die eingesetzten Ressourcen und die erzielten Ergebnisse im Rahmen der Projektziele.

4. Voraussichtlicher Nutzen und Verwertbarkeit des Ergebnisses im Sinne des fortgeschriebenen Verwertungsplans

Wirtschaftliche Erfolgsaussichten

-

Wissenschaftliche und technische Erfolgsaussichten

Die Ergebnisse in diesem Projekt bergen ein erhebliches Potenzial für künftige Anwendungen und die kommerzielle Nutzung. Die entwickelten Kerntechnologien, einschließlich der sicheren Schlüsselgenerierung auf der Grundlage von RSSI-Messungen und der Integration von Mikrocontrollern mit ASICs, bieten robuste Lösungen für die sichere Datenübertragung, Authentifizierung und Verschlüsselung in sensiblen Umgebungen. Die erfolgreiche Implementierung der Integration von gedruckten Physical Unclonable Functions (PUF) und Temperatursensoren zeigt die Machbarkeit der Entwicklung fortschrittlicher hybrider Sensorsysteme für Industrie- und Automobil- sowie IoT-Anwendungen.
Im Rahmen des Verwertungsplans werden sich die Projektpartner darauf konzentrieren, den Demonstrator zu verfeinern und in Zusammenarbeit mit der Industrie Markteintrittsstrategien zu untersuchen. Die fortschrittlichen Sicherheitsmechanismen, insbesondere im Bereich der verschlüsselten

Kommunikation und der sicheren Identifizierung, passen gut zu der wachsenden Nachfrage nach Cybersicherheit in vernetzten Geräten und positionieren die Projektergebnisse für eine starke zukünftige Marktakzeptanz und weitere Forschungsinitiativen.

Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

-

5. Während der Durchführung des Vorhabens dem ZE bekannt gewordener Fortschritt auf dem Gebiet des Vorhabens bei anderen Stellen

Das Projekt VE-FIDES wurde parallel zum Projekt Sens-IC entwickelt, und es war interessant zu sehen, wie sie einen mehrstufigen Fingerprinting-Ansatz entwickelten, um die Vertrauenswürdigkeit von Lieferketten zu verbessern.

6. Erfolgte oder geplante Veröffentlichungen des Ergebnisses nach Nr. 11

- Veröffentlichte Publikationen:
  - Scholz, A. et al. “Security Enhanced Hybrid Electronic System in Foil for Temperature Sensing” (IEEE IFETC)
- Geplante Veröffentlichungen:
  - Hadrich, W. et al. “Cryptographic key derivation using Bluetooth Low Energy channel entropy” (MDPI JCP).
  - Scholz, A. et al. "Hybrid System in Foil Containing Secure Identification and Temperature Sensing Units, " (IEEE ISCAS).